AX2200S/AX1250S/AX1240S Software Manual

Configuration Guide Vol. 2

For Version 2.4

AX1240S-S002X-70

AlaxalA

Relevant products

This manual applies to the AX2200S, AX1250S, and AX1240S series of switches. The manual describes the functionality of software version 2.4 for AX2200S, AX1250S, and AX1240S switches supported by the OS-LT4, OS-LT3, and OS-LT2 software and the optional licenses.

Export restrictions

In the event that any or all ALAXALA products (including technologies, programs and services) described or contained herein are controlled under any of applicable export control laws and regulations (including the Foreign Exchange and Foreign Trade Law of Japan and United States export control laws and regulations), such products shall not be exported without obtaining the required export licenses from the authorities concerned in accordance with the above laws.

Trademarks

- Ethernet is a registered trademark of Xerox Corporation.
- MagicPacket is a registered trademark of Advanced Micro Devices, Inc.
- Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and other countries.
- RSA and RSA SecurID are trademarks or registered trademarks of RSA Security Inc. in the United States and other countries.
- Wake on LAN is a registered trademark of IBM Corporation.
- Windows is a registered trademark of Microsoft Corporation in the United States and other countries.
- Other company and product names in this document are trademarks or registered trademarks of their respective owners.

Reading and storing this manual

Before you use the equipment, carefully read the manual and make sure that you understand all safety precautions.
After reading the manual, keep it in a convenient place for easy reference.

Notes

Information in this document is subject to change without notice.

Editions history

July 2012 (Edition 8) AX1240S-S002X-70

Copyright

History of Amendments

Ver. 2.4 (Edition 8)

Summary of amendments

Location and title	Changes
Addition of series	● A description of AX2200S was added.
5 Overview of Layer 2 authentication	The following were changed in the description in *Auto authentication mode accommodation at the same MAC port*: ● *Table 5-17 Actions corresponding to Tunnel-Private-Group-ID at RADIUS authentication* ● *Table 5-18 Actions based on the VLAN results for local authentication*

In addition to the above changes, minor editorial corrections were made.

Ver. 2.3 (Edition 7)

Summary of amendments

Location and title	Changes
1. Filters	● A note about filtering of frames with VLAN tags was added. ● The description in *Statistics for concurrent use with other functionality*, included in the notes on using the filter, was changed.
3. Flow Control	● A note about QoS flow detection for frames with VLAN tags was added. ● The description in *Statistics for concurrent use with other functionality*, included in the notes on using QoS flow detection, was changed. ● A description about user priority when sending frames with the user priority not implemented was added to *User priority updating*.
5. Overview of Layer 2 authentication	● The description about permitting communication by unauthenticated terminals was changed. ● The description about using DHCP snooping when the Layer 2 authentication method is used with other functionality was changed.
6. Description of IEEE 802.1X	● The description of terminal action detection switching option `disable` was changed.
8. Description of Web Authentication	● The notes on using fixed VLAN mode were changed.
13. Secure Wake-on-LAN [OP-WOL]	● The description in the front page of this chapter and the description in the overview were changed.
18. IEEE802.3ah/UDLD	● The description in the overview was changed.

In addition to the above changes, minor editorial corrections were made.

Ver. 2.3 (Edition 6)

Summary of amendments

Location and title	**Changes**
Send Control	• The description of the scheduling was changed. • The description of the port bandwidth control was changed.
Overview of Layer 2 authentication	• The description in *Configuring the priority for device default local authentication and RADIUS authentication* was changed in association with the support of `end-by-reject`. • A description about using the Layer 2 authentication method with other functionality was added.
Description of IEEE 802.1X	• The description of operating conditions in the overview was changed.
IEEE 802.1X Configuration and Operation	• The example of a configuration that has an excluded terminal with port-based authentication (dynamic) was changed.
Description of Web Authentication	• The description of a Web browser in the overview was changed. • The description of operating conditions in the overview was changed. • The description of the roaming in the dynamic VLAN mode was changed.
Web Authentication Configuration and Operation	• The example of the roaming configuration in dynamic VLAN mode was changed. • The example of the authentication exclusion configuration in dynamic VLAN mode was changed. • The example of authentication method group configuration was changed in association with the support of `end-by-reject`.
Description of MAC-based Authentication	• The description of operating conditions in the overview was changed. • The description of the roaming in dynamic VLAN mode was changed.
MAC-based Authentication Configuration and Operation	• The example of the roaming configuration in dynamic VLAN mode was changed. • The example of the authentication exclusion configuration in dynamic VLAN mode was changed. • The example of authentication method group configuration was changed in association with the support of `end-by-reject`.

In addition to the above changes, minor editorial corrections were made.

Ver. 2.2 (Edition 5)

Summary of amendments

Location and title	Changes
Addition of series	● A description of AX1250S was added.
Uplink redundancy	● The description related to active port locking at Switch startup has been added.

In addition to the above changes, minor editorial corrections were made.

Ver. 2.2 (Edition 4)

Summary of amendments

Location and title	Changes
Overview of Layer 2 authentication	● The authentication method has been changed to the authentication method group, and a description of the equipment defaults and authentication method list has been added. ● A description specifying the authentication method list (port-based authentication method, user ID-based authentication method) was added. ● A description of the RADIUS server group has been added. ● A description of the RADIUS accounting functionality has been added.
Description of IEEE 802.1X	● A description specifying the authentication method list (port-based authentication method) was added. ● A description of the RADIUS accounting functionality has been added. ● The RADIUS attributes used for RADIUS authentication have been standardized.
IEEE 802.1X Configuration and Operation	● A description specifying the authentication method list (port-based authentication method) was added. ● A description of the RADIUS accounting functionality has been added.
Description of Web Authentication	● A description of the user switch option has been added. ● A description specifying the authentication method list (port-based authentication method, user ID-based authentication method) was added. ● A description of the RADIUS accounting functionality has been added. ● A description of the Web authentication page by port has been added. ● The RADIUS attributes used for RADIUS authentication have been standardized.

Location and title	Changes
Web Authentication Configuration and Operation	● A description of the user switch option has been added. ● A description specifying the authentication method list (port-based authentication method, user ID-based authentication method) was added. ● A description of the RADIUS accounting functionality has been added. ● A description of the Web authentication page by port has been added.
Description of MAC-based Authentication	● A description specifying the authentication method list (port-based authentication method) was added. ● A description of the RADIUS accounting functionality has been added. ● The RADIUS attributes used for RADIUS authentication have been standardized.
MAC-based Authentication Configuration and Operation	● A description specifying the authentication method list (port-based authentication method) was added. ● A description of the RADIUS accounting functionality has been added.
Multistep authentication	● A description of the terminal authentication `dot1x` option for terminal authentication with IEEE 802.1X has been added.
Secure Wake-on-LAN [OP-WOL]	● English indications on the page have been changed. ● Japanese indications on the page have been added
CFM	● This chapter was added.
Log Data Output Functionality	● A description of the HEADER part when outputting to the syslog server has been added.

In addition to the above changes, minor editorial corrections were made.

Ver. 2.1 (Edition 3)

Summary of amendments

Location and title	Changes
Filters	● Notes when using with other functionality have been added to the notes when using a filter.
Flow control	● A list of frames that cannot be changed by determination of priority has been changed. ● The self-generated frame type and the setting range table of user priority have been changed. ● The user priority settings for the self-generating frame and the mapping table of CoS values have been changed.

Location and title	Changes
Overview of Layer 2 authentication	The following descriptions have been added as the functionality common to the Layer 2 authentication: ● Priority setting for the local authentication method and the RADIUS authentication method ● General-use RADIUS server information and RADIUS server information dedicated to authentication ● Automatic VLAN allocation for a MAC VLAN ● Authentication of tagged frames at the MAC port (`dot1q vlan` setting) ● Forced authentication common to the authentications
	The following descriptions have been moved from Chapter 12 to Chapter 5 as the functionality common to Layer 2 authentication (functionality description and configuration). ● Permitting communication by unauthenticated terminals (IPv4 access list dedicated to authentication) ● Specifying attached VLANs by VLAN name
	The descriptions about "selection of RADIUS servers" and "recovery of a RADIUS server" previously in *Login Security and RADIUS* of *Configuration Guide Vol. 1* were moved to *Dead-interval functionality of RADIUS server communication* in this manual.
	The description of the coexistence of the Layer 2 authentication functionality has been moved from Chapter 12 to Chapter 5 (functionality description and configuration).
	A list of operation commands has been added as an operation common to Layer 2 authentications.
Description of IEEE 802.1X	● `auto` has been added to the terminal detection behavior switching option. ● A non-communication terminal monitoring functionality has been added.
Description of MAC-based Authentication	● A regular re-authentication request functionality has been added to fixed VLAN mode.
Multistep authentication	● This chapter was added.
Secure Wake-on-LAN [OP-WOL]	● The description of the page of sending Web browser selection has been changed.
Uplink redundancy	● A description of the MAC address updating functionality has been added.
Storm Control	● A description of flow restriction has been added.
Port Mirroring	● The table of the ability of transmit mirroring has been changed.

In addition to the above changes, minor editorial corrections were made.

Ver. 2.0 (Edition 2)

Summary of amendments

Location and title	**Changes**
One-time password authentication [OP-OTP]	● The figure in the overview description has been corrected.

In addition to the above changes, minor editorial corrections were made.

Preface

Applicable products and software versions

This manual applies to the AX2200S, AX1250S, and AX1240S series of switches. The manual describes the functionality of software version 2.4 for the AX2200S, AX1250S, and AX1240S series switches supported by the OS-LT4, OS-LT3, and OS-LT2 and optional licenses.

Before you operate the equipment, carefully read the manual and make sure that you understand all instructions and cautionary notes. After reading the manual, keep it in a convenient place for easy reference.Unless otherwise noted, this manual describes the functionality applicable commonly to AX2200S, AX1250S, and AX1240S series switches. The functionalities specific to each model are indicated as follows:

[*AX2200S*]:

The description applies to the AX2200S Switch.

[*AX1250S*]:

The description applies to the AX1250S Switch.

[*AX1240S*]:

The description applies to the AX1240S Switch.

In addition, unless otherwise noted, this manual describes the functionality applicable to OS-LT4, OS-LT3, and OS-LT2. The functionality supported by option licenses are indicated as follows:

[*OP-WOL*]:

The description applies to the OP-WOL optional license.

[*OP-OTP*]:

The description applies to the OP-OTP optional license.

Corrections to the manual

Corrections to this manual might be contained in the *Release Notes* and *Manual Corrections* that come with the software.

Intended readers

This manual is intended for system administrators who wish to configure and operate a network system that uses the Switch.

Readers must have an understanding of the following:

- The basics of network system management

Manual URL

You can view this manual on our website at:

http://www.alaxala.com/en

Reading sequence of the manuals

The following shows the manuals you need to consult according to your requirements determined from the following workflow for installing, setting up, and starting regular operation of the Switch.

- Details on basic settings at initial installation, hardware requirements, and instructions for handling the switch
  - AX2200S/AX1250S/AX1240S Hardware Instruction Manual (AX1240S-H001X)
- Software functionality, configuration, and operation commands
  - Configuration Guide Vol. 1 (AX1240S-S001X)
  - Vol. 2 (AX1240S-S002X)
- Proper syntax for configuration commands and details on parameters
  - Configuration Command Reference (AX1240S-S003X)
- Proper syntax for operation commands and details on parameters
  - Operation Command Reference (AX1240S-S004X)
- Details on messages and logs
  - Message Log Reference (AX1240S-S005X)
- Details on MIBs
  - MIB Reference (AX1240S-S006X)
- Handling problems
  - Troubleshooting Guide (AX1240S-T001X)

Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System

AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	Bits per second (can also appear as bps)
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization

ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations, Administration, and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second (can also appear as pps)
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PoE	Power over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service

RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
ULR	Uplink Redundant
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VAA	VLAN Access Agent
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

1 KB (kilobyte) is 1024 bytes.

1 MB (megabyte) is 1024^2 bytes.

1 GB (gigabyte) is 1024^3 bytes.

1 TB (terabyte) is 1024^4 bytes.

Conventions: The terms "Switch" and "switch"

The term *Switch* (upper-case "S") is an abbreviation for any or all of the following models:

- AX2200S series switch
- AX1250S series switch
- AX1240S series switch

The term *switch* (lower-case "s") might refer to a Switch, another type of switch from the current vendor, or a switch from another vendor. The context decides the meaning.

Contents

Part 1: Filters

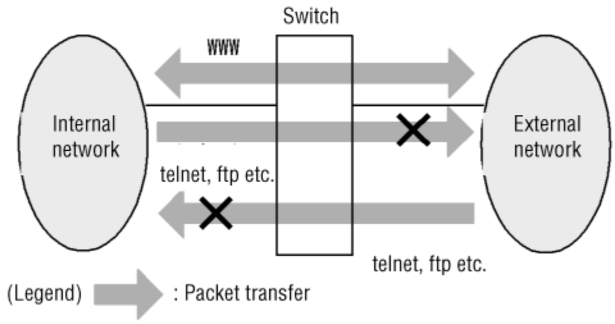
1. Filters

Filtering is functionality used for forwarding and discarding received frames. This chapter provides an overview of filters and describes its use.

1.1 Description

Filtering is functionality used to forward and discard certain types of received frames. It is used to strengthen network security. You can use filters to limit access to the network by each user. For example, you can forward Web data between an internal network and an external network while at the same time discarding any Telnet and FTP data. This prevents unauthorized access from the external network and leakage of information to the external network from the internal network. The following figure shows an example of network configuration that uses filters.

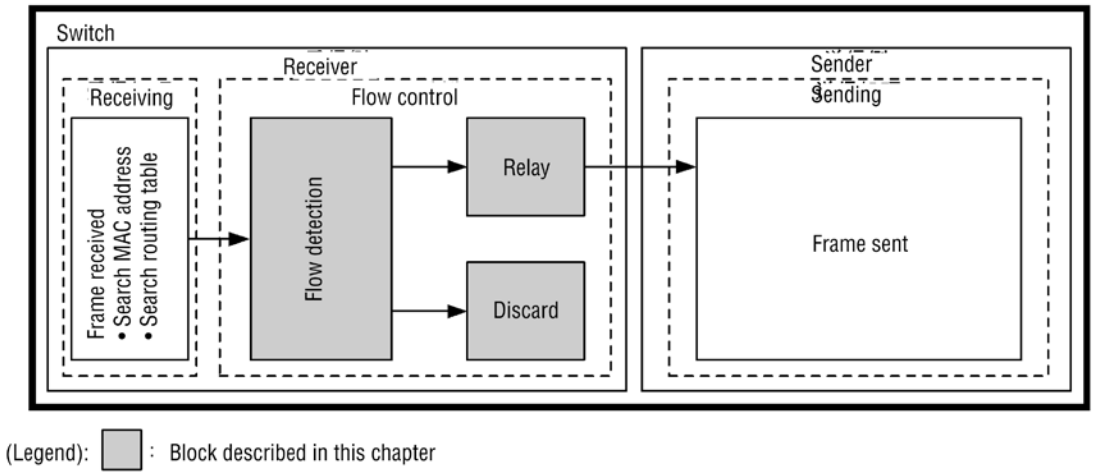
Figure 1-1 Configuration example of network using filtering



1.1.1 Overview of filters

The following figure shows the functional blocks for filters on the Switch.

Figure 1-2 Functional blocks for Switch filtering



The following table provides an overview of the functional blocks shown in the figure.

Table 1-1 Overview of functional blocks for filtering

Section and functional blocks		Overview of functionality
Flow control section	Flow detection	This block detects a flow (specific frames) that matches a condition, such as MAC address, protocol type, IP address, or TCP/UDP port number.

Section and functional blocks		Overview of functionality
	Forwarding and discard blocks	These blocks forward and discard frames found by the flow detection block.

To use filtering on a Switch, create a filter entry that defines a combination of flow detection conditions (such as MAC address, protocol type, IP address, or TCP/UDP port number) and an operation (forward or discard).

The following describes how a filter works on the Switch:

1. The filter entries set for each interface are searched in the order of priority specified by the user.
2. The search terminates when the filter entry matching the frame is found.
3. Whether the frame is forwarded or discarded is determined according to the operation specified for the filter entry.
4. If the frame does not match any filter entry, the frame is discarded. For details about discarding, see *1.1.6 Implicit discard*.

1.1.2 Flow detection

The flow detection functionality detects a flow, which is a sequence of frames, based on conditions, such as the MAC header, IP header, and TCP header. Settings are configured in access lists. For details about access lists, see *1.1.5 Access Lists*.

The Switch is able to perform flow detection for Ethernet V2 format frames and IEEE 802.3 SNAP/RFC 1042 format frames on the receiving-side Ethernet interface and VLAN interface. The interface that can be set depends on the flow detection mode.

Note that some control frames and the frames subject to snooping are excluded from filtering.

1.1.3 Flow detection mode

The Switch provides flow detection modes for network configuration and operation modes. The flow detection modes determine the allocation pattern of filter entries and QoS entries for the receiving-side interface. Select the mode appropriate for your operating requirements. Guidelines for selecting the flow detection mode are provided below. For details about the MAC condition and IPv4 condition, see *1.1.4 Flow detection conditions*.

- Use Layer 2-1 to set the MAC condition for detecting frames.
- Use Layer 2-2 to set only the IPv4 condition for detecting frames.

To specify the flow detection mode, use the configuration command `flow detection mode`. The selected flow detection mode applies to both filtering and QoS. To change the flow detection mode, you need to delete all the receiving-side interface settings set by the following commands:

- `mac access-group`
- `ip access-group`
- `mac qos-flow-group`
- `ip qos-flow-group`

If you do not specify the flow detection mode, Layer 2-2 is set as the default mode.

The following table describes the relationship between the flow detection modes and flow operations.

Table 1-2 Relationship between the flow detection modes and flow operations

Flow detection mode name	Purpose	Flow operation	Applicable interface
Layer 2-1	Use this mode to perform flow control for IP packets and other frames.	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type.	Ethernet, VLAN
Layer 2-2	Use this mode to perform fine-tuned flow control specialized for IPv4 packets.	For IPv4 packets, frames are detected based on the IP header and TCP/UDP header.	Ethernet, VLAN

1.1.4 Flow detection conditions

To perform flow detection, specify the conditions for identifying the flow in the configuration. The following table describes the flow detection conditions that can be specified for each flow detection mode.

Table 1-3 Configurable flow detection conditions

Type		Configuration item	Layer 2-1		Layer 2-2	
			Ethernet	VLAN	Ethernet	VLAN
MAC conditions	Configuration	VLAN ID#1	Y	--	--	--
	MAC header	Source MAC address	Y	Y	--	--
		Destination MAC address	Y	Y	--	--
		Ethernet type	Y	Y	--	--
		User priority#2	Y	Y	--	--
IPv4 conditions	Configuration	VLAN ID#1	--	--	Y	--
	MAC header	User priority#2	--	--	Y	Y
	IPv4 header#3	Upper-layer protocol	--	--	Y	Y
		Source IP address	--	--	Y	Y

Type		Configuration item	Layer 2-1		Layer 2-2	
			Ethernet	VLAN	Ethernet	VLAN
		Destination IP address	--	--	Y	Y
		TOS	--	--	Y	Y
		DSCP	--	--	Y	Y
		Precedence	--	--	Y	Y
	IPv4-TCP header	Source port number	--	--	Y	Y
		Destination port number	--	--	Y	Y
		TCP control flag#4	--	--	Y	Y
	IPv4-UDP header	Source port number	--	--	Y	Y
		Destination port number	--	--	Y	Y

Legend: Y: Can be specified, --: Cannot be specified

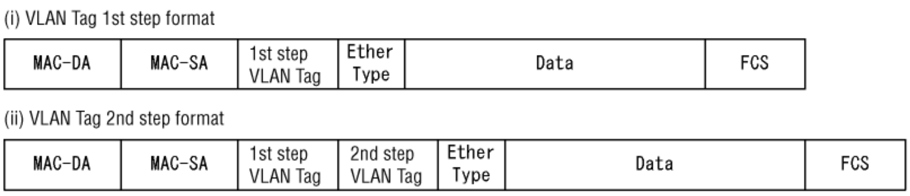
#1

VLAN IDs that can be detected by flow detection on the Switch are the values assigned to the VLANs entered in the VLAN configuration. The ID of the VLAN to which received frames belong will be detected.

#2

The user priority cannot be detected for frames that do not have a VLAN tag on the Switch. Therefore, user priority 3 is always detected.

The user priority for a frame that has multiple VLAN tags is detected by counting from the MAC address side. The first VLAN tag encountered will be detected. The following figure shows an example of a frame that has multiple VLAN tags.



#3

Supplementary note for the TOS field specification

TOS: The values of bit 3 to bit 6 of the TOS field

Precedence: Value of the three highest-order bits in the TOS field.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			TOS				-

DSCP: Value of the six highest-order bits in the TOS field.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

#4

Packets whose `ack`, `fin`, `psh`, `rst`, `syn`, or `urg` flag is set to `1` are detected.

1.1.5 Access Lists

To perform flow detection for the filter, set access lists in the configuration. The access list you need to set depends on the flow detection condition. The type of detectable frames also depends on the flow detection condition. The following table describes the relationship between the access lists for flow detection conditions and detectable frame types.

Table 1-4 Relationship between the access lists for flow detection conditions and detectable frame types

Flow detection conditions	Access list	Flow detection mode	Detectable frame type		
			Non-IP	IPv4	IPv6
MAC conditions	`mac access-list`	Layer 2-1	Y	Y#	Y#
IPv4 conditions	`ip access-list`	Layer 2-2	--	Y	--

Legend: Y: Can be detected, --: Cannot be detected

#: Can be detected only when specified for the Ethernet interface type.

An access list is applied to an interface by using the access group command. The application order is determined by the sequence number specified as a parameter of an access list.

(1) Operation performed when multiple filters are applied

(a) When filtering and QoS are set at the same time

If filtering and QoS are set at the same time, the received frames that have been denied by the filter are also counted in the QoS statistics.

(b) Filtering when Layer 2-1 or Layer 2-2 is set as the flow detection mode

When filters set for an Ethernet interface and for a VLAN interface are applied to a received frame, the result of the filtering is `permit` if the frame is permitted by both filters. The deny specification has precedence if either filtering setting yields deny (including an implicit deny entry).

Statistics are recorded for the Ethernet interface and VLAN interface.

The following table describes the operation performed when a frame matches multiple filter entries.

Table 1-5 Operation when multiple filter entries match

Combination for which multiple filter entries match		Filter entry that takes effect		Interface for which statistics are recorded
Ethernet	**VLAN**	**Interface**	**Operation**	
permit	permit	Ethernet	`permit`: (forward)	Ethernet VLAN
permit	deny	VLAN	`deny`: (discard)	Ethernet VLAN
deny	permit	Ethernet	`deny`: (discard)	Ethernet VLAN
deny	deny	Ethernet	`deny`: (discard)	Ethernet VLAN

1.1.6 Implicit discard

Frames that do not match any flow detection conditions are discarded on an interface for which filtering is specified.

Filter entries for implicit discard are automatically generated when access lists are generated. If no access lists are set, all frames are forwarded.

1.1.7 Notes on using the filter

(1) Operation when multiple filter entries match

See *(1) Operation performed when multiple filters are applied* in *1.1.5 Access Lists*.

(2) Filtering of frames with VLAN tags

You cannot filter frames with two or more VLAN tags by using an Ethernet type for the MAC condition or an IPv4 condition specified as a flow detection condition.

(3) Filtering of fragmented IPv4 packets

If the filter uses a TCP/UDP header specified as a flow detection condition for a fragmented IPv4 packet, the second and subsequent fragments cannot be detected because the TCP/UDP header is not in those packets. To filter frames that include fragmented packets, specify the MAC header or IP header in the flow detection conditions.

(4) Operation when filter entries are applied

When filter entries are applied to the interfaces on the Switch[#], an implicit discard entry is applied first. Accordingly, frames that match the implicit discard condition are temporarily discarded until user-specified filter entries are applied. In addition, statistics for the implicit discard entry are collected.

#

- When an access list containing one or more entries is applied to the interface by using the access group command
- When an access list is applied by using the access group command

and the first entry is added.

(5) Operation when a filter entry is changed

If a filter entry applied to an interface is changed on the Switch, detectable frames cannot be detected until the change has been applied. Consequently, such frames are detected as if they matched another filter entry or the implicit discard entry.

(6) Concurrent use with other functionality

(a) Concurrent use with other functionalities

The following table describes the operation when the filter functionality is used concurrently with the following functionality.

Table 1-6 Concurrent use of filter and other functionality

Functionality	Operation
DHCP snooping	Operating DHCP snooping on a port with filter conditions disables the filter functionality for DHCP frames, so that these frames are forwarded.
IGMP snooping	Operating IGMP snooping on a port with filter conditions disables the filter functionality for IGMP frames, so that these frames are forwarded.
MLD snooping	Operating MLD snooping on a port with filter conditions disables the filter functionality for MLD frames, so that these frames are forwarded.

(b) Statistics for concurrent use with other functionality

If any of the conditions listed below is satisfied for a frame, it is discarded. However, if a frame matches a filter entry specified for the interface, statistics for that filter entry are collected.

- Frames are received from the VLAN port whose data transfer status is `Blocking` (data transfer stopped).
- Frames are received from a port specified for inter-port isolation.
- Frames without a VLAN tag are received when the native LAN is not set as the VLAN that uses a trunk port for sending and receiving frames.
- Received frames that have a VLAN tag are not set for a VLAN that uses a trunk port for sending and receiving frames.
- Frames with a VLAN Tag are received at protocol or MAC ports.
- Frames are discarded by the MAC address learning functionality.
- Frames are discarded by the Layer 2 authentication functionality.
- Frames are discarded due to an invalid Layer 2 protocol.
- Frames are discarded by IGMP snooping or MLD snooping.
- Frames are discarded by DHCP snooping.
- Frames are discarded by storm control.

(7) Restrictions when applying filter conditions

For frames to be received in a channel group, only filter conditions for an access group set to a VLAN interface are applied.

1.2 Configuration

1.2.1 List of configuration commands

The following table describes the commands used to configure filtering.

Table 1-7 List of configuration commands

Command name	Description
`deny`	Specifies the condition by which the filter discards access.
`flow detection mode`	Sets the flow detection mode for the filter and QoS control.
`ip access-group`	Applies an IPv4 filter to an Ethernet interface or VLAN interface and enables IPv4 filtering.
`ip access-list extended`	Configures an access list to serve as an IPv4 packet filter.
`ip access-list resequence`	Resets the sequence numbers that determine the order in which the IPv4 address filter and IPv4 packet filter apply filter conditions.
`ip access-list standard`	Configures an access list to serve as an IPv4 address filter.
`mac access-group`	Applies a MAC filter to an Ethernet interface or VLAN interface and enables MAC filtering.
`mac access-list resequence`	Resets the sequence number for the order in which the filter conditions in a MAC filter are applied.
`mac access-list extended`	Sets an access list to be used in a MAC filter.
`permit`	Specifies the condition by which the filter forwards access.
`remark`	Specifies supplementary information for the filter.

1.2.2 Configuring frame forwarding and discarding by MAC header

(1) Setting the flow detection mode

The following is an example of specifying the flow detection mode for filtering.

Points to note

First set the flow detection mode to determine the basic operating conditions of the hardware.

Command examples

1. `(config)# flow detection mode layer2-1`

   Enables Layer 2-1 as the flow detection mode.

(2) Example of using MAC headers as the flow detection condition

The following shows an example of specifying frame forwarding and discarding based on specification of MAC header as the flow detection condition.

Points to note

When frames are received, flow detection is performed based on the MAC header. The frames that match the filter entry are either discarded or forwarded.

Command examples

1. `(config)# mac access-list extended IPX_DENY`

   Creates `mac access-list` (`IPX_DENY`), and then switches to MAC filtering mode.

2. `(config-ext-macl)# deny any any ipx`

   Sets a MAC filter that discards frames whose Ethernet type is IPX.

3. `(config-ext-macl)# permit any any`

   Sets a MAC filter that forwards all frames.

4. `(config-ext-macl)# exit`

   Returns to global configuration mode from MAC filtering mode.

5. `(config)# interface fastethernet 0/1`

   Moves to port 0/1 interface mode.

6. `(config-if)# mac access-group IPX_DENY in`

   `(config-if)# exit`

   Enables the MAC filtering on the receiving side.

1.2.3 Setting frame forwarding and discarding by IP header and TCP/UDP header

(1) Setting the flow detection mode

The following is an example of specifying the flow detection mode for filtering.

Points to note

First set the flow detection mode to determine the basic operating conditions of the hardware.

Command examples

1. `(config)# flow detection mode layer2-2`

   Enables Layer 2-2 as the flow detection mode.

(2) Using IPv4 address as the flow detection condition

The following shows an example of specifying frame forwarding and discarding based on specification of IPv4 address as the flow detection condition.

Points to note

When frames are received, flow detection is performed based on the sender IPv4 address. The frames that match the filter entry are forwarded. All IP packets that do not match the filter entry are discarded.

Command examples

1. `(config)# ip access-list standard FLOOR_A_PERMIT`

   Creates `ip access-list` (`FLOOR_A_PERMIT`), and then switches to IPv4 address filtering mode.

2. `(config-std-nacl)# permit 192.168.0.0 0.0.0.255`

   Sets an IPv4 address filter that forwards the frames from the sender IP address `192.168.0.0/24` network.

3. `(config-std-nacl)# exit`

   Returns to global configuration mode from IPv4 address filtering mode.

4. `(config)# interface vlan 10`

   Switches to interface mode for VLAN 10.

5. `(config-if)# ip access-group FLOOR_A_PERMIT in`

   `(config-if)# exit`

   Enables IPv4 filtering on the receiving side.

(3) Using IPv4 packet as the flow detection condition

The following shows an example of specifying frame forwarding and discarding based on specification of IPv4 Telnet packet as the flow detection condition.

Points to note

When frames are received, flow detection is performed based on the IP header or TCP/UDP header, and the frames that match the filter entry are discarded.

Command examples

1. `(config)# ip access-list extended TELNET_DENY`

   Creates `ip access-list` (`TELNET_DENY`), and then switches to IPv4 packet filtering mode.

2. `(config-ext-nacl)# deny tcp any any eq telnet`

   Sets an IPv4 packet filter that discards Telnet packets.

3. `(config-ext-nacl)# permit ip any any`

   Configures an IPv4 packet filter that forwards all frames.

4. `(config-ext-nacl)# exit`

   Returns to global configuration mode from IPv4 packet filtering mode.

5. `(config)# interface vlan 10`

   Switches to interface mode for VLAN 10.

6. `(config-if)# ip access-group TELNET_DENY in`

   `(config-if)# exit`

   Enables IPv4 filtering on the receiving side.

1.2.4 Configuring multiple interface filters

The following shows an example of specifying a filter on multiple Ethernet interfaces.

Points to note

A filter can be set for multiple Ethernet interfaces in `config-if-range` mode.

Command examples

1. `(config)# ip access-list standard HOST_IP`

   `(config-std-nacl)# permit host 192.168.0.1`

   `(config-std-nacl)# exit`

   Sets an IPv4 address filter that forwards only frames from the host `192.168.0.1`.

2. `(config)# interface range fastethernet 0/1-4`

   Switches to the interface mode for ports 0/1-4.

3. `(config-if-range)# ip access-group HOST_IP in`

   `(config-if-range)# exit`

   Enables IPv4 filtering on the receiving side.

1.3 Operation

To make sure that the information you have set is applied, use the operation command `show access-filter`.

1.3.1 List of operation commands

The following table describes the operation commands used for filtering.

Table 1-8 List of operation commands

Command name	Description
`show access-filter`	Displays statistics on the access lists (`mac access-list` and `ip access-list`) set by the access group commands (`mac access-group` and `ip access-group`).
`clear access-filter`	Clears statistics on the access lists (`mac access-list` and `ip access-list`) set by the access group commands (`mac access-group` and `ip access-group`).

1.3.2 Checking filters

(1) Checking the entries set for an Ethernet interface

The following figure shows how to check operation when a filter is set for an Ethernet interface.

Figure 1-3 Checking operation when a filter is set for an Ethernet interface

```
> show access-filter 0/1

Date 19.09.08 03:11:21 PM UTC
Using Port: interface fastethernet 0/1 in
Extended MAC access-list: acl-mac
  remark "permit of mac access-list extended"
  10 permit host 001b.7888.1ffa any
    matched packets        :        0
  implicitly denied packets :        20

>
```

Make sure that `Extended MAC access-list` is displayed for the filter for the specified port.

(2) Checking the entries set for a VLAN interface

The following figure shows how to check operation when a filter is set for a VLAN interface.

Figure 1-4 Checking operation when a filter is set for a VLAN interface

```
> show access-filter interface vlan 1

Date 18.09.08 12:56:14 PM UTC
Using Port: interface vlan 1 in
Extended IP access-list: acl-ext
  remark "permit of ip access-list extended"
```

```
 10 permit tcp 172.16.89.29 0.0.0.255 any
   matched packets        :         0
 implicitly denied packets :        14

>
```

Make sure that `Extended IP access-list` is displayed for the filter for the specified VLAN.

Part 2: QoS

2. Overview of QoS Control

The QoS control functionality provides marking, determination of priority, and bandwidth control as a means of controlling communications quality and ensuring the efficient use of limited network resources, such as line bandwidth and queue buffer capacity. This chapter describes QoS control on the Switch.

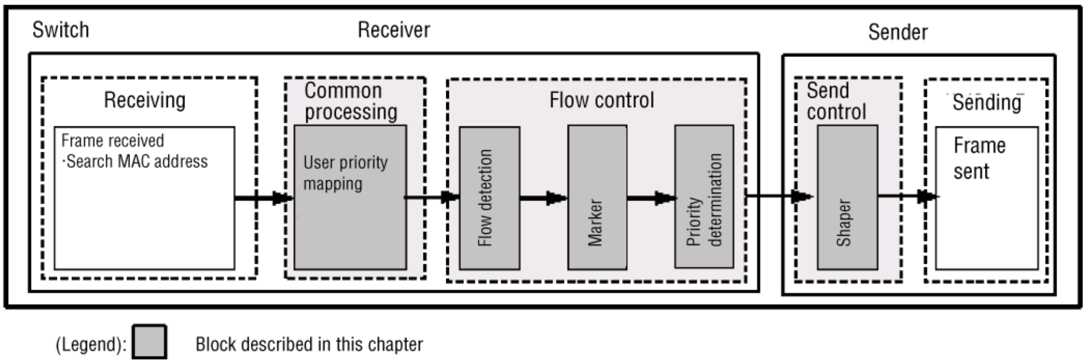
2.1 Structure of QoS control

Along with best-effort traffic that does not require guaranteed communications quality, the growing diversification of network services has meant an increase in real-time and guaranteed bandwidth traffic. You can use QoS control on the Switch to provide communications quality appropriate for the type of traffic.

QoS control on the Switch ensures the efficient use of limited network resources, such as line bandwidth and queue buffer capacity. To satisfy the many types of communications quality required for applications, use QoS control to distribute network resources in the most appropriate manner.

The following figure shows the functional blocks for QoS control on the Switch.

Figure 2-1 Functional blocks for QoS control on the Switch



The following table provides an overview of the functional blocks shown in the figure.

Table 2-1 Overview of functional blocks for QoS control

Section and functional block		Functionality overview
Receive processing section	Frame reception	Receives frames and searches the MAC address table.
Common processing section	User priority mapping	Determines priority based on the user priority in the VLAN tag of received frames.
Flow control section	Flow detection	Detects a flow matching a condition, such as MAC header, protocol type, IP address, and port number.
	Marking	Updates the user priority in the DSCP or VLAN tag in the IP header.
	Priority determination	Determines the priority of frames.
Send control section	Shaper	Controls the output order of frames from queues and the output bandwidth.

Section and functional block		Functionality overview
Send processing section	Frame sending	Sends frames controlled by the shaper.

QoS control on the Switch uses user priority mapping or flow control to determine the priority of received frames. User priority mapping determines the priority based on the user priority in the VLAN tag of a received frame. You can use flow control to determine the priority based on whether the frame matches a specific condition, such as the MAC address or IP address, rather than based on the user priority.

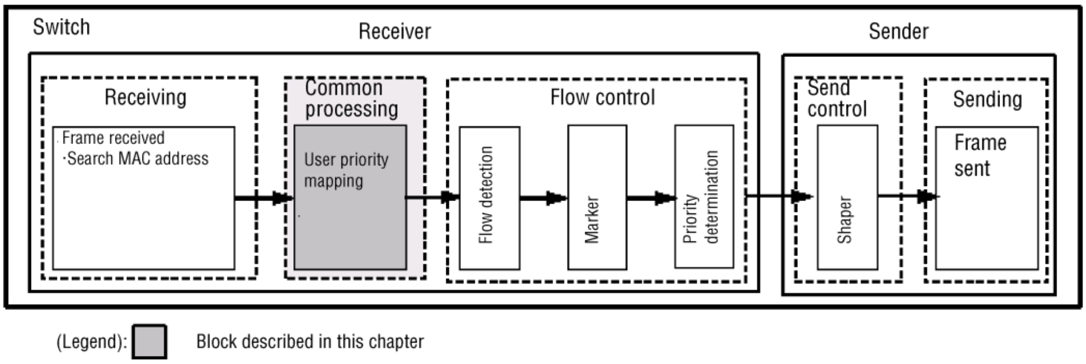
The priority determined by flow control has precedence over user priority mapping. You can also use flow control to employ marking in addition to priority determination. Marking and priority determination can operate concurrently for the flow detected by flow detection.

Send control uses the shaper based on the priority determined by user priority mapping or flow control.

2.2 Description of common processing

The following figure shows the positioning of user priority mapping described in this section.

Figure 2-2 Positioning of user priority mapping



2.2.1 User priority mapping

User priority mapping functionality determines priority based on the user priority in the VLAN tags of received frames. User priority mapping is always running on the Switch to determine the priority for all received frames.

CoS values that indicate the priority on the Switch are used as priority values. The user priority value of the received frame is mapped to a CoS value, and the send queue is determined based on the CoS value. For details about the correspondence between the CoS values and send queues, see *3.7.2 CoS mapping functionality*.

The user priority is the three highest-order bits of the Tag Control field (VLAN tag header information). Note that CoS value 3 is always used for frames without a VLAN tag.

When running, priority determination by flow control has precedence over user priority mapping.

Table 2-2 Mapping of user priority values to CoS values

Frame type		
VLAN tag	**User priority value**	**Mapped CoS value**
Without VLAN tag	n/a	3
With VLAN tag	0	0
	1	1
	2	2
	3	3

Frame type		Mapped CoS value
VLAN tag	**User priority value**	
	4	4
	5	5
	6	6
	7	7

Legend: n/a: Not applicable

2.3 Configuration common to QoS control

2.3.1 List of configuration commands

The following table describes the commands used to configure QoS control.

Table 2-3 List of configuration commands

Command name	Description
flow detection mode	Sets the flow detection mode for the filter and QoS control.
ip qos-flow-group	Applies an IPv4 QoS flow list to an Ethernet interface or VLAN interface, and enables IPv4 QoS control.
ip qos-flow-list	Sets the QoS flow list used for IPv4 QoS flow detection.
ip qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the IPv4 QoS flow list are applied.
limit-queue-length	Sets the queue length of a physical port for the Switch.
mac qos-flow-group	Applies a MAC QoS flow list to an Ethernet interface or VLAN interface, and enables MAC QoS control.
mac qos-flow-list	Sets the QoS flow list used for MAC QoS flow detection.
mac qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the MAC QoS flow list are applied.
qos	Sets the flow detection condition and operation to be performed in the QoS flow list.
qos-queue-group	Applies QoS queue list information to an Ethernet interface and enables the legacy shaper.
qos-queue-list	Sets the scheduling mode in QoS queue list information.
remark	Specifies supplementary information for QoS.
traffic-shaper rate	Sets port bandwidth control for an Ethernet interface.
control-packet user-priority	Sets the user priority in the VLAN tags of frames spontaneously sent by a Switch.

2.4 Operations common to QoS control

2.4.1 List of operation commands

The following table describes the operation commands common to QoS control.

Table 2-4 List of operation commands

Command name	Description
`show qos-flow`	Displays statistics on the QoS flow lists (`mac qos-flow-list` and `ip qos-flow-list`) set by the QoS flow group commands (`mac qos-flow-group` and `ip qos-flow-group`).
`clear qos-flow`	Clears statistics on the QoS flow lists (`mac qos-flow-list` and `ip qos-flow-list`) set by the QoS flow group commands (`mac qos-flow-group` and `ip qos-flow-group`).
`show qos queueing`	Displays statistics on send queues for the Ethernet interface.
`clear qos queueing`	Clears statistics on send queues for the Ethernet interface.

3. Flow Control

This chapter describes flow control (flow detection, marking, and priority determination) for Switches.

3.1 Description of flow detection

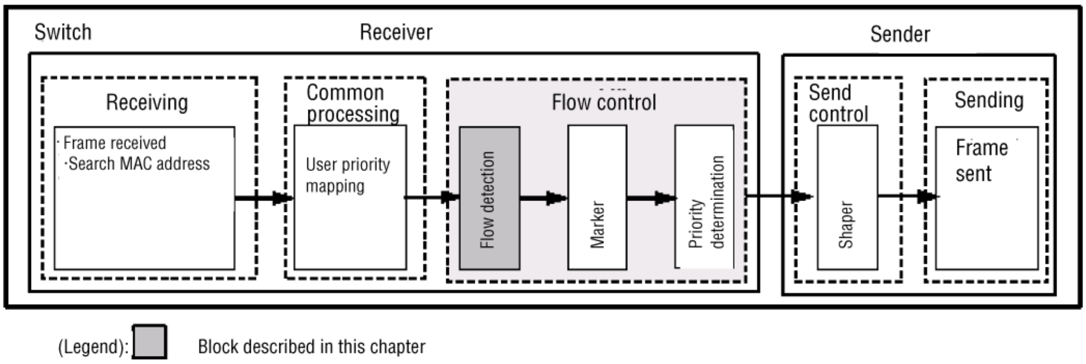
The flow detection functionality detects the sequence of frames based on conditions, such as the MAC header, IP header, and TCP header. QoS flow lists are used to set up flow detection. For details about the QoS flow lists, see *3.1.3 QoS flow lists*.

The Switch is able to perform flow detection for Ethernet V2 format frames and IEEE 802.3 SNAP/RFC 1042 format frames on the receiving-side Ethernet interface and VLAN interface. The interface that can be set depends on the flow detection mode.

Note that some control frames and the frames subject to snooping are excluded from QoS processing.

The following figure shows the positioning of the flow detection block described in this section.

Figure 3-1 Positioning of the flow detection block



3.1.1 Flow detection mode

The Switch provides flow detection modes for network configuration and operation modes. The flow detection modes determine the allocation pattern of filter entries and QoS entries for the receiving-side interface. Select the mode appropriate for your operating requirements. Guidelines for selecting the flow detection mode are provided below. For details about the MAC condition and IPv4 condition, see *3.1.2 Flow detection conditions*.

- Use Layer 2-1 to set the MAC condition for detecting frames.
- Use Layer 2-2 to set only the IPv4 condition for detecting frames.

To specify the flow detection mode, use the configuration command `flow detection mode`. The selected flow detection mode applies to both filtering and QoS. To change the flow detection mode, you need to delete all the receiving-side interface settings set by the following commands:

- `mac access-group`
- `ip access-group`
- `mac qos-flow-group`
- `ip qos-flow-group`

If you do not specify the flow detection mode, Layer 2-2 is set as the default mode.

The following table describes the relationship between the flow detection modes and flow operations.

Table 3-1 Relationship between the flow detection modes and flow operations

Flow detection mode name	Purpose	Flow operations	Applicable interfaces
Layer 2-1	Use this mode to perform flow control for IP packets and other frames.	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type.	Ethernet, VLAN
Layer 2-2	Use this mode to perform fine-tuned flow control specialized for IPv4 packets.	For IPv4 packets, frames are detected based on the IP header and TCP/UDP header.	Ethernet, VLAN

3.1.2 Flow detection conditions

To perform flow detection, specify the conditions for identifying the flow in the configuration. The following table describes the flow detection conditions that can be specified for each flow detection mode.

Table 3-2 Configurable flow detection conditions

Type		Configuration items	Layer 2-1		Layer 2-2	
			Ethernet	VLAN	Ethernet	VLAN
MAC conditions	Configuration	VLAN ID#1	Y	--	--	--
	MAC header	Source MAC address	Y	Y	--	--
		Destination MAC address	Y	Y	--	--
		Ethernet type	Y	Y	--	--
		User priority#2	Y	Y	--	--
IPv4 conditions	Configuration	VLAN ID#1	--	--	Y	--
	MAC header	User priority#2	--	--	Y	Y
	IPv4 header#3	Upper-layer protocol	--	--	Y	Y
		Source IP address	--	--	Y	Y

Type		Configuration items	Layer 2-1		Layer 2-2	
			Ethernet	VLAN	Ethernet	VLAN
		Destination IP address	--	--	Y	Y
		TOS	--	--	Y	Y
		DSCP	--	--	Y	Y
		Precedence	--	--	Y	Y
	IPv4-TCP header	Source port number	--	--	Y	Y
		Destination port number	--	--	Y	Y
		TCP control flag#4	--	--	Y	Y
	IPv4-UDP header	Source port number	--	--	Y	Y
		Destination port number	--	--	Y	Y

Legend: Y: Can be specified, --: Cannot be specified

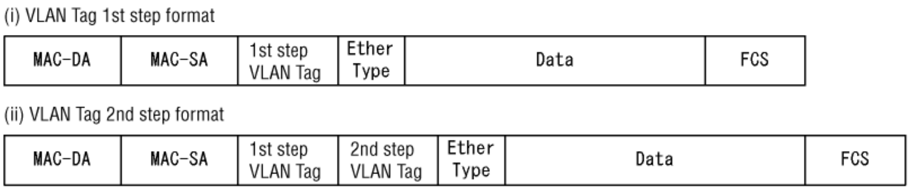
#1

VLAN IDs that can be detected by flow detection on the Switch are the values assigned to the VLANs entered in the VLAN configuration. The ID of the VLAN to which received frames belong will be detected.

#2

The user priority cannot be detected for frames that do not have a VLAN tag on the Switch. Therefore, user priority 3 is always detected.

The user priority for a frame that has multiple VLAN tags is detected by counting from the MAC address side. The first VLAN tag encountered will be detected. The following figure shows an example of a frame that has multiple VLAN tags.



#3

Supplementary note for the TOS field specification

TOS: The values of bit 3 to bit 6 of the TOS field

Precedence: Value of the three highest-order bits in the TOS field.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			TOS				-

DSCP: Value of the six highest-order bits in the TOS field.

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP						-	

#4

Packets whose `ack`, `fin`, `psh`, `rst`, `syn`, or `urg` flag is set to `1` are detected.

3.1.3 QoS flow lists

To perform QoS flow detection, set QoS flow list in the configuration. The QoS flow list you need to configure depends on the flow detection condition. The type of detectable frames also depends on the flow detection condition. The following table describes the relationship between the QoS flow lists for flow detection conditions and detectable frame types.

Table 3-3 Relationship between the QoS flow lists for flow detection conditions and detectable frame types

Flow detection condition	QoS flow list	Flow detection mode	Detectable frame type		
			Non-IP	**IPv4**	**IPv6**
MAC conditions	`mac qos-flow-list`	Layer 2-1	Y	Y#	Y#
IPv4 conditions	`ip qos-flow-list`	Layer 2-2	--	Y	--

Legend: Y: Can be detected, --: Cannot be detected

#: Can be detected only when specified for the Ethernet interface type.

Use a QoS flow group command to apply the QoS flow lists to an interface. The order in which the flow lists are applied is determined by the sequence number specified as a parameter of the QoS flow list.

(1) Operation performed when multiple QoS entries are applied

(a) When filtering and QoS are set at the same time

If filtering and QoS are set at the same time, the received frames that have been denied by the filter are also counted in the QoS statistics.

(b) QoS flow when Layer 2-1 or Layer 2-2 is set as the flow detection mode

If QoS flow lists# are set for both the Ethernet interface that receives frames and the VLAN interface to which the received frames belong, both QoS flow lists take effect. This applies when the operations specified for the `action` parameters do not conflict (for example, `replace-dscp` is specified for Ethernet and `replace-user-priority` is specified for VLAN).

#

Indicates the `mac qos-flow-group` or `ip qos-flow-group` configuration command.

If the operations specified for the `action` parameters conflict, the operation specified for the QoS flow list for the Ethernet interface takes effect.

Statistics are recorded for both the Ethernet interface and the VLAN interface.

(c) Concurrent specification of a CoS value and a user priority value

If you specify a CoS value and a user priority at the same time, the user priority is set based on the specified CoS value.

3.1.4 Notes on using flow detection

(1) Operation when multiple QoS entries are matched

See *(1) Operation performed when multiple QoS entries are applied* in *3.1.3 QoS flow lists*.

(2) QoS flow detection for frames with VLAN tags

You cannot perform QoS flow detection for frames with two or more VLAN tags by using an Ethernet type for the MAC condition or an IPv4 condition specified as a flow detection condition.

(3) QoS flow detection for fragmented IPv4 packets

If QoS flow detection uses a TCP/UDP header specified as a flow detection condition for a fragmented IPv4 packet, the second and subsequent fragments cannot be detected because the TCP/UDP header is not in those packets. To perform QoS flow detection for frames that include fragmented packets, specify the MAC header or IP header in the flow detection conditions.

(4) Operation when a QoS entry is changed

If a QoS entry applied to an interface is changed on the Switches, detectable frames cannot be detected until the change has been applied. Consequently, such frames are detected as if they matched another QoS entry.

(5) Concurrent use with other functionality

(a) Statistics for concurrent use with other functionality

If any of the conditions listed below is satisfied for a frame, it is discarded. However, if a frame matches a QoS entry specified for the interface, statistics for that QoS entry are collected.

- Frames are received from the VLAN port whose data transfer status is `Blocking` (data transfer stopped).
- Frames are received from a port specified for inter-port isolation.
- Frames without a VLAN tag are received when the native VLAN is not set as the VLAN that uses a trunk port for sending and receiving frames.
- Received frames that have a VLAN tag are not set for a VLAN that uses a trunk port for sending and receiving frames.
- Frames that match a filter entry specifying discard (including an implicit discard entry) are received.
- Frames with a VLAN Tag are received at protocol or MAC ports.
- Frames are discarded by the MAC address learning functionality.
- Frames are discarded by the Layer 2 authentication functionality.

- Frames are discarded due to an invalid Layer 2 protocol
- Frames are discarded by IGMP snooping or MLD snooping.
- Frames are discarded by DHCP snooping.
- Frames are discarded by storm control.

(6) Restrictions when applying QoS flow detection conditions

For frames to be received in a channel group, only QoS flow detection conditions are applied for a QoS flow group set to a VLAN interface.

3.2 Flow detection configuration

3.2.1 Setting the flow detection mode

The following is an example of specifying the flow detection mode for QoS control.

Points to note

First set the flow detection mode to determine the basic operating conditions of the hardware.

Command examples

1. `(config)# flow detection mode layer2-2`

   Enables Layer 2-2 as the flow detection mode.

3.2.2 Configuring QoS control for multiple interfaces

The following shows an example of specifying QoS control on multiple Ethernet interfaces.

Points to note

By enabling QoS control in `config-if-range` mode, you can set QoS control for multiple Ethernet interfaces.

Command examples

1. `(config)# ip qos-flow-list QOS-LIST1`

   Creates an IPv4 QoS flow list (`QOS-LIST1`), and then switches to IPv4 QoS flow list mode.

2. `(config-ip-qos)# qos ip any host 192.168.100.10 action cos 6`

   Configures the QoS flow list for destination IP address `192.168.100.10`, and then sets a CoS value of 6.

3. `(config-ip-qos)# exit`

   Returns to global configuration mode from IPv4 QoS flow list mode.

4. `(config)# interface range fastethernet 0/1-4`

   Switches to the interface mode for ports 0/1-4.

5. ```
   (config-if-range)# ip qos-flow-group QOS-LIST1 in
   (config-if-range)# exit
   ```

   Enables the IPv4 QoS flow list on the receiving side.
   ```

3.3 Flow detection operation

To make sure that the set information is applied, use the operation command `show qos-flow`.

3.3.1 Checking QoS control operation when IPv4 packets are set as the flow detection condition

The following figure shows how to check QoS control operation when IPv4 packets are set as the flow detection condition.

Figure 3-2 Checking QoS control operation when IPv4 packets are set as the flow detection condition

```
> show qos-flow 0/1

Date 18.09.08 06:47:48 PM UTC
Using Port: interface fastethernet 0/1 in
IP qos-flow-list:QOS-LIST1
  remark "cos 6"
  10 qos tcp any host 10.10.10.2 eq 80 action cos 6
    matched packets        :         0

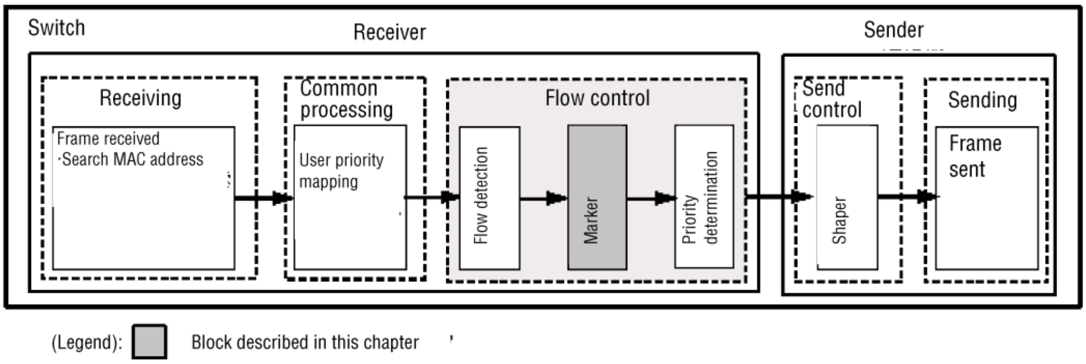
>
```

Make sure that `IP qos-flow-list` is displayed for the QoS control for the specified port.

3.4 Description of marking

Marking is functionality used for updating the user priority in a VLAN tag and the DSCP in an IP header for frames detected by flow detection. The following figure shows the positioning of the marking block described in this section.

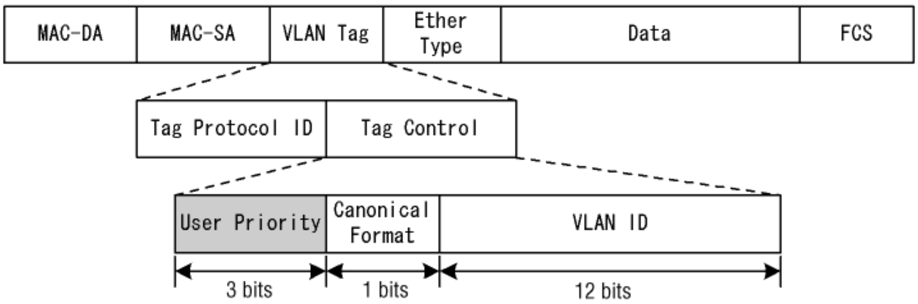
Figure 3-3 Positioning of the marking block



3.4.1 User priority updating

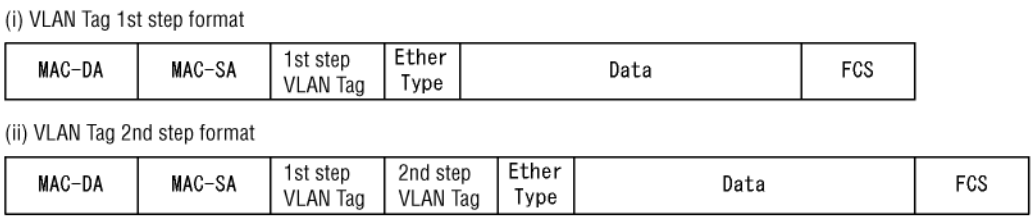
User priority updating is functionality that updates the user priority in the VLAN tag of a frame detected by flow detection. The user priority is the three highest-order bits of the Tag Control field shown in the following figure:

Figure 3-4 Header format of a VLAN tag



When the user priority is updated for frames that have multiple VLAN tags, the user priority in the first VLAN tag encountered when counting from the MAC address side is updated. When the user priority is updated for frames that have multiple VLAN tags, the user priority in the first VLAN tag encountered when counting from the MAC address side is updated.

Figure 3-5 The following figure shows the format of a frame that has multiple VLAN tags.



If user priority updating is not used, the user priority is set as described in the following table.

Table 3-4 User priority when sending frames

User priority ,when sending frames	Applicable frames
3	Frames received without a VLAN tag and sent with a VLAN tag
User priority of received frames	Frames received with a VLAN tag and sent with a VLAN tag

If user priority updating and priority determination are specified at the same time, the user priority is determined by the CoS value determined by the priority determination functionality.

The following table shows user priority when priority determination and user priority updating are specified at the same time.

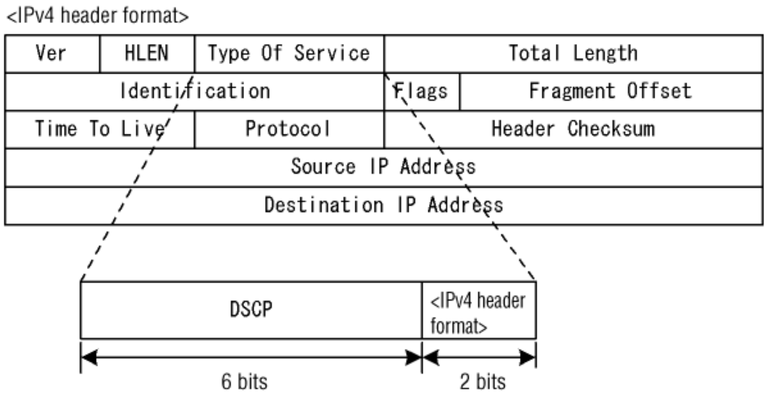
Table 3-5 User priority when priority determination and user priority updating are specified at the same time

CoS value determined by the priority determination	User priority
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

3.4.2 DSCP updating

DSCP updating is functionality that is used to update the DSCP, which is the six highest-order bits of the TOS field in the IPv4 header. The following figure shows the format of the TOS field.

Figure 3-6 Format of the TOS field



As shown, the six highest-order bits of the TOS field of the detected frame are updated.

3.5 Marking configuration

3.5.1 Configuring user priority updating

The following describes the configuration when the user priority is to be updated for certain types of flows.

Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then the user priority is updated.

Command examples

1. `(config)# ip qos-flow-list QOS-LIST1`

   Creates an IPv4 QoS flow list (`QOS-LIST1`), and then switches to IPv4 QoS flow list mode.

2. `(config-ip-qos)# qos ip any host 192.168.100.10 action replace-user-priority 6`

   Configures the IPv4 QoS flow list for destination IP address `192.168.100.10`, and then changes the current user priority to 6.

3. `(config-ip-qos)# exit`

   Returns to global configuration mode from IPv4 QoS flow list mode.

4. `(config)# interface fastethernet 0/1`

   Moves to port 0/1 interface mode.

5. `(config-if)# ip qos-flow-group QOS-LIST1 in`

   `(config-if)# exit`

   Enables the IPv4 QoS flow list (`QOS-LIST1`) on the receiving side.

3.5.2 Configuring DSCP updating

The following describes the configuration when the DSCP is to be updated for certain types of flows.

Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then the DSCP value is updated.

Command examples

1. `(config)# ip qos-flow-list QOS-LIST2`

   Creates an IPv4 QoS flow list (`QOS-LIST2`), and then switches to IPv4 QoS flow list mode.

2. `(config-ip-qos)# qos ip any host 192.168.100.10 action`

`replace-dscp 63`

Configures the IPv4 QoS flow list for destination IP `192.168.100.10`, and then sets that the DSCP value is to be updated to 63.

3. `(config-ip-qos)# exit`

   Returns to global configuration mode from IPv4 QoS flow list mode.

4. `(config)# interface fastethernet 0/3`

   Moves to port 0/3 interface mode.

5. `(config-if)# ip qos-flow-group QOS-LIST2 in`

   `(config-if)# exit`

   Enables the IPv4 QoS flow list (`QOS-LIST2`) on the receiving side.

3.6 Marking operation

To make sure that the set information is applied, use the operation command `show qos-flow`.

3.6.1 Checking user priority updating

The following figure shows how to check user priority updating.

Figure 3-7 Checking user priority updating

```
> show qos-flow 0/2

Date 18.09.08 06:55:30 PM UTC
Using Port: interface fastethernet 0/2 in
IP qos-flow-list:  QOS-LIST10
  remark "cos 4"
  10 qos ip any host 192.168.100.10 action replace-user-priority 6
    matched packets        :         0
>
```

Make sure that `replace-user-priority 6` is displayed in the information for `QOS-LIST10`.

3.6.2 Checking DSCP updating

The following figure shows how to check the DSCP updating.

Figure 3-8 Checking DSCP updating

```
> show qos-flow 0/3

Date 18.09.08 06:57:25 PM UTC
Using Port: interface fastethernet 0/3 in
IP qos-flow-list: QOS-LIST20
  remark "cos 4"
  10 qos ip any host 192.168.100.10 action replace-dscp 63
    matched packets        :         0
>
```

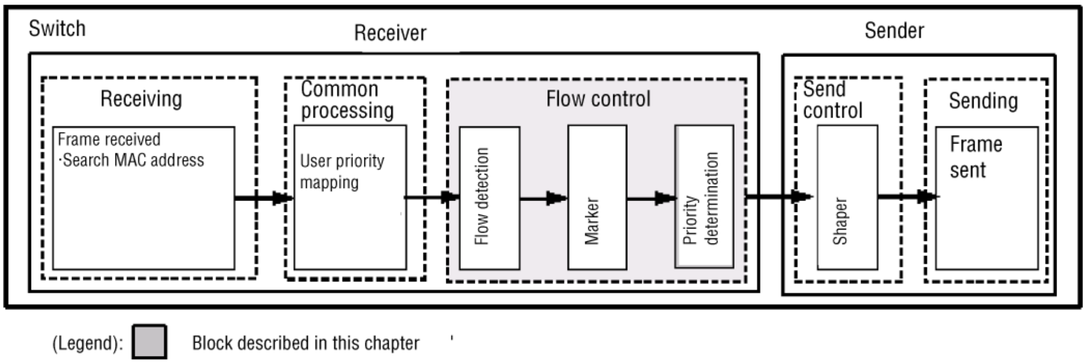
Make sure that `replace-dscp 63` is displayed in the information for `QOS-LIST20`.

3.7 Description of priority determination

Priority determination is functionality that uses CoS values to specify the priority of frames detected by flow detection in order to determine the send queue.

The following figure shows the positioning of the priority determination block described in this section.

Figure 3-9 Positioning of the priority determination block



3.7.1 CoS value

CoS values are used as an index for showing the priority of frames on the Switch.

The following table describes the specifiable range of CoS values.

Table 3-6 Specifiable range of CoS values

Item	Range
CoS value	0 to 7

If priority determination is not set for flow control, the following default CoS values are used.

Table 3-7 Default CoS values

Item	Default value	Frame type
CoS value	Conforms to the result of user priority mapping	Frames that do not match priority determination for flow control Frames that match priority determination for flow control and whose priority determination is not set

Note that the CoS values are fixed for the frames indicated in the table below regardless of whether priority determination for flow control is set.

The following table indicates the frames whose values cannot be changed by priority determination.

Table 3-8 Frames whose values cannot be changed by priority determination

Frame type	CoS value
Frames spontaneously sent by the Switch (IP packets: ping, Telnet, FTP, etc.)#2	#1
Frames spontaneously sent by the Switch (other than IP packets: BPDU, LLDP, LACP, etc.) #3	7
The following frames received by the Switch: ● Spanning tree (BPDU) ● Link aggregation ● LLDP ● GSRP (GSRP aware) ● CFM	7
The following frames received by the Switch: ● Frame addressed to the MAC address of the Switch ● Flush control frame (for unlink redundancy)	6
The following frames received by the Switch: ● IGMP/MLD snooping ● Frame working as a MAC authentication trigger received from a port on MAC authentication legacy mode ● EAPOL	5

#1

You cannot change the value with propriety determination by flow control, but it is mapped with a setting of the configuration command `control-packet user-priority`. For details, see *3.10 Explanation of user priority for self-generated frames.*

#2

The IGMP and MLD cannot be changed.

#3

The BPDU that has a VLAN tag, L2 loop detection, and flush control frame for uplink redundancy are classified into here.

3.7.2 CoS mapping functionality

The CoS mapping functionality determines the send queue based on the CoS value determined by either user priority mapping or priority determination for flow control.

The following table shows the mapping of CoS values to send queues.

Table 3-9 Mapping of CoS values and send queues

CoS value	Queue number for sending		
	Send queue length: 32	**Send queue length: 128**	**Send queue length: 728**
0	1	1	1

CoS value	Queue number for sending		
	Send queue length: 32	**Send queue length: 128**	**Send queue length: 728**
1	2	1	1
2	3	2	1
3	4	2	1
4	5	3	1
5	6	3	1
6	7	4	1
7	8	4	2

- For the send queue length, also see *4.1.2 Specifying the send queue length*.

3.7.3 Notes on using priority determination

(1) Priority determination for frames sent to a Switch

On a Switch, frames to be forwarded and frames sent to the Switch are subject to QoS flow detection. Therefore, when the priority of frames sent to a Switch is set to the value equivalent or higher than the CoS value of received frames shown in *Table 3-8 Frames whose values cannot be changed by priority determination*, a higher load to frames received by the Switch might interfere with the reception of protocol control frames.

If this problem occurs, specify an operation that lowers the priority of the frame to the Switch.

3.8 Priority determination configuration

3.8.1 Configuring the CoS value

Sets the CoS value for certain types of flows.

Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then the CoS value is set.

Command examples

1. `(config)# ip qos-flow-list QOS-LIST1`

   Creates an IPv4 QoS flow list (`QOS-LIST1`), and then switches to IPv4 QoS flow list mode.

2. `(config-ip-qos)# qos ip any host 192.168.100.10 action cos 6`

   Configures the IPv4 QoS flow for destination IP address `192.168.100.10`, and then sets a CoS value of 6.

3. `(config-ip-qos)# exit`

   Returns to global configuration mode from IPv4 QoS flow list mode.

4. `(config)# interface fastethernet 0/1`

   Moves to port 0/1 interface mode.

5. `(config-if)# ip qos-flow-group QOS-LIST1 in`

   `(config-if)# exit`

   Enables the IPv4 QoS flow list (`QOS-LIST1`).

3.9 Priority operation

3.9.1 Checking the priority

When traffic (frames whose destination IP address is 192.168.100.10) flows into a line, use the operation command `show qos queuing` to check the queue number. The target Ethernet interface is port 0/1.

Figure 3-10 Checking the priority

```
> show qos queueing 0/1

Date 21.11.08 12:07:46 PM UTC
Port 0/1 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=10Mbit/s, Qmode=wfq/tail_drop
  Queue 1: Qlen=    0, Limit_Qlen=   32
  Queue 2: Qlen=    0, Limit_Qlen=   32
  Queue 3: Qlen=    0, Limit_Qlen=   32
  Queue 4: Qlen=    0, Limit_Qlen=   32
  Queue 5: Qlen=    0, Limit_Qlen=   32
  Queue 6: Qlen=    1, Limit_Qlen=   32
  Queue 7: Qlen=    0, Limit_Qlen=   32
  Queue 8: Qlen=    0, Limit_Qlen=   32
   discard packets
    HOL1=       0, HOL2=       0, Tail_drop=       0

>
```

Make sure that the `Qlen` value for `Queue 6` has a count value.

3.10 Explanation of user priority for self-generated frames

You can change the user priority of frames generated by a Switch itself to an arbitrary value using the configuration command `control-packet user-priority`. The user priority can be specified by Layer 2 and Layer 3 of self-generated frames. Frames on the same layer whose user priority is specified operate using the same user priority value.

In case that configuration is not set, the user priority of self-generated frames is 7.

Because this setting is applied after the setting value is entered, you do not have to restart the Switch.

The following table describes the frame type in each protocol and user priority setting range.

Table 3-10 Self-generated frame types and user priority setting ranges

Self-generated frame type	Layer	Setting range of control-packet user-priority		
		User priority (default)	**Layer to specify user priority**	**User priority setting range**
BPDU # L2 loop detection# Flush control frame (for uplink redundancy)# MAC address update frame (for uplink redundancy)# CFM#	2	7	layer-2	0 to 7
ICMP ARP Telnet FTP NTP SNMP syslog IGMP MLD Start command (for secure Wake on LAN)	3	7	layer-3	0 to 7

#

The user priority cannot be set for Layer 2 self-generated frames other than those shown in the above table, because they do not have VLAN tags.

When the user priority of self-generated frames is set, the CoS value of self-generated frames are mapped as shown in the following table. The CoS value of BPDU/L2 loop detection/flush control frame for uplink redundancy/ IGMP/MLD/CFM is always mapped to 7 and that of other frames is mapped according to the setting value of the user priority.

Table 3-11 Mapping of user priority of self-generated frames to CoS values

Self-generated frame type	Setting value of control-packet user-priority		Mapped CoS values
BPDU L2 Loop Detection Flush control frame (for uplink redundancy) MAC address update frame (for uplink redundancy) CFM	Layer-2	0 to 7	7
IGMP MLD	Layer-3		
ICMP	Layer-3	0	0
ARP		1	1
Telnet		2	2
FTP		3	3
NTP		4	4
SNMP		5	5
syslog		6	6
Start command (for secure Wake on LAN)		7	7

3.11 Configuring user priority for self-generated frames

3.11.1 Setting user priority for self-generated frames

Points to note

The user priority value of self-generated frames is set by layer.

Command examples

1. `(config)# control-packet user-priority layer-2 5`

   Sets the user priority of Layer 2 self-generated frames to 5.

   The user priority of Layer 3 self-generated frames that are not specified is 7.

Points to note

The user priority values of both Layer 2 and Layer 3 self-generated frames are set.

Command examples

1. `(config)# control-packet user-priority layer-2 5 layer-3 2`

   Sets the user priority of Layer 2 self-generated frames to 5 and Layer 3 self-generated frames to 2.

4. Send Control

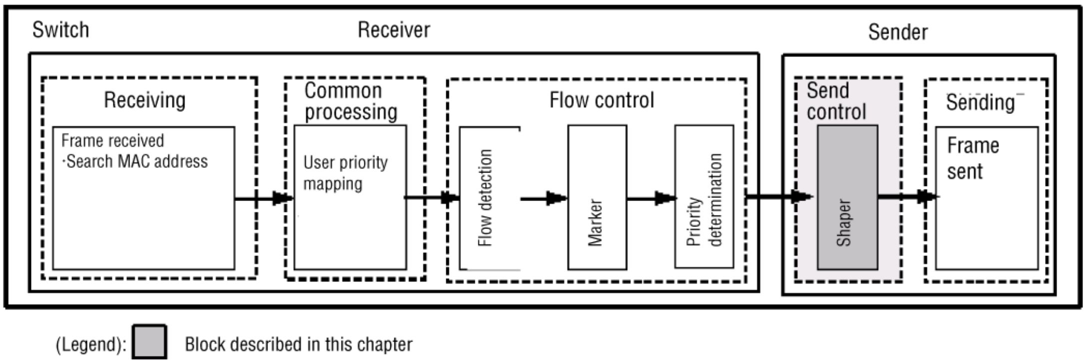
This chapter describes send control (shaper) used on the Switch.

4.1 Description of the shaper

4.1.1 Overview of the legacy shaper

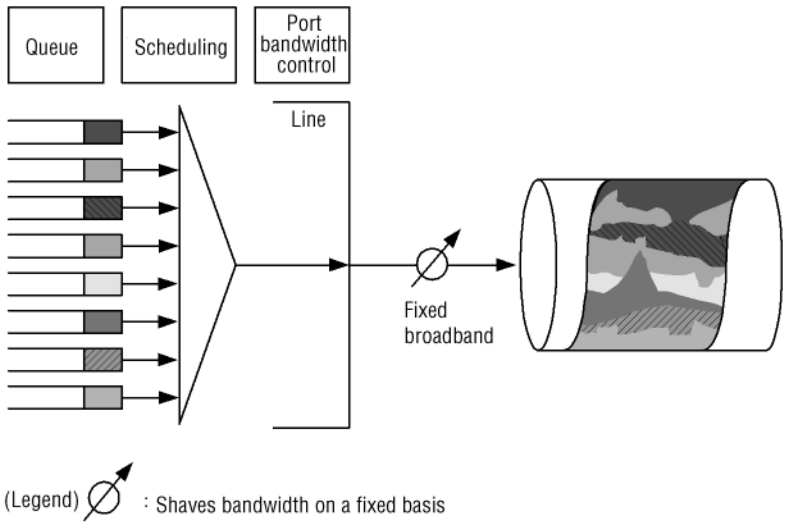
The shaper functionality is used to control the output order of frames from each queue and output bandwidth for each port. The following figure shows the positioning of the shaper block described in this section.

Figure 4-1 Positioning of the shaper block



As shown in the figure below, the legacy shaper consists of scheduling, which determines the queue from which the next frame will be sent, and port bandwidth control, which shapes the Ethernet interface bandwidth. The following figure provides an overview of the legacy shaper.

Figure 4-2 Overview of the legacy shaper



4.1.2 Specifying the send queue length

You can change the send queue length on the Switch to fit the network configuration and operation mode. To do so, use the `limit-queue-length` configuration command. Increasing the send queue length can reduce queue overflows caused by burst traffic. Note that the specified send queue length is in effect for all Ethernet interfaces on the Switch.

If you do not specify the send queue length, a default queue length of 32 is used.

Table 4-1 Statuses of send queue lengths when they are specified

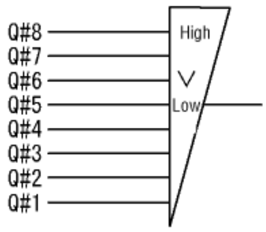
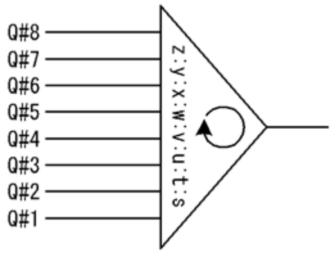
Queue number	Send queue length: 32	Send queue length: 128	Send queue length: 728
1	32	128	728
2	32	128	32
3	32	128	0
4	32	128	0
5	32	0	0
6	32	0	0
7	32	0	0
8	32	0	0

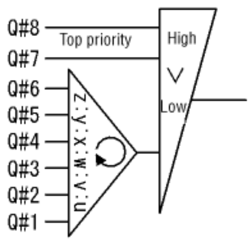
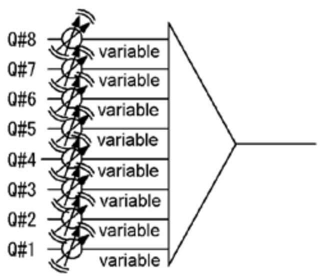
For details about send queue length and CoS mapping, see *Table 3-9 Mapping of CoS values and send queues.*

4.1.3 Scheduling

Scheduling is functionality that controls the order in which the frames in each queue will be sent. The Switch provides the four types of scheduling functionality described below. The following table describes the scheduling operations:

Table 4-2 Scheduling operations

Scheduling type	Conceptual diagram	Description	Application example
PQ		Priority queuing. When frames are queued in multiple queues, frames from queue 8 (Q#8 in the figure on the left), which has the highest priority, are always given priority.	When traffic priority must be strictly observed
WRR		Weighted (number of frames) round-robin. When there are frames in multiple queues, while looking at the queues in order, depending on the set weights (z, y, x, w, v, u, t, s), frames are sent from queues 8 to 1 (Q#8 to Q#1 in the figure on the left).	When sending all types of traffic is required and there is both preferential and non-preferential traffic

Scheduling type	Conceptual diagram	Description	Application example
2PQ+6WRR		Top-priority queues and weighted (number of frames) round robin. Frames in top-priority queue 8 (Q#8 in the figure on the left) are always given priority. Frames in queue 7 (Q#7 in the figure on the left), which is given priority after queue 8, are then sent. If there are no frames to be sent from queues 8 and 7, then frames are sent from queues 6-1 (Q#6 to Q#1 in the figure on the left), based on the set weights (z, y, x, w, v, u).	When video and audio data is used for the most preferred queue and the WRR queue is used for data traffic
WFQ		Weighted fair queuing. When a weight (minimum guaranteed bandwidth) is set for all queues, frames corresponding to the minimum bandwidth are sent from each queue.	When the minimum guaranteed bandwidth is requested for all traffic

The following table describes the scheduling specifications.

Table 4-3 Scheduling specifications

Item		Specifications
Number of queues		Eight
2PQ+6WRR	Setting range of the weights for queues 1 to 6	1 to 15
WFQ	Setting range of the weights for queues 1 to 8	See *Table 4-4 WFQ setting range.* Make sure that the sum of the minimum guaranteed bandwidths is equal to or smaller than the line bandwidth.
	The part of a frame to which the minimum guaranteed bandwidth applies	From the MAC header to the FCS header

The table below shows the WFQ setting range. WFQ does not work normally if the line status is in half duplex mode. Use WFQ in full-duplex mode.

Table 4-4 WFQ setting range

Setting unit[#1]	Setting range	Increment
Mbit/s	1 M to 1,000 M	1 Mbit/s
kbit/s	1000 to 1000000	100 kbit/s[#2]
	64 to 960	64 kbit/s[#3]

#1

1 M is treated as 1000000, and 1 k is treated as 1000 (k is used for the units of values in configurations displayed by operation commands).

#2

To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...1000000).

#3

To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192...960).

4.1.4 Port bandwidth control

The port bandwidth control functionality shapes the traffic to the send bandwidth specified for the relevant port after scheduling is performed. You can use this control to connect to wide-area Ethernet services.

For example, if the line bandwidth is 1 Gbit/s and the contract bandwidth with the ISP is 400 Mbit/s, you can use port bandwidth control to suppress the bandwidth to 400 Mbit/s or less when sending frames.

The following table shows the setting range for port bandwidth control. Set the bandwidth so that it is equal to or smaller than the line speed. Port bandwidth control does not work when the line status is in half duplex mode.

Table 4-5 Setting range for port bandwidth control

Setting unit[#1]	Setting range	Increment
Mbit/s	1 M to 1,000 M	1 Mbit/s
kbit/s	1000 to 1000000	100 kbit/s[#2]
	64 to 960	64 kbit/s[#3]

#1

1 M is treated as 1000000, and 1 k is treated as 1000 (k is used for the units of values in configurations displayed by operation commands).

#2

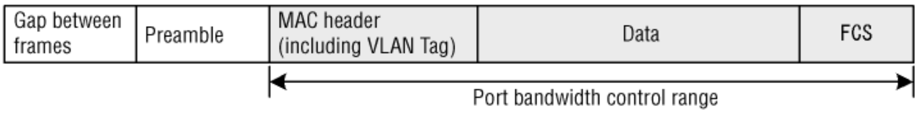
To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...1000000).

#3

To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192...960).

The part of a frame to which port bandwidth control applies is from the MAC header to the FCS. The following figure shows the part of the frame to which port bandwidth control applies.

Figure 4-3 Part of the frame to which port bandwidth control applies



4.1.5 Notes on using the shaper

(1) Notes on specifying the send queue length

- After changing the send queue length, restart the Switch to set basic operating conditions.
- Set the scheduling mode PQ before setting the send queue length. The PQ scheduling mode cannot be set from other scheduling modes.
- If the configuration command `limit-queue-length` has not been input, any scheduling mode is available.
- To set 728 for the send queue length, set "Send pause packets" via the `flowcontrol` configuration command.

(2) Note on scheduling when the packet buffer is depleted

If traffic exceeding the bandwidth of the output line is received, the packet buffer on the Switch might be depleted. As a result, frames might not be sent according to the specified schedule because the received frames are discarded and are not queued in the queue.

To check the packet buffer, execute the `show qos queuing` operation command, and check whether the `HOL1` and `HOL2` counters are incrementing.

If the packet buffer is depleted frequently, you need to review the network design.

4.2 Shaper configuration

4.2.1 PQ configuration

Points to note

The example below shows how to create QoS queue list information that sets PQ (priority queuing) for legacy shaper mode, and then applies that information to the relevant ports.

Command examples

1. `(config)# qos-queue-list QUEUE-PQ pq`

   Sets priority queuing for legacy shaper mode of the QoS queue list QoS name (`QUEUE-PQ`).

2. `(config)# interface fastethernet 0/11`

   Moves to port 0/11 interface mode.

3. `(config-if)# qos-queue-group QUEUE-PQ`

   `(config-if)# exit`

   Enables the QoS queue list (`QUEUE-PQ`).

4.2.2 WRR configuration

Points to note

The example below shows how to create QoS queue list information that sets WRR (weighted round robin) for legacy shaper mode, and then applies that information to the relevant ports.

Command examples

1. `(config)# qos-queue-list QUEUE-WRR wrr 1 2 3 4 6 8 10 12`

   Sets WRR for legacy shaper mode of the QoS queue list QoS name (`QUEUE-WRR`).

2. `(config)# interface fastethernet 0/14`

   Moves to port 0/14 interface mode.

3. `(config-if)# qos-queue-group QUEUE-WRR`

   `(config-if)# exit`

   Enables the QoS queue list (`QUEUE-WRR`).

4.2.3 2PQ+6WRR configuration

Points to note

The example below shows how to create QoS queue list information that sets

2PQ+6WRR (priority queuing + weighted (number of frames) round robin) for legacy shaper mode, and then applies that information to the relevant ports.

Command examples

1. `(config)# qos-queue-list QUEUE-PQ-WRR 2pq+6wrr 1 2 4 4 8 12`

   Sets 2pq+6wrr for legacy shaper mode of the QoS queue list QoS name (`QUEUE-PQ-WRR`).

2. `(config)# interface fastethernet 0/16`

   Moves to port 0/16 interface mode.

3. `(config-if)# qos-queue-group QUEUE-PQ-WRR`

   `(config-if)# exit`

   Enables the QoS queue list (`QUEUE-PQ-WRR`).

4.2.4 WFQ configuration

Points to note

The example below shows how to create QoS queue list information that sets WFQ (weighted fair queuing) for legacy shaper mode, and then applies that information to the relevant ports.

Command examples

1. `(config)# qos-queue-list QUEUE-WFQ wfq min-rate1 2M min-rate2 2M min-rate3 2M min-rate4 4M min-rate5 10M min-rate6 10M min-rate7 10M min-rate8 20M`

   Sets WFQ for legacy shaper mode of the QoS queue list QoS name (`QUEUE-WFQ`).

2. `(config)# interface fastethernet 0/6`

   Moves to port 0/6 interface mode.

3. `(config-if)# qos-queue-group QUEUE-WFQ`

   `(config-if)# exit`

   Enables the QoS queue list (`QUEUE-WFQ`).

4.2.5 Configuring port bandwidth control

The following describes how to set the output bandwidth of the relevant port so that it is lower than the bandwidth of the actual line.

Points to note

The example below shows how to use port bandwidth control to set the bandwidth for the relevant port (100 Mbit/s) to 20 Mbit/s.

Command examples

1. `(config)# interface fastethernet 0/3`

Moves to port 0/3 interface mode.

2.
```
(config-if)# traffic-shape rate 20M
(config-if)# exit
```
Sets the port bandwidth to 20 Mbit/s.

4.3 Shaper operation

Use the `show qos queuing` operation command to view the information about the legacy shaper set for an Ethernet interface.

4.3.1 Checking the scheduling

The following shows how to check the scheduling.

Figure 4-4 Checking the scheduling

```
> show qos queueing 0/11

Date 21.11.08 12:08:10 PM UTC
Port 0/11 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=100Mbit/s, Qmode=pq/tail_drop
  Queue 1: Qlen=    0, Limit_Qlen=   32
  Queue 2: Qlen=    0, Limit_Qlen=   32
  Queue 3: Qlen=    0, Limit_Qlen=   32
  Queue 4: Qlen=    0, Limit_Qlen=   32
  Queue 5: Qlen=    0, Limit_Qlen=   32
  Queue 6: Qlen=    0, Limit_Qlen=   32
  Queue 7: Qlen=    0, Limit_Qlen=   32
  Queue 8: Qlen=    0, Limit_Qlen=   32
   discard packets
    HOL1=        0, HOL2=        0, Tail_drop=        0

>
```

Confirm that the `Qmode` parameter is `pq/tail_drop`.

4.3.2 Checking port bandwidth control

The following shows how to check port bandwidth control.

Figure 4-5 Checking port bandwidth control

```
> show qos queueing 0/3

Date 21.11.08 12:15:23 PM UTC
Port 0/3 (outbound)
 Status : Active
 Max_Queue=8, Rate_limit=20Mbit/s, Qmode=pq/tail_drop
  Queue 1: Qlen=    0, Limit_Qlen=   32
  Queue 2: Qlen=    0, Limit_Qlen=   32
  Queue 3: Qlen=    0, Limit_Qlen=   32
  Queue 4: Qlen=    0, Limit_Qlen=   32
  Queue 5: Qlen=    0, Limit_Qlen=   32
  Queue 6: Qlen=    0, Limit_Qlen=   32
  Queue 7: Qlen=    0, Limit_Qlen=   32
  Queue 8: Qlen=    0, Limit_Qlen=   32
   discard packets
    HOL1=        0, HOL2=        0, Tail_drop=        0

>
```

Confirm that the `Rate_limit` parameter is `20Mbit/s`.

5. Overview of Layer 2 Authentication

These Switches support Layer 2 authentication methods such as IEEE 802.1X, Web authentication, and MAC-based authentication. This chapter describes the Layer 2 authentication method types supported by the Switches, common Layer 2 authentication methods, and interoperability of Layer 2 authentication. Note that the term *authentication functionality* is sometimes used instead of the term *authentication method*.

5.1 Overview of Layer 2 authentication

5.1.1 Layer 2 authentication types

The Switch supports the Layer 2 authentication methods in the table below.

Table 5-1 Supported Layer 2 authentication methods

Authentication type	Authentication method	Authentication method group	Authentication mode	Authentication sub-mode
Single authentication	IEEE802.1X	Switch default[#] Authentication method list	Port-based authentication (static) Port-based authentication (dynamic)	Single-terminal mode Terminal authentication mode
		Switch default[#]	VLAN-based authentication (dynamic)	--
	Web authentication	Switch default Authentication method list	Fixed VLAN mode Dynamic VLAN mode	--
		Switch default	Legacy mode	--
	MAC-based authentication	Switch default Authentication method list	Fixed VLAN mode Dynamic VLAN mode	--
		Switch default	Legacy mode	--
Multistep authentication	MAC-based authentication and IEEE 802.1X	Switch default[#] Authentication method list	Fixed VLAN mode Dynamic VLAN mode	IEEE 802.1X is used in terminal authentication mode
	MAC-based authentication and Web authentication		Fixed VLAN mode Dynamic VLAN mode	--
	IEEE 802.1X and Web authentication		Fixed VLAN mode Dynamic VLAN mode	IEEE 802.1X is used in terminal authentication mode

Legend:

--: None

#

Switch default IEEE 802.1X works with RADIUS authentication.

- Single authentication

  IEEE 802.1X, Web authentication and MAC-based authentication work independently.

- Multistep authentication

  Authentication is conducted in two steps. After the first authentication is finished, the second one starts. The Switch conducts IEEE 802.1X or Web authentication after completing MAC-based authentication. Web authentication can be conducted after IEEE 802.1X authentication is completed by using the terminal authentication `dot1x` option.

  For details about multistep authentication, see *12. Multistep authentication.*

- IEEE802.1X

  This method includes port-based authentication based on the IEEE 802.1 X port and VLAN-based authentication (dynamic) based on the VLAN MAC address.

  Both methods can use an ordinary RADIUS server for authentication, which is suitable for relatively small or medium systems.

  They can also use terminals including IEEE 802.1X's Supplicant software.

- Web authentication

  With this method, the user enters a user ID and password in a general Web browser from a terminal, and then authentication is performed through an internal authentication database (internal Web authentication DB) or an ordinary RADIUS server to permit or deny access to a VLAN specified by a MAC address.

  This method can be used from terminals with Web browsers such as Internet Explorer.

- MAC-based authentication

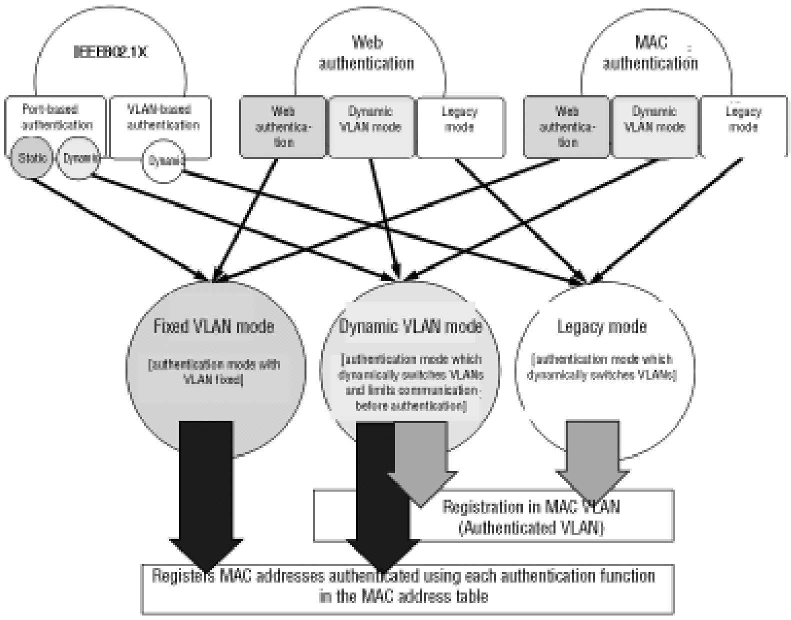
  This method performs authentication by using the MAC addresses of frames received from terminals through an internal authentication database (internal MAC-based authentication DB) or an ordinary RADIUS server to permit or deny access to a VLAN specified by a MAC address. This enables authentication without the need to install special software on terminals.

  This functionality authenticates terminals (for example, printers or IP telephones) without IEEE 802.1X's Supplicant software, or for which user IDs or passwords cannot be entered.

5.1.2 Authentication modes of each authentication method

Each authentication method works in fixed VLAN mode, dynamic VLAN mode, or legacy mode. The following figure shows the mutual relationships between authentication methods and authentication modes.

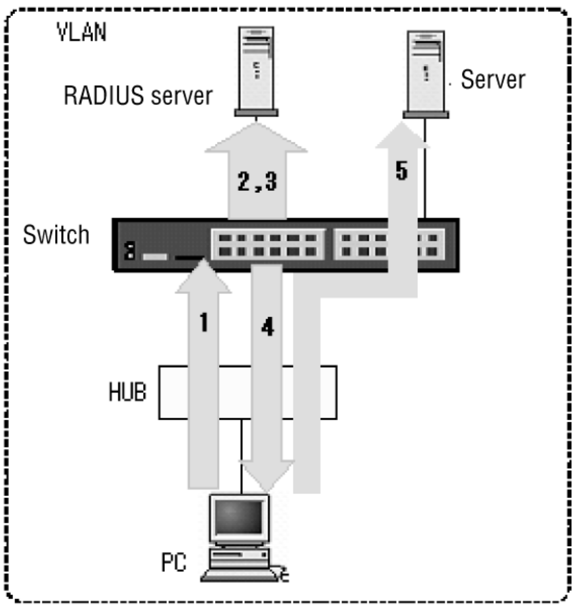
Figure 5-1 Mutual relationships between authentication methods and authentication modes



(1) Fixed VLAN mode

Fixed VLAN mode does not perform VLAN switching to a VLAN to which an authentication-requesting terminal belongs before and after authentication. The VLAN to which the terminal belongs is the VLAN to which the connection port of the terminal belongs.

Figure 5-2 Overview of fixed VLAN mode (for RADIUS authentication)



1. A user accesses the Switch from an authentication-requesting terminal (PC in

the figure above) connected via a hub.

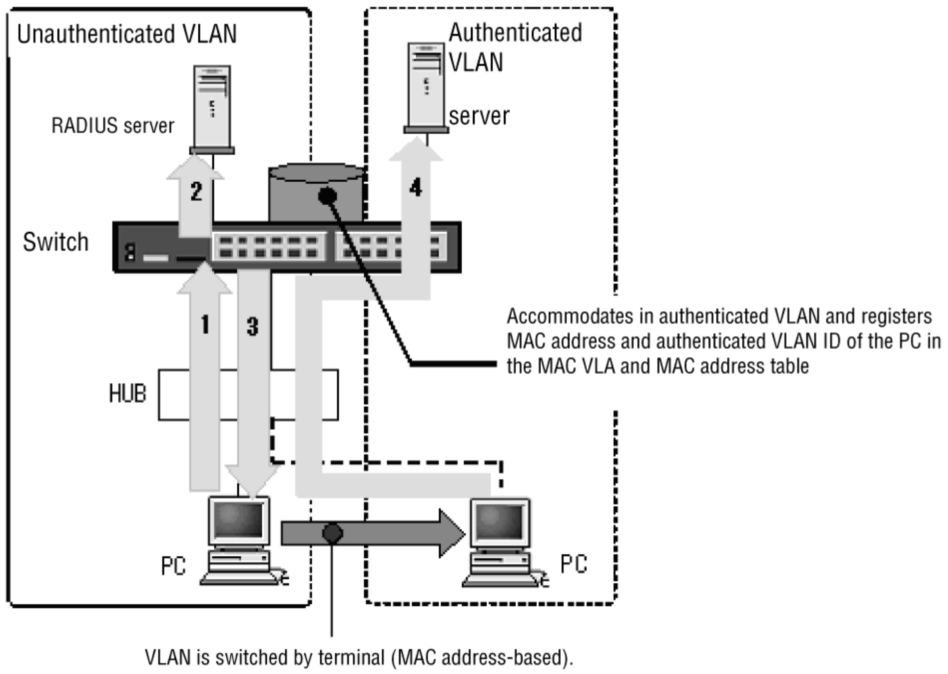
2. This system identifies the ID of a VLAN associated with the terminal based on its connection port or VLAN ID.
3. After the identified VLAN ID information is added to the terminal information and an authentication request is made to the RADIUS server, the VLANs for which authentication is possible can be limited.
4. If authentication succeeds, a page opens on the terminal indicating that authentication was successful. (For Web authentication)
5. The authenticated terminal can connect to a server of the post-authentication VLAN.

(2) Dynamic VLAN mode

In dynamic VLAN mode, VLANs are switched after authentication through MAC VLANs. The MAC address and VLAN ID of a successfully authenticated terminal are registered in the MAC VLAN and MAC address table.

A VLAN to which unauthenticated terminals belong is called a pre-authentication VLAN. The VLAN to which the terminal belongs after authentication is called the *post-authentication VLAN*.

Figure 5-3 Overview of dynamic VLAN mode (for RADIUS authentication)



1. A user accesses the Switch from an authentication-requesting terminal (PC in the figure above) connected via a hub.
2. Authentication is conducted by an external RADIUS server.
3. If authentication succeeds, a page opens on the terminal indicating that authentication was successful. (For Web authentication)

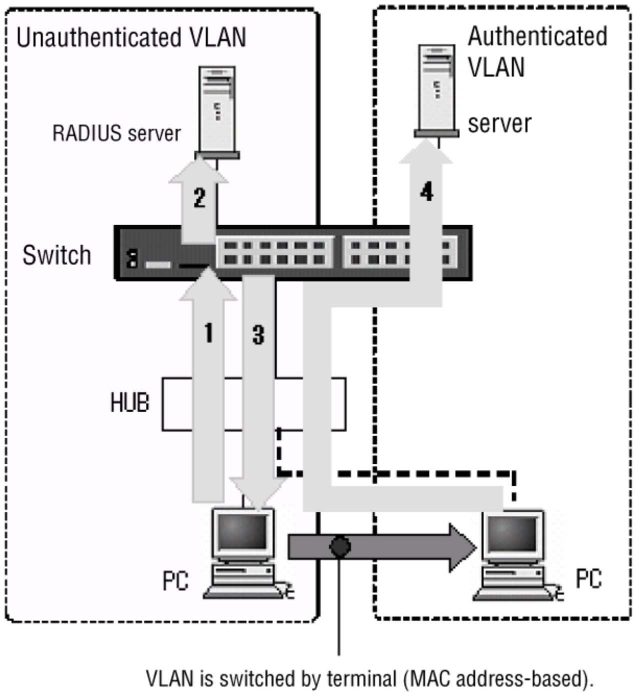
4. Based on the VLAN ID information sent by a RADIUS server, the authenticated terminal gains access to the post-authentication VLAN and can connect to the server.

(3) Legacy mode

In legacy mode, the Switch authenticates and inspects each authentication-requesting terminal by using the MAC VLAN functionality, and dynamically assigns VLANs to them to separate networks before and after authentication.

A VLAN to which unauthenticated terminals belong is called a pre-authentication VLAN. The VLAN to which the terminal belongs after authentication is called the *post-authentication VLAN*.

Figure 5-4 Overview of legacy mode (example of RADIUS authentication)



1. A user accesses the Switch from an authentication-requesting terminal (PC in the figure above) connected via a hub.
2. Authentication is conducted by an external RADIUS server.
3. If authentication succeeds, a page opens on the terminal indicating that authentication was successful. (For Web authentication)
4. Based on VLAN ID information sent by a RADIUS server and the post-authentication information specified in the configuration, the authenticated terminal gains access to the post-authentication VLAN.

(4) Capacity limit and mixed usage for authentication methods

For capacity limit of each authentication method, see *3.2 Capacity limits* in the *Configuration Guide Vol. 1*.

Authentication methods can be mixed and used within a Switch or on the same port. For details, see *5.7 Interoperability of Layer 2 authentication with other functionality*.

For details about authentication methods, see the later chapters.

5.1.3 Authentication method groups

For each authentication method, you can select *Switch default*, which is the standard for the entire Switch, or *authentication method list*, which applies to different RADIUS servers based on what conditions are met.

Table 5-2 Authentication method groups for Switch

Authentication method group	Selection range	Authentication request destination
Switch default	Local authentication	Internal authentication database
	RADIUS authentication	Host of authentication RADIUS server information
		Host of general-use RADIUS server information
Authentication method list	RADIUS server group	Server host in a specified RADIUS server group

(1) Switch default

For each authentication method, you can specify the type of authentication method for Switch default. There are two types of authentication methods: *local authentication* and *RADIUS authentication*. In addition, they can be configured separately or together. For details, see *5.3.3 Priority configuration for the Switch default local and RADIUS authentications.*

(a) Local authentication

This method checks the user ID and password, or MAC address, of a terminal against an internal database on the Switch (internal Web authentication or MAC-based authentication DB) and permits authentication when they match. The internal databases are registered on the Switch via operation commands.

(b) RADIUS authentication

This method sends the user ID and password, or MAC address, of a terminal to a RADIUS server and permits authentication when they match.

An ordinary external RADIUS server is used. Information about users (or terminals) subject to authentication is registered on the RADIUS server. For the registration procedures for user information on a RADIUS server, see the documentation for your RADIUS server.

In addition, RADIUS server information, such as the IP address and RADIUS key of the RADIUS authentication server, is registered on the Switch. The configured information includes general-use RADIUS server information and information about the dedicated RADIUS authentication server. For details, see *5.3.1 RADIUS server information used with the Layer 2 authentication method.*

(2) Authentication method list

For each authentication method, you can specify an authentication method list that applies to different RADIUS servers based on what conditions are met.

Only RADIUS server groups can be configured for an authentication method list.

Up to four entries for each authentication method can be registered in an authentication method list. For details, see *5.2 Authentication method group*.

Up to four RADIUS server groups can be configured for the entire Switch. For details, see *5.3.1 RADIUS server information used with the Layer 2 authentication method* and *8. Login Security and RADIUS* in the *Configuration Guide Vol. 1*.

5.2 Authentication method group

5.2.1 Overview

This section uses Web authentication as an example to describe a correlation diagram between the Switch default configuration, and the authentication method list configuration for RADIUS servers under certain conditions.

Normally, the Switch executes local authentication or RADIUS authentication based on the Switch default configuration.

- Switch default

  When RADIUS authentication is executed with Switch default, a general-use RADIUS server or authentication RADIUS server can be used.

  Up to four authentication RADIUS servers can be configured for each Layer 2 authentication method.

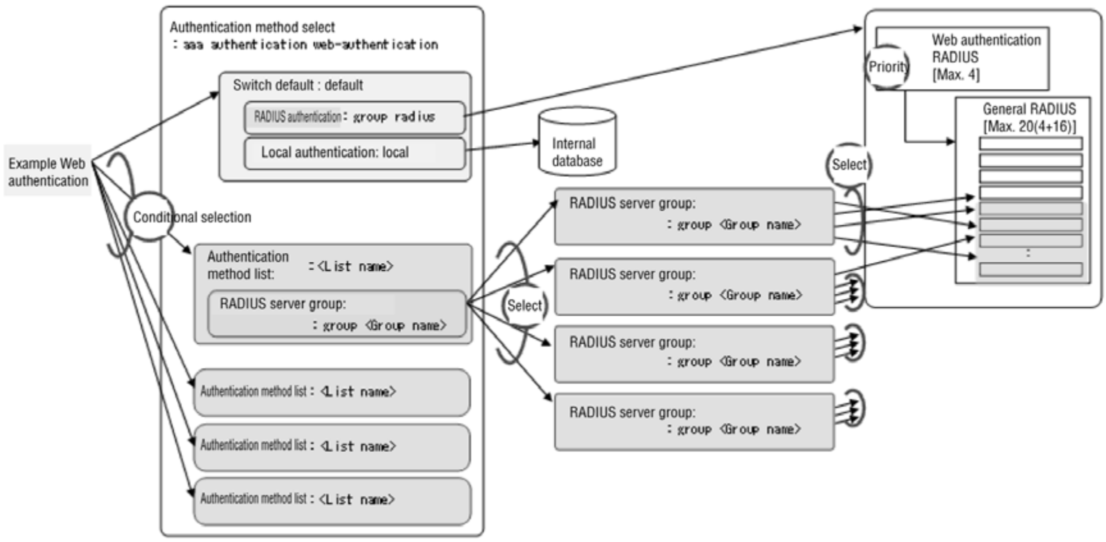
- Authentication method list

  Set specific conditions when using the authentication method list functionality.

  If the specific conditions are met, the Switch uses the RADIUS server group name registered in the authentication method list.

  To determine a RADIUS server group, specify and use the IP address of a general-use RADIUS server.

Figure 5-5 Correlation diagram of authentication method list configuration



5.2.2 Authentication method list

The authentication method list uses the following conditions:

- Port-based authentication
- User ID-based authentication method

The following table shows the possible authentication modes.

Table 5-3 Supported authentication modes of authentication method lists

Authentication type	Authentication mode	Port-based authentication method	User ID-based authentication method
IEEE802.1X	Port-based authentication (static)	Y	N
	Port-based authentication (dynamic)	Y	N
	VLAN-based authentication (dynamic)	N	N
Web authentication	Fixed VLAN mode	Y	Y
	Dynamic VLAN mode	Y	Y
	Legacy mode	N	N
MAC-based authentication	Fixed VLAN mode	Y	N
	Dynamic VLAN mode	Y	N
	Legacy mode	N	N

Legend:

Y: Supported

N: Not supported

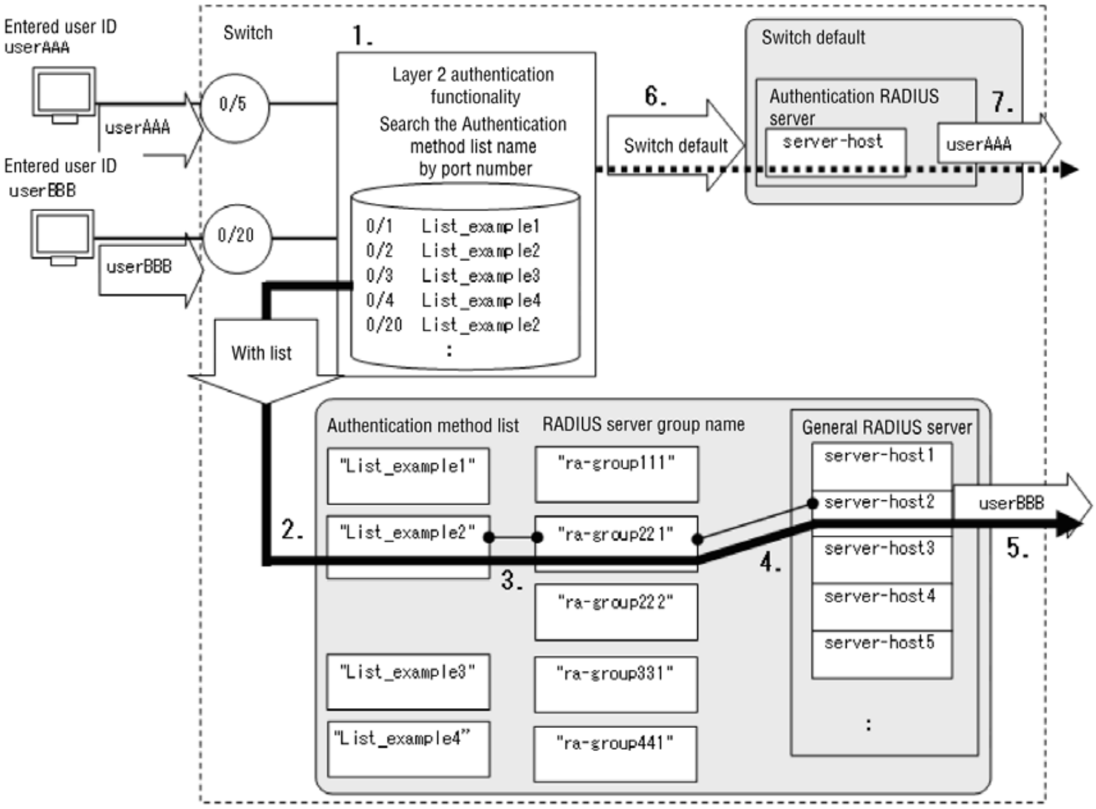
(1) Port-based authentication

This method uses an individual RADIUS server for authentication for each authentication port.

The method performs RADIUS authentication for a RADIUS server group specified in the authentication method list by specifying the authentication method list name for any authentication port.

The following figure shows an operational overview of the port-based authentication method.

Figure 5-6 Operational overview of the port-based authentication method



If an authentication method list name is configured for an authentication port:

1. When an authentication port receives an authentication request, the Switch checks whether the name of an authentication method list has been specified for the port by using an appropriate authentication method.
2. The Switch checks whether the authentication method list name (`List_example2` in the figure) is registered in the authentication method lists in the Switch.
3. If the name corresponds to a list on the Switch, the Switch references the RADIUS server group specified in the authentication method list (`ra-group221` in the figure).
4. The Switch checks the IP address of the general-use RADIUS server registered in the RADIUS server group (`server-host2` in the figure).
5. The Switch sends an authentication request to the target RADIUS server

If an authentication method list name is not configured for an authentication port:

6. If no authentication method list name has been specified for a port, the Switch references the IP address for the authentication RADIUS server for the appropriate authentication method. If an authentication RADIUS server has not been configured, information about the general-use RADIUS server is referenced.
7. The Switch sends an authentication request to the target RADIUS server

A RADIUS server group used for the port-based authentication method is a group of server IP addresses for general-use RADIUS server information. Therefore, authentication fails if the server IP address from the RADIUS server group does not correspond with the general-use RADIUS server information in the authentication method list.

When all RADIUS servers specified for a RADIUS server group in the authentication method list do not respond or request transmission fails, the Switch works based on the forced authentication configuration. Authentication fails if the forced authentication configuration has been disabled.

The Switch executes Switch default authentication in the following cases:

- If no authentication method list name has been configured for a port
- If the name of the authentication method list for a port does not correspond with that of an authentication method group
- If the name of the authentication method list for a port is not found in an authentication method group,

For the configuration, see the following:

- Example of port-based authentication method configuration: *(2) Example of port-based authentication method configuration* in *5.2.3 Authentication method list configuration*.
- IEEE 802.1X: *7. IEEE 802.1X Configuration and Operation*
- Web authentication: *9. Web Authentication Configuration and Operation*
- MAC-based authentication: *11. MAC-based Authentication Configuration and Operation*

(a) Port transfer

If this functionality is enabled, authentication is canceled if the following conditions are met:

- IEEE 802.1X: Authentication is canceled when port transfer is detected.
- Web authentication:Authentication is canceled if the authentication method list names before and after port transfer are different, regardless of the roaming settings.
- MAC-based authentication: Authentication is canceled the authentication method list names before and after port transfer are different, regardless of the roaming settings.

(2) User ID-based authentication method

This method uses individual RADIUS servers to perform authentication by user ID when performing Web authentication.

If the user ID authentication method is enabled for Web authentication, when a user logs in by using *user-ID*`@`*authentication-method-list-name*, RADIUS authentication is performed with a RADIUS server group in the authentication method list specified after the at mark (`@` character).

The following table describes the conditions for separating a user ID and authentication method list name. In the table, `userID` is the user ID and `List1` is the authentication method list name.

Table 5-4 Conditions for separating a user ID and authentication method list name

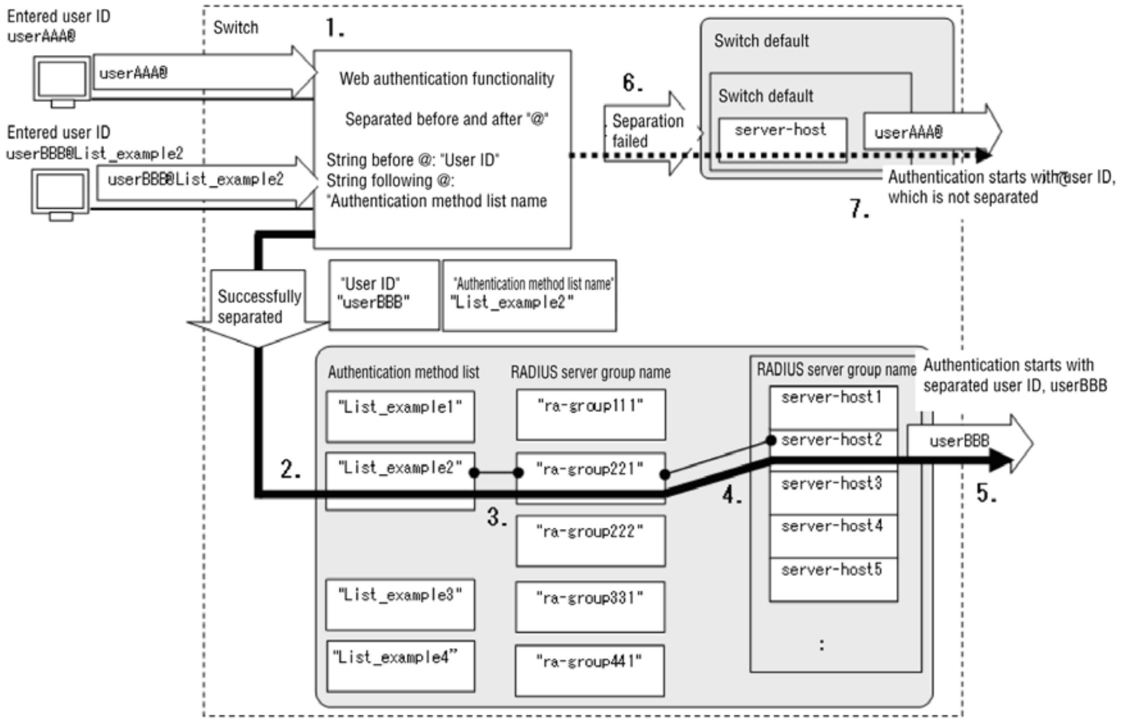
Entered combination of user ID and authentication method list name#	Success or failure of separation	Remarks
`userID@List1`	Successfully separates	
`userID@group1@List1`	Successfully separates	Multiple `@` characters are included, but the string is separated at the last `@` character.
`userID`	Separation fails	Separation fails because no `@` and subsequent characters are included.
`userID@`	Separation fails	Separation fails because no characters have been entered after the `@` character.
`@List1`	Separation fails	Separation fails because no characters have been entered before the `@` character.
`userID@`...(33 or more characters)	Separation fails	Separation fails because there are 33 or more characters after the `@` character.

#

Up to 128 characters can be entered for the user ID (including the `@` character and the following characters).

The following figure shows the operational overview of the user ID-based authentication method.

Figure 5-7 Operational overview of the user ID-based authentication method



If the user ID-based authentication method is enabled and separation of the user ID and list name succeeds

1. When the Switch receives an authentication request with *user-ID*`@`*authentication-method-list-name* (`userBBB@List_example2` in the figure), it separates the string at the `@` character (the string preceding the `@` character is the user ID and the string following the `@` character is the authentication method list name).
2. If separation succeeds, the Switch checks whether the separated authentication method list name (`List_example2` in the figure) has been registered.
3. If the name corresponds to a list on the Switch, the Switch references the RADIUS server group specified in the authentication method list (`ra-group221` in the figure).
4. The Switch checks the IP address of the general-use RADIUS server registered in the RADIUS server group (`server-host2` in the figure).
5. The Switch sends an authentication request to the target RADIUS server (because separation was successful, it sends the user ID `userBBB`).

If the user ID-based authentication method is disabled or separation of the user ID and list name fails

6. If the user ID-based authentication method is disabled or separation fails, the device references the IP address of the authentication RADIUS server information for the authentication method in use. If an authentication RADIUS server has not been configured, information about the general-use RADIUS server is referenced.
7. The Switch sends an authentication request to the target RADIUS server (because separation has failed, it sends the user ID `userAAA@`).

The RADIUS server group used with the user ID-based authentication method groups any server IP addresses in the general-use RADIUS server information. Therefore, authentication fails if the server IP address from the RADIUS server group does not correspond with the general-use RADIUS server information in the authentication method list.

When all RADIUS servers specified for a RADIUS server group in the authentication method list do not respond or request transmission fails, the Switch works based on the forced authentication configuration. Authentication fails if the forced authentication configuration has been disabled.

The Switch executes Switch default authentication in the following cases:

- If the authentication method list name (following the `@` character after the user ID) does not correspond with an authentication method list for an authentication method group of the authentication method in use
- When the user ID and the authentication method list name are not separated by an `@` character

For the configuration, see the following:

- Example of user ID-based authentication method configuration: *(3) Example of user ID-based authentication method configuration* in *5.2.3 Authentication method list configuration*.

(3) Exclusive relationship of authentication method list configuration

Port-based authentication method, user ID-based authentication method and legacy mode are not interoperable on the Switch. Select any one of these.

The following table describes the interoperability conditions of the authentication method list configuration.

Table 5-5 Interoperability conditions of the authentication method list configuration

Port-based authentication method configuration	User ID-based authentication method configuration	Legacy mode configuration
`dot1x authentication` `web-authentication authentication` `mac-authentication authentication`	`web-authentication user-group`	See ***Table 5-6 Legacy mode configurations that cannot be used with multistep authentication*.**
One of the above is configured	N	N
None of the above is configured	Configured	N
	Not configured	Y

Legend:

Y: Supported

N: Not supported

Table 5-6 Legacy mode configurations that cannot be used with multistep authentication

Authentication type	Configuration command
IEEE802.1X	`dot1x vlan dynamic enable` `dot1x vlan dynamic radius-vlan`
Web authentication	`web-authentication vlan`
MAC-based authentication	`mac-authentication interface` `mac-authentication vlan`

Authentication method lists are unavailable in legacy mode. Therefore, the configuration in legacy mode shown above is not interoperable with the port-based and user ID-based authentication methods.

5.2.3 Authentication method list configuration

(1) List of configuration commands

This section describes authentication method configuration using authentication method lists.

Table 5-7 Configuration commands and target authentication method lists

Command name	Description	Authentication method list	
		Port-based authentication	**Authentication method by user ID**
`aaa authentication dot1x` *<List name>*	Configures the Switch default and authentication method list with an authentication method group for IEEE 802.1X authentication.	Y	Y
`dot1x authentication` *<List name>*	Configures the authentication method list name of the port-based authentication method used with IEEE802 1X authentication.	Y	N
`aaa authentication web-authentication` *<List name>*	Configures the Switch default and authentication method list with the authentication method group for Web authentication.	Y	Y
`web-authentication authentication` *<List name>*	Configures an authentication method list name for the port-based authentication method used with Web authentication.	Y	Y
`web-authentication user-group`	Enables the user ID-based authentication method for Web authentication.	N	Y
`aaa authentication mac-authentication`	Configures the Switch default and authentication method list with the authentication method group for MAC-based authentication.	Y	Y
`mac-authentication authentication` *<List name>*	Configures the authentication method list name of the port-based authentication method used with MAC-based authentication.	Y	N

Command name	Description	Authentication method list	
		Port-based authentication	Authentication method by user ID
`radius-server host`	Configures general-use RADIUS server information.	Y	Y
`aaa group server radius` *<Group name>*	Configures the RADIUS server group name.	Y	Y
`server`	Registers general-use RADIUS server information in the RADIUS server group.	Y	Y

Legend:

Y: Supported

N: Not supported

(2) Example of port-based authentication method configuration

This is an example of triple authentication using the port-based authentication method. The following target port numbers and RADIUS subgroup names are used:

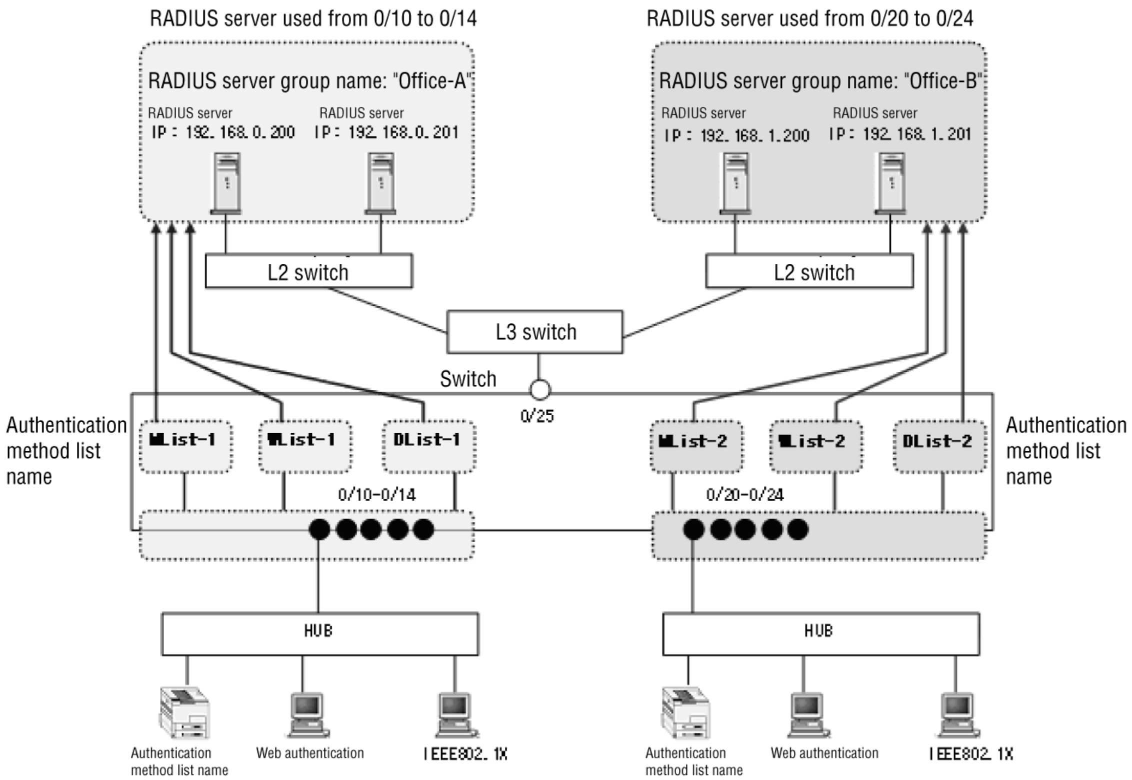
- Port 0/10-0/14: Authentication is performed using the RADIUS server group `Office-A`
- Port 0/20-0/24: Authentication is performed using the RADIUS server group `Office-B`

For configuration of authentication methods other than the port-based authentication method, see the following:

- IEEE 802.1X: *7. IEEE 802.1X Configuration and Operation*
- Web authentication*: 9. Web Authentication Configuration and Operation*
- MAC-based authentication: *11. MAC-based Authentication Configuration and Operation*

The following figure shows a configuration example of the port-based authentication method.

Figure 5-8 Configuration example of the port-based authentication method



Points to note

1. RADIUS server configuration
   - Configure general-use RADIUS server information used with authentication method lists.
   - Group general-use RADIUS server information.
2. Authentication method configuration
   - Associate authentication method lists and RADIUS server groups for each authentication method.
   - Configure authentication method lists by port for Web authentication.

Command examples

1.
```
(config)# radius-server host 192.168.0.200 key AuthKey
(config)# radius-server host 192.168.0.201 key AuthKey
(config)# radius-server host 192.168.1.200 key AuthKey
(config)# radius-server host 192.168.1.201 key AuthKey
```
Configures information of four general-use RADIUS servers.

2.
```
(config)# aaa group server radius Office-A
(config-group)# server 192.168.0.200
(config-group)# server 192.168.0.201
```

```
(config-group)# exit
```

Registers IP addresses of the RADIUS server group name Office-A and the general-use RADIUS server used with this group.

3.
```
(config)# aaa group server radius Office-B
(config-group)# server 192.168.1.200
(config-group)# server 192.168.1.201
(config-group)# exit
```

Registers the IP addresses of the RADIUS server group name Office-B and the general-use RADIUS server used with this group.

4.
```
(config)# aaa authentication dot1x DList-1 group Office-A
(config)# aaa authentication dot1x DList-2 group Office-B
(config)# aaa authentication web-authentication WList-1 group
Office-A
(config)# aaa authentication web-authentication WList-2 group
Office-B
(config)# aaa authentication mac-authentication MList-1 group
Office-A
(config)# aaa authentication mac-authentication MList-2 group
Office-B
```

Associates authentication method lists and RADIUS server groups for each authentication.

5.
```
(config)# interface range fastethernet 0/10-14
(config-if-range)# dot1x authentication DList-1
(config-if-range)# web-authentication authentication WList-1
(config-if-range)# mac-authentication authentication Mlist-1
(config-if-range)# exit
```

Configures authentication method list names, `DList-1`, `WList-1` and `MList-1` used in each authentication method to ports from 0/10 to 0/14.

6.
```
(config)# interface range fastethernet 0/20-24
(config-if-range)# dot1x authentication DList-2
(config-if-range)# web-authentication authentication WList-2
(config-if-range)# mac-authentication authentication Mlist-2
(config-if-range)# exit
```

Configures authentication method list names, `DList-2`, `WList-2` and `MList-2` used in each authentication method to ports from 0/20 to 0/24.

Notes

1. The Switch conducts Switch default authentication if the port-based authentication method has not been configured.
2. When a name of an authentication method list set for a port does not match the name of an authentication method list of an authentication method group or is not present in an authentication method group, authentication will be performed according to the device default.
3. The setting cannot be specified concurrently with the user ID-based

authentication method in Web authentication or legacy mode. For details, see *5.2.2 Authentication method list.*

(3) Example of user ID-based authentication method configuration

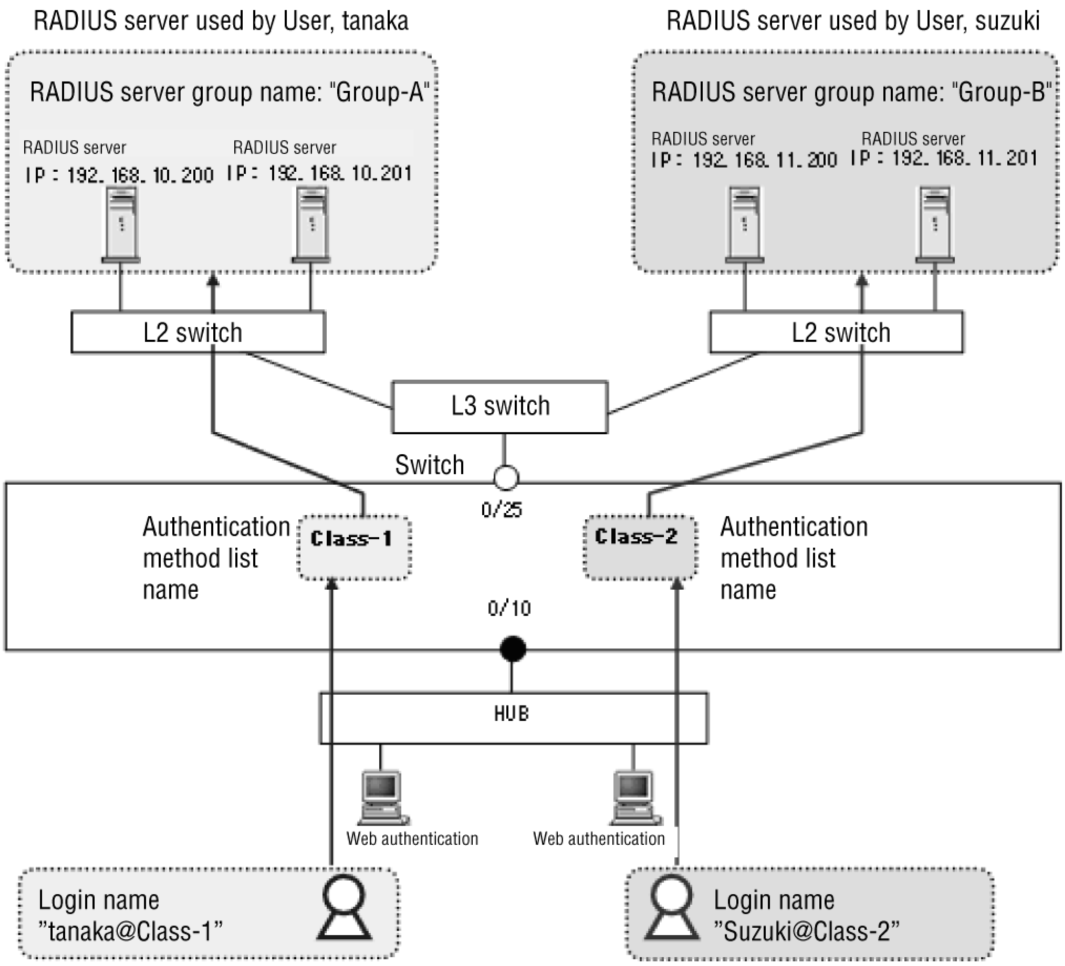
This section describes a structural example for Web authentication using the user ID-based authentication method. The following user IDs subject to Web authentication and the RADIUS server group names are used:

- User `tanaka`: Port 0/10 and RADIUS server group `Group-A` are used for authentication.
- User `suzuki`: Port 0/10 and RADIUS server group `Group-B` are used for authentication.

For other Web authentication method configuration, see *9. Web Authentication Configuration and Operation.*

The following figure shows a configuration example of the user ID-based authentication method.

Figure 5-9 Configuration example of the user ID-based authentication method



Points to note

1. RADIUS server configuration

   - Configure general-use RADIUS server information used with authentication method lists.

- Group general-use RADIUS server information.

2. Web authentication method configuration
   - Associate authentication method lists and RADIUS server groups for Web authentication.
   - Configure authentication method lists by user ID for Web authentication.

Command examples

1. `(config)# radius-server host 192.168.10.200 key AuthKey`

`(config)# radius-server host 192.168.10.201 key AuthKey`

`(config)# radius-server host 192.168.11.200 key AuthKey`

`(config)# radius-server host 192.168.11.201 key AuthKey`

Configures information of four general-use RADIUS servers.

2. `(config)# aaa group server radius Group-A`

`(config-group)# server 192.168.10.200`

`(config-group)# server 192.168.10.201`

`(config-group)# exit`

Registers IP addresses of the RADIUS server group name `Group-A` and the general-use RADIUS server used with this group.

3. `(config)# aaa group server radius Group-B`

`(config-group)# server 192.168.11.200`

`(config-group)# server 192.168.11.201`

`(config-group)# exit`

Registers IP addresses of the RADIUS server group name `Group-B` and the general-use RADIUS server used with this group.

4. `(config)# aaa authentication web-authentication Class-1 group Group-A`

`(config)# aaa authentication web-authentication Class-2 group Group-B`

Associates authentication method lists and RADIUS server groups for Web authentication.

5. `(config)# web-authentication user-group`

Configures user ID-based authentication method for Web authentication.

Notes

1. The Switch executes Switch default authentication if the user ID-based authentication method has not been configured.
2. Authentication is canceled for all Web authentication terminals when the user ID-based authentication method configuration is changed.
3. If the names of the authentication method list specified following the `@` character and the authentication method group do not correspond, the Switch executes Switch default authentication
4. The port-based authentication method and legacy mode cannot be

configured together. For details, see *5.2.2 Authentication method list.*

5.3 RADIUS authentication

This section describes the following items used with RADIUS authentication among Layer 2 authentication methods:

- RADIUS server information used with the Layer 2 authentication method
- Dead-interval functionality of RADIUS server communication
- Priority configuration for the Switch default local and RADIUS authentication
- RADIUS server account functionality

5.3.1 RADIUS server information used with the Layer 2 authentication method

(1) RADIUS server information configurable on the Switch

The following RADIUS server information is configurable on the Switch.

Table 5-8 RADIUS server information configurable on the Switch

RADIUS server information type	Configuration information	Functionality to use
General-useRADIUS server information	RADIUS server host information Auto recovery time (dead-interval time)	Login authentication IEEE802.1X Web authentication MAC-based authentication
RADIUS server information for IEEE 802.1X authentication	RADIUS server host information Auto recovery time (dead-interval time)	IEEE802.1X
RADIUS server information for Web authentication	RADIUS server host information Auto recovery time (dead-interval time)	Web authentication
RADIUS server information for MAC-based authentication	RADIUS server host information Auto recovery time (dead-interval time)	MAC-based authentication
RADIUS server group information	RADIUS server host information#	Login authentication IEEE802.1X Web authentication MAC-based authentication

#

Any configured general-use RADIUS server information (`radius-server host`) is assigned to the RADIUS server group. Set the same IP address as that of the general-use RADIUS server information, the port number for server authentication, and the port number for server accounting. Auto recovery time follows that of `radius-server dead-interval` in the general-use RADIUS server information.

You can configure the server IP address, port number for server authentication, port number for server accounting, RADIUS key, number of retransmissions, and response timeout period for the RADIUS server information. When the RADIUS key, number of retransmissions, and response timeout period are not configured, behavior follows the settings of the following configuration commands:

- RADIUS key: `radius-server key`
- Number of retransmissions: `radius-server retransmit`
- Response timeout period: `radius-server timeout`

If the specification of a port number for server authentication has been omitted, the system uses 1812. If the specification of a port number for accounting has been omitted, the system uses 1813.

For details on settings for RADIUS server information, see the following:

- For settings for general-use RADIUS server information, see *8. Login Security and RADIUS* in the *Configuration Guide Vol. 1*.
- For settings for authentication RADIUS server information, see the following:
    - IEEE 802.1X: *7.2.1 Configuring the authentication method group and RADIUS server information*
    - Web authentication: *9.2.1 Configuring the authentication method group and RADIUS server information*
    - MAC-based authentication: *11.2.1 Configuring the authentication method group and RADIUS server information*
- For settings for RADIUS server group information, see *8. Login Security and RADIUS* in the *Configuration Guide Vol. 1*.

(a) Auto recovery time (dead-interval time)

The settings for the auto recovery time operate on the various types of RADIUS server information. Other authentication RADIUS server information is not affected.

For details about auto recovery time, see *5.3.2 Dead-interval functionality of RADIUS server communication.*

(2) Handling the same IP address settings among the information of each RADIUS server

Information about each RADIUS server can be configured simultaneously. However, if the same IP address has been configured for them, they are considered the same RADIUS server.

Therefore, the same RADIUS key, number of retransmissions, and response timeout periods are applied in the communication between the same RADIUS servers.

Because of this, the following tasks are performed when any configuration command is entered:

1. Specifying the same IP address for general-use RADIUS servers.

    If the IP address matches the settings of an existing RADIUS server, replace the entered commands with ones with all parameters renewed.

    If parameters are omitted when entering the new commands, the defaults are returned.

2. Specifying the same IP address in the information of the same type of authentication RADIUS server.

    This is the same as for general-use RADIUS server information.

3. Specifying the same IP address in the information of the same type of general-use RADIUS servers and authentication RADIUS servers.

   This is the same as for general-use RADIUS server information.

4. Specifying the same IP address for RADIUS servers of different types.

   This is the same as for general-use RADIUS server information.

- Example when the same IP address is configured for RADIUS servers of different types:

  After configuring general-use RADIUS servers, MAC-based authentication RADIUS servers are configured with the same IP address:

  - `(config)# radius-server host 192.168.7.7 retransmit 10 key aaaaa`

    General-use RADIUS server configuration (Default)

  - `(config)# mac-authentication radius-server host 192.168.7.7 key bbbbb`

    MAC-based authentication RADIUS server configuration

  When following the procedures above, the number of retransmissions of general-use RADIUS servers is automatically returned to the default (3) and the RADIUS key is restored to `bbbbb` as entered on the MAC-based authentication RADIUS server.

  Automatically changed results are also reflected in the operation command `show running-config`.

- Result displayed by the `show running-config` operation command:

  - `radius-server host 192.168.7.7 key bbbbb` (After automatically changed results are applied)
  - `mac-authentication radius-server host 192.168.7.7 key bbbbb`

  After that, general-use RADIUS server information is not restored to the default configuration even if the MAC-based authentication RADIUS server information is deleted.

(3) Operation when configuring joint use of RADIUS server information

If the port-based authentication method or the user ID-based authentication method for Web authentication is enabled, RADIUS server group information registered in the authentication method list is used.

If the port-based authentication method or the user ID-based authentication method for Web authentication is disabled, the Switch default is used. In the Switch default, general-use RADIUS server information or authentication RADIUS server information is used. When both of the two items of information above are enabled, authentication RADIUS server information for each authentication method is used.

The following table shows the operational relationship between the general-use RADIUS server and authentication RADIUS server.

Table 5-9 Operational relationship between the general-use RADIUS server and authentication RADIUS server information

Authentication RADIUS server information	**General-useRADIUS server information**	**Operation**
One or more servers are configured	One or more servers are configured	Authentication RADIUS server information is used for operation.
	No server is configured	Authentication RADIUS server information is used for operation.
No server is configured	One or more servers are configured	General-use RADIUS server information is used for operation.
	No server is configured	RADIUS authentication is unavailable.

The following describes the operational relationship between the general-use RADIUS server and authentication RADIUS server, using MAC-based authentication as an example:

1. When using MAC-based authentication RADIUS server information for operation:

   If the `mac-authentication radius-server host` configuration command has been configured for at least one server, only the MAC-based authentication RADIUS server configured with that command is used.

   In this case, authentication-requested RADIUS server selection and auto recovery (`dead-interval`) do not affect other authentication methods.

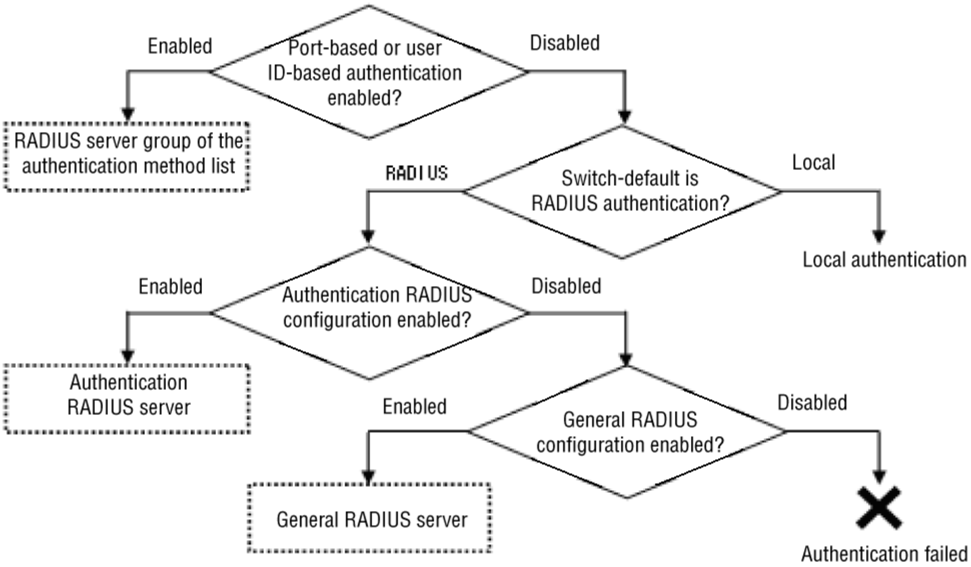
2. When using general-use RADIUS server information for operation:

   If the `mac-authentication radius-server host` configuration command has not been configured for any server, the general-use RADIUS server configured with the `radius-server host` configuration command is used.

   In this case, authentication-requested RADIUS server selection and auto recovery (`dead-interval`) are common among all authentication methods using the general-use RADIUS server.

The following figure shows the operation when configuring joint use of RADIUS server information.

Figure 5-10 Operation when configuring joint use of RADIUS server information

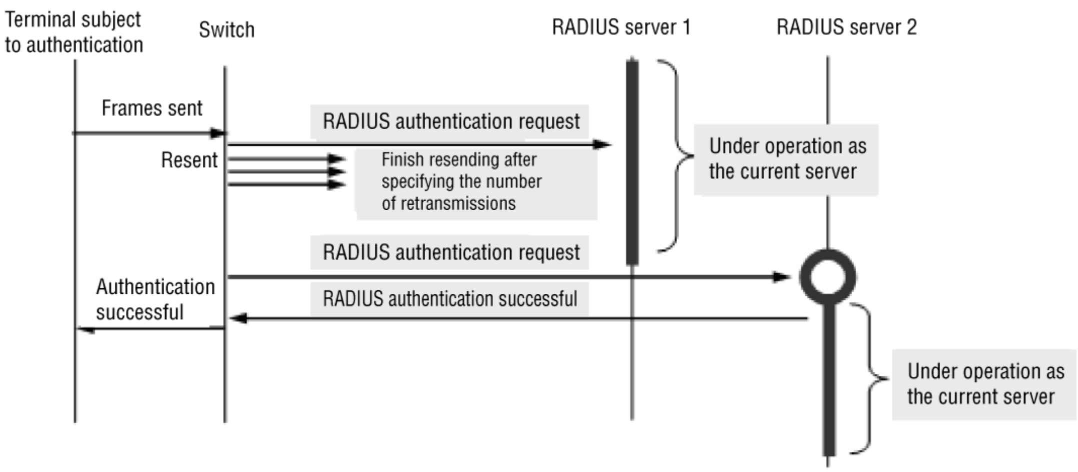


(4) Selecting an authentication-request destination RADIUS server

Multiple RADIUS server hosts can be configured in general-use RADIUS server information, authentication RADIUS server information, and the RADIUS server group (for the maximum number, see *3.2 Capacity limits* in the *Configuration Guide Vol. 1*).

If this system cannot communicate with one server and receives no authentication service, it tries to connect to other configured servers in sequence. The following figure shows the RADIUS server selection sequence.

Figure 5-11 RADIUS server selection sequence



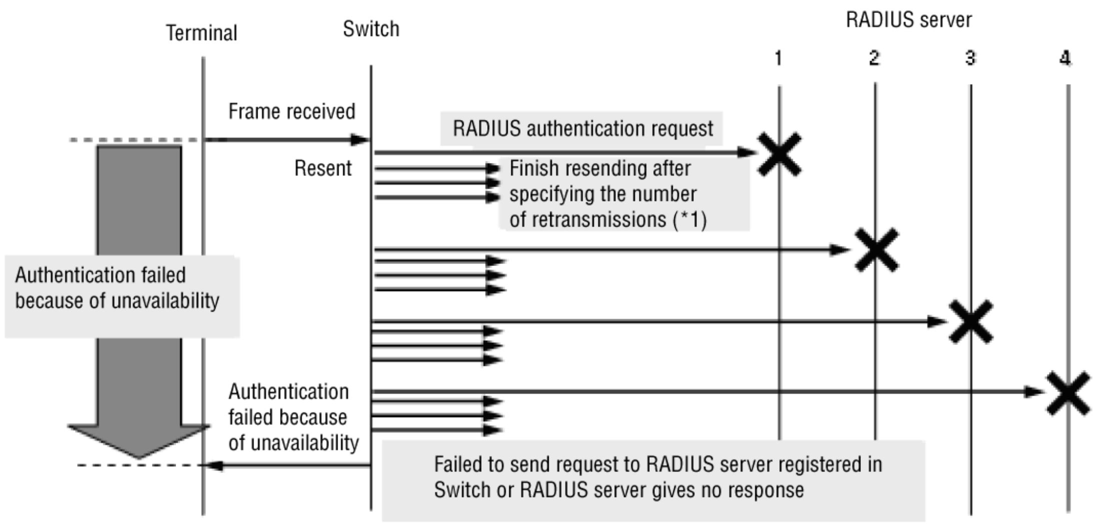
In this figure, when the Switch receives a new frame from the terminal subject to authentication, the Switch requests RADIUS authentication from RADIUS server 1. If RADIUS server 1 is unreachable, the RADIUS authentication request is sent to RADIUS server 2. When authentication is successful, the Switch can communicate with the authenticated network.

The RADIUS server in operation as an authentication request destination is called the *current server*.

(5) Maximum time before RADIUS authentication becomes unavailable

You can configure a response timeout period to determine whether communication with a RADIUS server is possible. The default is five seconds. If a RADIUS server times out, another attempt is made to connect to it. The number of retries can also be configured. The default is 3 times. Because of this, the maximum time before the system decides that RADIUS authentication is unavailable is as follows:
response-timeout-period x (*first-try* + *number-of-retries*) x *number-of-N-RADIUS-servers-configured*

Figure 5-12 Sequence before RADIUS authentication becomes unavailable (when the maximum number of RADIUS servers is configured)



The number of retransmissions*1: The number of retransmissions to RADIUS server (default: three times (can be configured))

The Switch can permit authentication using the forced authentication method if a configured RADIUS server is unavailable. For details, see *5.4.6 Forced authentication common to all authentication modes.*

5.3.2 Dead-interval functionality of RADIUS server communication

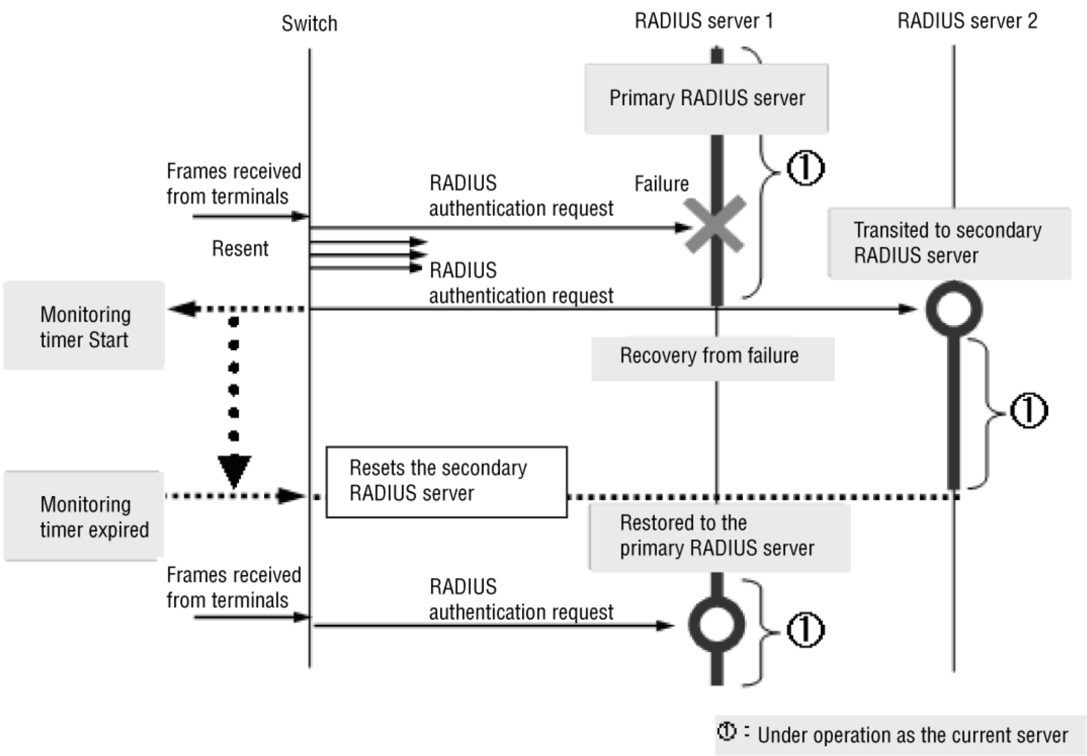
RADIUS authentication used by the Switch detects an effective RADIUS server when it detects a RADIUS authentication request by receiving a frame from a terminal subject to authentication. The following terminals always use the effective RADIUS server. In this method, time to authentication is reduced, but it cannot be automatically restored to a load-distributed state when a RADIUS server is used in a load-distributed structure and a failure occurs on a RADIUS server.

The Switch supports the dead-interval functionality provided by the monitoring timer as a method of auto recovery for the first RADIUS server. The RADIUS servers used by this functionality are as follows:

- Primary RADIUS server: The first effective RADIUS server
- Secondary RADIUS server: The second effective RADIUS server
- Current server: RADIUS server in operation as an authentication request destination

The following figure shows the sequence of recovery to the primary RADIUS server. Command names for MAC-based authentication RADIUS servers are explained below.

Figure 5-13 Sequence of recovery to the primary RADIUS server (1)



1. The RADIUS authentication request starts, using the primary RADIUS server#1 as the current server.
2. A failure occurs in the primary RADIUS server. The system switches to the next effective server (secondary RADIUS server).
3. The monitoring timer starts as soon as the current server switches to the secondary RADIUS server.
4. Authentication fails#2 if an authentication request cannot be sent to the last effective RADIUS server. Using this status as the current server#3, the monitoring timer starts#4 (if the timer has already started, the timer continues).
5. When the monitoring timer expires, the current server recovers to the primary RADIUS server.
6. Even if the recovery to the primary RADIUS server occurs after the monitoring timer expires, if the primary RADIUS server has not recovered from the failure, the effective RADIUS server is selected again. As soon as the current server switches to the secondary RADIUS server, the monitoring timer restarts.

#1

A RADIUS server configured using the `mac-authentication radius-server host` configuration command is effective when one of the following conditions is met:

- The `key` parameter of `mac-authentication radius-server host` has been configured.
- Even though the key parameter for the `mac-authentication radius-server host` has not been configured, the `radius-server key` parameter has been configured.

A RADIUS server that has not met any of the conditions above is disabled and, even if it was configured first, it does not become the primary RADIUS server.

#2

When a login authentication method is used, authentication fails.

When a Layer 2 authentication method is used, forced authentication or authentication fails. For forced authentication of Layer 2 authentication methods to be used in common, see *5.4.6 Forced authentication common to all authentication modes.* For individual use, see the description of each authentication method.

#3

The operation command `show radius-server` displays `* hold down`.

#4

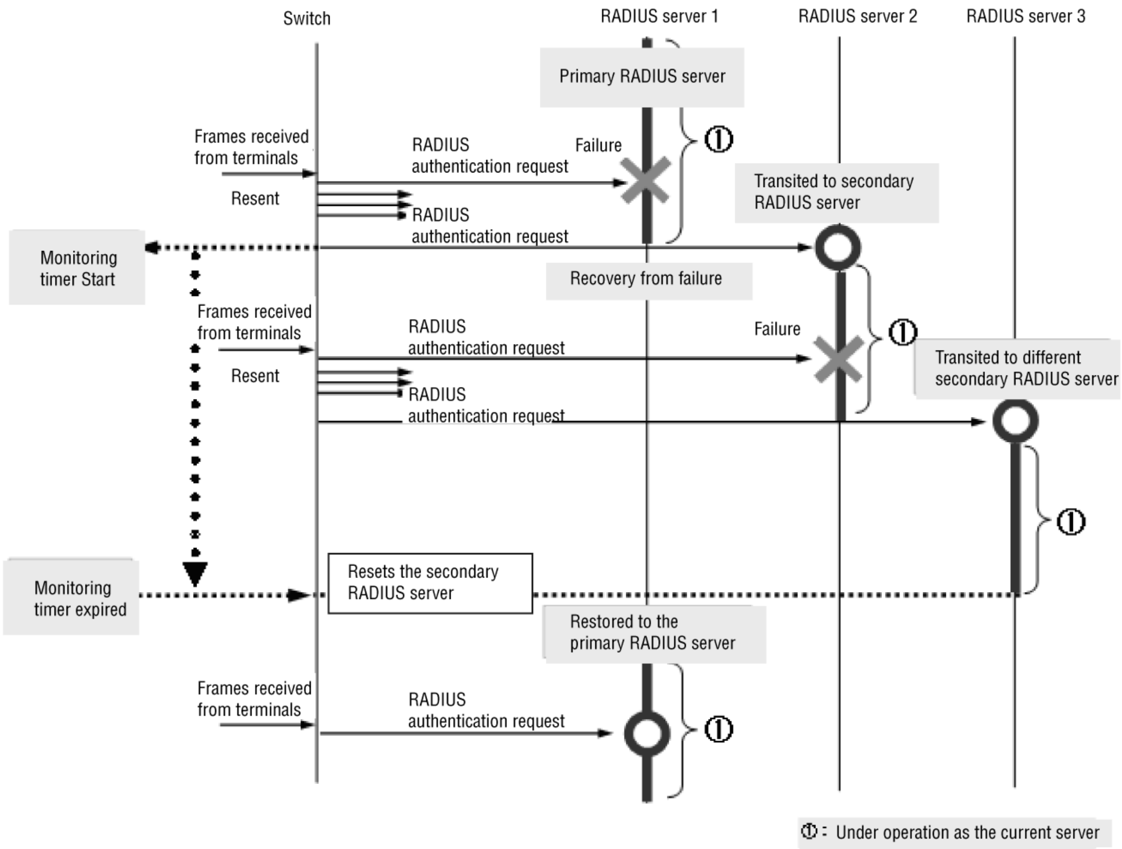
The Switch decides that authentication has failed (forced authentication or authentication of a Layer 2 authentication method failed) without sending an authentication request to a RADIUS server before the monitoring time expires. (If the `mac-authentication radius-server dead-interval 0` configuration command has been configured, the primary RADIUS server is restored without starting the monitoring timer.)

Once the monitoring timer starts, it will not be reset before expiration, in principle.

As shown below, after the monitoring timer starts in an environment in which three or more RADIUS servers are configured, when the current server switches to another RADIUS server, the monitoring timer continues until expiry without resetting.

The following figure shows the sequence with three or more RADIU servers configured.

Figure 5-14 Sequence of recovery to the primary RADIUS server (2)



As exceptions, the monitoring timer is reset before it expires in the following cases:

- When `mac-authentication dead-interval 0` is configured using the configuration command
- When information of the RADIUS server operating as the current server is deleted using the `mac-authentication radius-server host` configuration command
- When the `clear radius-server` operation command is executed

5.3.3 Priority configuration for the Switch default local and RADIUS authentications

The Switch default configuration described in *5.2 Authentication method group* can be set in the configuration for the local authentication method, or the RADIUS authentication method, or both. When configured for both, the second specified method is used for authentication if the first specified method fails.

The following table shows the supported range of priority settings for local authentication methods and RADIUS authentication methods.

Table 5-10 Supported range of priority settings for local authentication methods and RADIUS authentication methods

Authentication type	**Authentication mode**	**Authentication method**		
		Local	**RADIUS**	**Priority configuration**
IEEE802.1X	Port-based authentication (static)	N	Y	N
	Port-based authentication (dynamic)	N	Y	N
	VLAN-based authentication (dynamic)	N	Y	N
Web authentication	Fixed VLAN mode	Y	Y	Y
	Dynamic VLAN mode	Y	Y	Y
	Legacy mode	Y	Y	Y
MAC-based authentication	Fixed VLAN mode	Y	Y	Y
	Dynamic VLAN mode	Y	Y	Y
	Legacy mode	Y	Y	Y

Legend:

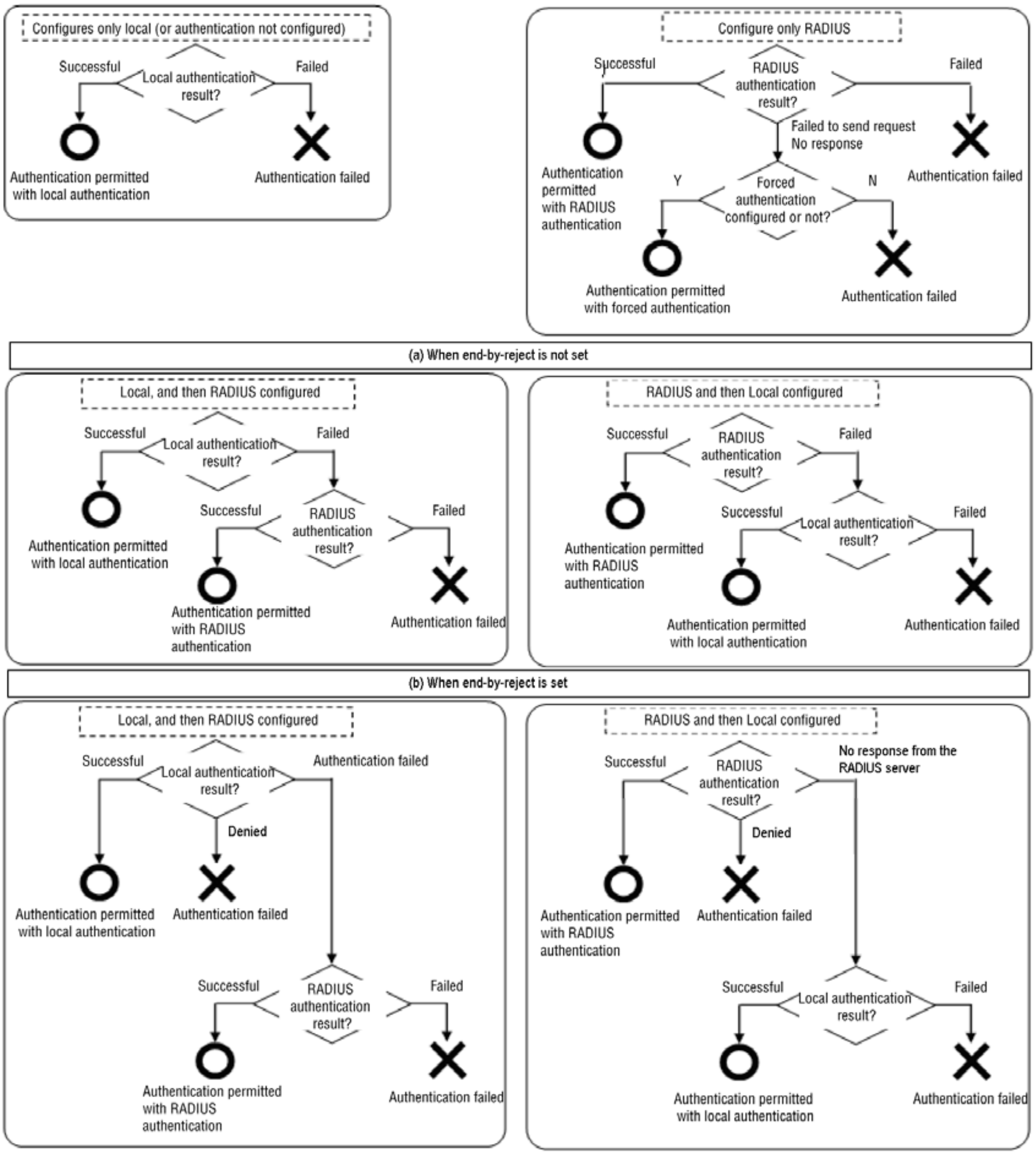
Y: Supported

N: Not supported

When both authentication methods are specified, you can use the `aaa authentication web-authentication end-by-reject` (or `aaa authentication mac-authentication end-by-reject` for MAC-based authentication) configuration command to change how the authentication method is selected if the first specified method fails.

The following figure shows the relations among authentication method configuration types and authentication results.

Figure 5-15 Relations among authentication method configuration types and authentication results



(a) When `end-by-reject` is not set

If authentication fails when using the first specified method when `end-by-reject` is not set, authentication can be performed using the next specified method regardless of the reason of failure.

For example, when a request is received from an unauthenticated terminal, the Switch requests the RADIUS server to perform RADIUS authentication. If authentication by the RADIUS server fails because RADIUS authentication is denied, the Switch performs local authentication. If authentication is successful, the Switch manages the terminal as an authenticated terminal.

(b) When `end-by-reject` is set

If authentication fails when using the first specified method when `end-by-reject` is set, authentication is not performed using the next specified method. The entire authentication process is terminated at the first denial and is treated as a failure. The next authentication is performed only when authentication failed due to communication failure (for example, the RADIUS server does not respond).

For example, when a request is received from an unauthenticated terminal, the Switch requests the RADIUS server to perform RADIUS authentication. If authentication by the RADIUS server fails because RADIUS authentication is denied, the Switch ends the entire authentication process. The Switch does not perform the local authentication specified as the next authentication method. As a result, the Switch manages the terminal as a terminal failing to be authenticated.

For details on authentication method configurations, see the following:

- IEEE 802.1X: *7.2.1 Configuring the authentication method group and RADIUS server information*
- Web authentication: *9.2.1 Configuring the authentication method group and RADIUS server information*
- MAC-based authentication: *11.2.1 Configuring the authentication method group and RADIUS server information*

5.3.4 RADIUS account functionality

(1) Overview

The Switch supports account functionality that uses RADIUS servers (RADIUS account functionality).

The RADIUS account functionality of the Switch is used only for Layer 2 authentication methods. The following table shows the functionality supported by the RADIUS account functionality.

Table 5-11 Functionality supported by the RADIUS account functionality

Target functionality	**Account method group**		**Issuing timing**		**Accounting server type**
	Switch default	**Account method list**	**start-stop**	**stop-only**	**group radius**
Login	N	N	N	N	N
IEEE802.1X	Y	N	Y	N	Y
Web authentication	Y	N	Y	N	Y
MAC-based authentication	Y	N	Y	N	Y

Legend:

Y: Supported

N: Not supported

(2) Destination of accounting information

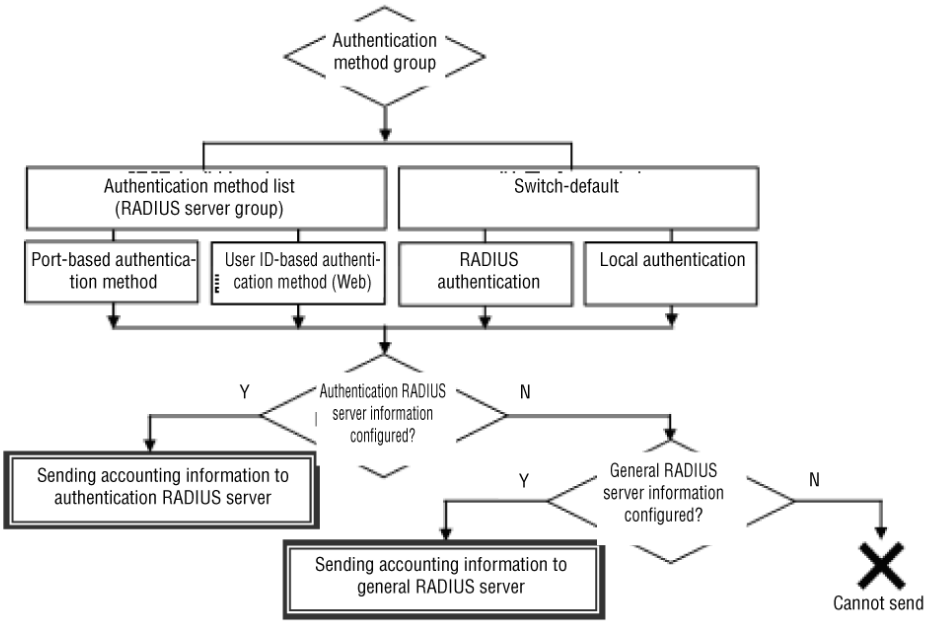
Accounting information is sent to a RADIUS server operating as the device default of the authentication method (authentication RADIUS server or general-use RADIUS server). It is not applied to a RADIUS server group.

Therefore, even when authentication is performed by a RADIUS server group using the port-based authentication method or the user ID-based Web authentication method, accounting information is sent to the authentication RADIUS server or the general-use RADIUS server.

In addition, for local authentication, the information is sent to the authentication RADIUS server or the general-use RADIUS server.

The following figure shows the selection of the RADIUS server that is the destination of accounting information.

Figure 5-16 Selection of the RADIUS server that is the destination of accounting information



When both authentication for the authentication RADIUS server and the general-use RADIUS server are configured, the information is sent to the authentication RADIUS server.

(3) Selection and recovery of a RADIUS server

If the Switch cannot verify whether accounting information has been sent to the RADIUS server, it selects a destination RADIUS server in sequence in the same way as for RADIUS authentication.

As soon as the Switch confirms that the information has been successfully received, the current server information is switched and the auto recovery period (dead-interval timer) starts.

The dead-interval timer value is the same value as the one configured for RADIUS authentication. However, the dead-interval timer for RADIUS authentication and the RADIUS accounting functionality are started and controlled separately on the Switch. The same sequences are used for dead-interval timer counts and recovery as for RADIUS authentication.

When the dead-interval timer in use is reset (current server is the default) using the `clear radius-server` operation command, the dead-interval timers for RADIUS authentication and the RADIUS account functionality are reset simultaneously.

(4) RADIUS attributes

For details about RADIUS attributes with this functionality, see the description for each authentication method:

- IEEE 802.1X*: 6.7 Preparation*
- Web authentication: *8.6 Preparation* and *8.6.2 For RADIUS authentication*
- MAC-based authentication: *10.6 Preparation* and *10.6.2 RADIUS authentication*

5.4 Functionality common to all Layer 2 authentication methods

This section describes the functionality used in common by all Layer 2 authentication methods.

- Permitting communication by unauthenticated terminals (IPv4 access list dedicated to authentication)
- Specifying post-authentication VLANs by VLAN name
- Auto VLAN assignment for a MAC VLAN
- Auto authentication mode accommodation on the same MAC port
- Authenticating tagged frames on a MAC port
- Forced authentication common to all authentication modes

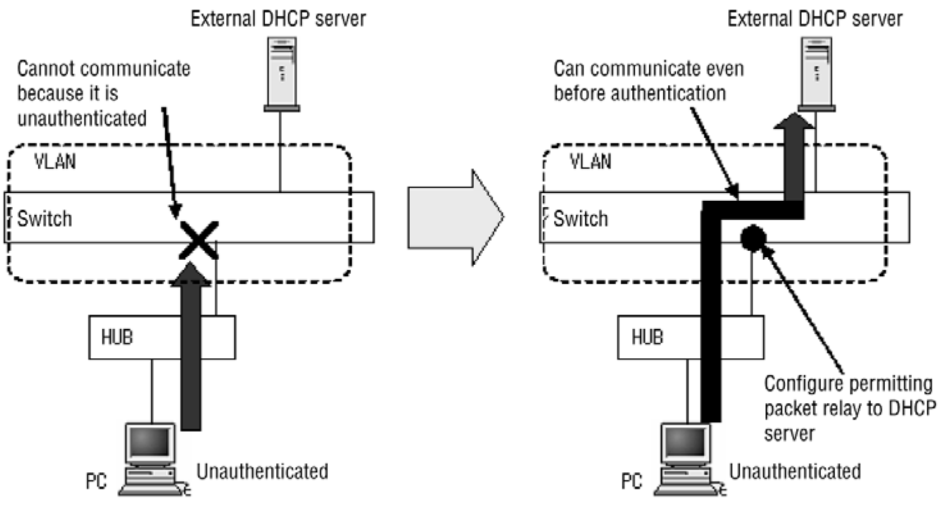
5.4.1 Permitting communication by unauthenticated terminals (IPv4 access list dedicated to authentication)

When an external DHCP server or domain server is used with the following functionality and authentication modes, a frame must be passed before authentication:

- IEEE 802.1X: Port-based authentication (static), port-based authentication (dynamic)
- Web authentication: Fixed VLAN mode, dynamic VLAN mode
- MAC-based authentication: Fixed VLAN mode, dynamic VLAN mode

You can send specific frames beyond the Switch from unauthenticated terminals by using the `authentication ip access-group` configuration command to configure the authentication IPv4 access list for a port subject to any of the above authentication methods.

Figure 5-17 Before and after the authentication IPv4 access list is used



The authentication IPv4 access list differs from standard access lists (such as those configured by the `ip access-group` configuration command) in that the filtering conditions no longer apply after authentication.

If you configure a standard access list and an authentication IPv4 access list for an authenticating port, the filtering conditions in the standard access list will apply before and after authentication. For this reason, make sure that you include the filtering conditions of the authentication IPv4 access list in the standard access list.

Before an unauthenticated terminal can obtain an IP address from an external DHCP server or the Switch's internal DHCP server, the authentication IPv4 access list must permit the transmission of DHCP packets to the DHCP server. Make sure that you include filtering conditions like the following in the access list:

Example of filtering conditions required for DHCP access:

In this example, the IP address of the DHCP server is 10.10.10.254, and the network of the terminal being authenticated is 10.10.10.0/24.

```
permit udp 10.10.10.0 0.0.0.255 host 10.10.10.254 eq bootps
permit udp host 0.0.0.0 host 10.10.10.254 eq bootps
permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
```

Notes on configuring the authentication IPv4 access list:

Note the following when using the `authentication ip access-group` configuration command:

- You can only specify one authentication IPv4 access list. When using the `authentication ip access-group` configuration command, make sure that you configure the same settings at each port where authentication will take place.
- If the filtering conditions specified in the authentication IPv4 access list exceeds the capacity limit, the configuration command ignores the excess conditions.
- Authentication functions implicitly discard all frames that are not expressly permitted. This does not count in the number of filtering conditions.
- Configure the `authentication arp-relay` command to pass ARP frames sent from terminals before authentication.

5.4.2 Specifying post-authentication VLANs by VLAN name

You can specify, by name, the VLAN to be accommodated in dynamic VLAN mode for each authentication method. The VLAN name is specified using the `name` configuration command of the VLAN interface. By setting the specified VLAN name in a RADIUS server, you can use the VLAN name to control the post-authentication VLANs in dynamic VLAN mode.

The following table shows this VLAN name functionality and the possible authentication modes.

Table 5-12 VLAN authentication modes supporting the VLAN name specification

Authentication type	Authentication mode	Supported/ Not supported	Remarks
IEEE802.1X	Port-based authentication (static)	N	Fixed VLAN mode
	Port-based authentication (dynamic)	Y	Dynamic VLAN mode
	VLAN-based authentication (dynamic)	Y	Legacy mode

Authentication type	Authentication mode	Supported/ Not supported	Remarks
Web authentication	Fixed VLAN mode	N	
	Dynamic VLAN mode	Y	
	Legacy mode	Y	
MAC-based authentication	Fixed VLAN mode	N	
	Dynamic VLAN mode	Y	
	Legacy mode	Y	

Legend:

Y: Supported

N: Not supported

For RADIUS server configuration, see *Preparing the RADIUS server* in the descriptions of each authentication method.

5.4.3 Auto VLAN assignment for a MAC VLAN

The Switch can automatically assign post-authentication VLANs that accommodate ports subject to authentication. Auto assignment is performed based on the following authentication results:

- When a post-authentication VLAN is specified by an internal authentication database after successful local authentication
- When a post-authentication VLAN is specified using RADIUS attributes after successful RADIUS authentication
- When a post-authentication VLAN has been configured at forced authentication

Auto VLAN assignment and cancellation for a MAC VLAN depend on whether the above post-authentication VLAN has been configured after the above authentication, and follows the status of the authenticated terminal of the port. The following table shows the conditions of auto VLAN assignment and cancellation.

Table 5-13 Conditions of auto VLAN assignment and cancellation

Post-authenticaton VLAN configuration				
Device's VLAN configuration (mac-based)	**Port's MAC VLAN configuration**	**Port's authenticated terminal configuration**	**Auto VLAN assignment and cancellation**	**Remarks**
Configured	Not configured	Not configured -> Configured	Y1	
		Configured -> Not	Y2	(1)(2)[#1]

Post-authenticaton VLAN configuration				
Device's VLAN configuration (mac-based)	**Port's MAC VLAN configuration**	**Port's authenticated terminal configuration**	**Auto VLAN assignment and cancellation**	**Remarks**
		configured		
	Not configured -> Configured	--	Y2	#2
	Configured -> Not configured	Configured	Y1	
	Configured	--	N	
Not configured	--	--	N	
Configured -> Not configured	--	Configured -> Not configured	Y2	(3)#1

Legend:

Y1: Assigns the VLAN.

Y2: Cancels of the assigned VLAN.

N: Does not assign the VLAN.

--: Both are OK.

#1

Conditions under which automatically assigned VLANs are deleted are as follows:

- When there is no authenticated terminal in the VLAN of the corresponding port ((1)(2) in the above table)
- When all authenticated terminals of the corresponding port are canceled due to the corresponding port being in a link-down state ((1)(2) in the above table)
- When all authenticated terminals are canceled because VLAN configuration is deleted ((3) in the table above)

#2

When you configure a VLAN for a port using the `switchport mac vlan` configuration command, automatically assigned VLANs are canceled. However, authenticated terminals follow the configuration, so authentication is not canceled.

The following table shows the authentication modes supporting this functionality.

Table 5-14 Authentication modes supporting auto VLAN assignment

Authentication type	Authentication mode	Supported/ Not supported	Remarks
IEEE802.1X	Port-based authentication	N	Fixed VLAN mode

Authentication type	Authentication mode	Supported/ Not supported	Remarks
	(static)		
	Port-based authentication (dynamic)	Y	Dynamic VLAN mode
	VLAN-based authentication (dynamic)	N	Legacy mode
Web authentication	Fixed VLAN mode	N	
	Dynamic VLAN mode	Y	
	Legacy mode	N	
MAC-based authentication	Fixed VLAN mode	N	
	Dynamic VLAN mode	Y	
	Legacy mode	N	

Legend:

Y: Supported

N: Not supported

(1) Handling automatically assigned VLANs

The Switch handles automatically assigned VLANs as described below.

When interoperating with the following functionality, automatically assigned VLANs work based on each functionality:

- The Spanning Tree Protocol
- Uplink redundancy
- The L2 loop detection functionality
- DHCP snooping (including dynamic ARP inspection functionality)

5.4.4 Auto authentication mode accommodation on the same MAC port

In the Switch, fixed VLAN mode and dynamic VLAN mode can be used at the same MAC port.

When untagged frames are received from a terminal subject to authentication, the Switch automatically controls the terminal subject to authentication as one in fixed VLAN mode or dynamic VLAN mode according to the post-authentication VLANs determined by the authentication results.

The following table shows the authentication modes supporting this functionality.

Table 5-15 Authentication modes supporting auto authentication mode accommodation at a single MAC port

Authentication type	Authentication mode	Supported/ Not supported	Remarks
IEEE802.1X	Port-based authentication (static)	Y	Fixed VLAN mode
	Port-based authentication (dynamic)	Y	Dynamic VLAN mode
	VLAN-based authentication (dynamic)	N	Legacy mode
Web authentication	Fixed VLAN mode	Y	
	Dynamic VLAN mode	Y	
	Legacy mode	N	
MAC-based authentication	Fixed VLAN mode	Y	
	Dynamic VLAN mode	Y	
	Legacy mode	N	

Legend:

Y: Supported

N: Not supported

(1) Auto authentication mode accommodation at RADIUS authentication

In RADIUS authentication, the terminal authentication mode is determined depending on the RADIUS attributes of `Access-Accept` received from the RADIUS server.

The target RADIUS attributes are `Tunnel-Type`, `Tunnel-Medium-Type`, and `Tunnel-Private-Group-ID` when `Access-Accept` is received from the RADIUS server.

The following table shows the behavior based on combinations of RADIUS attributes when `Access-Accept` is received.

Table 5-16 Behaviors based on combinations of RADIUS attributes when Access-Accept is received

Tunnel-Type	Tunnel-Medium -Type	Tunnel-Private-Group-ID	Authentication behavior	Terminal authentication mode state
None	None	None	Accommodated in a native VLAN as a post-authentication VLAN	Fixed VLAN mode

Tunnel-Type	Tunnel-Medium -Type	Tunnel-Private-Group-ID	Authentication behavior	Terminal authentication mode state
VLAN(13)	IEEE-802(6)	Based on *Table 5-17*.	Based on *Table 5-17*.	
Combinations other than above			Failed authentication	Failed authentication

Table 5-17 Actions corresponding to Tunnel-Private-Group-ID at RADIUS authentication

Tunnel-Private-Group-ID contents	Compared with native VLAN of an authentication port	Authentication behavior	Terminal authentication mode state	FDB[#1] registration	MAC VLAN registration
None or blank	--	Accommodated in a native VLAN	Fixed VLAN mode	Registered	Unregistered
• Numeric value • Numeric value after string VLAN • VLAN name	Other than native VLAN[#2]	Accommodated in the VLAN specified for Tunnel-Private-Group-ID[#3]	Dynamic VLAN mode	Registered	Registered
	Same as native VLAN	Failed authentication	Mode not determined due to failed authentication	Unregistered	Unregistered
	No VLAN name	Failed authentication	Mode not determined due to failed authentication	Unregistered	Unregistered
All other cases	--	Failed authentication	Mode not determined due to failed authentication	Unregistered	Unregistered

Legend:

--: Does not depend on the contents.

#1

FDB: Indicates the MAC address table.

- The MAC address of a terminal accommodated in fixed VLAN mode is registered in the MAC address table as an authentication entry.
- The MAC address of a terminal accommodated in dynamic VLAN mode is registered in the MAC address table and MAC VLAN table as an authentication entry.

#2

Authentication fails if the VLAN matches the VLAN specified by the `switchport mac dot1q vlan` command for the authentication port.

#3

The VLAN specified for Tunnel-Private-Group-ID must be set on the Switch in advance by using the `vlan mac-based` configuration command.

(2) Auto authentication mode accommodation at local authentication

In local authentication, the terminal authentication mode is determined depending on the VLAN results of the internal authentication database.

Table 5-18 Actions based on the VLAN results for local authentication

Authentication result VLAN for the internal authentication database	**Compared with native VLAN of an authentication port**	**Authentication behavior**	**Terminal authentication mode state**	**FDB[#1] registration**	**MAC VLAN registration**
None or blank	--	Accommodated in a native VLAN	Fixed VLAN mode	Registered	Unregistered
Exist	Other than native VLAN[#2]	Accommodated in the VLAN specified for the internal authentication database[#3]	Dynamic VLAN mode	Registered	Registered
	Same as native VLAN	Failed authentication	Mode not determined due to failed authentication	Unregistered	Unregistered

Legend:

--: Does not depend on the contents.

#1

FDB: Indicates the MAC address table.

- The MAC address of a terminal accommodated in fixed VLAN mode is registered in the MAC address table as an authentication entry.
- The MAC address of a terminal accommodated in dynamic VLAN mode is registered in the MAC address table and MAC VLAN table as an authentication entry.

#2

Authentication fails if the VLAN matches the VLAN specified by the `switchport mac dot1q vlan` command for the authentication port.

#3

The VLAN specified for the internal authentication database must be set on the Switch in advance by using the `vlan mac-based` configuration command.

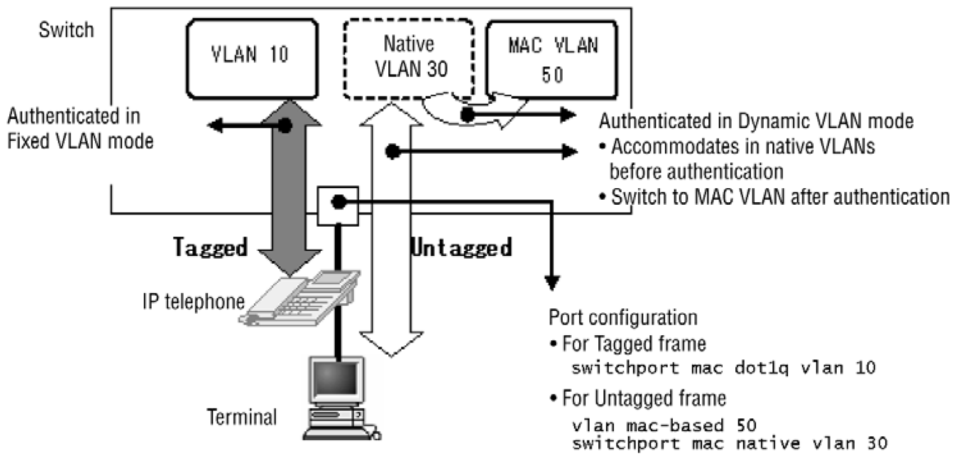
5.4.5 Tagged frame authentication on a MAC port (dot1q vlan configuration)

If you use the `switchport mac dot1q vlan` configuration command for a MAC port, when tagged frames from a terminal subject to authentication are received, the frames are authenticated based on fixed VLAN mode.

Untagged frames are authenticated based on dynamic VLAN mode. Before untagged frames are authenticated, they are accommodated in a native VLAN, and switched to a post-authentication after authentication is successful.

The following figure shows the operation when `dot1q vlan` is set for the MAC port.

Figure 5-18 Behavior when dot1q vlan is configured for the MAC port



For behavior of this functionality at a port, see *(4) Interoperability of dynamic VLAN mode and fixed VLAN mode on the same port* in *5.7.2 Interoperability on the same port.*

5.4.6 Forced authentication common to all authentication modes

Forced authentication common to all authentication modes is enabled by using the `authentication force-authorized enable` configuration command.

This functionality works when either of the following conditions is met:

- Only RADIUS authentication is configured as the authentication method for each type of authentication method (forced authentication is disabled if you have set the priority as RADIUS authentication followed by local authentication).
- When the Switch cannot send a request to the configured RADIUS server

The following table describes the authentication modes that support forced authentication.

Table 5-19 Support for forced authentication common to all authentication modes

Authentication type	Authentication mode	Operation of forced authentication
IEEE802.1X	Port-based authentication (static)	Y
	Port-based authentication (dynamic)	Y
	VLAN-based authentication (dynamic)	N
Web	Fixed VLAN mode	Y

Authentication type	Authentication mode	Operation of forced authentication
authentication		
	Dynamic VLAN mode	Y
	Legacy mode	N
MAC-based authentication	Fixed VLAN mode	Y
	Dynamic VLAN mode	Y
	Legacy mode	N

Legend:

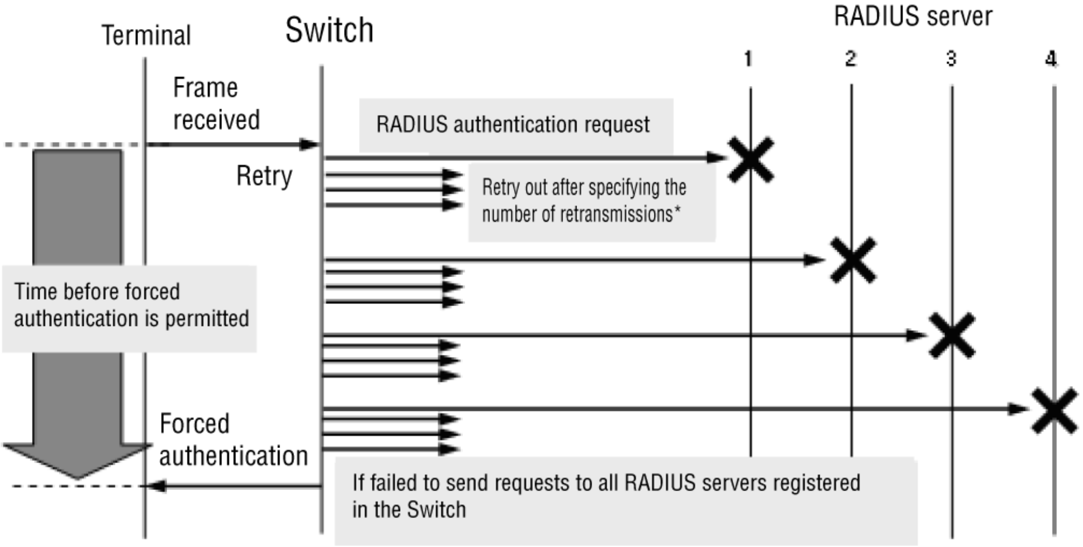
Y: Supported

N: Not supported

(1) Behavior from the start of an RADIUS authentication request to permission for forced authentication

Forced authentication is permitted within the period from the start of the authentication request to timeout of all RADIUS servers registered in the Switch.

Figure 5-19 Sequence before permission of forced authentication (when the maximum number of RADIUS servers is configured)



Number of retransmissions*: Number of retransmissions to RADIUS server (default: three times (can be configured)

Each authentication-requesting terminal requires time before permission for forced authentication in the sequence above.

The number of retries by a RADIUS server, as well as the IP addresses, can be configured using each configuration command of the general-use RADIUS server information and authentication RADIUS server information. For details, see *5.3.1 RADIUS server information used with the Layer 2 authentication method.*

If a request failed to be sent to a RADIUS server or there was no response from the RADIUS server, each authentication method collects the account log data shown in the table below.

Table 5-20 Account logs collected by each authentication method

Authentication type	Account log message
IEEE802.1X	● `No=82` `WARNING:SYSTEM: (`*<Additional information>*`) Failed to connect to RADIUS server.` *<Additional information>*`: IP` You can use the `show dot1x logging` command to check the account log.
Web authentication	● `No=21` `NOTICE:LOGIN:(`*<Additional information>*`) Login failed ; Failed to connection to RADIUS server.` *<Additional information>*`: MAC, USER, IP, PORT, VLAN` You can use the `show web-authentication logging` operation command to check the account log.
MAC-based authentication	● `No=21` `NOTICE:LOGIN: (`*<Additional information>*`) Login failed ; Failed to connection to RADIUS server` *<Additional information>*`:MAC, PORT, VLAN` You can use the the `show mac-authentication logging` operation command to check the account log.

(2) Configuration for forced authentication to work

You need to enable the forced authentication method common to all authentication modes for these modes to work, and configure the following authentication settings.

Table 5-21 Configuration for forced authentication to work

Authentication type	Authentication mode	Authentication method configuration
IEEE802.1X	IEEE 802.1X common	● `dot1x system-auth-control` Switch default ● `aaa authentication dot1x default group radius` ● `dot1x radius-server host` or `radius-server host` Authentication method list and port-based authentication ● `aaa authentication dot1x` *<List name>* `group` *<Group name>*#1 ● `aaa group server radius` *<Group name>* ● `server` ● `radius-server host`

Authentication type	Authentication mode	Authentication method configuration
	Port-based authentication (static)	• `dot1x port-control auto` • `switchport mode access` • `dot1x authentication`[#2]
	Port-based authentication (dynamic)	• `vlan` *<VLAN ID>* `mac-based` • `dot1x port-control auto` • `switchport mode mac-vlan` • `dot1x authentication`[#2]
	VLAN-based authentication (dynamic)	N
Web authentication	Web authentication common	• `web-authentication system-auth-control` Switch default • `aaa authentication web-authentication default group radius`[#1] • `web-authentication radius-server host` or `radius-server host` Authentication method list, port-based authentication method, and user ID-based authentication method • `aaa authentication web-authentication` *<List name>* `group` *<Group name>*[#1] • `aaa group server radius` *<Group name>* • `server` • `radius-server host` • `web-authentication user-group`[#3]
	Fixed VLAN mode	• `web-authentication port` • `switchport mode access` • `web-authentication authentication`[#2]
	Dynamic VLAN mode	• `vlan` *<VLAN ID>* `mac-based` • `web-authentication port` • `switchport mode mac-vlan` • `web-authentication authentication`[#2]
	Legacy mode	N
MAC-based authentication	MAC-based authentication common	• `mac-authentication system-auth-control` Switch default • `aaa authentication mac-authentication default group radius`[#1] • `mac-authentication radius-server host` or `radius-server host` Authentication method list and port-based authentication • `aaa authentication mac-authentication` *<List name>* `group`

Authentication type	Authentication mode	Authentication method configuration
		<Group name>[#1] ● `aaa group server radius` *<Group name>* ● `server` ● `radius-server host`
	Fixed VLAN mode	● `mac-authentication port` ● `switchport mode access` ● `mac-authentication authentication`[#2]
	Dynamic VLAN mode	● `vlan` *<VLAN ID>* `mac-based` ● `mac-authentication port` ● `switchport mode mac-vlan` ● `mac-authentication authentication`[#2]
	Legacy mode	N

Legend:

N: Forced authentication common to all authentication modes is not supported.

#1

When using forced authentication by Switch default, set only `default group radius`.

When using port-based authentication or user ID-based authentication, set *<list-name>* `group` *<group-name>*.

#2

Specify this when using port-based authentication.

#3

Set this when using user ID-based authentication.

(3) Post-authentication VLAN by forced authentication

You can configure post-authentication VLAN in dynamic VLAN mode by using the `authentication force-authorized vlan` configuration command.

If this configuration command is bypassed, the target terminal is accommodated in the native VLAN. The target terminal is handled as one in fixed VLAN mode.

A terminal accommodated in a VLAN using forced authentication before configuring this command does not change the post-authentication VLAN before the next authentication even after configuration is changed.

(4) Interoperability of this functionality and forced authentication of each authentication method

This functionality and forced authentication of each authentication method are not interoperable. Configure only one.

Table 5-22 Common to all authentication modes and forced authentication configuration

Forced authentication configuration	Configuration of post-authentication VLAN at forced authentication	Forced authentication of each authentication method
`authentication force-authorized enable`	`authentication force-authorized vlan`	See *Table 5-23 Non-interoperable forced authentication configuration*.
Configured	Not configured	N
	Configured	N
Not configured	Not configured	Y
	Configured	N

Legend:

Y: Supported

N: Not supported

Table 5-23 Non-interoperable forced authentication configuration

Authentication type	Configuration command
IEEE802.1X	`dot1x force-authorized`
	`dot1x force-authorized vlan`
Web authentication	`web-authentication static-vlan force-authorized`
	`web-authentication force-authorized vlan`
MAC-based authentication	`mac-authentication static-vlan force-authorized`
	`mac-authentication force-authorized vlan`

The configurations above are impossible if forced authentication common to all authentication modes has been configured.

If any one of the configurations above has been configured, forced authentication configuration common to all authentication modes cannot be configured.

(5) Private trap for forced authentication

With forced authentication common to all authentication modes, the private trap for forced authentication can be issued in an authentication mode corresponding to *Table 5-19 Support for forced authentication common to all authentication modes* as soon as specific account log data (SYSTEM) is logged by each authentication method.

Though the IEEE 802.1X forced authentication configuration does not support specification of the private trap, it can be issued in forced authentication configuration common to all authentication modes.

Table 5-24 Account log (SYSTEM) and conditions for issuing a private trap

Authentication type	Authentication mode	Configuration necessary to issue trap	
		Command	Parameter
IEEE802.1X	Port-based authentication (static)	snmp-server host	dot1x
		authentication force-authorized	enable
	Port-based authentication (dynamic)	snmp-server host	dot1x
		authentication force-authorized	enable
		authentication force-authorized	vlan#
	VLAN-based authentication (dynamic)	-- (There is no configuration because this mode is not supported.)	
Web authentication	Fixed VLAN mode	snmp-server host	web-authentication
		authentication force-authorized	enable
	Dynamic VLAN mode	snmp-server host	web-authentication
		authentication force-authorized	enable
		authentication force-authorized	vlan#
	Legacy mode	-- (There is no configuration because this mode is not supported.)	
MAC-based authentication	Fixed VLAN mode	snmp-server host	mac-authentication
		authentication force-authorized	enable
	Dynamic VLAN mode	snmp-server host	mac-authentication
		authentication force-authorized	enable

Authentication type	Authentication mode	Configuration necessary to issue trap	
		Command	Parameter
		`authentication force-authorized`	`vlan`#
	Legacy mode	-- (There is no configuration because this mode is not supported.)	

#

If `authentication force-authorized vlan` has not been configured, control is done in fixed VLAN mode. See *(3) Post-authentication VLAN by forced authentication.*

5.4.7 Terminal control when authentication fails

The Switch controls up to 256 terminals in MAC address units using information related to authentication-failed terminals in Layer 2 authentication modes. The information is in the authentication-failed terminal list. You can display this list by using the `show authentication fail-list` operation command.

Each authentication method registers the terminals in the list when the terminal authentication failure is confirmed. Processing in case of authentication failure is common to local and RADIUS authentication.

The following table shows processing in case of authentication failure

Table 5-25 Processing in case of authentication failure

Authentication type	Item	Authentication result for new authentication		Authentication result when re-authentication is executed	
		Reject	Failure other than `Reject`	Reject	Failure other than `Reject`
IEEE802.1X	Status of the target terminal in the authentication control table	"HELD" (period specified with `quiet-period` maintained)	"Connecting" (waiting for the next authentication)	"HELD" (period specified with `quiet-period` maintained)	"Connecting" (waiting for the next authentication)
	Status of the entry for the target terminal in the MAC address table	--	--	Deleted	Deleted
	Timing to register in the failed terminal list	Immediately registered in case of failure	Immediately registered in case of failure	Immediately registered in case of failure	Immediately registered in case of failure

Authentication type	Item	Authentication result for new authentication		Authentication result when re-authentication is executed	
		Reject	Failure other than `Reject`	Reject	Failure other than `Reject`
	(`fail-list`)				
Web authentication	Status of the target terminal in the authentication control table	Target entry deleted	Target entry deleted	"Authenticated" (No period update leaving the existing entry)	"Authenticated" (No period update leaving the existing entry)
	Status of the entry for the target terminal in the MAC address table	--	--	Remaining registered	Remaining registered
	Timing to register in the failed terminal list (`fail-list`)	Immediately registered in case of failure	Immediately registered in case of failure	Immediately registered in case of failure	Immediately registered in case of failure
MAC-based authentication	Status of the target terminal in the authentication control table	Held (period specified with `quiet-period` maintained)	Held (period specified with `quiet-period` maintained)	Held (period specified with `quiet-period` maintained)	Held (period specified with `quiet-period` maintained)
	Status of the entry for the target terminal in the MAC address table	--	--	Deleted	Deleted
	Timing to register in the failed terminal list (`fail-list`)	Registered when `quiet-period` expires	Registered when `quiet-period` expires	Registered when `quiet-period` expires	Registered when `quiet-period` expires

Legend:

--: No entry for a target terminal in the MAC address table because new authentication has failed

5.5 Configuration commands common to all Layer 2 authentication modes

5.5.1 List of configuration commands

This section describes configuration common to all Layer 2 authentication modes.

Table 5-26 List of configuration commands common to all Layer 2 authentication modes and all authentication modes

Command name	Description	Authentication mode		
		F	D	L
`authentication arp-relay`	Outputs ARP frames sent from unauthenticated terminals to other devices to a non-authenticating port.	Y	Y	N
`authentication ip access-group`	Outputs only the frames specified by applying the IPv4 access list, among the IP frames sent from an unauthenticated terminal destined for another device, to a non-authenticating port.	Y	Y	N
`authentication force-authorized enable`	Enables forced authentication common to all authentication modes.	Y	Y	N
`authentication force-authorized vlan`	Specifies the post-authentication VLAN accommodated by sharing of dynamic VLAN mode of the target port.	Y	Y	N
`name`	Specifies a VLAN name for a VLAN.	--	Y	Y

Legend:

F: Fixed VLAN mode

D: Dynamic VLAN mode

L: Legacy mode

Y: The command operates according to the settings.

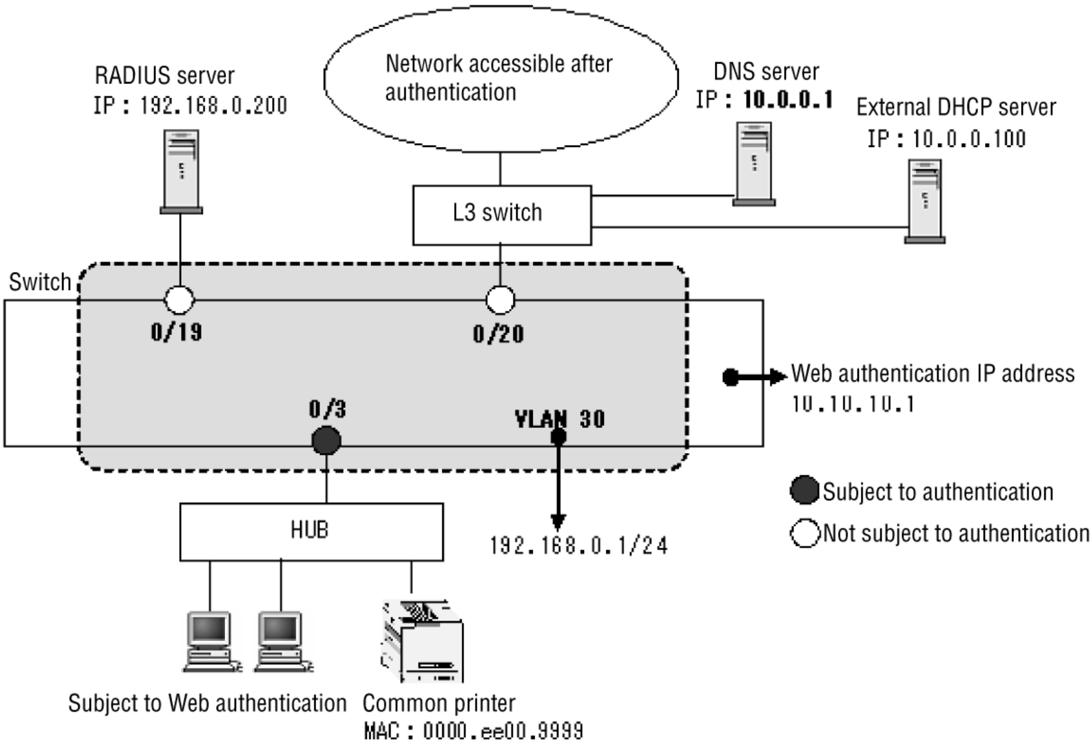
N: The command cannot be entered.

-: Outside the scope of *5.4.2 Specifying post-authentication VLANs by VLAN name.*

5.5.2 Configuring the authentication IPv4 access list

This example uses an external DHCP server in Web authentication fixed VLAN mode. For details about the Web authentication fixed VLAN mode configuration, see *9.3* Configuring fixed VLAN mode.

Figure 5-20 Example of using an authentication IPv4 access list



Points to note

The example below shows how to configure an authentication IPv4 access list that allows the passing of ARP frames and traffic from unauthenticated terminals to destinations beyond the Switch.

(The configuration necessary for other authentication has been set in the configuration, and this example displays only the settings used for passage before authentication.)

Command examples

1.
```
(config)# ip access-list extended L2-auth
(config-ext-nacl)# permit udp any any eq bootps
(config-ext-nacl)# permit ip any host 10.0.0.1
(config-ext-nacl)# exit
(config)# interface fastethernet 0/3
(config-if)# web-authentication port
(config-if)# authentication ip access-group L2-auth
(config-if)# authentication arp-relay
(config-if)# exit
```

Configures an authentication IPv4 access list that permits unauthenticated terminals to access DHCP frames (`bootp`) and IP address 10.0.0.1 (DNS server).

Configures the authentication mode setting (`web-authentication port`) and the access list name (`L2-auth`) of conditions for access before authentication, to port 0/3.

Configures ARP frames so that they are passed to devices beyond the Switch.

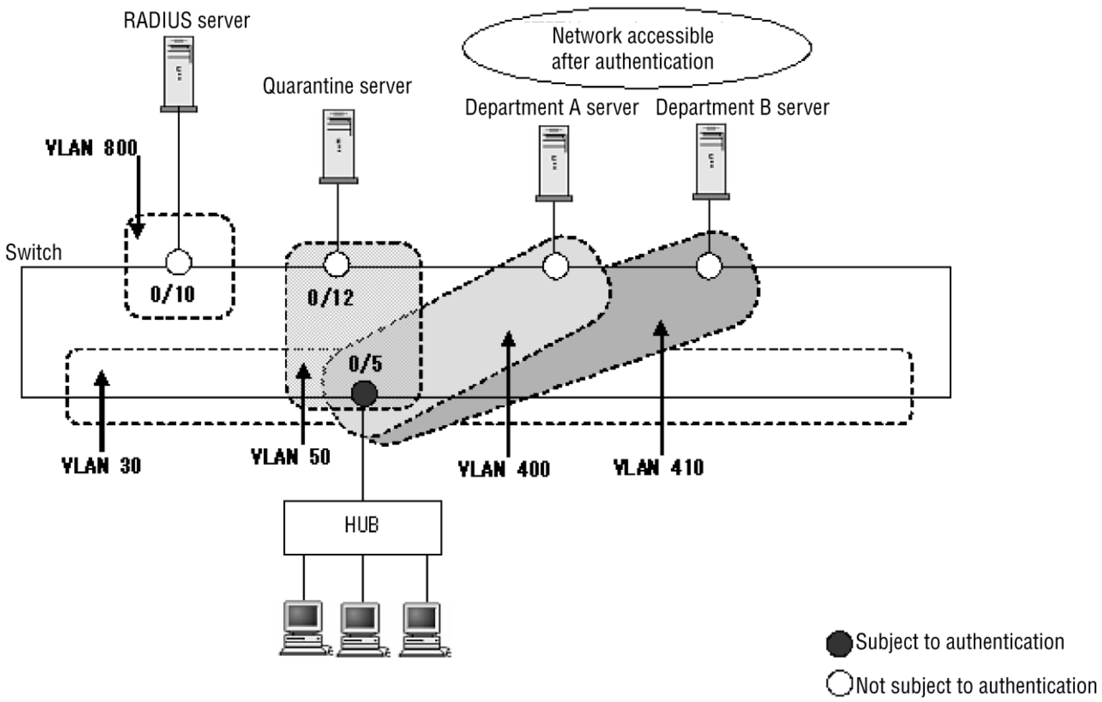
Notes

1. Configure any one of the following before configuring an authentication IPv4 access list and passage of ARP frames to a port.
   - `dot1x port-control auto`
   - `web-authentication port`
   - `mac-authentication port`
2. Delete both of the following commands from the target port before deleting the authentication configuration of the port where an authentication IPv4 access list and passage of ARP frames have been configured.
   - `authentication arp-relay`
   - `authentication ip access-group`

5.5.3 Specifying post-authentication VLANs by VLAN name

This example uses the Web authentication dynamic VLAN mode.

Figure 5-21 Example of specifying a VLAN name in dynamic VLAN mode



Points to note

The following example configures dynamic VLAN mode and a control name for post-authentication VLANs. The example also uses a control name to set the VLAN to be accommodated after authentication by the RADIUS server after authentication

- `VLAN 30`: Pre-authentication VLAN

- `VLAN 50`: Quarantine VLAN
- `VLAN400`: Department A network after authentication
- `VLAN410`: Department B network after authentication

  For other configurations necessary for Web authentication, see *9. Web Authentication Configuration and Operation.*

Command examples

1. `(config)# vlan 30,800`

   `(config-vlan)# exit`

   Configures VLAN ID 30, 800.

2. `(config)# vlan 50 mac-based`

   `(config-vlan)# name Keneki-Network`

   `(config-vlan)# exit`

   Configures the MAC VLAN and the quarantine VLAN name to VLAN ID 50.

3. `(config)# vlan 400 mac-based`

   `(config-vlan)# name GroupA-Network`

   `(config-vlan)# exit`

   Configures the MAC VLAN and Department A network VLAN after authentication to VLAN ID 400.

4. `(config)# vlan 410 mac-based`

   `(config-vlan)# name GroupB-Network`

   `(config-vlan)# exit`

   Configures the MAC VLAN and Department B network VLAN after authentication to VLAN ID 410.

5. `(config)# interface fastethernet 0/5`

   `(config-if)# switchport mode mac-vlan`

   `(config-if)# switchport mac native vlan 30`

   Configures the port 0/5 for the MAC port. Also, configures a native VLAN30 (pre-authentication VLAN) of the MAC port. (The post-authentication VLAN is assigned according to *5.4.3 Auto VLAN assignment for a MAC VLAN.)*

6. `(config-if)# web-authentication port`

   `(config-if)# exit`

   Configures the authentication mode (`web-authentication port`) to port 0/5.

7. `(config)# interface fastethernet 0/10`

```
(config-if)# switchport mode access
(config-if)# switchport access vlan 800
(config-if)# exit
```

Configures port 0/10 as an access port for VLAN 800. This command does not configure the authentication mode because authentication is exempted. This command configures the port as the port for the RADIUS server in the figure.

8.

```
(config)# interface fastethernet 0/12
(config-if)# switchport mode access
(config-if)# switchport access vlan 50
(config-if)# exit
```

Configures port 0/12 as the access port for VLAN50. This command does not configure the authentication mode because authentication is exempted. This command configures the port as the port for the quarantine port in the figure.

Configure the following for the RADIUS server.

- When the quarantine result is `NG`: `Keneki-Network` to `Tunnel-Group-ID`
- When the quarantine result is `OK`:
  - Switches to post-authentication VLAN of Department A : `GroupA-Network` to `Tunnel-Group-ID`
  - Switches to post-authentication VLAN of Department B: `GroupB-Network` to `Tunnel-Group-ID`

In Legacy mode, configure the following instead of 5 and 6 in the configuration command example.

- In step 5, configure the following:

```
(config)# interface fastethernet 0/5
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 50,400,410
(config-if)# switchport mac native vlan 30
(config-if)# exit
```

- In step 6, configure the following:

```
(config)# web-authentication vlan 50
(config)# web-authentication vlan 400
(config)# web-authentication vlan 410
```

Configures VLAN ID 50, 400, 410 of post-authentication VLANs in Legacy mode.

Notes

1. Be careful of the following when using a VLAN name configured using the `name` configuration command as a post-authentication VLAN.
   - Specify a unique VLAN name. If the same VLAN name is used for two or more VLANs, the smallest VLAN ID is assigned as the post-authentication VLAN in RADIUS authentication mode.

- Do not specify a number at the beginning of the VLAN name. A number at the beginning will be recognized as the VLAN ID, which might result in an authentication failure.

2. Be careful of the following when assigning the post-authentication VLAN using auto VLAN assignment for the MAC VLAN.
    - Use the `vlan mac-based` configuration command to set the VLAN to be notified from the RADIUS server when automatically allocating post-authentication VLANs in dynamic VLAN mode. (In this case, you do not have to assign the `switchport mac vlan` configuration command to the MAC port.)
    - If there is no auto VLAN assignment information in RADIUS attributes and when `Accept` is received from the RADIUS server, the terminal is accommodated in the native VLAN of the target MAC port. The terminal will be authenticated in fixed VLAN mode.
    - Legacy mode cannot be used. Set the post-authentication VLAN by using the `switchport mac vlan` configuration command.

5.5.4 Forced authentication configuration common to all authentication modes

Configure the forced authentication method used in all authentication modes.

Points to note

The example below configures forced authentication when multistep authentication is used:

- Configure RADIUS authentication as the authentication method for each authentication method.
- Configure multistep authentication for port 0/1.
- Configure the post-authentication VLAN at forced authentication.

For other procedures necessary for multistep authentication, see *12. Multistep authentication.*

Command examples

1. `(config)# vlan 40,600 mac-based`

   `(config-vlan)# exit`

   Configures VLAN ID 40, 600 as a MAC VLAN.

2. `(config)# vlan 20`

   `(config-vlan)# exit`

   Configures VLAN ID 20.

3. `(config)# aaa authentication web-authentication default group radius`

   `(config)# aaa authentication mac-authentication default group radius`

   Configures RADIUS authentication as an authentication method for each authentication method.

4. `(config)# authentication force-authorized enable`

   Enables forced authentication common to all authentication modes.

5. ```
   (config)# interface fastethernet 0/1
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac native vlan 20
   (config-if)# mac-authentication port
   (config-if)# web-authentication port
   (config-if)# authentication multi-step
   ```

   Configures a MAC port, Web authentication mode, MAC-based authentication mode, and multistep authentication mode for port 0/1. Also, configures native VLAN 20 (pre-authentication VLAN) on a MAC port. (The post-authentication VLAN is assigned according to *5.4.3 Auto VLAN assignment for a MAC VLAN.)*

6. ```
   (config-if)# authentication force-authorized vlan 600
   (config-if)# exit
   ```

   Sets 600 for the post-authentication VLANs at forced authentication.

Notes

1. If forced authentication for each authentication method has been configured, forced authentication configuration common to all authentication modes cannot be configured.

   Delete specified configurations in *Table 5-23 Non-interoperable forced authentication configuration,* and then configure forced authentication common to all authentication modes.
2. Configure only RADIUS authentication as an authentication method for each authentication method. If you have set priority of RADIUS authentication and local authentication, the forced authentication method is disabled.
3. Configure the following for RADIUS attribute Filter-Id of a RADIUS server for multistep authentication in this example.
   - For a MAC-based authentication RADIUS server: `@@Web-Auth@@`
4. Use the `vlan mac-based` configuration command to set the VLAN to be notified from the RADIUS server when automatically allocating post-authentication VLANs in dynamic VLAN mode. (In this case, you do not have to assign the `switchport mac vlan` configuration command to the MAC port.)
5. If there is no auto VLAN assignment information in RADIUS attributes and when `Accept` is received from the RADIUS server, the terminal is accommodated in the native VLAN of the target MAC port. The terminal will be authenticated in fixed VLAN mode.

5.6 Operations common to all Layer 2 authentication methods

5.6.1 List of operation commands

This section describes the operation commands common to all Layer 2 authentication modes.

Table 5-27 List of the operation commands common to all Layer 2 authentication modes

Command name	Description
`show authentication fail-list`	Shows information related to terminals that failed to pass Layer 2 authentication in the ascending order of MAC addresses.
`clear authentication fail-list`	Clears information related to terminals that failed to pass Layer 2 authentication.
`show authentication logging`	Shows operational log messages logged by each Layer 2 authentication in the order they were logged.
`clear authentication logging`	Clears operational log messages shown in the order they were logged..

5.7 Interoperability of Layer 2 authentication with other functionality

This section uses the following terms for the authentication modes: *fixed VLAN mode*, *dynamic VLAN mode*, and *legacy mode*. The authentication modes for IEEE 802.1X correspond to the following:

- Port-based authentication (static): Fixed VLAN mode
- Port-based authentication (dynamic): Dynamic VLAN mode
- VLAN-based authentication (dynamic): Legacy mode

5.7.1 Interoperability on the Switch

In the Switch, the authentication methods of fixed VLAN mode, dynamic VLAN mode, and legacy mode are interoperable based on the port type.

The following figure shows interoperable authentication methods and behavior that is supported or not supported.

Figure 5-22 Interoperable authentication methods and supported/unsupported behavior

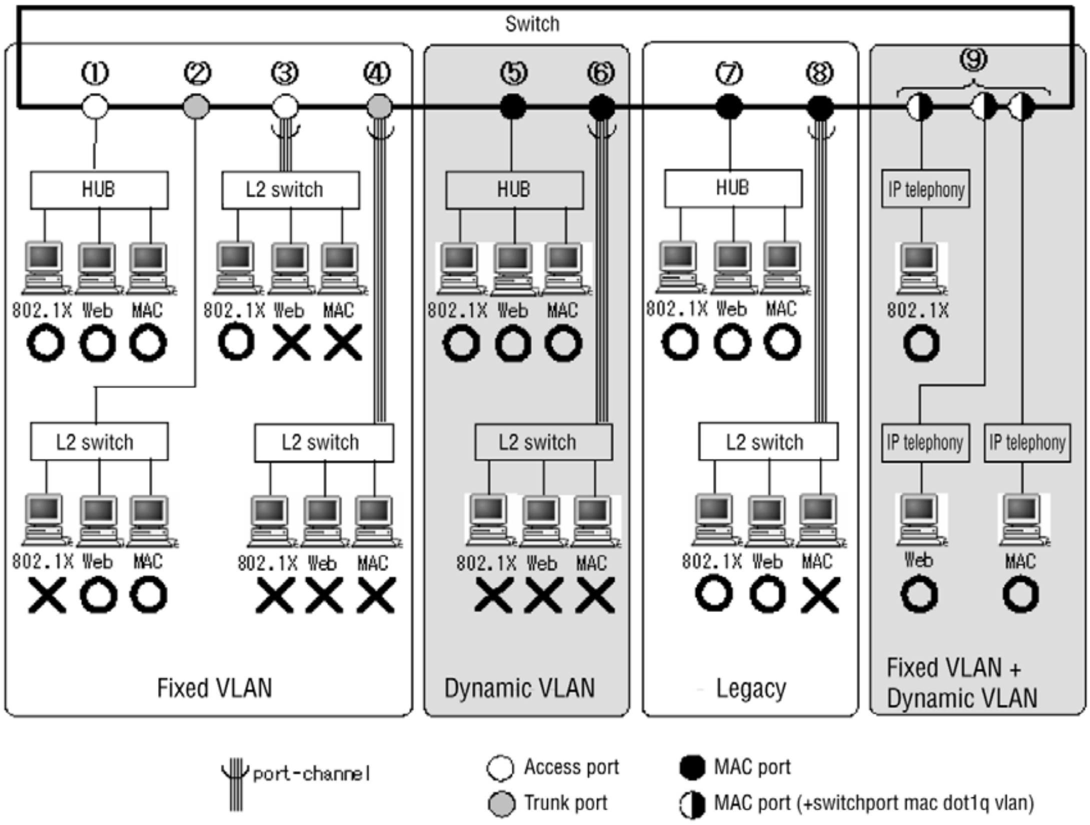


Table 5-28 Combinations of authentication modes and port types, and supported/unsupported authentication methods

Authentication mode Category	In the figure No.	Port type	Supported/unsupported authentication methods and corresponding authentication modes		
			IEEE802.1X	Web authentication	MAC-based authentication
Fixed VLAN	①	Access	Y Port-based authentication (static)	Y Fixed VLAN mode	Y Fixed VLAN mode
	②	Trunk	N	Y Fixed VLAN mode	Y Fixed VLAN mode
	③	Access (port-channel)	Y Port-based authentication (static)	N	N
	④	Trunk (port-channel)	N	N	N
Dynamic VLAN	⑤	MAC	Y Port-based authentication (dynamic)	Y Dynamic VLAN mode	Y Dynamic VLAN mode
	⑥	MAC (port-channel)	N	N	N
Legacy	⑦	MAC	Y VLAN-based authentication (dynamic)	Y Legacy mode	Y Legacy mode
	⑧	MAC (port-channel)	Y VLAN-based authentication (dynamic)	Y Legacy mode	N
Fixed VLAN + dynamic VLAN	⑨	MAC# (Tagged)	N	Y Fixed VLAN mode	Y Fixed VLAN mode
		MAC# (Untagged)	Y Port-based authentication (dynamic)	Y Dynamic VLAN mode	Y Dynamic VLAN mode

Legend:

Y: Supported

N: Not supported

--: Not applicable

#

This is when the permission to forward tagged frames is set (the `switchport mac dot1q vlan configuration` configuration command). In this case, a tagged frame is received from an IP telephone and authenticated in fixed VLAN mode while an untagged frame is received from a terminal and operated in dynamic VLAN mode.

The legacy port does not work on a MAC port that has this setting.

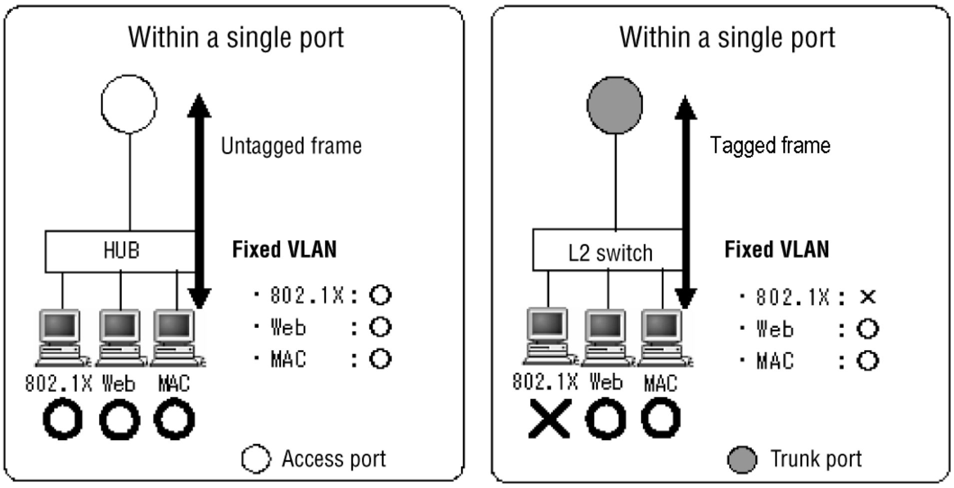
5.7.2 Interoperability on the same port

The following modes are interoperable simultaneously on the same port:

- Fixed VLAN mode
- Dynamic VLAN mode
- Legacy mode
- Dynamic VLAN mode and fixed VLAN mode

(1) Interoperability of fixed VLAN modes on the same port

Figure 5-23 Interoperability of fixed VLAN modes on the same port



When using interoperability of fixed VLAN mode on the same port, supported authentication methods depend on the port type (access port, trunk port) that connects to the Switch as shown in *Figure 5-23 Interoperability of fixed VLAN modes on the same port*. In addition, some authentication methods are not supported depending on the configuration.

Table 5-29 Supported/unsupported authentication methods based on configuration of an access port shows the authentication methods supported and not supported depending on the configuration when fixed VLAN mode interoperability is used at an access port.

Table 5-29 Supported/unsupported authentication methods based on configuration of an access port

Configuration contents		Authentication type		
Common configuration	**Authentication method configuration**	**IEEE802.1X**	**Web authentication**	**MAC-based authentication**
`switchport mode access` `switchport access`	`dot1x port-control auto` `dot1x multiple-authentication`# `web-authentication port` `mac-authentication port`	Y	Y	Y
	`web-authentication port` `mac-authentication port`	N	Y	Y
	`dot1x port-control auto` `dot1x multiple-authentication`# `mac-authentication port`	Y	N	Y
	`dot1x port-control auto` `dot1x multiple-authentication`# `web-authentication port`	Y	Y	N

Legend:

Y: Supported

N: Not supported

#

If configuring port-based authentication of IEEE 802.1X for a port where Web authentication or MAC-based authentication has been configured, configure the terminal authentication mode (`dot1x multiple-authentication`).

Table 5-30 Supported/unsupported authentication methods depending on configuration of a trunk port shows the authentication methods supported and not supported depending on the configuration when interoperability of fixed VLAN mode is used at a trunk port.

Table 5-30 Supported/unsupported authentication methods depending on configuration of a trunk port

Configuration contents		Authentication type		
Common configuration	**Authentication method configuration**	**IEEE802.1X**	**Web authentication**	**MAC-based authentication**
`switchport mode trunk` `switchport trunk`	`dot1x port-control auto` `web-authentication port` `mac-authentication port`	N	Y	Y

Configuration contents		Authentication type		
Common configuration	**Authentication method configuration**	**IEEE802.1X**	**Web authentication**	**MAC-based authentication**
	`web-authentication port` `mac-authentication port`	N	Y	Y
	`dot1x port-control auto` `mac-authentication port`	N	N	Y
	`dot1x port-control auto` `web-authentication port`	N	Y	N

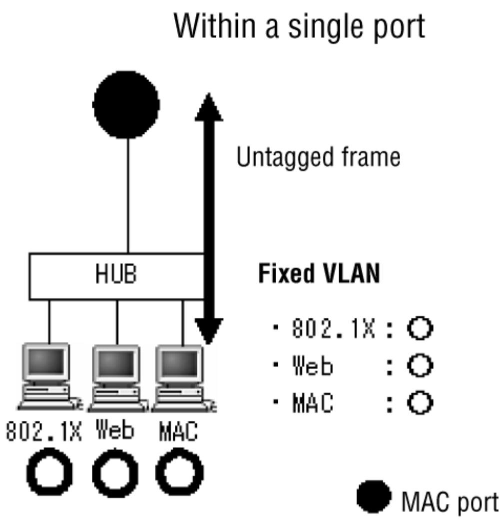
Legend:

Y: Supported

N: Not supported

(2) Dynamic VLAN mode interoperability on the same port

Figure 5-24 Interoperability of dynamic VLAN modes for the same port



When using dynamic VLAN mode interoperability for the same port, interoperability can be supported for all authentication methods (IEEE 802.1X, Web authentication, MAC-based authentication) by specifying the MAC port as a port connection for the Switch, as shown in *Figure 5-24 Interoperability of dynamic VLAN modes for the same port*. However, some authentication methods are not supported depending on the configuration.

For details, see *Table 5-31 Supported/unsupported authentication methods depending on configuration of a MAC port*.

Table 5-31 Supported/unsupported authentication methods depending on configuration of a MAC port

Configuration contents		Authentication type		
Common configuration	**Authentication method configuration**	**IEEE802.1X**	**Web authentication**	**MAC-based authentication**
`switchport mode mac-vlan` #1, #2	`dot1x port-control auto` `dot1x multiple-authentication`#3 `web-authentication port` `mac-authentication port`	Y	Y	Y
	`web-authentication port` `mac-authentication port`	N	Y	Y
	`dot1x port-control auto` `dot1x multiple-authentication`#3 `mac-authentication port`	Y	N	Y
	`dot1x port-control auto` `dot1x multiple-authentication`#3 `web-authentication port`	Y	Y	N

Legend:

Y: Supported

N: Not supported

#1

The post-authentication VLAN on the MAC port is assigned according to *5.4.3 Auto VLAN assignment for a MAC VLAN.*

#2

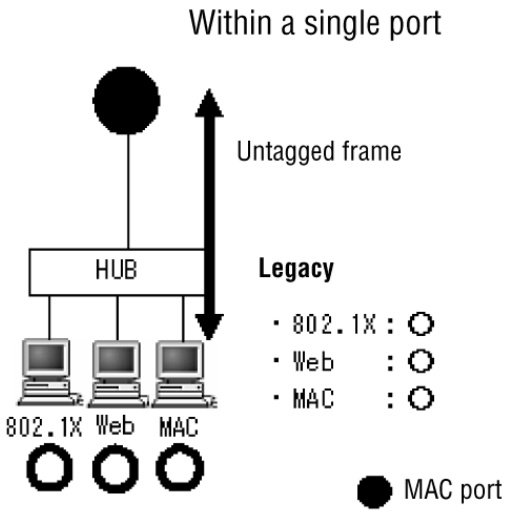
If there is no auto VLAN assignment information in RADIUS attributes and when `Accept` is received from the RADIUS server, the terminal is accommodated in the native VLAN of the target MAC port. The terminal will be authenticated in fixed VLAN mode.

#3

If configuring port-based authentication of IEEE 802.1X for a port where Web authentication or MAC-based authentication has been configured, configure the terminal authentication mode (`dot1x multiple-authentication`).

(3) Legacy mode interoperability on the same port

Figure 5-25 Interoperability of legacy modes on the same port



When using the legacy mode interoperability for the same port, interoperability can be supported for all authentication methods (IEEE 802.1X, Web authentication, MAC-based authentication) by specifying the MAC port as a port connection for the Switch, as shown in *Figure 5-25 Interoperability of legacy modes on the same port.* However, some authentication methods are not supported depending on the configuration.

For details, see *Table 5-32 Supported/unsupported authentication methods in Legacy mode depending on configuration of a MAC port.*

Table 5-32 Supported/unsupported authentication methods in Legacy mode depending on configuration of a MAC port

Configuration contents		Authentication type		
Configuration at interface	**Configuration in global configuration mode**	**IEEE802.1X**	**Web authentication**	**MAC-based authentication**
`switchport mode mac-vlan` `switchport mac vlan`	`aaa authorization network default` `dot1x vlan dynamic enable` `dot1x vlan dynamic vlan` `web-authentication vlan` `mac-authentication vlan`	Y	Y	Y
`switchport mode mac-vlan` `switchport mac vlan` `dot1x port-control auto`	`aaa authorization network default` `dot1x vlan dynamic enable` `dot1x vlan dynamic vlan` `web-authentication vlan` `mac-authentication vlan`	D	N	N

Configuration contents		Authentication type		
Configuration at interface	Configuration in global configuration mode	IEEE802.1X	Web authentication	MAC-based authentication
switchport mode mac-vlan switchport mac vlan web-authentication port	aaa authorization network default dot1x vlan dynamic enable dot1x vlan dynamic vlan web-authentication vlan mac-authentication vlan	N	D	N
switchport mode mac-vlan switchport mac vlan mac-authentication port	aaa authorization network default dot1x vlan dynamic enable dot1x vlan dynamic vlan web-authentication vlan mac-authentication vlan	N	N	D

Legend:

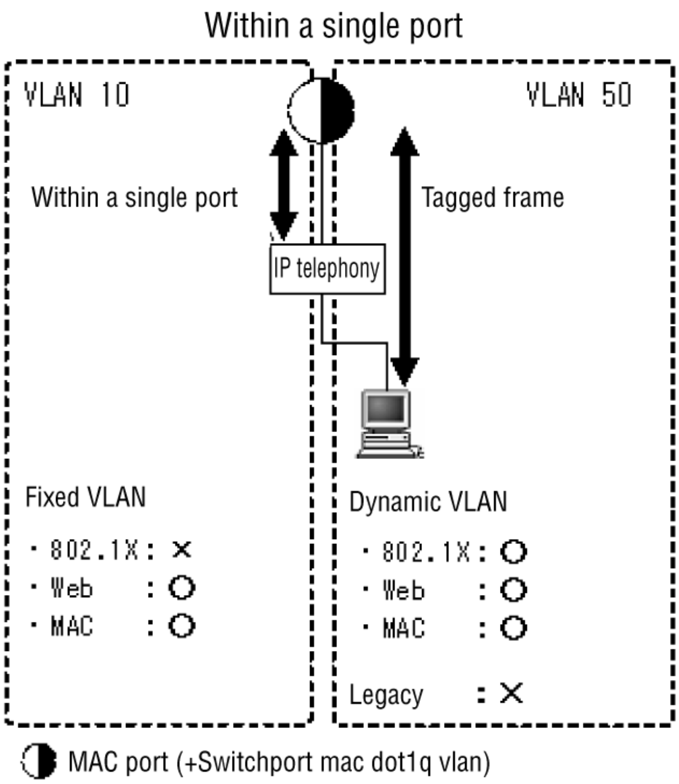
Y: Supported

N: Not supported

D: Supported in dynamic VLAN mode

(4) Interoperability of dynamic VLAN mode and fixed VLAN mode on the same port

Figure 5-26 Example of interoperability of dynamic VLAN mode and fixed VLAN mode on the same port



When using fixed VLAN mode and dynamic VLAN mode together for the same port, interoperability can be supported for all authentication methods (IEEE 802.1X, Web authentication, MAC-based authentication) by specifying the MAC port as the port connection for the Switch as shown in *Figure 5-26 Example of interoperability of dynamic VLAN mode and fixed VLAN mode on the same port*. However, IEEE 802.1X is unavailable in fixed VLAN mode. In addition, some authentication methods are not supported depending on the configuration.

For details, see *Table 5-33 Supported/unsupported authentication methods depending on configuration of a MAC port with interoperability of fixed VLAN mode and dynamic VLAN mode*.

Table 5-33 Supported/unsupported authentication methods depending on configuration of a MAC port with interoperability of fixed VLAN mode and dynamic VLAN mode

Configuration contents	Frame type	Authentication type		
		IEEE802.1X	**Web authentication**	**MAC-based authentication**
- vlan 50 mac-based[#1, #4]	Tagged	N	F[#2]	F[#2]

Configuration contents	Frame type	Authentication type		
		IEEE802.1X	Web authentication	MAC-based authentication
- switchport mode mac-vlan - switchport mac dot1q vlan 10[#1]	Untagged	D[#3]	D[#3]	D[#3]
		F[#5]	F[#5]	F[#5]

Legend:

F: Supported in fixed VLAN mode

D: Supported in dynamic VLAN mode

N: Not supported

#1

VLAN numbers are arranged based on *Figure 5-26 Example of interoperability of dynamic VLAN mode and fixed VLAN mode on the same port*. The assumption is that each authentication mode has been configured (`dot1x port-control auto`, `web-authentication port`, `mac-authentication port`).

#2

Receives a tagged frame and authenticates it in fixed VLAN mode (authentication of IP telephone in *Figure 5-26 Example of interoperability of dynamic VLAN mode and fixed VLAN mode on the same port)*

#3

Receives an untagged frame and authenticates it in dynamic VLAN mode (authentication of a terminal in *Figure 5-26 Example of interoperability of dynamic VLAN mode and fixed VLAN mode on the same port)*

#4

The post-authentication VLAN on the MAC port is assigned according to *5.4.3 Auto VLAN assignment for a MAC VLAN.*

#5

If there is no auto VLAN assignment information in RADIUS attributes and when `Accept` is received from the RADIUS server, the terminal is accommodated in the native VLAN of the target MAC port. The terminal will be authenticated in fixed VLAN mode.

5.8 Configuration for interoperability of Layer 2 authentication

An example of the configuration for interoperability of Layer 2 authentication is given below:

- Fixed VLAN mode and dynamic VLAN mode are interoperable on the same port.

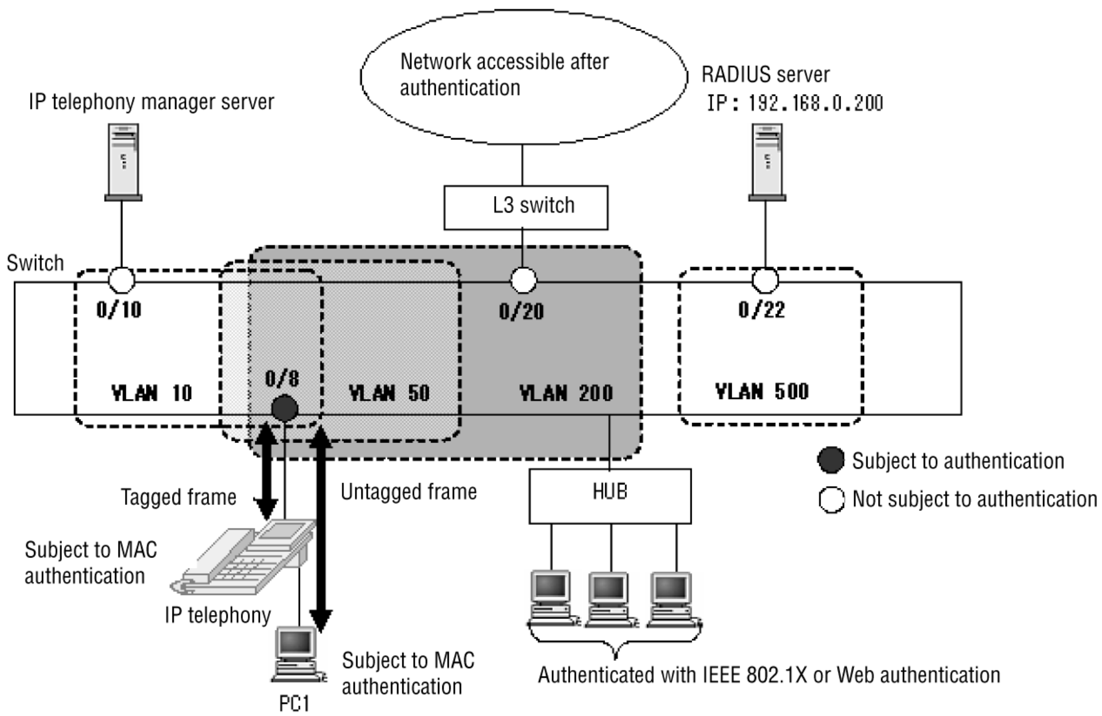
  See *5.8.1 Configuration where a tagged frame is authenticated on a MAC port*.

5.8.1 Configuration where a tagged frame is authenticated on a MAC port

A tagged frame is forwarded to the MAC port by using the `switchport mac dot1q vlan` configuration command.

This example uses MAC-based authentication and receives the tagged frame on the same port in fixed VLAN mode, which authenticates an untagged frame in dynamic VLAN mode.

Figure 5-27 Example of a configuration where a tagged frame is authenticated on a MAC port



Points to note

The example below shows how to configure a MAC port as one subject to MAC-based authentication, and to configure the same port to handle tagged and untagged frames. RADIUS authentication is used as an example of the authentication method.

- VLAN 10: Handles tagged frames and authenticates them in fixed VLAN mode.
- VLAN 50, 200: Handles untagged frames and authenticates them in

dynamic VLAN mode (pre-authentication VLAN: 50, authenticated VLAN: 200).

For other items necessary to configure for MAC-based authentication, see *11. MAC-based Authentication Configuration and Operation.*

Command examples

1. `(config)# vlan 200 mac-based`

   `(config-vlan)# exit`

   Configures VLAN ID 200 as a MAC VLAN.

2. `(config)# vlan 10,50,500`

   `(config-vlan)# exit`

   Configures VLAN ID 10, 50, 500.

3. `(config)# interface fastethernet 0/8`

   `(config-if)# switchport mode mac-vlan`

   Specifies the port 0/8 for as a MAC port.

4. `(config-if)# switchport mac dot1q vlan 10`

   Configures VLAN 10 as the VLAN that handles a tagged frame on a MAC port.

5. `(config-if)# switchport mac native vlan 50`

   Configures a native VLAN50 (pre-authentication VLAN) of a MAC port. (The post-authentication VLAN is assigned according to *5.4.3 Auto VLAN assignment for a MAC VLAN.)*

6. `(config-if)# mac-authentication port`

   `(config-if)# exit`

   Configures the authentication mode (`mac-authentication port`) for port 0/8

7. `(config)# interface fastethernet 0/10`

   `(config-if)# switchport mode access`

   `(config-if)# switchport access vlan 10`

   `(config-if)# exit`

   Configures port 0/10 as the access port of VLAN 10. Does not configure the authentication mode because authentication is exempted. Communication is possible after IP telephony in the figure is authenticated.

8. `(config)# interface fastethernet 0/20`

   `(config-if)# switchport mode access`

```
(config-if)# switchport access vlan 200
(config-if)# exit
```

Configures port 0/20 as the access port of VLAN200. Does not configure the authentication mode because authentication is exempted. Communication is possible after the terminal PC1 in the figure is authenticated.

9.
```
(config)# interface fastethernet 0/22
(config-if)# switchport mode access
(config-if)# switchport access vlan 500
(config-if)# exit
```

Configures port 0/22 as the access port of VLAN500. Does not configure the authentication mode because authentication is exempted. This is set for port used for the RADIUS server in the figure.

Notes

1. For details about tagged frame relay of a MAC port, see *17.7 Description of MAC VLANs* in the *Configuration Guide Vol. 1*.
2. Use the `vlan mac-based` configuration command to set the VLAN to be notified from the RADIUS server when automatically allocating post-authentication VLANs in dynamic VLAN mode. (In this case, you do not have to assign the `switchport mac vlan` configuration command to the MAC port.)
3. If there is no auto VLAN assignment information in RADIUS attributes and when `Accept` is received from the RADIUS server, the terminal is accommodated in the native VLAN of the target MAC port. The terminal will be authenticated in fixed VLAN mode.

5.9 Notes on using Layer 2 authentication methods

5.9.1 Notes on using common Layer 2 authentication methods

(1) Configuring an authentication method list

The port-based authentication method and the user ID-based Web authentication method are not interoperable on the Switch. Legacy mode is also not interoperable with other methods. See *(3) Exclusive relationship of authentication method list configuration* in *5.2.2 Authentication method list.*

(2) Permitting communication by unauthenticated terminals

Use the following commands for each authentication mode to configure ports subject to authentication before configuring the `authentication ip access-group` configuration command. You cannot use the `authentication ip access-group` command before you complete the following configurations:

- IEEE 802.1X: `dot1x port-control auto`
- Web authentication: `web-authentication port`
- MAC-based authentication: `mac-authentication port`

(3) Auto VLAN assignment for a MAC VLAN

Use the `vlan mac-based` configuration command to configure, in the Switch the post-authentication VLAN to be notified by a RADIUS server. Configure a MAC port for the port subject to authentication.

(4) Auto authentication mode accommodation on the same MAC port

When an untagged frame is received from a terminal subject to authentication, the Switch determines the authentication mode based on the VLAN ID obtained by using the RADIUS attribute `Tunnel-Private-Group-ID` of `Access-Accept` received from RADIUS authentication. If the obtained VLAN ID has been configured by using the `switchport mac dot1q vlan` configuration command for a port, it is judged as an invalid VLAN and authentication fails.

(5) Forced authentication common to all authentication modes

The Switch provides forced authentication methods common to all authentication modes and specific to each authentication mode, both of which are not interoperable. See *(4) Interoperability of this functionality and forced authentication of each authentication method* in *5.4.6 Forced authentication common to all authentication modes.*

5.9.2 Interoperability of several Layer 2 authentication methods

(1) Using several Layer 2 authentication methods on the same port

The authentication permitted first will be given priority when executing VLAN-based IEEE 802.1X authentication (dynamic), Web authentication, and MAC-based authentication using one terminal.

Because MAC-based authentication uses all frames sent from terminals subject to authentication as the trigger for authentication, MAC-based authentication typically executes first. However, if no permission information for MAC-based authentication has been registered on a RADIUS server or the information cannot be checked in the internal MAC-based authentication DB, MAC-based authentication is held (for `mac-authentication timeout quiet-period`) during which it waits for IEEE 802.1X or Web authentication to execute.

If IEEE 802.1X or Web authentication executes during this period, the first permitted authentication method is enabled, and other authentication methods cannot be overwritten until the authentication state is canceled.

In this case, authentication failure is recorded in the account logs of other authentication methods that failed to overwrite.

If IEEE 802.1X or Web authentication is not completed during the time in which MAC-based authentication is held, a failure log is written in the account log for MAC-based authentication.

(2) When exceeding the maximum number of accommodations with several authentication methods used together

When exceeding the maximum number of accommodations with several authentication methods used together, authentication failure is recorded in the account log information of the authentication method under processing.

5.9.3 Interoperability of the Layer 2 authentication functionality and other functionality

The following table describes the specifications for interoperability of the Layer 2 authentication functionality with other functionality.

Table 5-34 Interoperability specifications for Layer 2 authentication functionality with other functionality

Layer 2 authentication functionality	Function name		Interoperability
IEEE802.1X	Link aggregation		Port-based authentication (static) or port-based authentication (dynamic) can be used for a port that belongs to a channel group for static or LACP link aggregation.
	VLAN	Port VLAN	Can be used with port-based (static) authentication.
		Protocol VLAN	Cannot coexist on the same device.
		MAC VLAN	Can be used for port-based authentication (static or dynamic) and VLAN-based authentication (dynamic).
	Default VLAN		Can be used with port-based (static) authentication. For port-based authentication (dynamic) or VLAN-based authentication (dynamic), the default VLAN can be used as a pre-authentication VLAN.
	Extended VLAN functionality	EAPOL forwarding	Cannot coexist on the same device.
	Spanning Tree Protocol		The Spanning Tree Protocol cannot be used on an IEEE 802.1X authentication port.

Layer 2 authentication functionality	**Function name**		**Interoperability**
	Ring Protocol		The Ring Protocol cannot be used on an IEEE 802.1X authentication port.
	IGMP snooping		IGMP snooping cannot be used on an IEEE 802.1X authentication port.
	DHCP snooping		Can be used concurrently.#
	L2 loop detection		Can be used concurrently.
	GSRP aware		The GSRP aware functionality cannot be used on an IEEE 802.1X authentication port.
	Uplink redundancy		Cannot be used on uplink ports
	CFM		See *20.1.9 Notes on using the CFM functionality*.
	IEEE 802.3ah/UDLD		UDLD cannot be used on an IEEE 802.1X authentication port.
	LLDP		LLDP cannot be used on an IEEE 802.1X authentication port.
Web authentication	Link aggregation		Legacy mode can be used for a port that belongs to a channel group for static or LACP link aggregation.
	VLAN	Port VLAN	Can be used in fixed VLAN mode.
		Protocol VLAN	Cannot coexist on the same device.
		MAC VLAN	Can be used in fixed LAN mode, dynamic VLAN mode, and legacy mode.
	Default VLAN		Can be used in fixed VLAN mode. Can also be used in dynamic VLAN mode and legacy mode on the pre-authentication VLAN.
	Extended VLAN functionality	EAPOL forwarding	Can be used on the same device.
	Spanning Tree Protocol		The Spanning Tree Protocol cannot be used on a Web authentication port.
	Ring protocol		The Ring Protocol cannot be used on a Web authentication port.
	IGMP snooping		IGMP snooping cannot be used on a Web authentication port.

Layer 2 authentication functionality	Function name		Interoperability
	DHCP snooping		Can be used concurrently.#
	L2 loop detection		Can be used concurrently.
	GSRP aware		The GSRP aware functionality cannot be used on a Web authentication port.
	Uplink redundancy		Cannot be used on uplink ports
	CFM		See *20.1.9 Notes on using the CFM functionality*.
	IEEE 802.3ah/UDLD		Do not use IEEE 802.3ah/UDLD on a port configured for Web authentication.
	LLDP		LLDP cannot be used on a Web authentication port.
MAC-based authentication	Link aggregation		MAC-based authentication is disabled on a port that belongs to a channel group for static or LACP link aggregation.
	VLAN	Port VLAN	Can be used in fixed VLAN mode.
		Protocol VLAN	Cannot coexist on the same device.
		MAC VLAN	Can be used in fixed LAN mode, dynamic VLAN mode, and legacy mode.
	Default VLAN		Can be used in fixed VLAN mode. Can also be used in dynamic VLAN mode and legacy mode on the pre-authentication VLAN.
	Extended VLAN functionality	EAPOL forwarding	Can be used on the same device.
	Spanning Tree Protocol		The Spanning Tree Protocol cannot be used on a MAC-based authentication port.
	Ring protocol		The Ring Protocol cannot be used on a MAC-based authentication port.
	IGMP snooping		IGMP snooping cannot be used on a MAC-based authentication port.
	DHCP snooping		Can be used concurrently.#
	L2 loop detection		Can be used concurrently.
	GSRP aware		The GSRP aware functionality cannot be used on a MAC-based authentication port.

Layer 2 authentication functionality	Function name	Interoperability
	Uplink redundancy	Cannot be used on uplink ports
	CFM	See *20.1.9 Notes on using the CFM functionality*.
	IEEE 802.3ah/UDLD	Do not use IEEE 802.3ah/UDLD on a port configured for MAC-based authentication.
	LLDP	LLDP cannot be used on a MAC-based authentication port.

#

When a Layer 2 authentication method and DHCP snooping are used together, the maximum number of terminals that can communicate is the number of the DHCP snooping-controlled terminals (a maximum of 246 terminals).

6. Description of IEEE 802.1X

IEEE 802.1X functionality authenticates Layer 2 of the OSI layer model. This chapter provides an overview of IEEE802.1X.

6.1 Overview of IEEE 802.1X functionality

The IEEE 802.1X authentication functionality prevents unauthorized clients from connecting to the network. A back-end authentication server, typically a RADIUS server, authenticates each terminal before making available any services offered by the Switch.

The following table describes the entities involved in IEEE 802.1X authentication, and how they interact.

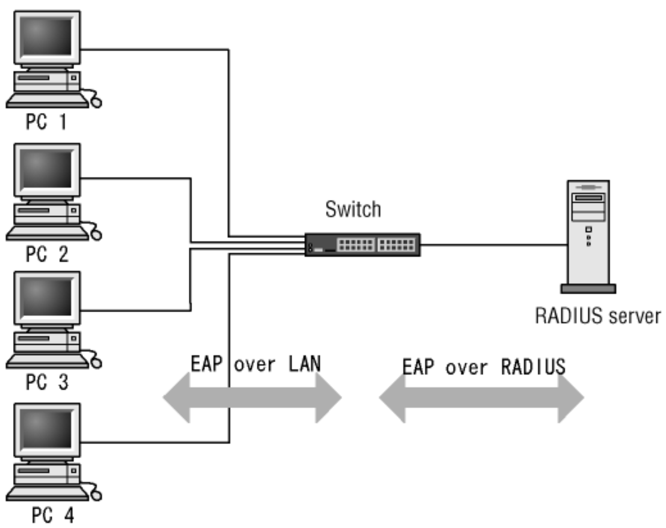
Table 6-1 Entities in IEEE 802.1X and their roles

Hardware components	Role
Switch (authenticator)	The authenticator controls access to the LAN and relays authentication information between the supplicant and the authentication server. EAP Over LAN (EAPOL) carries authentication traffic between the terminal and the Switch. Messages between the Switch and the authentication server are encapsulated into EAP over RADIUS. In this chapter, the term *Switch* refers to the Switch itself, and *authenticator* refers to the authenticator software running on the Switch.
Terminal (supplicant)	The terminal uses EAPOL packets to provide authentication information for the terminal to the Switch. In this manual, the terms *terminal* and *supplicant* include the terminal itself and the supplicant software running on it. The term *supplicant software* refers only to the software that provides supplicant functionality.
Authentication server	Performs the actual authentication of the terminal. The authentication server verifies the identity of the terminal and notifies the Switch as to whether the terminal is authorized to access the Switch services.

In a standard IEEE 802.1X configuration, terminals are connected directly to the ports of the Switch.

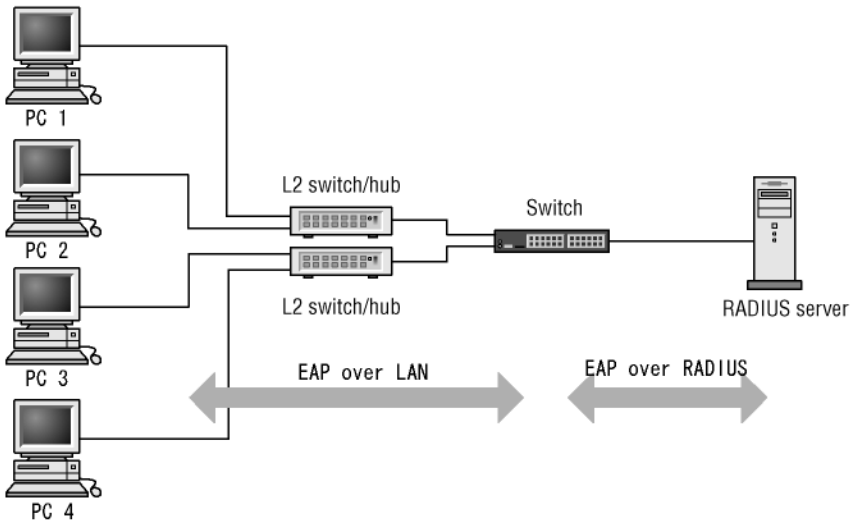
The following figure shows the basic configuration of IEEE 802.1X. whichi is used on a Switch.

Figure 6-1 Basic IEEE 802.1X model



The Switch supports extended functionality to authenticate several terminals on a single port (terminal authentication mode). This allows you to configure a topology in which the number of ports does not limit the number of terminals, by positioning an L2 switch or hub between the terminals and a Switch. For this configuration to work, the L2 switch between the terminals and the Switch must be configured to forward EAPOL packets. The following figures show the configuration.

Figure 6-2 IEEE 802.1X configuration with L2 switches between a Switch and terminals



6.1.1 Basic functionality

The IEEE 802.1X basic functionality supported by the Switch is shown below:

(1) Authentication operation mode supported by the Switch

The Switch takes the role of the authenticator in the IEEE 802.1X model. You cannot configure the Switch to act as a supplicant.

(2) Authentication method group

The Switch uses a RADIUS server for authentication. In this method, EAPOL packets received from the terminal are encapsulated into EAP over RADIUS packets and forwarded to the RADIUS server for authentication. The RADIUS server must support EAP.

You can configure the Switch into IEEE 802.1X authentication method groups as described below. (The configured authentication method groups can be used in all IEEE 802.1X authentication modes.)

- Switch default: RADIUS authentication method

  Authentication is performed by using a RADIUS server deployed on the network.

- Authentication method list

  Authentication is performed by using a RADIUS server group registered in the authentication method list when specific conditions are met.

For details, see the following sections:

- *5.1.3 Authentication method groups*

- *5.2.2 Authentication method list*
- *5.3.1 RADIUS server information used with the Layer 2 authentication method*
- *7.2.1 Configuring the authentication method group and RADIUS server information*

(3) Authentication algorithm

The following table describes the supported authentication algorithms.

Table 6-2 Supported authentication algorithms

Authentication algorithm	Overview
EAP-MD5-Challenge	Uses a challenge value to test the validity of user passwords.
EAP-TLS	Performs authentication based on a certificate authentication mechanism.
EAP-PEAP	Performs authentication using a separate EAP authentication algorithm encapsulated within an EAP-TLS tunnel.
EAP-TTLS	Performs authentication using an authentication algorithm of an existing protocol (such as EAP, PAP, or CHAP) encapsulated within an EAP-TLS tunnel.

6.1.2 Overview of extended functionality

The Switch extends the functionality of the standard IEEE 802.1X. An overview of the extended functionality is given below.

(1) Authentication mode

IEEE 802.1X of the Switch has three basic authentication modes and authentication submodes. The basic authentication modes indicate the units for authentication control, while the submode specifies the terminal connection mode in the unit of authentication.

The supported basic authentication modes of the Switch (the authentication modes) are the following:

- Port-based authentication (static)

  Registers the MAC address of a successfully authenticated terminal in the MAC address table and allows access to the VLAN designated by the configuration for communication.

- Port-based authentication (dynamic)

  Registers the MAC address of a successfully authenticated terminal in the MAC VLAN and MAC address table. Terminals are given access to different VLANs before and after authentication.

- VLAN-based authentication (dynamic)

  Performs VLAN switching via the MAC VLAN and enables terminals to access different VLANs before and after authentication.

(2) Supported functionality by authentication mode

The following table lists the supported functionality of each authentication mode.

Table 6-3 Supported functionality by authentication mode

Functionality		**Port-based authentication (static)**	**Port-based authentication (dynamic)**	**VLAN-based authentication (dynamic)**
Switch default: Local authentication		N	N	N
Switch default: RADIUS authentication	External server ● IEEE 802.1X authentication RADIUS server information ● General-use RADIUS server information	Y See *5.3.1*. See *6.7*. See *7.2.1*.	Y See *5.3.1*. See *6.7*. See *7.2.1*.	Y See *5.3.1*. See *6.7*. See *7.2.1*.
	VLAN (VLAN after authentication)	N	Y	Y
	Access control by quarantine (using `Filter-Id` of the `RADIUS` attribute)	Y See *6.2.3*.	N	N
	Forced authentication	Y See *6.2.2*.	Y See *6.3.2*.	Y See *6.4.2*.
	Authentication permission port configured	Y See *7.3.3*.	Y See *7.4.3*.	Y See *7.5.3*.
	Private trap	Y[#1] See *5.4.6*.	Y[#1] See *5.4.6*.	N
Authentication method list	External server ● RADIUS server group	Y See *5.3.1*. See *6.7*. See *7.2.1*.	Y See *5.3.1*. See *6.7*. See *7.2.1*.	N
	Port-based authentication	Y See *5.2.2*. See *5.2.3*.	Y See *5.2.2*. See *5.2.3*.	N
Authentication sub-modes	Single-terminal mode	Y See *6.2.1*.	Y See *6.3.1*.	N

Functionality			Port-based authentication (static)	Port-based authentication (dynamic)	VLAN-based authentication (dynamic)
	Terminal authentication mode		Y See *6.2.1*.	Y See *6.3.1*.	Y See *6.4.1*.
Authentication mode option	Terminal authentication exemption option		Y See *6.2.1*. See *7.3.2*.	Y See *6.3.1*. See *7.4.2*.	Y See *6.4.1*. See *7.5.2*.
	Default authentication VLAN		N	N	Y See *7.5.2*.
Authentication	Switching terminal detection operation		Y See *6.2.2*.	Y See *6.3.2*.	Y See *6.4.2*.
		Sending an EAP-Request frame by multicast	Y See *7.3.2*.	Y See *7.4.2*.	Y See *7.5.2*.
		Sending an EAP-Request frame by unicast	Y See *7.3.2*.	Y See *7.4.2*.	N
		Stopping sending an EAP-Request frame	Y See *7.3.2*.	Y See *7.4.2*.	Y See *7.5.2*.
	Sending an EAP-Request/Identity frame to the terminal		Y See *6.2.2*. See *7.3.3*.	Y See *6.3.2*. See *7.4.3*.	Y See *6.4.2*. See *7.5.3*.
	Resending an EAP-Request frame to the terminal		Y See *6.2.2*. See *7.3.3*.	Y See *6.3.2*. See *7.4.3*.	Y See *6.4.2*. See *7.5.3*.
	Suppressing re-authentication requests from the terminals		Y See *6.2.2*. See *7.3.3*.	Y See *6.3.2*. See *7.4.3*.	Y See *6.4.2*. See *7.5.3*.
	Communication blocked state holding time when an authentication is requested by several terminals		Y[#2] See *6.2.1*. See *7.3.3*.	Y[#2] See *6.3.1*. See *7.4.3*.	N
	Wait time before authentication restarts in the event of authentication failure		Y See *6.2.2*. See *7.3.3*.	Y See *6.3.2*. See *7.4.3*.	Y See *6.4.2*. See *7.5.3*.

Functionality		Port-based authentication (static)	Port-based authentication (dynamic)	VLAN-based authentication (dynamic)
	Wait time for response from an authentication server	Y See *6.2.2*. See *7.3.3*.	Y See *6.3.2*. See *7.4.3*.	Y See *6.4.2*. See *7.5.3*.
	Pre-authentication pass (IPv4 access list for authentication)	Y See *5.4.1*. See *5.5.2*.	Y See *5.4.1*. See *5.5.2*.	N
Authentication status cleared	Canceling authentication for a terminal that does not respond to an authentication request	Y See *6.2.2*. See *7.3.3*.	Y See *6.3.2*. See *7.4.3*.	Y See *6.4.2*. See *7.5.3*.
	Monitoring for authenticated terminal non-communication	Y#3 See *6.2.2*. See *7.3.3*.	Y See *6.3.2*. See *7.4.3*.	N
	Monitoring for MAC address table aging	Y#4 See *6.2.2*. See *7.3.3*.	N#5	Y See *6.4.2*. See *7.5.3*.
	Authenticated terminal connection port link-down	Y See *6.2.2*.	Y See *6.3.2*.	Y See *6.4.2*.
	VLAN configuration change	Y See *6.2.2*.	Y See *6.3.2*.	Y See *6.4.2*.
	Operation commands	Y See *6.2.2*.	Y See *6.3.2*.	Y See *6.4.2*.
EAPOL forwarding		Common to all modes. See *6.5*.		
Account logs	Account log built in the Switch	2100 lines (combining all modes). See *6.6*.		
	RADIUS server account functionality	Common to all modes See *5.3.4*. See *6.6*. See *7.2.2*.		

Legend:

Y: Supported

N: Not supported

See *5.x.x*: See the relevant section in *5. Overview of Layer 2 Authentication*.

See *6.x.x*: See the relevant section in this chapter.

See *7.x.x*: See the relevant section in *7. IEEE 802.1X Configuration and Operation.*

#1

A private trap can be issued when forced authentication common to all authentication modes is set.

#2

The Switch applies only the single-terminal mode of port-based authentication (static) and port-based authentication (dynamic).

#3

Targets terminals requesting full access permission (authenticated and out-of-quarantine).

#4

Targets terminals requesting limited access permission (under quarantine).

#5

When the first step terminal is successfully authenticated by IEEE 802.1X in multistep authentication, an authentication entry are monitored by using MAC address table aging. For details, see *12. Multistep authentication.*

Table 6-4 Operational conditions of IEEE 802.1X

Type		Port setting	Specifiable VLAN type	Frame type	Port-based authentication (static)	Port-based authentication (dynamic)	VLAN-based authentication (dynamic)
Port type	Access port	native	Port VLAN MAC VLAN	Untagged	Y	N	N
	Trunk port	native	Port VLAN	Untagged	N	N	N
		allowed	Port VLAN MAC VLAN	Tagged	N	N	N
	Protocol port	--	--	--	N	N	N
	MAC Port	native	Port VLAN	Untagged	Y#	N	N
		mac	MAC VLAN	Untagged	N	Y	Y
		dot1q	Port VLAN MAC VLAN	Tagged	N	N	N

Type		Port setting	Specifiable VLAN type	Frame type	Port-based authentication (static)	Port-based authentication (dynamic)	VLAN-based authentication (dynamic)
Default VLAN					Y	N	N
Interface Type	fastethernet				Y	Y	Y
	gigabitethernet				Y	Y	Y
	port channel				Y	N	Y

Legend:

Y: Supported

N: Not supported

--: Not applicable for authentication ports

#

For details, see *5.4.4 Auto authentication mode accommodation on the same MAC port.*

IEEE 802.1X as implemented on the Switch treats a channel group as a single aggregate port. In describing this functionality, the term *port* includes normal ports and channel groups.

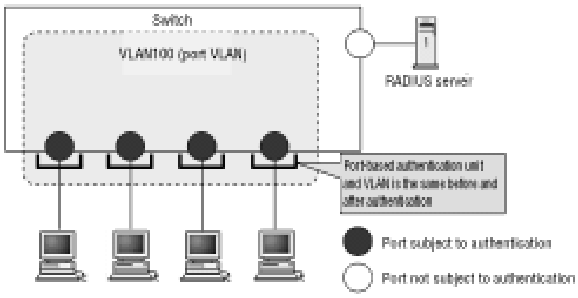
The following sections provide an overview of port-based authentication (static), port-based authentication (dynamic), and VLAN-based authentication (dynamic) in turn. For the same functionality and operation in authentication modes, see the relevant cross-references. (See....)

6.2 Port-based authentication (static)

In port-based authentication mode, IEEE 802.1X controls authentication at the physical port or channel group level. This is the default mode for IEEE 802.1X. This authentication mode does not support EAPOL frames with the IEEE 802.1Q VLAN tag. When this mode receives an EAPOL frame with the IEEE 802.1Q VLAN tag, it discards the frame.

The figure below shows a configuration using port-based authentication (static).

Figure 6-3 Configuration example of port-based authentication (static)



Prior to authentication, a terminal cannot start communication until it is successfully authenticated. The terminal can communicate once the terminal is successfully authenticated by port-based authentication (static), and after the terminal's MAC address and VLAN are registered in the MAC address table as an IEEE 802.1X port-based authentication entry. (Entries registered in the MAC address table can be confirmed by using the `show mac-address-table` operation command.)

6.2.1 Authentication submodes and the authentication mode options

IEEE 802.1X of the Switch has authentication modes and authentication submodes. The authentication modes indicate the unit for authentication control, while the submodes specify the terminal connection mode in the authentication unit. In addition, authentication mode options configurable in each mode are provided.

The table below shows the relationship among authentication modes, authentication submodes, and the authentication mode options.

Table 6-5 Relationship between the authentication submodes and the authentication mode options

Authentication mode	Authentication sub-modes	Authentication mode options
Port-based authentication (static)	Single-terminal mode	--
	Terminal authentication mode	Terminal authentication exemption option

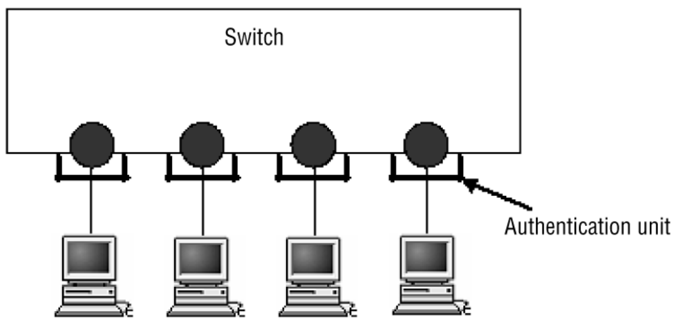
(1) Authentication submodes

Port-based authentication (static) provides the single-terminal mode and terminal authentication mode. The default is the single-terminal mode. You can use the terminal authentication mode by using the `dot1x multiple-authentication` configuration command.

(a) Single-terminal mode

In single-terminal mode, only one terminal can be authenticated at a given authentication unit. This is the default mode. If an EAP is received from another terminal while a first terminal is authenticated, the port of the terminal returns to unauthenticated status, and authentication restarts after the time specified by the `dot1x timeout keep-unauth` configuration command.

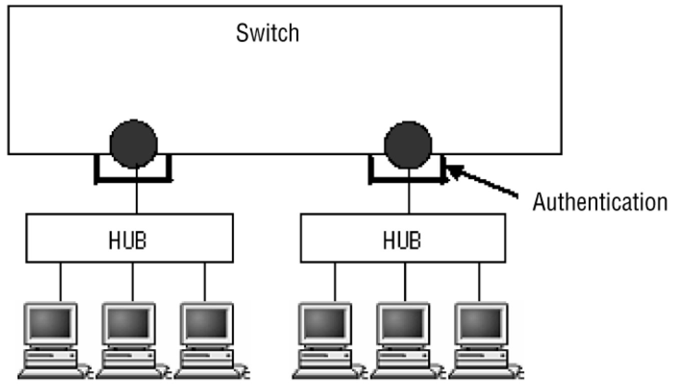
Figure 6-4 Single mode configuration



(b) Terminal authentication mode

Terminal authentication mode allows you to attach multiple terminals to a single authentication unit, but requires that each terminal (identified by sender MAC address) be authenticated. If an EAP is received from another terminal while the first terminal is authenticated, authentication is individually started with the terminal that sent the EAP.

Figure 6-5 Terminal authentication mode configuration



(2) Authentication mode options

(c) Terminal authentication exemption option

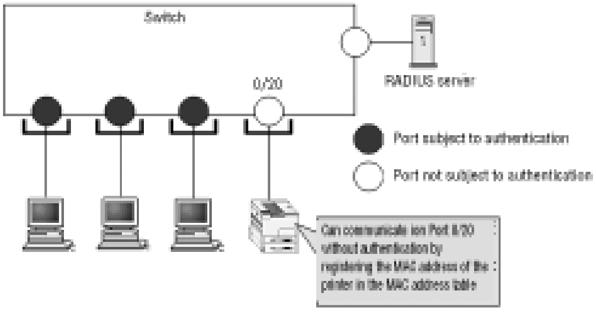
This option permits communication without authentication for terminals where the MAC address has been configured by using the static MAC address learning functionality.# You can use this option to authorize devices such as printers that cannot operate as a supplicant, and specific terminals such as servers that do not need to be authenticated. This option is available only in terminal authentication mode.

#

You can configure a MAC address in the MAC address table by using the `mac-address-table static` configuration command.

The figure below shows an example of a configuration for terminal authentication exemption with port-based authentication (static).

Figure 6-6 Example of a configuration that has an excluded terminal with port-based authentication (static)



6.2.2 Authentication functionality

(1) Trigger for authentication

Authentication starts when the Switch receives EAPOL-Start from a port subject to port-based authentication (static).

(2) Sending an EAP-Request/Identity frame

You can use the `dot1x timeout tx-period` configuration command to set a time interval at which EAP-Request/Identity is sent regularly from the Switch, thereby triggering the start of port-based authentication (static), to a terminal that will not start port-based authentication (static) by itself.

(3) Terminal detection behavior switching option

The Switch multicasts EAP-Request/Identity at intervals specified in the configuration to trigger the start of authentication of a terminal. When the authentication submode is the terminal authentication mode, there might be several terminals in an authentication unit. Because of this, the Switch continues to send EAP-Request/Identity by default until authentication of all terminals is completed.

As the number of terminals in an authentication unit increases, the authentication processing required for every terminal that responds to the EAP-Request/Identity request might put a heavy load on the Switch. To reduce this load, you can apply an abbreviated authentication sequence to authenticated terminals that respond to such requests.

However, depending on the supplicant software that the terminal uses, omitting the authentication sequence might result in a loss of communication with the authenticated terminal. For this reason, the Switch provides an option that lets you choose the behavior with regard to authenticated terminals. This option allows you to make a selection by using the `dot1x supplicant-detection` configuration command, and allows you to specify any of the three actions shown below.

Table 6-6 Types of terminal detection action switching options

Option type	Timing of sending EAP-Request/Identity frame for terminal detection	Omitting authentication sequence	Authentication start frame
shortcut	Sends the frame on a multicast basis regularly	Omitted	● Response to multicast sending of EAP-Request/Identity (EAP-Response/Identity) received ● EAPOL-Start received#
auto	Sends the frame on a unicast basis when receiving an ARP/IP frame from a new terminal	Not omitted	● When an ARP/IP frame is received from a new terminal ● EAPOL-Start received#
disable	Stops sending	Not omitted	● EAPOL-Start received

#

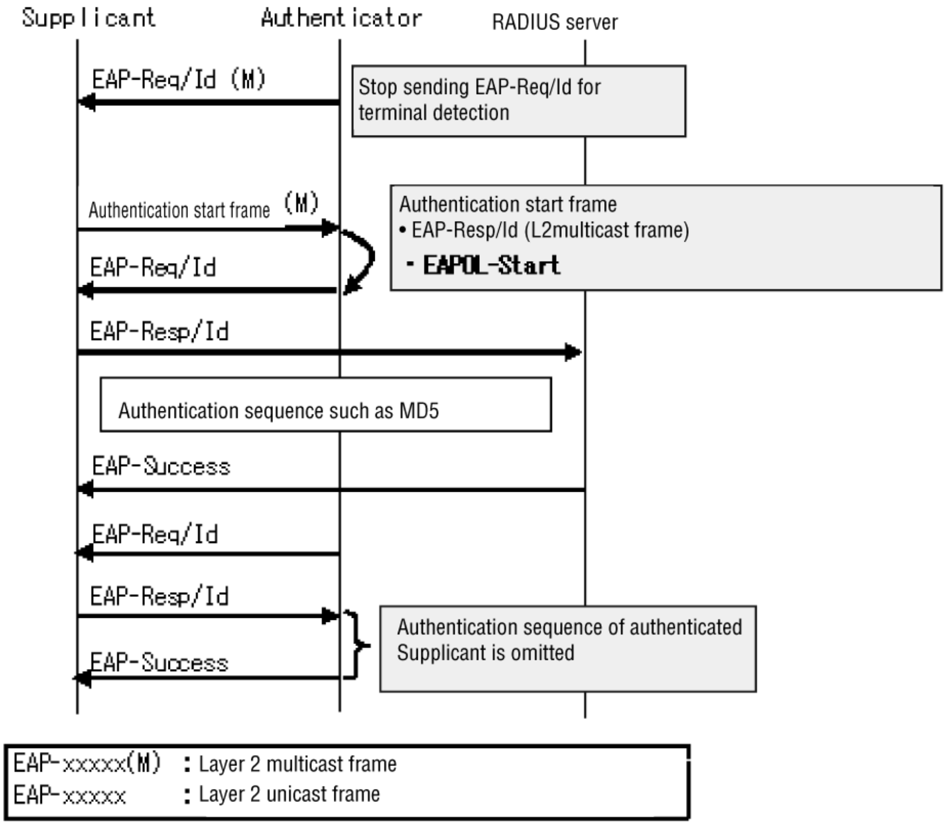
If the functionality to suppress a re-authentication request from the terminal is disabled, the Switch starts an authentication sequence when it receives EAPOL-Start.

The terminal detection action switching option is effective only in terminal authentication mode.

(a) shortcut

To reduce the load on the Switch, authenticated terminals that respond to an EAP-Request/Identity packet do not participate in a full authentication sequence. Depending on the type of supplicant software, this might cause the Switch to lose communication with the authenticated terminal. In this case, if the Supplicant software to be used can send EAPOL-Start by itself, specify `disable`.

Figure 6-7 EAP-Request/Identity sequence when a shortcut is used

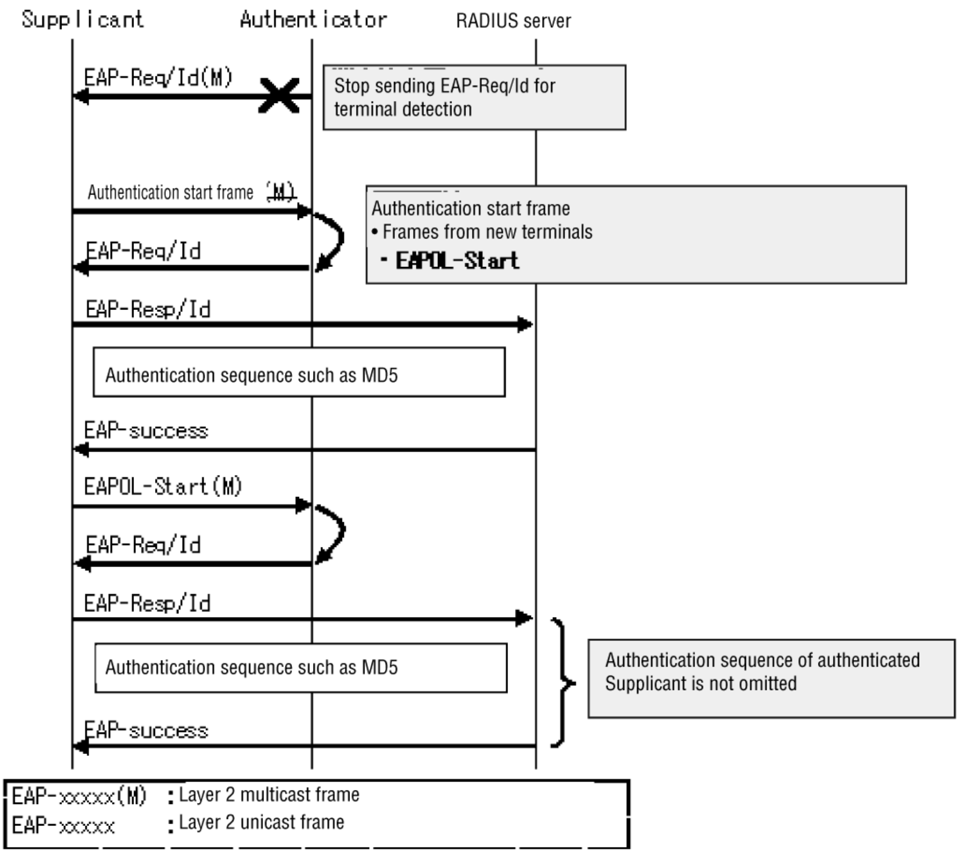


(b) auto

In this mode, terminals are not detected by the transmission of an EAP-Request/Identity message to the multicast address. An unauthenticated terminal is detected by reception of any frame sent from the terminal, and authentication is started by sending EAP-Request/Identity from a unicast address to each terminal.

Because the EAP-Request/Identity message is not sent to the multicast address, authenticated terminals are never prompted to begin an authentication sequence.

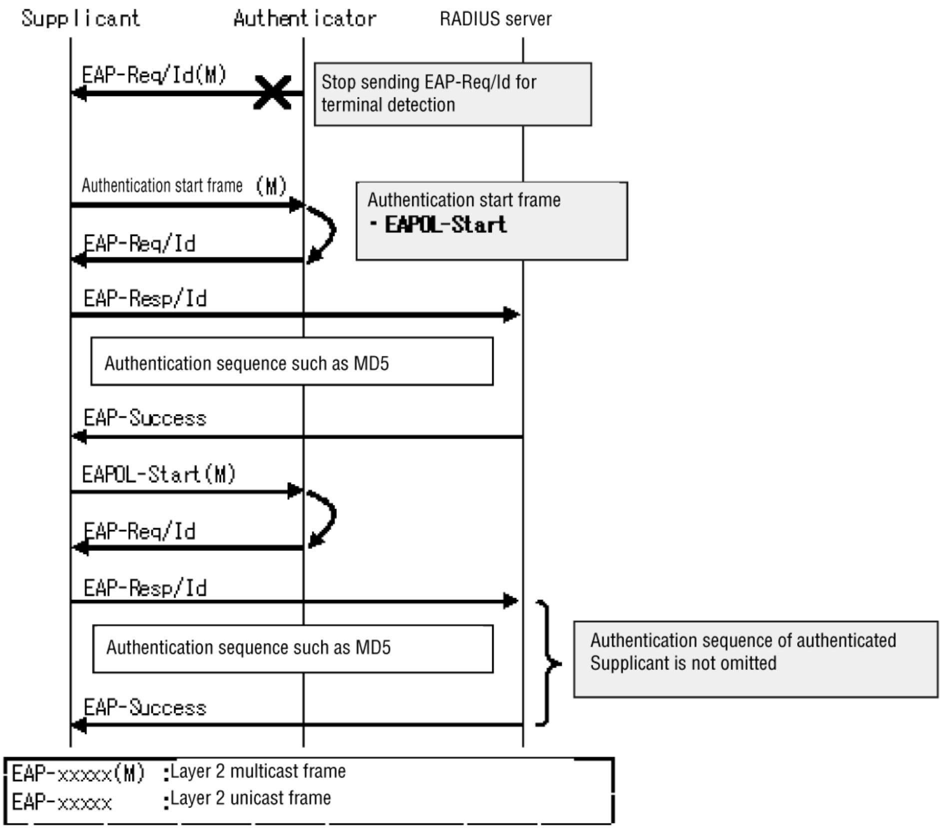
Figure 6-8 EAP-Request/Identity sequence when auto is used



(c) disable

If a terminal is detected on the port, transmission of an EAP-Request/Identity packet to trigger the start of authentication of terminals stops. An authentication sequence starts when EAPOL-Start is received from the terminal.

Figure 6-9 EAP-Request/Identity sequence when disable is used



When this mode is used with Supplicant software that does not send EAPOL-Start voluntarily, authentication will not start because the timing of the start authentication is lost. Windows-standard Supplicant software does not send EAPOL-Start voluntarily. However, it can do this by changing a registry value, `SupplicantMode`. For details about the registry, see the Microsoft website and associated documentation. Exercise caution when editing the registry, as changing the wrong registry entry might prevent Windows from starting. We recommend that you back up the registry before making any changes.

(4) Resending an EAP-Request frame to the terminal

This process specifies how long the Switch should wait for a terminal to respond to an EAP-Request frame before resending the request, and the maximum number of times that the Switch resends the request.

You can use the `dot1x timeout supp-timeout` configuration command to set the period until resending, and can use the `dot1x max-req` configuration command to set the resend count.

(5) Functionality to suppress authentication requests from the terminals

(a) Suppressing re-authentication requests from the terminals

This functionality suppresses authentication that is started by EAPOL-Start sent from a terminal. When re-authentication requests are received at short intervals from many terminals, this functionality prevents the load on the Switch from increasing by stopping the sending of EAP-Request/Identity.

You can configure this functionality by using the `dot1x re-authentication` and `dot1x ignore-eapol-start` configuration commands.

After configuring the functionality, re-authentication for the terminal is executed by sending EAP-Request/Identity from the Switch at an interval specified with either of the following configuration commands:

- `dot1x timeout tx-period`
- `dot1x timeout reauth-period`

(b) Communication interruption when authentication requests are received from several terminals

If authentication requests from several terminals are detected at a port where single-terminal mode port-based authentication works, you can configure a time for interrupting communication with the target port.

You can use the `dot1x timeout keep-unauth` configuration command to set the communication interruption period.

(6) Wait time before authentication restarts in the event of authentication failure

You can use the `dot1x timeout quiet-period` configuration command to configure the wait time before the restart of authentication for a terminal that was unsuccessfully authenticated.

(7) Wait time for response from an authentication server

You can use the `dot1x timeout server-timeout` configuration command to configure the wait time for a response to a request from an authentication server. When the specified time has elapsed, the Switch notifies the supplicant that authentication has failed. Comparing the time with the total time, including resending configured with the `radius-server` configuration command, the Switch notifies the Supplicant of the authentication failure based on the time that is shorter.

(8) Specifying a forced authentication port

When a terminal connected to a port for which forced authentication is specified undergoes RADIUS authentication, and sending a request to the RADIUS server fails due to a line failure or the RADIUS does not respond, the terminal becomes authenticated.

In the Switch, the configuration for forced authentication can shared among all authentication methods or specified separately per authentication method. For details about shared authentication configuration, see *5.4.6 Forced authentication common to all authentication modes.*

Use the `dot1x force-authorized` configuration command for a port where forced authentication is to be permitted. Also, use the `dot1x force-authorized eapol` configuration command to send an EAP-Success response to the terminal where forced authentication is permitted.

Forced authentication is successful when the following conditions are met.

Table 6-7 Conditions for successful forced authentication

Item	Condition
Configuration	All the following configurations have been set: ● `aaa authentication dot1x`[#1] ● `dot1x radius-server host` or `radius-server host` ● `dot1x system-auth-control` ● `dot1x port-control auto`[#2] ● `dot1x force-authorized`[#2] ● `switchport mode access`[#2] ● `dot1x authentication`[#3]
Account log	The following account log is collected when an authentication request is sent to the RADIUS server: ● `No=82` `WARNING:SYSTEM: (`*<Additional information>*`) Failed to connect to RADIUS server.` *<Additional information>*`:IP` You can use the `show dot1x logging` command to check the account log.

#1

When forced authentication is used as the Switch default, set `default group radius`.

When using port-based authentication, set *<list-name>* `group` *<group-name>*.

#2

Configure the same port.

#3

Specify this when using port-based authentication.

The authentication status of a terminal where authentication is permitted by forced authentication is canceled in the same way as for a normally authenticated terminal, as described in *(9) Authentication status cleared* in *6.2.2 Authentication functionality*.

Furthermore, all operations from the start of requesting authentication to the RADIUS server to successful forced authentication are the same, whether forced authentication common to all authentication modesor forced authentication based on individual authentications is used. For details about the operations, see *(1) Behavior from the start of an RADIUS authentication request to permission for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

All EAPOL frames sent from terminals that went through forced authentication are discarded before the next re-authentication time.

(9) Authentication status cleared

The following methods of canceling authentication are provided in port-based authentication (static).

- Canceling authentication for a terminal that does not respond to an authentication request
- Canceling authentication by monitoring the non-communication state of

authenticated terminals

- Canceling authentication by monitoring MAC address table aging for a terminal in quarantine status
- Canceling authentication of terminals connected to link-down ports
- Canceling authentication resulting from changes to the VLAN configuration
- Canceling authentication using an operation command

(a) Canceling authentication for a terminal that does not respond to an authentication request

Because the authentication of a terminal that is removed from the network after authentication cannot be canceled from the Switch, re-authentication is requested from authenticated terminals. If no response is received, the authentication of the terminal is canceled.

For the target port, use the `dot1x reauthentication` configuration command to request re-authentication, and then use the `dot1x timeout reauth-period` configuration command to configure the re-authentication interval.

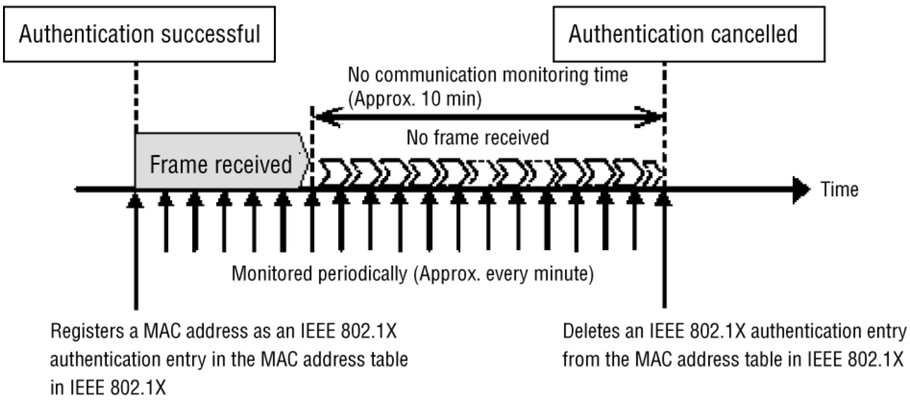
(b) Canceling authentication by monitoring the non-communication state of authenticated terminals

This functionality targets quarantined terminals and authenticated terminals.

This functionality automatically cancels the authentication of an authenticated terminal if the terminal remains in a non-communication status for a certain period of time.

This functionality monitors the IEEE 802.1X authentication entries in the MAC address table periodically (approx. every minute) and checks whether a frame has been received from an authenticated terminal registered with IEEE 802.1X. If no frame is detected from a target terminal for a certain period of time (approximately 10 minutes), it deletes the target IEEE 802.1X authentication entry from the MAC address table and cancels authentication.

Figure 6-10 Overview of non-communication monitoring of authenticated terminals



Non-communication monitoring is enabled for authenticated terminals when the following condition is met:

- IEEE 802.1X port-based authentication (static) or port-based authentication (dynamic) is enabled and `dot1x auto-logout` is enabled.

You can use the `no dot1x auto-logout` configuration command to stop this functionality from canceling authentication automatically.

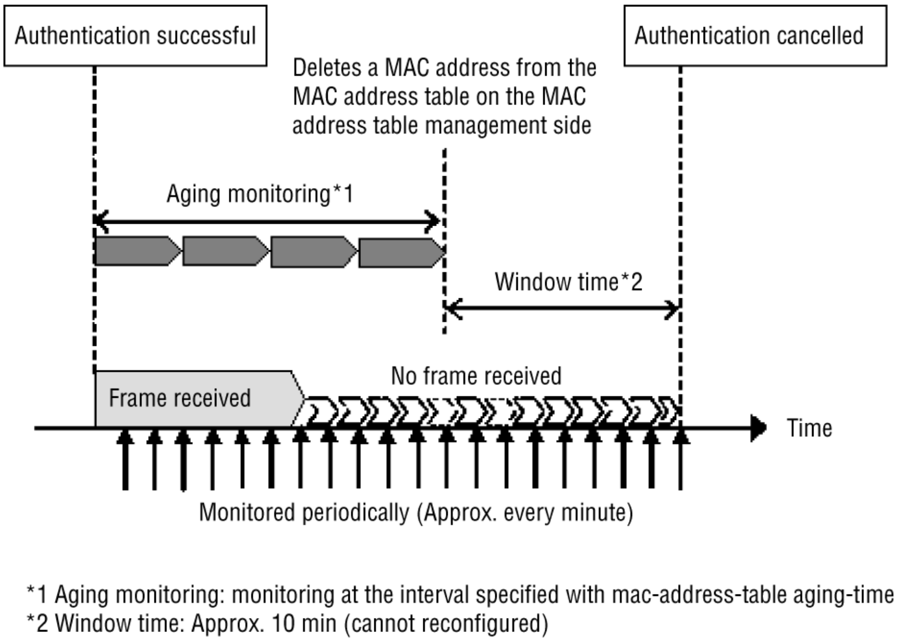
(c) Canceling authentication by monitoring MAC address table aging for a terminal in quarantine status

This functionality targets a registered terminal in quarantine status when terminals are authenticated with port-based authentication (static). (For details about the quarantine status, see *6.2.3 Collaboration with the NAP quarantine system*.)

This functionality monitors the dynamic entries from terminals into the MAC address table periodically (approx. every one minute) and checks whether the MAC address of a terminal is old or not. The quarantine status of a terminal is automatically canceled if its MAC address is deleted from the MAC address due to a timeout.

However, to prevent cancellation due to an effect such as an instantaneous interruption of a line, this functionality cancels the quarantine status if a MAC address is not registered into the MAC address table for approx. 10 minutes (time before cancellation) after the MAC address is deleted from the MAC address table.

Figure 6-11 Overview of canceling authentication by monitoring MAC address table aging



This functionality is enabled when the following conditions are met:

- IEEE 802.1X port-based authentication (static) is enabled, and `dot1x auto-logout` is enabled.
- The target terminal is in quarantine status

You can use the `no dot1x auto-logout` configuration command to keep this functionality from canceling authentication automatically even when an aging timeout occurs.

(d) Canceling authentication of terminals connected to link-down ports

This functionality automatically cancels authentication for an authenticated terminal if it detects a link-down at a port connected to the authenticated terminal.

(e) Canceling authentication resulting from changes to the VLAN configuration

If you use configuration commands to change the configuration of a VLAN that includes authenticated terminals, the Switch clears the authentication status of terminals associated with that VLAN.

The following configuration changes trigger a logout:

- Deletion of a VLAN
- Suspension of a VLAN

(f) Canceling authentication using an operation command

You can use the `clear dot1x auth-state` command to manually cancel authentication of a terminal subject to IEEE 802.1X authentication.

6.2.3 Collaboration with the NAP quarantine system

The Network Access Protection (NAP) quarantine system examines system normality of terminals while they are not yet connected to the network, and restricts network access by terminals that do not conform to a security policy.

In the NAP quarantine system, a device that monitors the security status of terminals is called a *network policy server* (NPS), and a terminal that is monitored is called a *NAP client*. The Switch is positioned between the NPS and NAP clients.

(1) Operational overview

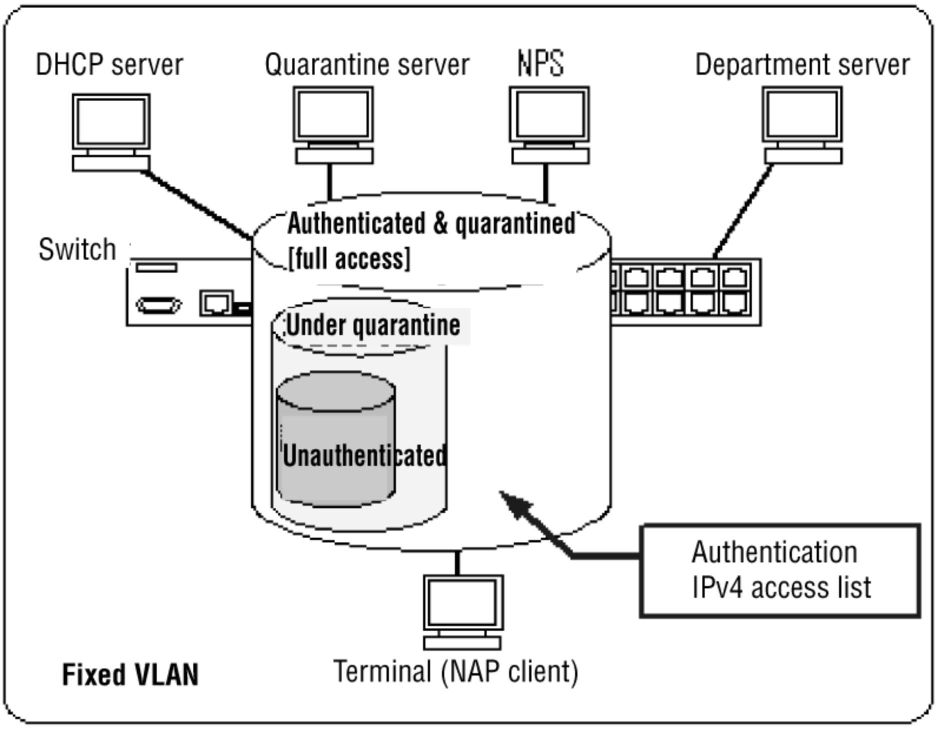
The Switch can work with the NAP quarantine system with port-based authentication (static). Because port-based authentication (static) does not automatically switch VLANs, the NPS monitors the NAP client in any of the following statuses and reports its status to the Switch.

- Before authentication
- Under quarantine
- After authentication and out of quarantine

The Switch only permits full-access communication to a NAP client that conforms to the security policy (authenticated and quarantined terminals) based on information sent from the NPS.

The figure below shows the overview of collaboration with the NAP quarantine system in port-based authentication (static).

Figure 6-12 Overview of collaboration with the NAP quarantine system in port-based authentication (static)



The Switch controls access to the terminal based on `Filter-Id` included in the `Access-Accept` attribute as a response from the RADIUS server (corresponds to the NPS in the figure above). An authentication IPv4 access list has been configured for `Filter-Id`.

The figure below shows actions of the Switch based on the response from the RADIUS server.

Table 6-8 Actions of the Switch based on the response from the RADIUS server (NPS)

In RADIUS server				Action of the Switch		Access
Authentication result	**Quarantine result**	**RADIUS response**	**Contents of the attribute Filter-Id**	**Registration into the MAC address table**	**Sent to the terminal**	
Not OK	--	Reject	--	Not implemented	EAPoL-Failure	This is the same as for standard authentication
OK	Not OK	Accept	Filter-Id = authentication ACL	Not implemented	EAPoL-Success	Restricted access under quarantine status (Range of authentication

In RADIUS server				Action of the Switch		Access
Authentication result	Quarantine result	RADIUS response	Contents of the attribute Filter-Id	Registration into the MAC address table	Sent to the terminal	
						ACL)
OK	OK	Accept	Filter-Id = 0 or no Filter-Id	Implemented	EAPoL-Success	Full access permission with an authenticated and out-of-quarantine status (Limitation canceled)

Legend:

ACL for authentication: authentication IPv4 access list

--: Not applicable because this is the same as for normal failure

Configure access permission to an quarantine server for the Switch using the authentication IPv4 access list, while configuring the name of the authentication IPv4 access list to `Filter-Id` of the `Access-Accept` attribute of a RADIUS server.

For details about RADIUS server attributes, see *6.7 Preparation.*

(2) Displaying "under quarantine" and "authenticated and out-of-quarantine" statuses for a terminal

In collaboration with the NAP quarantine system, "under quarantine" (permitting limited access) and "authenticated and out-of-quarantine" (permitting full access) statuses occur. Check these statuses through the authentication substatus of the `show dot1x` command. For details, see the operation command reference.

Table 6-9 Status displayed by IEEE 802.1X

Authentication result	Quarantine result	Displayed by the operation command `show dot1x`		Remarks
		AuthState Authentication status of the terminal	Substatus Authentication substatus	
Not OK	--	Other than authentication completed	No authentication sub status because authentication is not completed	Before authentication
OK	Not OK	Authentication complete	Permitting limited access	Under quarantine
OK	OK	Authentication complete	Permitting full access	Authenticated and out of quarantine

Legend:

--: Not applicable because this is the same as for normal failure.

(3) Configuration to enable this functionality

No special configuration to enable collaboration with the NAP quarantine system is provided. Configure the settings necessary for IEEE 802.1X port-based authentication (static). In addition, configure access permission for a quarantine server to the authentication IPv4 access list.

- Port-based authentication (static) configuration: See *7.3 Configuring port-based authentication (static)*.
- Authentication IPv4 access list configuration: See *5.5.2 Configuring the authentication IPv4 access list.*

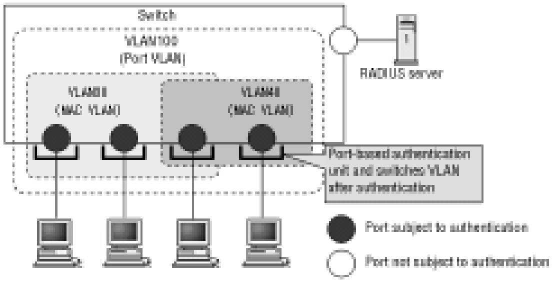
6.3 Port-based authentication (dynamic)

In Port-based authentication (dynamic), authentication is controlled for a physical port belonging to a MAC VLAN. This authentication mode does not support EAPOL frames with the IEEE 802.1Q VLAN tag. When this mode receives an EAPOL frame with the IEEE 802.1Q VLAN tag, it discards the frame.

When a terminal is successfully authenticated, the Switch dynamically switches VLANs based on the VLAN information (the VLAN ID of a MAC VLAN) received from the RADIUS server.

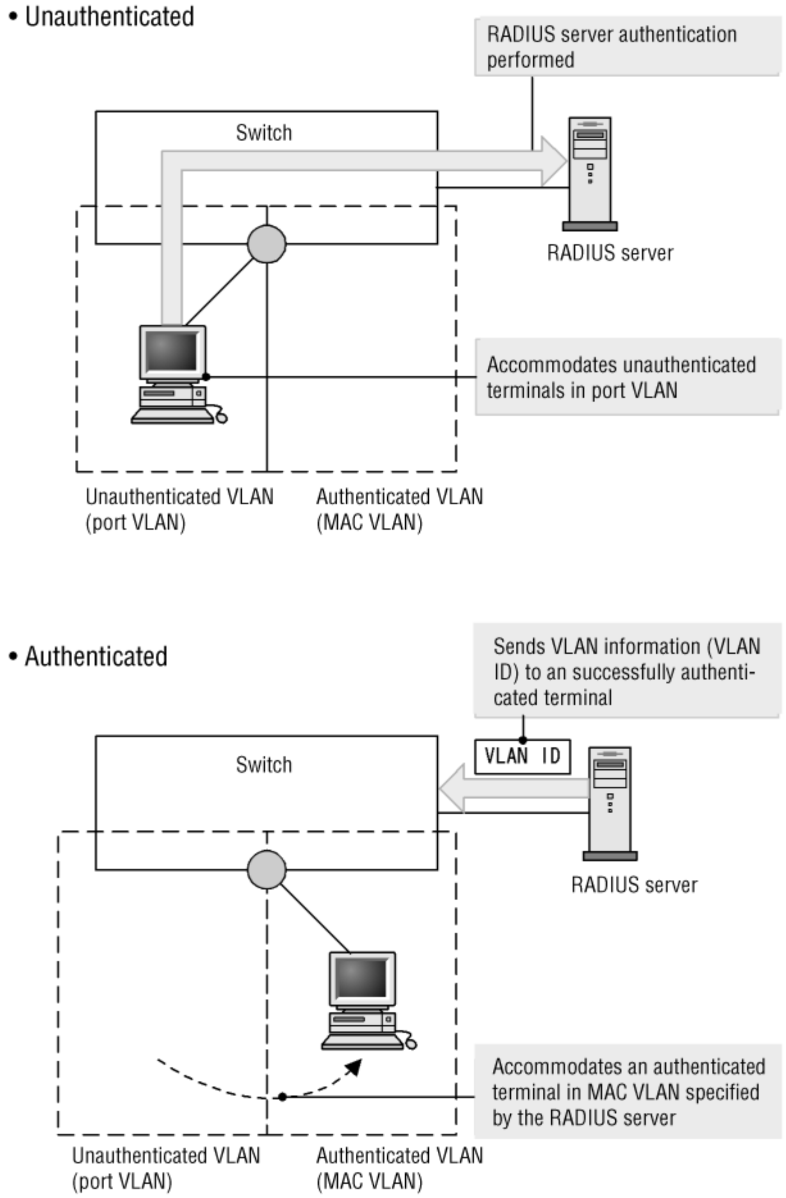
The figure below shows an example of a port-based authentication (dynamic) configuration.

Figure 6-13 Configuration example of port-based authentication (dynamic)



Prior to authentication, a terminal cannot start communication until it is successfully authenticated. If successfully authenticated with port-based authentication (dynamic), the MAC address of a successfully authenticated terminal and its VLAN ID after authentication are registered in the MAC VLAN and MAC address table as IEEE 802.1X port-based authentication entries and communication is enabled. (Entries registered in the MAC address table can be confirmed by using the `show mac-address-table` operation command.)

Figure 6-14 Operational image of port-based authentication (dynamic)



When communicating with a pre-authentication VLAN, configure an authentication IPv4 access list.

6.3.1 Authentication submode and the authentication mode options

IEEE 802.1X of the Switch has authentication modes and authentication submodes. The authentication modes indicate the unit for authentication control, while the submodes specify the terminal connection mode in the authentication unit. In addition, authentication mode options configurable in each mode are provided.

The table below shows the relationship among authentication modes, authentication submodes, and the authentication mode options.

Table 6-10 Relationship between the authentication submodes and the authentication mode options

Authentication mode	Authentication submode	Authentication mode option
Port-based authentication (dynamic)	Single-terminal mode	--
	Terminal authentication mode	Terminal authentication exemption option

(1) Authentication submodes

This procedure is the same as for port-based authentication (static). See *(1) Authentication submodes* in *6.2.1 Authentication submodes and the authentication mode options.*

(2) Authentication mode options

(a) Terminal authentication exemption option

This option permits communication without authentication for terminals where the MAC address has been configured by using the static MAC address learning functionality#1 and the MAC VLAN functionality#2. You can use this option to authorize devices such as printers that cannot operate as a supplicant, and specific terminals such as servers that do not need to be authenticated. This option is available only in terminal authentication mode.

#1

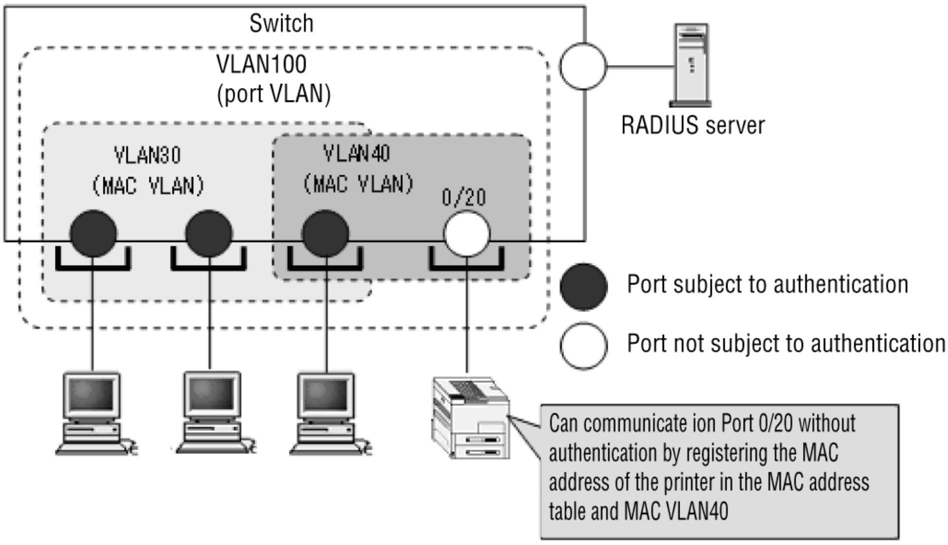
You can configure a MAC address in the MAC address table by using the `mac-address-table static` configuration command.

#2

You can configure a MAC address of a MAC VLAN by using the `mac-address` configuration command.

The figure below shows an example of a configuration for terminal authentication exemption in port-based authentication (dynamic).

Figure 6-15 Example of a configuration that has an excluded terminal with port-based authentication (dynamic)



6.3.2 Authentication type

(1) Trigger for authentication

Authentication starts when the Switch receives EAPOL-Start from a port subject to port-based authentication (dynamic).

(2) Sending an EAP-Request/Identity frame

This procedure is the same as for port-based authentication (static). For details, see *(2) Sending an EAP-Request/Identity frame* in *6.2.2 Authentication functionality.*

(3) Terminal detection behavior switching option

This procedure is the same as for port-based authentication (static). For details, see *(3) Terminal detection behavior switching option* in *6.2.2 Authentication functionality.*

(4) Resending an EAP-Request frame to the terminal

This procedure is the same as for port-based authentication (static). For details see *(4) Resending an EAP-Request frame to the terminal* in *6.2.2 Authentication functionality.*

(5) Functionality to control authentication requests from the terminals

This procedure is the same as for port-based authentication (static). For details see *(5) Functionality to suppress authentication requests from the terminals* in *6.2.2 Authentication functionality.*

(6) Wait time before authentication restarts in the event of authentication failure

This procedure is the same as for port-based authentication (static). For details, see *(6) Wait time before authentication restarts in the event of authentication failure* in *6.2.2 Authentication functionality.*

(7) Wait time for response from an authentication server

This procedure is the same as for port-based authentication (static). For details, see *(7) Wait time for response from an authentication server* in *6.2.2 Authentication functionality.*

(8) Specifying a forced authentication port

When a terminal connected to a port for which forced authentication is specified undergoes RADIUS authentication, and sending a request to the RADIUS server fails due to a line failure or the RADIUS does not respond, the terminal becomes authenticated.

In the Switch, the configuration for forced authentication can shared among all authentication methods or specified separately per authentication method. For details about shared authentication configuration, see *5.4.6 Forced authentication common to all authentication modes.*

Use the `dot1x force-authorized vlan` configuration command for a port where forced authentication is to be permitted. Also, use the `dot1x force-authorized eapol` configuration command to send an EAP-Success response to the terminal where forced authentication is permitted.

Forced authentication is successful when the following conditions are met.

Table 6-11 Conditions for successful forced authentication

Item	Conditions
Configuration	All the following configurations have been set: ● `aaa authentication dot1x`#1 ● `dot1x radius-server host` or `radius-server host` ● `dot1x system-auth-control` ● `dot1x force-authorized vlan`#2 ● `dot1x port-control auto`#3 ● `vlan` *<VLAN ID>* `mac-based`#2 ● `switchport mode mac-vlan`#3 ● `dot1x authentication`#4
Account log	The following account log is collected when an authentication request is sent to the RADIUS server: ● `No=82` `WARNING:SYSTEM: (`*<Additional information>*`) Failed to connect to RADIUS server.` *<Additional information>*`: IP` You can use the `show dot1x logging` command to check the account log.

#1

When forced authentication is used as the Switch default, set `default group radius`.

When using port-based authentication, set *<list-name>* `group` *<group-name>*.

#2

Set the same VLAN ID.

#3

Configure the same port.

#4

Specify this when using port-based authentication.

The authentication status of a terminal where authentication is permitted by forced authentication is canceled in the same way as for a normally authenticated terminal, as described in *(9) Authentication cancellation* in *6.3.2 Authentication type.*

Furthermore, all operations from the start of requesting authentication to the RADIUS server to successful forced authentication are the same, whether forced authentication common to all authentication modes or forced authentication based on individual authentications is used. For details about the operations, see *(1) Behavior from the start of an RADIUS authentication request to permission for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

All EAPOL frames sent from terminals that went through forced authentication are discarded before the next re-authentication time.

(9) Authentication cancellation

The following methods of canceling authentication are provided in port-based authentication (dynamic).

- Canceling authentication for a terminal that does not respond to an authentication request
- Canceling authentication by monitoring the non-communication state of authenticated terminals
- Canceling authentication of terminals connected to link-down ports
- Canceling authentication resulting from changes to the VLAN configuration
- Canceling authentication using an operation command

Each authentication cancellation is the same for port-based authentication (static). For details, see *(9) Authentication status cleared* in *6.2.2 Authentication functionality.*

6.4 VLAN-based authentication (dynamic)

In this mode, IEEE 802.1X controls authentication at the level of terminals associated with a MAC VLAN. The Switch cannot process EAPOL frames that use IEEE 802.1Q VLAN tagging. If such a frame is received, it is discarded.

The specified trunk port or access port in the MAC VLAN is treated as a non-authenticating port.

When a terminal is successfully authenticated, the Switch dynamically switches VLANs based on the VLAN information (the VLAN ID of a MAC VLAN) received from the RADIUS server. However, authentication fails if VLAN information received from the RADIUS server is not included in the authenticated VLAN settings (`dot1x vlan dynamic radius-vlan` configuration command) after VLAN-based authentication (dynamic).

The figures below describe an example of a configuration using VLAN-based authentication (dynamic), and illustrate its operation.

Figure 6-16 Configuration example using VLAN-based authentication (dynamic)

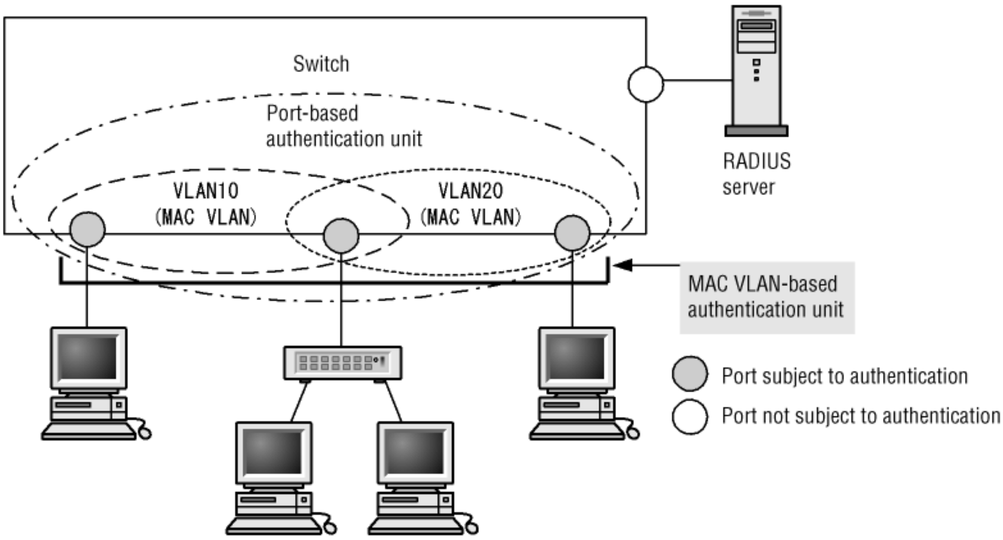
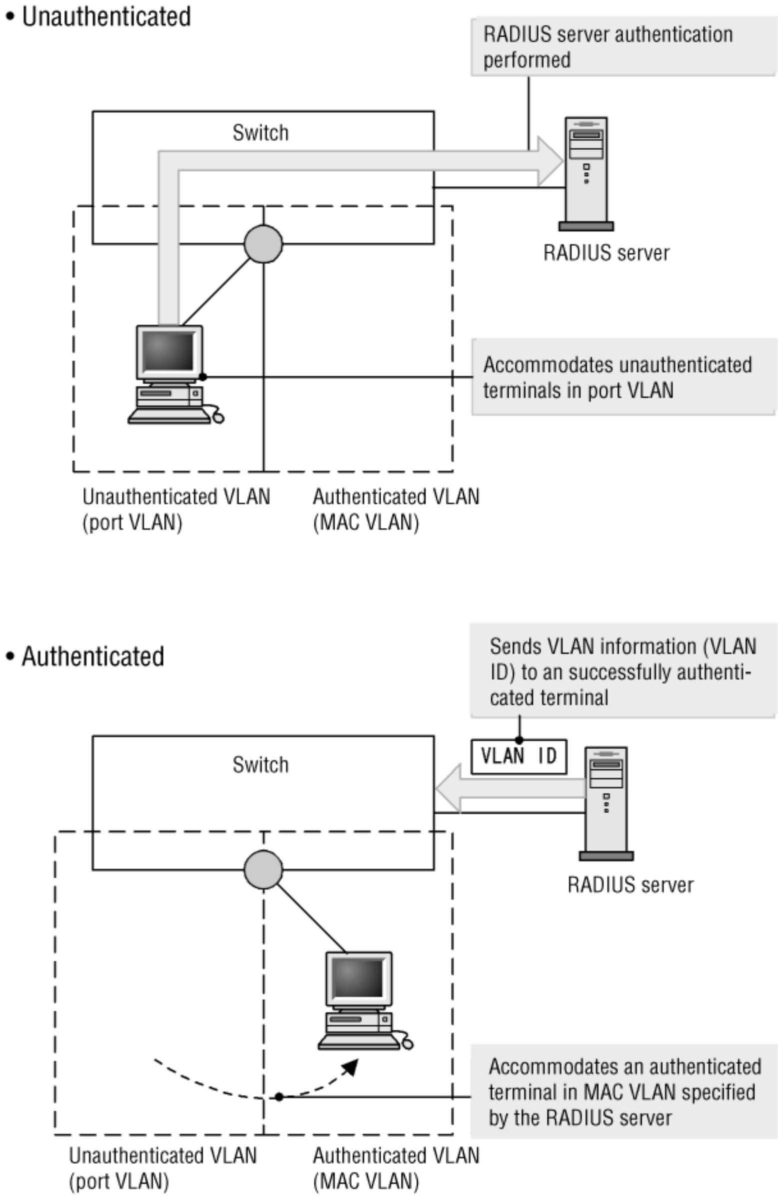


Figure 6-17 Operation of VLAN-based authentication (dynamic) authentication



6.4.1 Authentication submodes and authentication mode options

IEEE 802.1X of the Switch has authentication modes and authentication submodes. The authentication modes indicate the unit for authentication control, while the submodes specify the terminal connection mode in the authentication unit. In addition, authentication mode options configurable in each mode are provided.

The table below shows the relationship among authentication mode, authentication submode, and the authentication mode option.

Table 6-12 Relationship between the authentication submode and the authentication mode option

Authentication mode	Authentication submode	Authentication mode option
VLAN-based authentication (dynamic)	Terminal authentication mode	Terminal authentication exemption option
		Default authentication VLAN

(1) Authentication submodes

The only authentication submode of VLAN-based authentication (dynamic) is the terminal authentication mode.

(a) Terminal authentication mode

This procedure is the same as for port-based authentication (static). For details, see *(b) Terminal authentication mode* in *(1) Authentication submodes* in *6.2.1 Authentication submodes and the authentication mode options.*

(2) Authentication mode options

(a) Terminal authentication exemption option

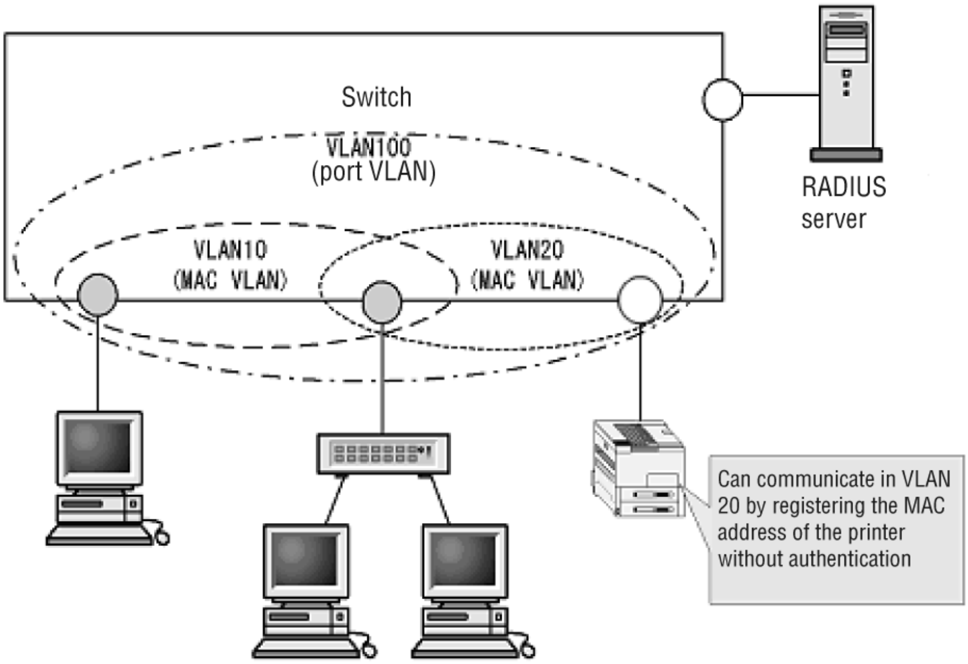
This option permits communication, eliminating the need for authentication for the terminal where a MAC address has been configured using the MAC VLAN functionality#. You can use this option to authorize devices such as printers that cannot operate as a supplicant, and specific terminals such as servers that do not need to be authenticated. This option is available only in terminal authentication mode.

#

You can configure a MAC address of a MAC VLAN by using the `mac-address` configuration command.

The figure below shows an example of configuration for terminal authentication exemption in VLAN-based authentication (dynamic).

Figure 6-18 Configuration example of terminal bypassing VLAN-based authentication (dynamic)



(b) Authentication default VLAN functionality

This functionality assigns a port-based VLAN to terminals that cannot obtain membership to a MAC VLAN due to a lack of IEEE 802.1X support or other circumstances. If a port-based VLAN or default VLAN is set up at a port configured for VLAN-based authentication (dynamic), that VLAN will serve as the authentication default VLAN. Terminals are attached to the authentication default VLAN in the following circumstances:

- The terminal does not support IEEE 802.1X authentication
- The terminal has not been authenticated by IEEE 802.1X
- The terminal fails authentication or re-authentication
- The VLAN ID returned by the RADIUS server does not correspond to a MAC VLAN
- If a VLAN ID specified by the RADIUS server has not been configured to a port

6.4.2 Authentication functionality

(1) Trigger for authentication

Authentication starts when the Switch receives EAPOL-Start from a port subject to VLAN-based authentication (dynamic).

(2) Sending an EAP-Request/Identity frame

You can use the `dot1x vlan dynamic timeout tx-period` configuration command to set a time interval at which EAP-Request/Identity is sent regularly from the Switch, thereby triggering the start of VLAN-based authentication (dynamic), to a terminal that will not start authentication by itself.

(3) Terminal detection behavior switching option

The Switch multicasts EAP-Request/Identity at intervals specified in the configuration to trigger the start of authentication of a terminal. When the authentication submode is the terminal authentication mode, there might be several terminals in an authentication unit. Because of this, the Switch continues to send EAP-Request/Identity by default until authentication of all terminals is completed.

As the number of terminals in an authentication unit increases, the authentication processing required for every terminal that responds to the EAP-Request/Identity request might put a heavy load on the Switch. To reduce this load, you can apply an abbreviated authentication sequence to authenticated terminals that respond to such requests.

However, depending on the supplicant software that the terminal uses, abbreviating the authentication sequence might result in a loss of communication with the authenticated terminal. For this reason, the Switch provides an option that lets you choose the behavior with regard to authenticated terminals. This option allows you to make a selection by using the `dot1x vlan dynamic supplicant-detection` configuration command and specifies either of the two actions shown below:

(a) shortcut

This procedure is the same as for port-based authentication (static). For details see *(a) shortcut* in *(3) Terminal detection behavior switching option* in *6.2.2 Authentication functionality.*

(b) disable

This procedure is the same as for port-based authentication (static). For details see *(c) disable* in *(3) Terminal detection behavior switching option* in *6.2.2 Authentication functionality.*

(4) Resending an EAP-Request frame to the terminal

This process specifies how long the Switch should wait for a terminal to respond to an EAP-Request frame before resending the request, and the maximum number of times that the Switch resends the request.

You can use the `dot1x vlan dynamic timeout supp-timeout` configuration command to set the period until resending, and can use the `dot1x vlan dynamic max-req` configuration command to set the resend count.

(5) Functionality to suppress authentication requests from the terminals

(a) Suppressing re-authentication requests from the terminals

This functionality suppresses authentication that is started by EAPOL-Start sent from a terminal. When re-authentication requests are received at short intervals from many terminals, this functionality prevents the load on the Switch from increasing by stopping the sending of EAP-Request/Identity.

You can configure this functionality by using the `dot1x vlan dynamic re-authentication` and `dot1x vlan dynamic ignore-eapol-start` configuration commands.

After configuring the functionality, re-authentication for the terminal is executed by sending EAP-Request/Identity from the Switch at an interval specified with either of the following configuration commands:

- `dot1x vlan dynamic timeout tx-period`
- `dot1x vlan dynamic timeout reauth-period`

(6) Wait time before authentication restarts in the event of authentication failure

You can use the `dot1x vlan dynamic timeout quiet-period` configuration command to configure the wait time before the restart of authentication for a terminal that was unsuccessfully authenticated.

(7) Wait time for response from an authentication server

You can use the `dot1vlan dynamic timeout server-timeout` configuration command to configure the wait time for a response to a request to an authentication server. When the specified time has elapsed, the Switch notifies the supplicant that authentication has failed. Comparing the time with the total time, including resending configured with the `radius-server` configuration command, the Switch notifies the Supplicant of the authentication failure based on the time that is shorter.

(8) Specifying a forced authentication port

When a terminal connected to a port for which forced authentication is specified undergoes RADIUS authentication, and sending a request to the RADIUS server fails due to a line failure or the RADIUS does not respond, the terminal becomes authenticated.

Forced authentication of the Switch is configured for all shared authentication settings and each authentication functionality, respectively. However, VLAN-based authentication (dynamic) does not work on configurations common to all authentication methods. Use the forced authentication functionality of IEEE 802.1X.

Use the `dot1x force-authorized vlan` configuration command for a port where forced authentication is to be permitted. Also, use the `dot1x force-authorized eapol` configuration command to send an EAP-Success response to the terminal where forced authentication is permitted.

Forced authentication is successful when the following conditions are met.

Table 6-13 Conditions for successful forced authentication

Item	Condition
Configuration	All the following configurations have been set: ● `aaa authentication dot1x`[#1] ● `dot1x radius-server host` or `radius-server host` ● `dot1x system-auth-control` ● `aaa authorized network default group radius` ● `dot1x vlan dynamic enable` ● `dot1x vlan dynamic radius-vlan`[#2] ● `dot1x force-authorized vlan`[#2] ● `vlan` *<VLAN ID>* `mac-based`[#2] ● `switchport mac`[#2, #3] ● `switchport mode mac-vlan`[#3]
Account log	The following account log is collected when an authentication request is sent to the RADIUS server: ● `No=82` `WARNING:SYSTEM: (`*<Additional information>*`) Failed to connect to RADIUS server.` *<Additional information>*`: IP` You can use the `show dot1x logging` command to check the account

Item	Condition
	log.

#1

When forced authentication is used as the Switch default, set `default group radius`.

#2

Set the same VLAN ID.

#3

Configure the same port.

The authentication status of a terminal where authentication is permitted by forced authentication is canceled in the same way as for a normally authenticated terminal, as described in *(9) Authentication cancellation* in *6.4.2 Authentication functionality.*

Furthermore, all operations from the start of requesting authentication to the RADIUS server to successful forced authentication are the same, whether shared forced authentication common to all authentication modes or forced authentication based on individual authentications is used. For details about the operations, *(1) Behavior from the start of an RADIUS authentication request to permission for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

All EAPOL frames sent from terminals that went through forced authentication are discarded before the next re-authentication time.

(9) Authentication cancellation

The following methods of canceling authentication are provided in VLAN-based authentication (dynamic).

- Canceling authentication for a terminal that does not respond to an authentication request
- Canceling authentication by monitoring the aging of the MAC address table
- Canceling authentication of terminals connected to link-down ports
- Canceling authentication resulting from changes to the VLAN configuration
- Canceling authentication using an operation command

Monitoring of MAC address table aging monitoring of VLAN-based authentication (dynamic) targets authenticated terminals. The aging monitoring behavior is the same as for port-based monitoring (dynamic). For details, see *(9) Authentication status cleared* in *6.2.2 Authentication functionality.*

6.5 EAPOL forwarding

You can use the EAPOL forwarding functionality to relay EAPOL frames when IEEE 802.1X authentication is disabled. Because an EAPOL frame has a destination MAC address reserved by IEEE 802.1D, it is not forwarded on a standard basis. However, it can be forwarded if IEEE 802.1X is not in use. Configure EAPOL forwarding when using the Switch as an L2 switch between a terminal and another authenticator.

For an example of configuring the Switch, see *18.2 Configuring the L2 protocol frame transparency functionality* in the *Configuration Guide Vol. 1*.

6.6 Account functionality

Authentication results of IEEE 802.1X are recorded using the following account functionality:

- Internal account log of the Switch
- Recording information to the RADIUS server account functionality
- Recording authentication information to the RADIUS server
- Outputting account log information to the syslog server

(1) Internal account log of the Switch

Operation log information, including IEEE 802.1X authentication results and operation information, is recorded in the internal accounting log of the Switch.

The account log built into the Switch can record up to 2100 lines in total for the authentication of IEEE 802.1X. When the maximum number of 2,100 lines is exceeded, the oldest lines are deleted, and the newest account log information is added.

The following table lists the account log information that is recorded.

Table 6-14 Account log types

Account log type	Description
LOGIN	Information (success or failure) relating to authentication operations
LOGOUT	Causes for success or failure of authentication operations
SYSTEM	Relates to actions of IEEE 802.1X (including permission of forced authentication)

Table 6-15 Information output to the internal account log of the Switch

Account log type		Time	IP	MAC	VLAN	Port	Message
LOGIN	succeeded	Y	N	Y	Y#1	Y	Authentication success message
	failed	Y	N	Y	Y#1	Y	Authentication failure reason message
LOGOUT		Y	N	Y	Y#1	Y	Authentication cancellation message
SYSTEM		Y	Y#1, #2	Y#1	N	Y#1	Message related to operations of IEEE 802.1X

Legend:

Y: Output

N: Not output

#1

Some messages might not be output.

#2

Frame sender IP address or destination RADIUS server IP address

For details about messages, see *show dot1x logging* in *25. IEEE 802.1X* in the manual *Operation Command Reference*.

In addition, the following lists the output functionality of the account logs:

1. Console display per event

   Even when the `trace-monitor enable` operation command has been executed, account log information is not output to the console each time an event occurs.

2. Operation command display

   The accounting log collected is displayed from the latest information using the `show dot1x logging` operation command.

3. Outputting to the syslog server

   For details, see *(4) Outputting account logs information to the syslog server.*

4. Private traps

   The Switch supports the functionality that issues private traps, which is triggered by the account log collected when a specific event of IEEE 802.1X authentication occurs. Use configuration commands to specify whether traps are issued and also the type of traps that are issued.

Table 6-16 Account log (LOGIN/LOGOUT) and conditions to issue a private trap

Account log type		Configuration required for issuing a private trap	
		Command	**Parameter**
LOGIN	succeeded	`snmp-server host`	`dot1x`
		`snmp-server traps`	`dot1x-trap all`
	failed	`snmp-server host`	`dot1x`
		Not configured, or one of the following configured:	
		`snmp-server traps`	`dot1x-trap all`
		`snmp-server traps`	`dot1x-trap failure`
LOGOUT		`snmp-server host`	`dot1x`
		`snmp-server traps`	`dot1x-trap all`

In account log type (`SYSTEM`), a private trap can only be issued with forced authentication common to all authentication modes. For conditions to issue the private trap with forced authentication, see *(5) Private trap for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

(2) Recording information to the RADIUS server account functionality

You can use the `aaa accounting dot1x` configuration command to use the account functionality of a RADIUS server.

For details about the RADIUS attributes used when sending accounting information to the RADIUS server, see *6.7 Preparation.*

(3) Recording authentication information in the RADIUS server

If you are using RADIUS authentication, the account functionality of the RADIUS server records the success or failure of authentication attempts. Note that the information that is recorded might differ depending on the type of RADIUS server. For details, see the documentation for the RADIUS server deployed in your network.

(4) Outputting account logs information to the syslog server

Accounting log information for IEEE 802.1X and operation log information for all Switches are output to all the syslog servers defined in the `syslog` configuration.

Figure 6-19 Format of output to syslog server

```
Fac Mon Date Time hostname [number]:AUT Mon/Date/Time xxx log message body
|(1)|---(2) ---|--(3)---|--(4)-|(5)|----(6)---|(7)|------------(8)-------------|
```

(1) Facility
(2) Date and time output in TIMESTAMP: syslog
(3) Identification name of HOSTNAME: Switch
(4) Function number
(5) Log type representing authentication function
(6) Event occurrence time
(7) Authentication function type representing IEEE 802.1X authentication
(8) Message body

For details about outputting log information to the syslog server, see *22. Log Data Output Functionality*.

With this Switch, you cannot specify output or suppression of only the accounting log information for IEEE 802.1X to a syslog server.

6.7 Preparation

To use RADIUS authentication, the following preparations are required:

- Configuration definition
- Preparing the RADIUS server

(1) Configuration definition

In order to use IEEE 802.1X, create the configuration commands to configure VLAN and IEEE 802.1X information for the Switch. (For details, see *7. IEEE 802.1X Configuration and Operation.)*

(2) Preparing the RADIUS server

(a) RADIUS attributes to use

The following table shows the RADIUS attributes used by the Switch.

Table 6-17 Attributes used in authentication (Part 1: Access-Request)

Attribute name	Type value	Description
`User-Name`	1	User ID to be authenticated
`NAS-IP-Address`	4	IP address of the Switch requesting authentication. From among the VLAN interfaces that have an IP address registered, the IP address of the smallest VLAN ID is used.
`NAS-Port`	5	● Port-based authentication (static): `IfIndex` of an authentication unit which is authenticating ● Port-based authentication (dynamic): `IfIndex` of an authentication unit which is authenticating ● VLAN-based authentication (dynamic): 4,296
`Service-Type`	6	The type of service to be provided. Fixed as `Framed(2)`.
`Framed-MTU`	12	Maximum frame size between the supplicant and the authenticator. Fixed at (1466).
`State`	24	Allows state information to be maintained between the authenticator and a RADIUS server.
`Called-Station-Id`	30	MAC address of the Switch (lower-case ASCII#, separated by a hyphen (-)).
`Calling-Station-Id`	31	MAC address of the Supplicant (lower-case ASCII#, separated by a hyphen (-)).
`NAS-Identifier`	32	Character string to identify the authenticator (by host name).
`NAS-Port-Type`	61	Type of physical port the authenticator is using to authenticate the user.

Attribute name	Type value	Description
		Fixed as Ethernet (15).
Connect-Info	77	Character string to show characteristics of supplicant's connection ● Port-based authentication (static): Physical port ("CONNECT Ethernet") Channel group port ("CONNECT Port-Channel") ● Port-based authentication (dynamic): Physical port ("CONNECT Ethernet") ● VLAN-based authentication (dynamic): ("CONNECT DVLAN")
EAP-Message	79	Encapsulates an EAP frame.
Message-Authenticator	80	Used to protect a RADIUS/EAP frame.
NAS-Port-Id	87	Character string to identify a port of Authenticator to authenticate Supplicant (x, y:numeric values). ● Port-based authentication (static):"Port x/y", "ChGr x" ● Port-based authentication (dynamic):"Port x/y" ● VLAN-based authentication (dynamic):"DVLAN x"

#

The Swich uses MAC addresses of Called-Station-Id and Calling-Station-Id in lower case. However, the letters a to f in the MAC addresses can be converted to upper-case letters by using the radius-server attribute station-id capitalize configuration command.

Table 6-18 Attributes used in authentication (Part 2: Access-Accept)

Attribute name	Type value	Description
Service-Type	6	The type of service to be provided. Fixed as Framed(2).
Filter-Id	11	Text character string. ● Authentication IPv4 access list name to filter an unauthenticated frame. ● Used in multistep authentication.#1
Reply-Message	18	Message displayed to a user#2.
Tunnel-Type	64	Tunnel type#3 Important in port-based authentication (dynamic) and VLAN-based (dynamic). Fixed as VLAN(13).

Attribute name	Type value	Description
Tunnel-Medium-Type	65	Indicates the protocol to use to create a tunnel[#3]. Important in port-based authentication (dynamic) and VLAN-based (dynamic). Fixed as IEEE 802(6).
EAP-Message	79	Encapsulates an EAP frame.
Message-Authenticator	80	Used to protect a RADIUS/EAP frame.
Tunnel-Private-Group-ID	81	Character string for VLAN identification.[#4] In an Access-Accept packet, this attribute indicates the VLAN to be assigned to the authenticated supplicant. Important in port-based authentication (dynamic) and VLAN-based (dynamic). The character strings can be formatted as follows: (1) As a character string indicating a VLAN ID (2) As a character string containing the word "VLAN" followed by a VLAN ID The character string cannot contain spaces. If it does, VLAN assignment will fail. (3) Character string representing the name of a VLAN defined for a VLAN interface by the name configuration command (The smaller VLAN ID takes precedence.)[#5] Examples VLAN ID: 10 Configuration command name: Authen_VLAN For (1): 10 For (2): VLAN10 For (3): Authen_VLAN

#1

For details about character strings used in multistep authentication, see *12. Multistep authentication.*

#2

The Switch collects the Reply-Message character string as account log information.

#3

The tag area is ignored

#4

The Switch selects a character string format and identifies the VLAN ID in accordance with the following conditions:

1. Conditions for selecting character string formats (1), (2) and (3) for Tunnel-Private-Group-ID:
    - Format (1) is used for a character string that begins with a number from 0 to 9.
    - Format (2) is used for a character string that begins with VLAN followed by a number from 0 to 9.

- Format (3) is used for a character string other than the above character strings.

In addition, when the first byte is in the range from 0x00 to 0x1f, it means that a tag is present but the tag area is ignored.

2. Conditions for identifying the VLAN ID from character strings in formats (1) and (2):

- Converts only the numerical characters 0 to 9 into a decimal number and its first four characters become valid. (The fifth and the subsequent characters are all ignored.)

  Example: `0010` is equivalent to `010` or `10`, and it is handled as VLAN ID = 10.

  However, `01234` is handled as VLAN ID = 123.

- If a character other than 0 through 9 exists in the middle of the character string, the character is considered to be the end of the string.

  Example: `12+3` is handled as VLAN ID = 12.

#5

For details about specifying the VLAN name by using the `name` configuration command, see *5.4.2 Specifying post-authentication VLANs by VLAN name.*

Table 6-19 Attributes used for authentication (Part 3: Access-Challenge)

Attribute name	Type value	Description
`Reply-Message`	18	Message displayed to a user#
`State`	24	Allows State information to be maintained between the Authenticator and a RADIUS server.
`EAP-Message`	79	Encapsulates an EAP frame.
`Message-Authenticator`	80	Used to protect a RADIUS/EAP frame.

#

The Switch collects the `Reply-Message` character string as account log information.

Table 6-20 Attributes used in authentication (Part 4: Access-Reject)

Attribute name	Type value	Description
`Reply-Message`	18	Message displayed to a user#
`EAP-Message`	79	Encapsulates an EAP frame.
`Message-Authenticator`	80	Used to protect a RADIUS/EAP frame.

#

The Switch collects the `Reply-Message` character string as account log information.

Table 6-21 Attribute names used in RADIUS account functionality

Attribute name	Type value	Description
`User-Name`	1	User ID to be authenticated
`NAS-IP-Address`	4	IP address of the Switch requesting authentication From among the VLAN interfaces that have an IP address registered, the IP address of the smallest VLAN ID is used.
`NAS-Port`	5	● Port-based authentication (static): `IfIndex` of an authentication unit which is authenticating ● Port-based authentication (dynamic): `IfIndex` of an authentication unit which is authenticating ● VLAN-based authentication (dynamic): 4296
`Service-Type`	6	The type of service to be provided Fixed as `Framed(2)`.
`Calling-Station-Id`	31	The MAC address of the Supplicant (lower-case ASCII#, separated by a hyphen (-))
`NAS-Identifier`	32	A string identifying the authenticator (by host name).
`Acct-Status-Type`	40	Accounting request type Start(1), Stop(2)
`Acct-Delay-Time`	41	Accounting information (send delay time) (in seconds)
`Acct-Input-Octets`	42	Accounting information (number of received octets) Fixed at (0).
`Acct-Output-Octets`	43	Accounting information (number of sent octets) Fixed at (0).
`Acct-Session-Id`	44	ID to identify accounting information
`Acct-Authentic`	45	Authentication method RADIUS(1)
`Acct-Session-Time`	46	Accounting information (session duration time) Fixed at (0).
`Acct-Input-Packets`	47	Accounting information (number of incoming packets) Fixed at (0).
`Acct-Output-Packets`	48	Accounting information (number of outgoing packets) Fixed at (0).
`Acct-Terminate-Cause`	49	Accounting information (cause of session termination) See *Table 6-22 Disconnection causes returned by Acct-Terminate-Cause.*

Attribute name	Type value	Description
NAS-Port-Type	61	Type of physical port the authenticator is using to authenticate the user. Fixed as Ethernet (15).
NAS-Port-Id	87	Character string to identify a port of Authenticator to authenticate Supplicant (x, y:numeric values). ● Port-based authentication (static):"Port x/y", "ChGr x" ● Port-based authentication (dynamic):"Port x/y" ● VLAN-based authentication (dynamic):"DVLAN x"

#

The Switch uses the MAC addresses of Calling-Station-Id in lower case. However, the letters a to f in the MAC addresses can be converted to upper-case letters by using the radius-server attribute station-id capitalize configuration command.

Table 6-22 Disconnection causes returned by Acct-Terminate-Cause

Attribute name	Type value	Description
User Request	1	Disconnected due to the request of the supplicant. ● When a logoff request was received from the authenticated terminal Disconnection due to detection of a terminal move
Idle Timeout	4	Disconnection due to non-communication continuing for a certain period of time
Admin Reset	6	Disconnected by the administrator. ● When configuration is deleted in an authentication unit ● When dot1x port-control force-authorized is configured ● When dot1x port-control force-unauthorized is configured ● When dot1x port-control is deleted ● When clear dot1x auth-state is performed using the operation command Also includes disconnection causes due to changes to other authentication configurations and operation commands.
NAS Request	10	The first-step IEEE 802.1X authentication disconnected because the second step authentication is successful in multistep authentication (the authentication multistep dot1x configuration command has been configured)
Reauthentication Failure	20	Re-authentication failed.

Attribute name	Type value	Description
Port Reinitialized	21	The port's MAC address has been reinitialized. ● When a port is linked down ● When vlan is deleted from a port by the configuration ● When shutdown is set in by the configuration ● When the inactivate operation command is executed
Port Administratively Disabled	22	Port disabled administratively. ● When an authentication submode detects the second terminal on a port in the single-terminal mode

(b) Recording information to be configured to the RADIUS server

Before using the RADIUS authentication method, configure the user ID, password, and VLAN ID for each user in the RADIUS server.

For details about how to configure the RADIUS server, see the documentation for the RADIUS server deployed in your network.

The following shows an example of configuring VLAN information for each user subject to authentication in the RADIUS server:

- For port-based authentication (static): Configuration not required
- For port-based authentication (dynamic)and VLAN-based authentication (dynamic): The VLAN ID of the post-authentication is 40.
- For configuration using the name configuration command: dot1x-authen-vlan

Table 6-23 Example of RADIUS server configuration

Configuration items	Description
User-Name	User ID of the terminal subject to authentication.
Auth-Type	Local
User-Password	Password of the terminal subject to authentication.
NAS-Identifier	Host name of the Switch. (Character string configured using the hostname configuration command)
Tunnel-Type	Virtual VLAN (value of 13)
Tunnel-Medium-Type	IEEE-802 (value of 6)

Configuration items	Description
Tunnel-Private-Group-ID	Port-based authentication (dynamic) and VLAN-based authentication (dynamic): Any of the following formats is used: ● "40" The post-authentication VLAN ID is defined as a number. ● VLAN40 The post-authentication VLAN ID is defined as a number immediately after the character string VLAN ● dot1x-authen-vlan A character string representing a VLAN name defined by the name configuration command
Authentication method	EAP

6.8 Notes on IEEE 802.1X

6.8.1 Interoperability of IEEE 802.1X and other functionality

For details about the interoperability of IEEE 802.1X and other functionality, see *5.9.3 Interoperability of the Layer 2 authentication functionality and other functionality.*

6.8.2 Notes on using IEEE 802.1X

(1) Aging time settings for MAC address learning in VLAN-based authentication (dynamic)

When using VLAN-based authentication (dynamic), do not specify 0 (infinite) as the time period for an MAC address entry. If you specify `0` (infinite), when a terminal is assigned to a new VLAN, MAC address entries relating to the former VLAN will not be aged out from the MAC address table. As a result, the MAC address table will become populated with unused addresses. When unnecessary MAC address entries accumulate, use the `clear mac-address-table` operation command to delete them.

(2) Displaying the MAC address table for an authenticated terminal

The terminal authenticated with port-based authentication displays `Dot1x` as a type using the `show mac-address-table` operation command. The terminal authenticated with VLAN-based authentication (dynamic) displays `Dynamic`. However, the terminal under quarantine in port-based authentication (static) displays `Dynamic`.

(3) Connecting an authenticated terminal to another port

When connecting an authenticated terminal to an IEEE 802.1X-effective port, authentication is canceled. However, when an authenticated terminal with VLAN-based authentication (dynamic) is connected to a port of a single VLAN belonging to VLAN-based authentication (dynamic), authentication continues.

In addition, when an authenticated terminal is connected to a different port that does not go through authentication within a single VLAN, communication is impossible until the authentication status is canceled. Use the `clear dot1x auth-state` operation command to cancel the authentication status of the terminal.

(4) Changing timer values

If you change the value of a timer (`tx-period`, `reauth-period`, `supp-timeout`, `quiet-period`, or `keep-unauth`), the change does not take effect until that timer times out for the authentication unit. If you want to reflect new values immediately, use the `clear dot1x auth-state` operation command to cancel their authentication statuses.

(5) Notes on placing L2 switches between terminals and the Switch

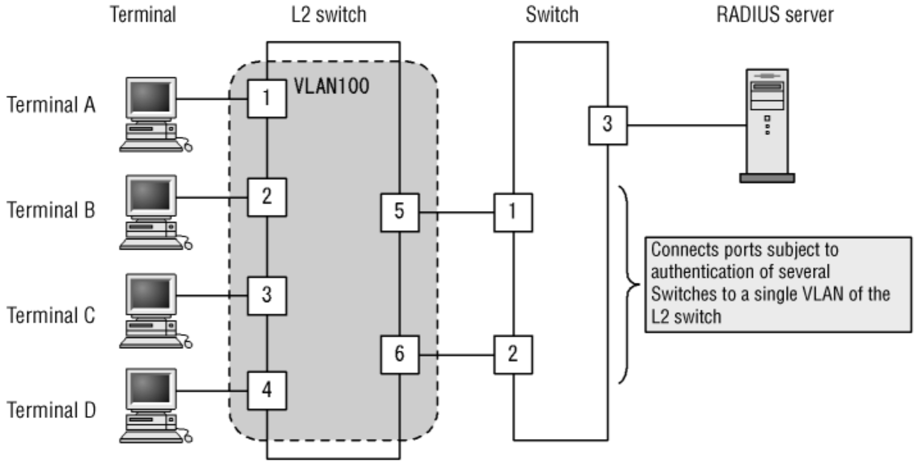
Responses from terminals are typically multicast. Therefore, if you connect an L2 switch between the terminal and the Switch, EAPOL frames that encapsulate responses from the terminal are forwarded to every port in the same VLAN on the L2 switch. Therefore, if an L2 switch is arranged as described in the list below, EAPOL frames from a single terminal are transferred to several ports of the Switch and authentication is performed for a single terminal on several ports. This affects the stability of the authentication process, and might result in dropped connections, failed authentication, and other issues.

- Ports in the same VLAN on the L2 switch connect to multiple ports that are subject to authentication by the Switch
- Ports in the same VLAN on the L2 switch connect to the authenticating ports of multiple Switches

The figures below show examples of correct and prohibited configurations of an L2 switch between terminals and the Switch.

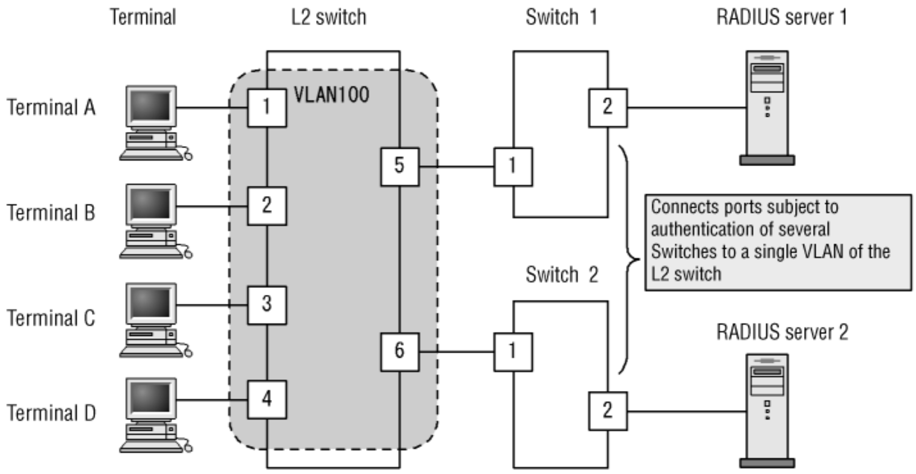
Figure 6-20 Examples of prohibited configurations

• Example of connecting ports subject to authentication of several Switches to a single VLAN of the L2 switch



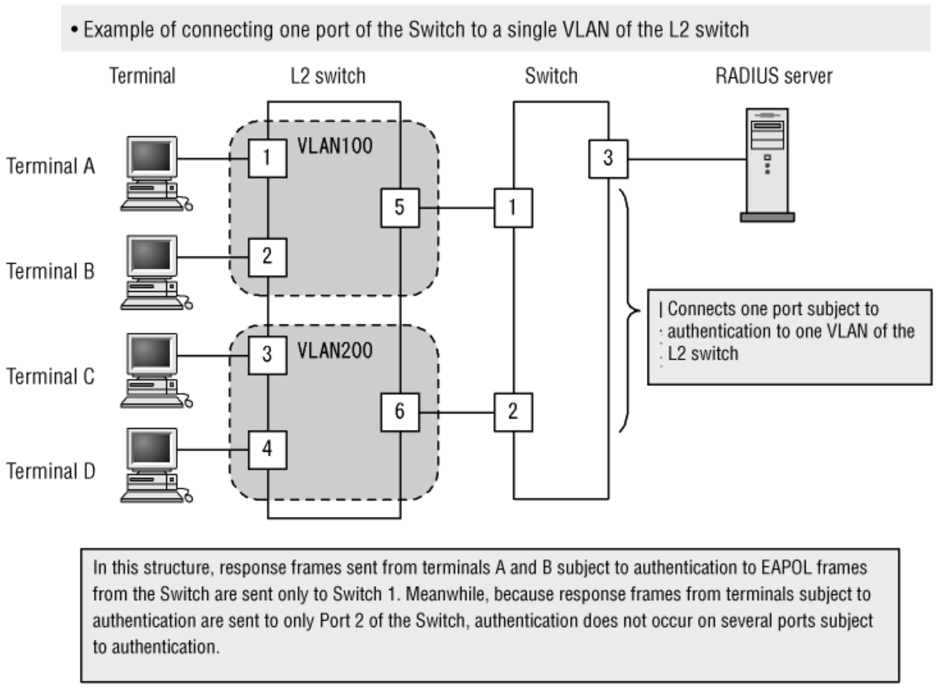
In this structure, response frames sent from terminals subject to authentication, A, B, C, and D to EAPOL frames sent from the Switch are sent to ports subject to authentication 1 and 2 of the Switch. This executes authentication on authentication ports subject to authentication 1 and 2 of the Switch. If a port subject to authentication has been authenticated on other ports, each authentication port cancels terminals subject to authentication on the ports and performs authentication on it. As a result, communication of an authenticated terminal is interrupted.

• Example of connecting ports subject to authentication of several Switches to a single VLAN of the L2 switch



In this structure, the EAPOL-Start frame sent from terminals subject to authentication is sent to the Switches 1 and 2 on a multicast basis. Meanwhile, authentication is performed on Switches 1 and 2, which receives this EAPOL-Start frame, and one terminal becomes authenticated on Switches 1 and 2.

Figure 6-21 Examples of correct configuration



(6) Note on specifying a MAC VLAN as an access port

- When specifying a MAC VLAN in VLAN-based authentication (dynamic) as an access port, an EAPOL frame is sent from a specified port of the Switch. However, the specified port is handled as an authentication-exempted port even when a user sends authentication response to an EAPOL frame. This enables communication on the specified port regardless of the authentication result.
- Configure port-based authentication (static) for an interface where a MAC VLAN has been specified as the access port. However, it is not interoperable with port-based authentication (dynamic) on a single port. (They can interoperate in the Switch. For details, see *5. Overview of Layer 2 Authentication*.)

(7) Using a forced authentication port

- Be especially careful when using this functionality, as it can pose a security problem.
- The Switch provides the forced authentication functionality common to all authentication modes and for IEEE 802.1X authentication, which are not interoperable. Prior to using this functionality, see *(4) Interoperability of this functionality and forced authentication of each authentication method* in *5.4.6 Forced authentication common to all authentication modes.*

(8) Interoperability of VLAN-based authentication (dynamic) and multistep authentication

VLAN-based authentication (dynamic) and multistep authentication are not interoperable in the Switch. When using VLAN-based authentication (dynamic), check that multistep authentication has not been configured.

7. IEEE 802.1X Configuration and Operation

IEEE 802.1X functionality authenticates Layer 2 of the OSI layer model. This chapter describes IEEE 802.1X operations.

7.1 IEEE 802.1X configuration

7.1.1 List of configuration commands

The following table describes the configuration commands and authentication modes for IEEE 802.1X.

Table 7-1 Configuration commands and authentication modes for IEEE 802.1X

Command name	Description	Authentication mode		
		Port-based		VLAN-based
		Static	Dynamic	Dynamic
`aaa accounting dot1x`	Sends IEEE 802.1X accounting information to the accounting server.	Y	Y	Y
`aaa authentication dot1x`	Sets an IEEE 802.1X authentication method group.	Y	Y	Y
`aaa authorization network default`	Enables VLAN-based authentication (dynamic) using VLAN information provided by the RADIUS server.	--	--	Y
`authentication arp-relay`#1	Outputs ARP frames that were sent to other devices from unauthenticated terminals to a non-authenticating port.	Y	Y	N
`authentication ip access-group`#1	Outputs only the frames specified by applying the IPv4 access list, from among the IP frames sent from an unauthenticated terminal destined for another device, to a non-authenticating port.	Y	Y	N
`dot1x authentication`	Sets the name of an authentication method list for the port-based authentication method.	Y	Y	N
`dot1x auto-logout`	The `no dot1x auto-logout` command disables the setting to automatically cancel authentication when no frame is received from a terminal authenticated by	Y	Y	Y

Command name	Description	Authentication mode		
		Port-based		VLAN-based
		Static	Dynamic	Dynamic
	IEEE 802.1X for a certain period of time.			
dot1x force-authorized	When using RADIUS authentication, and a request to the RADIUS server fails because of a route failure or other problem, forcibly changes a terminal to be authenticated to an authenticated state when that terminal requests authentication at the relevant port.	Y	N	N
dot1x force-authorized eapol	Sends the EAPOL-Success response frame from the Switch to the terminal when it is forcibly authenticated.	Y	Y	Y
dot1x force-authorized vlan	When using RADIUS authentication, and a request to the RADIUS server fails because of a route failure or other problem, forcibly changes a terminal to be authenticated to an authenticated state when that terminal requests authentication at the relevant port, and assigns a post-authentication VLAN.	N	Y	Y
dot1x ignore-eapol-start	Configures the switch not to transmit EAP-Request/Identity packets in response to an EAPOL-Start message received from a supplicant.	Y	Y	--
dot1x max-req	Specifies the maximum number of times that the Switch sends an EAP-Request/Identity packet when there is no response from the supplicant.	Y	Y	--
dot1x multiple-authentication	Applies an authentication submode to port-based	Y	Y	--

Command name	Description	Authentication mode		
		Port-based		VLAN-based
		Static	Dynamic	Dynamic
	authentication.			
`dot1x port-control`#2	Enables port-based authentication.	Y	Y	--
`dot1x radius-server host`	Specifies information about the RADIUS server dedicated to IEEE 802.1X authentication.	Y	Y	Y
`dot1x radius-server dead-interval`	Specifies the monitoring timer until automatic recovery to the primary RADIUS server when using a RADIUS server dedicated to IEEE 802.1X authentication.	Y	Y	Y
`dot1x reauthentication`	Enables or disables periodic re-authentication of authenticated terminals.	Y	Y	--
`dot1x supplicant-detection`	Configures how terminal detection is performed when terminal authentication mode is specified as the authentication submode.	Y	Y	--
`dot1x system-auth-control`	Enables IEEE 802.1X.	Y	Y	Y
`dot1x timeout keep-unauth`#3	In the context of port-based authentication in single-terminal mode, this command configures how long the port blocks traffic after receiving authentication requests from multiple terminals.	Y	Y	--
`dot1x timeout quiet-period`	Configures how long the Switch waits before allowing a supplicant that failed authentication (including re-authentication) to try again.	Y	Y	--
`dot1x timeout reauth-period`	Specifies the interval between re-authentication attempts for authenticated terminals.	Y	Y	--

Command name	Description	Authentication mode		
		Port-based		VLAN-based
		Static	Dynamic	Dynamic
`dot1x timeout server-timeout`	Specifies how long the Switch waits for a response from the authentication server.	Y	Y	--
`dot1x timeout supp-timeout`	Configures how long the Switch waits for a supplicant to respond to an EAP-Request/Identity packet.	Y	Y	--
`dot1x timeout tx-period`	Specifies the sending interval for EAP-Request/Identity packets.	Y	Y	--
`dot1x vlan dynamic enable`	Enables VLAN-based authentication (dynamic).	--	--	Y
`dot1x vlan dynamic ignore-eapol-start`	Configures the Switch not to transmit EAP-Request/Identity packets in response to an EAPOL-Start message received from a supplicant.	--	--	Y
`dot1x vlan dynamic max-req`	Specifies the maximum number of times that the Switch sends an EAP-Request/Identity packet when there is no response from the supplicant.	--	--	Y
`dot1x vlan dynamic radius-vlan`	In the context of VLAN-based authentication (dynamic), this command specifies the VLANs that the Switch can dynamically assign on the basis of information received from the RADIUS server.	--	--	Y
`dot1x vlan dynamic reauthentication`	Enables or disables periodic re-authentication of authenticated terminals.	--	--	Y
`dot1x vlan dynamic supplicant-detection`	Configures how terminal detection is performed when terminal authentication mode is specified as the	--	--	Y

Command name	Description	Authentication mode		
		Port-based		VLAN-based
		Static	Dynamic	Dynamic
	authentication submode.			
`dot1x vlan dynamic timeout quiet-period`	Configures how long the Switch waits before allowing a supplicant that failed authentication (including re-authentication) to try again.	--	--	Y
`dot1x vlan dynamic timeout reauth-period`	Specifies the interval between re-authentication attempts for authenticated terminals.	--	--	Y
`dot1x vlan dynamic timeout server-timeout`	Specifies how long the Switch waits for a response from the authentication server.	--	--	Y
`dot1x vlan dynamic timeout supp-timeout`	Configures how long the Switch waits for a supplicant to respond to an EAP-Request/Identity packet.	--	--	Y
`dot1x vlan dynamic timeout tx-period`	Specifies the sending interval for EAP-Request/Identity packets.	--	--	Y

Legend:

Port-based, Static: Port-based authentication (static)

Port-based, Dynamic: Port-based authentication (dynamic)

VLAN-based, Dynamic: VLAN-based authentication (dynamic)

Y: The command operates according to the settings.

--: The command can be entered, but has no effect.

N: The command cannot be entered.

#1

For details about the configuration, see *5. Overview of Layer 2 Authentication.*

#2

The specification of this command affects the switching of authentication modes.

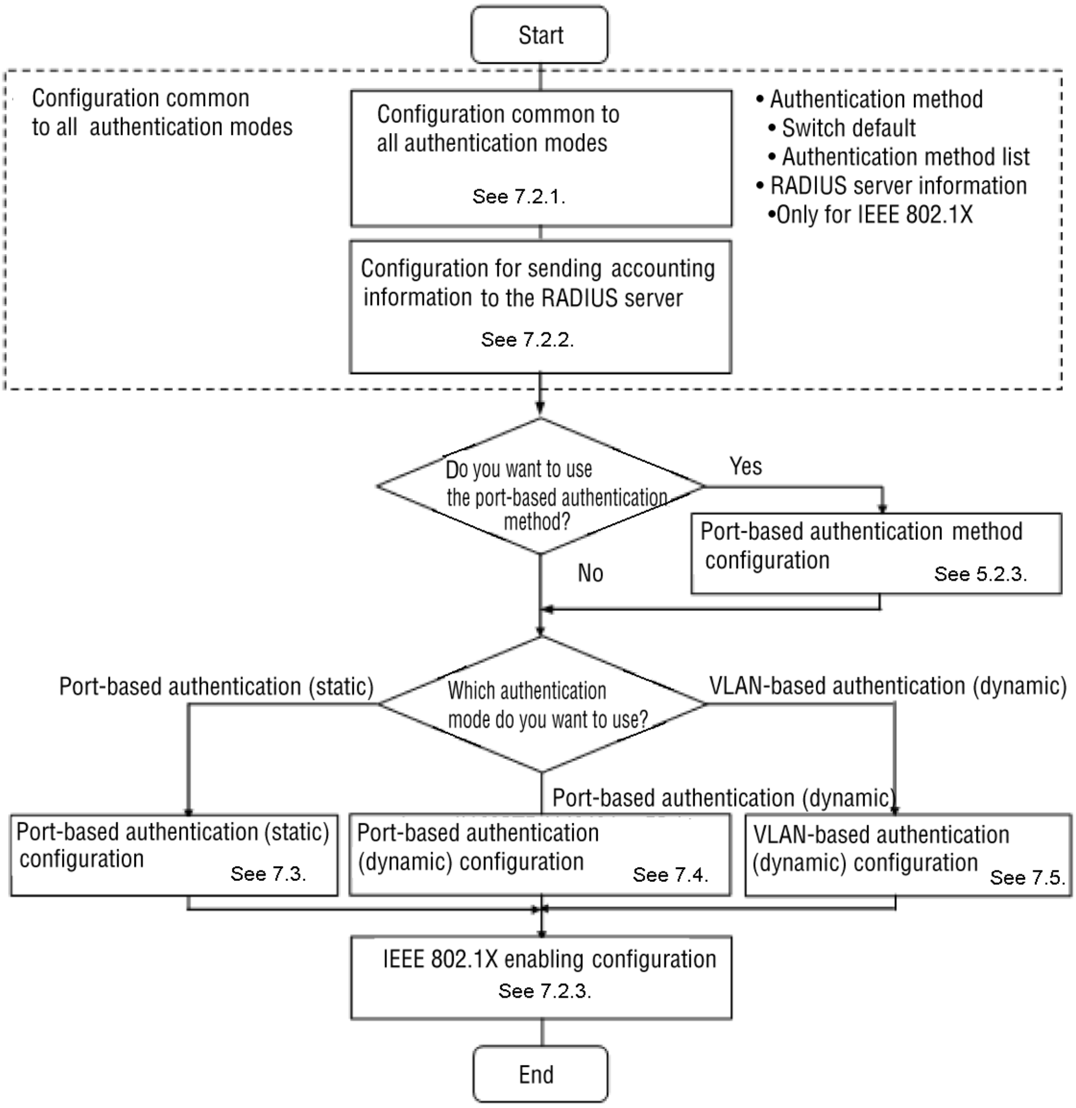
#3

The specification of this command applies only to single-terminal mode of port-based authentication (static) and port-based authentication (dynamic).

7.1.2 Configuration procedure for IEEE 802.1X

Use the procedure described below to configure IEEE 802.1X.

Figure 7-1 Configuration procedure for IEEE 802.1X



For details about the configuration, see the following:

1. Configuration common to all authentication modes

   The following subsections describe configuration common to all authentication modes.

   - Configuring the authentication method group and RADIUS server information: *7.2.1 Configuring the authentication method group and RADIUS server information*
   - Configuring the transmission of accounting information to the RADIUS

server: *7.2.2 Configuring the transmission of accounting information*

- Configuring port-based authentication methods: *(2) Example of port-based authentication method configuration* in *5.2.3 Authentication method list configuration*

2. Configuring individual authentication modes

   The following sections describe how to configure individual authentication modes.

   Some items are the same as in other authentication modes. In such cases, see the sections referenced in the text.

   - Configuring port-based authentication (static): *7.3 Configuring port-based authentication (static)*
   - Configuring port-based authentication (dynamic): *7.4 Configuring port-based authentication (dynamic)*
   - Setting VLAN-based authentication (dynamic): *7.5 Configuring VLAN-based authentication (dynamic)*

3. Enabling IEEE 802.1X

   The following section describes how to enable IEEE 802.1X to finish IEEE 802.1X configuration.

   - *7.2.3 Enabling IEEE 802.1X*

Authentication modes are enabled by using the configuration settings described in the table below.

Table 7-2 Conditions for enabling authentication modes

Authentication mode	**Configuration settings**
Common	● `aaa authentication dot1x` ● `dot1x radius-server host` or `radius-server` ● `dot1x system-auth-control`
Port-based authentication (static)	● `vlan` *<VLAN-ID-list>* ● `dot1x port-control auto` ● `switchport mode access` ● `switchport access vlan`
Port-based authentication (dynamic)	● `vlan` *<VLAN ID list>* `mac-based` ● `dot1x port-control auto` ● `switchport mode mac-vlan`
VLAN-based authentication (dynamic)	● `vlan` *<VLAN ID list>* `mac-based` ● `aaa authorization network default` ● `dot1x vlan dynamic enable` ● `dot1x vlan dynamic radius-vlan` ● `switchport mode mac-vlan` ● `switchport mac vlan`

7.2 Configuration common to all authentication modes

7.2.1 Configuring the authentication method group and RADIUS server information

(1) Configuring the authentication method group

Points to note

Set an IEEE 802.1X authentication method group.

Specify one device default entry for use in common with IEEE 802.1X, and two entries for the authentication method lists used at authenticating ports.

1. Switch default

   RADIUS authentication is specified as the device default in this sample.

2. Authentication method list

   For the RADIUS server group information to be specified for authentication method lists, `Keneki-group1` and `Keneki-group2` are assumed to have been set in advance.

   For details about authentication method lists, see *5.2.2 Authentication method list.*

   For RADIUS server group information, see *5.3.1 RADIUS server information used with the Layer 2 authentication method*, and *8. Login Security and RADIUS* in the *Configuration Guide Vol. 1*.

Command examples

1. `(config)# aaa authentication dot1x default group radius`

Specifies RADIUS authentication as the default authentication method of the device.

2. `(config)# aaa authentication dot1x DOT1X-list1 group Keneki-group1`

Specifies the RADIUS server group name `Keneki-group1` in the authentication method list `DOT1 X-list1`.

3. `(config)# aaa authentication dot1x DOT1X-list2 group Keneki-group2`

Specifies the RADIUS server group name `Keneki-group2` in the authentication method list `DOT1 X-list2`.

Notes

If the configuration of an authentication method group changes, authentication for the terminals affected by the change is canceled.

- If a Switch default is added, authentication is not canceled.
- If the Switch default is changed or deleted, authentication for the terminals that have been authenticated by using the Switch default is canceled.
- If an authentication method list is added, authentication for terminals on the ports that specify the corresponding authentication method list is canceled. (If the authentication method list specified for the port has not been set by using the `aaa authentication dot1x` configuration command, the Switch default is used for authentication.)

- If an authentication method list is changed or deleted, authentication for the terminals that have been authenticated by using the authentication method list is canceled.

(2) Configuring RADIUS server information

(a) When using a RADIUS server dedicated to IEEE 802.1X

Points to note

The example below shows how to specify information about a RADIUS server dedicated to IEEE 802.1X authentication.

An IP address and a RADIUS key must be specified to enable the RADIUS server settings. The configuration command `dot1x radius-server host` requires only an IP address for configuration, but the RADIUS server is not used for authentication until you specify a RADIUS key.

In this example, a monitoring timer (`dead-interval` time) is also configured to automatically recover an unavailable RADIUS server dedicated to IEEE 802.1X authentication.

Command examples

1. `(config)# dot1x radius-server host 192.168.10.200 key "dot1x-auth"`

Specifies the IP address and RADIUS key for the RADIUS server dedicated to IEEE 802.1X authentication. In this example, the default values are used for the omitted `auth-port`, `acct-port`, `timeout`, and `retransmit`.

2. `(config)# dot1x radius-server dead-interval 15`

Specifies 15 minutes for the monitoring timer (`dead-interval` time) until automatic recovery when the RADIUS server dedicated to IEEE 802.1X authentication is unavailable.

Notes

- If this information is not specified, the settings for a general-use RADIUS server are used. If both the information for a RADIUS server dedicated to IEEE 802.1X authentication and the information for a general-use RADIUS server are unspecified, RADIUS authentication cannot be performed.
- Up to four entries can be specified on the entire Switch for information about RADIUS servers dedicated to IEEE 802.1X authentication.
- When the RADIUS key, retry count, and response timeout time are omitted, the settings specified by the configuration commands `radius-server key`, `radius-server retransmit`, and `radius-server timeout` are used, respectively.

(b) When using a general-use RADIUS server

For details about the settings for a general-use RADIUS server, see *8. Login Security and RADIUS* in the *Configuration Guide Vol. 1*.

7.2.2 Configuring the transmission of accounting information

Points to note

The example below shows how to specify that IEEE 802.1X accounting information be sent to the RADIUS server.

Command examples

1. `(config)# aaa accounting dot1x default start-stop group radius`

   Specifies the transmission of accounting information to the RADIUS server.

7.2.3 Enabling IEEE 802.1X

Points to note

The command below enables IEEE 802.1X authentication in global configuration mode. You cannot execute other IEEE 802.1X-related commands unless you execute this command first.

Command examples

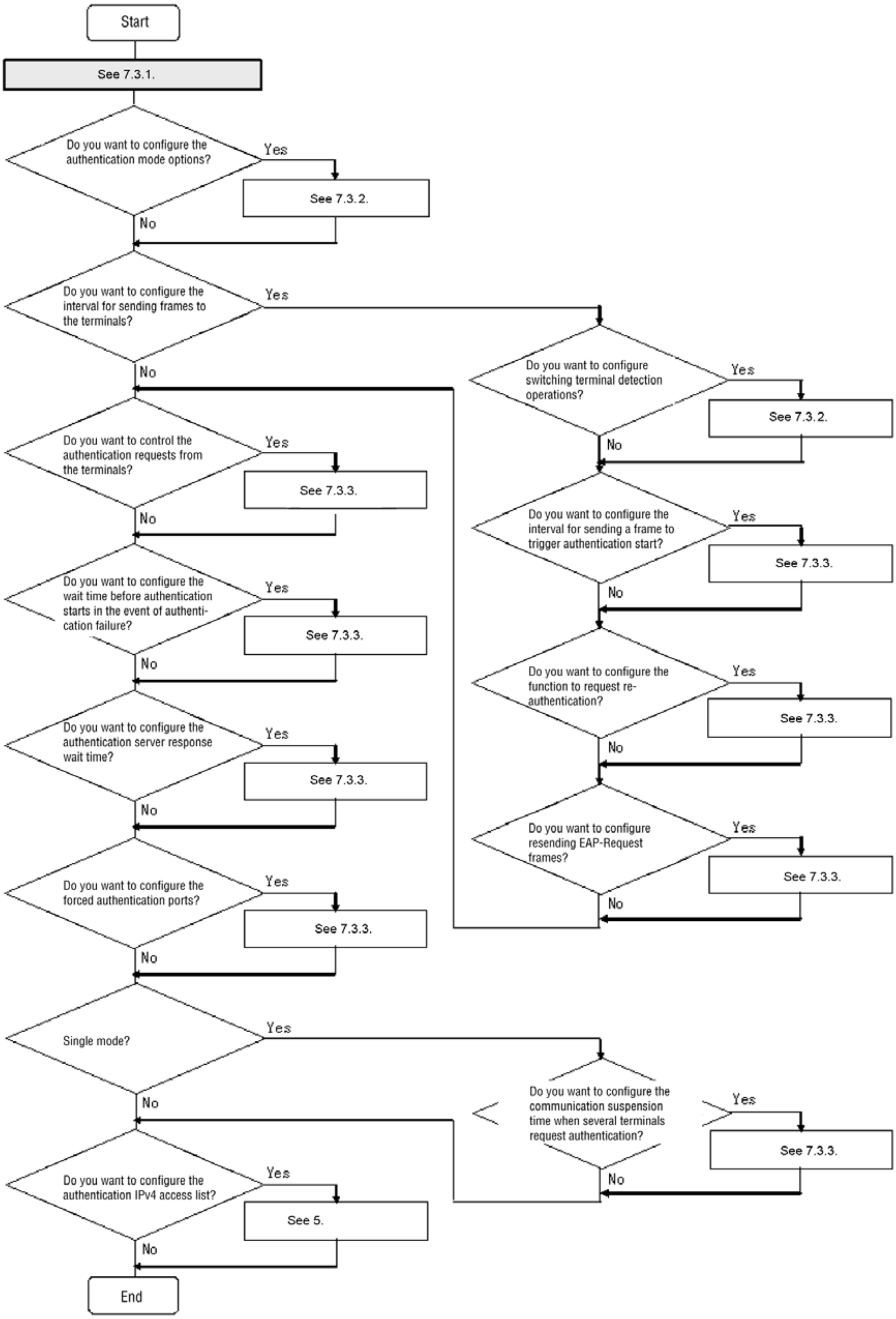
1. `(config)# dot1x system-auth-control`

   Enables IEEE 802.1X.

7.3 Configuring port-based authentication (static)

Configure port-based authentication (static) according to the following flow chart after the configuration based on *7.1 IEEE 802.1X configuration* and *7.2 Configuration common to all authentication modes.*

Figure 7-2 Configuration procedure of port-based authentication (static)



For details about the configuration, see the following:

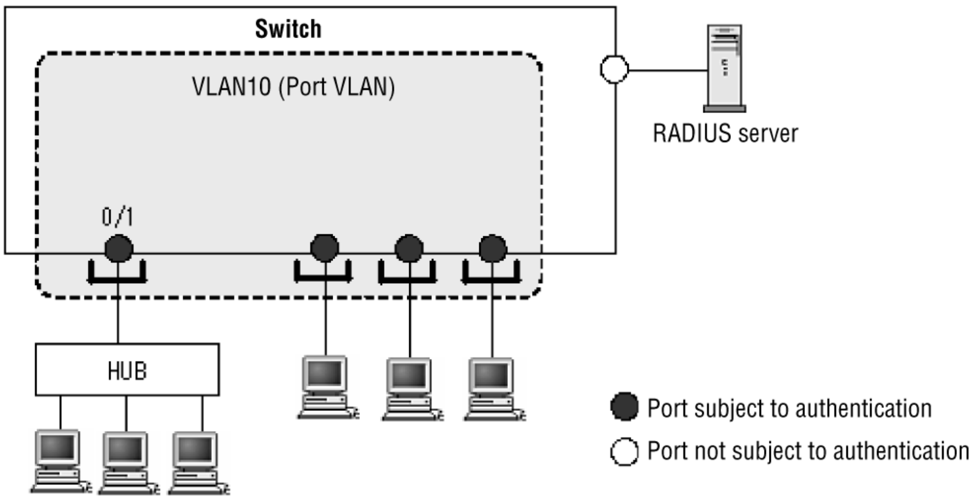
1. Configuring port-based authentication (static): *7.3.1 Configuring port-based authentication (static)*
2. Configuring authentication mode options: *7.3.2 Configuring authentication mode options*
3. Configuring the transmission interval of the frames sent to terminals
    - Switching terminal detection modes: *(2) Switching the terminal detection mode* in *7.3.2 Configuring authentication mode options*
    - Controlling the transmission of the frame that prompts authentication to start: *(1) Configuring the transmission interval of the frame that prompts a terminal to start authentication* in *7.3.3 Configuration related to authentication processing*
    - Functionality for requesting terminal re-authentication: *(2) Configuring the functionality for requesting terminal re-authentication* in *7.3.3 Configuration related to authentication processing*
    - Retransmission of EAP-Request frames: *(3) Configuring the retransmission of EAP-Request frames to terminals* in *7.3.3 Configuration related to authentication processing*
4. Configuring the suppression of authentication requests from terminals: *(4) Configuring the functionality for suppressing authentication requests from terminals* in *7.3.3 Configuration related to authentication processing*
5. Configuring the idle period for terminals that fail authentication: *(5) Configuring the idle period for terminals that fail authentication* in *7.3.3 Configuration related to authentication processing*
6. Configuring a timeout period for responses from the authentication server: *(6) Configuring a timeout period for responses from the authentication server* in *7.3.3 Configuration related to authentication processing*
7. Configuring forced authentication ports: *(8) Configuring a forced authentication port* in *7.3.3 Configuration related to authentication processing*
8. Configuring traffic blocking in response to authentication requests from multiple terminals: *(7) Configuring traffic blocking in response to authentication requests from multiple terminals* in *7.3.3 Configuration related to authentication processing*
9. Configuring the authentication IPv4 access list: *5.5.2 Configuring the authentication IPv4 access list*

7.3.1 Configuring port-based authentication (static)

(1) Configuring authentication ports and VLAN information for authentication

This step designates a physical port or channel group as an authenticating port.

Figure 7-3 Configuration example of port-based authentication (static)



Points to note

This procedure configures a port as an access port, and then enables port-based authentication (static) for the port. You then specify the authentication submode. If you omit the authentication submode setting, the port will operate in single-terminal mode.

Command examples

1. `(config)# vlan 10`

   `(config-vlan)# exit`

   Specifies VLAN ID 10.

2. `(config)# interface fastethernet 0/1`

   `(config-if)# switchport mode access`

   `(config-if)# switchport access vlan 10`

   Specifies port 0/1 as an access port and VLAN ID 10.

3. `(config-if)# dot1x multiple-authentication`

   Specifies terminal authentication mode as the authentication submode.

4. `(config-if)# dot1x port-control auto`

   `(config-if)# exit`

   Enables port-based authentication.

(2) Configuring the name of the method list for port-based authentication

Points to note

The example below shows how to configure the name of the method list for port-based authentication.

For details about setting authentication method lists, see *(1) Configuring the authentication method group* in *7.2.1 Configuring the authentication method group and RADIUS server information.*

Command examples

1.
```
(config)# interface fastethernet 0/1
(config-if)# dot1x authentication DOT1X-list1
(config-if)# exit
```
Specifies the authentication method list name `DOT1X-list1` for port 0/1.

Notes

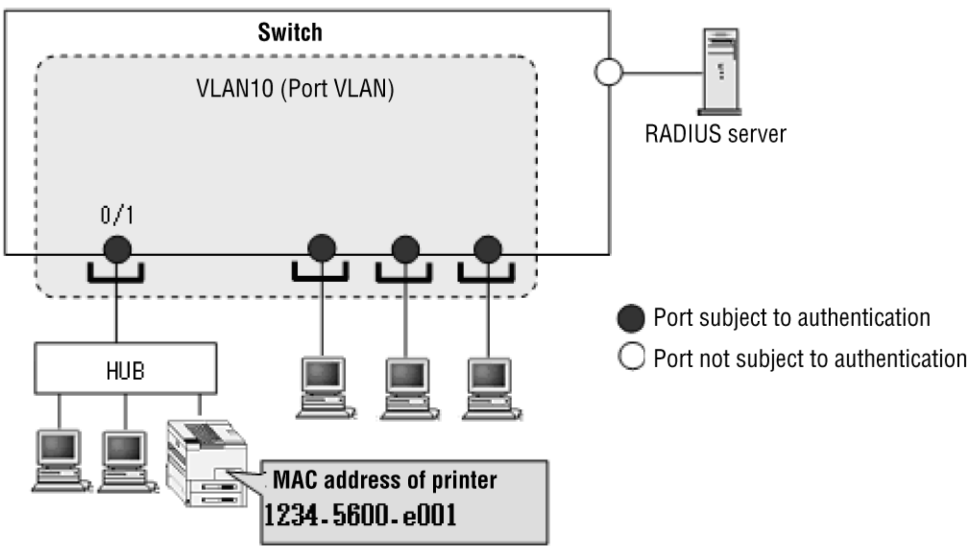
- If this information has not been configured, authentication follows the Switch default in *(1) Configuring the authentication method group* in *7.2.1 Configuring the authentication method group and RADIUS server information.*
- When a name of an authentication method list set for a port does not match the name of an authentication method list of an authentication method group or is not present in an authentication method group, authentication is performed according to the device default.
- Port-based authentication (dynamic) cannot be configured at the same time as the user-ID-based authentication method for Web authentication or VLAN-based authentication (dynamic). For details, see *5.2.2 Authentication method list.*

7.3.2 Configuring authentication mode options

(1) Configuring authentication exclusion options

This step specifies, by MAC address, a terminal that the Switch allows to bypass authentication. You can use this option to allow network access for devices that do not support IEEE 802.1X. The example below connects a printer that is allowed unauthenticated access (MAC address: 1234.5600.e001) to port 0/1, which was configured above in *7.3.1 Configuring port-based authentication (static).*

Figure 7-4 Configuration example of authentication exclusion for port-based authentication (static)



Points to note

The example below shows how to register a static entry in the MAC address table for port-based authentication (static).

Command examples

1. `(config)# mac-address-table static 1234.5600.e001 vlan 10 interface fastethernet 0/1`

   Adds the MAC address (`1234.5600.e001`) for which you want to permit unauthenticated access to VLAN ID 10 at port 0/1 to the MAC address table.

(2) Switching the terminal detection mode

The Switch sends EAP-Request/Identity packets to the multicast address at the interval specified by the `tx-period` command to prompt terminals to begin an authentication sequence. This procedure specifies what form of authentication sequence takes place when a terminal that is already authenticated responds to an EAP-Request/Identity packet. By default, such terminals do not participate in authentication.

Points to note

- In `shortcut` mode, the authentication sequence is abbreviated to reduce the load on the Switch.
- In `disable` mode, the Switch does not send regular EAP-Request/Identity packets if authenticated terminals are present on the port.
- The `auto` setting sends an EAP-Request/Identity packet only to a new terminal when an ARP/IP frame is received from it.

Command examples (`shortcut`)

1.
```
(config)# interface fastethernet 0/1
(config-if)# dot1x multiple-authentication
(config-if)# dot1x port-control auto
(config-if)# dot1x supplicant-detection shortcut
(config-if)# exit
```

   Specifies that re-authentication is skipped and that authentication is considered successful when an EAP-Response/Identity packet is received from an authenticated terminal at port 0/1.

Command examples (`auto`)

1.
```
(config)# interface fastethernet 0/1
(config-if)# dot1x multiple-authentication
(config-if)# dot1x port-control auto
(config-if)# dot1x supplicant-detection auto
(config-if)# exit
```

   Specifies that an EAP-Request/Identity packet is sent only to a target terminal at port 0/1 when an ARP/IP frame is received from a new terminal.

7.3.3 Configuration related to authentication processing

(1) Configuring the transmission interval of the frame that prompts a terminal to start authentication

This configuration specifies the interval at which the Switch transmits EAP-Request/Identity packets to prompts authentication for a terminal that does not begin authentication by itself.

Points to note

This functionality sends EAP-Request/Identity packets to the multicast address at the interval specified by the `tx-period` timer. Because authenticated terminals also respond to an EAP-Response/Identity packet, specify a value that satisfies the following expression to ensure that the Switch does not become overloaded.

reauth-period > tx-period ≥ (*total-number-of-terminals-to-be-authenticated-on-Switch* / 20) × 2

The default value of `tx-period` is 30 seconds. Therefore, in an environment where the Switch authenticates 300 or more terminals, you need to change the value of the `tx-period` timer.

Command examples

1.
```
(config)# interface fastethernet 0/1
(config-if)# dot1x timeout tx-period 300
(config-if)# exit
```

Specifies a 300-second interval for the transmission of EAP-Request/Identity packets to port 0/1 configured for port-based authentication.

(2) Configuring the functionality for requesting terminal re-authentication

Because the authentication of a terminal that is removed from the network after authentication cannot be canceled from the Switch, re-authentication is requested from authenticated terminals. If no response is received, the authentication of the terminal is canceled.

Points to note

This procedure configures the Switch to transmit an EAP-Request/Identity message to each authenticated terminal at the interval specified by the `reauth-period` timer. Make sure that the value of the `reauth-period` timer is greater than the value of the `tx-period` timer.

Command examples

1.
```
(config)# interface fastethernet 0/1
(config-if)# dot1x reauthentication
(config-if)# dot1x timeout reauth-period 360
(config-if)# exit
```

Enables the re-authentication request functionality at port 0/1, and then sets the re-authentication interval to 360 seconds.

(3) Configuring the retransmission of EAP-Request frames to terminals

This procedure specifies how long the Switch should wait for a terminal to respond to an EAP-Request frame (a request message from the authentication server) before resending the request, and the maximum number of times that the Switch resends the request.

Points to note

Make sure that the product of the resending interval multiplied by the number of retransmissions does not exceed the value specified for the `reauth-period` timer.

Command examples

1. `(config)# interface fastethernet 0/1`

   `(config-if)# dot1x timeout supp-timeout 60`

   Specifies a retransmission period of 60 seconds for EAP-Request frames at port 0/1.

2. `(config-if)# dot1x max-req 3`

   `(config-if)# exit`

   Specifies that EAP-Request frames be retransmitted a maximum of three times at port 0/1.

(4) Configuring the functionality for suppressing authentication requests from terminals

You can prevent an authentication from being initiated by EAPOL-Start frames from terminals. With this functionality enabled, the authentication of new terminals and re-authentication of existing terminals take place at the intervals specified by the `tx-period` timer and `reauth-period` timer, respectively.

Points to note

This functionality reduces the load on the Switch in situations where a large number of terminals send re-authentication requests over a short period. You cannot execute the commands below unless you execute the `dot1x reauthentication` command first.

Command examples

1. `(config)# interface fastethernet 0/1`

   `(config-if)# dot1x reauthentication`

   `(config-if)# dot1x ignore-eapol-start`

   `(config-if)# exit`

   Prevents authentication processing from being initiated in response to EAPOL-Start frames received at port 0/1.

(5) Configuring the idle period for terminals that fail authentication

This procedure configures how long a terminal that fails authentication must remain idle before it can try again.

Points to note

This configuration prevents a situation in which the Switch becomes overloaded by a large number of authentication requests received over a short period from terminals that fail authentication.

Note that the idle period you specify also applies to users who fail authentication because they enter the wrong user name or password.

Command examples

1.
```
(config)# interface fastethernet 0/1
(config-if)# dot1x timeout quiet-period 300
(config-if)# exit
```

Specifies an idle period of 300 seconds before terminals attached to port 0/1 configured for port-based authentication can retry the authentication process.

(6) Configuring a timeout period for responses from the authentication server

This procedure configures how long the Switch waits for the authentication server to respond to a request. When the specified time has elapsed, the Switch notifies the Supplicant that authentication has failed. The Supplicant learns of the failed authentication after the shorter of the times specified in the commands below and the total time including retransmissions specified by the attributes of the `radius-server` configuration command.

Points to note

When multiple RADIUS servers are configured by using the `radius-server` configuration command, and you specify a shorter time than the total wait time, including retransmissions by each server, the Supplicant will be notified that authentication has failed before the Switch can send requests to all the authentication servers. If you want this notification to wait until the Switch has failed to obtain a response from all of the configured authentication servers, be sure to specify a longer value for this command.

Command examples

1.
```
(config)# interface fastethernet 0/1
(config-if)# dot1x timeout server-timeout 300
(config-if)# exit
```

Specifies a 300-second timeout period for responses from the authentication server at port 0/1 configured for port-based authentication.

(7) Configuring traffic blocking in response to authentication requests from multiple terminals

This procedure specifies how long to block traffic at a port configured for port-based authentication in single-terminal mode in the event that the port receives authentication requests from multiple terminals.

Points to note

The example below shows how to specify how long to block traffic at a target port when it detects authentication requests from multiple terminals.

Command examples

1.
```
(config)# interface fastethernet 0/1
```

```
(config-if)# dot1x timeout keep-unauth 1800
(config-if)# exit
```

Specifies that port 0/1 configured for port-based authentication blocks traffic for 1800 seconds.

(8) Configuring a forced authentication port

Points to note

This procedure allows forced authentication at a port for port-based authentication (static).

Command examples

1.
```
(config)# interface fastethernet 0/1
(config-if)# dot1x force-authorized
(config-if)# exit
```

Specifies port 0/1 as a forced authentication port.

2.
```
(config)# dot1x force-authorized eapol
```

Sends the EAPOL-Success response frame from the Switch to the terminal when it is forcibly authenticated.

(9) Configuring the conditions for automatic cancellation of authentication

(a) Configuring the functionality to monitor non-communication of an authenticated terminal

When port-based authentication (static) or port-based authentication (dynamic) is enabled, this functionality is enabled even if the `dot1x auto-logout` configuration command is not specified. In port-based authentication (static), non-communication monitoring is performed for quarantined and authenticated terminals.

If `no dot1x auto-logout` is specified with the configuration command, authentication is not canceled automatically.

(b) Configuring the monitoring of MAC address table aging

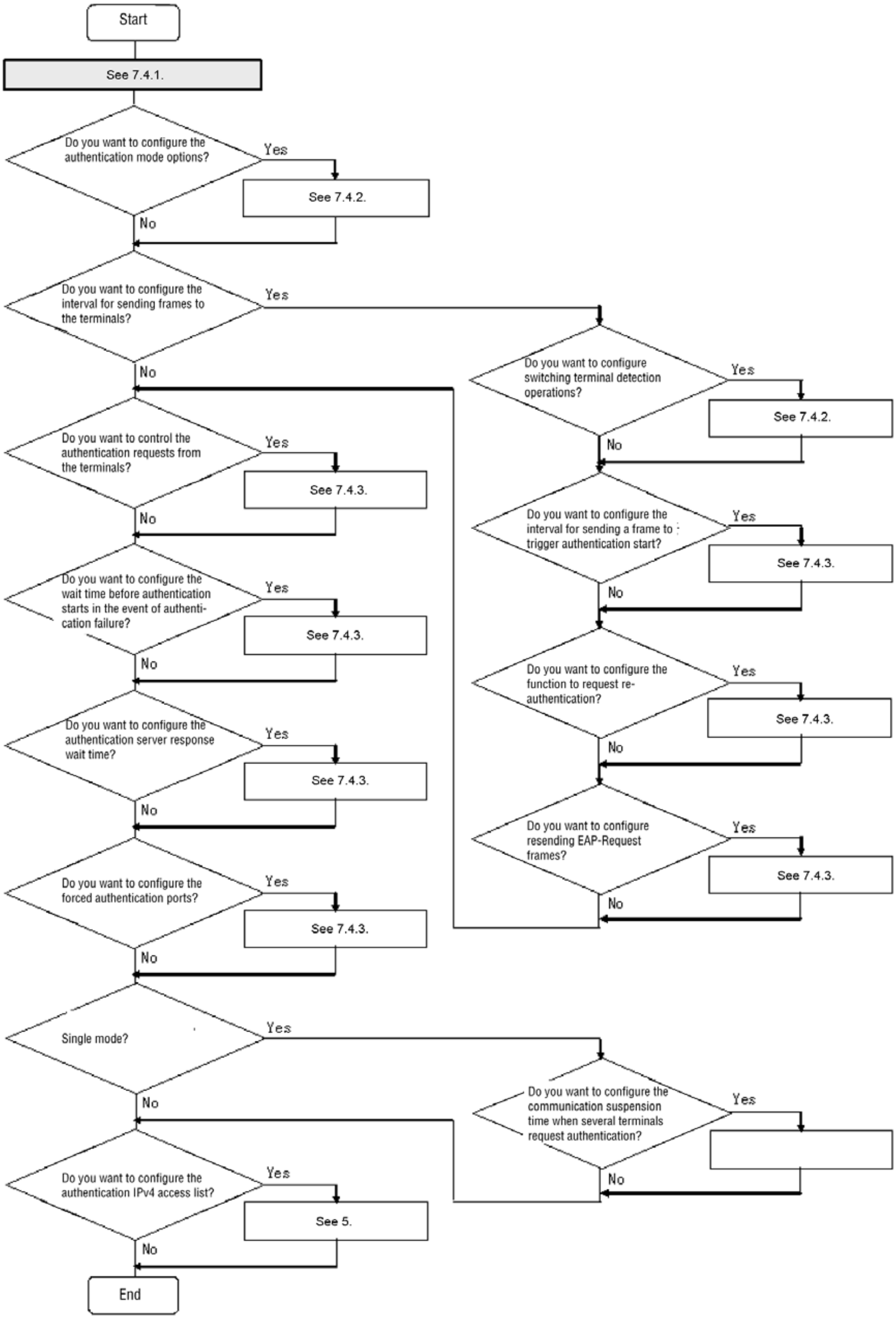
When port-based authentication (static) or VLAN-based authentication (dynamic) is enabled, this functionality is enabled even if the `dot1x auto-logout` configuration command is not specified. In port-based authentication (static), MAC address table aging is monitored for terminals in a quarantine state.

If `no dot1x auto-logout` is specified with the configuration command, authentication is not canceled automatically.

7.4 Configuring port-based authentication (dynamic)

Configure port-based authentication (dynamic) according to the following flow chart after the configuration based on *7.1 IEEE 802.1X configuration* and *7.2 Configuration common to all authentication modes.*

Figure 7-5 Configuration procedure of port-based authentication (dynamic)



For details about the configuration, see the following:

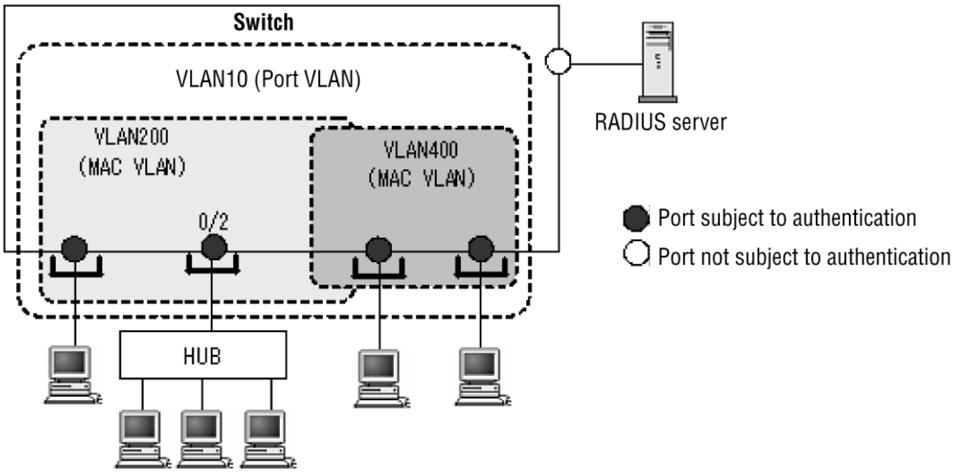
1. Configuring port-based authentication (static): *7.4.1 Configuring port-based authentication (dynamic)*
2. Configuring authentication mode options: *7.4.2 Configuring authentication mode options*
3. Configuring the transmission interval of the frames sent to terminals
    - Switching terminal detection modes: *(2) Switching the terminal detection mode* in *7.4.2 Configuring authentication mode options*
    - Controlling the transmission of the frame that prompts authentication to start: *(1) Configuring the transmission interval of the frame that prompts a terminal to start authentication* in *7.4.3 Configuration related to authentication processing*
    - Functionality for requesting terminal re-authentication: *(2) Configuring the functionality for requesting terminal re-authentication* in *7.4.3 Configuration related to authentication processing*
    - Retransmission of EAP-Request frames: *(3) Configuring the retransmission of EAP-Request frames to terminals* in *7.4.3 Configuration related to authentication processing*
4. Configuring the suppression of authentication requests from terminals: *(4) Configuring the functionality for suppressing authentication requests from terminals* in *7.4.3 Configuration related to authentication processing*
5. Configuring the idle period for terminals that fail authentication: *(5) Configuring the idle period for terminals that fail authentication* in *7.4.3 Configuration related to authentication processing*
6. Configuring a timeout period for responses from the authentication server: *(6) Configuring a timeout period for responses from the authentication server* in *7.4.3 Configuration related to authentication processing*
7. Configuring forced authentication ports: *(8) Configuring a forced authentication port* in *7.4.3 Configuration related to authentication processing*
8. Configuring traffic blocking in response to authentication requests from multiple terminals: *(7) Configuring traffic blocking in response to authentication requests from multiple terminals* in *7.4.3 Configuration related to authentication processing*
9. Configuring the authentication IPv4 access list: *5.5.2 Configuring the authentication IPv4 access list*

7.4.1 Configuring port-based authentication (dynamic)

(1) Configuring an authentication port and VLAN information for authentication

This procedure designates a physical port as an authenticating port.

Figure 7-6 Configuration example of port-based authentication (dynamic)



Points to note

The example below shows how to configure a MAC VLAN and a MAC port, and enable VLAN-based authentication (dynamic) for the port. You then specify the authentication submode. If you omit the authentication submode setting, the port will operate in single-terminal mode.

Command examples

1.
```
(config)# vlan 200,400 mac-based
(config-vlan)# exit
```
Configures VLAN ID 200, 400 as a MAC VLAN.

2.
```
(config)# vlan 10
(config-vlan)# exit
```
Specifies VLAN ID 10.

3.
```
(config)# interface fastethernet 0/2
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 10
```
Sets port 0/2 where terminals for authentication are connected as a MAC port, and sets VLAN 10 for pre-authentication. (The post-authentication VLAN is assigned according to *5.4.3 Auto VLAN assignment for a MAC VLAN*.)

4.
```
(config-if)# dot1x multiple-authentication
```
Specifies terminal authentication mode as the authentication submode.

5.
```
(config-if)# dot1x port-control auto
(config-if)# exit
```
Enables port-based authentication (dynamic).

(2) Configuring the name of the method list for port-based authentication

Points to note

This procedure configures the name of the method list for the port-based authentication.

For details about setting authentication method lists, see *(1) Configuring the authentication method group* in *7.2.1 Configuring the authentication method group and RADIUS server information*.

Command examples

1.
```
(config)# interface fastethernet 0/2
(config-if)# dot1x authentication DOT1X-list1
(config-if)# exit
```

Specifies the authentication method list name `DOT1X-list1` for port 0/2.

Notes

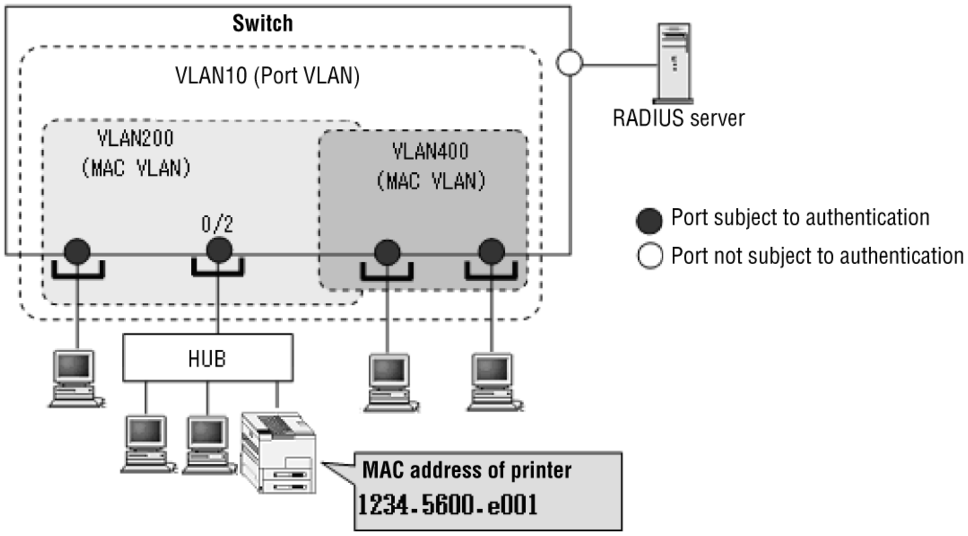
- If this information has not been configured, authentication follows the Switch default in *(1) Configuring the authentication method group* in *7.2.1 Configuring the authentication method group and RADIUS server information.*
- When a name of an authentication method list specified for a port does not match the name of an authentication method list of an authentication method group or is not present in an authentication method group, authentication is performed according to the device default.
- Port-based authentication (dynamic) cannot be configured at the same time as the user-ID-based authentication method for Web authentication or VLAN-based authentication (dynamic). For details, see *5.2.2 Authentication method list.*

7.4.2 Configuring authentication mode options

(1) Configuring authentication exclusion options

This procedure specifies the MAC address of a terminal that the Switch allows to bypass authentication. You can use this option to allow network access for devices that do not support IEEE 802.1X. The example below connects a printer that is allowed unauthenticated access (MAC address: 1234.5600.e001) to port 0/2, which was configured above in *7.4.1 Configuring port-based authentication (dynamic).*

Figure 7-7 Configuration example of authentication exclusion for port-based authentication (dynamic)



Points to note

The example below shows how to register a static entry in the MAC address table and MAC VLAN for port-based authentication (dynamic).

Command examples

1.
```
(config)# vlan 200 mac-based
(config-vlan)# mac-address 1234.5600.e001
(config-vlan)# exit
```
Specifies that the MAC address (`1234.5600.e001`) be allowed to access VLAN ID 200. The printer can now access VLAN ID 200 without performing IEEE 802.1X authentication.

2.
```
(config)# interface fastethernet 0/2
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 200
(config-if)# exit
```
Specifies MAC VLAN ID 200 to which the exempted terminal belongs for an authentication port.

3.
```
(config)# mac-address-table static 1234.5600.e001 vlan 200
interface fastethernet 0/2
```
Adds the MAC address (`1234.5600.e001`) for which you want to permit unauthenticated access to VLAN ID 200 at port 0/2 to the MAC address table.

Notes

Before adding the MAC address of a terminal excluded from authentication to the MAC address table, set the VLAN ID of MAC VLAN to the port to which the terminal belongs.

(2) Switching the terminal detection mode

This procedure is the same as for port-based authentication (static). For details, see*(2) Switching the terminal detection mode* in *7.3.2 Configuring authentication mode options.*

7.4.3 Configuration related to authentication processing

(1) Configuring the transmission interval of the frame that prompts a terminal to start authentication

This procedure is the same as for port-based authentication (static). For details, see *(1) Configuring the transmission interval of the frame that prompts a terminal to start authentication* in *7.3.3 Configuration related to authentication processing.*

(2) Configuring the functionality for requesting terminal re-authentication

This procedure is the same as for port-based authentication (static). For details, see *(2) Configuring the functionality for requesting terminal re-authentication* in *7.3.3 Configuration related to authentication processing.*

(3) Configuring the retransmission of EAP-Request frames to terminals

This procedure is the same as for port-based authentication (static). For details, see *(3) Configuring the retransmission of EAP-Request frames to terminals* in *7.3.3 Configuration related to authentication processing.*

(4) Configuring the functionality for suppressing authentication requests from terminals

This procedure is the same as for port-based authentication (static). For details, see *(4) Configuring the functionality for suppressing authentication requests from terminals* in *7.3.3 Configuration related to authentication processing*.

(5) Configuring the idle period for terminals that fail authentication

This procedure is the same as for port-based authentication (static). For details, see *(5) Configuring the idle period for terminals that fail authentication* in *7.3.3 Configuration related to authentication processing.*

(6) Configuring a timeout period for responses from the authentication server

This procedure is the same as for port-based authentication (static). For details, see *(6) Configuring a timeout period for responses from the authentication server* in *7.3.3 Configuration related to authentication processing*.

(7) Configuring traffic blocking in response to authentication requests from multiple terminals

This procedure is the same as for port-based authentication (static). For details, see *(7) Configuring traffic blocking in response to authentication requests from multiple terminals* in *7.3.3 Configuration related to authentication processing*.

(8) Configuring a forced authentication port

Points to note

This procedure allows forced authentication at a port for port-based authentication (dynamic) and specifies the post-authentication VLAN to be assigned.

Command examples

1. `(config)# interface fastethernet 0/2`

   `(config-if)# dot1x force-authorized vlan 200`

   `(config-if)# exit`

   Allows forced authentication at port 0/2 and specifies the VLAN ID of the post-authentication VLAN to be assigned.

2. `(config)# dot1x force-authorized eapol`

   Sends the EAPOL-Success response frame from the Switch to the terminal when it is forcibly authenticated.

(9) Configuring the conditions for automatic cancellation of authentication

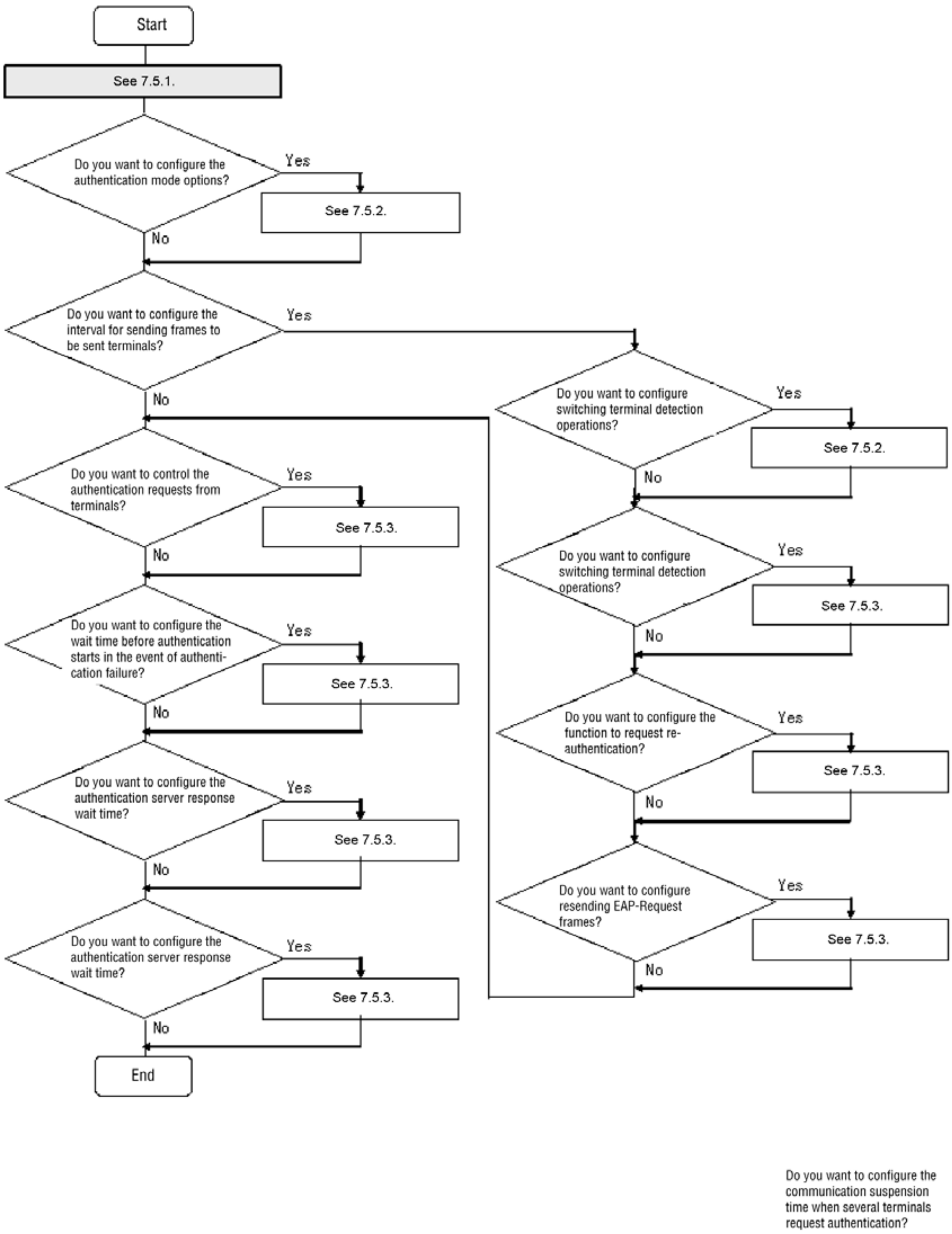
(a) Configuring the functionality to monitor non-communication of an authenticated terminal

This functionality cancels the status of an authenticated terminal. The procedure is the same as for configuring the non-communication monitoring functionality of port-based authentication (static). For details, see *(a) Configuring the functionality to monitor non-communication of an authenticated terminal* in *(9) Configuring the conditions for automatic cancellation of authentication* in *7.3.3 Configuration related to authentication processing.*

7.5 Configuring VLAN-based authentication (dynamic)

After performing configuration according to *7.1 IEEE 802.1X configuration* and *7.2 Configuration common to all authentication modes*, configure VLAN-based authentication (dynamic) by performing the procedure in the following figure.

Figure 7-8 Configuration procedure of VLAN-based authentication (dynamic)



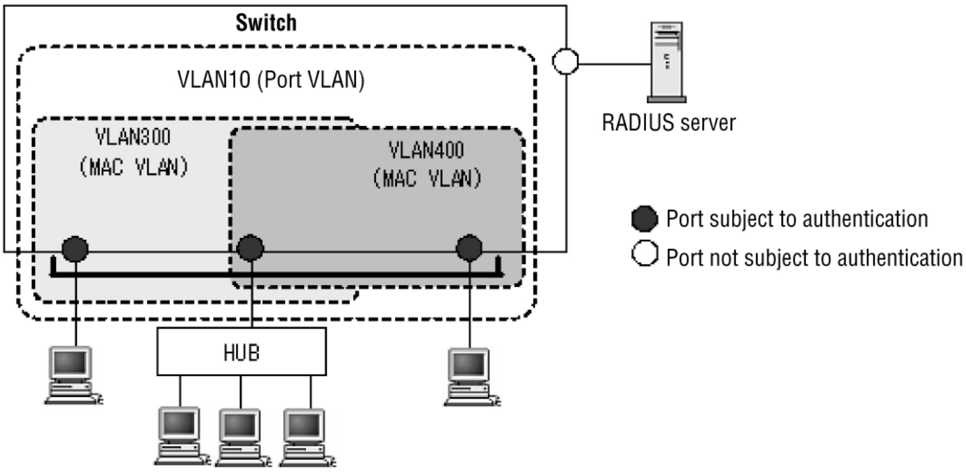
For details about the configuration, see the following:

1. Configuring port-based authentication (static): *7.5.1 Configuring VLAN-based authentication (dynamic)*
2. Configuring authentication mode options: *7.5.2 Configuring authentication mode options*
3. Configuring the transmission interval of the frames sent to terminals
   - Switching terminal detection modes: *7.5.2 Configuring authentication mode options*
   - Controlling the transmission of the frame that prompts authentication to start: *(1) Configuring the transmission interval of the frame that prompts a terminal to start authentication* in *7.5.3 Configuration related to authentication processing*
   - Functionality for requesting terminal re-authentication: *(2) Configuring the functionality for requesting terminal re-authentication* in *7.5.3 Configuration related to authentication processing*
   - Retransmission of EAP-Request frames: *(3) Configuring the retransmission of EAP-Request frames to terminals* in *7.5.3 Configuration related to authentication processing*
4. Configuring the suppression of authentication requests from terminals: *(4) Configuring the functionality for suppressing authentication requests from terminals* in *7.5.3 Configuration related to authentication processing*
5. Configuring the idle period for terminals that fail authentication: *(5) Configuring the idle period for terminals that fail authentication* in *7.5.3 Configuration related to authentication processing*
6. Configuring a timeout period for responses from the authentication server: *(6) Configuring a timeout period for responses from the authentication server* in *7.5.3 Configuration related to authentication processing*
7. Configuring forced authentication ports: *(7) Configuring a forced authentication port* in *7.5.3 Configuration related to authentication processing*

7.5.1 Configuring VLAN-based authentication (dynamic)

This functionality authenticates terminals belonging to a MAC VLAN.

Figure 7-9 Configuration example using VLAN-based authentication (dynamic)



Points to note

This procedure configures a MAC VLAN, and then enables VLAN-based authentication (dynamic) for that VLAN.

Register authenticated terminals according to the VLAN specified by the RADIUS server. Additionally, register the list of VLANs specified by the RADIUS server with the `dot1x vlan dynamic radius-vlan` configuration command.

Command examples

1. `(config)# vlan 300,400 mac-based`

   `(config-vlan)# exit`

   Configures VLAN ID 300, 400 as a MAC VLAN.

2. `(config)# vlan 10`

   `(config-vlan)# exit`

   Specifies VLAN ID 10.

3. `(config)# dot1x vlan dynamic radius-vlan 300,400`

   Specifies VLAN ID 300, 400 for VLAN-based authentication (dynamic).

4. `(config)# aaa authorization network default group radius`

   Registers according to the VLAN specified by the RADIUS server.

5. `(config)# dot1x vlan dynamic enable`

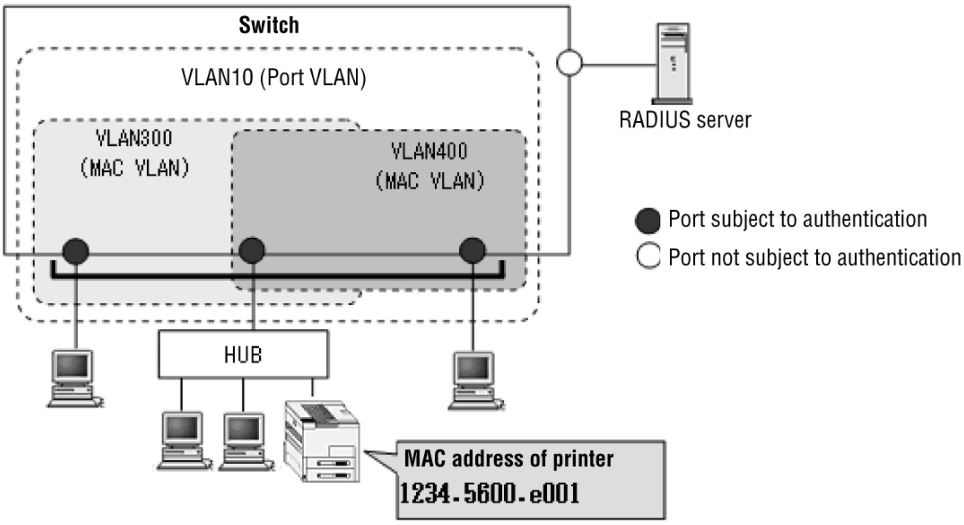
   Enables VLAN-based authentication (dynamic).

7.5.2 Configuring authentication mode options

(1) Configuring authentication exclusion options

This procedure specifies the MAC address of a terminal that the Switch allows to bypass authentication. You can use this option to allow network access for devices that do not support IEEE 802.1X. The example below connects a printer that is allowed unauthenticated access (MAC address:1234.5600.e001) to VLAN ID 300, which was configured above in *7.5.1 Configuring VLAN-based authentication (dynamic).*

Figure 7-10 Configuration example of authentication exclusion for VLAN-based authentication (dynamic)



Points to note

This configuration registers a MAC address in a MAC VLAN for VLAN-based authentication (dynamic).

Command examples

1.
```
(config)# vlan 300 mac-based
(config-vlan)# mac-address 1234.5600.e001
(config-vlan)# exit
```

Specifies the MAC address `(1234.5600.e001)` that is allowed to access the MAC VLAN with VLAN ID 300. The printer can now access VLAN ID 300 without performing IEEE 802.1X authentication.

(2) Switching the terminal detection mode

The Switch sends EAP-Request/Identity packets to the multicast address at the interval specified by the `tx-period` command to prompt terminals to begin an authentication. This procedure specifies what form of authentication sequence takes place when a terminal that is already authenticated responds to an EAP-Request/Identity packet. By default, such terminals do not participate in authentication.

Points to note

- In `shortcut` mode, the authentication sequence is abbreviated to reduce the load on the Switch.

- In `disable` mode, the Switch does not send regular EAP-Request/Identity packets if authenticated terminals are present on the port.

The `auto` setting cannot be specified for VLAN-based authentication (dynamic).

Command examples

1. `(config)# dot1x vlan dynamic supplicant-detection shortcut`

   Specifies that re-authentication is skipped and that authentication is considered successful when an EAP-Response/Identity packet is received from a terminal authenticated by VLAN-based authentication (dynamic).

7.5.3 Configuration related to authentication processing

(1) Configuring the transmission interval of the frame that prompts a terminal to start authentication

This configuration specifies the interval at which the Switch transmits EAP-Request/Identity packets to prompt authentication for a terminal that does not begin authentication by itself.

Points to note

This functionality sends EAP-Request/Identity packets to the multicast address at the interval specified by the `tx-period` timer. Because authenticated terminals also respond to an EAP-Response/Identity packet, specify a value that satisfies the following expression to ensure that the Switch does not become overloaded.

reauth-period > tx-period ≥ (*total-number-of-terminals-to-be-authenticated-on-Switch* / 20) × 2

The default value of `tx-period` is 30 seconds. Therefore, in an environment where the Switch authenticates 300 or more terminals, you need to change the value of the `tx-period` timer.

Command examples

1. `(config)# dot1x vlan dynamic timeout tx-period 300`

   Specifies a 300-second interval for the transmission of EAP-Request/Identity packets for VLAN-based authentication (dynamic).

(2) Configuring the functionality for requesting terminal re-authentication

Because the authentication of a terminal that is removed from the network after authentication cannot be canceled from the Switch, re-authentication is requested from authenticated terminals. If no response is received, the authentication of the terminal is canceled.

Points to note

This procedure configures the Switch to transmit an EAP-Request/Identity message to each authenticated terminal at the interval specified by the `reauth-period` timer. Make sure that the value of the `reauth-period` timer is greater than the value of the `tx-period` timer.

Command examples

1. `(config)# dot1x vlan dynamic reauthentication`

   `(config)# dot1x vlan dynamic timeout reauth-period 360`

   Enables the re-authentication functionality for terminals subject to VLAN-based authentication (dynamic), and then sets the re-authentication interval to 360 seconds.

(3) Configuring the retransmission of EAP-Request frames to terminals

This procedure specifies how long the Switch should wait for a terminal to respond to an EAP-Request frame before resending the request, and the maximum number of times that the Switch resends the request.

Points to note

Make sure that the product of the resending interval multiplied by the number of retransmissions does not exceed the value specified for the `reauth-period` timer.

Command examples

1. `(config)# dot1x vlan dynamic timeout supp-timeout 60`

   Specifies a retransmission period of 60 seconds for EAP-Request frames for VLAN-based authentication (dynamic).

2. `(config)# dot1x vlan dynamic max-req 3`

   Specifies that EAP-Request frames are retransmitted a maximum of 3 times for VLAN-based authentication (dynamic).

(4) Configuring the functionality for suppressing authentication requests from terminals

You can prevent an authentication from being initiated by EAPOL-Start frames from terminals. With this functionality enabled, the authentication of new terminals and re-authentication of existing terminals take place at the intervals specified by the `tx-period` timer and `reauth-period` timer, respectively.

Points to note

This functionality reduces the load on the Switch in situations where a large number of terminals send re-authentication requests over a short period. You cannot execute the commands below unless you execute the `dot1x reauthentication` command first.

Command examples

1. `(config)# dot1x vlan dynamic reauthentication`

   `(config)# dot1x vlan dynamic ignore-eapol-start`

   Prevents authentication processing from being initiated in response to EAPOL-Start frames received for VLAN-based authentication (dynamic).

(5) Configuring the idle period for terminals that fail authentication

This procedure configures how long a terminal that fails authentication must remain idle before it can try again.

Points to note

This configuration prevents a situation in which the Switch becomes overloaded by a large number of authentication requests received over a short period from terminals that fail authentication.

Note that the idle period you specify also applies to users who fail authentication because they enter the wrong user name or password.

Command examples

1. `(config)# dot1x vlan dynamic timeout quiet-period 300`

   Specifies an idle period of 300 seconds before terminals subject to VLAN-based authentication (dynamic) can retry the authentication process.

(6) Configuring a timeout period for responses from the authentication server

This procedure specifies how long the Switch waits for the authentication server to respond to a request. When the specified time has elapsed, the Switch notifies the supplicant that authentication has failed. The Supplicant learns of the failed authentication after the shorter of the times specified in the commands below and the total time including retransmissions specified by the attributes of the `radius-server` configuration command.

Points to note

When multiple RADIUS servers are configured by using the `radius-server` configuration command, and you specify a shorter time than the total wait time, including retransmissions by each server, the Supplicant will be notified that authentication has failed before the Switch can send requests to all the authentication servers. If you want this notification to wait until the Switch has failed to obtain a response from all of the configured authentication servers, be sure to specify a longer value for this command.

Command examples

1. `(config)# dot1x vlan dynamic timeout server-timeout 300`

   This procedure allows forced authentication at a port for VLAN-based authentication (dynamic).

(7) Configuring a forced authentication port

Points to note

This procedure allows forced authentication at a port for VLAN-based authentication (dynamic) and specifies the post-authentication VLAN to be assigned.

Command examples

1.
```
(config)# interface fastethernet 0/3
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 300
(config-if)# dot1x force-authorized vlan 300
(config-if)# exit
```

   Allows forced authentication at port 0/3 and specifies the VLAN ID of the post-authentication VLAN to be assigned.

2. `(config)# dot1x force-authorized eapol`

   Sends the EAPOL-Success response frame from the Switch to the terminal when it is forcibly authenticated.

(8) Configuring the conditions for automatic cancellation of authentication

(a) Configuring the monitoring of MAC address table aging

This functionality cancels the status of an authenticated terminal. The procedure is the same as when configuring the aging monitoring functionality for port-based authentication (static). For details, see *(b) Configuring the monitoring of MAC address table aging* in *(9) Configuring the conditions for automatic cancellation of authentication* in *7.3.3 Configuration related to authentication processing.*

7.6 IEEE 802.1X operation

7.6.1 List of operation commands

The following table shows the operation commands for IEEE 802.1X.

Table 7-3 List of operation commands

Command name	Description
`show dot1x`	Displays the status of each authentication unit and information about authenticated supplicants.
`show dot1x logging`	Displays the operation log messages collected by IEEE 802.1X authentication.
`show dot1x statistics`	Displays statistics about IEEE 802.1X authentication.
`clear dot1x auth-state`	Clears information related to authenticated terminals.
`clear dot1x logging`	Clears the operation log messages collected by IEEE 802.1X authentication.
`clear dot1x statistics`	Resets IEEE802.1X-related statistics to 0.
`reauthenticate dot1x`	Re-authenticates the status of IEEE 802.1X authentication.

7.6.2 Displaying the IEEE 802.1X status

(1) Displaying authentication statuses

Use the show `dot1x operation` command to display the status of IEEE 802.1X authentication.

(a) Displaying general status information

Execute the `show dot1x` operation command to display the status of an entire IEEE 802.1X device.

Figure 7-11 Output of show dot1x

```
> show dot1x

Date 2009/10/28 10:24:10 UTC
System 802.1X : Enable
   AAA Authentication Dot1x   : Enable
       Authorization Network  : Disable
       Accounting Dot1x       : Enable
                 Auto-logout  : Enable

Authentication Default      : RADIUS
Authentication port-list-DDD : RADIUS ra-group-3
Accounting Default          : RADIUS

Port/ChGr/VLAN    AccessControl  PortControl      Status      Supplicants
Port 0/1         ---            Auto          Authorized    1
Port 0/4(Dynamic)  Multiple-Auth  Auto              ---          1
```

```
ChGr 1           Multiple-Auth  Auto            ---         0

>
```

(b) Displaying the status of port-based authentication (static)

Use the `show dot1x port` operation command to display the status of each port in port-based authentication (static). Use the `show dot1x channel-group-number` operation command to view the status of each channel group.

- If you specify a port number, the command outputs status information for the specified port.
- Specify the `detail` parameter to include the information about terminals to be authenticated.

Figure 7-12 Output of show dot1x port command (with detail parameter specified)

```
> show dot1x port 0/1 detail

Date 2009/10/28 10:24:51 UTC
Port 0/1
AccessControl  : ---                    PortControl   : Auto
Status        : Authorized              Last EAPOL    : 0013.20a5.24ab
Supplicants    : 1 / 1                  ReAuthMode    : Disable
TxTimer       : 30                     ReAuthTimer   : 3600
ReAuthSuccess  : 0                      ReAuthFail    : 2
KeepUnauth     : 3600
Authentication : port-list-DDD
VLAN(s): 4

 Supplicants MAC  F  Status       AuthState     BackEndState   ReAuthSuccess
                  SessionTime(s) Date/Time                   SubState
 [VLAN 4]          Port(Static)  Supplicants : 1
 0013.20a5.24ab      Authorized     Authenticated  Idle          0
                  81          2009/10/28 10:23:30        Full

>
```

(c) Displaying the status of port-based authentication (dynamic)

Use the `show dot1x port` operation command to display the status of each port in port-based authentication.

- If you specify a port number, the command outputs status information for the specified port.
- Specify the `detail` parameter to include the information about the VLANs that terminals to be authenticated belong to and the information about the terminals.

Figure 7-13 Output of show dot1x port command (with detail parameter specified)

```
> show dot1x port 0/4 detail

Date 2009/10/28 10:25:15 UTC
Port 0/4 (Dynamic)
AccessControl  : Multiple-Auth           PortControl   : Auto
Status        : ---                    Last EAPOL    : 0013.20a5.3e4f
Supplicants    : 0 / 1 / 64               ReAuthMode    : Disable
TxTimer       : 30                     ReAuthTimer   : 3600
```

```
ReAuthSuccess  : 0                      ReAuthFail    : 1
SuppDetection  : Auto
Authentication : port-list-DDD
VLAN(s): 4,40

 Supplicants MAC  F  Status        AuthState     BackEndState   ReAuthSuccess
                  SessionTime(s) Date/Time                    SubState
 [Unauthorized]     Port(Unknown) Supplicants : 1
 0013.20a5.3e4f     Unauthorized   Connecting     Idle          0
                  2           2009/10/28 10:25:14        ---

>
```

(d) Displaying the status of VLAN-based authentication (dynamic)

Use the `show dot1x vlan dynamic` operation command to display the status of each VLAN in VLAN-based authentication (dynamic).

- If you specify a VLAN ID, the command outputs status information for the specified VLAN.
- Specify the `detail` parameter to include the information about the VLANs that terminals to be authenticated belong to and the information about the terminals.

Figure 7-14 Output of show dot1x vlan dynamic command (with detail parameter specified)

```
> show dot1x vlan dynamic detail

Date 2009/03/24 19:58:47 UTC
VLAN(Dynamic)
AccessControl  : Multiple-Auth          PortControl   : Auto
Status        : ---                  Last EAPOL    : 000a.799a.ddf0
Supplicants    : 1 / 1 / 256            ReAuthMode    : Disable
TxTimer       : 30                   ReAuthTimer   : 3600
ReAuthSuccess  : 0                      ReAuthFail    : 0
SuppDetection  : Shortcut
VLAN(s): 400

 Supplicants MAC  F  Status        AuthState     BackEndState   ReAuthSuccess
                  SessionTime(s) Date/Time
 [VLAN 400]        VLAN(Dynamic) Supplicants : 1
 000a.799a.ddf0     Authorized     Authenticated  Idle          0
                  46          2009/03/24 19:52:55

>
```

7.6.3 Changing the IEEE 802.1X authentication status

(1) Initializing the authentication status

Use the `clear dot1x auth-state` operation command to initialize the authentication status. You can specify a port number, VLAN ID, or terminal MAC address as the object of the command. If you omit this specification, the Switch will initialize all authentication information.

After you execute this command, affected terminals must undergo re-authentication before they can access the network again.

Figure 7-15 Example of initializing all IEEE 802.1X authentication statuses in the Switch

```
> clear dot1x auth-state
Do you wish to initialize all 802.1X authentication information? (y/n):y
```

(2) Forcing re-authentication

Use the `reauthenticate dot1x` operation command to force re-authentication. You can specify a port number, VLAN ID, or terminal MAC address as the object of the command. If you omit this specification, the Switch will force all authenticated terminals to undergo re-authentication.

Executing this command does not affect the network access of supplicants that are able to re-authenticate successfully.

Figure 7-16 Example of forcing re-authentication for all IEEE 802.1X-authenticated ports and VLANs in the Switch

```
> reauthenticate dot1x
Do you wish to reauthenticate all 802.1X ports and VLANs? (y/n):y
```

8. Description of Web Authentication

The Web authentication functionality controls access to VLANs by users authenticated from an ordinary Web browser. This chapter provides an overview of Web authentication.

8.1 Overview

In Web authentication, user authentication is based on a user ID and password that a user supplies through an ordinary Web browser, such as Internet Explorer (abbreviated hereafter to *Web browser*). The Switches change the status of the terminal to be authenticated on the basis of the MAC address of this authenticated user's terminal and grant terminal access to the post-authentication network.

Web authentication allows users to execute authentication using only a Web browser, without the need to install any special software on the terminal.

Web authentication also supports one-time password authentication using the SecurID mechanism engineered by RSA Security. For details about the one-time password authentication, see *14. One-time Password Authentication [OP-OTP].*

(1) Authentication mode

Web authentication includes the following authentication modes:

- Fixed VLAN mode

  Registers the MAC address of a successfully authenticated terminal in the MAC address table and allows access to the VLAN designated by the configuration for communication.

- Dynamic VLAN mode

  Registers the MAC address of a successfully authenticated terminal in the MAC VLAN and MAC address table. Terminals are given access to different VLANs before and after authentication.

- Legacy mode

  Performs VLAN switching via the MAC VLAN and enables terminals to access different VLANs before and after authentication.

(2) Authentication method group

You can configure the authentication method groups below for Web authentication. (The configured authentication method groups can be used in all Web authentication modes.)

- Switch default: Local authentication method

  This authentication method uses an authentication database stored on the Switch (called an internal MAC authentication DB).

- Switch default: RADIUS authentication method

  Authentication is performed by using a RADIUS server deployed on the network.

- Authentication method list

  Authentication is performed by using a RADIUS server group registered in the authentication method list when specific conditions are met.

(3) Authentication networks

Web authentication of the Switch supports IPv4 addresses only. Terminals seeking authentication must attach to a VLAN interface that has an IPv4 address.

(4) Supported functionality by authentication mode

The following table lists the supported functionality of each authentication mode.

Table 8-1 Supported functionality by authentication mode

Functionality		Fixed VLAN	Dynamic VLAN	Legacy
Switch default: Local authentication	Internal Web authentication DB	Y See *8.2.1*. See *8.6.1*.	Y See *8.3.1*. See *8.6.1*.	Y See *8.4.1*. See *8.6.1*.
	User ID	1 to 128 characters See *9.7.2*.	1 to 128 characters See *9.7.2*.	1 to 128 characters See *9.7.2*.
	Password	1 to 32 characters See *9.7.2*.	1 to 32 characters See *9.7.2*.	1 to 32 characters See *9.7.2*.
	VLAN (post-authentication VLAN)	Y See *9.7.2*.	Y See *9.7.2*.	Y See *9.7.2*.
Switch default: RADIUS authentication	External server ● RADIUS server information for Web authentication ● General-use RADIUS server information	Y See *5.3.1*. See *8.2.1*. See *8.6.2*. See *9.2.1*.	Y See *5.3.1*. See *8.3.1*. See *8.6.2*. See *9.2.1*.	Y See *5.3.1*. See *8.4.1*. See *8.6.2*. See *9.2.1*.
	User ID	1 to 128 characters See *8.2.1*. See *8.6.2*.	1 to 128 characters See *8.3.1*. See *8.6.2*.	1 to 128 characters See *8.4.1*. See *8.6.2*.
	Password	1 to 32 characters See *8.2.1*. See *8.6.2*.	1 to 32 characters See *8.3.1*. See *8.6.2*.	1 to 32 characters See *8.4.1*. See *8.6.2*.
	VLAN (post-authentication VLAN)	Y See *8.2.1*. See *8.6.2*.	Y See *8.3.1*. See *8.6.2*.	Y See *8.4.1*. See *8.6.2*. See *9.5.1*.
	Forced authentication	Y See *8.2.2*#.	Y See *8.3.2*#.	Y See *8.4.2*.
	Authentication permission port configured	Y See *9.3.2*.	Y See *9.4.2*.	Y See *9.5.2*.

Functionality			Fixed VLAN	Dynamic VLAN	Legacy
		Private trap	Y See *8.5*.	Y See *8.5*.	Y See *8.5*.
Authentication method list	External server ● RADIUS server group information		Y See *5.3.1*. See *8.2.1*. See *8.6.2*. See *9.2.1*.	Y See *5.3.1*. See *8.3.1*. See *8.6.2*. See *9.2.1*.	N
	Port-based authentication		Y See *5.2.2*. See *5.2.3*.	Y See *5.2.2*. See *5.2.3*.	N
	User ID-based authentication method		Y See *5.2.2*. See *5.2.3*.	Y See *5.2.2*. See *5.2.3*.	N
Terminal IP address assignment	Internal DHCP server		Y See *8.11*. See *9.6*.	Y See *8.11*. See *9.6*.	Y See *8.11*. See *9.6*.
Maximum number of authenticated users	Port-based		1,024 See *8.2.2*. See *9.3.2*.	256 See *8.3.2*. See *9.4.2*.	256 See *8.4.2*. See *9.5.2*.
	At the Switch level		1,024 See *8.2.2*. See *9.3.2*.	256 See *8.3.2*. See *9.4.2*.	256 See *8.4.2*. See *9.5.2*.
Login	Web authentication IP address		Y See *8.2.2*. See *9.2.2*.	Y See *8.3.2*. See *9.2.2*.	Y See *8.4.2*. See *9.2.2*.
	Pre-authentication pass (IPv4 access list for authentication)		Y See *5.4.1*. See *5.5.2*.	Y See *5.4.1*. See *5.5.2*.	N
	URL redirection		Y See *8.2.2*. See *9.3.2*.	Y See *8.3.2*. See *9.4.2*.	N
	TCP port specification for URL redirection trigger packets		Y See *8.2.2*. See *9.3.2*.	Y See *8.3.2*. See *9.4.2*.	N

Functionality		Fixed VLAN	Dynamic VLAN	Legacy
	Specifying a protocol for the Login page	Y See *8.2.2*. See *9.3.2*.	Y See *8.3.2*. See *9.4.2*.	N
	URL automatic display after successful authentication	Y See *8.2.2*. See *9.3.2*.	Y See *8.3.2*. See *9.4.2*.	Y See *8.4.2*. See *9.5.2*.
	User switching option	Y See *8.2.2*. See *9.2.5*.	Y See *8.3.2*. See *9.2.5*.	Y See *8.4.2*. See *9.2.5*.
logout	Maximum connection time exceeded	Y See *8.2.2*. See *9.2.3*.	Y See *8.3.2*. See *9.2.3*.	Y See *8.4.2*. See *9.2.3*.
	Monitoring for authenticated terminal non-communication	Y See *8.2.2*. See *9.3.2*.	Y See *8.3.2*. See *9.4.2*.	N
	Monitoring for MAC address table aging	N	N	Y See *8.4.2*. See *9.5.2*.
	Monitoring for connection of authenticated terminals	Y See *8.2.2*. See *9.3.2*.	N	N
	Receiving special frames from authenticated terminals	Y See *8.2.2*. See *9.2.3*.	Y See *8.3.2*. See *9.2.3*.	Y See *8.4.2*. See *9.2.3*.
	Authenticated terminal connection port link down	Y See *8.2.2*.	Y See *8.3.2*.	N
	VLAN configuration change	Y See *8.2.2*.	Y See *8.3.2*.	Y See *8.4.2*.
	Web pages operation	Y See *9.7.12*.	Y See *9.7.12*.	Y See *9.7.12*.
	Operation commands	Y See *8.2.2*.	Y See *8.3.2*.	Y See *8.4.2*.

Functionality		Fixed VLAN	Dynamic VLAN	Legacy
Roaming (moving authenticated terminals between ports)	Port move permission configured	Y See *8.2.2*. See *9.3.2*.	Y See *8.3.2*. See *9.4.2*.	N
	Private trap	Y See *8.5*.	Y See *8.5*.	N
Accounting log	Internal account log of the Switch	2,100 lines for all modes See *8.5*.		
	RADIUS server accounting functionality	Common to all modes See *5.3.4*. See *8.5*. See *9.2.4*.		
Web authentication page	Replacing Web authentication pages	Common to all modes See *8.9*. See *9.7.7*.		
	Specification of individual Web authentication pages by port	Y See *8.2.2*. See *9.3.2*.	Y See *8.3.2*. See *9.4.2*.	N

Legend:

Y: Supported

N: Not supported

5.x.x refers to the relevant sections in *5. Overview of Layer 2 Authentication.*

8.x.x refers to the relevant sections in this chapter.

9.x.x refers to the relevant sections in *9. Web Authentication Configuration and Operation.*

#

For details about using forced authentication common to all authentication modes, see *5.4.6 Forced authentication common to all authentication modes.*

The following table shows the operating conditions for Web authentication.

Table 8-2 Operating conditions for Web authentication

Type		Port setting	Specifiable VLAN type	Frame type	Fixed VLAN mode	Dynamic VLAN mode	Legacy mode
Port type	Access port	native	Port VLAN MAC VLAN	Untagged	Y	N	N
	Trunk	native	Port VLAN	Untagged	Y	N	N

Type		Port setting	Specifiable VLAN type	Frame type	Fixed VLAN mode	Dynamic VLAN mode	Legacy mode
	port	allowed	Port VLAN MAC VLAN	Tagged	Y	N	N
	Protocol port	--	--	--	N	N	N
	MAC port	native	Port VLAN	Untagged	Y#	N	N
		mac	MAC VLAN	Untagged	N	Y	Y
		dot1q	Port VLAN MAC VLAN	Tagged	Y	N	N
Default VLAN					Y	N	N
Interface type	fastethernet				Y	Y	Y
	gigabitethernet				Y	Y	Y
	port channel				N	N	Y

Legend:

Y: Supported

N: Not supported

--: Not applicable for authentication ports

#

For details, see *5.4.4 Auto authentication mode accommodation on the same MAC port.*

The subsequent sections give an overview of fixed VLAN mode, dynamic VLAN mode, and legacy mode. For the same functionality and same operation in each authentication mode, read the descriptions given in the references.

8.2 Fixed VLAN mode

Prior to authentication, a terminal cannot start communication until it is successfully authenticated. If authentication succeeds in fixed VLAN mode, the MAC address of the terminal and VLAN ID is registered in the MAC address table as a Web authentication entry, enabling the terminal to communicate. (Entries registered in the MAC address table can be confirmed by using the `show mac-address-table` operation command.)

Users can log in using the Web authentication IP address or using the URL redirection functionality. Either way, the authentication method described in *8.2.1 Authentication method group* can be used for authentication. Therefore, you must set both, or either Web authentication IP address, or URL redirection.

8.2.1 Authentication method group

The authentication method group uses an authentication method list in fixed VLAN mode and dynamic VLAN mode with the Switch default set to the mode that is common to all Web authentications. For details, see the following sections:

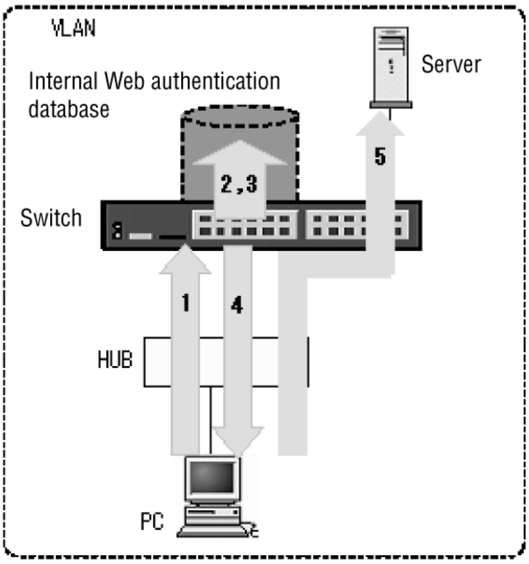
- *5.1.3 Authentication method groups*
- *5.3.3 Priority configuration for the Switch default local and RADIUS authentications*
- *5.2.2 Authentication method list*
- *5.3.1 RADIUS server information used with the Layer 2 authentication method*
- *9.2.1 Configuring the authentication method group and RADIUS server information*

(1) Switch default: Local authentication

Local authentication searches the internal Web authentication DB by a user ID and a password from the user seeking authentication and validates the credentials.

The following figure shows the authentication operation of the local authentication method:

Figure 8-1 Fixed VLAN mode (local authentication method)



1. A PC user connected via a hub opens a Web browser and accesses the Switch using the Web authentication IP address.
2. When the internal Web authentication DB is searched, the VLAN ID that the user to be authenticated (the PC in the figure above) belongs to is identified by using the connection port or VLAN ID of the user to be authenticated.
3. VLAN capacity can be restricted by searching the internal Web authentication DB with the VLAN ID information added to the user ID and password.
4. If authentication succeeds, a page opens on the PC indicating that authentication was successful.
5. The authenticated PC can access servers in the VLAN associated with the port.

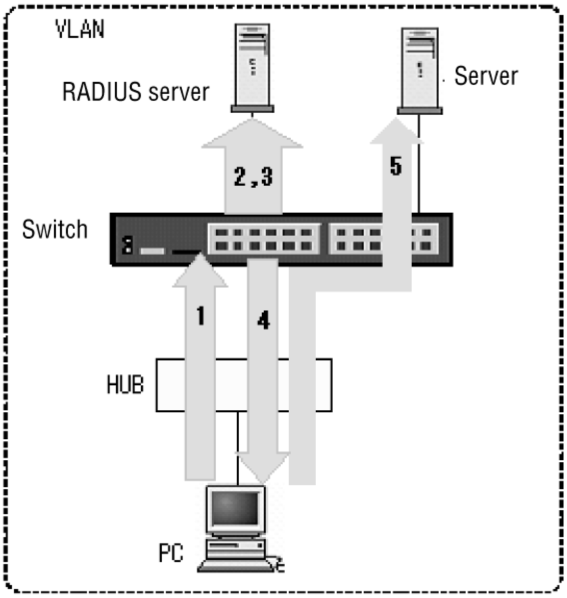
(a) VLAN restriction

The VLAN ID is extracted from the port where a user seeking authentication is connected, and the internal Web authentication DB is searched by VLAN ID with other credentials, thereby authentication can be restricted to a specific VLAN.

(2) Switch default: RADIUS authentication

The following figure shows the operation of RADIUS authentication method.

Figure 8-2 Fixed VLAN mode (RADIUS authentication method)



1. A PC user connected via a hub opens a Web browser and accesses the Switch using the specified URL.
2. When requesting an external RADIUS server to execute authentication, the VLAN ID that the user to be authenticated (the PC in the figure above) belongs to is identified by using the connection port or VLAN ID of the user to be authenticated.
3. VLAN capacity can be restricted by requesting that the RADIUS server execute authentication with the VLAN ID information added to the user ID and password.
4. If authentication succeeds, a page opens on the PC indicating that authentication was successful.
5. The authenticated PC can access servers in the VLAN associated with the port.

(a) VLAN restriction

RADIUS authentication uses the same method as local authentication to obtain VLAN information and executes authentication by setting the obtained VLAN ID information (the VLAN ID a terminal is associated with when requesting authentication) in the RADIUS attribute `NAS-Identifier` at the time the authentication request is sent to the RADIUS server.

VLAN information to be authenticated (the VLAN ID to which a terminal is associated when requesting authentication) is set in addition to a user ID and a password in `NAS-Identifier` as the RADIUS server configuration, thereby restricting VLAN capacity.

(3) Authentication method list

For Web authentication, you can authenticate by port or by user ID. For details about operations for these authentication methods, see *5.2.2 Authentication method list.*

8.2.2 Authentication functionality

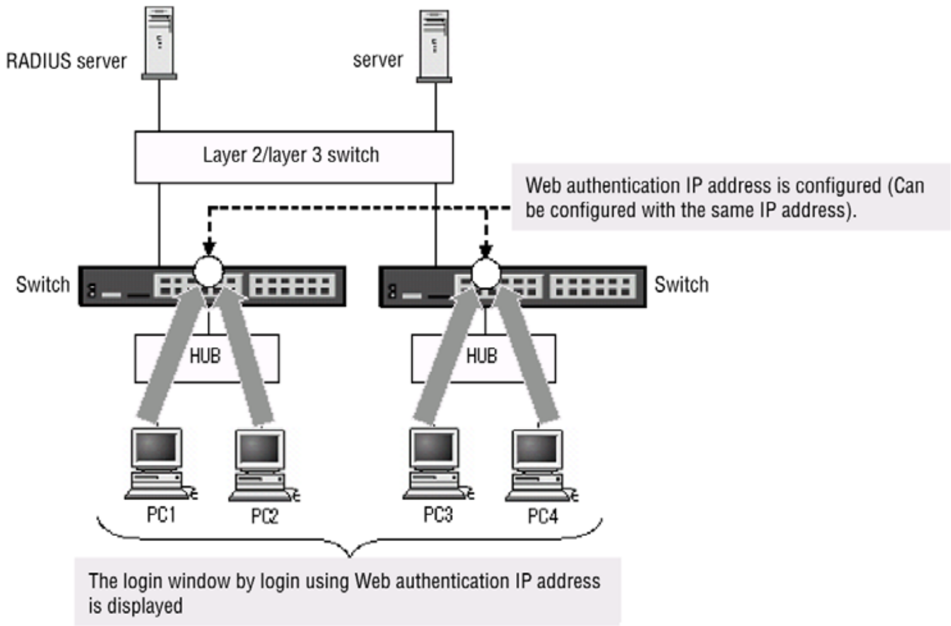
(1) Web authentication IP address

Users can log in and log out by using the Web authentication IP address configured on the Switch.

Unlike the IP address configured on each interface, a Web authentication IP address is used only for logging in or logging out of Web authentication.

A Web authentication IP address can be configured with the `web-authentication ip address` configuration command.

Figure 8-3 Logging in by using the Web authentication IP address



Note

- When using a Web authentication IP address, always set the IP address in a pre-authentication VLAN for Web authentication.
- As a Web authentication IP address, set the IP address of a subnet that does not duplicate the VLAN interface configured on the Switch.

(2) URL redirection

Configure the Switch to detect outgoing HTTP and HTTPS requests from an unauthenticated terminal and forcibly display the Login page on the terminal for the user to log in.

Note that, if configuring URL redirection, always set an IP address in the VLAN where a terminal seeking authentication is associated.

(a) Adding URL redirection trigger packet TCP port numbers

For the trigger packet for URL redirection, the TCP destination port numbers are 80 and 443, and only one TCP destination port numbers can be added with the configuration command. After the configuration, the basic TCP destination port numbers remain as 80 and 443.

Configure an additional port number with the configuration commands web-authentication redirect tcp-port and web-authentication web-port.

When different port numbers are added using the two commands above, basic port numbers and the additional port numbers configured by each of the commands are enabled. If the same additional port numbers are configured, the operations are shown as follows.

Table 8-3 Operations when configuring the same additional port number

		web-authentication redirect tcp-port	**web-authentication web-port**	
			http	**https**
web-authentication redirect tcp-port			Redirect as HTTP	Redirect as HTTP (HTTPS-specified port number is ignored.)
web-authentication web-port	http	Redirect as HTTP		Command entered first is valid.
	https	Redirect as HTTP (HTTPS-specified port number is ignored.)	Command entered first is valid.	

(b) Specifying a protocol for the Login page

When using the URL redirection functionality of Web authentication, select HTTP or HTTPS in the configuration for the protocol (URL) to display the Web authentication Login page. If not specified, the page is displayed via HTTPS.

Configure the protocol for a Login page with the web-authentication redirect-mode configuration command.

(3) Specifying the automatically displayed URL after successful authentication

Specify the URL of a page to be automatically displayed after displaying the page indicating successful authentication.

Configure this URL using the web-authentication jump-url configuration command.

(4) Specifying a forced authentication port

When a terminal connected to a port for which forced authentication is specified undergoes RADIUS authentication, and sending a request to the RADIUS server fails due to a line failure or the RADIUS does not respond, the terminal becomes authenticated.

The forced authentication configuration of the Switch includes both the configuration common to all authentication modes and the configuration by authentication functionality. For details about shared authentication configuration, see *5.4.6 Forced authentication common to all authentication modes.*

Set the web-authentication static-vlan force-authorized configuration command in the port that allows forced authentication.

Forced authentication is successful when the following conditions are met.

Table 8-4 Conditions for successful forced authentication

Item	Condition
Configuration	All the following configurations have been set: ● `aaa authentication web-authentication`#1 ● `web-authentication radius-server host` or `radius-server host` ● `web-authentication system-auth-control` ● `web-authentication port`#2 ● `web-authentication static-vlan force-authorized`#2 ● `web-authentication authentication`#3 ● `web-authentication user-group`#4
Accounting log	The following accounting log is collected when an authentication request is sent to the RADIUS server: `No=21` `NOTICE: LOGIN: (`*<Additional information>*`) Login failed ; Failed to connection to RADIUS server.` *<Additional information>*`: MAC, USER, IP, PORT, VLAN` Check the accounting log with the `show web-authentication logging` operation command.

#1

When using forced authentication by Switch default, set only `default group radius`.

When using port-based authentication method or user ID-based authentication method, set *<list-name>* `group` *<group-name>*.

#2

Specify the same Ethernet port.

#3

Specify this when using port-based authentication method.

#4

Specify this when using user ID-based authentication method.

The authentication status of a terminal where authentication is permitted by forced authentication is canceled in the same way as for a normally authenticated terminal, as described in *(6) Logout from authenticated status* in *8.2.2 Authentication functionality.*

Furthermore, all operations from the start of requesting authentication to the RADIUS server to successful forced authentication are the same for shared forced authentication and per-authentication-method forced authentication. For details about the operations, see *(1) Behavior from the start of an RADIUS authentication request to permission for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

(5) Maximum number of authenticated users

The maximum number of users to be authenticated can be configured both on a Switch basis and on a port basis. You can configure up to 1,024 authenticated users or terminals using the `web-authentication static-vlan max-user` configuration command.

The configuration can be simultaneously made on a Switch basis and on a port basis. However, after the number of users authenticated either way reaches the limit, authentication is no longer available for new users.

In addition, if the maximum number of users to be authenticated is changed to be less than the number of authenticated users during an operation, the authenticated user can continue to communicate, but new users cannot be authenticated.

(6) Logout from authenticated status

Fixed VLAN mode provides the following means of logging out:

- Logout when maximum connection time is exceeded
- Logout of an authenticated terminal by non-communication monitoring
- Logout of an authenticated terminal by the connection monitoring functionality
- Logout by receiving a special frame from an authenticated terminal
- Logout of a terminal connected to a link-down port
- Logout resulting from changes to the VLAN configuration
- Logout using the Web interface
- Logout using an operation command

(a) Logout when maximum connection time is exceeded

When a terminal exceeds the maximum connection time specified by the configuration command, the Web authentication status is automatically logged out. In this case, the user is not presented with a logout page.

When the user logs in again with the terminal authenticated, if local authentication (RADIUS authentication when using RADIUS authentication) succeeds, the authentication time can be extended. If the authentication fails, the time cannot be extended.

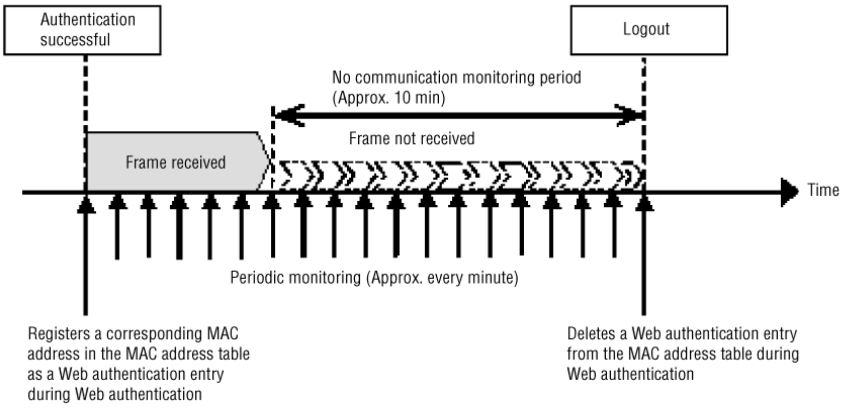
Configure the maximum connection time with the `web-authentication max-timer` configuration command.

(b) Logout of an authenticated terminal by non-communication monitoring

This functionality causes an authenticated terminal to automatically log out when it has not communicated with for a certain period of time.

The functionality periodically (approximately every minute) monitors the Web authentication entry of the MAC address table and verifies that the terminal receives a frame from the authenticated terminal registered with Web authentication. If no frame is received from the target terminal for a certain time period (approximately 10 minutes), the functionality deletes the target Web authentication entry from the MAC address table and causes the authentication to be logged out.

Figure 8-4 Overview of non-communication monitoring of authenticated terminals



Non-communication monitoring is enabled for authenticated terminals when the following condition is met:

- When Web authentication fixed VLAN mode or dynamic VLAN mode is in effect, and `web-authentication auto-logout` is valid.

The `no web-authentication auto-logout` configuration command prevents authentication from automatically being logged out.

(c) Logout of an authenticated terminal by the connection monitoring functionality

The Switch monitors the connection status of authenticated terminals by sending an ARP request at the interval specified by the `web-authentication logout polling interval` configuration command and monitoring for an ARP reply. If it receives no ARP reply within the time period defined by the `web-authentication logout polling retry-interval` and `web-authentication logout polling count` configuration commands, the Switch considers the connection to have timed out and automatically logs out of the Web authentication status of the terminal. The user is not presented with a logout page.

You can disable this functionality by using the `no web-authentication logout polling enable` configuration command.

(d) Logout by receiving a special frame from an authenticated terminal

The Switch logs out of the authentication status of target terminals from which it receives a special frame. The user is not presented with a logout page. Special frames are defined below. If all the following conditions are met, the authentication status is logged out:

- A ping frame is sent from an authenticated terminal to the Web authentication IP address.
- The TTL value of a ping frame must match the TTL value specified by the `web-authentication logout ping ttl` configuration command.
- The TOS value of a ping frame must match the TOS value specified by the `web-authentication logout ping tos-windows` configuration command.

(e) Logout of a terminal connected to a link-down port

When a port with Web authentication fixed VLAN mode (the `web-authentication port` configuration command) configured goes down, the Switch logs out of the authenticated terminal in the Web authentication fixed VLAN mode at the port. The user is not presented with a logout page.

(f) Logout resulting from changes to the VLAN configuration

When using configuration commands to change the configuration of a VLAN that includes authenticated terminals, the Switch logs out of the authentication status of terminals associated with that VLAN.

The following configuration changes trigger a logout:

- Deletion of a VLAN
- Suspension of a VLAN

(g) Logout using the Web interface

When a terminal accesses the Web-authenticated URL, a logout page appears on the terminal. When pressing the **Logout** button in the page, you can log out from Web authentication.

For details, see *9.7.12 Authentication procedure from terminal.*

(h) Logout using an operation command

Executing the `clear web-authentication auth-state` operation command forcibly logs out some of the Web-authenticated users or all the Web-authenticated users.

(7) Roaming (moving authenticated terminals between ports)

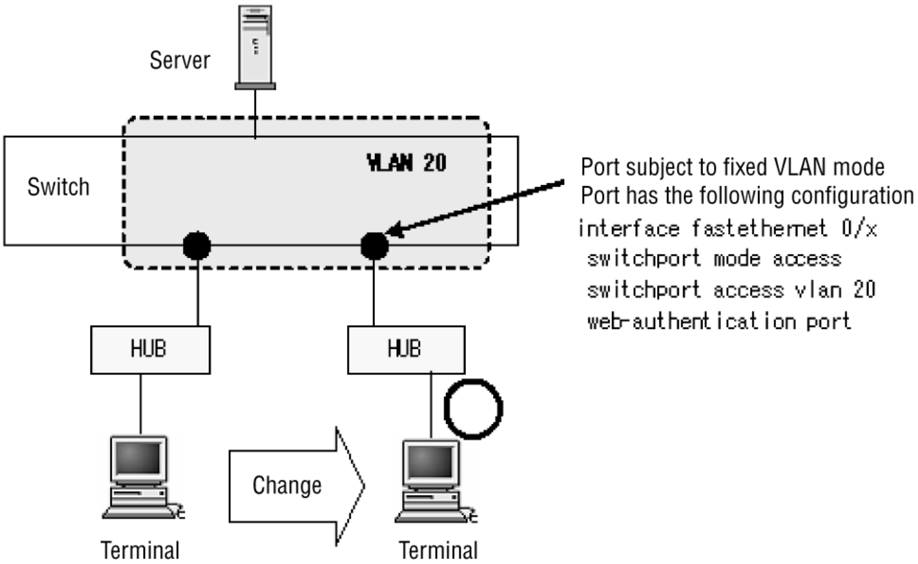
When an authenticated terminal connected to the network via, for example, a hub is moved between ports without the link going down, the roaming functionality enables the terminal to continue to communicate in the authentication status.

Roaming operates when the following conditions are met:

- The `web-authentication static-vlan roaming` configuration command is configured.
- Ports for fixed VLAN mode before and after moving
- The same VLAN before and after moving

When a terminal is moved between ports under conditions other than the above, the authentication of the target terminal is forcibly logged out.

Figure 8-5 Overview of roaming in fixed VLAN mode



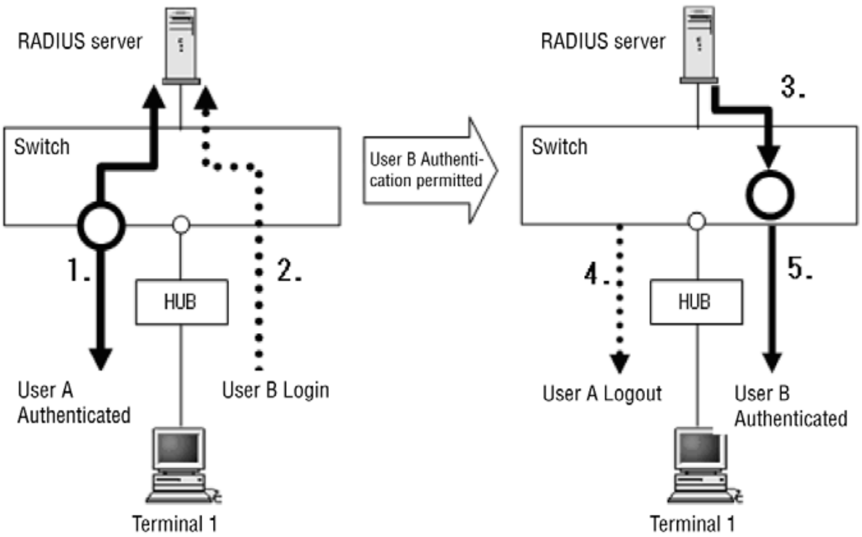
(8) User switching option

When a user logs in to a specific terminal using Web authentication, the option enables another user ID to log in without requiring the original user to log out. Enable this option using the `web-authentication user replacement` configuration command.

Note that this option switches user IDs without requiring a logout operation in one terminal (MAC address), not allows multiple users to simultaneously log in.

The following figure shows an operation example when the user switching option is configured.

Figure 8-6 Overview of user switching option (Example of RADIUS authentication)



1. When user A logs in from a specific terminal (Terminal 1 in the figure), authentication is executed using an authentication

method (RADIUS or local authentication) according to the configuration on the Switch. (In this example, user A is accepted and managed as an authenticated user.)

2. If another user ID (user B in the figure) logs in from an authenticated terminal (Terminal 1 in the figure), authentication is executed using an authentication method (RADIUS or local authentication) according to the configuration on the Switch.
3. As a result of the authentication, the new user (user B in the figure) is accepted.
4. The Switch logs out the old user (user A in the figure).
5. The management information on the Switch is updated with the new user as an authenticated user or authenticated, and the Switch notifies the new user that the login was successful. At this time, the management information, the login date and time, and the remaining time of the old user is updated with those information of the new user.

- VLANs to which terminals are attached and the authentication mode of a new user

  An authentication mode and VLAN where terminals are attached by the acceptance of new users are determined depending on authentication results of new users.

- When switching users simultaneously on multiple terminals

  When switching users simultaneously on multiple terminals, up to 1,280 terminals are managed as users, which is the limit of Web authentication.

- The failure of new users

  During authentication for user switching, if a logout condition is met due to link-down of the port, the Switch logs out all the authenticated terminals where the logout condition is met in the same way as the conventional operation during authentication, and the authentication of a new user fails.

  If authentication of a new user fails (is denied), the authentication status of the old user is maintained.

(a) Configuration of user ID-based authentication method and identification of user ID

The range of user ID identification differs depending on whether the user ID-based authentication method is configured. When the user ID-based authentication method is configured, the identification range are the user IDs sent for authentication request to the RADIUS server, not the entire entered user ID character strings. (For details about the user ID-based authentication method, see *5.2.2 Authentication method list*.)

The following table shows an example configuration status of the user ID-based authentication method and the range of user ID identification.

Table 8-5 Example configuration status of the user ID-based authentication method and the range of user ID identification

User ID-based authentication method	Number of authentications	Character string entered by user	Range of user ID identification	Result of user identification	User switching operation
Not configured	1	`userAAA@list111`	`userAAA@list111`	New user	--
	2	`userAAA@list111`	`userAAA@list111`	Same user	--
	3	`userBBB@list111`	`userBBB@list111`	Different user	Y
	4	`userBBB@list222`	`userBBB@list222`	Different user	Y
Configured	1	`userAAA@list111`	`userAAA`	New user	--
	2	`userAAA@list111`	`userAAA`	Same user	--
	3	`userBBB@list111`	`userBBB`	Different user	Y
	4	`userBBB@list222`	`userBBB`	Same user	--

Legend:

Y: Supported

--: Not supported

(b) User switching operation at multistep authentication ports

At a multistep authentication port, the Switch compares the Web authentication result (`Filter-Id`) of a new user with the result of the terminal authentication performed with the old user of the terminal, and determines whether authentication can be registered. (For details about the multistep authentication, see *12. Multistep authentication.)*

The following table shows user switching operation at multistep authentication ports.

Table 8-6 User switching at multistep authentication ports

Configuration of multistep authentication port	Authentication of old user				Authentication of new user	
	Terminal authentication		User authentication		User authentication	
	Type	Result	Result	Management status of terminal	Result	Management status of terminal

Configuration of multistep authentication port	**Authentication of old user**				**Authentication of new user**	
	Terminal authentication		**User authentication**		**User authentication**	
	Type	**Result**	**Result**	**Management status of terminal**	**Result**	**Management status of terminal**
No option	MAC-based authentication	Succeeded	Succeeded	Multistep authentication	Failed	Login status of old user
					Succeeded	Multistep authentication status of new user
User acceptance option configured	MAC-based authentication	Failed	Succeeded	Single authentication	Failed	Login status of old user
					Succeeded	Login status of old user[#1]
						Single authentication status of new user[#2]
		Succeeded	Succeeded	Multistep authentication	Failed	Login status of old user
					Succeeded	Multistep authentication status of new user
`dot1x` option for terminal authentication configured	MAC-based authentication	Succeeded	Succeeded	Multistep authentication	Failed	Login status of old user
					Succeeded	Multistep authentication status of new user
	IEEE802.1X	Succeeded	Succeeded	Multistep authentication	Failed	Login status of old user
					Succeeded	Multistep authentication status of new user

#1

Even though authentication of a new user was successful, if terminal authentication is also required for the user, the authentication of the new user is treated as failure, and the login status of the old user remains.

#2

If authentication of a new user succeeds and terminal authentication is not required for the user, the status becomes single authentication.

(9) Individual Web authentication page by port

This functionality handles the registered custom file set (the directory name) as the individual Web authentication page of a port, and displays the associated individual Web authentication page when Web authentication is accessed from the port. Use the `web-authentication html-fileset` configuration command to associate the individual Web authentication page to the port.

- When `Other destination` is accessed from unauthenticated terminals

  Use the URL redirection functionality to redirect the access to the individual Web authentication page associated with the port.

- The URL of redirect destinations when the URL redirection functionality operates at the port

  The URL of `http://`*IP-address*`/login.html` is common to a Web authentication page and an individual Web authentication page. However, the page to be displayed is the file set configured by port.

- When accessing an authenticated page file that is not associated

  Ports to which individual Web authentication pages are associated cannot access URLs or HTML files not associated with that port.

For example, if an individual Web authentication page file set redirected to the quarantine server is configured for a specific port, operations are possible that require the user who accesses an authentication page from the target authentication port to log in after the quarantine processing at the quarantine server and requires users at other ports to execute normal Web authentication.

An individual Web authentication page used for this functionality is registered on the Switch using the Web authentication switching page functionality. A file set registered on the Switch is called a *custom file set*. For details, see *8.9 Replacing Web authentication pages.*

8.2.3 Authentication behavior

In fixed VLAN mode, authentication is executed in the following sequence.

Figure 8-7 Authentication operation (When using Web authentication IP address)

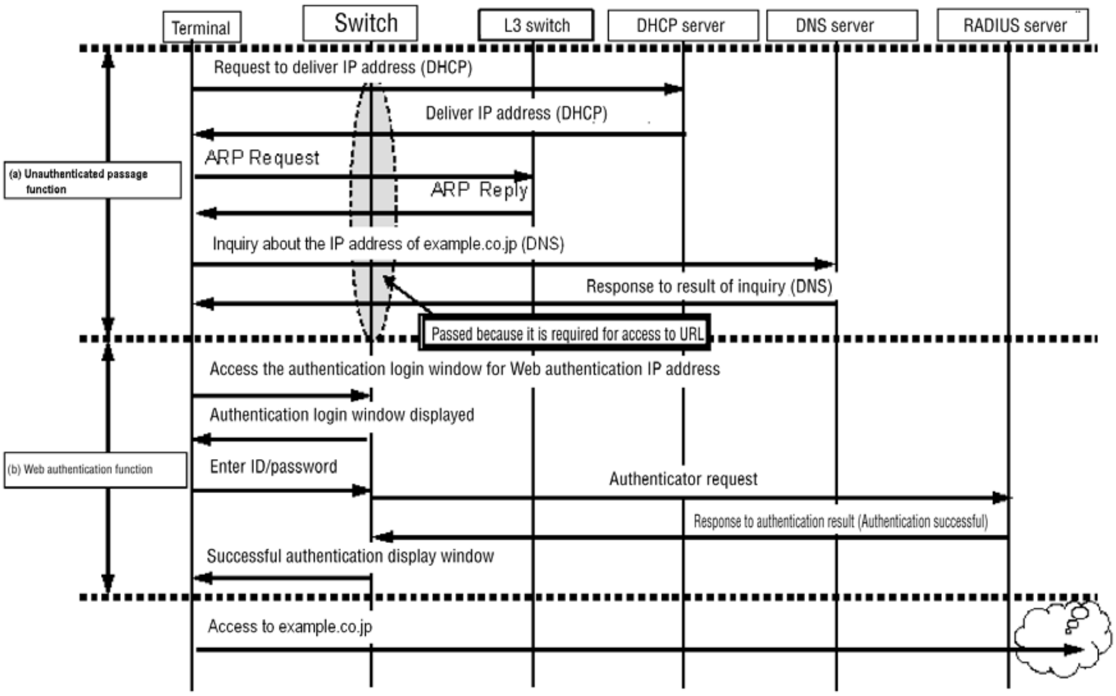
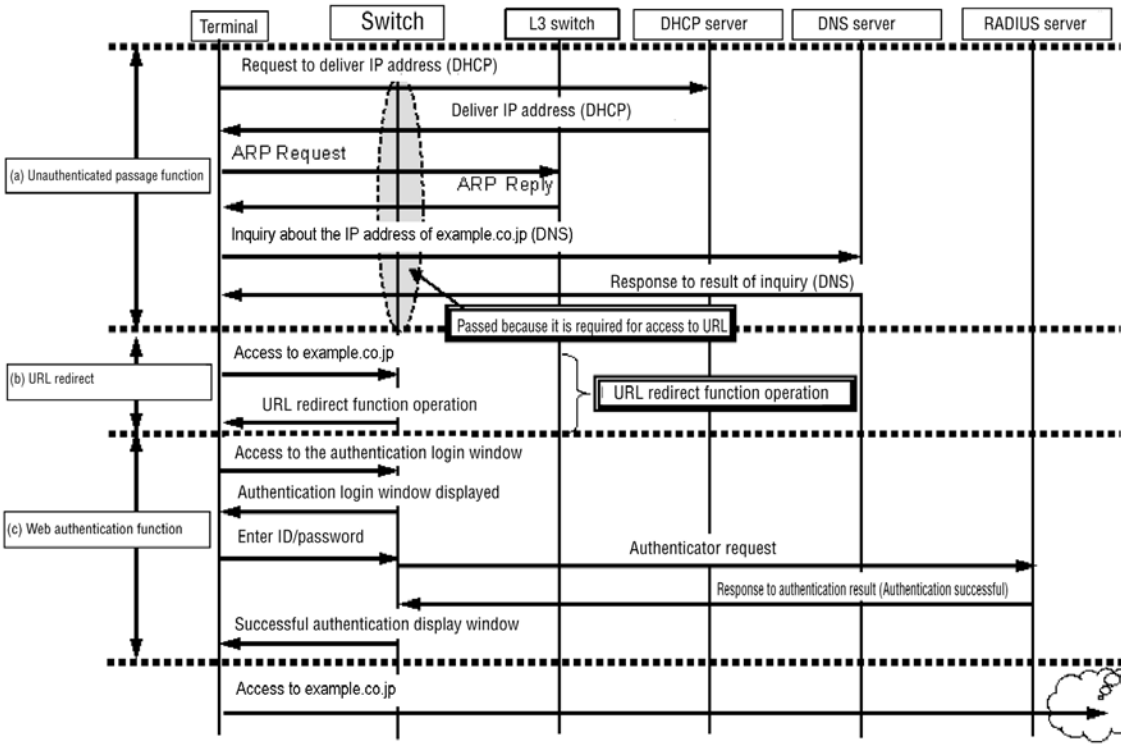


Figure 8-8 Authentication operation (when using URL redirection functionality)



8.3 Dynamic VLAN mode

Prior to authentication, a terminal cannot start communication until it is successfully authenticated. If authentication succeeds in dynamic VLAN mode, the MAC address of the terminal and the authenticated VLAN ID are registered in the MAC VLAN and the MAC address table as a Web authentication entry, enabling the terminal to communicate on the post-authentication VLAN. (Entries registered in the MAC address table can be confirmed by using the `show mac-address-table` operation command.)

While legacy mode operates by configuring post-authentication VLANs, dynamic VLAN mode operates by configuring MAC VLANs set for physical ports. For communication on pre-authentication VLANs in dynamic VLAN mode, configure an authentication IPv4 access list.

Users can log in using the URL redirection functionality or using the Web authentication IP address. Either way, the authentication method described in *8.3.1 Authentication method group* can be used for authentication.

8.3.1 Authentication method group

The authentication method group uses an authentication method list in fixed VLAN mode and dynamic VLAN mode with the Switch default set to the mode that is common to all Web authentications. For details, see the following sections:

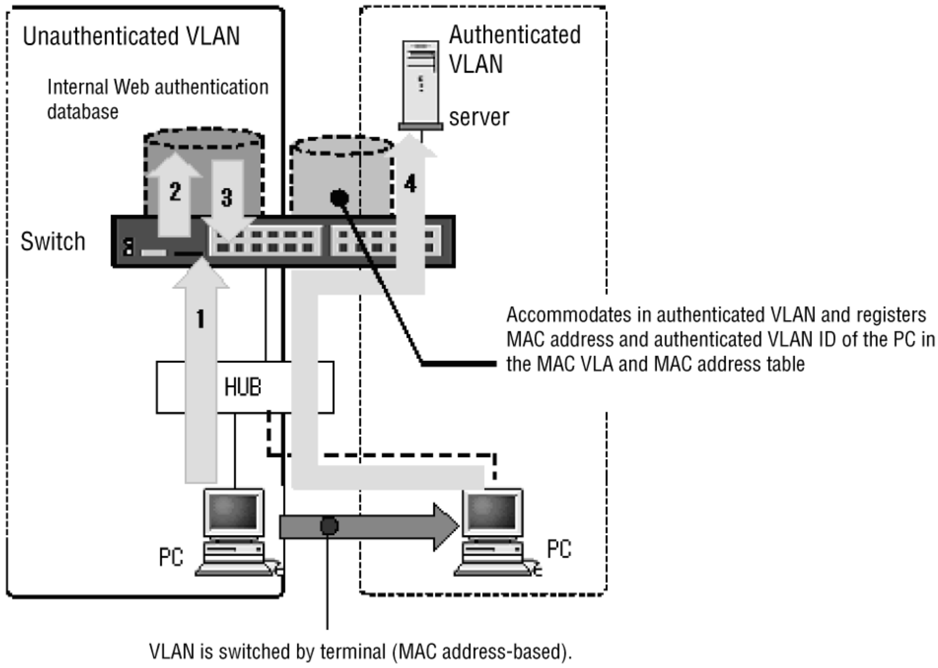
- *5.1.3 Authentication method groups*
- *5.3.3 Priority configuration for the Switch default local and RADIUS authentications*
- *5.2.2 Authentication method list*
- *5.3.1 RADIUS server information used with the Layer 2 authentication method*
- *9.2.1 Configuring the authentication method group and RADIUS server information*

(1) Switch default:local authentication

Local authentication searches the internal Web authentication DB by a user ID and a password from the user seeking authentication and validates the credentials by comparing the registration details. If validated, the Switch attaches the terminal to the VLAN registered in the internal Web authentication DB and allows the terminal to communicate.

The following figure shows the authentication operation of the local authentication method.

Figure 8-9 Dynamic VLAN mode (local authentication)



1. A PC user connected via a hub opens a Web browser and accesses the Switch using the specified URL.
2. The Switch validates the user ID and password by comparing them against the user information in the internal Web authentication DB.
3. If authentication succeeds, a page opens on the PC indicating that authentication was successful.
4. The authenticated PC is attached to the post-authentication VLAN and can connect to servers. The Switch also registers the MAC address of the authenticated PC and VLAN ID in the MAC VLAN and the MAC address table.

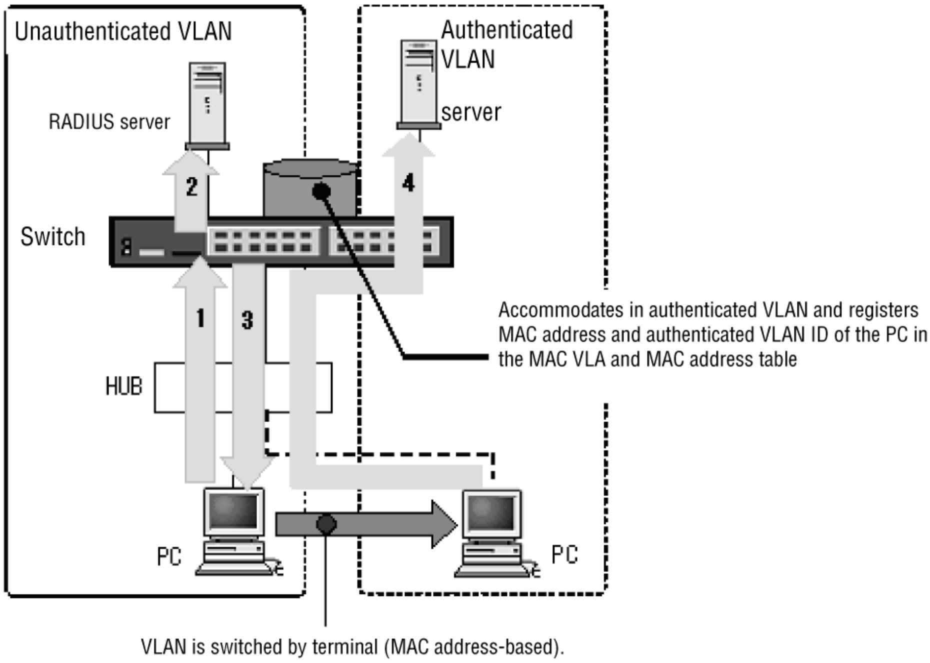
(a) Capacity limit of post-authentication VLANs

For details, see *5.4.3 Auto VLAN assignment for a MAC VLAN* and *5.4.4 Auto authentication mode accommodation on the same MAC port.*

(2) Switch default: RADIUS authentication

The following figure shows the operation of RADIUS authentication method.

Figure 8-10 Dynamic VLAN mode (RADIUS authentication)



1. A PC user connected via a hub opens a Web browser and accesses the Switch using the specified URL.
2. Authentication is executed using the user ID and password via the external RADIUS server.
3. If authentication succeeds, a page opens on the PC indicating that authentication was successful.
4. Based on the VLAN ID information sent from the RADIUS server, the authenticated PC is attached to the post-authentication VLAN and can connect to the server. The Switch also registers the MAC address of the authenticated PC and VLAN ID in the MAC VLAN and the MAC address table.

(a) Capacity limit of post-authentication VLANs

For details, see *5.4.3 Auto VLAN assignment for a MAC VLAN* and *5.4.4 Auto authentication mode accommodation on the same MAC port.*

(3) Authentication method list

In Web authentication, you can use authentication method by port or authentication method by user ID. For details about operations for these authentication methods, see *5.2.2 Authentication method list.*

8.3.2 Authentication functionality

(1) Web authentication IP address

Configuration is the same as for fixed VLAN mode. For details, see *(1) Web* *authentication IP address* in *8.2.2 Authentication functionality.*

(2) URL redirection

Configuration is the same as for fixed VLAN mode. For details, see *(2) URL redirection* in *8.2.2 Authentication functionality*.

(3) Specifying the automatically displayed URL after successful authentication

Specify the URL of a page to be automatically displayed after displaying the page indicating successful authentication. Set the time before URL transition to approximately 20 to 30 seconds because the IP address of the authenticated terminal must be changed at the time of switching from a pre-authentication VLAN to a post-authentication VLAN.

If IP addresses have been assigned to unauthenticated terminals on the internal DHCP server (default lease time:10 seconds), the IP addresses are obtained from the normal DHCP server for an authenticated VLAN. Accordingly, it might take approximately 20-30 seconds before a post-authentication VLAN can communicate after the completion of authentication.

Use the `web-authentication jump-url` configuration command to configure the URL of a page to be automatically displayed after displaying the page indicating successful authentication and the time period before URL transition.

(4) Specifying a forced authentication port

When a terminal connected to a port for which forced authentication is specified undergoes RADIUS authentication, and sending a request to the RADIUS server fails due to a line failure or the RADIUS does not respond, the terminal becomes authenticated.

In the Switch, the configuration for forced authentication can be shared among all authentication methods or be specified separately per authentication method. For details about shared authentication configuration, see *5.4.6 Forced authentication common to all authentication modes.*

Configure the `web-authentication force-authorized vlan` configuration command on the port where forced authentication is allowed.

Forced authentication is successful when the following conditions are met.

Table 8-7 Conditions for successful forced authentication

Item	Condition
Configuration	All the following configurations have been set: ● `aaa authentication web-authentication`#1 ● `web-authentication radius-server host` or `radius-server host` ● `web-authentication system-auth-control` ● `vlan` *<VLAN ID list>* `mac-based`#2 ● `web-authentication port`#3 ● `web-authentication force-authorized vlan`#2, #3 ● `switchport mode mac-vlan`#3 ● `web-authentication authentication`#4 ● `web-authentication user-group`#5

Item	Condition
Accounting log	The following accounting log is collected when an authentication request is sent to the RADIUS server: `No=21` `NOTICE:LOGIN: (`*<Additional information>*`) Login failed ; Failed to connection to RADIUS server.` *<Additional information>*`: MAC, USER, IP, PORT, VLAN` Check the accounting log with the `show web-authentication logging` operation command.

#1

When using forced authentication by Switch default, set only `default group radius`.

When using port-based authentication method or user ID-basaed authentication method, set *<list-name>* `group` *<group-name>*.

#2

Set the same VLAN ID.

#3

Specify the same Ethernet port.

#4

Specify this when using port-based authentication.

#5

Set this when using user ID-based authentication method.

The authentication status of a terminal where authentication is permitted by forced authentication is canceled in the same way as for a normally authenticated terminal, as described in *(6) Logout from authenticated status* in *8.3.2 Authentication functionality.*

Furthermore, all operations from the start of requesting authentication to the RADIUS server to successful forced authentication are the same for shared forced authentication and per-authentication-method forced authentication. For details about the operations, see*(1) Behavior from the start of an RADIUS authentication request to permission for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

(5) Maximum number of authenticated users

The maximum number of users to be authenticated can be configured both on a Switch basis and on a port basis. Configure up to 256 authenticated users or terminals using the `web-authentication max-user` configuration command.

The configuration can be simultaneously made on a Switch basis and on a port basis. However, after the number of users authenticated either way reaches the limit, authentication is no longer available for new users.

In addition, if the maximum number of users to be authenticated is changed to be less than the number of authenticated users during an operation, the authenticated user can continue to communicate, but new users cannot be authenticated.

(6) Logout from authenticated status

Dynamic VLAN mode provides the following means of logging out:

- Logout when maximum connection time is exceeded
- Logout of an authenticated terminal by non-communication monitoring
- Logout by receiving a special frame
- Logout of a terminal connected to a link-down port
- Logout resulting from changes to the VLAN configuration
- Logout using a Web page
- Logout using an operation command

The means of each logout is the same as that of fixed VLAN mode. For details, see *(6) Logout from authenticated status* in *8.2.2 Authentication functionality.*

(7) Roaming (moving authenticated terminals between ports)

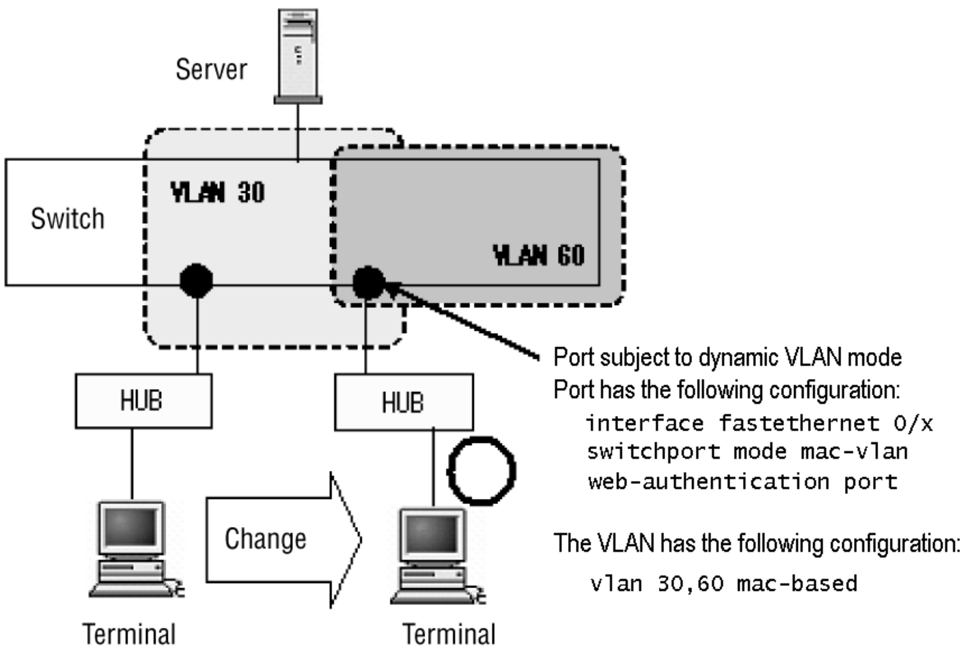
When an authenticated terminal connected to the network via, for example, a hub is moved between ports without the link going down, the roaming functionality enables the terminal to continue to communicate in the authentication status.

Roaming operates when the following conditions are met:

- The `web-authentication static-vlan roaming` configuration command is configured.
- Ports are in dynamic VLAN mode before and after moving

When a terminal is moved between ports under conditions other than the above, the authentication of the target terminal is forcibly logged out.

Figure 8-11 Roaming in dynamic VLAN mode



(8) User switching option

Configuration is the same as for fixed VLAN mode. For details, see *(8) User switching option* in *8.2.2 Authentication functionality.*

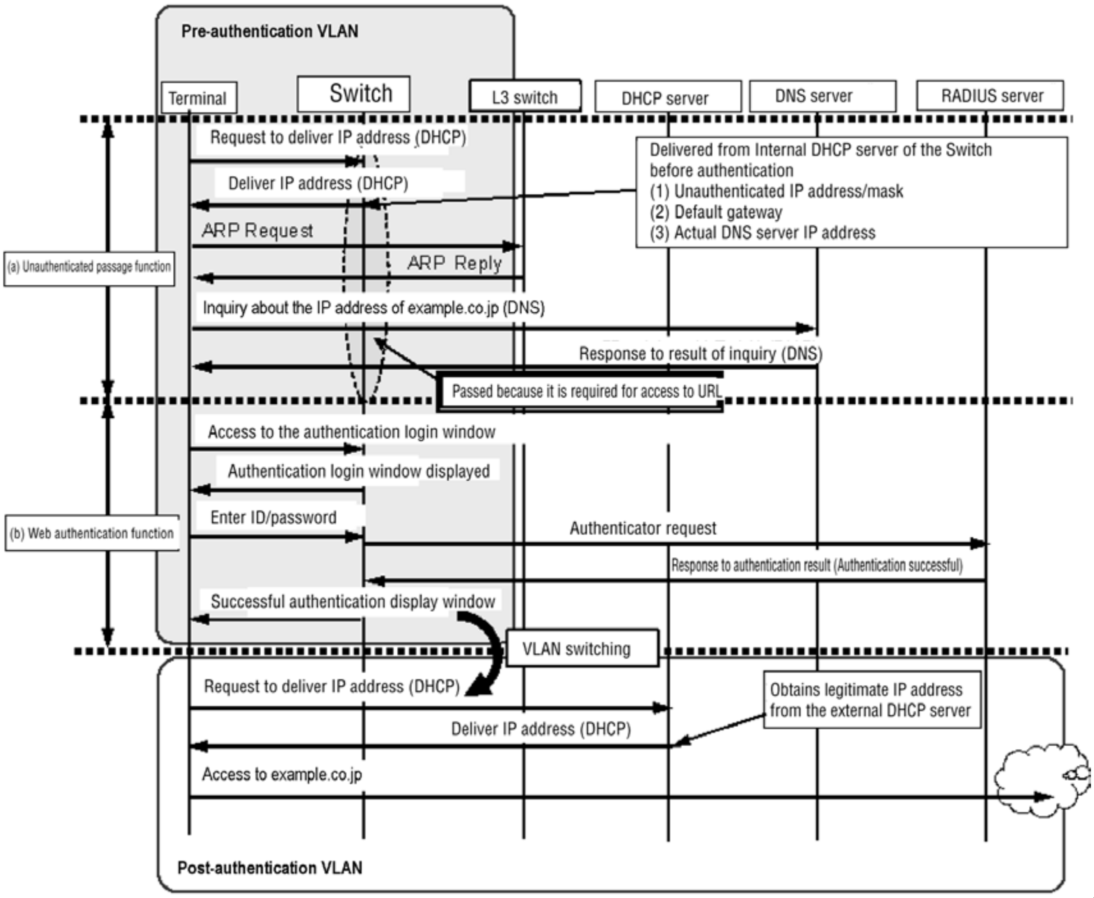
(9) Individual Web authentication page by port

Configuration is the same as for fixed VLAN mode. For details, see *(9) Individual Web authentication page by port* in *8.2.2 Authentication functionality.*

8.3.3 Authentication behavior

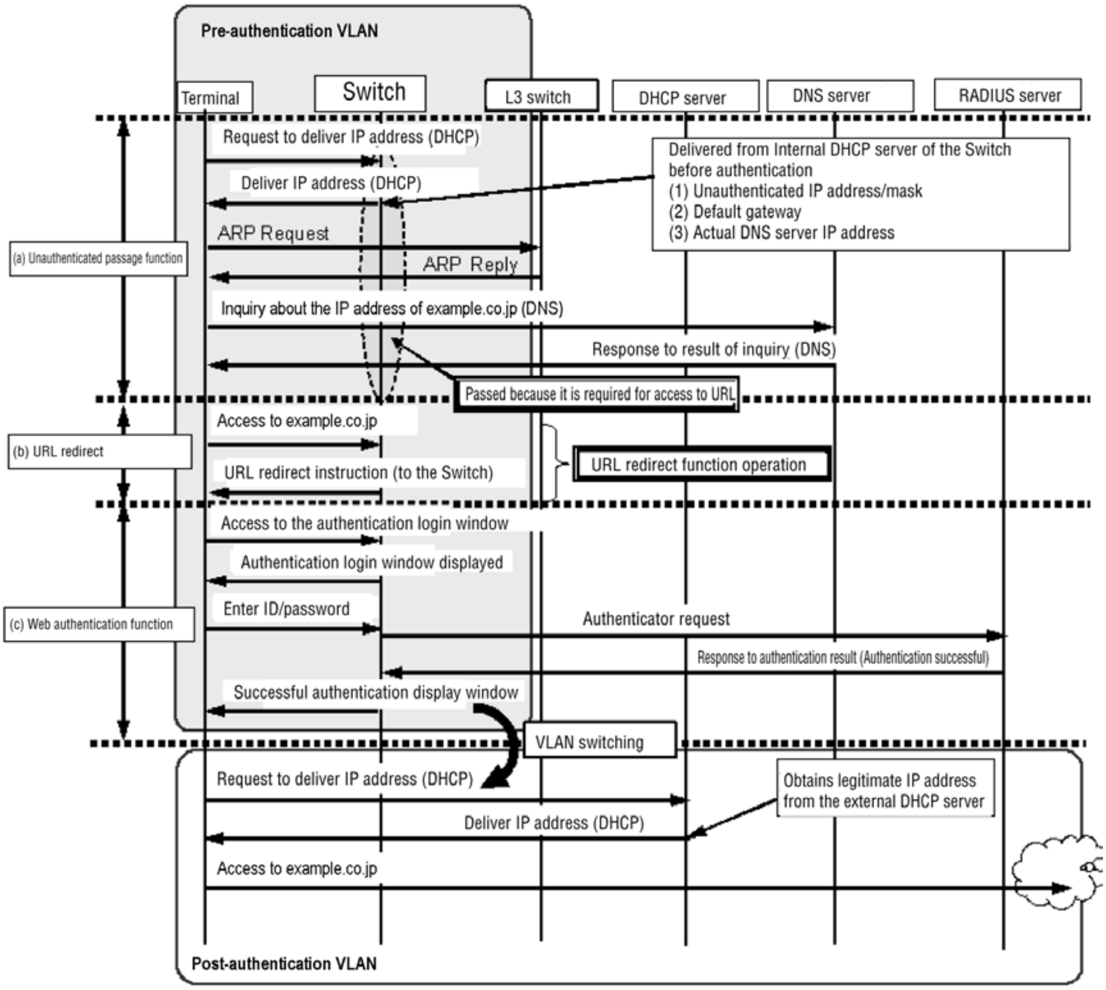
In dynamic VLAN mode, an authentication is executed in the following sequence.

Figure 8-12 Authentication operation (When using Web authentication IP address)



A

uthentication operation (when using URL redirection functionality)



Pre-authentication VLAN
Terminal
Switch
L3 switch
DHCP server
DNS server
RADIUS server
Request to deliver IP address (DHCP)
Deliver IP address (DHCP)
Delivered from Internal DHCP server of the Switch before authentication
(1) Unauthenticated IP address/mask
(2) Default gateway
(3) Actual DNS server IP address
ARP Request
ARP Reply
(a) Unauthenticated passage function
Inquiry about the IP address of example.co.jp (DNS)
Response to result of inquiry (DNS)
Passed because it is required for access to URL
Access to example.co.jp
(b) URL redirect
URL redirect instruction (to the Switch)
URL redirect function operation
Access to the authentication login window
Authentication login window displayed
Enter ID/password
(c) Web authentication function
Authenticator request
Response to authentication result (Authentication successful)
Successful authentication display window
VLAN switching
Request to deliver IP address (DHCP)
Obtains legitimate IP address from the external DHCP server
Deliver IP address (DHCP)
Access to example.co.jp
Post-authentication VLAN

8.4 Legacy mode

A terminal attached to a pre-authentication VLAN can communicate within the pre-authentication VLAN because frame reception allows the MAC address and the pre-authentication VLAN ID to be registered in the MAC address table as a dynamic entry. If authentication succeeds in legacy mode, the MAC address and the post-authentication VLAN ID is registered in a MAC VLAN, enabling the terminal to communicate within the post-authentication VLAN.

Users can log in using Web authentication IP address or the IP address of the pre-authentication VLAN. In either way, the local authentication method and the RADIUS authentication method can be used for authentication.

8.4.1 Authentication method group

A Web authentication method group uses the Switch default for all the Web authentication modes (legacy mode does not use an authentication method list.). For details, see the following sections:

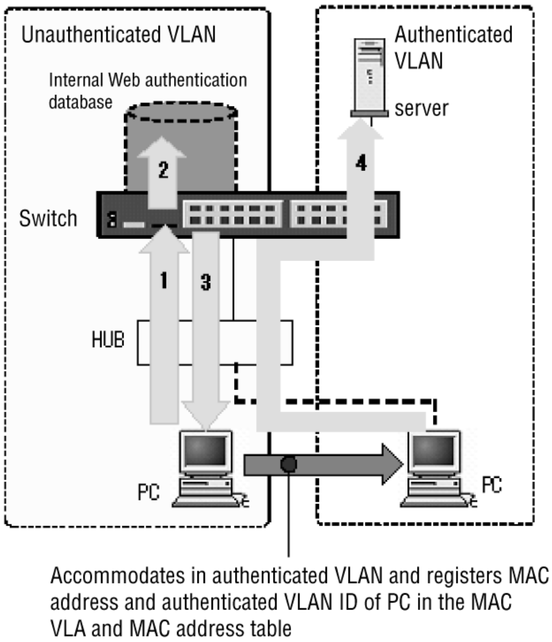
- *5.1.3 Authentication method groups*
- *5.3.3 Priority configuration for the Switch default local and RADIUS authentications*
- *5.3.1 RADIUS server information used with the Layer 2 authentication method*
- *9.2.1 Configuring the authentication method group and RADIUS server information*

(1) Switch default: Local authentication

Local authentication searches the internal Web authentication DB by a user ID and a password from the user seeking authentication and validates the credentials by comparing the registration details. If validated, the Switch attaches the terminal to the VLAN registered in the internal Web authentication DB and allows the terminal to communicate.

The following figure shows the authentication operation of the local authentication method.

Figure 8-14 Legacy mode (local authentication)



1. A PC user connected via a hub opens a Web browser and accesses the Switch using the specified URL.
2. The Switch validates the user ID and password by comparing them against the user information in the internal Web authentication DB.
3. If authentication succeeds, a page opens on the PC indicating that authentication was successful.
4. The authenticated PC is attached to the post-authentication VLAN and can connect to servers.

(a) Capacity limit of post-authentication VLANs

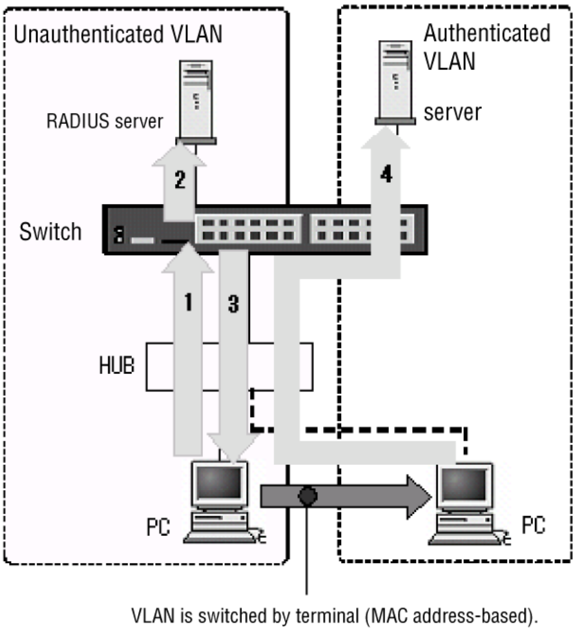
If the VLAN ID registered in the entry of the target user in the internal Web authentication DB is not included in the post-authentication VLAN configuration (the `web-authentication vlan` configuration command) in legacy mode, authentication fails.

(2) Switch default: RADIUS authentication

In a relatively large-scale configuration, it is recommended to use an external RADIUS server to execute authentication.

The following figure shows the operation of RADIUS authentication method.

Figure 8-15 Overview of legacy mode (example of RADIUS authentication)



1. A PC user connected via a hub opens a Web browser and accesses the Switch using the specified URL.
2. Authentication is executed using the user ID and password via the external RADIUS server.
3. If authentication succeeds, a page opens on the PC indicating that authentication was successful.
4. Based on the VLAN ID information sent from the RADIUS server, the authenticated PC is attached to the post-authentication VLAN and can connect to the server.

(a) Capacity limit of post-authentication VLANs

If the VLAN ID registered in the entry of the user in the RADIUS server is not included in the post-authentication VLAN configuration (the `web-authentication vlan` configuration command) in legacy mode, authentication fails.

8.4.2 Authentication functionality

(1) Web authentication IP address

Configuration is the same as for fixed VLAN mode. For details, see *(1) Web authentication IP address* in *8.2.2 Authentication functionality.*

(2) Specifying the automatically displayed URL after successful authentication

The configuration procedure is the same as for dynamic VLAN mode. For details, see *(3) Specifying the automatically displayed URL after successful authentication* in *8.3.2 Authentication functionality.*

(3) Specifying a forced authentication port

When a terminal connected to a port for which forced authentication is specified undergoes RADIUS authentication, and sending a request to the RADIUS server fails due to a line failure or the RADIUS does not respond, the terminal becomes authenticated.

In the Switch, the configuration for forced authentication can be shared among all authentication methods or be specified separately per authentication method. However, legacy mode does not operate when the configuration for forced authentication is shared among all authentication modes. Use the forced authentication functionality of Web authentication.

Configure the `web-authentication force-authorized vlan` configuration command on the port where forced authentication is allowed.

Forced authentication is successful when the following conditions are met.

Table 8-8 Conditions for successful forced authentication

Item	Condition
Configuration	All the following configurations have been set: ● `aaa authentication web-authentication`#1 ● `web-authentication radius-server host` or `radius-server host` ● `web-authentication system-auth-control` ● `vlan` *<VLAN ID list>* `mac-based`#2 ● `web-authentication vlan`#2 ● `web-authentication force-authorized vlan`#2, #3 ● `switchport mac vlan`#2, #3 ● `switchport mode mac-vlan`#3
Accounting log	The following accounting log is collected when an authentication request is sent to the RADIUS server: `No=21` `NOTICE:LOGIN: (`*<Additional information>*`) Login failed ; Failed to connection to RADIUS server.` *<Additional information>*`: MAC, USER, IP, PORT or CHGR, VLAN` Check the accounting log with the `show web-authentication logging` operation command.

#1

When using forced authentication by Switch default, set only `default group radius`.

#2

Set the same VLAN ID.

#3

Specify the same Ethernet port.

The authentication status of a terminal where authentication is permitted by forced authentication is canceled in the same way as for a normally authenticated terminal, as described in *(5) Logout from authenticated status* in *8.4.2 Authentication functionality.*

Furthermore, all operations from the start of requesting authentication to the RADIUS server to successful forced authentication are the same for shared forced authentication and per-authentication-method forced authentication. For details about the operations, see *(1) Behavior from the start of an RADIUS authentication request to permission for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

(4) Maximum number of authenticated users

The configuration procedure is the same as for dynamic VLAN mode. For details, see *(5) Maximum number of authenticated users* in *8.3.2 Authentication functionality.*

(5) Logout from authenticated status

Legacy mode provides the following means of logging out:

- Logout when maximum connection time is exceeded
- Logout by aging monitoring of the MAC address table
- Logout by receiving a special frame
- Logout resulting from changes to the VLAN configuration
- Logout using the Web interface
- Logout using an operation command

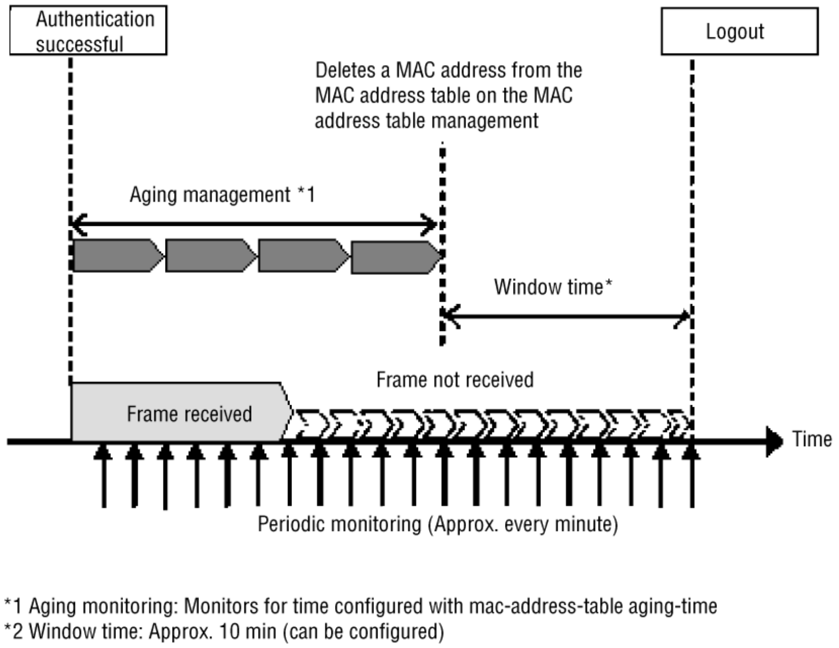
The means of logout other than "Logout by aging monitoring of the MAC address table" are the same as those of fixed VLAN mode. For details, see *(6) Logout from authenticated status* in *8.2.2 Authentication functionality.*

(a) Logout by aging monitoring of the MAC address table

Dynamic entries in the MAC address table are periodically monitored (at approximately one-minute intervals) for whether the MAC address of the terminal registered with a VLAN ID after legacy mode authentication has aged. Because of this, if the MAC address of the terminal has been deleted from the MAC address table due to an aging timeout, the authenticated status of Web authentication is automatically logged out and the terminal is changed to be attached to the pre-authentication VLAN ID. The user is not presented with a logout page.

Note that the Switch logs out the authentication status in order to prevent the authentication from being logged out due to an instant disconnection of the line, if the MAC address is not registered in the MAC address table within approximately 10 minutes (postponement time to being logged out) from when the MAC address is deleted from the MAC address table.

Figure 8-16 Overview of logout by aging monitoring of MAC address table



You can disable this functionality by using the `no web-authentication auto-logout` configuration command. (The configuration is possible so that the authentication is not forcibly logged out when aging timeout occurs.)

(6) Moving an authenticated terminal between ports and displaying the number of authenticated users

No roaming configurations are supported in legacy mode. If an attempt is made to move an authenticated terminal to another port, the following operations are performed:

1. When a terminal is authenticated, the number of authenticated users is counted up at the port where the terminal was authenticated.
2. If a terminal authenticated in legacy mode is moved to another port, it is allowed to continue communication as long as all of the following conditions are met:
   - The ports before and after the move are ports subject to legacy mode.
   - Post-authentication VLAN before moving has been specified by the configuration command `switchport mac vlan`.

   The moved terminal is allowed to continue communication until it is detected by monitoring of MAC address table aging. However, if DHCP snooping and filters are in use at the port after the move, whether communication can continue depends upon their conditions.

   If a terminal is moved under conditions other than the above, authentication is logged out. However, if an authenticated terminal is moved to the port that is not for authentication in legacy mode, the authentication might not be logged out.
3. During the next authentication, the Switch detects if the terminal is moved to

another port.

4. If legacy mode is available on the port to which the terminal is moved, the number of authenticated users is counted as follows:
   - If the count is the maximum number of authenticated users or less, the number of authenticated users at the port from which the terminal is moved is decreased and the authentication is registered at the destination port.
   - If the count exceeds the maximum number of authenticated users, the number of authenticated users at the port from which the terminal is moved is decreased and the authentication is logged out.
5. If the loss of a MAC address at the port before the move is detected by monitoring of MAC address table aging before the next time authentication is performed, the terminal is authenticated at the port after the move as a new terminal.

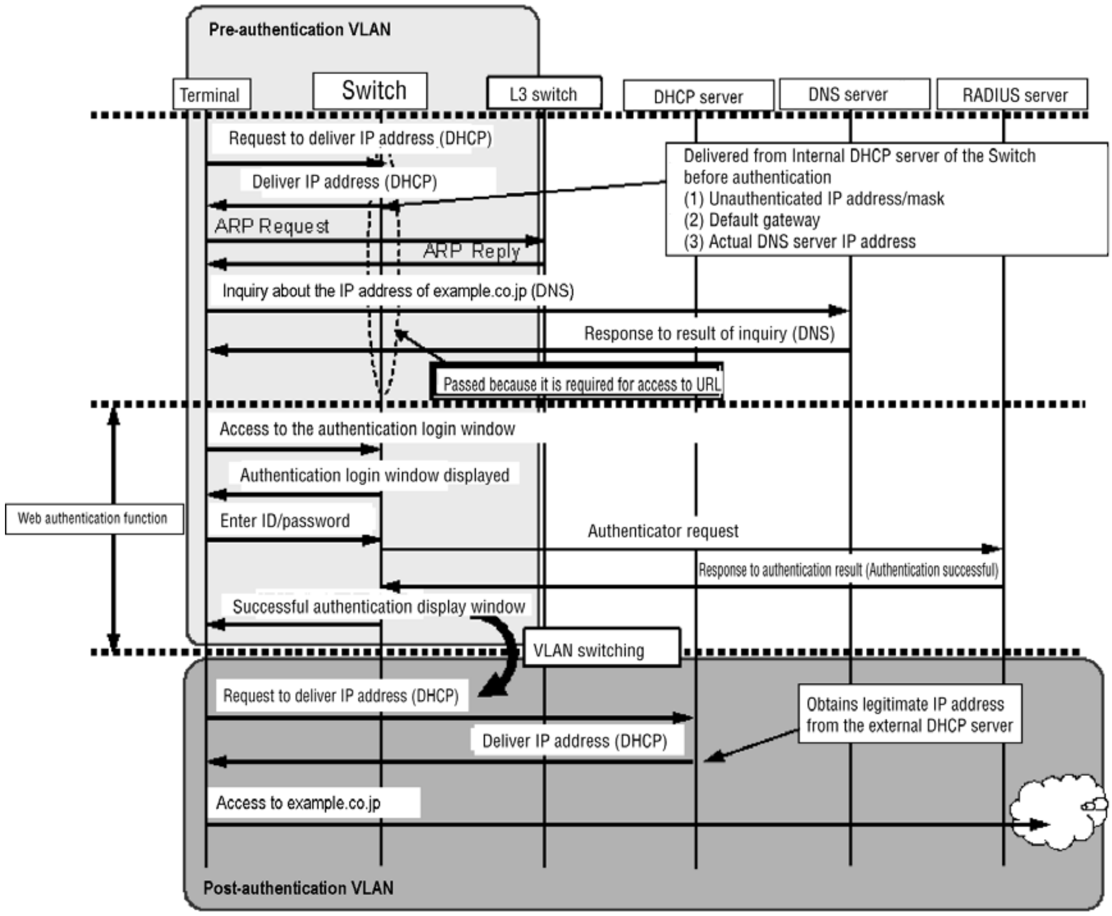
(7) User switching option

Configuration is the same as for fixed VLAN mode. For details, see *(8) User switching option* in *8.2.2 Authentication functionality.*

8.4.3 Authentication behavior

In legacy mode, an authentication is executed in the following sequence.

Figure 8-17 Authentication operation (When using the Web authentication IP address)



8.5 Accounting functionality

The Switch uses the following accounting functionality to record the results of Web authentication operations:

- Internal accounting log of the Switch
- Recording information to the RADIUS server accounting functionality
- Recording authentication information to the RADIUS server
- Outputting accounting log information to the syslog server

(1) Internal accounting log of the Switch

Operation log information, including Web authentication results and operation information, is recorded in the internal accounting log of the Switch.

The internal accounting log on the Switch can record up to 2,100 lines of information for all the authentication modes of Web authentication. When the maximum number of 2,100 lines is exceeded, the oldest lines are deleted, and the newest accounting log information is added.

The following table lists the accounting log information that is recorded.

Table 8-9 Accounting log entry types

Accounting log entry type	Description
LOGIN	Details on a login operation (succeeded, failed)
LOGOUT	Details on a logout operation (causes, etc.)
SYSTEM	Details on operations of Web authentication functionality (including roaming detection and forced authentication)

Table 8-10 Information output to the internal accounting log of the Switch

Accounting log entry type:		Time	User	IP	MAC	VLAN	Port#1	Message
LOGIN	Succeeded	Y	Y	Y#2	Y	Y#2	Y	Login success
	Failed	Y	Y	Y#3	Y#3	Y#3	Y#3	Cause for login failure
LOGOUT		Y	Y#3	Y#3	Y#3	Y#3	Y#3	Logout message
SYSTEM		Y	Y#3	Y#3	Y#3	N	Y#3	Message about operation of Web authentication functionality

Legend:

Y: Output

N: Not output

#1

Fixed VLAN mode, dynamic VLAN mode: The interface port number is output.

Legacy mode: The interface port number or the channel group number is output.

#2

In dynamic VLAN mode, the IP address displayed in the event of a successful authentication is that of the terminal prior to authentication. The VLAN ID is that of the post-authentication VLAN.

#3

Depending on the message, the information might not be output.

For details on messages, see *show web-authentication logging* in *26. Web Authentication* in the manual *Operation Command Reference*.

In addition, the following lists the output functionality of the accounting logs:

1. Console display per event

   Even when the `trace-monitor enable` operation command has been set, accounting log information is not output to the console each time an event occurs.

2. Operation command display

   By using the `web-authentication logging` operation command, you can display collected accounting log entries in chronological order starting from the latest one.

3. Output to the syslog server

   For details, see *(4) Outputting accounting log information to the syslog server.*

4. Private traps

   The Switch supports the functionality that issues private traps, which is triggered by the accounting log collected when a specific event of Web authentication occurs. Use configuration commands to specify whether traps are issued and also the type of traps that are issued.

Table 8-11 Accounting log entries (LOGIN/LOGOUT) and conditions for issuing private traps (1)

Accounting log entry type		**Configuration required for issuing private traps**	
		Command	**Parameter**
LOGIN	Succeeded	`snmp-server host`	`web-authentication`
		`snmp-server traps`	`web-authentication-trap all`

Accounting log entry type		Configuration required for issuing private traps	
		Command	**Parameter**
	Failed	`snmp-server host`	`web-authentication`
		Not configured, or one of the following configured:	
		`snmp-server traps`	`web-authentication-trap all`
		`snmp-server traps`	`web-authentication-trap failure`
LOGOUT		`snmp-server host`	`web-authentication`
		`snmp-server traps`	`web-authentication-trap all`

Table 8-12 Accounting log entry (SYSTEM) and conditions for issuing private traps (2)

Accounting log entry type: SYSTEM	Authentication mode	Configuration required for issuing private traps	
		Command	**Parameter**
Forced authentication	Fixed VLAN	`snmp-server host`	`web-authentication`
		`web-authentication static-vlan force-authorized`	`action trap`
	Dynamic VLAN	`snmp-server host`	`web-authentication`
		`web-authentication force-authorized vlan`	`action trap`
	Legacy	`snmp-server host`	`web-authentication`
		`web-authentication force-authorized vlan`	`action trap`
Roaming	Fixed VLAN	`snmp-server host`	`web-authentication`
		`web-authentication static-vlan roaming`	`action trap`
	Dynamic VLAN	`snmp-server host`	`web-authentication`
		`web-authentication roaming`	`action trap`
	Legacy	-- (There is no configuration because this mode is not supported.)	

A forced authentication private trap can also be issued when the configuration for forced authentication is shared among authentication modes. For details, see *(5) Private trap for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

(2) Recording information to the RADIUS server accounting functionality

You can enable the accounting functionality of the RADIUS server by using the `aaa accounting web-authentication` configuration command.

For details about the RADIUS attributes used when sending accounting information to the RADIUS server, see *8.6 Preparation.*

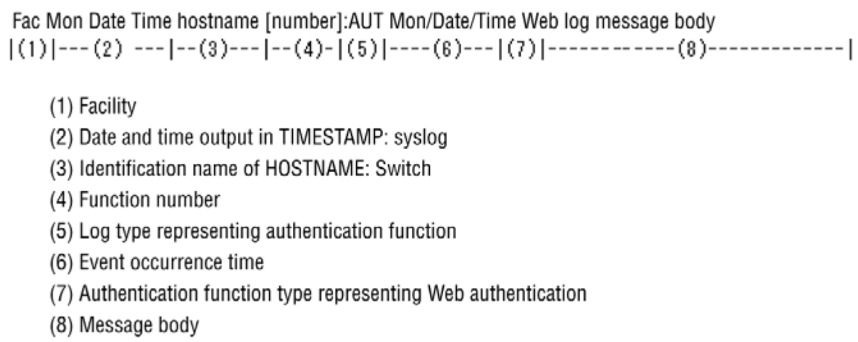
(3) Recording authentication information to the RADIUS server

If you are using RADIUS authentication, the accounting functionality of the RADIUS server records the success or failure of authentication attempts. Note that the information that is recorded differs between RADIUS server implementations. For details, see the documentation for the RADIUS server deployed in your network.

(4) Outputting accounting log information to the syslog server

Accounting log information for Web authentication and operation log information for all Switches are output to all the syslog servers defined in the `syslog` configuration.

Figure 8-18 Format of output to syslog server



For details about log output to the syslog server, see *22. Log Data Output Functionality.*

Note that the Switch cannot specify for outputting or preventing from outputting only the accounting log information of Web authentication to the syslog server.

8.6 Preparation

8.6.1 For local authentication

To use the local authentication method, the following preparations are required:

- Configuration definition
- Registering the internal Web authentication DB
- Backing up the internal Web authentication DB
- Restoring the internal Web authentication DB

(1) Configuration definition

To use Web authentication, configure VLAN information and Web authentication on the Switch by using the configuration commands. (See *9. Web Authentication Configuration and Operation.)*

(2) Registering the internal Web authentication DB

Before using the local authentication method, you must register the user information (the user ID, password, and post-authentication VLAN ID of a terminal seeking authentication) in the internal Web authentication DB using an operation command.

The procedure of registering the information in the internal Web authentication DB includes editing of the user information (adding, changing, deleting) and incorporating the updates in the internal Web authentication DB. The procedure is described below.

You need to complete the environmental settings for Web authentication and configuration before adding user information.

- Add the user information (the user ID, password, and post-authentication VLAN ID of the terminal seeking authentication) by using the `set web-authentication user` operation command.
- To change a registered password, use the `set web-authentication passwd` operation command.
- To change a registered post-authentication VLAN ID, use the `set web-authentication vlan` operation command.
- To delete registered user information, use the `remove web-authentication user` operation command.
- Incorporate the edited user information in the internal Web authentication DB by executing the `commit web-authentication` operation command.

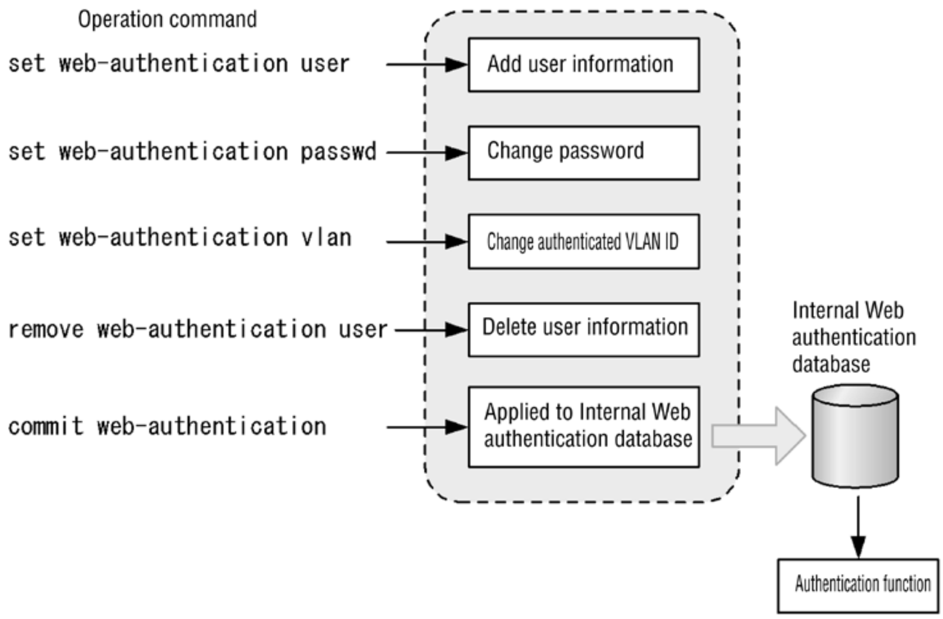
In addition, the user address information edited prior to execution of the `commit web-authentication` operation command can be viewed by using the `show web-authentication user` operation.

The following table shows the range of the number of characters and available characters for user ID and password.

Table 8-13 Range of the number of characters and available characters

Range of the number of characters for user ID	Range of the number of characters for password	Available character
1 to 128 characters	1 to 32 characters	0 to 9 A to Z a to z at mark (@) hyphen (-) underscore (_) dot (.)

Figure 8-19 Editing user information and incorporating updates into the internal Web authentication DB



(3) Backing up the internal Web authentication DB

Use the `store web-authentication` operation command to back up the internal Web authentication DB.

(4) Restoring the internal Web authentication DB

Use the `load web-authentication` operation command to restore the internal Web authentication DB from a backup file you created.

Note that any recent editing or registrations you made using the `set web-authentication user` command or similar will be lost and replaced with the contents of the backup file.

8.6.2 For RADIUS authentication

To perform RADIUS authentication, the following preparations are required:

- Configuration definition
- Preparing the RADIUS server

(1) Configuration definition

To user Web authentication, configure the information of VLAN and Web authentication on the Switch using the configuration commands. (See *9. Web Authentication Configuration and Operation.)*

(2) Preparing the RADIUS server

(a) RADIUS attributes to be used

The following table describes the RADIUS attribute names used by the Switch.

Table 8-14 Attribute names used in authentication (part 1: Access-Request)

Attribute name	Type value	Description
`User-Name`	1	User ID to be authenticated
`User-Password`	2	User password.
`NAS-IP-Address`	4	IP address of the Switch requesting authentication. From among the VLAN interfaces that have an IP address registered, the IP address of the smallest VLAN ID is used.
`NAS-Port`	5	● Fixed VLAN mode: `IfIndex` of authentication unit under authentication ● Dynamic VLAN mode: `IfIndex` of authentication unit under authentication ● Legacy mode: 4296
`Service-Type`	6	The type of service to be provided Fixed as `Framed(2)`.
`State`	24	Text character string When performing `Access-Request` for `Access-Challenge`, if `Access-Challenge` has `State`, the `State` information held on the Switch is added.
`Called-Station-Id`	30	Port MAC address (lowercase ASCII#, separated by hyphens (`-`))
`Calling-Station-Id`	31	Terminal MAC address (lowercase ASCII+, separtated by hyphens (`-`))
`NAS-Identifier`	32	● Fixed VLAN mode VLAN ID of VLAN to which a terminal that is requesting authentication belongs For VLAN10, `10` ● Dynamic VLAN mode Character string specified by the `hostname` configuration command ● Legacy mode Character string specified by the `hostname` configuration command
`NAS-Port-Type`	61	Type of the physical port used by a terminal for authentication Virtual(5)

Attribute name	Type value	Description
Connect-Info	77	Character string indicating the connection characteristics ● Fixed VLAN mode: Physical port ("CONNECT Ethernet") ● Dynamic VLAN mode: Physical port ("CONNECT Ethernet") ● Legacy mode: ("CONNECT DVLAN")
NAS-Port-Id	87	Character string for port identification (*x* and *y* represent numbers) ● Fixed VLAN mode: "Port *x*/*y*" ● Dynamic VLAN mode: "Port *x*/*y*" ● Legacy mode: "DVLAN *x*"

#

The MAC addresses for Called-Station-Id and Calling-Station-Id are lower case when used by the Switch. However, the letters a to f in the MAC addresses can be converted to upper-case letters by using the radius-server attribute station-id capitalize configuration command.

Table 8-15 Attributes used for one-time password authentication (Part 2: Access-Challenge) [OP-OTP]

Attribute name	Type value	Description
Reply-Message	18	Text character string#. The value of this attribute is displayed as a message in the Reply-Message page displayed during one-time password authentication.
State	24	Text character string. If State is specified for Access-Challenge used for one-time password authentication, the Switch retains the State information. For Access-Request corresponding to Access-Challenge, the State information held on the Switch is added.

#

The Switch collects the Reply-Message character string as accounting log information.

Table 8-16 Attributes used in authentication (Part 3: Access-Accept)

Attribute name	Type value	Description
Service-Type	6	The type of service to be provided Fixed as Framed(2).
Filter-Id	11	Text character string Used in multistep authentication#1.

Attribute name	Type value	Description
Reply-Message	18	Not used[#2].
Tunnel-Type	64	Tunnel type[#3] Fixed as VLAN(13).
Tunnel-Medium-Type	65	Indicates the protocol to use to create a tunnel[#3]. Fixed as IEEE 802(6).
Tunnel-Private-Group-ID	81	Character string for VLAN identification[#4]. The character strings can be formatted as follows: (1) As a character string indicating a VLAN ID (2) As a character string containing the word "VLAN" followed by a VLAN ID The character string cannot contain spaces. If it does, VLAN assignment will fail. (3) Character string representing the name of a VLAN defined for a VLAN interface by the name configuration command (The smaller VLAN ID takes precedence.)[#5] Examples VLAN ID: 10 Configuration command name: Authen_VLAN For (1): "10" For (2): "VLAN10" For (3): Authen_VLAN

#1

For details about character strings used in multistep authentication, see *12. Multistep authentication.*

#2

The Switch collects the Reply-Message character string as accounting log information.

#3

The tag area is ignored.

#4

The Switch selects a character string format and identifies the VLAN ID in accordance with the following conditions:

1. Conditions for selecting character string formats (1), (2) and (3) for Tunnel-Private-Group-ID:
   - Format (1) is used for a character string that begins with a number from 0 to 9.
   - Format (2) is used for a character string that begins with VLAN plus a number from 0 to 9.
   - Format (3) is used for a character string other than the above character strings.

   In addition, when the first byte is in the range from 0x00 to 0x1f, it means that a tag is present but the tag area is ignored.

2. Conditions for identifying the VLAN ID from character strings in formats (1) and (2):

   - Converts only the numerical characters 0 to 9 into a decimal number and its first four characters become valid. (The fifth and the subsequent characters are all ignored.)

     Example:`0010` is equivalent to `010` or `10`, and it is handled as VLAN ID = 10.

     However, `01234` is handled as VLAN ID = 123.

   - If a character other than 0 through 9 exists in the middle of the character string, the character is considered to be the end of the string.

     Example:`12+3` is handled as VLAN ID = 12.

#5

For details about specifying the VLAN name by using the `name` configuration command, see *5.4.2 Specifying post-authentication VLANs by VLAN name.*

Table 8-17 Attribute names used in RADIUS accounting functionality

Attribute name	**Type value**	**Description**
`User-Name`	1	User ID to be authenticated
`NAS-IP-Address`	4	IP address of the Switch requesting authentication From among the VLAN interfaces that have an IP address registered, the IP address of the smallest VLAN ID is used.
`NAS-Port`	5	● Fixed VLAN mode: `IfIndex` of authentication unit under authentication ● Dynamic VLAN mode: `IfIndex` of authentication unit under authentication ● Legacy mode: 4296
`Service-Type`	6	The type of service to be provided. Fixed as `Framed(2)`.
`Calling-Station-Id`	31	The MAC address of the authenticated terminal (lowercase ASCII#, separated by hyphens (`-`))
`NAS-Identifier`	32	● Fixed VLAN mode VLAN ID of VLAN to which a terminal that is requesting authentication belongs For VLAN10: `10` ● Dynamic VLAN mode Character string specified by the `hostname` configuration command ● Legacy mode Character string specified by the `hostname` configuration command

Attribute name	Type value	Description
Acct-Status-Type	40	Accounting request type Start(1), Stop(2)
Acct-Delay-Time	41	Accounting information (send delay time) (in seconds)
Acct-Input-Octets	42	Accounting information (number of received octets) Fixed at (0).
Acct-Output-Octets	43	Accounting information (number of sent octets) Fixed at (0).
Acct-Session-Id	44	ID for accounting information identification
Acct-Authentic	45	Authentication method. RADIUS(1) and Local(2).
Acct-Session-Time	46	Accounting information (session duration time) Fixed at (0).
Acct-Input-Packets	47	Accounting information (number of received packets) Fixed at (0).
Acct-Output-Packets	48	Accounting information (number of sent packets) Fixed at (0).
Acct-Terminate-Cause	49	Accounting information (cause of session termination). See *Table 8-18 Termination causes returned by Acct-Terminate-Cause.*
NAS-Port-Type	61	Type of physical port used by a terminal for authentication Fixed at `Virtual(5)`
NAS-Port-Id	87	Character string for port identification (*x* and *y* represent numbers) ● Fixed VLAN mode: `"Port` *x/y*`"` ● Dynamic VLAN mode: `"Port` *x/y*`"` ● Legacy mode: `"DVLAN` *x*`"`

#

The MAC addresses for `Calling-Station-Id` are lower case when used by the Switch. However, the letters `a` to `f` in the MAC addresses can be converted to upper-case letters by using the `radius-server attribute station-id capitalize` configuration command.

Table 8-18 Termination causes returned by Acct-Terminate-Cause

Attribute name	Type value	Description
User Request	1	Disconnected due to the logout request on the Web authentication page. Disconnection due to detection of a terminal move
Idle Timeout	4	Disconnection due to non-communication continuing for a certain

Attribute name	Type value	Description
		period of time
Session Timeout	5	Disconnection due to session expiration
Admin Reset	6	Disconnected by the administrator: ● Deletion of web-authentication port in the configuration: Also includes disconnection causes due to changes to other authentication configurations and operation commands.
Port Preempt	13	Session was terminated to provide a user having higher priority with services. For switching users, the user to be switched from is logged out. (When configuring the web-authentication user replacement configuration command)
Port Reinitialized	21	The port's MAC address has been reinitialized. ● When a port is linked down ● When vlan is deleted from a port by the configuration ● When shutdown is set by the configuration ● When *the* inactivate operation command is executed

(b) Recording information to be configured to the RADIUS server

Before using the RADIUS authentication method, configure the user ID, password, and VLAN ID for each user in the RADIUS server.

For details about how to configure the RADIUS server, see the documentation for the RADIUS server deployed in your network.

The following shows an example of configuring VLAN information for each user in the RADIUS server:

- For fixed VLAN mode: The VLAN ID of the VLAN to which the terminal seeking authentication belongs is 20.
- For dynamic VLAN mode and legacy mode: The VLAN ID of the post-authentication VLAN is 400
- Configuration using the name configuration command: GroupA-Network

Table 8-19 Example of RADIUS server configuration

Configuration item	Description
User-Name	User ID for authentication. Range of the number of characters: 1 to 128 characters Available characters: Range of character code is from 0x21 to 0x7E#
Auth-Type	Local

Configuration item	Description
`User-Password`	Password for the user seeking authentication Range of the number of characters: 1 to 32 characters Available characters: Range of character code is from 0x21 to 0x7E#
`Tunnel-Type`	`Virtual VLAN` (value of 13)
`NAS-Identifier`	For fixed VLAN mode ● `"20"` The VLAN ID of the VLAN to which the terminal seeking authentication is defined as a number.
`Tunnel-Medium-Type`	`IEEE-802` (value of 6)
`Tunnel-Private-Group-ID`	For dynamic VLAN mode and legacy mode: Any of the following formats is used: ● `"400"` The post-authentication VLAN ID is defined as a number. ● `"VLAN0400"` The post-authentication VLAN ID is defined as a number immediately after the character string `VLAN`. ● `"GroupA-Network"` A character string representing a VLAN name defined by the `name` configuration command
Authentication method	PAP

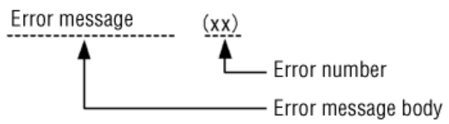
#

For details about the characters in the range of character code, see *List of character codes* in the manual *Configuration Command Reference*.

8.7 Authentication error messages

The following figure shows the format of the error messages displayed on the authentication error page.

Figure 8-20 Format of authentication error messages



The table below describes the cause of each authentication error you might encounter.

Table 8-20 Authentication error messages and their causes

Error message	Error no.	Cause
`User ID or password is wrong. Please enter correct user ID and password.`	11	You did not specify a user ID.
	12	The length of the login user ID exceeded the maximum number of characters.
	13	You did not specify a password.
	14	The specified user ID is not registered in the internal Web authentication DB.
	15	The length of the password exceeded the maximum number of characters or the password is not registered.
	22	An attempt to log in again from an authenticated terminal using local authentication failed because the user entered the wrong password.
`RADIUS: Authentication reject.`	31	A response other than `Accept` was received from the RADIUS server.
`RADIUS: No authentication response.`	32	No response was received from the RADIUS server. This error is triggered if communication with the RADIUS server times out or the RADIUS server is not configured.

Error message	Error no.	Cause
`You cannot login by this machine.`	33	The possible causes are as follows: ● The post-authentication VLAN specified by the RADIUS server does not appear in the Web authentication definition. ● The post-authentication VLAN in dynamic VLAN mode is not MAC VLAN. ● The post-authentication VLAN in legacy mode is not the MAC VLAN of the port. ● No VLAN interface is assigned to the post-authentication VLAN. ● The VLAN configured in the RADIUS attribute of the RADIUS server crashed with the native VLAN of the port for authentication. ● The VLAN configured in the RADIUS attribute of the RADIUS server crashed with the VLAN configured using the `switchport mac dot1q vlan` configuration command.
	35	The possible causes are as follows: ● The port is not specified as that in fixed VLAN mode or in dynamic VLAN mode. ● Because dynamic VLAN mode and legacy mode of IEEE 802.1X/Web authentication/MAC authentication coexist on the same port, the authentication in legacy mode is not possible. ● The terminal is connected to a link-down port.
	36	The VLAN containing the authenticated terminal has been suspended.
	37	In RADIUS authentication, the authentication failed because the number of users logged in exceeded the capacity of the device.
	41	A login request was received under a different user ID from the terminal having the same MAC address.
	42	The possible causes are as follows: ● The VLAN ID specified in the internal Web authentication DB does not match the VLAN specified in the Web authentication definition. ● The post-authentication VLAN in dynamic VLAN mode is not MAC VLAN. ● The post-authentication VLAN in legacy mode is not the MAC VLAN of the port. ● No VLAN interface is assigned to the post-authentication VLAN. ● The VLAN configured in the internal Web authentication DB crashed with the native VLAN on the port for authentication. ● The VLAN configured in the internal Web authentication DB crashed with the VLAN configured using the `switchport mac`

Error message	Error no.	Cause
		dot1q vlan configuration command.
	44	The possible causes are as follows: ● The terminal has already been authenticated by different authentication functionality. ● The MAC address has already been registered in the MAC address table by the mac-address-table static configuration command. ● The MAC address of the terminal has already been registered in the MAC VLAN by the mac-address configuration command.
	45	The possible causes are as follows: ● The port is not specified as that in fixed VLAN mode or in dynamic VLAN mode. ● Because dynamic VLAN mode and legacy mode of IEEE 802.1X/Web authentication/MAC authentication coexist on the same port, the authentication in legacy mode is not possible. ● The terminal is connected to a link-down port.
	46	The VLAN containing the authenticated terminal has been suspended.
	47	The authentication failed because the number of user logged in exceeded the capacity of the device.
	78	When the MAC address is registered in the MAC address table, the number of users logged in exceeded the capacity of the device. Alternatively, the MAC address might not be able to be registered in the MAC address table due to the restrictions of the hardware.
	101	The configuration of Web authentication is invalid.
	103	During the authentication (AUTHENTICATING), a login request was received from a terminal having the same MAC address.

Error message	Error no.	Cause
`Sorry, you cannot login just now.` `Please try again after a while.`	51	The Switch could not resolve the terminal's MAC address from its IP address.
	52	The possible causes are as follows: ● Multistep authentication is not available because the terminal's MAC authentication or IEEE 802.1X has been canceled. ● Multistep authentication is not available because another authentication has been completed.
`The system error occurred.` `Please contact the system administrator.`	64	The Switch could not access the RADIUS server.
`A fatal error occurred.` `Please inform the system administrator.`	71	An internal Web authentication error occurred (RADIUS authentication requests that exceeded the capacity occurred simultaneously.)
	72	The Switch could not register the MAC address of the authenticated terminal in the MAC VLAN.
`Sorry, you cannot logout just now.` `Please try again after a while.`	81	The Switch could not resolve a MAC address for the IP address of a terminal from which it received a logout request.
`The client PC is not authenticated.`	82	A logout request was received from a terminal that is not logged in.

Error resolution by error number

- 1x: Log in again using the correct user ID and password.
- 3x: Review the Web authentication information of the RADIUS server and the Switch.
- 4x: Review the configuration of the internal Web authentication DB.
- 5x: Repeat the login process after a while.
- 6x: Review the configuration of the RADIUS server information of the Switch.
- 7x: Check the system configuration.
- 8x: Check that the URL is correct and repeat the logout process.
- 9x: The 9x code appears when the one-time password authentication is used for Web authentication. For details, see *14. One-time Password Authentication [OP-OTP].*
- 101: Review the Web authentication information of the RADIUS server and the Switch.
- 103: Check that the login process is completed with another Web browser page.

#

For details about multistep authentication, see *12. Multistep authentication.*

8.8 Notes for Web authentication

8.8.1 Interoperability of Web authentication and other functionality

For details about the interoperability of Web authentication and other functionality, see *5.9.3 Interoperability of the Layer 2 authentication functionality and other functionality.*

8.8.2 Notes for all authentication modes

(1) Using a Web authentication IP address and URL redirection functionality

[Fixed VLAN mode] [Dynamic VLAN mode]

Users can log in using Web authentication IP address or using the URL redirection functionality. Either way, the local authentication method and the RADIUS authentication method are available for authentication.

Therefore, you must set both, or either Web authentication IP address, or URL redirection.

(2) Using the URL redirection functionality

[Fixed VLAN mode] [Dynamic VLAN mode]

(a) Setting IP addresses

To use the URL redirection, always set an IP address in the VLAN.

(b) Restrictions on using the functionality in a proxy environment

If all the following conditions are met when the functionality is used, the terminal cannot be authenticated because the Web authentication login page is not displayed on the terminal.

- A proxy is configured for the network.
- The URL redirection is enabled.

  (The `web-authentication redirect enable` configuration command is the default.)
- The Web authentication login page protocol HTTPS is specified for URL redirection.

  (The `web-authentication redirect-mode` configuration command is the default.)

In this case, configure the following on the Switch and the terminal seeking authentication.

- Switch side: Configure a Web authentication IP address.
- Terminal seeking authentication side: Configure a Web authentication IP address as a proxy exception address.

(c) External URL access via HTTPS from an unauthenticated terminal

When accessing a URL via HTTPS from an unauthenticated terminal, if the domain name of the certificate registered on the Switch does not match that of the terminal, a warning message indicating certificate mismatching appears on the Web browser. Even in that case, if you select the **Continue** operation, the Web authentication Login page is displayed and you can proceed with login processing.

(d) Access port (port waiting for TCP) number for Web authentication

The Switch does not support the specification of an access port for Web authentication.

The `web-authentication redirect tcp-port` and `web-authentication web-port` configuration commands are specified for use with the URL redirection functionality.

(3) Setting the lease time for IP addresses from the DHCP server

When using a DHCP server to assign pre-authentication IP addresses to terminals seeking authentication, specify as short a lease time as possible for IP addresses assigned by the DHCP server.

The smallest lease time the internal DHCP server of the Switch allows is 10 seconds. However, specifying such a small value in an environment with a large number of users can place a heavy load on the Switch. Consider this factor when setting the lease time.

(4) When changing the internal Web authentication DB

Additions and changes made for the internal Web authentication DB using operation commands do not apply to current authenticated users. The updates are incorporated from the next login.

(5) When restarting the Web authentication by restarting the Switch

If the Switch is restarted, all the current authentications are canceled. In this case, users need to perform re-authentication manually after the Switch restarts.

(6) Setting the maximum connection time

When shortening or extending the maximum connection time using the `web-authentication max-timer` configuration command, the change does not apply to the current authenticated user. The setting is enabled from the next login.

(7) Note on extending authentication connection time

When the user logs in again with the terminal authenticated, if local authentication (RADIUS authentication when using RADIUS authentication) succeeds, the authentication time can be extended. If the authentication fails, the time cannot be extended.

(8) Terminal IP address after logout

[Dynamic VLAN mode] [Legacy mode]

After logging out of the terminal (logout through the web page, forced logout due to exceeded connection time, or forced logout due to an aging timeout of the MAC address table), change the terminal's IP address to the IP address of the terminal before the authentication.

- In the case of a manual setting, manually set the terminal's IP address to the IP address of the terminal before the authentication.
- When using the DHCP server, delete the terminal's IP address, and then instruct the DHCP server to re-assign an IP address to the terminal. In Windows, for example, execute `ipconfig /release` and then `ipconfig /renew` from the command prompt.

(9) Using a forced authentication port

1. Be especially careful when using this functionality, as it can pose a security

problem.

2. This functionality supports only RADIUS authentication.

   When using forced authentication, set only the RADIUS authentication method. When setting both local authentication and RADIUS authentication as shown below, forced authentication does not operate even if it has been configured.

   - `aaa authentication web-authentication default gourp radius local`
   - `aaa authentication web-authentication default local gourp radius`

3. Although the Switch has the forced authentication functionality both for common to all authentication modes and for Web authentication, these two cannot be simultaneously configured. Prior to using the authentication functionality, see *(4) Interoperability of this functionality and forced authentication of each authentication method* in *5.4.6 Forced authentication common to all authentication modes.*

(10) Restriction when using roaming with DHCP snooping

[Fixed VLAN mode] [Dynamic VLAN mode]

When the DHCP snooping functionality is used with the `web-authentication static-vlan roaming` and `web-authentication roaming` configuration commands set, if an authenticated terminal is moved to another port, the authentication status is transited to the port to which the terminal has been moved, but the terminal cannot communicate because the binding database is not updated.

(11) Moving between ports and maximum number of authenticated users

[Fixed VLAN mode] [Dynamic VLAN mode]

The Switch checks the maximum number of authenticated users for only newly authenticated users.

Because of this, if an authenticated terminal moves between ports, the Switch does not check the maximum number of authenticated users at the port where the terminal is moved.

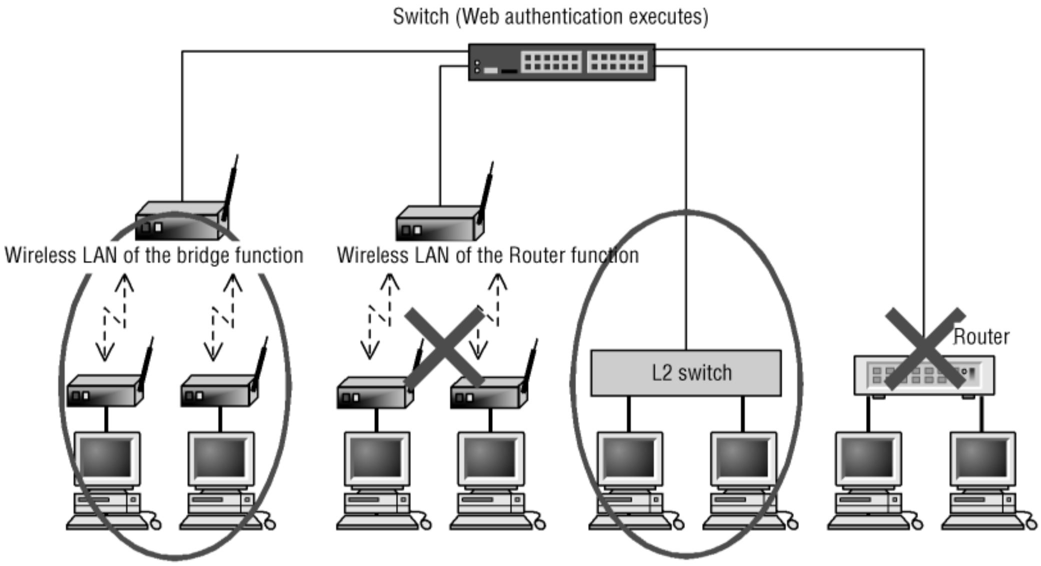
(12) Connecting devices between the terminal and the Switch

Do not connect a proxy server, router, or similar piece of equipment to the Switch.

If the terminal undergoing authentication is behind a device (such as a proxy server or router) that substitutes its own MAC address in outgoing packets, the Switch will identify the MAC address of the device as belonging to the terminal. This results in an inability to control authentication at the level of individual terminals.

Be careful when connecting a hub without inter-port relay-blocking functionality or a wireless LAN downstream from the Switch. PCs attached to that hub or wireless LAN will be able to communicate with each other regardless of their authentication status.

Figure 8-21 Connections between terminals and the Switch



8.8.3 Notes on using fixed VLAN mode

(1) Fixed VLAN mode port

Fixed VLAN mode can operate only on ports in an Ethernet interface.

In fixed VLAN mode, Web authentication can be processed with a tagged frame at an access port or trunk port and a MAC port where tagged frame relay is made available (by the `switchport mac dot1q vlan` configuration command).

8.8.4 Notes on using dynamic VLAN mode and legacy mode

(1) Notes on configuring aging time for MAC address learning

Note that if a terminal is not used for a while when the aging time of the MAC address table is set to be short, the terminal is forcibly logged out. Set the `no web-authentication auto-logout` configuration command in order to prevent being forcibly logged out.

(2) When receiving no communication from the terminal after switching to post-authentication VLAN

If non-communication is received from the terminal after switching to post-authentication VLAN, MAC address is not learned. In this case, the MAC address of the terminal will not appear in the MAC address table, and the terminal will be forcibly logged out. Be sure to make the terminal to communicate after it is authenticated. Set the `no web-authentication auto-logout` configuration command in order to prevent being forcibly logged out.

(3) Interoperability of legacy mode and multistep authentication

The Switch cannot use legacy mode and multistep authentication simultaneously. To use legacy mode, make sure that multistep authentication is not configured for the Switch.

8.9 Replacing Web authentication pages

For the file set types and the authentication page types used for the Switch's functionality of replacing Web authentication pages, the following terms are used.

Table 8-21 Terms used for the functionality of replacing Web authentication pages

Term		Description
File set		Generic term of a directory storing HTML files (`login.html`, `logout.html`, etc.) required for performing Web authentication.
	Default file set	Directory stored in the initial status on the Switch, and all the HTML files in the directory are in the initial status.
	Custom file set	Directory storing a user-created HTML file for Web authentication
Authentication page	Basic Web authentication page	The standard Web authentication page to be displayed when usual Web authentication is executed. For the basic Web authentication page, the Switch contains the default file set that can be replaced with a custom file set. (This is the authentication page usually used for Web authentication for the Switch.)
	Individual Web authentication page	Web authentication page to be displayed when a specific condition is met after the condition is associated with a custom file set. The Switch does not contain the default file set to add an individual Web authentication page. A custom file set is used to add the page. (This is the authentication page used for specifying an individual Web authentication page by port of the Switch.)

8.9.1 Replacing Web authentication pages

Use an external device (a PC) to create pages that appear during the Web authentication process, such as the login and logout pages (hereafter referred to as *Web authentication pages*), and use the `set web-authentication html-files` operation command to replace the pages on the Switch as the custom file set.

The pages you can replace are listed below.

Table 8-22 Replaceable page files

File type	HTML file name	Remarks
Login page	`login.html`	Required for the custom file set at the time of replacement
Logout page	`logout.html`	
Login success page	`loginOK.html`	

File type	HTML file name	Remarks
Login failed page	`loginNG.html`	
Logout completed page	`logoutOK.html`	
Logout failed page	`logoutNG.html`	
Authentication-in-progress	`loginProcess.html`	Used for one-time password authentication#
Icon	`favicon.ico`	

#

When using one-time password authentication, an authentication-in-progress page can be treated as a replaceable file. For details about an authentication-in-progress file, see *14. One-time Password Authentication [OP-OTP].*

The basic Web authentication page and the individual Web authentication page shown in *Table 8-21 Terms used for the functionality of replacing Web authentication pages* can be registered on the Switch as a custom file set.

- Custom file set of the basic Web authentication page

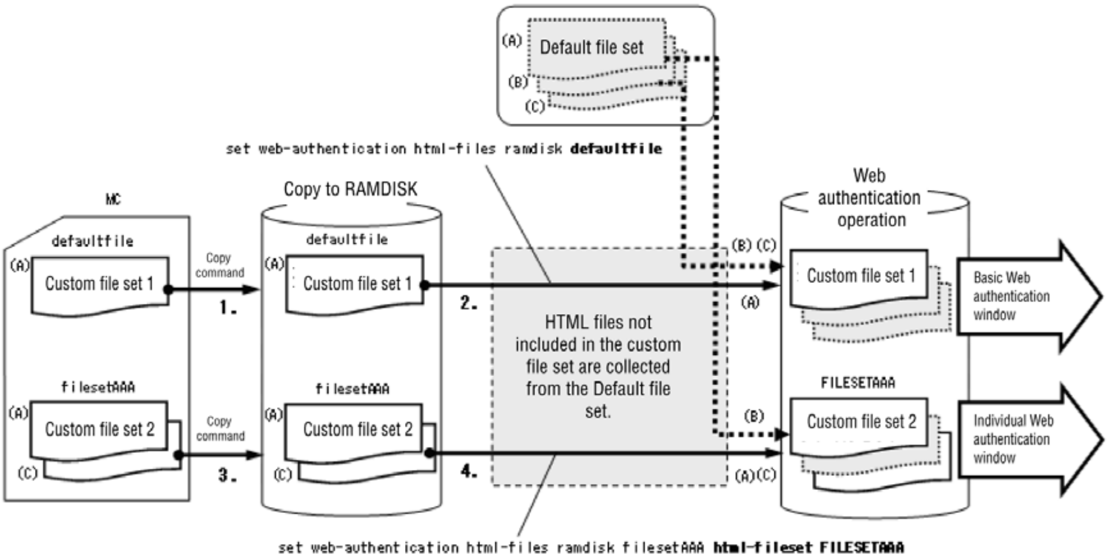
  Use the `set web-authentication html-files` operation command to register the specified RAMDISK file set on the Switch, and replace the basic authentication page currently in operation with the page file of the file set. In addition, you can simultaneously register an image file such as a GIF file as well as page files.

- Custom file set of the individual Web authentication page

  Use the `set web-authentication html-files` operation command to the file set on the Switch in the same fashion as the basic Web authentication page. However, individually register the file set with the file set name specified by the `html-fileset` parameter.

The following figure shows the procedure of registering a custom file set saved on a memory card as the individual Web authentication page. For an individual Web authentication page, you can register up to four types of files sets other than the basic Web authenticating page.

Figure 8-22 Procedure of registering a custom file set



1. Copy the custom file set 1 (`defaultfile`) on the memory card to the RAMDISK of the Switch via the `copy` operation command.
2. Specify the file set name `defaultfile` that has been copied to the RAMDISK, because `defaultfile` is used as the basic Web authentication page (set `web-authentication html-files ramdisk defaultfile`).

   The files that are not included in the custom file set ((B) and (C) in the above figure) are supplied from the default file set.
3. Copy the custom file set 2 (`filesetAAA`) to the RAMDISK of the Switch via the `copy` operation command.
4. `FilesetAAA` is used as the individual Web authentication page, so specify the file set name `filesetAAA` copied to the RAMDISK as the file set name to be registered on the Switch (`FILESETAAA` in the figure) (`set web-authentication html-files ramdisk filesetAAA html-fileset FILESETAAA`).

   The files that are not included in the custom file set ((B) in the above figure) are supplied from the default file set.

Note that during registration the command checks only the size of the file, not its contents. Make sure that the HTML and image files in the folder you specify work correctly before you replace the default pages.

For details about the total size of custom file sets and the number of the files that can be registered, see *3.2 Capacity limits* in the *Configuration Guide Vol. 1*.

Use the `clear web-authentication html-files` operation command to delete the Web authentication pages you have registered. In this case, the default pages are restored.

You can also replace the authentication error messages listed in *Table 8-20 Authentication error messages and their causes.* This process also lets you replace the icon (`favicon.ico`) that represents the pages in the Favorites menu of the Web browser.

The pages, messages, and icons registered by the `set web-authentication` html-files operation command are retained when the device is restarted.

For details about each file, see *8.10* Procedure for creating Web authentication pages.

8.9.2 Notes on using Web authentication page replacement functionality

(1) Storing and changing the created Web authentication page files

Store the Web authentication page file created by a PC onto an external media. To change a Web authentication page file, edit the stored Web authentication page file and register it on the Switch.

Use the store web-authentication html-files operation command to retrieve the Web authentication page file being operated on the Switch. The Web authentication page file retrieved is temporarily stored in the RAMDISK. Transfer the file to PC via FTP or store it on a memory card using the copy operation command. (Restarting the Switch deletes the file on the RAMDISK.)

(2) Transferring the created Web authentication page file

Transfer the created Web authentication page file to the RAMDISK on the Switch. Use FTP or transfer it or use the copy operation command to copy it from the memory card.

After you register the file on the Switch by the set web-authentication html-files operation command, the Web authentication page file that was transferred to the RAMDISK is no longer necessary. Delete the file using the del operation command. (Restarting the Switch also deletes the file on the RAMDISK.)

(3) Custom file set when changing the version

When the Switch is changed from Ver.2.2 or later to a version earlier than Ver.2.2 or when a file backed up with Ver.2.2 or later is restored in the device in a version earlier than Ver.2.2, all the registered custom file sets are deleted. This means that the basic Web authentication page custom file sets and the individual Web authentication page custom file sets are all deleted, and the default file set is restored.

8.10 Procedure for creating Web authentication pages

The following are the pages you can replace by using the Web authentication page replacement functionality and their corresponding file names:

- Login page (file name: `login.html`)
- Logout page (file name: `logout.html`)
- Login success page (file name: `loginOK.html`)
- Login failed page (file name: `loginNG.html`)
- Logout completed page (file name: `logoutOK.html`)
- Logout failed page (file name: `logoutNG.html`)

Create the files for each Web authentication page in HTML format.

When performing one-time password authentication, use the authentication-in-progress page as the replacement file. For details about an authentication-in-progress file, see *14. One-time Password Authentication [OP-OTP].*

Your customized HTML files can include client-side scripts in languages such as JavaScript. However, you cannot include code that involves server access or CGI scripts written in Perl or other languages.

Note that the login page, the logout page, and the `Reply-Message` page must include specific code that interacts with the Web authentication interface. For details about the login page and the logout page, see *8.10.1 Login page (login.html) and 8.10.2 Logout page (logout.html).*

You can also replace the authentication error messages listed in *Table 8-20 Authentication error messages and their causes* by creating a file with the file name given below. For details about how to create this file, see *8.10.3 Authentication error message file (webauth.msg).*

- Authentication error message file (file name: `webauth.msg`)

You can also replace the icon that represents the pages in the bookmarks menu of the Web browser.

- Icon displayed in Favorites menu of Web browser (file name: `favicon.ico`)

Note

Make sure that the file names you assign to your replacement pages and authentication error messages match the file names given in this section.

8.10.1 Login page (login.html)

This page prompts a client to log in by entering a user ID and password.

(1) Conditions for setting

You must include the code listed in the following table when creating an HTML file to serve as the login page.

Table 8-23 Code required in login page

Code	Meaning
`<form name="Login" method="post" action="/cgi-bin/Login.cgi"></form>`	Initiates a Web authentication login process. Do not modify this code.
`<input name="uid" size="40" maxlength="128" autocomplete="OFF" type="text">`	Provides a field for entering a user ID. Do not change any attributes except `size` and `maxlength`. Place this code inside the `<form></form>` tags. Make sure that `maxlength` allows for 6 or more characters.
`<input name="pwd" size="40" maxlength="32" autocomplete="OFF" type="password">`	Provides a field for entering a password. Do not change any attributes except `size` and `maxlength`. Place this code inside the `<form></form>` tags. Make sure that `maxlength` allows for 6 or more characters.
`<input value="Login" type="submit">`	Sends the login request to Web authentication. Do not modify this code. Place this code inside the `<form></form>` tags.

When creating an HTML file common to login and logout pages, see *Table 8-24 Code required in logout page.*

Note

If the `login.html` file contains a reference to another file, prefix the file name with a slash (`/`).

Example: `<img src="/image_file.gif">`

(2) Sample code

The following figure shows an example of the source code for the login page (`login.html`).

Figure 8-23 Example of source code for the login page (login.html)

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>

 <meta http-equiv="Pragma" content="no-cache">
 <meta http-equiv="Cache-Control" content="no-cache">
 <meta http-equiv="Expires" content="Thu, 01 Dec 1994 16:00:00 GMT">
 <title> </title>
</head>

<body oncontextmenu="return false;">
<!-- === Body === -->
<center>
<br>
<table width="100%">
 <tbody><tr><td align="center" bgcolor="#2b1872">
 <font color="#ffffff"><b>LOGIN</b></font>
 </td></tr></tbody>
</table>
<br>
Please enter your ID and password.<br>
<br>

<form name="Login" method="post" action="/cgi-bin/Login.cgi">
```

Description to instruct Web authentication to log in

```
<table><tbody><tr>
 <td>user ID</td>
 <td><input name="uid" size="40" maxlength="128" autocomplete="OFF" type="text"></td></tr>
```

Description to specify user ID

```
<tr>
 <td>password</td>
 <td><input name="pwd" size="40" maxlength="32" autocomplete="OFF" type="password"></td></tr>
```

Description to specify password

```
</tbody></table>
<br>
<input value="Login" type="submit">
```

Description to request to log in to Web authentication

```
</form>
<br>
<form name="Logout" action="/cgi-bin/Logout.cgi" method="post">
```

Description to instruct Web authentication to log out

```
<table width="100%">
 <tbody>
  <tr>
    <td align="center" bgcolor="#2b1872"><font color="#ffffff"><b>LOGOUT</b></font>
   </td></tr>
 </tbody>
</table>
 <br>Please push the following button.<br><br>
   <input value="Logout" type="submit">
```

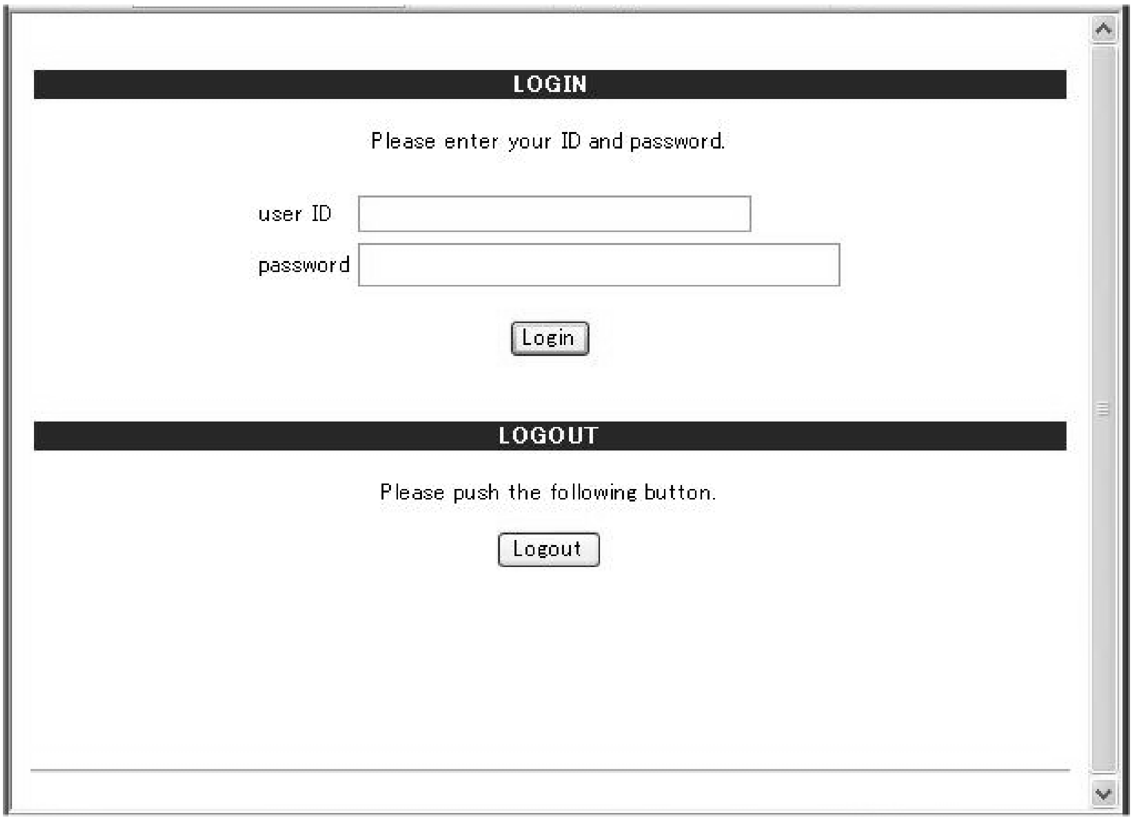
Description to request to log out of Web authentication

```
</form>
<br>
<br>
<br>
<br>
<br>
<br>
</center>
<!-- === Footer === -->
<hr>
<div align="right"></div>
</body>
</html>
```

(3) Display example

The following figure shows an example of how the login page appears to a user. (Example of the display common to the login and logout pages)

Figure 8-24 Example of the login page



8.10.2 Logout page (logout.html)

A client who has logged in using Web authentication uses this page to issue a logout request.

(1) Conditions for setting

You must include the code listed in the following table when creating an HTML file to serve as the logout page.

Table 8-24 Code required in logout page

Code	Meaning
<form name="Logout" action="/cgi-bin/Logout.cgi" method="post" ></form>	Initiates a Web authentication logout process. Do not modify this code.
<input value="Logout" type="submit">	Sends the logout request to Web authentication. Do not modify this code. Place this code inside the <form></form> tags.

Note

If the logout.html file contains a reference to another file, prefix the file name with a slash (`/`).

Example: `<img src="/image_file.gif">`

(2) Sample code

The following figure shows an example of the source code for the logout page (`logout.html`).

Figure 8-25 Example of source code for the logout page (logout.html)

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>

 <meta http-equiv="Pragma" content="no-cache">
 <meta http-equiv="Cache-Control" content="no-cache">
 <meta http-equiv="Expires" content="Thu, 01 Dec 1994 16:00:00 GMT">
 <title> </title>
</head>

<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
<br>
<form name="Logout" action="/cgi-bin/Logout.cgi" method="post">
<table width="100%">
  <tbody>
  <tr>
    <td align="center" bgColor="#2b1872"><font color="#ffffff"><b>LOGOUT</b></font>
    </td>
  </tr>
 </tbody>
</table>
 <br>Please push the following button.<br><br>
   <input value="Logout" type="submit">
</form>
<br><br><br><br><br><br>
</center>
<!-- ===== Footer ===== -->
<hr>

<div align="right"></div>
</body>
</html>
```

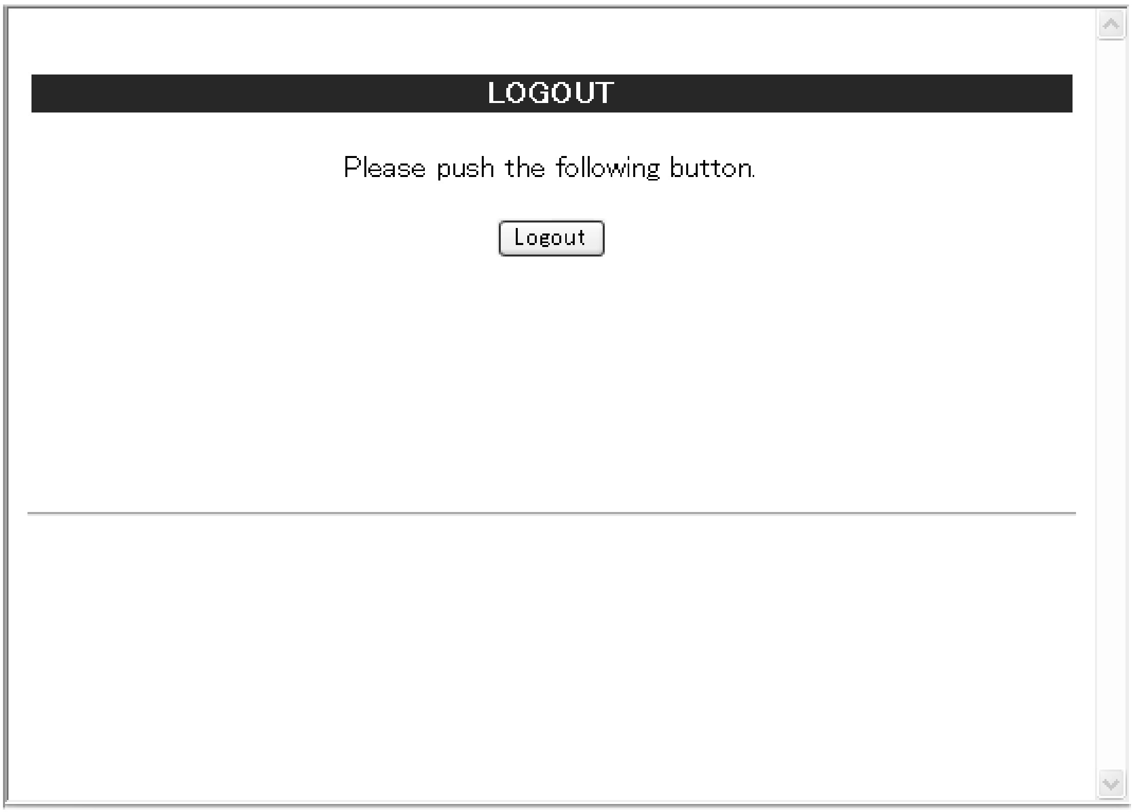
Description to instruct Web authentication to log out

Description to request to log out of Web authentication

(3) Display example

The following figure shows an example of how the logout page appears to a user.

Figure 8-26 Example of the logout page



8.10.3 Authentication error message file (webauth.msg)

The authentication error message file (`webauth.msg`) contains the messages presented to the user when an attempt to log in or out of Web authentication fails.

You can configure the Switch to send custom error messages instead of the default messages. This process requires that you create a file containing 9 lines of data, each corresponding to a specific message as described in the table below.

Table 8-25 Contents of the authentication error message file by line

Line number	Description
1	The message output when the user enters the wrong login ID or password, or when an authentication error is caused by the Web authentication DB. Default message: "`User ID or password is wrong. Please enter correct user ID and password.`"
2	The message output when an authentication error is caused by RADIUS. Default message: "`RADIUS: Authentication reject.`"
3	The message output in an environment configured to use RADIUS authentication when the Switch cannot establish a connection to the RADIUS server. Default message: "`RADIUS: No authentication response.`"

Line number	Description
4	The message output when login fails due to an error in the Switch configuration or a conflict with other functionality. Default message: "You cannot login by this machine."
5	The message output when a minor error occurs in a Web authentication program. Default message: "Sorry, you cannot login just now. Please try again after a while."
6	The message output when a major error occurs in a Web authentication program. Default message: "The system error occurred. Please contact the system administrator."
7	The message output when a critical error occurs in a Web authentication program. Default message: "A fatal error occurred. Please inform the system administrator."
8	The message output when logout fails for such reasons as the CPU becoming overloaded while processing the logout request. Default message: "Sorry, you cannot logout just now. Please try again after a while."
9	The message output when a user who is not logged in issues a logout request. Default message: "The client PC is not authenticated."

(1) Conditions for setting

- If a line contains only a line break, the Switch outputs the default message for that line.
- When saving the file, specify CR+LF or LF as the line break code.
- Each line can contain a maximum of 512 single-byte characters, including HTML markup and the line break tag
. Any excess characters are ignored.
- If the authentication error message file contains more than 9 lines, subsequent lines are ignored.

(2) Key points regarding error message file creation

- The text in the authentication error message file is handled as HTML text by the Web browser. If you include HTML markup in an error message, the message is formatted accordingly.
- Each message must occupy one line in the file. If you want to insert a line break in an error message, use the HTML line break tag
.

(3) Sample code

The following figure shows an example of the source code for the authentication error message file (webauth.msg).

Figure 8-27 Example of source code for authentication error message file (webauth.msg)

```
Invalid user ID or password
Invalid password
No authentication server found<BR>Contact your system administrator.
Error in system configuration<BR>Contact your system administrator.
System failure (minor)<BR>Retry later.
System failure (major)<BR>Contact your system administrator.
System failure (critical)<BR>Contact your system administrator.
System heavily loaded<BR>Retry later.
```

(4) Display example

The following figure shows an example of the login failed page displayed to a user who enters the wrong password in an environment where the default authentication error message file applies.

Figure 8-28 Example of the login failed page (invalid password)

8.10.4 Tags specific to Web authentication

(1) Type of tags specific to Web authentication

By inserting tags specific to Web authentication in the HTML file of the Web authentication page, the portion where the tag is written is converted into the intended information.

If you insert an appropriate tag in the HTML file, you can display the login time or an error message on the authentication page, or recognize the information through an application operating in the Web browser.

Table 8-26 Tags dedicated to Web authentication and converted information

Tags specific to Web authentication	Example of the text after conversion	Meaning of the converted information
`<!-- Login_Time -->`	"2008/11/20 19:56:01 UTC"	Time when login was successful
`<!-- Logout_Time -->`	"2008/11/20 20:56:01 UTC"	Logout time#1
`<!-- After_Vlan -->`	"100"	VLAN ID after successful login
`<!-- Error_Message -->`	"The user ID or password is invalid."	Error message#2
`<!-- Redirect_URL -->`	"http://www.example.com"	URL automatically displayed after successful authentication

#1: This tag has different meanings depending on the page where it appears:

Login success page: The time when auto-logout will take place when the maximum connection time is reached.

Logout completed page: The time when the logout process was completed

#2: The error that caused the login or logout attempt to fail

For examples of how to use these tags, see *8.10.5 Examples of other pages*.

The following table describes which combination of tags dedicated to Web authentication and the screens are valid for the conversion of information.

Table 8-27 Combinations of the tags specific to Web authentication and the pages that are valid for the conversion of information

Tags specific to Web authentication	Types of pages (to be converted)					
	Login page	Logout page	Login success page	Login failed page	Logout completed page	Logout failed page
`<!-- Login_Time -->`	--	--	Y	--	--	--
`<!-- Logout_Time -->`	--	--	Y	--	Y	--
`<!-- After_Vlan -->`	--	--	Y	--	--	--
`<!-- Error_Message -->`	--	--	--	Y	--	Y
`<!-- Redirect_URL -->`	--	--	Y	--	--	--

Legend:

Y: If the tag specific to Web authentication is included in the HTML file, it is converted into the intended information.

--: Even if the tag specific to Web authentication is included in the HTML file, it is not converted into the intended information.

(2) Notes

(a) The default HTML file for Web authentication

The default HTML file for Web authentication in advance contains tags specific to Web authentication to display its information on the web browser.

The exception is that VLAN ID after login was successful does not appear on the Web browser because the specific tag (`<!-- After_Vlan -->`) for converting its information is embedded as the following code in the default HTML file:

[HTML (`loginOK.html`) coded by default in the login success page]

```
<meta name="vlan-id" content="<!-- After_Vlan -->" />
```

#: The content with meta tags is handled as additional information, and does not appear in a common web browser.

To display the VLAN ID after login was successful on the web browser, optionally create a login success page file (`loginOK.html` file), and then follow the procedure described in *8.9.1 Replacing Web authentication pages* to display the VLAN ID on the login success page.

(b) Handling space characters (blank characters)

Space characters included in each tag specific to Web authentication are recognized as the delimiter between keywords. Although a keyword must not include space characters, if one or more space characters are included between each keyword, they are properly processed as the delimiters.

Note that the maximum number of characters recognized as a tag specific to Web authentication is 80 characters, including `<` and `>`, the beginning and end of the string.

[Keyword]

1. "`<!--`"
2. "`Login_Time`", "`Logout_Time`", "`After_Vlan`", "`Error_Message`"
3. "`-->`"

8.10.5 Examples of other pages

This section provides sample source code for the Web authentication pages `loginOK.html`, `logoutOK.html`, `loginNG.html`, and `logoutNG.html`.

(1) Login success page (loginOK.html)

The figures below show an example of the source code for the login success page and how the page appears to the user.

Figure 8-29 Example of source code for the login success page (loginOK.html)

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
  <title> </title>
  <meta name="vlan-id" content="<!-- After_Vlan -->" />
</head>
                                    VLAN ID tag after successful login

<body oncontextmenu="return false;">
<!-- === Body === -->
<center>
Login success
<br>
<br>
<table border="0">
<tbody>
 <tr>
  <td align="left">Login_Time</tb>
  <td align="left"> -- </td>
  <td align="left"><b><!-- Login_Time --></b></td>
 </tr>
                               Login time display tag
 <tr>
  <td align="left">Logout_Time</td>
  <td align="left"> -- </td>
  <td align="left"><b><!-- Logout_Time --></b></td>
 </tr>
</tboby>
                               Logout time display tag
</table>
<b><!-- Redirect_URL --></b>
<br>
         Automatically displayed URL tag after successful authentication
<br>
<form>
 <input value="close" onclick="window.close()" type="button">
</form><br>
<br>
<form name="Logout" action="/cgi-bin/Logout.cgi" method="post">
 <table width="100%">
  <tbody>
  <tr>
    <td align="center" bgcolor="#2b1872"><font color="#ffffff"><b>LOGOUT</b></font>
    </td>
  </tr>
  </tbody>
 </table>
 <br>Please push the following button.<br><br>
    <input value="Logout" type="submit">
</form>
<br>
</center>
<br>

<!-- === Footer === -->
<hr>
<div align="right"></div>

</body>
</html>
```

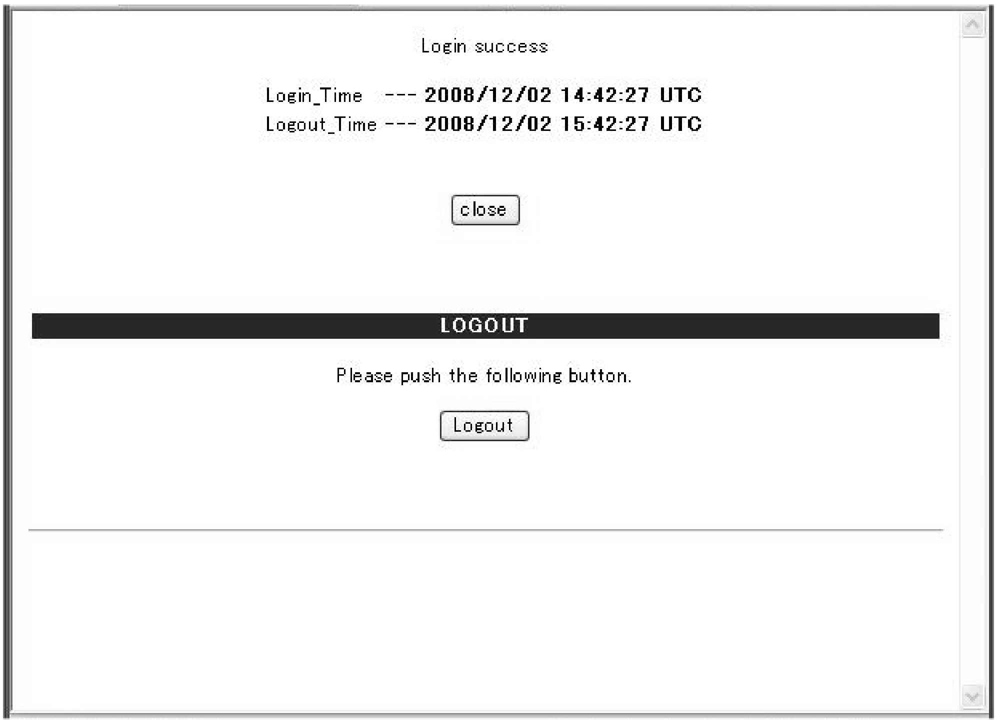
Note

- If the `loginOK.html` file contains a reference to another file, prefix the file name with a slash (`/`).

  Example: `<img src="/image_file.gif">`

- If the `loginOK.html` file contains a reference to another file while in dynamic VLAN mode or legacy mode, the login success page might not be displayed correctly.

Figure 8-30 Example of login success page



(2) Logout completed page (logoutOK.html)

The figures below show an example of the source code for a logout completed page and how the page appears to the user.

Figure 8-31 Example of source code for the logout completed page (logoutOK.html)

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
 <title> </title>
</head>
<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
Logout success
<br>
<br>
Logout Time --- <b><!-- Logout_Time --></b>
<br>
                        Logout time display tag
<br>
<br>

<form>
 <input value="close" onclick="window.close()" type="button">
</form>

<br>
<br>
</center>

<!-- ===== Footer ===== -->
<hr>
<div align="right"></div>
</body></html>
```

Note

If the `logoutOK.html` file contains a reference to another file, prefix the file name with a slash (`/`).

Example: `<img src="/image_file.gif">`

Figure 8-32 Example of the logout completed page

(3) Login/logout failed pages (loginNG.html/logoutNG.html)

The figures below show example of the source code for the login or logout failed page and how the page appears to the user.

Figure 8-33 Example source code for the login failed page (loginNG.html)

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title> </title>
</head>

<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
<br>
 <i style="color: red;"><b><!-- Error_Message --></b></i>
<br>
<br>
<br>
<br>

<form>
 <input value="login page" onclick="window.location.href='/login.html'" type="button">
 <input value="close" onclick="window.close()" type="button">
</form>

<br>
</center>
<!-- ===== Footer ===== -->
<hr>
<div align="right"></div>
</body>
</html>
```

Error message display tag

Figure 8-34 Example of source code for the logout failed page (logoutNG.html)

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title> </title>
</head>

<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
<br>
 <i style="color: red;"><b><!-- Error_Message --></b></i>
<br>
<br>
<br>
<br>

<form>
 <input value="back" onclick="history.back()" type="button">
 <input value="close" onclick="window.close()" type="button">
</form>

<br>
</center>
<!-- ===== Footer ===== -->
<hr>
<div align="right"></div>
</body>
</html>
```

Error message display tag

Note

If the `loginNG.html` or `logoutNG.html` file contains a reference to another file, prefix the file name with a slash (`/`).

Example: `<img src="/image_file.gif">`

Figure 8-35 Example of the login failed page

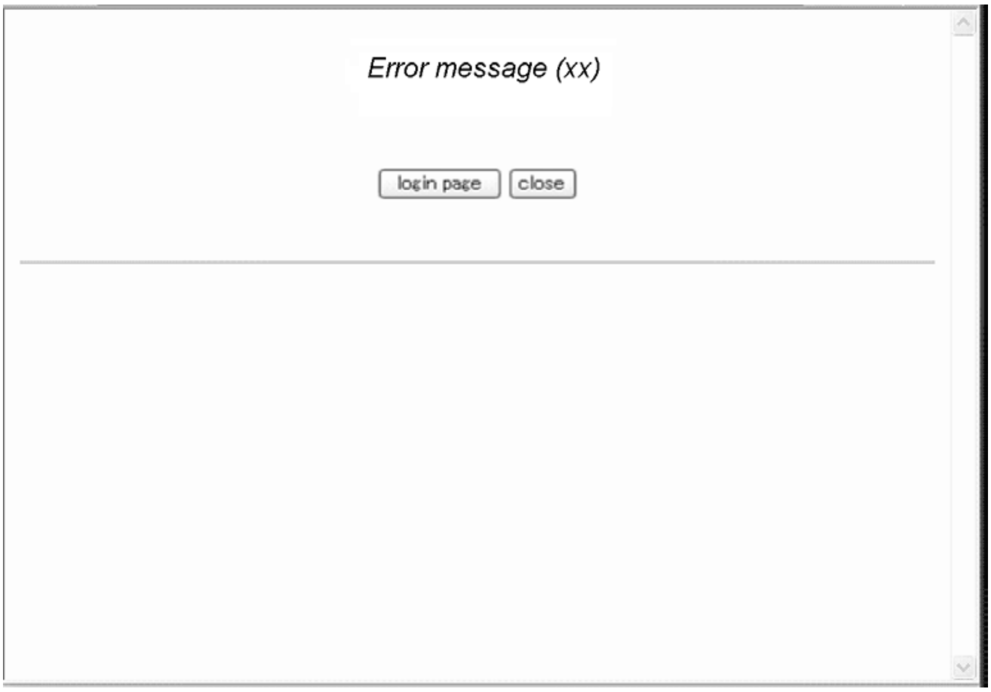
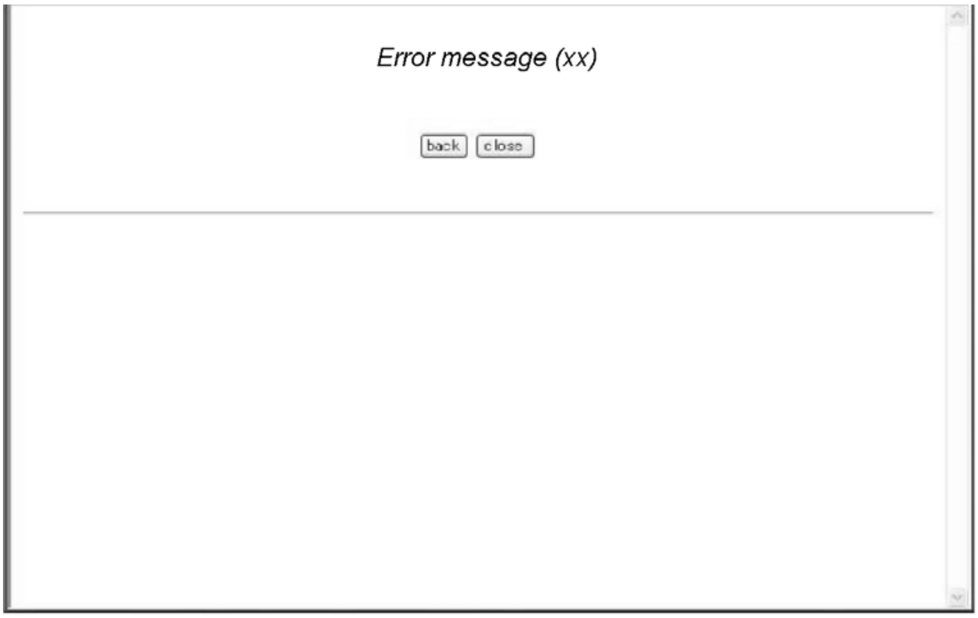


Figure 8-36 Example of the logout failed page



8.11 Description of the internal DHCP server functionality

The internal DHCP server functionality of the Switch dynamically assigns IP addresses or option information to DHCP clients.

8.11.1 Supported specifications

The following table shows the support specification of the internal DHCP server of the Switch. The DHCP server and the clients are direct-coupled on the same network.

Table 8-28 Support specification of the internal DHCP server

Item	Specification
Connection configuration	DHCP clients are directly connected to a DHCP server. DHCP clients cannot be contained via a DHCP relay agent.
BOOTP server functionality	Not supported
Linking dynamic DNS	Not supported
Dynamic IP address assignment functionality	Supported
Static IP address assignment functionality	Not supported

8.11.2 Information distributed to clients

The table below describes the types of information that the Switch can distribute to clients. Optional information is not distributed even if option numbers are specified on the Switch unless clients request optional information by submitting an option request list.

Table 8-29 Information distributed by the Switch to clients

Item	Specification
IP address	Set an IP address that can be used by a client.
IP address lease time	Set the lease time for an assigned IP address. In the Switch, the lease time is determined based on the values of the `default-lease-time` and `max-lease-time` parameters and the request from the client. (Option No. 51)
Subnet mask	The subnet mask length indicating a network address specified in the configuration is used. (Option No. 1)
Router (optional)	Specify the IP address of the router on the subnet of the client. This IP address is used as the gateway address of the client. (Option No. 3)

Item	Specification
DNS (optional)	Specify the IP address of a domain name server available for the client. (Option No. 6)

8.11.3 Preventing duplicate assignments of IP addresses

The DHCP server of the Switch does not support the prevention of duplicate assignments of an IP address via ICMP echo requests. The Switch uses the `show ip dhcp conflict` operation command to display the information of the terminal that has received the `decline` message.

8.11.4 Notes on using a DHCP server

The following are notes on using a DHCP server.

(1) Default lease time of the Switch

The default lease time of the Switch is 10 seconds, and you cannot set any smaller value than that. The setting range of the lease time is between 10 seconds and 365 days. The maximum number of IP addresses available for assignment is 512

.

9. Web Authentication Configuration and Operation

The Web authentication functionality controls access to VLANs by users authenticated from an ordinary Web browser. This chapter describes Web authentication configuration and operation.

9.1 Web authentication configuration

9.1.1 List of configuration commands

The table below describes the commands used to configure Web authentication.

Table 9-1 List of configuration commands and authentication modes

Command name	Description	Authentication mode		
		F	D	L
`aaa accounting web-authentication`	Sends accounting information for Web authentication to the accounting server.	Y	Y	Y
`aaa authentication web-authentication`	Sets an authentication method group for Web authentication.	Y	Y	Y
`aaa authentication web-authentication end-by-reject`	Terminates authentication if login authentication is denied. If authentication fails due to a communication failure (for example, the RADIUS server does not respond), the next authentication method specified by the `aaa authentication web-authentication` command is used to perform authentication.	Y	Y	Y
`authentication arp-relay`[#1]	Outputs ARP frames that were sent to other devices from unauthenticated terminals to a non-authenticating port.	Y	Y	N
`authentication ip access-group`[#1]	Outputs only the frames specified by applying the IPv4 access list, from among the IP frames sent from an unauthenticated terminal destined for another device, to a non-authenticating port.	Y	Y	N
`web-authentication authentication`	Sets the name of an authentication method list for the port-based authentication method.	Y	Y	N
`web-authentication auto-logout`	The `no web-authentication auto-logout` command disables the setting for automatic authentication logout when it is detected that the status that frames have not been received from a terminal authenticated via Web authentication for a certain period of time.	Y	Y	Y

Command name	Description	Authentication mode		
		F	D	L
`web-authentication force-authorized vlan`	Forcibly makes a terminal subject to authentication and authentication-permitted status and assigns a post-authentication VLAN when the VLAN RADIUS authentication method is used or when a request to a RADIUS server fails due to route failure.	--	Y	Y
`web-authentication html-fileset`	Configures custom file set names of individual Web authentication pages displayed by port.	Y	Y	N
`web-authentication ip address`	Configures an authentication IP address and domain name.	Y	Y	Y
`web-authentication jump-url`	Configures a URL to be automatically displayed after the Authentication Success page is displayed and the time required before jumping to the URL.	Y	Y	Y
`web-authentication logout ping tos-windows`	Specifies the TOS value of special frames to cancel an authentication status of a corresponding MAC address when receiving the special frames (ping) sent by authenticated terminals.	Y	Y	Y
`web-authentication logout ping ttl`	Specifies the TTL value of special frames to cancel an authentication status of a corresponding MAC address when receiving the special frames (ping) sent by authenticated terminals.	Y	Y	Y
`web-authentication logout polling count`	Specifies the number of times the Switch resends the monitoring packet when there is no response to a monitoring frame that periodically monitors a connection status of authenticated terminals.	Y	--	--
`web-authentication logout polling enable`	The `no web-authentication logout polling enable` command disables the auto logout functionality executed when periodic connection monitoring detects that an authenticated terminal is not connected.	Y	--	--
`web-authentication logout polling interval`	Specifies the polling interval of a monitoring frame that periodically monitors the connection status of	Y	--	--

Command name	Description	Authentication mode		
		F	D	L
	an authenticated terminal.			
`web-authentication logout polling retry-interval`	Specifies the interval between retransmissions of monitoring frames when there is no response.	Y	--	--
`web-authentication max-timer`	Specifies the maximum connection time.	Y	Y	Y
`web-authentication max-user`	Specifies the maximum number of authenticated users permitted by the Switch.	--	Y	Y
`web-authentication max-user (interface)`	Specifies the maximum number of authenticated users permitted on a corresponding port.	--	Y	Y
`web-authentication port`[#2]	Sets the authentication mode for ports.	Y	Y	--
`web-authentication radius-server host`	Configures RADIUS server information for Web authentication.	Y	Y	Y
`web-authentication radius-server dead-interval`	Configures a monitoring timer before auto recovery to the primary RADIUS server when Web authentication RADIUS server is used.	Y	Y	Y
`web-authentication redirect-mode`	Sets a protocol to display the Web authentication Login page when the URL redirect functionality is enabled.	Y	Y	--
`web-authentication redirect enable`	The `no web-authentication redirect enable` command disables the URL redirect functionality.	Y	Y	--
`web-authentication redirect tcp-port`	Adds a TCP destination port number for a frame subject to URL redirect on the Switch when the URL redirect functionality is enabled.	Y	Y	--
`web-authentication roaming`	Sets communication permissions (roaming) when the port for an authenticated terminal changes to another port connected via a hub or similar means without a link-down event occurring.	--	Y	--

Command name	Description	Authentication mode		
		F	D	L
`web-authentication static-vlan force-authorized`	Forcibly authenticates a terminal that is connected to the target port and subject to authentication and authentication-permitted status and assigns an authenticated VLAN when the RADIUS authentication method is used or when a request to a RADIUS server fails due to a route failure.	Y		
`web-authentication static-vlan max-user`	Specifies the maximum number of authenticated users permitted by the Switch.	Y	--	--
`web-authentication static-vlan max-user (interface)`	Specifies the maximum number of authenticated users permitted on a corresponding port.	Y	--	--
`web-authentication static-vlan roaming`	Sets communication permissions (roaming) when the port for an authenticated terminal changes to another port connected via a hub or similar means without a link-down event occurring.	Y	--	--
`web-authentication system-auth-control`	Enables Web authentication.	Y	Y	Y
`web-authentication user-group`	Enables the user ID-based authentication method.	Y	Y	N
`web-authentication user replacement`	Enables authentication with a different user ID after successful authentication with the first user ID when several user IDs are used for a terminal.	Y	Y	Y
`web-authentication vlan`	Sets the VLAN ID to dynamically switch after user authentication.	--	--	Y
`web-authentication web-port`	Adds a TCP destination port number for a frame subject to URL redirect on the Switch when the URL redirect functionality is enabled.	Y	Y	--

Legend:

F: Fixed VLAN mode

D: Dynamic VLAN mode

L: Legacy mode

Y: The command operates according to the settings.

--: The command can be entered, but has no effect.

N: The command cannot be entered.

#1

For details about the configuration, see *5. Overview of Layer 2 Authentication.*

#2

The specification of this command affects the switching of authentication modes.

The table below shows the list of internal DHCP server configuration commands.

Table 9-2 List of internal DHCP server configuration commands

Command name	Description	Authentication mode		
		F	**D**	**L**
`default-router`	Specifies a router option to distribute to a client. A router option is an IP address the client can use as a router IP address over the subnet (default router). Configure the IP address of a router used by the client (refer to *9.6 Configuring internal DHCP server).*	--	Y	Y
`dns-server`	Sets the domain name server option that is distributed to clients.	--	Y	Y
`ip dhcp excluded-address`	Specifies the range of IP addresses to be excluded from ones to distribute among ones specified by the network command. In the range of IP addresses for the network, set the IP addresses which will not be assigned to a client (refer to *9.6 Configuring internal DHCP server).*	--	Y	Y
`ip dhcp pool`	Sets DHCP address pool information.	--	Y	Y
`lease`	Specifies the default lease time for the IP address assigned to a client. Set the lease time for the IP address used by the client (refer to *9.6 Configuring internal DHCP server).*	--	Y	Y
`max-lease`	Specifies the maximum lease time allowed when a client requests an IP address with a specific lease time.	--	Y	Y
`network`	Specifies the subnet of the network to which an IP address is dynamically assigned by DHCP. IP addresses whose host bits all are not 0 or 1 are actually registered in the DHCP address pool. Set the network to which an IP address is assigned by DHCP (refer to *9.6 Configuring internal DHCP server).*	--	Y	Y

Command name	Description	Authentication mode		
		F	D	L
`service dhcp`	Specifies the interface on which a DHCP server is enabled. Only the VLAN interface with this configuration receives DHCP packets. Set the VLAN interface to which the DHCP client is connected (refer to *9.6 Configuring internal DHCP server).*	--	Y	Y

Legend:

F: Fixed VLAN mode

D: Dynamic VLAN mode

L: Legacy mode

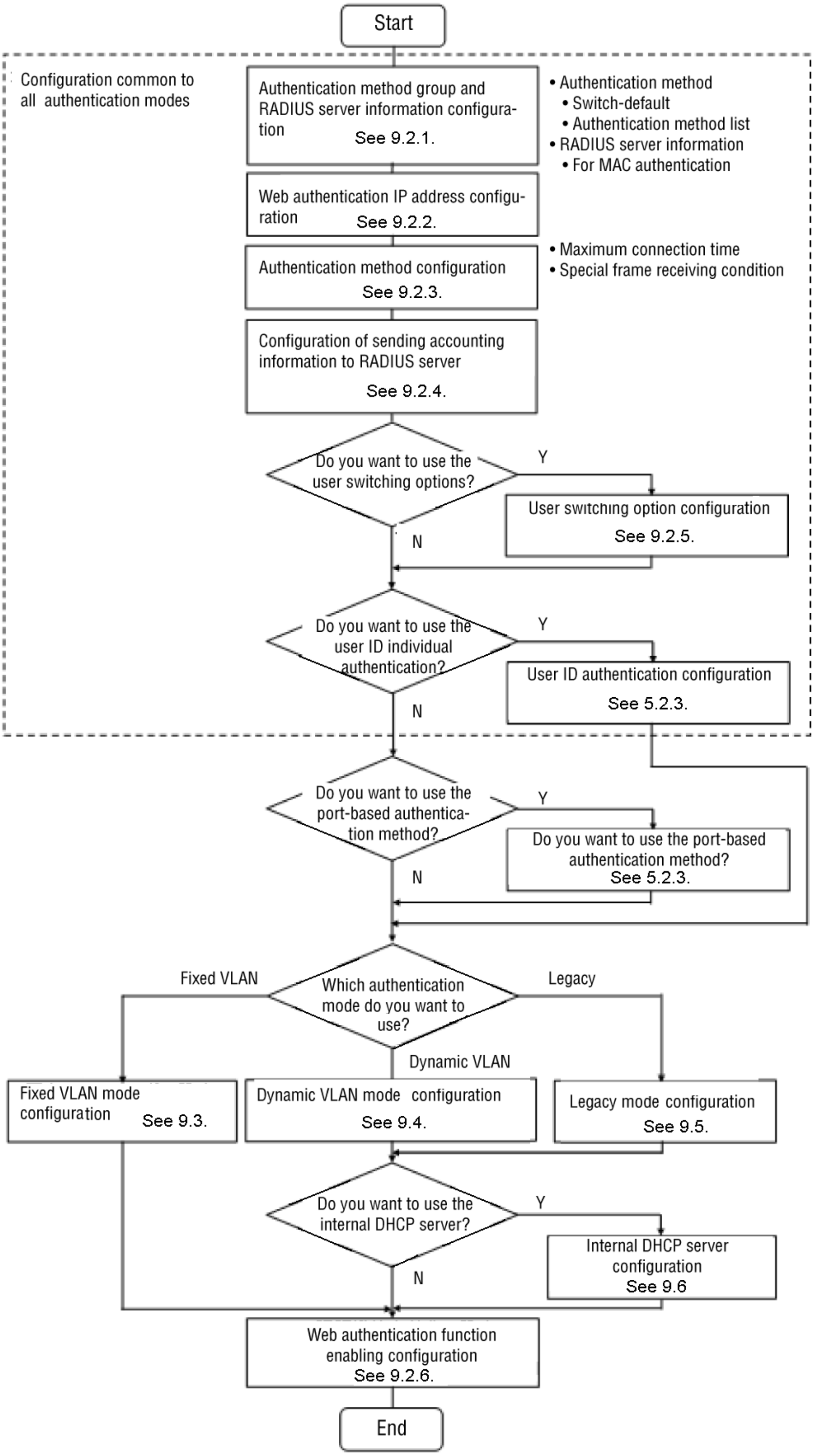
Y: The command operates according to the settings.

--: The command can be entered, but has no effect.

9.1.2 Procedure for configuring Web authentication

Configure Web authentication following the procedure below.

Figure 9-1 Procedure for configuring Web authentication



Start
Configuration common to all authentication modes
Authentication method group and RADIUS server information configuration See 9.2.1.
• Authentication method
• Switch-default
• Authentication method list
• RADIUS server information
• For MAC authentication
Web authentication IP address configuration See 9.2.2.
Authentication method configuration See 9.2.3.
• Maximum connection time
• Special frame receiving condition
Configuration of sending accounting information to RADIUS server See 9.2.4.
Do you want to use the user switching options?
Y
N
User switching option configuration See 9.2.5.
Do you want to use the user ID individual authentication?
Y
N
User ID authentication configuration See 5.2.3.
Do you want to use the port-based authentication method?
Y
N
Do you want to use the port-based authentication method? See 5.2.3.
Fixed VLAN
Legacy
Which authentication mode do you want to use?
Dynamic VLAN
Fixed VLAN mode configuration See 9.3.
Dynamic VLAN mode configuration See 9.4.
Legacy mode configuration See 9.5.
Do you want to use the internal DHCP server?
Y
N
Internal DHCP server configuration See 9.6
Web authentication function enabling configuration See 9.2.6.
End

For details about the configuration, see the following:

1. Configuration common to all authentication modes

   The following subsections describe configuration common to all authentication modes.

   - Configuring the authentication method group and RADIUS server information: *9.2.1 Configuring the authentication method group and RADIUS server information*
   - Configuring the Web authentication IP address: *9.2.2 Configuring Web authentication IP addresses*
   - Auto logout condition configuration common to all authentication modes: *9.2.3 Configuring auto logout condition common to all authentication modes*
   - Configuring the transmission of accounting information to the RADIUS server: *9.2.4 Configuring the transmission of accounting information*
   - User switching option configuration: *9.2.5 Configuring user switching options*
   - User ID-based authentication method: *(3) Example of user ID-based authentication method configuration* in *5.2.3 Authentication method list configuration*
   - Configuring authentication methods by port: *(2) Example of port-based authentication method configuration* in *5.2.3 Authentication method list configuration*

2. Configuring individual authentication modes

   The following sections describe how to configure individual authentication modes.

   Some items are the same as in other authentication modes. In such cases, see the sections referenced in the text.

   - Configuring fixed VLAN mode: *9.3 Configuring fixed VLAN mode*
   - Configuring dynamic VLAN mode: *9.4 Configuring dynamic VLAN mode*
   - Configuring legacy mode: *9.5 Configuring legacy mode*

3. Internal DHCP server configuration

   For dynamic VLAN mode and legacy mode, the internal DHCP server in the Switch is available.

   - Internal DHCP server configuration: *9.6 Configuring internal DHCP server*

4. Enabling Web authentication

   Web authentication is completed when the Web authentication method is enabled at the end.

   - *9.2.6 Enabling Web authentication*

Authentication modes are enabled by using the configuration settings described in the table below.

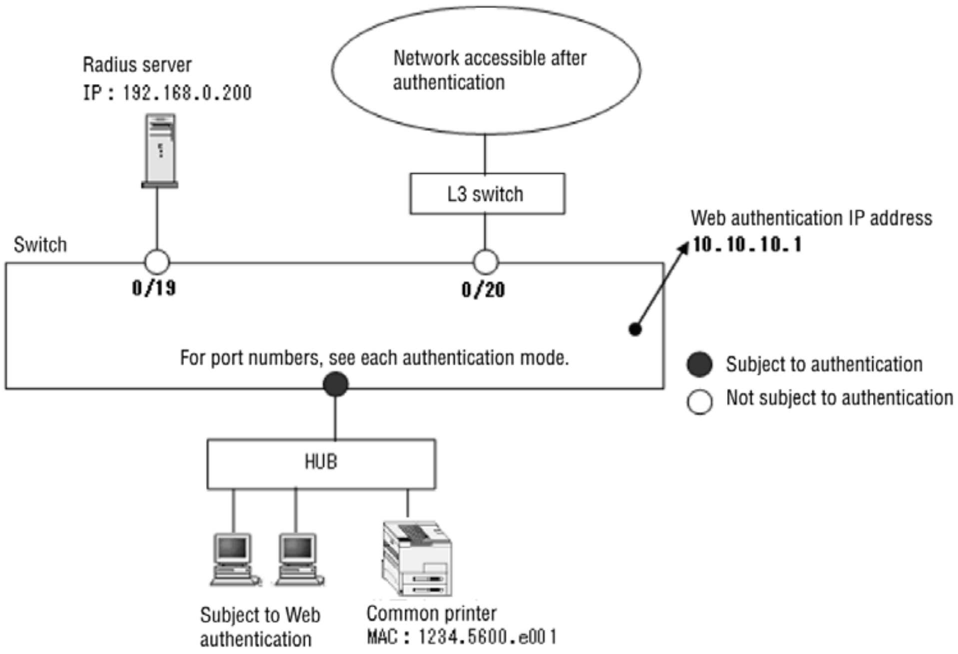
Table 9-3 Conditions for enabling authentication modes

Authentication mode	Configuration settings
Common	● aaa authentication web-authentication ● web-authentication radius-server host or radius-server ● web-authentication system-auth-control
Fixed VLAN mode	When used at access ports ● vlan *<VLAN-ID-list>* ● web-authentication port ● switchport mode access ● switchport access vlan When used at trunk ports ● vlan *<VLAN-ID-list>* ● web-authentication port ● switchport mode trunk ● switchport trunk allowed vlan ● switchport trunk native vlan When used at MAC ports ● vlan *<VLAN-ID-list>* or vlan *<VLAN-ID-list>* mac-based ● web-authentication port ● switchport mode mac-vlan ● switchport mac dot1q vlan
Dynamic VLAN mode	● vlan *<VLAN ID list>* mac-based ● web-authentication port ● switchport mode mac-vlan
Legacy mode	● vlan *<VLAN ID list>* mac-based ● web-authentication vlan ● switchport mode mac-vlan ● switchport mac vlan

9.2 Configuration common to all authentication modes

This section describes how to configure each authentication mode by using the following basic configuration. For this example, the port numbers used for the RADIUS server and the post-authentication network are 0/19 and 0/20, respectively. For details about port numbers for connecting terminals to be authenticated, see the configuration examples of each authentication mode.

Figure 9-2 Basic configuration



9.2.1 Configuring the authentication method group and RADIUS server information

(1) Configuring the authentication method group

Points to note

Sets an authentication method group for Web authentication.

Configure one entry of Switch default used in common for Web authentication and two entries of the authentication method list used for the authentication ports.

1. Switch default

   In this example, the Switch default authentication methods are RADIUS authentication and local authentication, and the Switch is configured so that local authentication is performed when RADIUS authentication fails due to a communication failure (for example, the RADIUS server does not respond).

   If authentication fails because RADIUS authentication is denied, the Switch ends the authentication process at that point and does not perform local authentication.

   - The internal Web authentication DB is used as a local authentication method. See *9.7.2 Registering the internal Web authentication DB,* and register the internal Web authentication DB on the Switch.

2. Authentication method list

   For the RADIUS server group information to be specified for authentication method lists, `Keneki-group1` and `Keneki-group2` are assumed to have been set in advance.

   For details about authentication method lists, see *5.2.2 Authentication method list.*

   For RADIUS server group information, see *5.3.1 RADIUS server information used with the Layer 2 authentication method,* and *8. Login Security and RADIUS* in the *Configuration Guide Vol. 1*.

Command examples

1. `(config)# aaa authentication web-authentication default group radius local`

   Configures the default authentication method for the Switch, in the sequence of RADIUS authentication method and then local authentication method.

2. `(config)# aaa authentication web-authentication end-by-reject`

   Configures the settings so that the authentication process ends when denied by RADIUS authentication and no local authentication is performed.

3. `(config)# aaa authentication web-authentication WEB-list1 group Keneki-group1`

   Configures the RADIUS server group name `Keneki-group1` for the authentication method list `WEB-list1`.

4. `(config)# aaa authentication web-authentication WEB-list2 group Keneki-group2`

   Configures the RADIUS server group name `Keneki-group2` for the authentication method list `WEB-list2`.

Notes

- If the Switch default setting is changed, authentication is canceled for the terminals that have been authenticated by using the Switch default authentication method.
- If the settings for the authentication method list are changed, authentication is canceled for the terminals that have been authenticated by using the authentication method list.
- If `aaa authentication web-authentication` is configured, the local authentication method is used.
- When using the forced authentication functionality, specify only `default group radius` by using the above commands. Forced authentication cannot be used with only local authentication, or when the priority for RADIUS authentication and local authentication (as in the above settings) has been specified.
- If the setting for `aaa authentication web-authentication end-by-reject` is changed, authentication is canceled for the terminals that have been authenticated by using Web authentication.

(2) Configuring RADIUS server information

(a) When using a Web authentication RADIUS server

Points to note

Configure authentication RADIUS server information used only with Web authentication.

An IP address and a RADIUS key must be specified to enable the RADIUS server settings. Configure only the IP address using the `web-authentication radius-server host` configuration command. In this case, a RADIUS key is not used in authentication.

Also, configure the monitoring timer (dead-interval) to automatically recover itself when the Web authentication RADIUS server is unavailable as in this example.

Command examples

1.
```
(config)# web-authentication radius-server host 192.168.10.201
key "web-auth"
```

Configure the IP address and the RADIUS key of a RADIUS server used only in Web authentication. In this example, the default values are used for the omitted `auth-port`, `acct-port`, `timeout`, and `retransmit`.

2.
```
(config)# web-authentication radius-server dead-interval 15
```

Configure the monitoring timer (dead-interval) to 15 minutes before auto recovery if the configured Web authentication RADIUS server is unavailable.

Notes

- If this information is not specified, the settings for a general-use RADIUS server are used. If both Web authentication RADIUS server information and the general RADIUS server information have not been configured, RADIUS authentication cannot be executed.
- Up to four entries of Web authentication RADIUS server information can be configured for the Switch.
- When the RADIUS key, retry count, and response timeout time are omitted, the settings specified by the configuration commands `radius-server key`, `radius-server retransmit`, and `radius-server timeout` are used, respectively.

(b) When using a general-use RADIUS server

For details about the settings for a general-use RADIUS server, see *8. Login Security and RADIUS* in the *Configuration Guide Vol. 1*.

9.2.2 Configuring Web authentication IP addresses

Points to note

Configure an IP address and a domain name to be used exclusively for Web authentication.

Command examples

1.
```
(config)# web-authentication ip address 10.10.10.1 fqdn
ax1240s.example.com
```

Configures an IP address (10.10.10.1) and domain name exclusive for Web authentication.

9.2.3 Configuring auto logout condition common to all authentication modes

(1) Configuring maximum connection time

Points to note

Configure the maximum connection time for an authenticated user. The user automatically logs out when exceeding the maximum connection time.

Command examples

1. `(config)# web-authentication max-timer 60`

   Configures 60 minutes as the maximum connection time of an authenticated user.

(2) Configuring logout conditions by receiving special frames

Points to note

Configure logout conditions by receiving special frames from authenticated terminals.

Command examples

1. `(config)# web-authentication logout ping tos-windows 2`

   `(config)# web-authentication logout ping ttl 2`

   Automatically logs out the terminal of a corresponding MAC address only when conforming to both TOS and TTL values.

9.2.4 Configuring the transmission of accounting information

Points to note

Configure for Web authentication accounting information to a RADIUS server.

Command examples

1. `(config)# aaa accounting web-authentication default start-stop group radius`

   Specifies the transmission of accounting information to the RADIUS server.

9.2.5 Configuring user switching options

Points to note

Configure user-switching options that can be authenticated with a different user ID after successful authentication with the first user ID on a single terminal.

Command examples

1. `(config)# web-authentication user replacement`

   Configures user-switching options.

Notes

- Does not return to the first user ID even after a successful authenticated user ID when user switching is canceled.

9.2.6 Enabling Web authentication

Points to note

Enable Web configuration after configuration for Web authentication is executed.

Command examples

1. `(config)# web-authentication system-auth-control`

   Enables Web authentication.

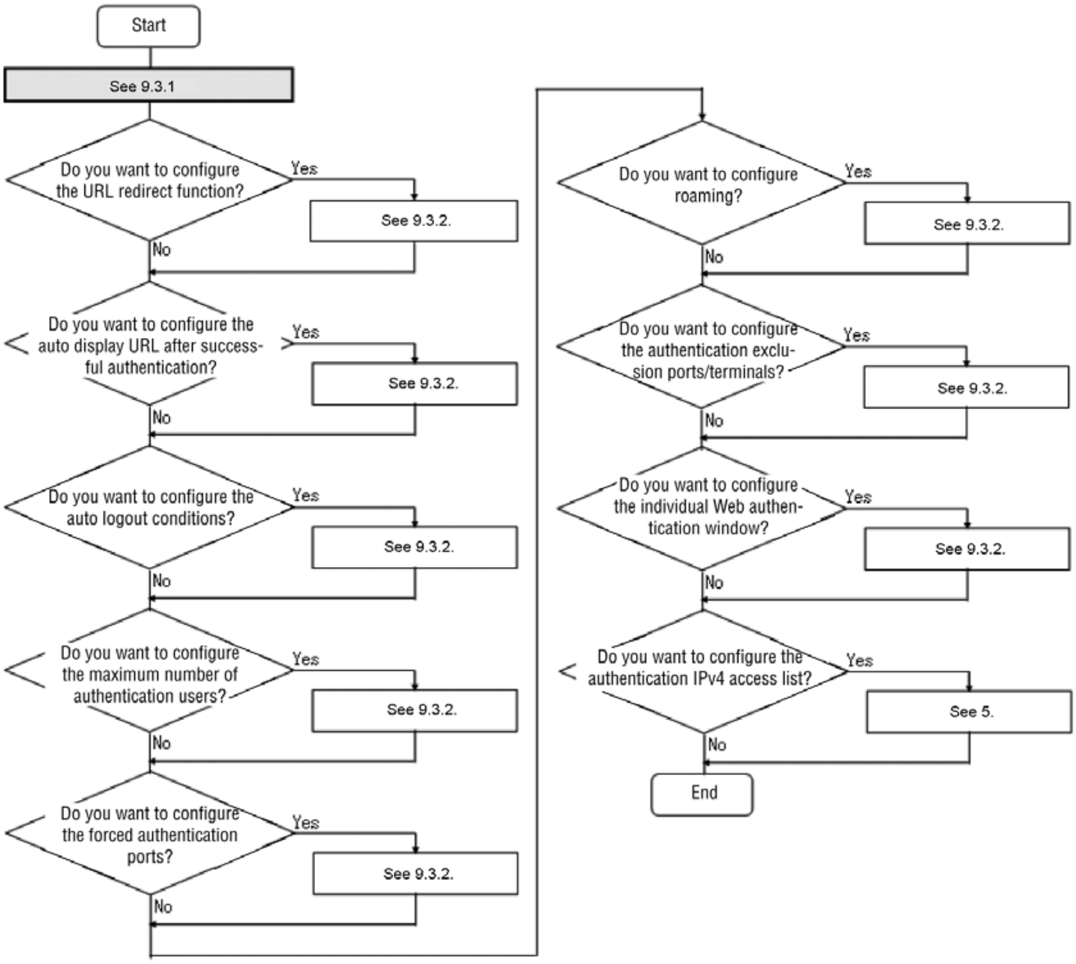
Notes

Configure this command after quitting all Web authentication configurations. If MAC authentication is enabled before configuration is complete, account logs might be collected for authentication failures.

9.3 Configuring fixed VLAN mode

Configure fixed VLAN mode according to the following flow chart after configuration based on *9.1 Web authentication configuration* and *9.2 Configuration common to all authentication modes.*

Figure 9-3 Configuration procedure for fixed VLAN mode



For details about the configuration, see the following:

1. Configuring fixed VLAN mode: *9.3.1 Configuring fixed VLAN mode*
2. URL redirect functionality configuration: *(1) Configuring URL redirect functionality* in *9.3.2 Configuration related to authentication processing*
3. Auto display URL configuration after successful authentication: *(2) Configuring auto display URL after successful authentication* in *9.3.2 Configuration related to authentication processing*
4. Auto logout condition configuration: *(3) Configuring auto logout conditions* in *9.3.2 Configuration related to authentication processing*
5. Configuration of the maximum number of users subject to authentication: *(4)*

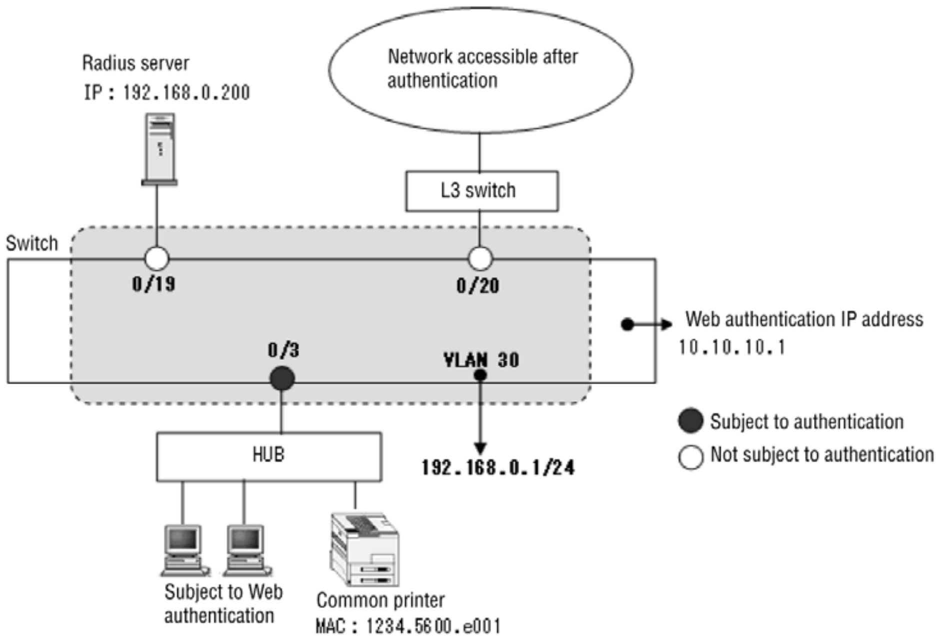
Configuring the maximum number of users subject to authentication in *9.3.2 Configuration related to authentication processing*

6. Configuring forced authentication ports: *(5) Configuring forced authentication ports* in *9.3.2 Configuration related to authentication processing*
7. Configuring roaming: *(6) Roaming (allowing communication for authenticated terminals moved between ports)configuration* in *9.3.2 Configuration related to authentication processing*
8. Configuring authentication exclusion: *(7) Configuring authentication exemption* in *9.3.2 Configuration related to authentication processing*
9. Individual Web authentication page configuration: *(8) Configuring individual Web authentication page by port* in *9.3.2 Configuration related to authentication processing*
10. Configuring the authentication IPv4 access list: *5.5.2 Configuring the authentication IPv4 access list*

    Before an unauthenticated terminal can obtain an IP address from the internal DHCP server of the Switch or an external DHCP server, an authentication IPv4 access list must be configured to allow communication with the target DHCP server before authentication. For details, see *5.5.2 Configuring the authentication IPv4 access list.*

9.3.1 Configuring fixed VLAN mode

Figure 9-4 Configuration example of fixed VLAN mode



(1) Configuring authentication ports and VLAN information for authentication

Points to note

Configure fixed VLAN mode and VLAN information for authentication for ports used for fixed VLAN mode.

Command examples

1. `(config)# vlan 30`

   `(config-vlan)# exit`

   Specifies VLAN ID 30.

2. `(config)# interface fastethernet 0/3`

   `(config-if)# switchport mode access`

   `(config-if)# switchport access vlan 30`

   Configures port 0/3 connected to terminals subject to authentication as an access port and configures VLAN 30 for authentication.

3. `(config-if)# web-authentication port`

   `(config-if)# exit`

   Sets fixed VLAN mode to port 0/3.

(2) Assigning IP addresses to VLAN interfaces

Points to note

Assign an IP address to a VLAN used in Web authentication.

Command examples

1. `(config)# interface vlan 30`

   `(config-if)# ip address 192.168.0.1 255.255.255.0`

   `(config-if)# exit`

   Configures an IP address to VLAN 30 used with Web authentication.

(3) Configuring authentication method list names for port-based authentication method

Points to note

Configure the name of an authentication method list for the port-based authentication method.

For details about the configuration of the authentication method list, see *(1) Configuring the authentication method group* in *9.2.1 Configuring the authentication method group and RADIUS server information.*

Command examples

1. `(config)# interface fastethernet 0/3`

   `(config-if)# web-authentication authentication WEB-list1`

   `(config-if)# exit`

   Configures an authentication method list name `WEB-list1` to port 0/3.

Notes

- If this information has not been configured, authentication follows the Switch default as explained in *(1)* Configuring the authentication method group in *9.2.1 Configuring the authentication method group* *and RADIUS server information.*

- When a name of an authentication method list set for a port does not match the name of an authentication method list of an authentication method group or is not present in an authentication method group, authentication will be performed according to the device default.
- The setting cannot be specified concurrently with the user ID-based authentication method in Web authentication or legacy mode. For details, see *5.2.2 Authentication method list.*

9.3.2 Configuration related to authentication processing

This subsection describes the settings for authentication processing for fixed VLAN mode.

(1) Configuring URL redirect functionality

(a) TCP port configuration for trigger packet

Points to note

Configure the destination TCP port number where trigger packets of redirect are sent. Packets to default TCPs (80 and 443) and the TCP port number configured here are included in these packets.

You can also add TCP port numbers for HTTP and HTTPS one by one using the `web-authentication web-port` configuration command.

Command examples

1. `(config)# web-authentication redirect tcp-port 8080`

   Adds TCP port number 8080.

   `(config)# web-authentication web-port https 24000`

   Adds TCP port number 24000 for HTTPS.

Notes

When different port numbers are added using the two commands above, basic port numbers and the additional port numbers configured by each of the commands are enabled. For operations when a single port number is added, see *(a) Adding URL redirection trigger packet TCP port numbers in (2) URL redirection* in *8.2.2 Authentication functionality.*

(b) Configuring a protocol for login operation

Points to note

Configure the protocol used for login operations that are subject to URL redirection.

Command examples

1. `(config)# web-authentication redirect-mode http`

   Uses HTTP with the URL redirect functionality for Web authentication.

(2) Configuring auto display URL after successful authentication

Points to note

Set the URL that a terminal accesses after successful authentication.

Command examples

1. `(config)# web-authentication jump-url "http://www.example.com/"`

   The user is directed to `http://www.example.com/` after successful authentication.

Notes

You can change the time before moving to the URL specified using the configuration command (default five seconds), but you do not need to configure the time in fixed VLAN mode. Change the time when you want to display the specified URL faster than by default.

(3) Configuring auto logout conditions

(a) Configuring maximum connection time

This configuration is common to all authentication modes of Web authentication. For details, see *9.2.3 Configuring auto logout condition common to all authentication modes* in *9.2 Configuration common to all authentication modes.*

(b) Configuring the functionality to monitor non-communication of an authenticated terminal

This functionality is enabled without configuring the `web-authentication auto-logout` configuration command when fixed VLAN mode and dynamic VLAN mode of Web authentication are enabled.

The user does not automatically log out using the `no web-authentication auto-logout` configuration command.

(c) Configuring the functionality to monitor connection of an authenticated terminal

Points to note

Configure the connection monitoring functionality to monitor connection of an authenticated terminal.

Command examples

1. `(config)# web-authentication logout polling enable`

   Enables the connection monitoring functionality.

2. `(config)# web-authentication logout polling interval 300`

   Configures 300 seconds to a polling interval of the connection-monitoring frame.

3. `(config)# web-authentication logout polling retry-interval 10`

   Configures 10 seconds to the number of retransmissions of the connection-monitoring frame.

4. `(config)# web-authentication logout polling count 5`

   Configures five times as the number of retransmissions of the connection-monitoring frame.

(d) Configuring special frame receiving conditions

This configuration is common to all authentication modes of Web authentication. For details, see *9.2.3 Configuring auto logout condition common to all authentication modes* in *9.2 Configuration common to all authentication modes.*

(4) Configuring the maximum number of users subject to authentication

Points to note

Configure the maximum number of users who can be authenticated in fixed VLAN mode.

For device settings, set this number by using global configuration mode, and to adjust the settings for ports, set this number by using the configuration mode corresponding to the ports.

Command examples

1. `(config)# web-authentication static-vlan max-user 30`

   Configures 30 users as the maximum number of users who can be authenticated in Web authentication.

(5) Configuring forced authentication ports

Points to note

Configure a port that will be permitted for forced authentication in fixed VLAN mode.

Command examples

1. `(config)# interface fastethernet 0/3`

   `(config-if)# web-authentication static-vlan force-authorized`

   `(config-if)# exit`

   Sets port 0/3 to a forced authentication port.

Notes

When using forced authentication, set only the RADIUS authentication method. Forced authentication does not operate with the following settings:

- `aaa authentication web-authentication default gourp radius local`
- `aaa authentication web-authentication default local gourp radius`

(6) Roaming (allowing communication for authenticated terminals moved between ports)configuration

Points to note

Configure an authentication terminal in fixed VLAN mode so that the terminal can communicate even if it has been moved to another port without port link-down.

Command examples

1. `(config)# web-authentication static-vlan roaming`

   Continues communication if an authenticated terminal is moved to a different port.

Notes

Roaming operates when the following conditions are met:

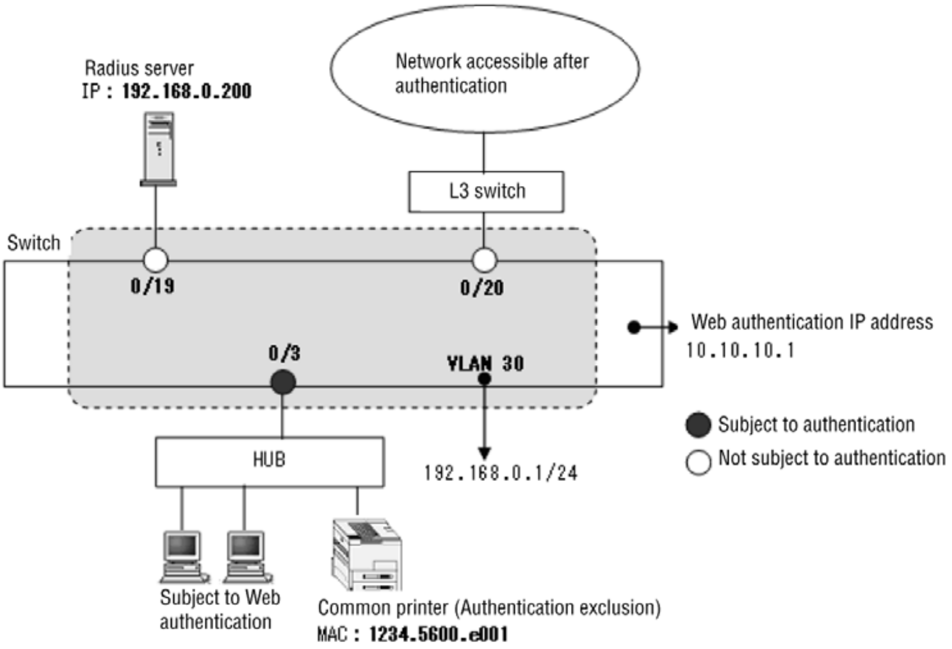
- Ports for fixed VLAN mode before and after moving

- The same VLAN before and after moving

(7) Configuring authentication exemption

Set ports and terminals in fixed VLAN mode to be exempted from authentication. In the figure below, ports 0/19 and 0/20, and the shared printer are exempted.

Figure 9-5 Configuration example of authentication exclusion in fixed VLAN mode



(a) Configuring ports exempted from authentication

Points to note

Do not configure authentication mode for ports to be exempted from authentication in fixed VLAN mode.

Command examples

1.
```
(config)# interface range fastethernet 0/19-20
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 30
(config-if-range)# exit
```

Sets ports 0/19 and 0/20 in VLAN ID 30 as access ports. Does not configure an authentication mode (web-authentication port).

(b) Configuring terminals exempted from authentication

Points to note

Register MAC addresses into the MAC address table for MAC addresses of terminals exempted from authentication in fixed VLAN mode.

Command examples

1.
```
(config)# mac-address-table static 1234.5600.e001 vlan 30
interface fastethernet 0/3
```

Configures the MAC addresses of a terminal to be exempted from authentication targets and where communication is permitted VLAN ID 30 (MAC address of the shared printer in the figure: 1234.5600.e001) in the MAC address table.

(8) Configuring individual Web authentication page by port

Points to note

Configure the custom file set names of individual Web authentication pages used for ports subject to authentication in fixed VLAN mode.

1.
```
(config)# interface fastethernet 0/3
(config-if)# web-authentication port
(config-if)# web-authentication html-fileset FILESETAAA
(config-if)# exit
```

Configures the custom file set name `FILESETAAA` for the individual Web authentication page used on port 0/3 (the name registered in the Switch using the `set web-authentication html-files` operation command as the custom file set name).

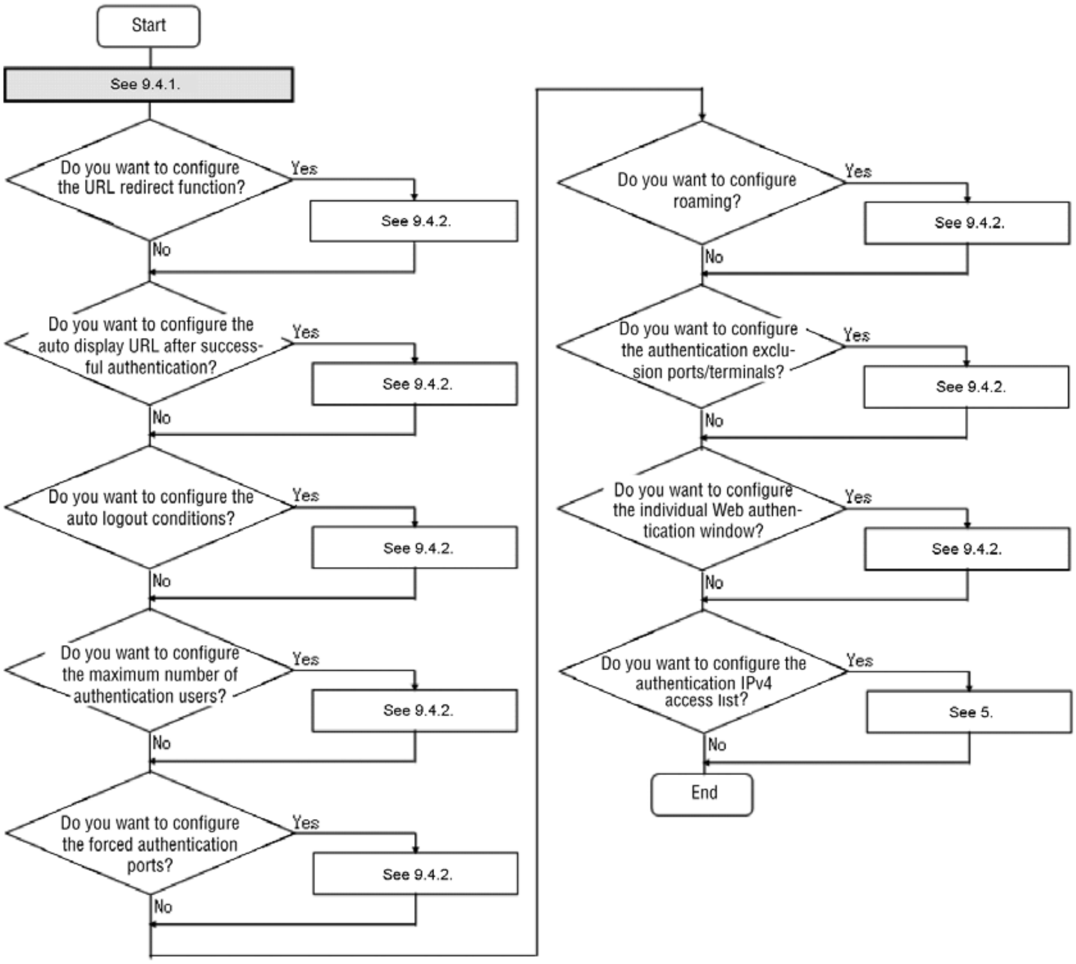
Notes

1. Configure the `web-authentication port` command to a port where this command is configured beforehand.
2. Register the custom file set of the individual Web authentication page to the Switch using the `set web-authentication html-files` operation command.

9.4 Configuring dynamic VLAN mode

Configure dynamic VLAN mode according to the following flow chart after configuration based on *9.1 Web authentication configuration* and *9.2 Configuration common to all authentication modes.*

Figure 9-6 Configuration procedure for dynamic VLAN mode



For details about the configuration, see the following:

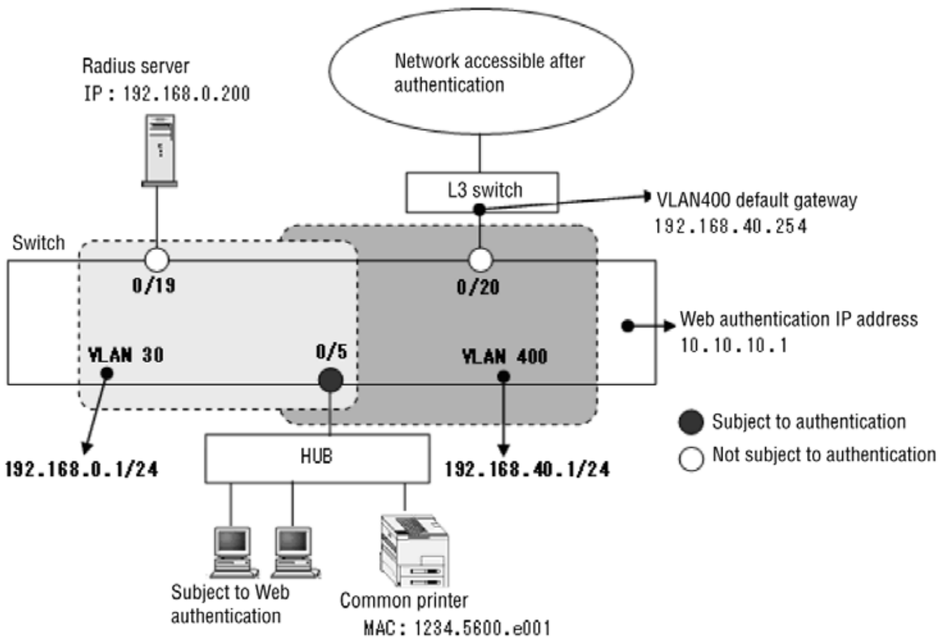
1. Configuring dynamic VLAN mode: *9.4.1 Configuring dynamic VLAN mode*
2. URL redirect functionality configuration: *(1) Configuring URL redirect functionality* in *9.4.2 Configuration related to authentication processing*
3. Auto display URL configuration after successful authentication: *(2) Configuring automatically displayed URL and time before moving from URL to URL after successful authentication* in *9.4.2 Configuration related to authentication processing*
4. Auto logout condition configuration: *(3) Configuring auto logout conditions* in *9.4.2 Configuration related to authentication processing*

5. Configuration of the maximum number of users subject to authentication: *(4) Configuring the maximum number of users subject to authentication* in *9.4.2 Configuration related to authentication processing*
6. Configuring forced authentication ports: *(5) Configuring forced authentication ports* in *9.4.2 Configuration related to authentication processing*
7. Configuring roaming: *(6) Roaming (allowing communication for authenticated terminals moved between ports) configuration* in *9.4.2 Configuration related to authentication processing*
8. Configuring authentication exclusion: *(7) Configuring authentication exemption* in *9.4.2 Configuration related to authentication processing*
9. Individual Web authentication page configuration: *(8) Configuring individual Web authentication page by port* in *9.4.2 Configuration related to authentication processing*
10. Configuring the authentication IPv4 access list: *5.5.2 Configuring the authentication IPv4 access list*

    Before an unauthenticated terminal can obtain an IP address from the internal DHCP server of the Switch or an external DHCP server, an authentication IPv4 access list must be configured to allow communication with the target DHCP server before authentication. For details, see *5.5.2 Configuring the authentication IPv4 access list.*

9.4.1 Configuring dynamic VLAN mode

Figure 9-7 Configuration example of dynamic VLAN mode



(1) Configuring authentication ports and VLAN information for authentication

Points to note

Configure dynamic VLAN mode and VLAN information for authentication for ports used for dynamic VLAN mode.

Command examples

1.
```
(config)# vlan 400 mac-based
(config-vlan)# exit
```
Configures VLAN ID 400 as a MAC VLAN.

2.
```
(config)# vlan 30
(config-vlan)# exit
```
Specifies VLAN ID 30.

3.
```
(config)# interface fastethernet 0/5
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 30
```
Configures port 0/5 where a terminal subject to authentication as a MAC port and specifies pre-authentication VLAN 30 (The post-authentication VLAN is assigned according to *5.4.3 Auto VLAN assignment for a MAC VLAN.)*

4.
```
(config-if)# web-authentication port
(config-if)# exit
```
Sets port 0/5 to dynamic VLAN mode.

(2) Assigning IP addresses to VLAN interfaces

Points to note

Configure the IP addresses to pre-authentication and post-authentication VLANs used in Web authentication.

Command examples

1.
```
(config)# interface vlan 30
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# exit
```
Configures the IP address to pre-authentication VLAN 30 used in Web authentication.

2.
```
(config)# interface vlan 400
(config-if)# ip address 192.168.40.1 255.255.255.0
(config-if)# exit
```
Configures an IP address to post-authentication VLAN 400 used in Web authentication.

(3) Configuring authentication method list names for authentication method by port

Points to note

Set the name of an authentication method list for the port-based authentication method.

For details about the configuration of the authentication method list, see *(1) Configuring the authentication method group* in *9.2.1 Configuring the authentication method group and RADIUS server information.*

Command examples

1.
```
(config)# interface fastethernet 0/5
(config-if)# web-authentication authentication WEB-list1
(config-if)# exit
```

Configures an authentication method list name `WEB-list1` to port 0/5.

Notes

- If this information has not been configured, authentication follows the Switch default in *(1) Configuring the authentication method group* in *9.2.1 Configuring the authentication method group and RADIUS server information.*
- When a name of an authentication method list set for a port does not match the name of an authentication method list of an authentication method group or is not present in an authentication method group, authentication will be performed according to the device default.
- User ID-based authentication method and legacy mode of Web authentication are not interoperable. For details, see *5.2.2 Authentication method list.*

9.4.2 Configuration related to authentication processing

The subsection describes settings concerning authentication processing for dynamic VLAN mode.

(1) Configuring URL redirect functionality

Configuration is the same as for fixed VLAN mode. For details, see *(1) Configuring URL redirect functionality* in *9.3.2 Configuration related to authentication processing.*

(2) Configuring automatically displayed URL and time before moving from URL to URL after successful authentication

Points to note

Configure a URL for terminal access after successful authentication and time required to move to a different URL.

Command examples

1.
```
(config)# web-authentication jump-url "http://www.example.com/"
delay 30
```

Displays the page of http://www.example.com/ 30 seconds after successful authentication.

Notes

Because the IP address of a terminal needs to be changed with switching from a pre-authentication VLAN to a post-authentication VLAN, configure approximately 20-30 seconds as the time before moving to a different URL.

If IP addresses have been distributed to unauthenticated terminals on the internal DHCP server (default lease time: 10 seconds), the IP addresses are obtained from the normal DHCP server for a post-authentication VLAN. Accordingly, it might take approximately 20-30 seconds before an authenticated VLAN can communicate after the completion of authentication.

(3) Configuring auto logout conditions

(a) Configuring maximum connection time

This configuration is common to all authentication modes of Web authentication. For details, see *9.2.3 Configuring auto logout condition common to all authentication modes* in *9.2 Configuration common to all authentication modes.*

(b) Configuring the functionality to monitor non-communication of an authenticated terminal

This configuration is the same as for fixed VLAN mode. For details, see *(b) Configuring the functionality to monitor non-communication of an authenticated terminal* in *(3) Configuring auto logout conditions* in *9.3.2 Configuration related to authentication processing.*

(c) Configuring special frame receiving conditions

This configuration is common to all authentication modes of Web authentication. For details, see *9.2.3 Configuring auto logout condition common to all authentication modes* in *9.2 Configuration common to all authentication modes.*

(4) Configuring the maximum number of users subject to authentication

Points to note

Configure the maximum number of users who can be authenticated in dynamic VLAN mode.

For device settings, set this number by using global configuration mode, and to adjust the settings for ports, set this number by using the configuration mode corresponding to the ports.

Command examples

1. `(config)# web-authentication max-user 5`

   Configures 5 users as the maximum number of users who can be authenticated in Web authentication.

(5) Configuring forced authentication ports

Points to note

Allow forced authentication and assign a post-authentication VLAN to ports in dynamic VLAN mode.

Command examples

1. `(config)# interface fastethernet 0/5`

   `(config-if)# web-authentication force-authorized vlan 400` `(config-if)# exit`

Allows forced authentication at port 0/5 and specifies the VLAN ID of the post-authentication VLAN to be assigned.

Notes

1. By using the `vlan` configuration command, set the VLAN ID with the `mac-based` setting (MAC VLAN setting).
2. When using forced authentication, set only the RADIUS authentication method. Forced authentication does not operate with the following settings:
   - `aaa authentication web-authentication default gourp radius local`
   - `aaa authentication web-authentication default local gourp radius`

(6) Roaming (allowing communication for authenticated terminals moved between ports) configuration

Points to note

Configure an authentication terminals in dynamic VLAN mode so that the terminal can communicate even if it has been moved to another port without linking down the ports.

Command examples

1. `(config)# web-authentication roaming`

   Continues communication if an authenticated terminal is moved to a different port.

Notes

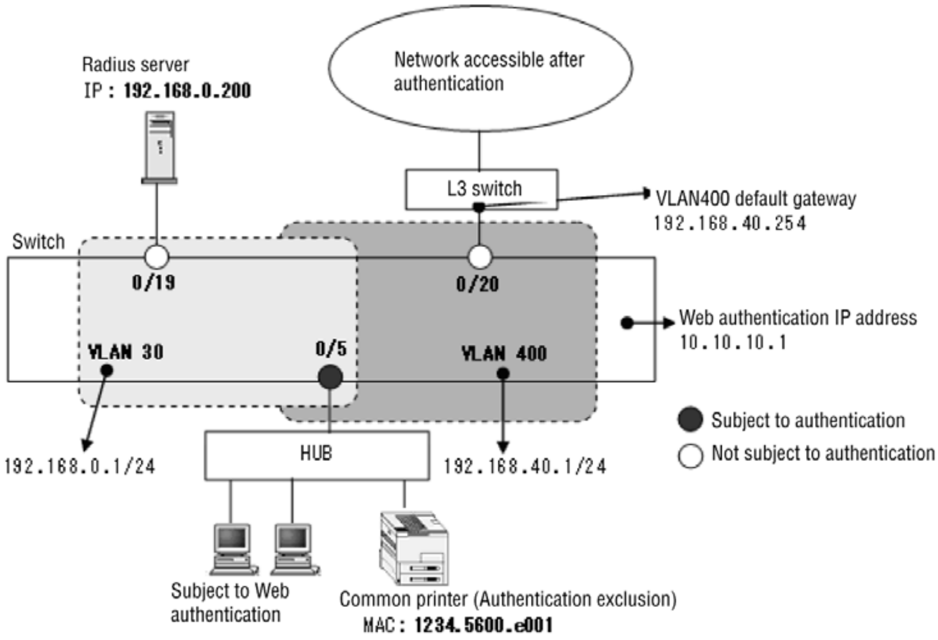
Roaming operates when the following conditions are met:

- Ports for dynamic VLAN mode before and after moving

(7) Configuring authentication exemption

Set ports and terminals in dynamic VLAN mode to be exempted from authentication. In the figure below, ports 0/19 and 0/20, and the shared printer are exempted.

Figure 9-8 Configuration example of authentication exclusion in dynamic VLAN mode



(a) Configuring ports exempted from authentication

Points to note

Configure ports exempted from authentication as access ports, without specifying the authentication mode.

Command examples

1.
```
(config)# interface fastethernet 0/19
(config-if)# switchport mode access
(config-if)# switchport access vlan 30
(config-if)# exit
```

Sets port 0/19 in VLAN ID 30 as an access port. Does not configure an authentication mode (web-authentication port).

2.
```
(config)# interface fastethernet 0/20
(config-if)# switchport mode access
(config-if)# switchport access vlan 400
(config-if)# exit
```

Sets port 0/20 in MAC VLAN ID 400 as an access port. Does not configure an authentication mode (web-authentication port).

(b) Configuring terminals exempted from authentication

Points to note

Register the MAC address of a terminal exempted from authentication in a

MAC VLAN and a MAC address table.

Command examples

1. `(config)# vlan 400 mac-based`

   `(config-vlan)# mac-address 1234.5600.e001`

   `(config-vlan)# exit`

   Configures the MAC address to be exempted from authentication to the MAC VLAN ID 400 (MAC address of the shared printer in the figure: `1234.5600.e001`).

2. `(config)# interface fastethernet 0/5`

   `(config-if)# switchport mode mac-vlan`

   `(config-if)# switchport mac vlan 400`

   `(config-if)# exit`

   Specifies MAC VLAN ID 400 to which the exempted terminal belongs for an authentication port.

3. `(config)# mac-address-table static 1234.5600.e001 vlan 400 interface fastethernet 0/5`

   Configures, into the MAC address table, the MAC address of a terminal exempted from authentication on port 0/5 of MAC VLAN ID 400 (MAC address of the shared printer in the figure: `1234.5600.e001`).

Notes

Before adding the MAC address of the terminal excluded from authentication to the MAC address table, set the VLAN ID of MAC VLAN to the port to which the terminal belongs.

(8) Configuring individual Web authentication page by port

Points to note

Configure the custom file set names of individual Web authentication pages used for ports subject to authentication in dynamic VLAN mode.

Command examples

1. `(config)# interface fastethernet 0/5`

   `(config-if)# web-authentication port`

   `(config-if)# web-authentication html-fileset FILESETBBB`

   `(config-if)# exit`

   Configures the custom file set name `FILESETBBB` for the individual Web authentication page used on port 0/5 (the name registered in the Switch using the `set web-authentication html-files` operation command as the custom file set name).

Notes

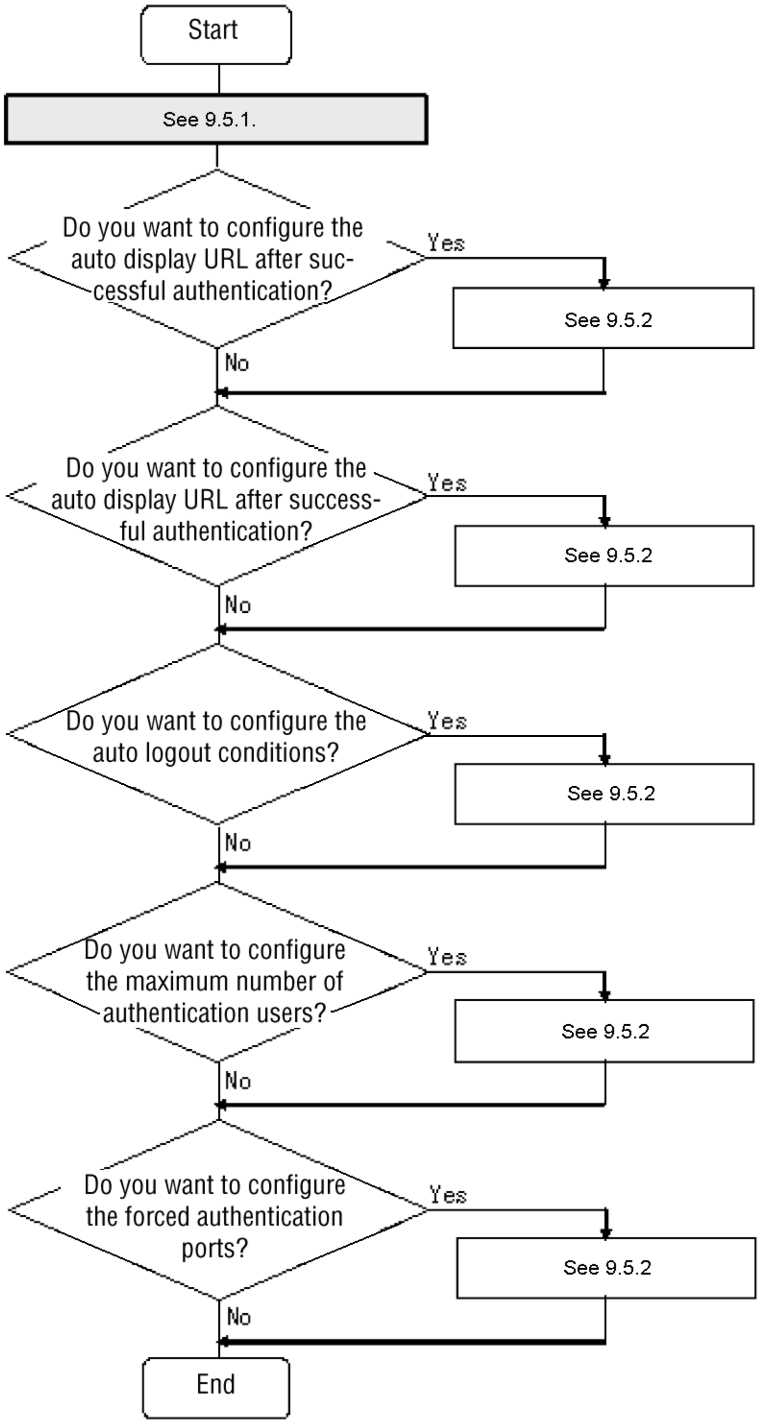
1. Configures the `web-authentication port` command to a port where this command is configured beforehand.
2. Registers the custom file set of the individual Web authentication page

to the Switch using the `set web-authentication html-files` operation command.

9.5 Configuring legacy mode

Configure legacy mode according to the following flow chart after configuration based on *9.1 Web authentication configuration* and *9.2 Configuration common to all authentication modes.*

Figure 9-9 Configuration procedure for legacy mode

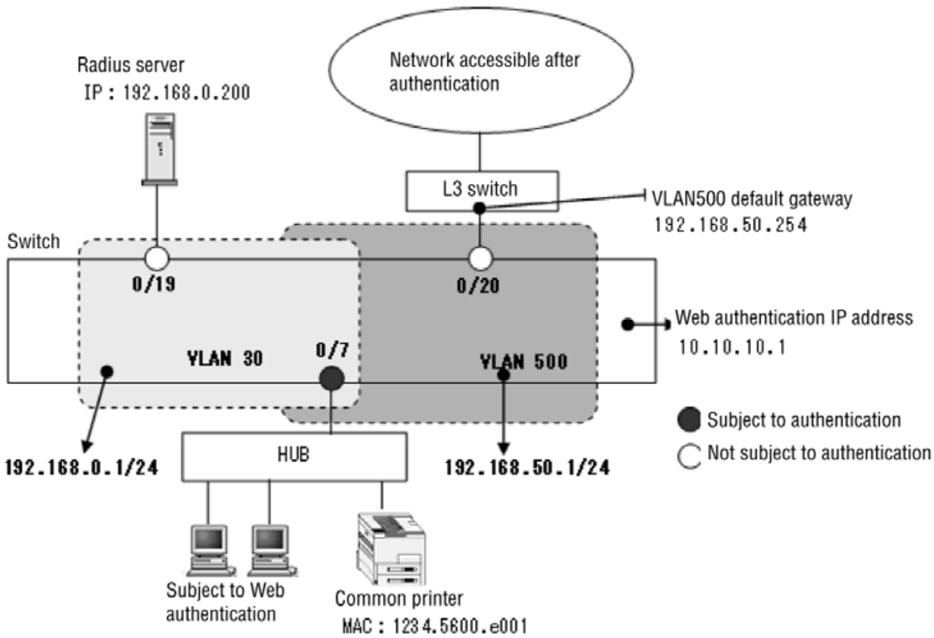


For details about the configuration, see the following:

1. Configuring legacy mode: *9.5.1 Configuring legacy mode*
2. Auto display URL configuration after successful authentication: *(1) Configuring automatically displayed URL and time before moving from URL to URL after successful authentication* in *9.5.2 Configuration related to authentication processing*
3. Auto logout condition configuration: *(2) Configuring auto logout conditions* in *9.5.2 Configuration related to authentication processing*
4. Configuration of the maximum number of users subject to authentication: *(3) Configuring the maximum number of users subject to authentication* in *9.5.2 Configuration related to authentication processing*
5. Configuring forced authentication ports: *(4) Configuring forced authentication ports* in *9.5.2 Configuration related to authentication processing*
6. Configuring authentication exclusion: *(5) Configuring authentication exemption* in *9.5.2 Configuration related to authentication processing*

9.5.1 Configuring legacy mode

Figure 9-10 Configuration example for legacy mode



(1) Configuring authentication ports and VLAN information for authentication

Points to note

Configure the authentication VLAN information to the port used in legacy mode.

Command examples

1.
```
(config)# vlan 500 mac-based
(config-vlan)# exit
```

Configures VLAN ID 500 as a MAC VLAN.

2.
```
(config)# vlan 30
(config-vlan)# exit
```
Configures VLAN ID 30.

3.
```
(config)# interface fastethernet 0/7
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 500
(config-if)# switchport mac native vlan 30
(config-if)# exit
```
Configures port 0/7 where a terminal subject to authentication as a MAC port and specifies pre-authentication VLAN 30 and post-authentication VLAN ID 500.

(2) Configuring the post-authentication VLAN

Points to note

Configure the post-authentication VLAN ID used for legacy mode. After authentication succeeds in legacy mode, the network is switched dynamically to the VLAN set by this command.

Command examples

1.
```
(config)# web-authentication vlan 500
```
Configures VLAN ID 500 of a post-authentication VLAN in legacy mode.

Notes

When this information is not set, authentication in legacy mode fails. Set the target VLAN ID.

(3) Assigning IP addresses to VLAN interfaces

Points to note

Configure the IP addresses to pre-authentication and post-authentication VLANs used in Web authentication.

Command examples

1.
```
(config)# interface vlan 30
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# exit
```
Configures the IP address to pre-authentication VLAN 30 used in Web authentication.

2.
```
(config)# interface vlan 500
(config-if)# ip address 192.168.50.1 255.255.255.0
(config-if)# exit
```

Configures an IP address to post-authentication VLAN 500 used in Web authentication.

9.5.2 Configuration related to authentication processing

This subsection describes the settings for the authentication processing of legacy mode.

(1) Configuring automatically displayed URL and time before moving from URL to URL after successful authentication

The configuration procedure is the same as for dynamic VLAN mode. For details, see *(2) Configuring automatically displayed URL and time before moving from URL to URL after successful authentication* in *9.4.2 Configuration related to authentication processing.*

(2) Configuring auto logout conditions

(a) Configuring maximum connection time

This configuration is common to all authentication modes of Web authentication. For details, see *9.2.3 Configuring auto logout condition common to all authentication modes* in *9.2 Configuration common to all authentication modes.*

(b) Configuring MAC address table aging monitoring

This functionality is enabled without configuring the `web-authentication auto-logout` configuration command when legacy mode of Web authentication is enabled.

The user does not automatically log out using the `no web-authentication auto-logout` configuration command.

(c) Configuring special frame receiving conditions

This configuration is common to all authentication modes of Web authentication. See *9.2.3 Configuring auto logout condition common to all authentication modes* in *9.2 Configuration common to all authentication modes.*

(3) Configuring the maximum number of users subject to authentication

The configuration procedure is the same as for dynamic VLAN mode. For details, see *(4) Configuring the maximum number of users subject to authentication* in *9.4.2 Configuration related to authentication processing.*

(4) Configuring forced authentication ports

Points to note

Allow forced authentication at a legacy mode port, and specify the post-authentication VLAN to be assigned.

Command examples

1.
```
(config)# interface fastethernet 0/7
(config-if)# web-authentication force-authorized vlan 500
(config-if)# exit
```

Allows forced authentication at port 0/7 and specifies the VLAN ID of the post-authentication VLAN to be assigned.

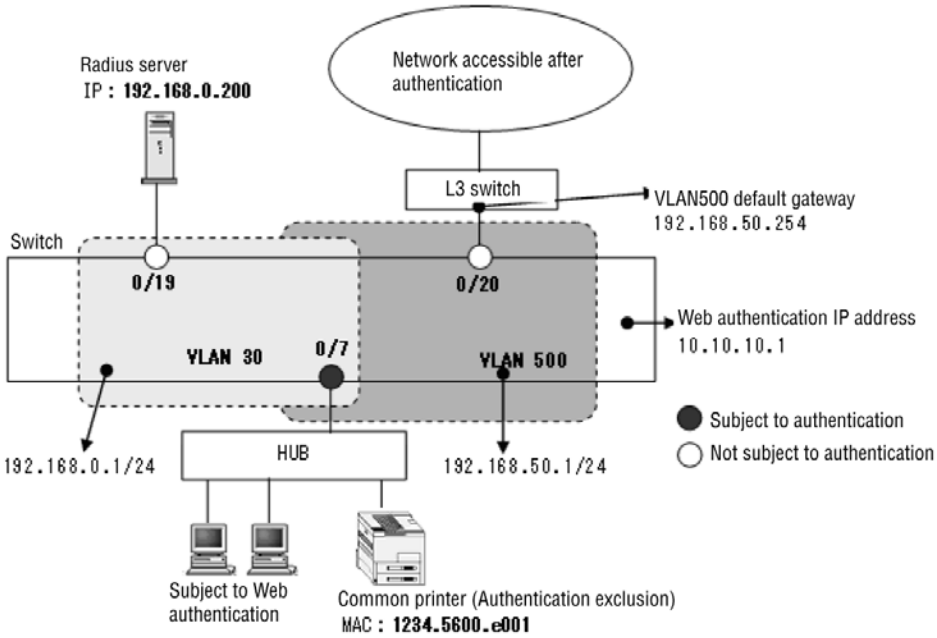
Notes

1. By using the `vlan` configuration command, set the VLAN ID with the `mac-based` setting (MAC VLAN setting).
2. When using forced authentication, set only the RADIUS authentication method. Forced authentication does not operate with the following settings:
   - `aaa authentication web-authentication default gourp radius local`
   - `aaa authentication web-authentication default local gourp radius`

(5) Configuring authentication exemption

Configure ports and terminals to be exempted from authentication in legacy mode. In the figure below, ports 0/19 and 0/20, and the shared printer are exempted.

Figure 9-11 Configuration example of authentication exclusion in legacy mode



(a) Configuring ports exempted from authentication

Points to note

Designates the port where you wish to bypass authentication as an access port.

Command examples

1. `(config)# interface fastethernet 0/19`
   `(config-if)# switchport mode access`
   `(config-if)# switchport access vlan 30`
   `(config-if)# exit`

   Sets port 0/19 in VLAN ID 30 as an access port.

2.
```
(config)# interface fastethernet 0/20
(config-if)# switchport mode access
(config-if)# switchport access vlan 500
(config-if)# exit
```
Sets port 0/20 of MAC VLAN ID 500 as an access port.

(b) Configuring terminals exempted from authentication

Points to note

Register MAC addresses of terminals exempted from authentication to a MAC VLAN.

Command examples

1.
```
(config)# vlan 500 mac-based
(config-vlan)# mac-address 1234.5600.e001
(config-vlan)# exit
```
Configures the MAC address to be exempted from authentication to the MAC VLAN ID 500 (MAC address of the shared printer in the figure: `1234.5600.e001`).

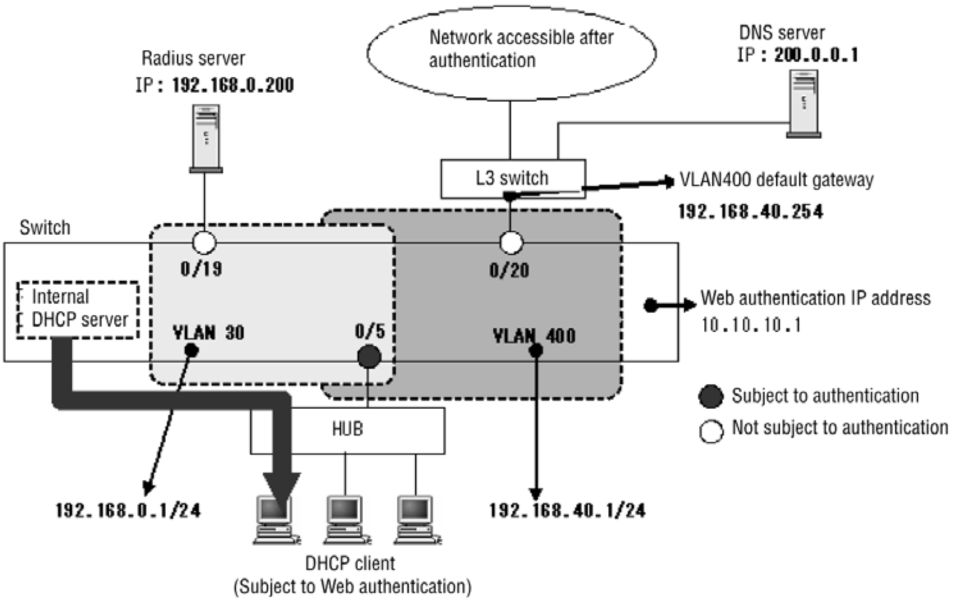
9.6 Configuring internal DHCP server

This configuration distributes IP addresses to DHCP clients (terminals subject to authentication) in Web authentication. This example includes the internal DHCP server using *9.4 Configuring dynamic VLAN mode* as a basic structure.

Points to note

Specify the IP addresses that you want to be excluded from assignment to DHCP clients. Create a DHCP address pool and use it to dynamically assign IP addresses to DHCP clients.

Figure 9-12 Configuration example of internal DHCP server (dynamic VLAN mode)



Command examples

1. `(config)# service dhcp vlan 30`

   Enables the DHCP server for pre-authentication VLAN 30.

2. `(config)# ip dhcp excluded-address 192.168.0.1`

   `(config)# ip dhcp excluded-address 192.168.0.200`

   Excludes the IP addresses for VLAN 30 of the Switch and the RADIUS server.

3. `(config)# ip dhcp pool POOL30`

   `(dhcp-config)# network 192.168.0.0/24`

   Configures the address pool name `POOL30` and the network address of the address pool (configure the same network address as pre-authentication VLAN 30).

4. `(dhcp-config)# lease 0 0 1`

   Configures the lease time of the address (1 minute).

5. `(dhcp-config)# default-router 192.168.0.1`

   Configures the IP address of pre-authentication VLAN 30 as the default router.

6. `(dhcp-config)# dns-server 200.0.0.1`

   `(dhcp-config)# exit`

   Configures the IP address of the DNS server.

Configure the following to use the internal DHCP server for post-authentication VLAN.

Command examples

1. `(config)# service dhcp vlan 400`

   Enables the DHCP server for post-authentication VLAN 400.

2. `(config)# ip dhcp excluded-address 192.168.40.1`

   `(config)# ip dhcp excluded-address 192.168.40.254`

   Excludes the IP address of VLAN 400 of the Switch and the default gateway address of the L3 switch.

3. `(config)# ip dhcp pool POOL400`

   `(dhcp-config)# network 192.168.40.0/24`

   Configures the address pool name `POOL400` and the network address of the address pool (configure the same network address as post-authentication VLAN 400).

4. `(dhcp-config)# lease 1`

   Configures the lease time of the address (one day).

5. `(dhcp-config)# default-router 192.168.40.1`

   Configures the IP address of the post-authentication VLAN 400 as the default router.

6. `(dhcp-config)# dns-server 200.0.0.1`

   `(dhcp-config)# exit`

   Configures the IP address of the DNS server.

9.7 Operation of Web authentication

9.7.1 List of operation commands

The following table describes the operation commands used in Web authentication.

Table 9-4 List of operation commands

Command name	Description
`set web-authentication user`	Adds user information (user ID, password, and post-authentication VLAN ID for Web authentication to the internal Web authentication DB (editing user information).
`set web-authentication passwd`	Changes the password of a registered user ID in the internal Web authentication DB (editing user information).
`set web-authentication vlan`	Changes the post-authentication VLAN ID of a registered user ID in the internal Web authentication DB (editing user information).
`remove web-authentication user`	Deletes user information from the internal Web authentication DB (editing user information).
`commit web-authentication`	Applies any additions or changes you made to the internal Web authentication DB.
`store web-authentication`	Backs up the internal Web authentication DB to a file.
`load web-authentication`	Restores the internal Web authentication DB from a backup file.
`show web-authentication user`	Displays the contents of the internal Web authentication DB and any pending additions or changes.
`clear web-authentication auth-state`	Forcibly logs out an authenticated user.
`show web-authentication`	Displays the configuration for Web authentication.
`show web-authentication login`	Displays the configuration for Web authentication.
`show web-authentication login select-option`	Displays the authentication status for Web authentication after selecting the display option.
`show web-authentication login summary`	Displays the number of authenticated users.
`show web-authentication statistics`	Displays statistics for Web authentication.
`clear web-authentication statistics`	Clears the statistics.

Command name	Description
show web-authentication logging	Displays the operation log messages collected by Web authentication.
clear web-authentication logging	Clears the operation log messages collected by Web authentication.
set web-authentication html-files	Registers the specified custom file set for the Web authentication page in the Switch.
clear web-authentication html-files	Deletes the custom file set for the Web authentication page registered in the Switch.
show web-authentication html-files	Displays the file names and sizes of the custom file set for the Web authentication page, as well as the date and time of registration.
store web-authentication html-files	Collects the running custom file set for the Web authentication page and stores the files in a directory of a RAMDISK.

The table below shows the list of operation commands for the internal DHCP server.

Table 9-5 List of operation commands for the internal DHCP server

Command name	Description
show ip dhcp binding	Displays the binding information on the DHCP server.
clear ip dhcp binding	Deletes the binding information from the DHCP server database.
show ip dhcp conflict	Displays an IP address conflict detected by the DHCP server. An IP address conflict refers to when an IP address is indicated as available in the IP address pool on the DHCP server but is already assigned to a terminal on the network.
clear ip dhcp conflict	Clears the IP address conflict information from the DHCP server.
show ip dhcp server statistics	Displays statistics about the DHCP server.
clear ip dhcp server statistics	Resets statistics on the DHCP server.

9.7.2 Registering the internal Web authentication DB

Use the set web-authentication user operation command to register information about a Web authentication user (such as a user ID, password, and post-authentication VLAN ID) in the internal Web authentication DB. Specifically, you can use this command to edit (add/change/delete) user information and apply additions or changes to the internal Web authentication DB. Examples of the registration are shown below.

You need to complete the environmental settings for Web authentication and configuration before adding user information.

(1) Adding user information

Use the set `web-authentication user` operation command to add a user ID, password, and post-authentication VLAN ID for each user subject to authentication.

- Fixed VLAN mode: Specify the VLAN ID for the port connected to the user (terminal) subject to authentication.
- Dynamic VLAN mode and legacy mode: Specify the VLAN ID that accommodates the user (terminal) subject to authentication.

In the example below, USER01-USER05 (five users) are registered.

Command input

```
# set web-authentication user USER01 PAS0101 100
# set web-authentication user USER02 PAS0200 100
# set web-authentication user USER03 PAS0300 100
# set web-authentication user USER04 PAS0320 100
# set web-authentication user USER05 PAS0400 100
```

(2) Changing or deleting user information

Follow the procedure below to change the password of the registered user and post-authentication VLAN ID, and then delete the user.

(a) Changing the password

Use the `set web-authentication passwd` operation command to change the password of the registered user. In the example below, the password is for the user ID (`USER01`).

Command input

```
# set web-authentication passwd USER01 PAS0101 PPP4321
```

Changes the password of `USER01` from `PAS0101` to `PPP4321`.

(b) Changing post-authentication VLAN ID

Use the `set web-authentication vlan` operation command to change the post-authentication VLAN ID of the registered user.

- Fixed VLAN mode: Specify the VLAN ID for the port connected to the user (terminal) subject to authentication.
- Dynamic VLAN mode and legacy mode: Specify the VLAN ID that accommodates the user (terminal) subject to authentication.

In the example below, the post-authentication VLAN ID is for the user ID (`USER01`).

Command input

```
# set web-authentication vlan USER01 200
```

Changes the post-authentication VLAN ID of the user ID (`USER01`) to 200.

(c) Deleting user information

Use the `remove web-authentication user` operation command to delete registered user information. In the example below, user information is for the user ID (`USER01`).

Command input

```
# remove web-authentication user USER01
Remove web-authentication user  Are you sure? (y/n): y

#
```

Deletes the user ID (`USER01`).

(3) Applying additions or changes to the internal Web authentication DB

Applies additions or changes in user information to the internal Web authentication DB by the `commit web-authentication` operation command.

Command input

```
# commit web-authentication
Commitment web-authentication user data. Are you sure? (y/n): y

Commit complete.
#
```

9.7.3 Backing up and restoring the internal Web authentication DB

This subsection describes how to back up the internal Web authentication DB and restore the database from the backup file.

(1) Backing up the internal Web authentication DB

Create a backup file (`backupfile` in the example below) for the internal Web authentication DB using the `store web-authentication` operation command.

Command input

```
# store web-authentication ramdisk backupfile
Backup web-authentication user data.  Are you sure? (y/n): y

Backup complete.
#
```

(2) Restoring the internal Web authentication DB

Use the `load web-authentication` operation command to restore the internal Web authentication DB from a backup file (`backupfile` in the example below).

Command input

```
# load web-authentication ramdisk backupfile
Restore web-authentication user data.  Are you sure? (y/n): y

Restore complete.
#
```

9.7.4 Displaying Web authentication configuration status

Web authentication configuration status is displayed with the `show web-authentication` operation command.

Figure 9-13 Displaying Web authentication configuration status

```
# show web-authentication

Date 2011/02/23 06:45:42 UTC
<<<Web-Authentication mode status>>>
  Dynamic-VLAN     : Enable
```

```
 Static-VLAN     : Enable

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Dynamic-VLAN
  ip address      : Disable
  web-port        : HTTP : 80(Fixed)  HTTPS : 443(Fixed)
  max-user        : 256
  user-group      : Disable
  user replacement : Disable
  roaming         : Disable
  html-files      : Default
  web-authentication vlan :

 * AAA methods
  Authentication Default      : RADIUS
  Authentication port-list-AAA : RADIUS ra-group-1
  Authentication End-by-reject : Disable
  Accounting Default         : RADIUS

 * Logout parameter
  max-timer       : 60(min)
  auto-logout     : Enable
  logout ping     : tos-windows:   1  ttl:   1
  logout polling   : -

 * Redirect parameter
  redirect        : Enable
  redirect-mode    : HTTPS
  tcp-port        : 80(Fixed), 443(Fixed)
  web-port        : HTTP : 80(Fixed)  HTTPS : 443(Fixed)
  jump-url        : Disable

 * Logging status
  [Syslog send]    : Disable
  [Traps]         : Disable

 * Internal DHCP sever status
  service dhcp vlan: Disable

<Port configuration>
  Port Count          : 2

  Port               : 0/6
  VLAN ID             : 40
  Forceauth VLAN       : Disable
  Access-list-No       : L2-auth
  ARP relay           : Enable
  Max-user            : 256
  HTML fileset         : FILESETXYZ

  Port               : 0/22
  VLAN ID             : 40
  Forceauth VLAN       : Disable
  Access-list-No       : L2-auth
  ARP relay           : Enable
  Max-user            : 256
  Authentication method : port-list-AAA
  HTML fileset         : FILESETXYZ
```

```
<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Static-VLAN
  ip address      : Disable
  web-port        : HTTP : 80(Fixed)  HTTPS : 443(Fixed)
  max-user        : 1024
  user-group      : Disable
  user replacement : Disable
  roaming         : Disable
  html-files      : Default
  web-authentication vlan : -

 * AAA methods
  Authentication Default      : RADIUS
  Authentication port-list-AAA : RADIUS ra-group-1
  Authentication End-by-reject : Disable
  Accounting Default         : RADIUS

 * Logout parameter
  max-timer       : 60(min)
  auto-logout     : Enable
  logout ping     : tos-windows:   1  ttl:   1
  logout polling   : Enable  [ interval: 300, count: 3, retry-interval: 1 ]

 * Redirect parameter
  redirect        : Enable
  redirect-mode    : HTTPS
  tcp-port        : 80(Fixed), 443(Fixed)
  web-port        : HTTP : 80(Fixed)  HTTPS : 443(Fixed)
  jump-url        : Disable

 * Logging status
  [Syslog send]    : Disable
  [Traps]         : Disable

 * Internal DHCP sever status
  service dhcp vlan: -

<Port configuration>
  Port Count          : 3

  Port               : 0/5
  VLAN ID             : 4
  Forceauth VLAN       : Disable
  Access-list-No       : L2-auth
  ARP relay           : Enable
  Max-user            : 1024
  Authentication method : port-list-AAA
  HTML fileset        : FILESETXYZ

  Port               : 0/6
  VLAN ID             : 4
  Forceauth VLAN       : Disable
  Access-list-No       : L2-auth
  ARP relay           : Enable
  Max-user            : 1024
  HTML fileset        : FILESETXYZ
```

```
  Port                : 0/22
  VLAN ID              : 4
  Forceauth VLAN        : Disable
  Access-list-No        : L2-auth
  ARP relay            : Enable
  Max-user             : 1024
  Authentication method : port-list-AAA
  HTML fileset          : FILESETXYZ

#
```

9.7.5 Displaying the status of Web authentication

Use the `show web-authentication statistics` command to display the status of Web authentication and the status of communication with the RADIUS server.

Figure 9-14 Displaying the status of Web authentication

```
# show web-authentication statistics

Date 2009/10/29 03:05:10 UTC
Web-Authentication Information:
  Authentication Request Total :       13
  Authentication Current Count :        1
  Authentication Error Total   :        2

RADIUS Web-Authentication Information:
[RADIUS frames]
  TxTotal   :       15  TxAccReq  :       14  TxError   :        1
  RxTotal   :       12  RxAccAccpt:       10  RxAccRejct:        2
                      RxAccChllg:        0  RxInvalid :        0
Account Web-Authentication Information:
[Account frames]
  TxTotal   :       19  TxAccReq  :       18  TxError   :        1
  RxTotal   :       18  RxAccResp :       18  RxInvalid :        0

#
```

9.7.6 Displaying the status of Web authentication sessions

(1) Displaying without specifying display options

Use the `show web-authentication login` command to display the authentication status of users logged in using Web authentication.

Figure 9-15 Displaying the status of Web authentication sessions

```
# show web-authentication login

Date 2009/03/24 17:12:13 UTC
 Dynamic VLAN mode total login counts(Login/Max):   1 / 256
  Authenticating client counts :    0
  Port roaming : Disable
   No F User name                    Port VLAN Login time        Limit
    1 * USER20-all_floor@example.com    0/20  200 2009/03/24 17:09:15 00:57:02

 Static VLAN mode total login counts(Login/Max):    1 / 1024
  Authenticating client counts :    0
  Port roaming : Disable
   No F User name                    Port VLAN Login time        Limit
    1   USER10-all_floor@example.com    0/10   10 2009/03/24 17:08:25 00:56:12
```

```
#
```

(2) Displaying by specifying display options (specifying select-option)

Displays the Web authentication configuration status by the `show web-authentication login select-option` operation command with the display option specified. The following example illustrates an implementation where an interface port number is specified.

Figure 9-16 Displaying information when a port is specified

```
# show web-authentication login select-option port 0/10

Date 2009/03/24 17:12:22 UTC
 Static VLAN mode total login counts(Login/Max):    1 / 1024
  Authenticating client counts :    0
  Port roaming : Disable
   No F User name                    Port VLAN Login time         Limit
    1   USER10-all_floor@example.com     0/10   10 2009/03/24 17:08:25 00:56:03

#
```

(3) Displaying only the number of authenticated terminals (summary display)

Displays the number of authenticated users by using the `show web-authentication login summary` operation command.

Figure 9-17 Displaying only the number of authenticated users

```
# show web-authentication login summary port

Date 2009/03/24 17:15:42 UTC
 Dynamic VLAN mode total login counts(Login/Max):   1 / 256
  Port roaming : Disable
   No  Port  Login /  Max
    1  0/20     1 /  256

 Static VLAN mode total login counts(Login/Max):    1 / 1024
  Port roaming : Disable
   No  Port  Login /  Max
    1  0/10     1 / 1024

#
```

9.7.7 Registering Web authentication files

(1) Registering the basic Web authentication page custom file set

Register the basic Web authentication custom file set as shown below.

1. Using a PC or other external device, create the HTML pages to be used as the Web authentication pages. (The set of the files is referred to as the basic Web authentication custom file set.)
2. Copy the basic Web authentication custom file set onto a RAMDISK from a memory card.
3. Register the basic Web authentication custom file set using the set `web-authentication html-files` operation command.

Figure 9-18 Registering the basic Web authentication page custom file set

```
# copy mc webfileset ramdisk webfileset
```

```
# set web-authentication html-files ramdisk webfileset
Do you wish to install new html-files ? (y/n):y
executing...
Install complete.
#
```

(2) Registering the individual Web authentication page custom file set

Register the individual Web authentication custom file set as shown below.

1. Using a PC or other external device, create the HTML pages to be used as the Web authentication pages. (The set of the files is referred to as the individual Web authentication custom file set.)
2. Copy the individual Web authentication custom file set onto a RAMDISK from a memory card.
3. Register the individual Web authentication custom file set using the set `web-authentication html-files` operation command.

Figure 9-19 Registering the individual Web authentication page files

```
# copy mc filesetAAA ramdisk filesetAAA

# set web-authentication html-files ramdisk filesetAAA html-fileset FILESETAAA
Do you wish to install new html-files ? (y/n):y
executing...
Install complete.
#
```

Notes

- Be sure to specify the `html-fileset` parameter and the custom file set name using the `set web-authentication html-files` operation command when registering individual Web authentication page custom file sets. If these settings are not specified, files are registered as basic Web authentication custom file sets.
- Specify the name of the individual Web authentication page custom file set to be registered in the Switch in uppercase alphanumeric characters.
- Specify the custom file set name registered using this command (`FILESETAAA` in the example above) when specifying the individual Web authentication page custom file set by port. (For information about configuration of the individual Web authentication page by port, see *(8)* Configuring individual Web authentication page by port in *9.3.2 Configuration related to authentication processing.)*

9.7.8 Displaying information about Web authentication page file

To display information about the Web authentication page files you registered, use the `show web-authentication html-files` operation command.

Figure 9-20 Displaying information about Web authentication page file

```
# show web-authentication html-files

Date 2009/10/29 02:59:53 UTC
   Total Size :        50,356
```

```
File Date           Size Name
2009/10/29 02:12     1,507 login.html         ...1
2009/10/29 02:12     1,307 loginProcess.html   ...2
2009/10/29 02:12     1,260 loginOK.html
2009/10/29 02:12       666 loginNG.html
2009/10/29 02:12       937 logout.html
2009/10/29 02:12       586 logoutOK.html
2009/10/29 02:12       640 logoutNG.html
2009/10/29 02:12       545 webauth.msg
default now              0 favicon.ico        ...3
2009/10/29 02:12    17,730 the other files
< FILESETXYZ >                              ...4
2009/10/29 02:14     1,507 login.html
2009/10/29 02:14     1,307 loginProcess.html
2009/10/29 02:14     1,260 loginOK.html
2009/10/29 02:14       666 loginNG.html
2009/10/29 02:14       937 logout.html
2009/10/29 02:14       586 logoutOK.html
2009/10/29 02:14       640 logoutNG.html
2009/10/29 02:14       545 webauth.msg
default now              0 favicon.ico
2009/10/29 02:14    17,730 the other files

#
```

1. Displays the time when the basic Web authentication page custom file set was registered.
2. `loginProcess.html` is used for one-time password authentication. For details, see *14. One-time Password Authentication [OP-OTP].*
3. For the default status, `default now` is displayed.
4. Displayed when the individual Web authentication page custom file set is being registered.

9.7.9 Deleting the registered individual Web authentication page custom file set

Use the `clear web-authentication html-files` command to delete the Web authentication pages you registered using the `set web-authentication html-files` operation command.

Figure 9-21 Deleting the individual Web authentication page custom file set

```
# clear web-authentication html-files
Do you wish to clear registered html-files and initialize? (y/n):y
executing...
Clear complete.

#
```

Figure 9-22 Deleting the individual Web authentication page custom file set

```
# clear web-authentication html-files html-fileset FILESETAAA
Do you wish to clear registered html-files and initialize? (y/n):y
executing...
Clear complete.

#
```

Figure 9-23 Deleting all custom file sets

```
# clear web-authentication html-files -all
Do you wish to clear registered html-files and initialize? (y/n):y
executing...
Clear complete.

#
```

9.7.10 Retrieving the running Web authentication page custom file set

Use the `store web-authentication html-files` operation command to store the running Web authentication page custom file set in a directory in a RAMDISK. Use the `copy` operation command to copy the Web authentication page custom file set stored in the RAMDISK to a memory card. (When restarting the Switch, files in the RAMDISK are deleted.)

Because the Web authentication page custom file sets are retrieved at the same time, you cannot specify files individually.

Figure 9-24 Retrieving the basic Web authentication page custom file set

```
# store web-authentication html-files ramdisk webfileset
Do you wish to store html-files? (y/n): y
executing...
Store complete.

#
```

Figure 9-25 Retrieving the individual Web authentication page custom file set

```
# store web-authentication html-files ramdisk filesetAAA html-filset FILESETAAA
Do you wish to store html-files? (y/n): y
executing...
Store complete.

#
```

Notes

Use the `set web-authentication html-files` operation command to specify the custom file set name specified by the `html-fileset` parameter when retrieving individual Web authentication page custom file sets. If these settings are not specified, files are retrieved as basic Web authentication custom file sets.

9.7.11 Checking the DHCP server

(1) Checking the number of IP addresses that can be assigned

The number of IP addresses that can be assigned to clients is displayed by `address pools`, which is the result of executing the `show ip dhcp server statistics` operation command. Make sure that the number displayed here is greater than the number of IP addresses you want to assign to clients.

Figure 9-26 Result of executing show ip dhcp server statistics

```
# show ip dhcp server statistics

Date 2009/04/13 09:31:14 UTC
  < DHCP Server use statistics >
```

```
    address pools         : 252
    automatic bindings     : 1
    expired bindings      : 1
    over pools request     : 0
    discard packets       : 0
  < Receive Packets >
    DHCPDISCOVER          : 8
    DHCPREQUEST           : 4
    DHCPDECLINE           : 2
    DHCPRELEASE           : 1
    DHCPINFORM            : 1
 < Send Packets >
    DHCPOFFER             : 8
    DHCPACK               : 4
    DHCPNAK               : 0

#
```

(2) Checking the assigned IP addresses

Use the `show ip dhcp binding` operation command to check IP addresses assigned to DHCP clients. IP addresses that are still in lease are displayed.

Figure 9-27 Result of executing show ip dhcp binding

```
> show ip dhcp binding

Date 2008/11/26 09:29:33 UTC
 No  IP Address       MAC Address     Lease Expiration      Type
 1   192.168.100.1    00d0.5909.7121   2008/11/26 10:29:16    Automatic

>
```

9.7.12 Authentication procedure from terminal

This subsection describes the procedure for logging in and logging out from a Web authentication terminal. Follow the procedure below after the configuration necessary for Web authentication is complete.

(1) Configuring IP address to unauthenticated terminal

If you use a DHCP server for the IP address settings for a terminal and connect a terminal subject to authentication to a pre-authentication VLAN, the terminal requests an IP address from the DHCP server. The DHCP server assigns an unauthenticated IP address to the terminal. The terminal can access Web authentication.

If you do not use the DHCP server, assign the IP address for authentication (IP address to access the Switch) to the terminal manually.

(2) Displaying the login page for Web authentication

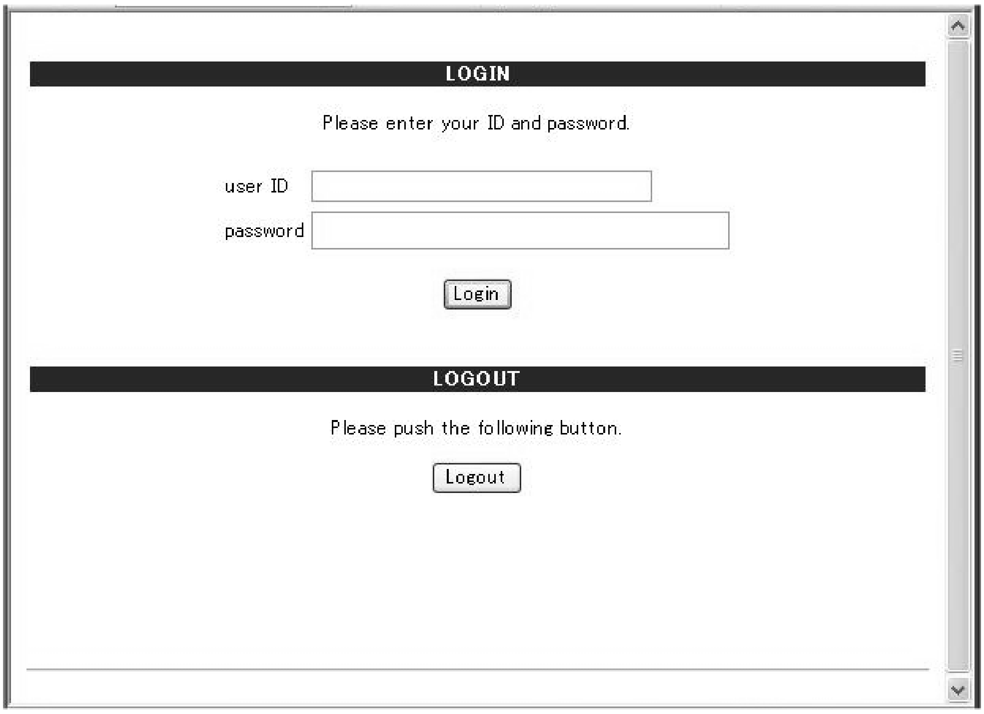
Accesses the WEB authentication URL (`http://`*pre-authentication-VLAN-interface-IP address*`/login.htm`) if no Web authentication IP address has been configured.

Accesses the WEB authentication URL (`http://`*Web-authentication-IP-address*`/login.htm`) if a Web authentication IP address has been configured.

Enter your user ID and password in the Web authentication Login page.

This page is common to logging in and logging out. For details, see *(7) Specifying the common URL for login and logout* and *(8) Logout from the Login Success page* in *9.7.12 Authentication procedure from terminal.*

Figure 9-28 Login page



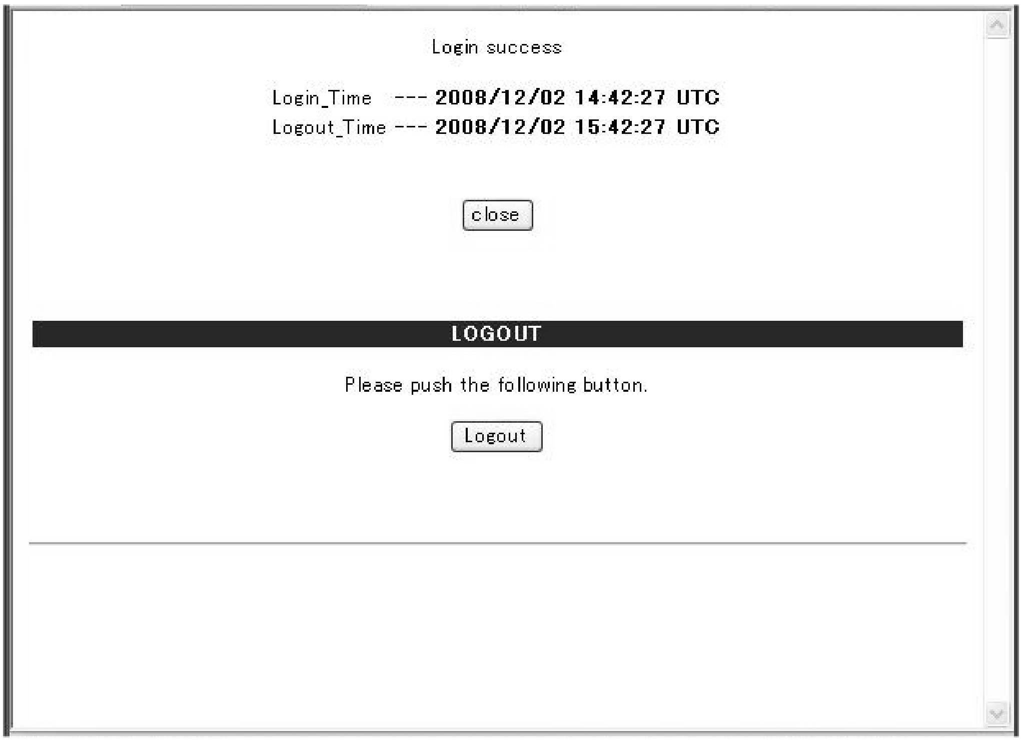
(3) Authenticating the user ID and password entered in the login page

In local authentication mode, the Switch compares the entered user ID and password against user information stored in the internal Web authentication DB. Also, checks whether authentication is possible after requesting the RADIUS server.

(4) Displaying the Authentication Success page with successful authentication

When a user matches the information in the internal Web authentication DB or RADIUS server, the Login Success page is displayed enabling communication within a VLAN. Furthermore, accommodation in the VLAN is changed according to the VLAN IDs registered by the user.

Figure 9-29 Login success page



Cancel authentication by pressing the **Logout** button in the page instead of closing the page. To use the **Logout** button in the Login Success page, see *(8)* Logout from the Login Success page in *9.7.12 Authentication procedure from terminal.*

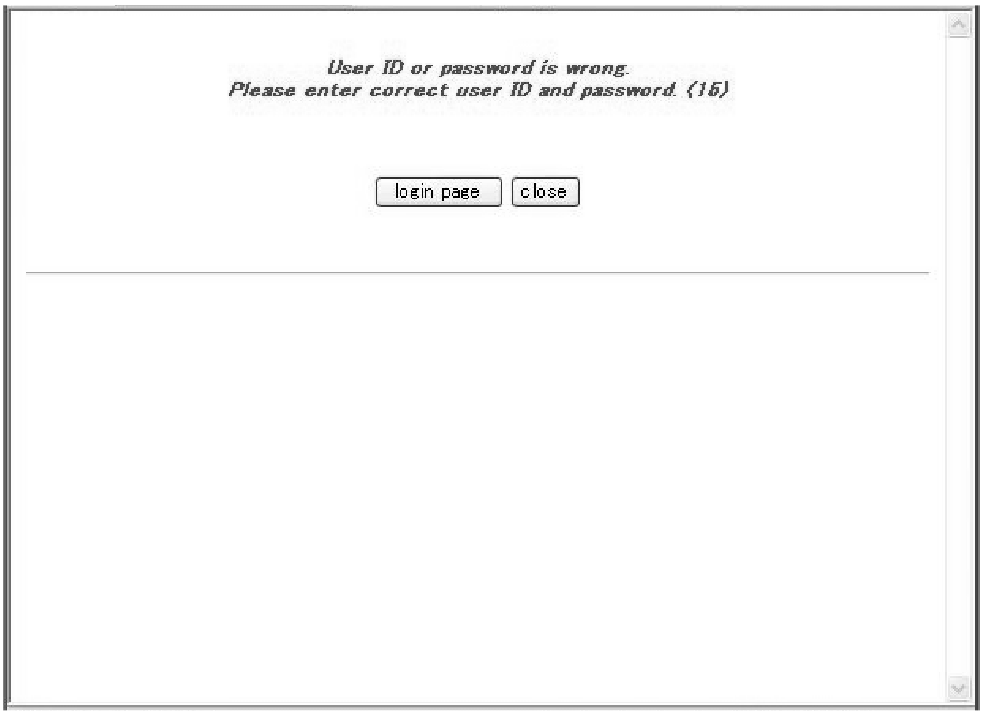
If you used the `web-authentication jump-url` configuration command to direct users to a specific URL after authentication, the user's Web browser automatically accesses the specified URL after the login success page appears.

(5) Displaying a page when login fails

The Authentication Error page is displayed when authentication fails.

8.7 Authentication error messages shows the causes of errors displayed in the Authentication Error page.

Figure 9-30 Login failed page



(6) logout

A terminal logs out by any of the following means (auto logout depends on the authentication mode provided by the Switch. For more details, see *8. Description of Web Authentication).*

- Logout when maximum connection time is exceeded
- Logout of an authenticated terminal by monitoring non-communication monitoring (in legacy mode, logout by MAC address table aging monitoring)
- Logout of an authenticated terminal by the connection monitoring functionality
- Logout by receiving a special frame from an authentication terminal
- Logout of a terminal connected to a link-down port
- Logout resulting from changes to the VLAN configuration
- Logout using the Web interface
- Logout using an operation command

After logging out in the Web page or if forcibly logged out from Web authentication, change the IP address of the terminal with the unauthenticated IP address. If you are using the DHCP server, request an IP address for the terminal.

(a) Logout using the Web interface

Access the URL that has successfully passed Web authentication from the terminal (`http://`*post-authentication-VLAN-interface-IP-address*`/login.html`) to display the Logout page on the terminal. When pressing the **Logout** button in the page, you can log out from Web authentication.

After authentication is canceled, the VLAN ID is re-accommodated in the original VLAN, and the Logout Completion page is displayed.

Figure 9-31 Logout page

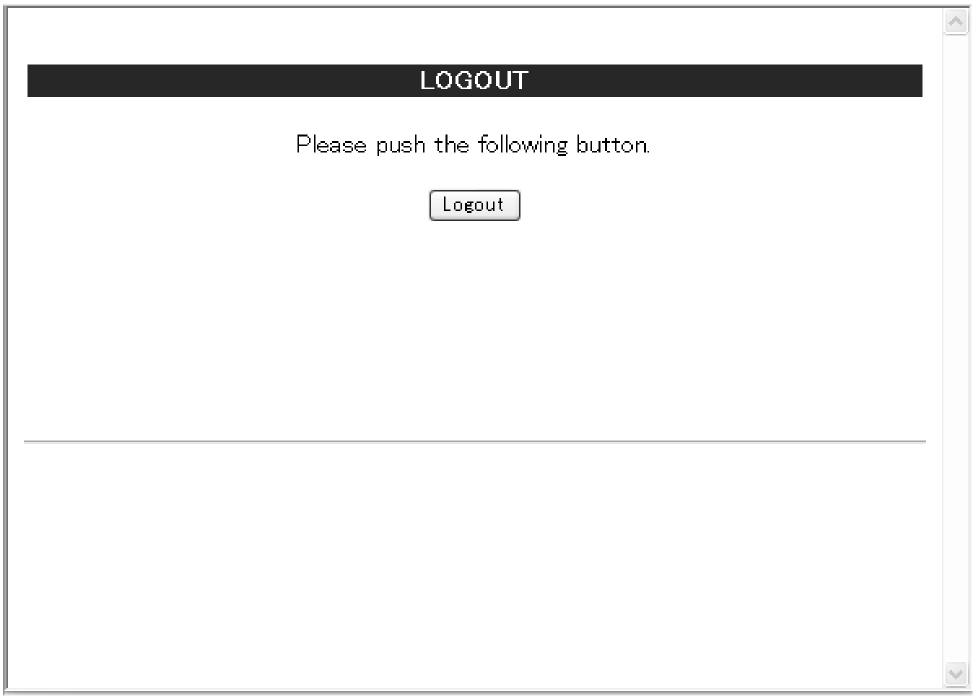


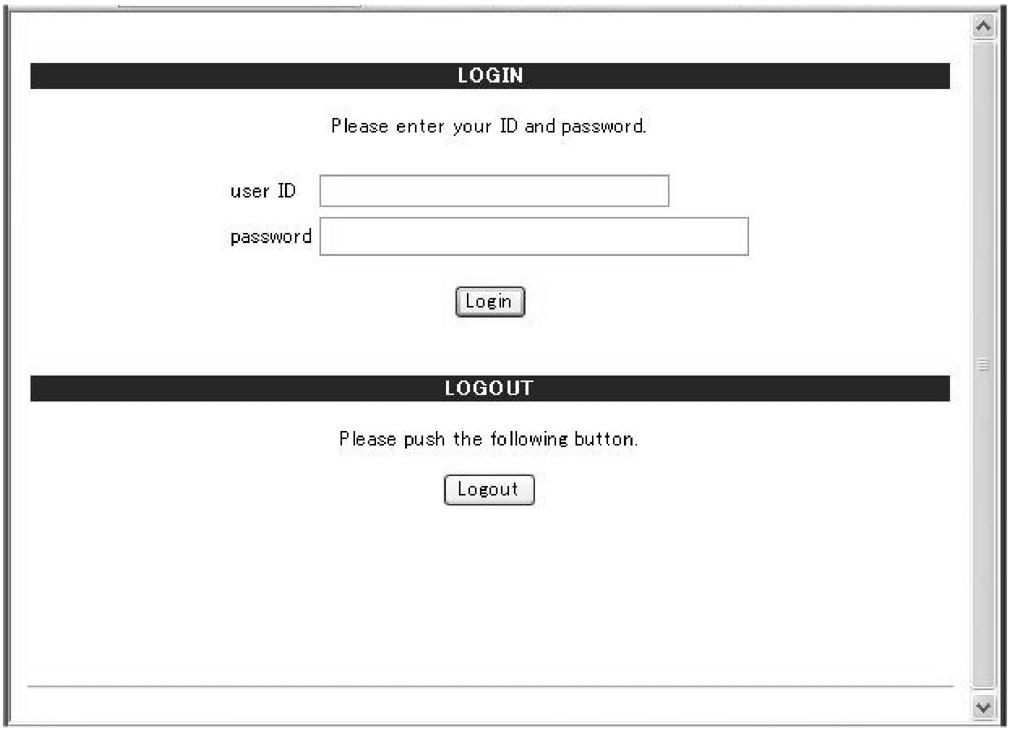
Figure 9-32 Logout completed page

(7) Specifying the common URL for login and logout

You can specify the URL common to logging in and logging out (`http://`*pre-authentication-or-post-authentication-VLAN-interface-IP-address*`/`). (You do not need to specify `login.html` or `logout.html` after the IP address.)

You need to configure the default gateway to use the **Logout** button. For details, see *(8) Logout from the Login Success page* in *9.7.12 Authentication procedure from terminal.*

Figure 9-33 Common Login and Logout page



(8) Logout from the Login Success page

You can log out by clicking the **Logout** button in the Login Success page by specifying the IP address of the post-authentication VLAN interface for the terminal to be authenticated as the default gateway. (same as logout in the page common to logging in and logging out).

- When using the DHCP server to configure a terminal's IP address, configure the IP address of the post-authentication VLAN interface to address information to be distributed as the default router option.
- If you do not use the DHCP server, manually specify the IP address of the post-authentication VLAN interface for a terminal as the default gateway.

Specify the URL common to logging in and logging out (`http://`*post-authentication-VLAN-interface-IP-address*`/`) when logging in to Web authentication.

Use the Login Success page (see *Figure 9-29 Login success page)* after it is displayed without closing it. You can cancel authentication by clicking the **Logout** button in the page.

(9) IP address of authenticated terminal

If you have used the DHCP server to configure the IP address for a terminal, an authenticated IP address is sent by the DHCP server and you can access the authenticated network after the accommodated VLAN of the terminal is changed.

If you do not use the DHCP server, manually change the IP address for the terminal to the network address after authentication after the Login Success page is displayed. When you use the default gateway, change the address.

10. Description of MAC-based Authentication

The MAC-based authentication functionality controls access to VLANs by terminals authenticated by using MAC addresses. This chapter provides an overview of MAC-based authentication.

10.1 Overview

MAC-based authentication provides functionality for authenticating a terminal by using the source MAC address of a frame sent from a terminal and allows communication only from authenticated terminals.

(1) Authentication mode

The following authentication modes are available for MAC-based authentication:

- Fixed VLAN mode

  Registers the MAC address of a successfully authenticated terminal in the MAC address table and allows access to the VLAN designated by the configuration for communication.

- Dynamic VLAN mode

  Registers the MAC address of a successfully authenticated terminal in the MAC VLAN and MAC address table. Terminals are given access to different VLANs before and after authentication.

- Legacy mode

  Performs VLAN switching via the MAC VLAN and enables terminals to access different VLANs before and after authentication.

(2) Authentication method group

You can configure the authentication method groups below for MAC-based authentication. (The configured authentication method groups can be used in all MAC-based authentication modes.)

- Switch default: Local authentication method

  This authentication method uses an authentication database stored on the Switch (called an internal MAC-based authentication DB).

- Switch default: RADIUS authentication method

  Authentication is performed by using a RADIUS server deployed on the network.

- Authentication method list

  Authentication is performed by using a RADIUS server group registered in the authentication method list when specific conditions are met.

(3) Supported functionality by authentication mode

The following table lists the supported functionality of each authentication mode.

Table 10-1 Supported functionality by authentication mode

Functionality		Fixed VLAN	Dynamic VLAN	Legacy
Switch default: Local authentication	Internal MAC-based authentication DB	Y See *10.2.1*. See *10.6.1*.	Y See *10.3.1*. See *10.6.1*.	Y See *10.4.1*. See *10.6.1*.

Functionality			Fixed VLAN	Dynamic VLAN	Legacy
		MAC address	Y See *11.6.2*.	Y See *11.6.2*.	Y See *11.6.2*.
		VLAN	Y See *11.6.2*.	Y See *11.6.2*.	Y See *11.6.2*.
		Password	N	N	N
	VLAN (Post-authentication VLAN)		Y See *10.2.1*. See *11.3.2*.	Y See *10.3.1*. See *11.4.1*.	Y See *10.4.1*. See *11.5.1*.
Switch default: RADIUS authentication	External server ● RADIUS server information for MAC-based authentication ● General-purpose RADIUS server information		Y See *5.3.1*. See *10.2.1*. See *10.6.2*. See *11.2.1*.	Y See *5.3.1*. See *10.3.1*. See *10.6.2*. See *11.2.1*.	Y See *5.3.1*. See *10.4.1*. See *10.6.2*. See *11.2.1*.
		User ID (MAC address)	1 to 32 characters See *10.2.1*. See *10.6.2*. See *11.2.4*.	1 to 32 characters See *10.3.1*. See *10.6.2*. See *11.2.4*.	1 to 32 characters See *10.4.1*. See *10.6.2*. See *11.2.4*.
		VLAN	Y See *10.6.2*.	Y See *10.6.2*.	Y See *10.6.2*.
		Password	1 to 32 characters See *10.6.2*. See *11.2.4*.	1 to 32 characters See *10.6.2*. See *11.2.4*.	1 to 32 characters See *10.6.2*. See *11.2.4*.
	VLAN (Post-authentication VLAN)		Y See *10.2.1*. See *10.6.2*. See *11.3.2*.	Y See *10.3.1*. See *10.6.2*. See *11.4.1*.	Y See *10.4.1*. See *10.6.2*. See *11.5.1*.
	Forced authentication		Y See *10.2.2*[#].	Y See *10.3.2*[#].	Y See *10.4.2*.
		Authentication permission port configured	Y See *11.3.2*	Y See *11.4.2*.	Y See *11.5.2*.

Functionality			Fixed VLAN	Dynamic VLAN	Legacy
		Private trap	Y See *10.5*.	Y See *10.5*.	Y See *10.5*.
	MAC address format at authentication and password specification		Y See *10.6.2*. See *11.2.4*.	Y See *10.6.2*. See *11.2.4*.	Y See *10.6.2*. See *11.2.4*.
Authentication method list	External server ● RADIUS server group information		Y See *5.3.1*. See *10.2.1*. See *10.6.2*. See *11.2.1*.	Y See *5.3.1*. See *10.3.1*. See *10.6.2*. See *11.2.1*.	N
	Port-based authentication		Y See *5.2.2*. See *5.2.3*.	Y See *5.2.2*. See *5.2.3*.	N
Maximum number of authenticated terminals	Port-based		1,024 See *10.2.2*. See *11.3.2*.	256 See *10.3.2*. See *11.4.2*.	256 See *10.4.2*. See *11.5.2*.
	At the Switch level		1,024 See *10.2.2*. See *11.3.2*.	256 See *10.3.2*. See *11.4.2*.	256 See *10.4.2*. See *11.5.2*.
Authentication and re-authentication	Re-authentication delay timer		Y See *10.2.2*. See *11.2.4*.	Y See *10.3.2*. See *11.2.4*.	Y See *10.4.2*. See *11.2.4*.
	Periodic re-authentication request		Y See *10.2.2*. See *11.2.4*.	Y See *10.3.2*. See *11.2.4*.	Y See *10.4.2*. See *11.2.4*.
	Authentication target MAC address restriction (MAC access list)		Y See *10.2.2*. See *11.2.2*.	Y See *10.3.2*. See *11.2.2*.	Y See *10.4.2*. See *11.2.2*.
	Authentication IPv4 access list		Y See *5.4.1*. See *5.5.2*.	Y See *5.4.1*. See *5.5.2*.	N
Authentication status canceled	Maximum connection time exceeded		Y See *10.2.2*. See *11.2.3*.	Y See *10.3.2*. See *11.2.3*.	Y See *10.4.2*. See *11.2.3*.

Functionality		Fixed VLAN	Dynamic VLAN	Legacy
	Monitoring for authenticated terminal non-communication	Y See *10.2.2*. See *11.3.2*.	Y See *10.3.2*. See *11.4.2*.	N
	Monitoring for MAC address table aging	N	N	Y See *10.4.2*. See *11.5.2*.
	Authenticated terminal connection port link down	Y See *10.2.2*.	Y See *10.3.2*.	N
	VLAN configuration change	Y See *10.2.2*.	Y See *10.3.2*.	Y See *10.4.2*.
	Operation command	Y See *10.2.2*.	Y See *10.3.2*.	Y See *10.4.2*.
Roaming (moving authenticated terminal between ports)	Port move permission configured	Y See *10.2.2*. See *11.3.2*.	Y See *10.3.2*. See *11.4.2*.	N
	Private trap	Y See *10.5*.	Y See *10.5*.	N
Accounting log	Accounting log built in the Switch	2,100 lines for all modes See *10.5*.		
	RADIUS server accounting functionality	Common to all modes See *5.3.4*. See *10.5*. See *11.2.5*.		

Legend:

Y: Supported

N: Not supported

See *5.x.x*: See the relevant section in *5. Overview of Layer 2 Authentication.*

See *10.x.x*: See the relevant section in this chapter.

See *11.x.x*: See the relevant section in *11. MAC-based Authentication Configuration and Operation.*

#

For details about using forced authentication common to all authentication modes, see *5.4.6 Forced authentication common to all authentication modes.*

The following table summarizes the operating conditions of MAC-based authentication.

Table 10-2 Operating conditions of MAC-based authentication

<table>
<tr><th colspan="2">Type</th><th>Port setting</th><th>Specifiable VLAN type</th><th>Frame type</th><th>Fixed VLAN mode</th><th>Dynamic VLAN mode</th><th>Legacy mode</th></tr>
<tr><td rowspan="7">Port type</td><td>Access port</td><td>native</td><td>Port VLAN
MAC VLAN</td><td>Untagged</td><td>Y</td><td>N</td><td>N</td></tr>
<tr><td rowspan="2">Trunk port</td><td>native</td><td>Port VLAN</td><td>Untagged</td><td>Y</td><td>N</td><td>N</td></tr>
<tr><td>allowed</td><td>Port VLAN
MAC VLAN</td><td>Tagged</td><td>Y</td><td>N</td><td>N</td></tr>
<tr><td>Protocol port</td><td>--</td><td>--</td><td>--</td><td>N</td><td>N</td><td>N</td></tr>
<tr><td rowspan="3">MAC Port</td><td>native</td><td>Port VLAN</td><td>Untagged</td><td>Y#</td><td>N</td><td>N</td></tr>
<tr><td>mac</td><td>MAC VLAN</td><td>Untagged</td><td>N</td><td>Y</td><td>Y</td></tr>
<tr><td>dot1q</td><td>Port VLAN
MAC VLAN</td><td>Tagged</td><td>Y</td><td>N</td><td>N</td></tr>
<tr><td colspan="5">Default VLAN</td><td>Y</td><td>N</td><td>N</td></tr>
<tr><td rowspan="3">Interface type</td><td colspan="4">fastethernet</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td colspan="4">gigabitethernet</td><td>Y</td><td>Y</td><td>Y</td></tr>
<tr><td colspan="4">port channel</td><td>N</td><td>N</td><td>N</td></tr>
</table>

Legend:

Y: Available

N: Not available

--: Not applicable for authentication ports

#

For details, see *5.4.4 Auto authentication mode accommodation on the same MAC port.*

The subsequent sections give an overview of fixed VLAN mode, dynamic VLAN mode, and legacy mode. For the same functionality and same operation in each authentication mode, read the descriptions given in the references.

10.2 Fixed VLAN mode

Prior to authentication, a terminal cannot start communication until it is successfully authenticated. If authentication succeeds in fixed VLAN mode, the MAC address of the terminal and the post-authentication VLAN are registered in the MAC address table as a MAC-based authentication entry, enabling the terminal to communicate. (Entries registered in the MAC address table can be confirmed by using the `show mac-address-table` operation command.)

10.2.1 Authentication method group

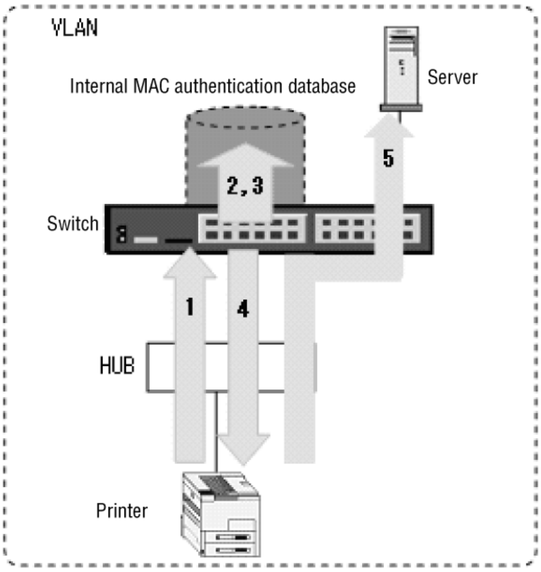
In the MAC-based authentication method group, the Switch default is used in common for all MAC-based authentication modes, and an authentication method list is used in both fixed VLAN mode and dynamic VLAN mode. For details, see the following sections:

- *5.1.3 Authentication method groups*
- *5.3.3 Priority configuration for the Switch default local and RADIUS authentications*
- *5.2.2 Authentication method list*
- *5.3.1 RADIUS server information used with the Layer 2 authentication method*
- *11.2.1 Configuring the authentication method group and RADIUS server information*

(1) Switch default: local authentication

The source MAC address of frames received from a terminal is compared with the MAC addresses in the internal MAC-based authentication DB. If the source MAC address matches an entry in the database, authentication is successful, and the terminal is allowed to access the network.

Figure 10-1 Fixed VLAN mode (local authentication method)



1. The Switch receives a frame from a terminal (the printer in the figure) connected via a hub.
2. The VLAN ID of the terminal to be authenticated (the printer in the figure) is determined from a connection port or VLAN ID of the terminal to be authenticated.
3. The MAC address of the received frame is compared with those in the internal MAC-based authentication DB of the Switch.

   For details about VLAN ID matching, see *Table 10-3 VLAN ID matching in local authentication.*
4. Authentication succeeds if the MAC address is registered in the internal MAC-based authentication DB.
5. The terminal (printer in the figure) can now communicate with the servers belonging to the connected VLAN.

Local authentication can be based on the MAC address only, or on a combination of MAC address and VLAN ID. You can use the `mac-authentication vlan-check` configuration command to specify which method the Switch uses.

A combination of the MAC address and MAC mask can be registered in the internal MAC-based authentication DB. The table below summarizes the priorities for matching. The authentication database also allows the registration of entries having only MAC addresses as well as entries having combinations of MAC addresses and MAC masks.

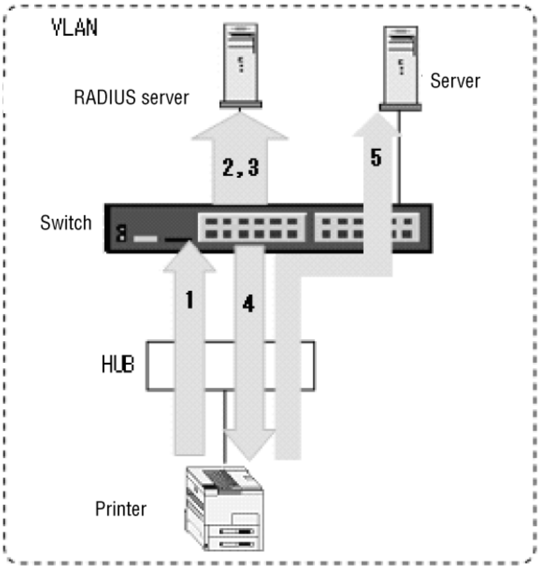
Table 10-3 VLAN ID matching in local authentication

Configuration mac-authentication vlan-check	**VLAN ID configured in internal MAC-based authentication DB ((1) and (2) indicate the priority)**	
	Yes	**No**
Yes	(1) Matches MAC address and VLAN ID (2) Matches MAC address, MAC mask, and VLAN ID	(1) Matches MAC address only (2) Matches MAC address and MAC mask
No	(1) Matches MAC address only (2) Matches MAC address and MAC mask	(1) Matches MAC address only (2) Matches MAC address and MAC mask

(2) Switch default: RADIUS authentication

In RADIUS authentication, the Switch submits the source MAC address of a frame received from a terminal to an external RADIUS server for authentication. When the source MAC address matches an entry in the server, authentication is successful, and the terminal is allowed to access the network.

Figure 10-2 Fixed VLAN mode (RADIUS authentication method)



1. The Switch receives a frame from a terminal (the printer in the figure) connected via a hub.
2. The VLAN ID of the terminal (the printer in the figure) to be authenticated is determined from a connection port or VLAN ID of the terminal to be authenticated.
3. An authentication request is issued to the external RADIUS server by sending a user ID (terminal MAC address), password (terminal MAC address or password), and VLAN ID.
4. A response indicating successful authentication is received from the RADIUS server.
5. The terminal (printer in the figure) can now communicate with the servers belonging to the connected VLAN.

RADIUS authentication can be based on the MAC address only, or on a combination of MAC address and VLAN ID. You can use the `mac-authentication vlan-check` configuration command to specify which method the Switch uses.

The following table describes the conditions for performing RADIUS authentication based on a combination of MAC address and VLAN ID.

Table 10-4 VLAN ID matching in RADIUS authentication

Configuration mac-authentication vlan-check	**Behavior**
Yes	Matches MAC address and VLAN ID
No	Matches MAC address only

The format of the MAC address to be used for RADIUS authentication can be defined by using the `mac-authentication id-format` configuration command.

In addition, the password to be used for issuing an authentication request to the RADIUS server can be set by using the `mac-authentication password` configuration command. If the `mac-authentication password` command is not set, the MAC address of the terminal to be authenticated can be used as the password.

For details, see *(c) MAC address format and password at authentication request in fixed VLAN mode* in *(2) Preparing the RADIUS server* in *10.6.2 RADIUS authentication.*

(3) Authentication method list

You can use the port-based authentication method for MAC-based authentication. For details about operations in port-based authentication, see *5.2.2 Authentication method list.*

10.2.2 Authentication functionality

(1) Trigger for authentication

In fixed VLAN mode, authentication starts for all the frames received by the Switch from the ports specified for MAC-based authentication fixed VLAN mode.

The target ports in the MAC-based authentication fixed VLAN mode can be set to target Ethernet ports by using the `mac-authentication port` configuration command.

(2) Restricting MAC addresses to be authenticated

In MAC-based authentication, a MAC access list is used to specify a specific range of MAC addresses as the target for MAC-based authentication.

- Valid MAC access list parameters

  Specified contents of the source MAC address and source mask.(Optional information such as a destination MAC address is not valid.)

- Handling of MAC addresses matching the MAC access list permit condition

  The device with the matching MAC address is handled as an authentication target, and authentication is performed.

- Handling of MAC addresses matching the MAC access list deny condition

  The device with the matching MAC address is not handled as an authentication target, and authentication is not performed.

In addition, when there is no MAC address list ID specified by the `mac-authentication access-group` configuration command, no restriction is imposed on the MAC addresses, and all MAC addresses are subject to authentication.

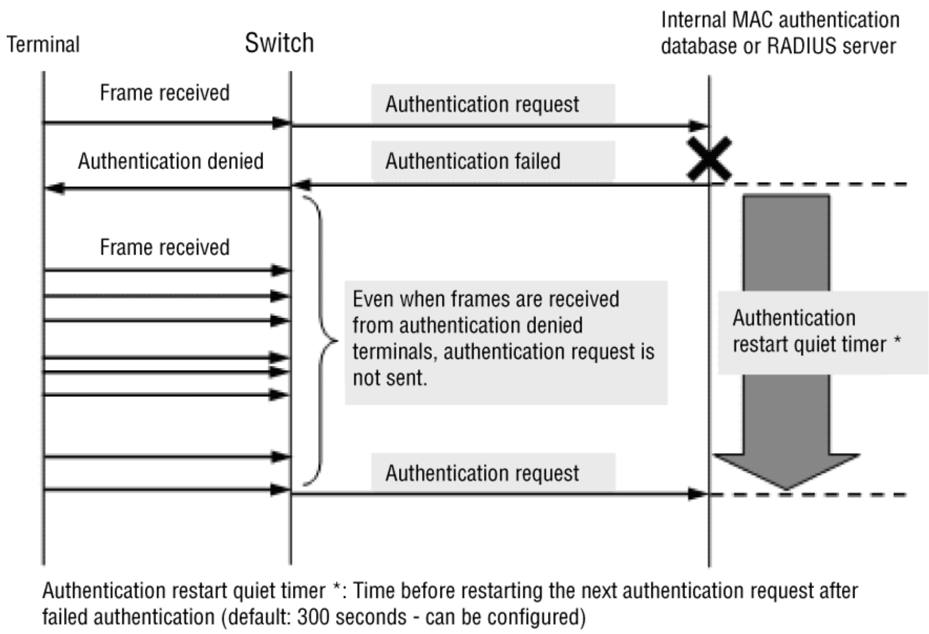
(3) Re-authentication delay timer

MAC-based authentication allows a re-authentication delay timer to be set.

This functionality reduces the number of re-authentication attempts when frames are repeatedly received from a terminal that was denied authentication.

If a frame is received within the re-authentication delay timer time interval (300 seconds by default) from a terminal that was denied authentication, authenticated is not performed.

Figure 10-3 Overview of authentication restart delay timer



In addition, this functionality prevents unnecessary collection of the MAC-based authentication error log when MAC-based authentication and IEEE 802.1X or Web authentication are operating on the same port.

In a configuration where multiple authentication methods operate on the same port, terminals scheduled for IEEE 802.1X or Web authentication are also subject to MAC-based authentication, so authentication requests are unnecessarily processed, and the MAC-based authentication error log is unnecessarily collected.

For this reason, if a terminal is successfully authenticated by some other authentication method during a re-authentication delay timer interval, no MAC-based authentication error log is collected for the terminal. The MAC-based authentication error log is collected only when the re-authentication delay timer expires and the terminal is not successfully authenticated by the other authentication method.

The use of authentication MAC address restrictions and the re-authentication delay timer makes it possible to reduce the chances for unnecessary authentication request processing and MAC-based authentication error log collection.

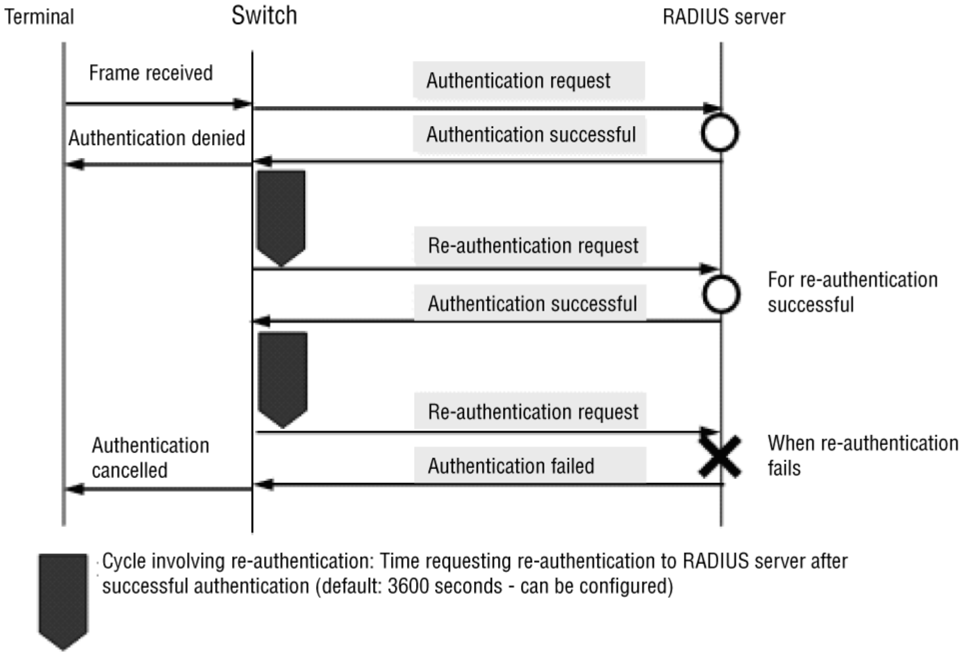
The `mac-authentication timeout quiet-period` configuration command can be used to disable the re-authentication delay timer or change its timer value.

(4) Periodic re-authentication request

After successful authentication, a re-authentication request must be issued to the RADIUS server within a certain period of time (3,600 seconds by default) to reflect the configuration information of the RADIUS server.

When a periodic re-authentication request results in successful authentication, the authentication status continues. Otherwise, the authentication of the target terminal is forcibly canceled.

Figure 10-4 Overview of a periodic re-authentication request to the RADIUS server



The re-authentication cycle can be configured by using the `mac-authentication timeout reauth-period` configuration command.

(5) Specifying a forced authentication port

When a terminal connected to a port for which forced authentication is specified undergoes RADIUS authentication, and sending a request to the RADIUS server fails due to a line failure or the RADIUS does not respond, the terminal becomes authenticated.

In the Switch, the configuration for forced authentication can be shared among all authentication methods or be specified separately per authentication method. For details about shared authentication configuration, see *5.4.6 Forced authentication common to all authentication modes.*

The port subject to forced authentication is configured by using the `mac-authentication static-vlan force-authorized` configuration command.

Forced authentication is successful when the following conditions are met.

Table 10-5 Conditions for successful forced authentication

Item	Condition
Configuration	All the following configurations have been set: ● `aaa authentication mac-authentication`#1 ● `mac-authentication radius-server host` or `radius-server host` ● `mac-authentication system-auth-control` ● `mac-authentication port`#2 ● `mac-authentication static-vlan force-authorized`#2 ● `mac-authentication authentication`#3

Item	Condition
Accounting log	The following accounting log is collected when an authentication request is sent to the RADIUS server: `No=21` `NOTICE:LOGIN: (`*<Additional information>*`) Login failed ; Failed to connection to RADIUS server.` *<Additional information>*`: MAC, PORT, VLAN` The accounting log data can be confirmed by using the `show mac-authentication logging` operation command.

#1

When using forced authentication by Switch default, set only `default group radius`.

When using port-based authentication, set *<list-name>* `group` *<group-name>*.

#2

Specify the same Ethernet port.

#3

Specify this when using port-based authentication.

The authentication status of a terminal where authentication is permitted by forced authentication is canceled in the same way as for a normally authenticated terminal, as described in *(7) Authentication cancellation* in *10.2.2 Authentication functionality.*

Furthermore, all operations from the start of requesting authentication to the RADIUS server to successful forced authentication are the same for shared forced authentication and per-authentication-method forced authentication. For details about the operations, see *(1) Behavior from the start of an RADIUS authentication request to permission for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

(6) Maximum number of authenticated terminals

The maximum number of authentication terminals can be specified per Switch and per port. The maximum number of authentication terminals (up to 1,024) can be specified by using the `mac-authentication static-vlan max-user` configuration command.

Though the maximum number of authentication terminals can be specified per Switch and per port simultaneously, if either limit is reached, no more terminals can be authenticated.

Also, if the maximum number of authentication terminals is changed to a value lower than the number of currently authenticated terminals, the currently authenticated terminals can continue communication, but no more terminals can be authenticated.

(7) Authentication cancellation

Fixed VLAN mode provides the following authentication cancellation methods:

- Canceling authentication when the maximum connection time is exceeded
- Canceling authentication by monitoring the non-communication state of authenticated terminals

- Canceling authentication of terminals connected to link-down ports
- Canceling authentication resulting from changes to the VLAN configuration
- Canceling authentication using an operation command

(a) Canceling authentication when the maximum connection time is exceeded

The maximum connection time is monitored per authenticated terminal (by MAC address) starting from successful terminal authentication, and authentication of a terminal is automatically canceled when the maximum connection time is exceeded.

The maximum connection time can be configured by using the `mac-authentication max-timer` configuration command.

(b) Canceling authentication by monitoring the non-communication state of authenticated terminals

This functionality automatically cancels authentication of an authenticated terminal if the terminal remains in a non-communication status for a certain period of time.

Also, the MAC-based authentication entry of the MAC address table is periodically monitored (at approximately one-minute intervals) to confirm whether frames are being received from each authenticated terminal. If no frame is received from a target terminal for a certain period of time#, the target MAC-based authentication entry is deleted from the MAC address table, and the terminal authentication is canceled.

#

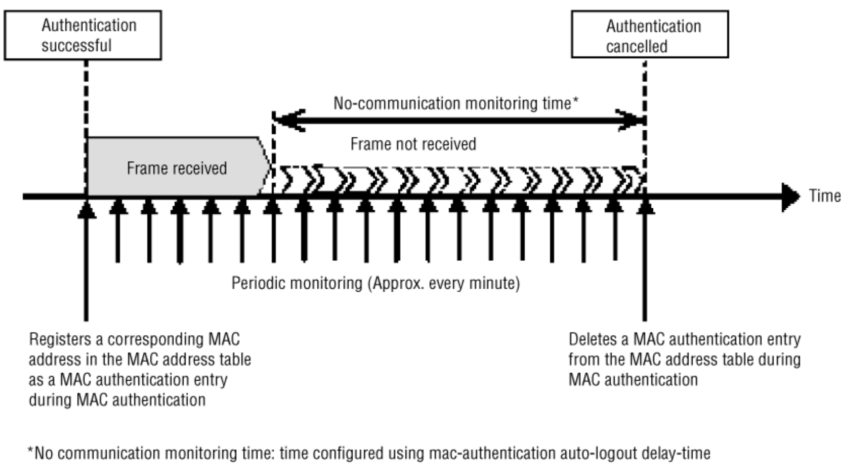
Configured by using the `mac-authentication auto-logout` configuration command

(`delay-time`: 3,600 seconds by default)

The non-communication monitoring time can be changed or disabled by using the `mac-authentication auto-logout` configuration command.

Note that if the non-communication monitoring time (`delay-time`) is set to `0`, the default value (3,600 seconds) is used.

Figure 10-5 Overview of non-communication monitoring of authenticated terminals



Non-communication monitoring is enabled for authenticated terminals when the following condition is met:

- The MAC-based authentication fixed VLAN mode or dynamic VLAN mode is in effect and `mac-authentication auto-logout` is enabled.

If the `no mac-authentication auto-logout` configuration command is set, terminal authenticaton is not canceled.

(c) Canceling authentication of terminals connected to link-down ports

When a link-down is detected on a port for which the `mac-authentication port` configuration command is set, the authentication of the authenticated terminal in the MAC-based authentication fixed VLAN mode of the port is automatically canceled.

(d) Canceling authentication resulting from changes to the VLAN configuration

If you use configuration commands to change the configuration of a VLAN that includes authenticated terminals, the Switch cancels the authentication status of terminals associated with that VLAN.

The following configuration changes trigger a logout:

- Deletion of a VLAN
- Suspension of a VLAN

(e) Canceling authentication using an operation command

You can manually cancel the authentication of some or all MAC-authenticated terminals by using the `clear mac-authentication auth-state` operation command.

(8) Roaming (moving authenticated terminals between ports)

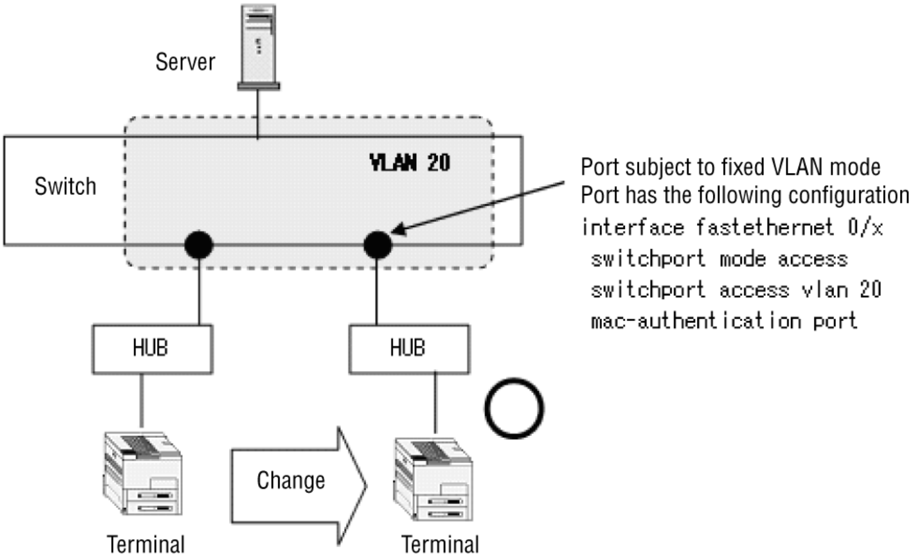
If an authenticated terminal (the printer in the figure below) connected via a hub is moved among ports without a link-down occurring, the terminal is still authenticated can continue communication.

Roaming operates when the following conditions are met:

- The `mac-authentication static-vlan roaming` configuration command is set.
- Ports for fixed VLAN mode before and after moving
- The same VLAN before and after moving

If terminal movement among ports is detected while the above conditions are not met, authentication of the target terminal is forcibly canceled.

Figure 10-6 Overview of roaming in fixed VLAN mode



10.3 Dynamic VLAN mode

Prior to authentication, a terminal cannot start communication until it is successfully authenticated. If authentication succedds in dynamic VLAN mode, the MAC address of the terminal and the post-authentication VLAN ID are registered in the MAC VLAN and the MAC address table as a MAC-based authentication entry, enabling the terminal to communicate on the post-authentication VLAN. (Entries registered in the MAC address table can be confirmed by using the `show mac-address-table` operation command.)

10.3.1 Authentication method group

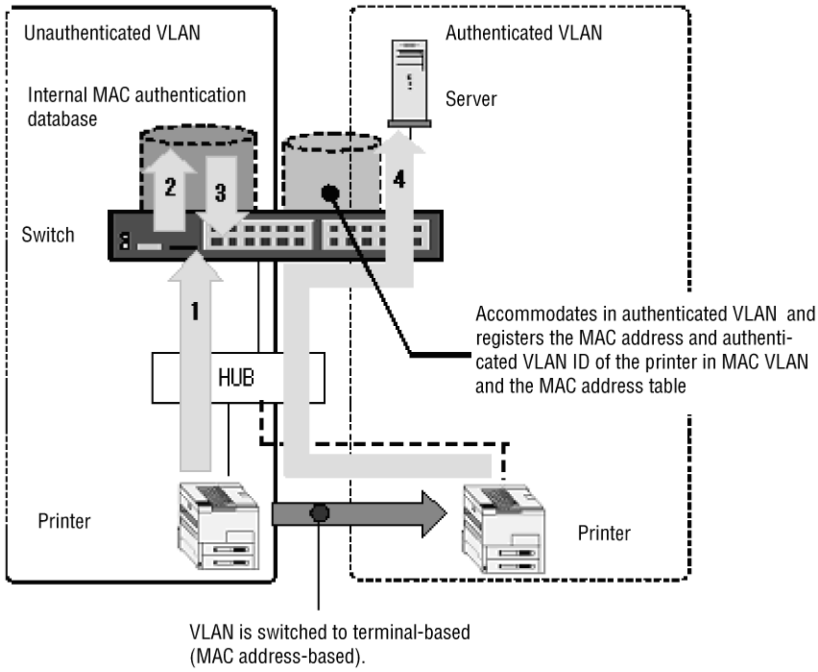
In the MAC-based authentication method group, the Switch default is used in common for all MAC-based authentication modes, and an authentication method list is used in both fixed VLAN mode and dynamic VLAN mode. For details, see the following sections:

- *5.1.3 Authentication method groups*
- *5.3.3 Priority configuration for the Switch default local and RADIUS authentications*
- *5.2.2 Authentication method list*
- *5.3.1 RADIUS server information used with the Layer 2 authentication method*
- *11.2.1 Configuring the authentication method group and RADIUS server information*

(1) Switch default: local authentication

The source MAC address of a frame received from a terminal is compared with the MAC addresses in the internal MAC-based authentication DB. If the source MAC address matches an entry in the database, authentication is successful. The terminal gains membership to the VLAN registered in the internal MAC-based authentication DB, and communication becomes possible.

Figure 10-7 Dynamic VLAN mode (local authentication)



1. The Switch receives a frame from a terminal (the printer in the figure) connected via a hub.
2. The MAC address of the received frame is compared with those in the internal MAC-based authentication DB of the Switch.
3. If the MAC address matches on in the database, the VLAN to which the terminal will become a member is determined according to the VLAN registered in the internal MAC-based authentication DB.
4. The terminal (the printer in the figure) gains membership to the VLAN (post-authentication VLAN) registered in the internal MAC-based authentication DB, and then the terminal is allowed to communicate with the servers that belong to the post-authentication VLAN. In addition, the MAC address and VLAN ID of the authenticated terminal are registered in the MAC VLAN and MAC address table.

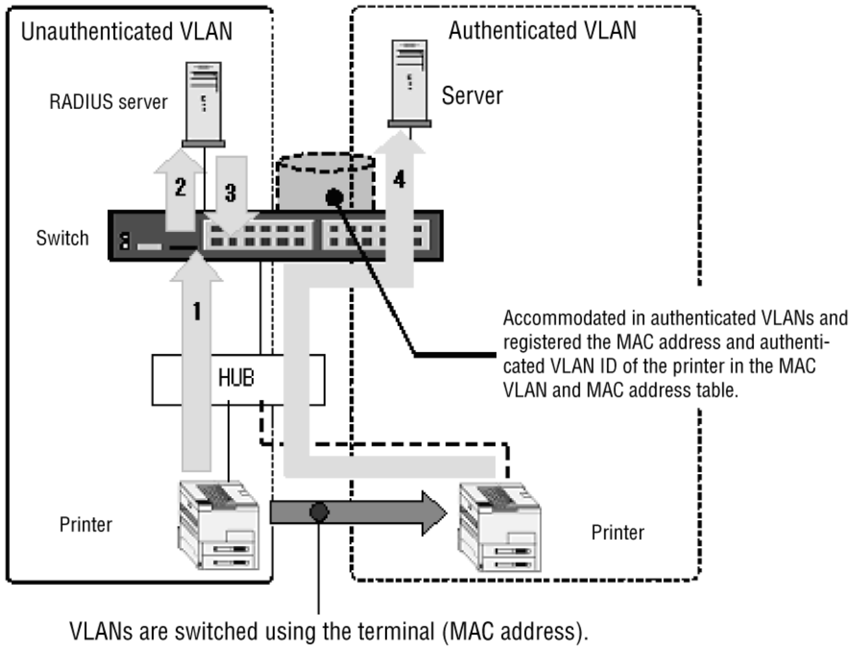
(a) Switching accommodation VLANs

For details, see *5.4.3 Auto VLAN assignment for a MAC VLAN* and *5.4.4 Auto authentication mode accommodation on the same MAC port*.

(2) Switch default: RADIUS authentication

In RADIUS authentication, an authentication request is sent to an external RADIUS server by using the source MAC address of frames sent from a terminal. If authentication is successful, in the terminal gains membership to the specified post-authentication VLAN, and communication becomes possible.

Figure 10-8 Dynamic VLAN mode (RADIUS authentication)



1. The Switch receives a frame from a terminal (the printer in the figure) connected via a hub.
2. An authentication request is issued to an external RADIUS server by sending a user ID (terminal MAC address) and a password (terminal MAC address or password).
3. If authentication is successful, VLAN information from the RADIUS server is received.
4. The terminal (the printer in the figure) gains membership to the VLAN (post-authentication VLAN) received from the RADIUS server and is allowed to communicate with the terminals that belong to the post-authentication VLAN. In addition, the MAC address and VLAN ID of the authenticated terminal are registered in the MAC VLAN and MAC address table.

(a) Switching accommodation VLANs

For details, see *5.4.3 Auto VLAN assignment for a MAC VLAN* and *5.4.4 Auto authentication mode accommodation on the same MAC port.*

(3) Authentication method list

You can use the port-based authentication method for MAC-based authentication.

For details about operations in port-based authentication, see *5.2.2 Authentication method list.*

10.3.2 Authentication functionality

(1) Trigger for authentication

In dynamic VLAN mode, all frames received by the Switch via the port subject to the MAC-based authentication dynamic VLAN mode become triggers that start authentication.

The port subject to the MAC-based authentication dynamic VLAN mode is set to the target Ethernet port by the `mac-authentication port` configuration command. In addition, the type of the target Ethernet port (`switchport mode` configuration command) must be set to the MAC port in advance.

(2) Restricting MAC addresses to be authenticated

Configuration is the same as for fixed VLAN mode. For details, see *(2) Restricting MAC addresses to be authenticated* in *10.2.2 Authentication functionality.*

(3) Re-authentication delay timer

This function works the same as in fixed VLAN mode. For details, see *(3) Re-authentication delay timer* in *10.2.2 Authentication functionality.*

(4) Periodic re-authentication request

Configuration is the same as in fixed VLAN mode. For details, see *(4) Periodic re-authentication request* in *10.2.2 Authentication functionality.*

(5) Specifying a forced authentication port

When a terminal connected to a port for which forced authentication is specified undergoes RADIUS authentication, and sending a request to the RADIUS server fails due to a line failure or the RADIUS does not respond, the terminal becomes authenticated.

In the Switch, the configuration for forced authentication can be shared among all authentication methods or be specified separately per authentication method. For details about shared authentication configuration, see *5.4.6 Forced authentication common to all authentication modes.*

The port subject to forced authentication is configured by using the `mac-authentication force-authorized vlan` configuration command.

Forced authentication is successful when the following conditions are met.

Table 10-6 Conditions for successful forced authentication

Item	Condition
Configuration	All the following configurations have been set: ● `aaa authentication mac-authentication`#1 ● `mac-authentication radius-server host` or `radius-server host` ● `mac-authentication system-auth-control` ● `vlan` *<VLAN ID list>* `mac-based`#2 ● `mac-authentication force-authorized vlan`#2, #3 ● `mac-authentication port`#3 ● `switchport mode mac-vlan`#3 ● `mac-authentication authentication`#4
Accounting log	The following accounting log is collected when an authentication request is sent to the RADIUS server: `No=21` `NOTICE:LOGIN: (`*<Additional information>*`) Login failed ; Failed to connection to RADIUS server.` *<Additional information>*`: MAC, PORT, VLAN` The accounting log data can be confirmed by using the `show`

Item	Condition
	`mac-authentication logging` operation command.

#1

When using forced authentication by Switch default, set only `default group radius`.

When using port-based authentication, set *<list-name>* `group` *<group-name>*.

#2

Set the same VLAN.

#3

Set the same Ethernet port.

#4

Set this when using port-based authentication.

The authentication status of a terminal where authentication is permitted by forced authentication is canceled in the same way as for a normally authenticated terminal, as described in *(7) Authentication cancellation* in *10.3.2 Authentication functionality.*

Furthermore, all operations from the start of requesting authentication to the RADIUS server to successful forced authentication are the same for shared forced authentication and per-authentication-method forced authentication. For details about the operations, see *(1) Behavior from the start of an RADIUS authentication request to permission for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

(6) Maximum number of authenticated terminals

The maximum number of authentication terminals can be specified per Switch and per port. The maximum number of authentication terminals (up to 256) can be specified by using the `mac-authentication max-user` configuration command.

Though the maximum number of authentication terminals can be specified per Switch and per port simultaneously, if either limit is reached, no more terminals can be authenticated.

Also, if the maximum number of authentication terminals is changed to a value lower than the number of currently authenticated terminals, the currently authenticated terminals can continue communication, but no more terminals can be authenticated.

(7) Authentication cancellation

Dynamic VLAN mode provides the following authentication cancellation methods:

- Canceling authentication when the maximum connection time is exceeded
- Canceling authentication by monitoring the non-communication state of authenticated terminals
- Cancling the authentication of terminals connected to link-down ports

- Canceling authentication resulting from changes to the VLAN configuration
- Canceling authentication using an operation command

Each authentication cancellation method operates the same as those for fixed VLAN mode. For details, see *(7) Authentication cancellation* in *10.2.2 Authentication functionality.*

(8) Roaming (moving authenticated terminals between ports)

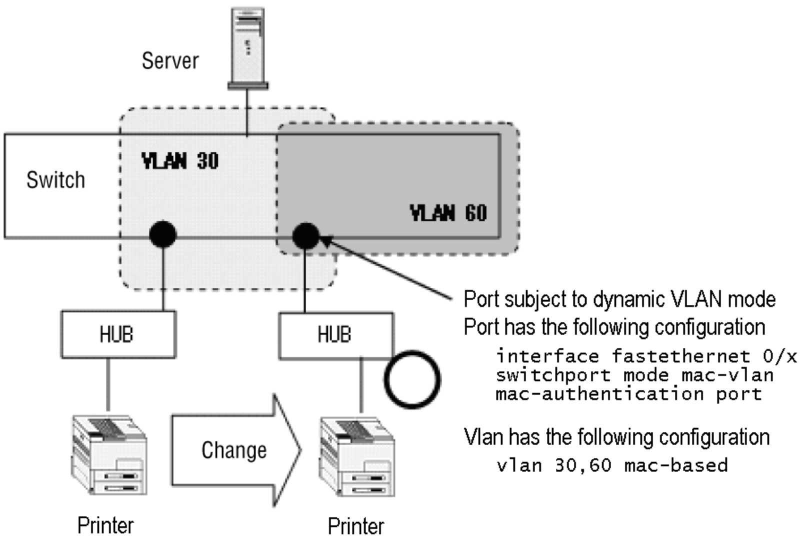
If an authenticated terminal (the printer in the figure below) connected via a hub is moved among ports without a link-down occurring, the terminal is still authenticated can continue communication.

Roaming operates when the following conditions are met:

- The `mac-authentication roaming` configuration command is set.
- Ports for dynamic VLAN mode before and after moving

If terminal movement among ports is detected while the above conditions are not met, authentication of the target terminal is forcibly canceled.

Figure 10-9 Roaming in dynamic VLAN mode



10.4 Legacy mode

10.4.1 Authentication method group

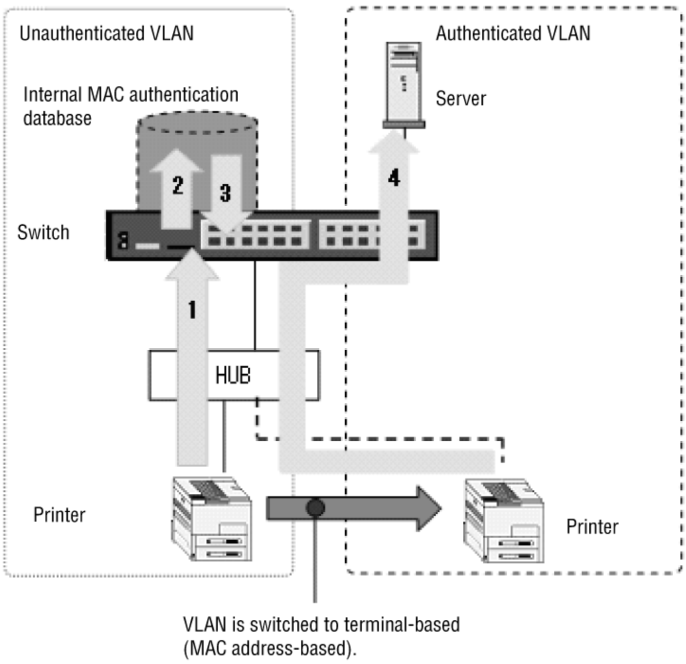
A MAC-based authentication method group uses the Switch default for all the MAC-based authentication modes (legacy mode does not use an authentication methods list). For details, see the following sections:

- *5.1.3 Authentication method groups*
- *5.3.3 Priority configuration for the Switch default local and RADIUS authentications*
- *5.3.1 RADIUS server information used with the Layer 2 authentication method*
- *11.2.1 Configuring the authentication method group and RADIUS server information*

(1) Switch default: local authentication

The source MAC address of a frame received from a terminal is compared with the MAC addresses in the internal MAC-based authentication DB. If the source MAC address matches an entry in the database, authentication is successful. The terminal gains membership to the VLAN registered in the internal MAC-based authentication DB, and communication becomes possible.

Figure 10-10 Legacy mode (local authentication)



1. The Switch receives a frame from a terminal (the printer in the figure) connected via a hub.
2. The MAC address of the received frame is compared with those in the

internal MAC-based authentication DB of the Switch.

3. If the MAC address matches on in the database, the VLAN to which the terminal will become a member is determined according to the VLAN registered in the internal MAC-based authentication DB.
4. The terminal (the printer in the figure) gains membership to the VLAN (post-authentication VLAN) registered in the internal MAC-based authentication DB, and then the terminal is allowed to communicate with the servers that belong to the post-authentication VLAN.

(a) Switching accommodation VLANs

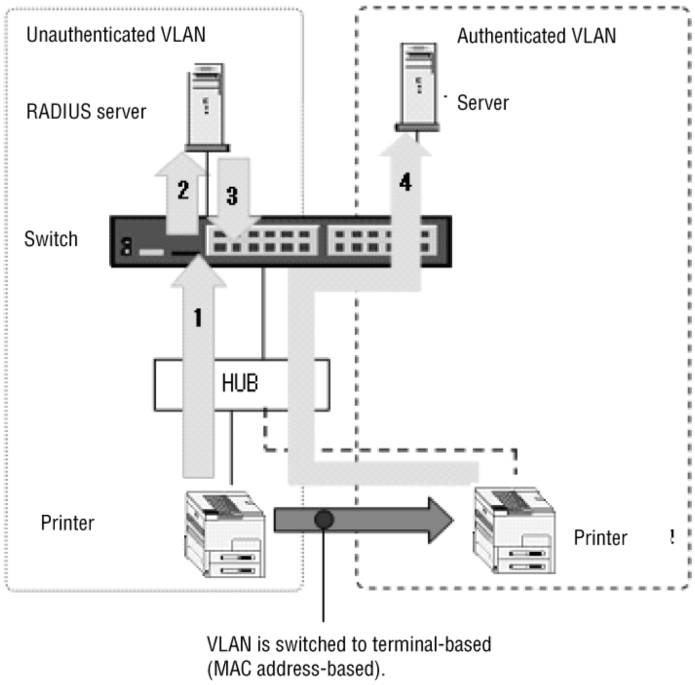
Authentication fails after legacy mode authentication is performed if the VLAN ID registered for the entry of the target MAC address in the internal MAC-based authentication DB has not been included in the post-authentication VLAN configuration (`mac-authentication vlan` configuration command).

Authentication also fails if no VLAN information has been registered for the entry of the target MAC address in the internal MAC-based authentication DB.

(2) Switch default: RADIUS authentication

In RADIUS authentication, an authentication request is sent to an external RADIUS server by using the source MAC address of frames sent from a terminal. If authentication is successful, in the terminal gains membership to the specified post-authentication VLAN, and communication becomes possible.

Figure 10-11 Legacy mode (RADIUS authentication)



1. The Switch receives a frame from a terminal (the printer in the figure) connected via a hub.
2. An authentication request is issued to an external RADIUS server by sending a user ID (terminal MAC address) and a password (terminal MAC address or

password).

3. If authentication is successful, VLAN information from the RADIUS server is received.

4. The terminal (the printer in the figure) gains membership to the VLAN (post-authentication VLAN) received from the RADIUS server and is allowed to communicate with the terminals that belong to the post-authentication VLAN.

(a) Switching accommodation VLANs

Authentication fails after legacy mode authentication is performed if the VLAN ID registered for the entry of the target MAC address in the internal MAC-based authentication DB has not been included in the post-authentication VLAN configuration (`mac-authentication vlan` configuration command).

10.4.2 Authentication functionality

(1) Trigger for authentication

In legacy mode, all frames received by the Switch from the port that is a member of the MAC VLAN, and from the native VLAN of the port specified to be subject to the MAC-based authentication legacy mode are triggers to start authentication.

All frames are subject to authentication regardless of whether they are MAC unicast, MAC broadcast, or MAC multicast frames.

For this reason, if terminals in the native VLAN of the MAC VLAN attempt to communicate with each other, communication data among all terminals are frames subject to MAC-based authentication, and MAC-based authentication is performed. To cope with this, it is essential to ensure the proper settings and operations by restricting MAC addresses subject to authentication or using similar functionality.

In MAC-based authentication, the need for special settings and authentication procedures is eliminated by simply connecting the target terminal to the Switch directly or via another Switch. However, note that MAC-based authentication is never started unless a frame is sent from the target MAC terminal.

The authentication port in legacy mode differs from that in fixed VLAN mode and dynamic VLAN mode. An Ethernet port number is specified per Switch rather than per port for legacy mode operation.

This port number for legacy mode operation can be set by using the `mac-authentication interface` command.

(2) Restricting MAC addresses to be authenticated

This functionality works the same as in fixed VLAN mode. For detail see *(2) Restricting MAC addresses to be authenticated* in *10.2.2 Authentication functionality.*

(3) Re-authentication delay timer

This functionality works the same as in fixed VLAN mode. For details, see *(3) Re-authentication delay timer* in *10.2.2 Authentication functionality.*

(4) Periodic re-authentication request

This functionality works the same as for fixed VLAN mode. For details, see *(4) Periodic re-authentication request* in *10.2.2 Authentication functionality.*

(5) Specifying a forced authentication port

When a terminal connected to a port for which forced authentication is specified undergoes RADIUS authentication, and sending a request to the RADIUS server fails due to a line failure or the RADIUS does not respond, the terminal becomes authenticated.

In the Switch, the configuration for forced authentication can be shared among all authentication methods or be specified separately per authentication method. However, legacy mode does not operate when the configuration for forced authentication is shared among all authentication modes. In this case, be sure to use the forced authentication functionality for MAC-based authentication.

The port subject to forced authentication is configured by using the `mac-authentication force-authorized vlan` configuration command.

Forced authentication is successful when the following conditions are met.

Table 10-7 Conditions for successful forced authentication

Item	Condition
Configuration	All the following configurations have been set: ● `aaa authentication mac-authentication`#1 ● `mac-authentication radius-server host` or `radius-server host` ● `mac-authentication system-auth-control` ● `mac-authentication vlan`#2 ● `vlan` <*VLAN ID list*> `mac-based`#2 ● `mac-authentication force-authorized vlan`#2, #3 ● `switchport mac vlan`#2, #3 ● `switchport mode mac-vlan`#3 ● `mac-authentication interface`#4
Accounting log	The following accounting log is collected when an authentication request is sent to the RADIUS server: `No=21` `NOTICE:LOGIN: (`<*Additional information*>`) Login failed ; Failed to connection to RADIUS server.` <*Additional information*>`:MAC, PORT, VLAN` The accounting log data can be confirmed by using the `show mac-authentication logging` operation command.

#1

When using forced authentication by Switch default, set only `default group radius`.

#2

Set the same VLAN ID for commands marked #3.

#3

Specify the same Ethernet port.

#4

Specify an Ethernet port number for which the command in #3 has been set.

The authentication status of a terminal where authentication is permitted by forced authentication is canceled in the same way as for a normally authenticated terminal, as described in *(7) Authentication cancellation* in *10.4.2 Authentication functionality.*

Furthermore, all operations from the start of requesting authentication to the RADIUS server to successful forced authentication are the same for shared forced authentication and per-authentication-method forced authentication. For details about the operations, see *(1) Behavior from the start of an RADIUS authentication request to permission for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

(6) Maximum number of authenticated terminals

The maximum number of authentication terminals can be specified per Switch and per port. The maximum number of authentication terminals (up to 256) can be specified by using the `mac-authentication max-user` configuration command.

Though the maximum number of authentication terminals can be specified per Switch and per port simultaneously, if either limit is reached, no more terminals can be authenticated.

Also, if the maximum number of authentication terminals is changed to a value lower than the number of currently authenticated terminals, the currently authenticated terminals can continue communication, but no more terminals can be authenticated.

(7) Authentication cancellation

Legacy mode provides the following authentication cancellation methods:

- Canceling authentication when the maximum connection time is exceeded
- Canceling authentication by monitoring the aging of the MAC address table
- Canceling authentication resulting from changes to the VLAN configuration
- Canceling authentication using an operation command

With the exception of "Canceling authentication by monitoring the aging of the MAC address table", each authentication cancellation method operates the same as those for fixed VLAN mode. See *(7) Authentication cancellation* in *10.2.2 Authentication functionality.*

(a) Canceling authentication by monitoring the aging of the MAC address table

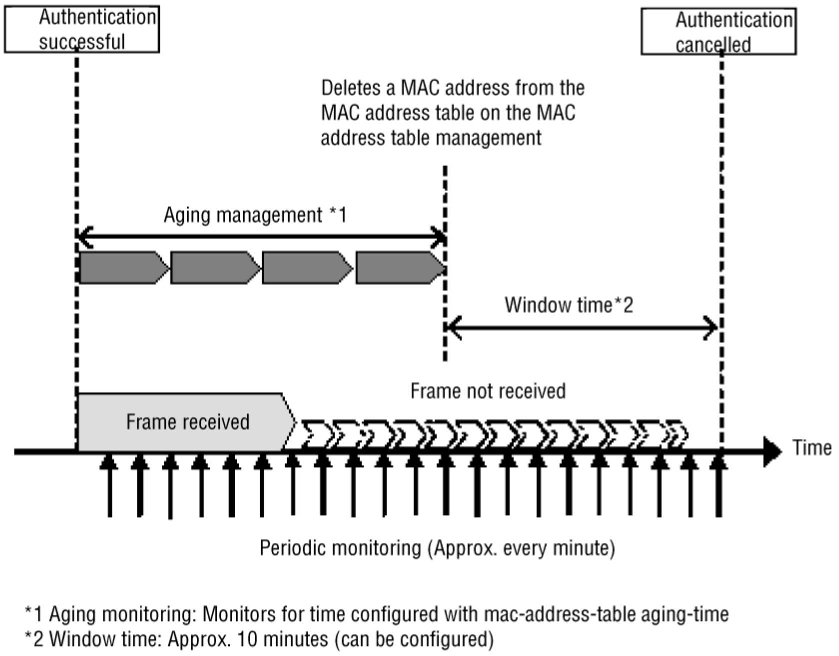
Dynamic entries in the MAC address table are periodically monitored (at approximately one-minute intervals) for whether the MAC address of the terminal registered with a post-authentication VLAN ID in legacy mode has aged.

The MAC address aging time in legacy mode differs from that in fixed VLAN mode and dynamic VLAN mode, and conforms to the setting of the `mac-address-table aging-time` configuration command. After a target MAC address is deleted due to aging timeout as specified by `mac-address-table aging-time`, if the MAC address is still deleted after the delay time specified by the `mac-authentication auto-logout` configuration command (delay-time: 3,600 seconds by default), authentication is automatically canceled.

The delay time after aging timeout can be changed or disabled by using the `mac-authentication auto-logout` configuration command.

In addition, if the delay time (`delay-time`) is set to `0`, authentication is canceled immediately after the target MAC address is deleted due to aging timeout.

Figure 10-12 Overview of MAC address table aging of authenticated terminals in legacy mode



(8) Moving authenticated terminals among ports and displaying the number of authenticated terminals

No roaming configurations are supported in legacy mode. If an attempt is made to move an authenticated terminal to another port, the following operations are performed:

1. After a terminal is authenticated successfully, it is counted towards the number of authentication terminals on the port at which it was authenticated.
2. If a terminal authenticated in legacy mode is moved to another port, it is allowed to continue communication as long as all of the following conditions are met:
   - The ports before and after the move are ports subject to legacy mode.
   - Post-authentication VLAN before moving has been specified by the `switchport mac vlan` configuration command.

   The moved terminal is allowed to continue communication until it is detected by monitoring of MAC address table aging. However, if DHCP snooping and filters are in use at the port after the move, whether communication can continue depends upon their conditions.

   If a terminal is moved while the above conditions are not met, its authentication is canceled. However, if a terminal authenticated in legacy mode is moved to a port not subject to authentication, the terminal authentication might not be canceled.
3. The movement of a terminal to another port is detected when the next re-authentication is performed.
4. If the port after the move is subject to legacy mode authentication, the number of authenticated terminals is counted as follows:

- If the number of authenticated terminals is less than the maximum, the number of authenticated terminals at the port prior to the move is subtracted, and terminal authentication and registration is performed at the port after the move.
- If the number of authenticated terminals is equal to or greater than the maximum, the number of authenticated terminals at the port prior to the move is subtracted, and terminal authentication is canceled.

5. If the loss of a MAC address at the port before the move is detected by monitoring of MAC address table aging before the next time authentication is performed, the terminal is authenticated at the port after the move as a new terminal.

10.5 Accounting functionality

The Switch uses the following accounting functionality to record the results of MAC-based authentication operations:

- Internal accounting log of the Switch
- Recording information to the RADIUS server accounting functionality
- Recording authentication information to the RADIUS server
- Outputting accounting log information to the syslog server

(1) Internal accounting log of the Switch

Operation log information, including MAC-based authentication results and operation information, is recorded in the internal accounting log of the Switch.

The internal accounting log of the Switch can log a maximum of 2,100 lines total for all the MAC-based authentication modes. When the maximum number of 2,100 lines is exceeded, the oldest lines are deleted, and the newest accounting log information is added.

The following table lists the accounting log information that is recorded.

Table 10-8 Accounting log entry types

Accounting log entry type	Description
LOGIN	Information (success or failure) relating to an authentication operation
LOGOUT	Information (reason, etc.) relating to authentication cancellation operation
SYSTEM	Information relating to operation of MAC-based authentication functionality (including roaming detection and forced authentication)

Table 10-9 Information output to the internal accounting log of the Switch

Accounting log type		Time	MAC	VLAN	PORT	Message
LOGIN	Succeeded	Y	Y	Y#	Y	Authentication success message
	Failed	Y	Y	Y#	Y#	Authentication failure reason message
LOGOUT		Y	Y	Y#	Y	Authentication cancellation message
SYSTEM		Y	Y	Y#	Y#	Message relating to MAC-based authentication functionality operation

Legend:

Y: Message output

N: No message output

#

Some messages might not be output.

For details about the messages, see *show mac-authentication logging* in *27. MAC-based Authentication* in the manual *Operation Command Reference*.

In addition, the following lists the output functionality of the accounting logs:

1. Console display per event

   Even when the `trace-monitor enable` operation command has been set, accounting log information is not output to the console each time an event occurs.

2. Operation command display

   By using the `show mac-authentication logging` operation command, you can display the collected accounting log entries in chronological order starting from the latest one.

3. Output to the syslog server

   For details, see *(4) Outputting accounting log information to the syslog server.*

4. Private traps

   The Switch supports functionality that issues private traps, which is triggered by the accounting log collected when a specific even of MAC-based authentication occurs. Use configuration commands to specify whether traps are issued and also the type of traps that are issued.

Table 10-10 Accounting log entries(LOGIN/LOGOUT) and conditions for issuing private traps (1)

Accounting log entry type		Configuration required for issuing private traps	
		Command	**Parameter**
LOGIN	Succeeded	`snmp-server host`	`mac-authentication`
		`snmp-server traps`	`mac-authentication-trap all`
	Failed	`snmp-server host`	`mac-authentication`
		Not configured, or one of the following configured:	
		`snmp-server traps`	`mac-authentication-trap all`
		`snmp-server traps`	`mac-authentication-trap failure`
LOGOUT		`snmp-server host`	`mac-authentication`
		`snmp-server traps`	`mac-authentication-trap all`

Table 10-11 Accounting log entry (SYSTEM) and conditions for issuing private traps (2)

Accounting log entry type: SYSTEM	**Authentication mode**	**Configuration required for issuing private traps**	
		Command	**Parameter**
Forced authentication	Fixed VLAN	`snmp-server host`	`mac-authentication`
		`mac-authentication static-vlan force-authorized`	`action trap`
	Dynamic VLAN	`snmp-server host`	`mac-authentication`
		`mac-authentication force-authorized vlan`	`action trap`
	Legacy	`snmp-server host`	`mac-authentication`
		`mac-authentication force-authorized vlan`	`action trap`
Roaming	Fixed VLAN	`snmp-server host`	`mac-authentication`
		`mac-authentication static-vlan roaming`	`action trap`
	Dynamic VLAN	`snmp-server host`	`mac-authentication`
		`mac-authentication roaming`	`action trap`
	Legacy	-- (There is no configuration because this mode is not supported.)	

A forced authentication private trap can also be issued when the configuration for forced authentication is shared among authentication modes. For details, see *(5) Private trap for forced authentication* in *5.4.6 Forced authentication common to all authentication modes.*

(2) Recording information to the RADIUS server accounting functionality

You can enable the accounting functionality of the RADIUS server by using the `aaa accounting mac-authentication` configuration command.

For details about the RADIUS attributes used when sending accounting information to the RADIUS server, see *10.6 Preparation.*

(3) Recording authentication information to the RADIUS server

If you are using RADIUS authentication, the accounting functionality of the RADIUS server records the success or failure of authentication attempts. Note that the information that is recorded differs between RADIUS server implementations. For details, see the documentation for the RADIUS server deployed in your network.

(4) Outputting accounting log information to the syslog server

Accounting log information for MAC-based authentication and operation log information for all Switches are output to all the syslog servers defined in the `syslog` configuration.

Figure 10-13 Format of output to syslog server

```
 Fac Mon Date Time hostname [number]:AUT Mon/Date/Time MAC log message body
|(1)|---(2) ---|--(3)---|--(4)-|(5)|----(6)---|(7)|------------(8)-------------|
```

(1) Facility
(2) Date and time output in TIMESTAMP: syslog
(3) Identification name of HOSTNAME: Switch
(4) Function number
(5) Log type representing authentication function
(6) Event occurrence time
(7) Authentication function type representing MAC authentication
(8) Message body

For details about log output to the syslog server, see *22. Log Data Output Functionality.*

In addition, the Switch cannot specify or suppress the output of only MAC-based authentication accounting log information to the syslog server.

10.6 Preparation

10.6.1 For local authentication

To use the local authentication method, the following preparations are required:

- Configuration definition
- Registering the internal MAC-based authentication DB
- Backing up the internal MAC-based authentication DB
- Restoring the internal MAC-based authentication DB

(1) Configuration definition

To use MAC-based authentication, set the VLAN information and MAC authentication information on the Switch by using configuration commands. (See *11.1 MAC-based authentication configuration.)*

(2) Registering the internal MAC-based authentication DB

Before using the local authentication method, you must register the MAC address information (the MAC addresses of the terminals to be authenticated and the post-authentication VLAN ID) in the internal MAC-based authentication DB.

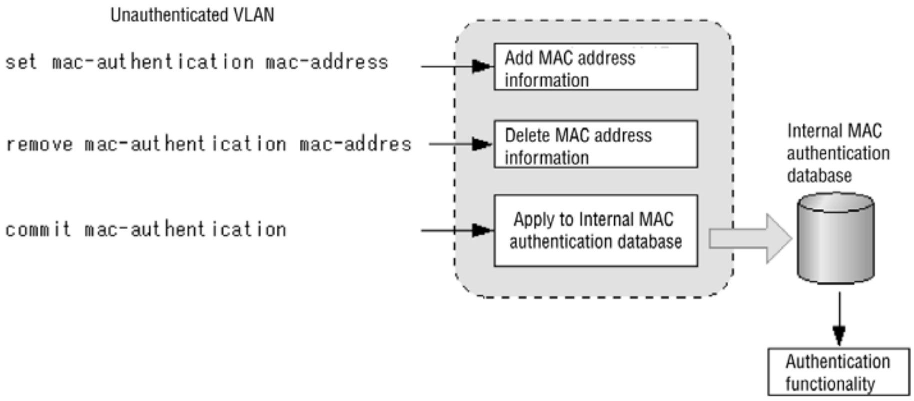
The procedure for registering the MAC address information includes editing the MAC address information (addition and deletion), and then reflecting it in the internal MAC-based authentication DB. The procedure is described below.

Before adding MAC address information, you must finish setting up the environment for the MAC-based authentication system and configuration must be complete using an operation command.

- Add the MAC address information (the MAC addresses of the terminals to be authenticated and the post-authentication VLAN ID) by using the `set mac-authentication mac-address` operation command.
- To delete registered MAC address information, use the `remove mac-authentication mac-address` operation command.
- Incorporate the edited MAC address information in the internal MAC-based authentication DB by executing the `commit mac-authentication` operation command.

In addition, the MAC address information edited prior to execution of the `commit mac-authentication` operation command can be viewed by using the `show mac-authentication mac-address` operation command.

Figure 10-14 Editing the MAC address information and reflecting the result in the internal MAC-based authentication DB



In local authentication, the MAC address is retrieved in the order that is displayed when the `show mac-authentication mac-address` operation command is executed.

(a) Registering the same MAC address

Multiple identical MAC addresses with different VLAN IDs (or no VLAN ID at all) can be defined for VLAN IDs in the internal MAC-based authentication DB.

(b) Registering MAC mask information

The internal MAC-based authentication DB allows MAC address and MAC mask entries to be registered.

An entry with a MAC mask can be registered in the database even if they are contained in another entry with a MAC mask. However, it cannot be registered if the numeric value of the entry is completely identical to another entry.

Note that only one entry with the `any` condition can be registered. (If a registered entry already exists, it is overwritten.)

The `show mac-authentication mac-address` operation command displays entries in ascending order by MAC address. However, entries are displayed in order of entries that are only MAC addresses, entries with MAC masks, and then the entry with the `any` condition.

(3) Backing up the internal MAC-based authentication DB

To back up the internal MAC-based authentication DB, use the `store mac-authentication` operation command.

Two backup files are automatically generated. One file contains MAC-address-only entries, and the other file contains entries that have MAC masks.

- *<file-name>*: File containing entries that do not have MAC masks
- *<file-name>*`.msk`: File containing entries that have MAC masks

(4) Restoring the internal MAC-based authentication DB

To restore the internal MAC-based authentication DB from the backup files, use the `load mac-authentication` operation command.

Be careful when restoring the database. The information edited and registered by using commands such as the `set mac-authentication mac-address` operation command immediately before the restoration are discarded and replaced with the restored information.

Two backup files are automatically generated. One file contains MAC-address-only entries, and the other file contains entries that have MAC masks. (For details, see *(3) Backing up the internal MAC-based authentication DB.)*

- When using MAC-address-only entries, restore from a backup file containing entries that do not have MAC masks.
- When using MAC address entries and entries with MAC masks, restore from a backup file containing entries that have MAC masks.

10.6.2 RADIUS authentication

When using RADIUS authentication, the following preparations are required:

- Configuration definition
- Preparing the RADIUS server

(1) Configuration definition

To use MAC-based authentication, configure VLAN information and MAC authentication information on the Switch by using configuration commands. (See *11.1 MAC-based authentication configuration.)*

(2) Preparing the RADIUS server

(a) RADIUS attributes to be used

The following table describes the RADIUS attribute names used by the Switch.

Table 10-12 Attribute names used in authentication (part 1:Access-Request)

Attribute name	Type value	Description
`User-Name`	1	Terminal MAC address. Each byte of the terminal MAC address is separated by a hyphen (-).#1
`User-Password`	2	User password. Each byte of the terminal MAC address is separated by a hyphen (-).#1
`NAS-IP-Address`	4	IP address of the Switch requesting authentication. From among the VLAN interfaces that have an IP address registered, the IP address of the smallest VLAN ID is used.
`NAS-Port`	5	• Fixed VLAN mode: `IfIndex` of authentication unit under authentication • Dynamic VLAN mode: `IfIndex` of authentication unit under authentication • Legacy mode: 4296
`Service-Type`	6	The type of service to be provided Fixed as `Framed(2)`.

Attribute name	Type value	Description
Called-Station-Id	30	Port MAC address (lower-case ASCII[#2], separated by hyphens (-))
Calling-Station-Id	31	Terminal MAC address (lower-case ASCII[#2], separated by hyphens (-))
NAS-Identifier	32	● Fixed VLAN mode VLAN ID of VLAN to which a terminal that is requesting authentication belongs For VLAN10, 10 ● Dynamic VLAN mode Character string specified by the hostname configuration command ● Legacy mode Character string specified by the hostname configuration command
NAS-Port-Type	61	Type of physical port used by a terminal for authentication Virtual(5)
Connect-Info	77	Character string indicating the connection characteristics ● Fixed VLAN mode: Physical port ("CONNECT Ethernet") ● Dynamic VLAN mode: Physical port ("CONNECT Ethernet") ● Legacy mode: ("CONNECT DVLAN")
NAS-Port-Id	87	Character string for port identification (*x* and *y* represent numbers) ● Fixed VLAN mode: "Port *x*/*y*" ● Dynamic VLAN mode: "Port *x*/*y*" ● Legacy mode: "DVLAN *x*""

#1

For details, see *(b) Information to be set in the RADIUS server.*

#2

The MAC addresses for Called-Station-Id and Calling-Station-Id are lower case when used by the Switch. However, the letters a to f in the MAC addresses can be converted to upper-case letters by using the radius-server attribute station-id capitalize configuration command.

Table 10-13 Attribute names used in authentication (part 2: Access-Accept)

Attribute name	Type value	Description
Service-Type	6	The type of service to be provided Fixed as Framed(2).
Filter-Id	11	Text character string Used in multistep authentication[#1].

Attribute name	Type value	Description
Reply-Message	18	Not used[#2]
Tunnel-Type	64	Tunnel type[#3] Fixed as VLAN(13).
Tunnel-Medium-Type	65	Indicates the protocol to use to create a tunnel[#3]. Fixed as IEEE 802(6).
Tunnel-Private-Group-ID	81	Character string for VLAN identification.[#4] The character strings can be formatted as follows: (1) As a character string indicating a VLAN ID (2) As a character string containing the word "VLAN" followed by a VLAN ID The character string cannot contain spaces. If it does, VLAN assignment will fail. (3) Character string representing the name of a VLAN defined for a VLAN interface by the name configuration command (The smaller VLAN ID takes precedence.)[#5] Examples VLAN ID: 10 Configuration command name: Authen_VLAN Format (1): "10" Format (2): "VLAN10" Format (3): Authen_VLAN

#1

For details about character strings used in multistep authentication, see *12. Multistep authentication.*

#2

The Switch collects the Reply-Message character string as accounting log information.

#3

The tag area is ignored.

#4

The Switch selects a character string format and identifies the VLAN ID in accordance with the following conditions:

1. Conditions for selecting character string formats (1), (2) and (3) for Tunnel-Private-Group-ID
    - Format (1) is used for a character string that begins with a number from 0 to 9.
    - Format (2) is used for a character string that begins with VLAN plus a number from 0 to 9.
    - Format (3) is used for a character string other than the above character strings.

    In addition, when the first byte is in the range from 0x00 to 0x1f, it means that a tag is present but the tag area is ignored.

2. Conditions for identifying the VLAN ID from character strings in formats (1) and (2):
   - Converts only the numerical characters 0 to 9 into a decimal number and its first four characters become valid. (The fifth and the subsequent characters are all ignored.)

     Example: `0010` is equivalent to `010` or `10`, and it is handled as VLAN ID = 10.

     However, `01234` is handled as VLAN ID = 123.
   - If a character other than 0 through 9 exists in the middle of the character string, the character is considered to be the end of the string.

     Example: `12+3` is handled as VLAN ID = 12.

#5

For details about specifying the VLAN name by using the `name` configuration command, see *5.4.2 Specifying post-authentication VLANs by VLAN name.*

Table 10-14 Attribute names used in RADIUS accounting functionality

Attribute name	Type value	Description
`User-Name`	1	Terminal MAC address. Each byte of the terminal MAC address is separated by a hyphen (-).#1
`NAS-IP-Address`	4	IP address of the Switch requesting authentication. From among the VLAN interfaces that have an IP address registered, the IP address of the smallest VLAN ID is used.
`NAS-Port`	5	● Fixed VLAN mode: `IfIndex` of authentication unit under authentication ● Dynamic VLAN mode: `IfIndex` of authentication unit under authentication ● Legacy mode: 4296
`Service-Type`	6	The type of service to be provided. Fixed as `Framed(2)`.
`Calling-Station-Id`	31	MAC address of authentication terminal (lower-case ASCII#2, separated by hyphens (`-`))
`NAS-Identifier`	32	● Fixed VLAN mode VLAN ID of VLAN to which a terminal that is requesting authentication belongs For VLAN10, `10` ● Dynamic VLAN mode Character string specified by the `hostname` configuration command ● Legacy mode Character string specified by the `hostname` configuration command

Attribute name	Type value	Description
Acct-Status-Type	40	Accounting request type Start(1), Stop(2)
Acct-Delay-Time	41	Accounting information (transmission delay time) (in seconds)
Acct-Input-Octets	42	Accounting information (number of received octets) Fixed at (0).
Acct-Output-Octets	43	Accounting information (number of sent octets) Fixed at (0).
Acct-Session-Id	44	ID for accounting information identification
Acct-Authentic	45	Authentication method RADIUS(1) and Local(2)
Acct-Session-Time	46	Accounting information (session duration time) Fixed at (0).
Acct-Input-Packets	47	Accounting information (number of received packets) Fixed at (0).
Acct-Output-Packets	48	Accounting information (number of sent packets) Fixed at (0).
Acct-Terminate-Cause	49	Accounting information (cause of session termination). See *Table 10-15 Termination causes returned by Acct-Terminate-Cause.*
NAS-Port-Type	61	Type of physical port used by a terminal for authentication Fixed at Virtual(5)
NAS-Port-Id	87	Character string for port identification (*x* and *y* represent numbers) ● Fixed VLAN mode: "Port *x*/*y*" ● Dynamic VLAN mode: "Port *x*/*y*" ● Legacy mode: "DVLAN *x*""

#1

For details, see *(b) Information to be set in the RADIUS server.*

#2

The MAC addresses for Calling-Station-Id are lower case when used by the Switch. However, the letters a to f in the MAC addresses can be converted to upper-case letters by using the radius-server attribute station-id capitalize configuration command.

Table 10-15 Termination causes returned by Acct-Terminate-Cause

Attribute name	Type value	Description
User Request	1	Disconnection due to detection of a terminal move
Idle Timeout	4	Disconnection due to non-communication continuing for a certain period of time
Session Timeout	5	Disconnection due to session expiration
Admin Reset	6	Disconnected by the administrator: ● Deletion of mac-authentication port in configuration Also includes disconnection causes due to changes to other authentication configurations and operation commands.
NAS Request	10	First-step MAC-based authentication disconnected because the second-step authentication succeeded in multistep authentication
Service Unavailable	15	Service no longer able to be provided: ● If authentication is canceled by the max-user check of a destination port after a terminal moved
Reauthentication Failure	20	Re-authentication failed.
Port Reinitialized	21	Port MAC address reinitialized ● Port link down ● Deletion of vlan from port by the configuration ● Setting of shutdown by the configuration ● Execution of inactivate operation command

(b) Information to be set in the RADIUS server

The user ID and password used to request authentication from the RADIUS server by the MAC-based authentication functionality are both the MAC address of the terminal. When setting MAC-based authentication terminal information for the RADIUS server, it is necessary to separate each byte of the MAC address of the terminal with a hyphen (-) for both the user ID and password.

The MAC address format of the user ID and password can be specified by the configuration. For details about setting this specification by the configuration, see *(c) MAC address format and password at authentication request in fixed VLAN mode* and *(d) MAC address format and password at authentication request in dynamic VLAN mode and legacy mode.*

For details about how to configure the RADIUS server, see the documentation for the RADIUS server deployed in your network.

The configuration example below is for a RADIUS server configuration that is based on the following authenticated terminal information:

- Terminal MAC address: 12-34-56-00-ff-e1
- For fixed VLAN mode: The VLAN ID of the VLAN to which the terminal

requesting authentication belongs is 10.

- For dynamic VLAN mode and legacy mode: The VLAN ID of the post-authentication VLAN is 311
- Setting of the name configuration command: mac-authen-vlan

Table 10-16 Example of RADIUS server configuration

Configuration item	Description
User-Name	12-34-56-00-ff-e1 Each byte of the terminal MAC address is separated by a hyphen (-).#1
Auth-Type	Local
User-Password	12-34-56-00-ff-e1 Each byte of the terminal MAC address is separated by a hyphen (-).#2
Tunnel-Type	Virtual VLAN (value of 13)
NAS-Identifier	For fixed VLAN mode "10" The VLAN ID of the VLAN to which the terminal requesting authentication is defined as a number.
Tunnel-Medium-Type	IEEE-802 (value of 6)
Tunnel-Private-Group-ID	For dynamic VLAN mode and legacy mode: Any of the following formats is used: ● "311" The post-authentication VLAN ID is defined as a number. ● "VLAN0311" The post-authentication VLAN ID is defined as a number immediately after the character string VLAN. ● "mac-authen-vlan" A character string representing a VLAN name defined by the name configuration command
Authentication method	PAP

#1

If the upper-case letters A to F are included in a MAC address, they must be converted to the lower-case characters a to f before the MAC address is specified in the RADIUS server.

When a MAC address format has been set by the configuration, be sure to use that format.

#2

When a MAC address format has been set by the configuration, be sure to use that format.

When a password has been set by the configuration, be sure to use the character string defined by the configuration.

(c) MAC address format and password at authentication request in fixed VLAN mode

Because VLAN does not move in fixed VLAN mode, VLAN ID included in the result of an authentication request to the RADIUS server is not taken into consideration. For this reason, the following VLAN limitation functionality is supported to prevent authentication from unintended VLANs.

- Limiting VLAN by using User-Name
- Limiting VLANs by using NAS-Identifier

1. Limiting VLAN by using User-Name

   When an authentication request is issued to the RADIUS server, a user ID is created for authentication by including a delimiter (default: `%VLAN`) and added information (VLAN ID). The delimiter character string can be specified by the `mac-authentication vlan-check` configuration command.

   The example shown below is where the address is `12-34-56-00-ff-e1` and VLAN ID is `100`.

Table 10-17 Configuration definition and RADIUS server authentication request format

Configuration definition			RADIUS server authentication request format	
id-format	**vlan-check**	**password**	**User ID**	**Password**
None	None	None	12-34-56-00-ff-e1	12-34-56-00-ff-e1
	vlan-check		12-34-56-00-ff-e1%VLAN100	
	vlan-check key @VLAN		12-34-56-00-ff-e1@VLAN100	
id-format 0	None		12-34-56-00-ff-e1	12-34-56-00-ff-e1
	vlan-check		12-34-56-00-ff-e1%VLAN100	
	vlan-check key @VLAN		12-34-56-00-ff-e1@VLAN100	
id-format 0 capitals	None		12-34-56-00-FF-E1	12-34-56-00-FF-E1
	vlan-check		12-34-56-00-FF-E1%VLAN100	
	vlan-check key @VLAN		12-34-56-00-FF-E1@VLAN100	
id-format 1	None		12345600ffe1	12345600ffe1
	vlan-check		12345600ffe1%VLAN100	

Configuration definition			RADIUS server authentication request format	
id-format	**vlan-check**	**password**	**User ID**	**Password**
	vlan-check key @VLAN		12345600ffe1@VLAN100	
id-format 1 capitals	None		12345600FFE1	12345600FFE1
	vlan-check		12345600FFE1%VLAN100	
	vlan-check key @VLAN		12345600FFE1@VLAN100	
id-format 2	None		1234.5600.ffe1	1234.5600.ffe1
	vlan-check		1234.5600.ffe1%VLAN100	
	vlan-check key @VLAN		1234.5600.ffe1@VLAN100	
id-format 2 capitals	None		1234.5600.FFE1	1234.5600.FFE1
	vlan-check		1234.5600.FFE1%VLAN100	
	vlan-check key @VLAN		1234.5600.FFE1@VLAN100	
id-format 3	None		12:34:56:00:ff:e1	12:34:56:00:ff:e1
	vlan-check		12:34:56:00:ff:e1%VLAN100	
	vlan-check key @VLAN		12:34:56:00:ff:e1@VLAN100	
id-format 3 capitals	None		12:34:56:00:FF:E1	12:34:56:00:FF:E1
	vlan-check		12:34:56:00:FF:E1%VLAN100	
	vlan-check key @VLAN		12:34:56:00:FF:E1@VLAN100	
None	None	Configured	12-34-56-00-ff-e1	Specified character string
	vlan-check	(Arbitrary character string)	12-34-56-00-ff-e1%VLAN100	

Configuration definition			RADIUS server authentication request format	
id-format	**vlan-check**	**password**	**User ID**	**Password**
	vlan-check key @VLAN		12-34-56-00-ff-e1@VLAN100	
id-format 0	None		12-34-56-00-ff-e1	
	vlan-check		12-34-56-00-ff-e1%VLAN100	
	vlan-check key @VLAN		12-34-56-00-ff-e1@VLAN100	
id-format 0 capitals	None		12-34-56-00-FF-E1	
	vlan-check		12-34-56-00-FF-E1%VLAN100	
	vlan-check key @VLAN		12-34-56-00-FF-E1@VLAN100	
id-format 1	None		12345600ffe1	
	vlan-check		12345600ffe1%VLAN100	
	vlan-check key @VLAN		12345600ffe1@VLAN100	
id-format 1 capitals	None		12345600FFE1	
	vlan-check		12345600FFE1%VLAN100	
	vlan-check key @VLAN		12345600FFE1@VLAN100	
id-format 2	None		1234.5600.ffe1	
	vlan-check		1234.5600.ffe1%VLAN100	
	vlan-check key @VLAN		1234.5600.ffe1@VLAN100	
id-format 2 capitals	None		1234.5600.FFE1	
	vlan-check		1234.5600.FFE1%VLAN100	
	vlan-check key @VLAN		1234.5600.FFE1@VLAN100	

Configuration definition			RADIUS server authentication request format	
id-format	**vlan-check**	**password**	**User ID**	**Password**
id-format 3	None		12:34:56:00:ff:e1	
	vlan-check		12:34:56:00:ff:e1%VLAN100	
	vlan-check key @VLAN		12:34:56:00:ff:e1@VLAN100	
id-format 3 capitals	None		12:34:56:00:FF:E1	
	vlan-check		12:34:56:00:FF:E1%VLAN100	
	vlan-check key @VLAN		12:34:56:00:FF:E1@VLAN100	

2. Limiting VLANs by using `NAS-Identifier`

   In fixed VLAN mode, the acquired VLAN ID (the VLAN ID to which a terminal belongs at authentication request) is set in the `NAS-Identifier` RADIUS attribute when an authentication request is issued to RADIUS server.

   The number of VLANs that can belong to the RADIUS server can be limited by setting the user ID and password in `NAS-Identifier` together with authentication VLAN information (the VLAN ID to which the terminal belongs at authentication request).

(d) MAC address format and password at authentication request in dynamic VLAN mode and legacy mode

In MAC-based authentication of the Switch, a terminal MAC address is used for the user ID and password when issuing an authentication request to the RADIUS server, but the MAC address format and password character string can be changed by the configuration. In addition, the letters `a` to `f` can be changed into the corresponding upper-case letters by specifying `capitals`.

The following table summarizes an example of issuing an authentication request to the RADIUS server with the terminal MAC address set to `12-34-56-00-ff-e1`.

Table 10-18 Configuration definition and RADIUS server authentication request format

Configuration definition		RADIUS server authentication request format	
id-format	**password**	**User ID**	**Password**
None	None	12-34-56-00-ff-e1	12-34-56-00-ff-e1
id-format 0		12-34-56-00-ff-e1	12-34-56-00-ff-e1

Configuration definition		RADIUS server authentication request format	
id-format	**password**	**User ID**	**Password**
id-format 0 capitals		12-34-56-00-FF-E1	12-34-56-00-FF-E1
id-format 1		12345600ffe1	12345600ffe1
id-format 1 capitals		12345600FFE1	12345600FFE1
id-format 2		1234.5600.ffe1	1234.5600.ffe1
id-format 2 capitals		1234.5600.FFE1	1234.5600.FFE1
id-format 3		12:34:56:00:ff:e1	12:34:56:00:ff:e1
id-format 3 capitals		12:34:56:00:FF:E1	12:34:56:00:FF:E1
None	Configured	12-34-56-00-ff-e1	Specified character string
id-format 0	(Arbitrary character string)	12-34-56-00-ff-e1	
id-format 0 capitals		12-34-56-00-FF-E1	
id-format 1		12345600ffe1	
id-format 1 capitals		12345600FFE1	
id-format 2		1234.5600.ffe1	
id-format 2 capitals		1234.5600.FFE1	
id-format 3		12:34:56:00:ff:e1	
id-format 3 capitals		12:34:56:00:FF:E1	

10.7 Notes for MAC-based authentication

10.7.1 Interoperability of MAC-based authentication and other functionality

For details about the interoperability of MAC-based authentication and other functionality, see *5.9.3 Interoperability of the Layer 2 authentication functionality and other functionality.*

10.7.2 Notes for all authentication modes

(1) Frames that trigger authentication

[Fixed VLAN mode] [Dynamic VLAN mode]

The first frame that triggers authentication is not forwarded because it is a frame prior to authentication.

(2) Setting the maximum connection time

When the maximum connection time is shortened or lengthened by the `mac-authentication max-timer` configuration command, the changed time does not apply to currently authenticated terminals. It becomes effective starting from the next authentication.

(3) Internal MAC-based authentication DB

(a) Changing the internal MAC-based authentication DB

When an operation command is used to make an addition or change to the internal MAC-based authentication DB, the addition or change does not apply to currently authenticated terminals. It becomes effective starting from the next authentication.

(b) Specifying multiple identical MAC addresses to the internal MAC-based authentication DB

Multiple identical MAC addresses with different VLAN IDs (or no VLAN ID at all) can be defined for VLAN IDs in the internal MAC-based authentication DB. In this case, the operation is performed as follows for the first matched MAC address depending on the authentication mode and the configuration.

Table 10-19 Information displayed in fixed VLAN mode

VLAN ID setting in internal MAC-based authentication DB for first matching MAC address	Configuration mac-authentication vlan-check	Operation
Configured	Configured	Authentication is successful when the internal MAC-based authentication DB and the MAC address and VLAN of an authentication request terminal match.(VLAN comparison is also performed.)#.
	Not configured	Authentication is successful for the VLAN to which the target authentication terminal belongs when the internal MAC-based authentication DB and the first MAC address match.(No VLAN comparison is performed.)

VLAN ID setting in internal MAC-based authentication DB for first matching MAC address	Configuration mac-authentication vlan-check	Operation
Not configured	Configured	Authentication is successful for the VLAN to which the target authentication terminal belongs when the internal MAC-based authentication DB and the first MAC address match.(No VLAN comparison is performed.)
	Not configured	

#

If both do not match, authentication fails. (Under this condition, this is not necessarily the first matching MAC address.)

Table 10-20 For dynamic VLAN mode and legacy mode

VLAN ID setting in internal MAC-based authentication DB for first matching MAC address	Operation
Configured	The terminal gains membership to the VLAN of the first matching MAC address, and authentication is successful.
Not configured	● [Dynamic VLAN mode] Accommodation in the native VLAN as a post-authentication VLAN[#] (Management of terminals as an authenticated terminal in fixed VLAN mode) ● [Legacy mode] Authentication fails because the terminal is unable to gain membership to the post-authentication VLAN.

#

See *5.4.4 Auto authentication mode accommodation on the same MAC port.*

(c) Searching for an entry with a MAC mask

When no matching entry is found in the entries that have no MAC masks, entries that have MAC masks are searched to find a match. The behavior for when a matching entry is found is the same as that for entries that have no MAC mask.

The entries that have MAC masks are searched in ascending order of MAC addresses (as displayed by using the `show mac-authentication mac-address` operation command). Depending on how MAC masks are specified, some entries including MAC address might appear. Confirm that they appear in the intended order by using the `show mac-authentication mac-address` operation command.

(4) Using a forced authentication port

1. Be especially careful when using this functionality, as it can pose a security problem.
2. This functionality supports only RADIUS authentication.

   When using forced authentication, set only the RADIUS authentication method. When setting both local authentication and RADIUS authentication as shown below, forced authentication does not operate even if it has been configured.

- `aaa authentication mac-authentication default gourp radius local`
- `aaa authentication mac-authentication default local gourp radius`

3. The Switch supports forced authentication common to all authentication modes and forced authentication by MAC-based authentication but does not allow both to be configured concurrently. Prior to using the authentication functionality, see *(4) Interoperability of this functionality and forced authentication of each authentication method* in *5.4.6 Forced authentication common to all authentication modes.*

(5) Restrictions on interoperation of roaming settings and DHCP snooping

[Fixed VLAN mode] [Dynamic VLAN mode]

When the DHCP snooping functionality is used while the `mac-authentication static-vlan roaming` and `mac-authentication roaming` configuration commands are set, if an attempt is made to move the authenticated terminal, its authentication state changes to that of a port after the move, but communication is not allowed because the binding DB is not updated.

(6) Moving a terminal among ports and the maximum number of authentication terminals

[Fixed VLAN mode] [Dynamic VLAN mode]

The maximum number of authentication terminals is checked only when terminals are newly authenticated.

For this reason, if an authenticated terminal is moved to another port, the maximum number of authentication terminals is not checked at the port after the move.

10.7.3 Notes on use of fixed VLAN mode

(1) Fixed VLAN mode port

Fixed VLAN mode can operate only on ports in an Ethernet interface. In addition, fixed VLAN mode allows MAC-based authentication using tagged frames to operate at a port defined so that tagged frames can be forwarded via the access port/trunk port and MAC port (by using the `switchport mac dot1q` vlan configuration command).

10.7.4 Notes on use of legacy mode

(1) Notes on configuring aging time for MAC address learning

When a short aging time is set for the MAC address table (by using the `mac-address-table aging-time` configuration command), the time until authentication cancellation is shortened automatically by the MAC address aging monitoring functionality. To prevent authentication being automatically canceled, use the `no mac-authentication auto-logout` configuration command.

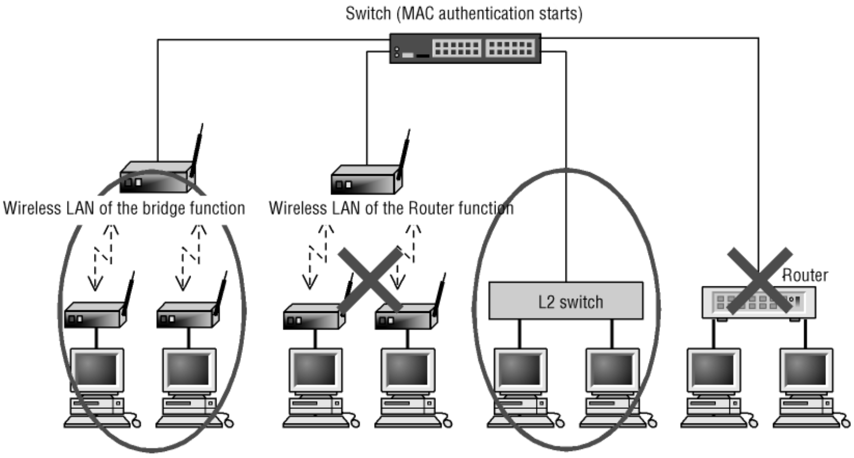
(2) Connecting devices between the terminal and the Switch

Do not connect proxy servers or routers under the Switch.

For example, if there is something that rewrites the MAC address of a client terminal (such as proxy server and router) on a route between the Switch and any authentication terminal, authentication cannot be performed per terminal because the terminal with the rewritten MAC address cannot be recognized as the terminal to be authenticated.

Exercise caution when connecting a hub without inter-port isolation functionality or a wireless LAN downstream from the Switch. PCs attached to that hub or wireless LAN will be able to communicate with each other regardless of their authentication status.

Figure 10-15 Connections between terminals and the Switch



(3) Port number information in accounting log information

Port number information is available as information for authentication and re-authentication.

When the connection port for an authenticated terminal is moved, the information is not collected immediately. The detected port number information is collected of the next time re-authentication occurs.

(4) Interoperability of legacy mode and multistep authentication

The Switch cannot use legacy mode and multistep authentication simultaneously. To use legacy mode, make sure that multistep authentication is not configured for the Switch.

11. MAC-based Authentication Configuration and Operation

MAC-based authentication functionality controls access to VLANs by users authenticated from MAC addresses. This chapter describes MAC-based authentication configuration and operation.

11.1 MAC-based authentication configuration

11.1.1 List of configuration commands

The following table describes configuration commands for MAC-based authentication and authentication modes.

Table 11-1 List of configuration commands and authentication modes

Command name	Description	Authentication mode		
		F	D	L
`aaa accounting mac-authentication`	Sends accounting information for MAC-based authentication to an accounting server.	Y	Y	Y
`aaa authentication mac-authentication`	Specifies the authentication method group for MAC-based authentication.	Y	Y	Y
`aaa authentication mac-authentication end-by-reject`	Terminates authentication if authentication is denied. If authentication fails due to a communication failure (for example, the RADIUS server does not respond), the next authentication method specified by the `aaa authentication mac-authentication` command is used to perform authentication.	Y	Y	Y
`authentication arp-relay`#1	Outputs ARP frames that were sent to other devices from unauthenticated terminals to a non-authenticating port.	Y	Y	N
`authentication ip access-group`#1	Outputs only the frames specified by applying the IPv4 access list, from among the IP frames sent from an unauthenticated terminal destined for another device, to a non-authenticating port.	Y	Y	N
`mac-authentication access-group`	By applying the MAC access list to MAC-based authentication ports, sets whether terminals are to be authenticated or not by using MAC addresses.	Y	Y	Y
`mac-authentication authentication`	Sets the name of an authentication method list for the port-based authentication method.	Y	Y	N
`mac-authentication auto-logout`	The `no mac-authentication auto-logout` command disables automatic cancellation of authentication if no frames are received from a terminal authenticated by MAC-based authentication for a certain period of time.	Y	Y	Y

Command name	Description	Authentication mode		
		F	D	L
mac-authentication force-authorized vlan	When using RADIUS authentication, and a request to the RADIUS server fails because of a route failure or other problem, forcibly changes a terminal connected to the target port to an authenticated state.	N	Y	Y
mac-authentication id-format	When using RADIUS authentication, specifies MAC address format for authentication requests to the RADIUS server.	Y	Y	Y
mac-authentication interface	Specifies Ethernet ports for MAC-based authentication.	--	--	Y
mac-authentication max-timer	Sets the maximum connection time.	Y	Y	Y
mac-authentication max-user	Sets the maximum number of terminals that can be authenticated on a Switch.	--	Y	Y
mac-authentication max-user (interface)	Sets the maximum number of authentication terminals that can be authenticated on the applicable port.	--	Y	Y
mac-authentication password	When the RADIUS authentication method is used, this command sets the password used for sending authentication requests to the RADIUS server.	Y	Y	Y
mac-authentication port[#2]	Sets the authentication mode for ports.	Y	Y	--
mac-authentication radius-server host	Specifies information for using a RADIUS server dedicated to MAC-based authentication.	Y	Y	Y
mac-authentication radius-server dead-interval	When using a RADIUS server dedicated to MAC-based authentication, specifies the monitoring timer for the period up to automatic recovery of the primary RADIUS server.	Y	Y	Y
mac-authentication roaming	Specifies communication permissions when moving an authenticated terminal to another port connected via a hub or other device without a link down.	--	Y	--
mac-authentication static-vlan force-authorized	When using RADIUS authentication, and a request to the RADIUS server fails because of a route failure or other problem, forcibly changes a terminal connected to the target port to an authenticated state.	Y	--	--
mac-authentication	Sets the maximum number of terminals that	Y	--	--

Command name	Description	Authentication mode		
		F	D	L
`static-vlan max-user`	can be authenticated on a Switch.			
`mac-authentication static-vlan max-user (interface)`	Sets the maximum number of terminals that can be authenticated on the applicable port.	Y	--	--
`mac-authentication static-vlan roaming`	Specifies the communication permissions when moving an authenticated terminal to another port connected via a hub or other device without a link down.	Y	--	--
`mac-authentication system-auth-control`	Enables MAC-based authentication.	Y	Y	Y
`mac-authentication timeout quiet-period`	Sets the time during which re-authentication will not be attempted (re-authentication delay timer) for the same terminal (MAC address) when authentication fails.	Y	Y	Y
`mac-authentication timeout reauth-period`	Sets the interval for re-authenticating terminals after an authentication has been successful.	Y	Y	Y
`mac-authentication vlan`	Specifies the VLAN ID for dynamic switching after terminals are authenticated.	--	--	Y
`mac-authentication vlan-check`	Checks the VLAN ID when checking a MAC address during authentication processing.	Y	--	--

Legend:

F: Fixed VLAN mode

D: Dynamic VLAN mode

L: Legacy mode

Y: The command operates according to the settings.

--: The command can be entered, but has no effect.

N: The command cannot be entered.

#1

For details about the configuration, see *5. Overview of Layer 2 Authentication.*

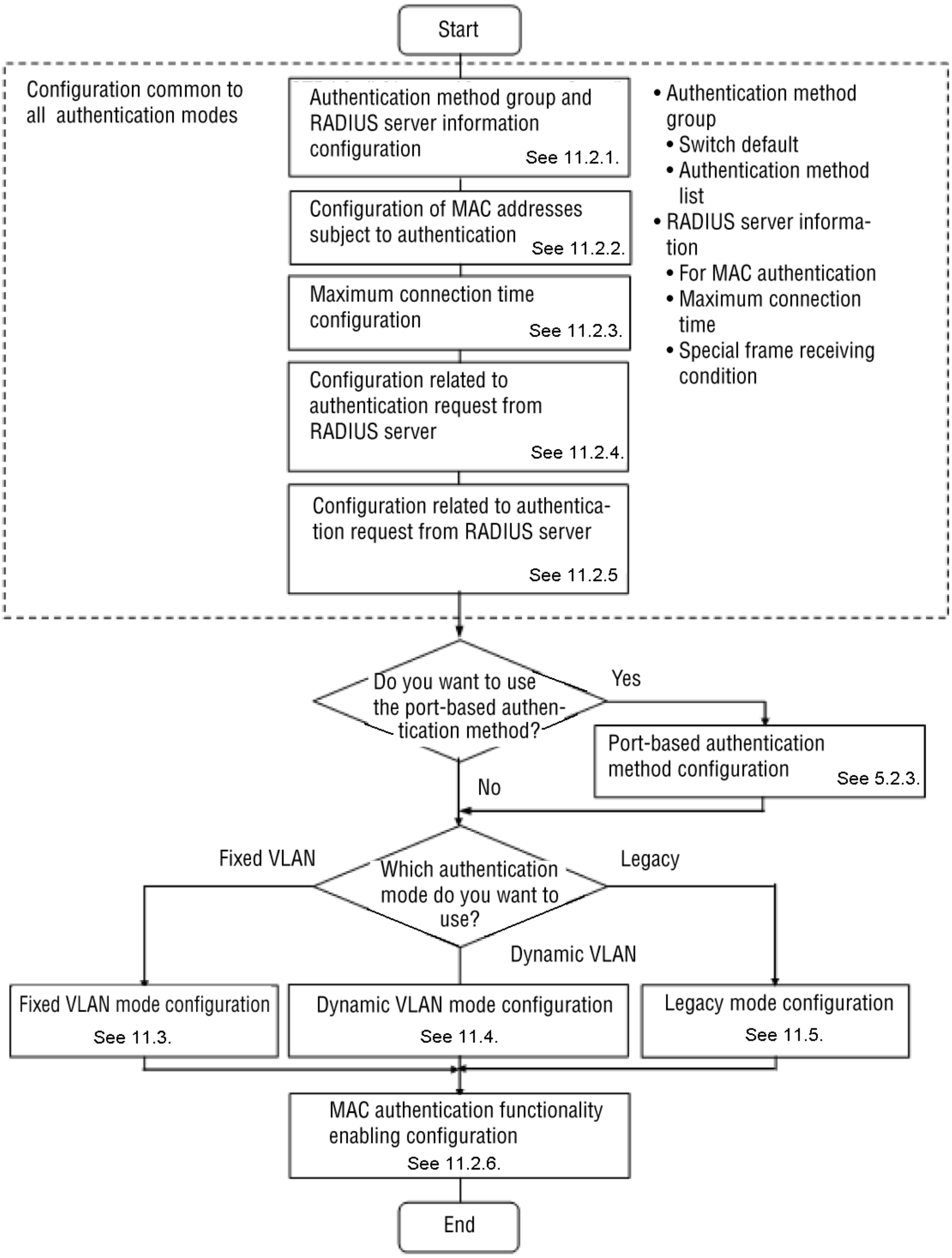
#2

The specification of this command affects the switching of authentication modes.

11.1.2 Configuration procedure for MAC-based authentication

Use the procedure described below to configure MAC-based authentication.

Figure 11-1 Configuration procedure for MAC-based authentication



For details about the configuration, see the following:

1. Configuration common to all authentication modes

   The following subsections describe configuration common to all authentication modes.

   - Configuring the authentication method group and RADIUS server information: *11.2.1 Configuring the authentication method group and*

RADIUS server information

- Configuring MAC addresses for authentication: *11.2.2 Restricting MAC addresses to be authenticated*
- Maximum connection time: *11.2.3 Maximum connection time*
- Configuring authentication requests to the RADIUS server: *11.2.4 Configuring authentication requests to the RADIUS server*
- Configuring the transmission of accounting information to the RADIUS server: *11.2.5 Configuring the transmission of accounting information*
- Configuring port-based authentication methods: *(2) Example of port-based authentication method configuration* in *5.2.3 Authentication method list configuration*

2. Configuring individual authentication modes

   The following sections describe how to configure individual authentication modes.

   Some items are the same as in other authentication modes. In such cases, see the sections referenced in the text.

   - Configuring fixed VLAN mode: *11.3 Configuring fixed VLAN mode*
   - Configuring dynamic VLAN mode: *11.4 Configuring dynamic VLAN mode*
   - Configuring legacy mode: *11.5 Configuring legacy mode*

3. Enabling MAC-based authentication functionality

   Enabling the MAC-based authentication functionality completes the configuration of MAC-based authentication.

   - *11.2.6 Enabling MAC-based authentication functionality*

Authentication modes are enabled by using the configuration settings described in the table below.

Table 11-2 Conditions for enabling authentication modes

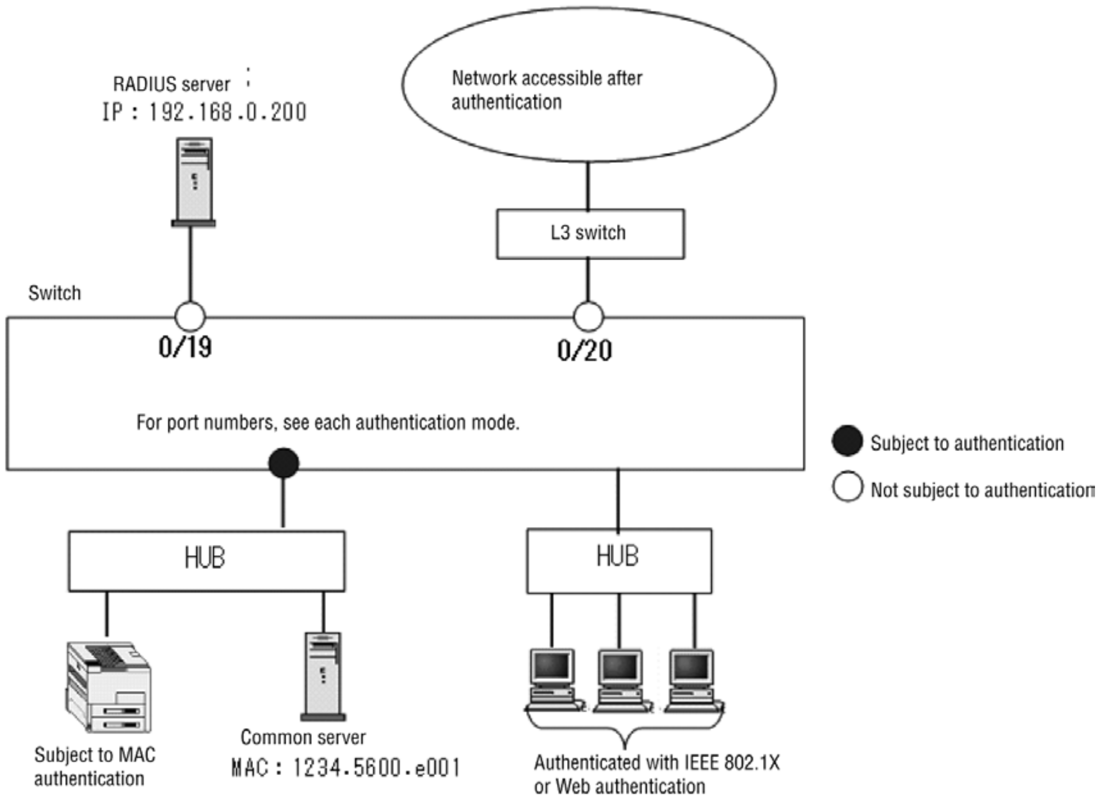
Authentication mode	Configuration settings
Common	● `aaa authentication mac-authentication` ● `mac-authentication radius-server host` or `radius-server` ● `mac-authentication system-auth-control`

Authentication mode	**Configuration settings**
Fixed VLAN mode	When used at access ports ● `vlan` *<VLAN-ID-list>* ● `mac-authentication port` ● `switchport mode access` ● `switchport access vlan` When used at trunk ports ● `vlan` *<VLAN-ID-list>* ● `mac-authentication port` ● `switchport mode trunk` ● `switchport trunk allowed vlan` ● `switchport trunk native vlan` When used at MAC ports ● `vlan` *<VLAN-ID-list>* or `vlan` *<VLAN-ID-list>* `mac-based` ● `mac-authentication port` ● `switchport mode mac-vlan` ● `switchport mac dot1q vlan`
Dynamic VLAN mode	● `vlan` *<VLAN ID list>* `mac-based` ● `mac-authentication port` ● `switchport mode mac-vlan`
Legacy mode	● `vlan` *<VLAN ID list>* `mac-based` ● `mac-authentication interface` ● `mac-authentication vlan` ● `switchport mode mac-vlan` ● `switchport mac vlan`

11.2 Configuration common to all authentication modes

This chapter describes how to configure each authentication mode by using the following basic configuration. For this example, the port numbers used for the RADIUS server and the post-authentication network are 0/19 and 0/20, respectively. For details about port numbers for connecting terminals to be authenticated, see the configuration examples of each authentication mode.

Figure 11-2 Basic configuration



11.2.1 Configuring the authentication method group and RADIUS server information

(1) Configuring the authentication method group

Points to note

Configure an authentication method group for MAC-based authentication.

Specify one device default entry for use in common with MAC-based authentication, and two entries for the authentication method lists used at authenticating ports.

1. Switch default

   In this example, the Switch default authentication methods are RADIUS authentication and local authentication, and the Switch is configured so that local authentication is performed when RADIUS authentication fails due to a communication failure (for example, the RADIUS server does not respond).

If authentication fails because RADIUS authentication is denied, the Switch ends the authentication process at that point and does not perform local authentication.

- For RADIUS authentication, you can configure settings such as for passwords and the format of the MAC address when making authentication requests. For details about the configuration, see *11.2.4 Configuring authentication requests to the RADIUS server*.
- Local authentication uses the internal MAC-based authentication DB. See *11.6.2 Registering an internal MAC-based authentication DB,* and register the internal MAC-based authentication DB on the Switch.

2. Authentication method list

   For the RADIUS server group information to be specified for authentication method lists, `Keneki-group1` and `Keneki-group2` are assumed to have been set in advance.

   For details about authentication method lists, see *5.2.2 Authentication method list.*

   For RADIUS server group information, see *5.3.1 RADIUS server information used with the Layer 2 authentication method,* and *8. Login Security and RADIUS* in the *Configuration Guide Vol. 1*.

Command examples

1. `(config)# aaa authentication mac-authentication default group radius local`

   Sets the default authentication method for the device, in the sequence of RADIUS authentication method and then local authentication method.

2. `(config)# aaa authentication mac-authentication end-by-reject`

   Configures the settings so that the authentication process ends when denied by RADIUS authentication and no local authentication is performed.

3. `(config)# aaa authentication mac-authentication MAC-list1 group Keneki-group1`

   Sets the RADIUS server group name `Keneki-group1` in the authentication method list `MAC-list1`.

4. `(config)# aaa authentication mac-authentication MAC-list2 group Keneki-group2`

   Sets the RADIUS server group name `Keneki-group2` in the authentication method list `MAC-list2`.

Notes

- If the Switch default setting is changed, authentication is canceled for the terminals that have been authenticated by using the Switch default authentication method.
- If the settings for the authentication method list are changed, authentication is canceled for the terminals that have been authenticated by using the authentication method list.
- When `aaa authentication mac-authentication` is not specified, local authentication is assumed.

- When using the forced authentication functionality, specify only `default group radius` by using the above commands. Forced authentication cannot be used with only local authentication, or when the priority for RADIUS authentication and local authentication (as in the above settings) has been specified.
- If the setting for `aaa authentication mac-authentication end-by-reject` is changed, authentication is canceled for the terminals that have been authenticated by using MAC-based authentication.

(2) Configuring RADIUS server information

(a) When using a RADIUS server dedicated to MAC-based authentication

Points to note

Specify information about a RADIUS server dedicated to MAC-based authentication.

An IP address and a RADIUS key must be specified to enable the RADIUS server settings. The configuration command `mac-authentication radius-server host` requires only an IP address for configuration, but the RADIUS server is not used for authentication until you specify a RADIUS key.

In this example, a monitoring timer (`dead-interval` time) is also configured to automatically recover an unavailable RADIUS server dedicated to MAC-based authentication.

1. `(config)# mac-authentication radius-server host 192.168.10.202 key "mac-auth"`

   Specifies the IP address and RADIUS key for the RADIUS server dedicated to MAC-based authentication. In this example, the default values are used for the omitted `auth-port`, `acct-port`, `timeout`, and `retransmit`.

2. `(config)# mac-authentication radius-server dead-interval 15`

   Specifies 15 minutes for the monitoring timer (`dead-interval` time) until automatic recovery when the RADIUS server dedicated to MAC-based authentication is unavailable.

Notes

- If this information is not specified, the settings for a general-use RADIUS server are used. If both the information for a RADIUS server dedicated to MAC-based authentication and the information for a general-use RADIUS server are unspecified, RADIUS authentication cannot be performed.
- Up to four entries can be specified on the entire Switch for information about RADIUS servers dedicated to MAC-based authentication.
- When the RADIUS key, retry count, and response timeout time are omitted, the settings specified by the configuration commands `radius-server key`, `radius-server retransmit`, and `radius-server timeout` are used, respectively.

(b) When using a general-use RADIUS server

For details about the settings for a general-use RADIUS server, see *8. Login Security and RADIUS* in the *Configuration Guide Vol. 1*.

11.2.2 Restricting MAC addresses to be authenticated

Points to note

Specify a range of terminals (MAC addresses) that request MAC-based authentication and a range of terminals that do not request MAC-based authentication.

Command examples

1.

```
(config)# mac-authentication access-group MacAuthFilter
(config)# mac access-list extended MacAuthFilter
(config-ext-macl)# permit 1234.5600.e000 0000.0000.ffff any
(config-ext-macl)# exit
```

Specifies that the terminals with MAC addresses ranging from `1234.5600.e000` to `1234.5600.efff` request MAC-based authentication.

Notes

- An access list used by this functionality does not depend on the settings of the flow detection mode.
- Because only extended MAC access lists are supported, specify the effective range of MAC addresses in the MAC address (`src` specification) portion of the sender.
- For configuration commands concerning MAC access lists, destination MAC addresses (`dst` and afterward) must also be specified. However, these addresses are ignored as filters for MAC-based authentication, so you can specify values of your choice.
- MAC addresses satisfying permit conditions are subject to MAC-based authentication processing.

  MAC addresses satisfying deny conditions are not subject to MAC-based authentication processing, and authentication requests are not sent to the RADIUS server.

  The last line of the MAC access list contains implicit deny conditions for all MAC addresses. This example only sets one line as a permit condition. If this permit condition is not satisfied, the implicit deny condition is considered satisfied. In this case, the MAC addresses in question are not subject to MAC-based authentication processing and authentication requests are not sent to the RADIUS server.

11.2.3 Maximum connection time

Points to note

Specify the maximum connection time for authenticated terminals. When the maximum connection time is exceeded, authentication is automatically canceled.

Command examples

1.

```
(config)# mac-authentication max-timer 60
```

Specifies that the time at which authentication for authenticated terminals is canceled is 60 minutes.

11.2.4 Configuring authentication requests to the RADIUS server

(1) Specifying the MAC address format when sending a request to the RADIUS

server

Points to note

Specify the MAC address format of terminals used for authentication requests to the RADIUS server. For combined settings, see *(2) Preparing the RADIUS server* in *10.6.2 RADIUS authentication.*

Command examples

1. `(config)# mac-authentication id-format 3 capitals`

   Specifies the MAC address format for authentication requests to the RADIUS server to be in the form *nn*:*nn*:*nn*:*nn*:*nn*:*nn* and to use the upper-case characters A to F. (If `capitals` is not specified, use lower-case characters.)

Notes

If this command is not specified, the format of *nn-nn-nn-nn-nn-nn* using lower-case characters `a` to `f` is assumed.

(2) Specifying the password used for requests to the RADIUS server

Points to note

Specify the password used when terminals request authentication from the RADIUS server. For combined settings, see *(2) Preparing the RADIUS server* in *10.6.2 RADIUS authentication.*

Command examples

1. `(config)# mac-authentication password system1-pc0001`

   Specifies the character string to be used as the password when requesting authentication from the RADIUS server. The password must be in the range from 1 to 32 characters.

Notes

- When this command is not specified, the MAC addresses of terminals to be authenticated are treated as passwords. MAC address formats depend on the setting of the configuration command `mac-authentication id-format`.
- Passwords specified by this command are common to all MAC-based authentication terminals.

(3) Specifying the delay timer for resumption of RADIUS authentication

Points to note

Specify the interval of time from suspension of authentication processing to resumption of processing for terminals (MAC addresses) for which requests for authentication to the RADIUS server have been denied.

Command examples

1. `(config)# mac-authentication timeout quiet-period 60`

   Specifies the interval from suspension of authentication processing to resumption of processing to 60 seconds.

   Suspension of authentication processing is applied only to MAC-based authentication, and processing for IEEE 802.1X and Web authentication are not affected.

Notes

- This functionality operates with a default of 300 seconds when the

MAC-based authentication functionality is enabled. When the value of the timer is set to `0`, no time is available for authentication. Note that requests for authentication to the RADIUS server start immediately when the packets are sent from terminals for which authentication has been denied.

- With this setting, the configuration at the time MAC-based authentication is denied is applied. Therefore, when the authentication of a terminal is suspended because of a denial of MAC-based authentication, and the delay timer for resumption of RADIUS authentication is changed, the changed values apply to the terminal being suspended only after its authentication has been resumed and from the point when authentication is denied again.

(4) Specifying the interval for periodic requests for re-authentication to the RADIUS server

Points to note

Specify the interval at which to send requests to the RADIUS server to check the authentication information of authenticated terminals.

Command examples

1. `(config)# mac-authentication timeout reauth-period 600`

   Specifies the interval at which to send periodic requests for re-authentication to the RADIUS server to `600` seconds.

   For terminals authenticated by MAC-based authentication, this functionality periodically requests re-authentication from the RADIUS server after the specified time has elapsed from the time when the terminals were authenticated.

Notes

1. When `0` is set for the periodic re-authentication request interval, periodic re-authentication requests to the RADIUS server are terminated. In this case, the changes in the authentication information of the RADIUS server are not reflected, and terminals that have been authenticated remain moved to a post-authentication VLAN.
2. For details about canceling authentication status, see the following:
   - Fixed VLAN mode: *(7) Authentication cancellation* in *10.2.2* Authentication functionality
   - Dynamic VLAN mode: *(7) Authentication cancellation* in *10.3.2* Authentication functionality
   - Legacy mode: *(7) Authentication cancellation* in *10.4.2 Authentication functionality*
3. For this setting, the configuration at the time the terminals were authenticated by MAC-based authentication applies. Therefore, with terminals authenticated under MAC-based authentication, the time to send periodic requests for re-authentication to the RADIUS server changes, and the changed values apply to the authenticated terminals only after re-authentication is requested and from the point when the terminals are authenticated.

11.2.5 Configuring the transmission of accounting information

Points to note

Specify the transmission of accounting information for MAC-based authentication to the RADIUS server.

Command examples

1. `(config)# aaa accounting mac-authentication default start-stop group radius`

   Specifies the transmission of accounting information to the RADIUS server.

11.2.6 Enabling MAC-based authentication functionality

Points to note

Enable MAC-based authentication after configuration for MAC-based authentication is complete.

Command examples

1. `(config)# mac-authentication system-auth-control`

   Enables MAC-based authentication.

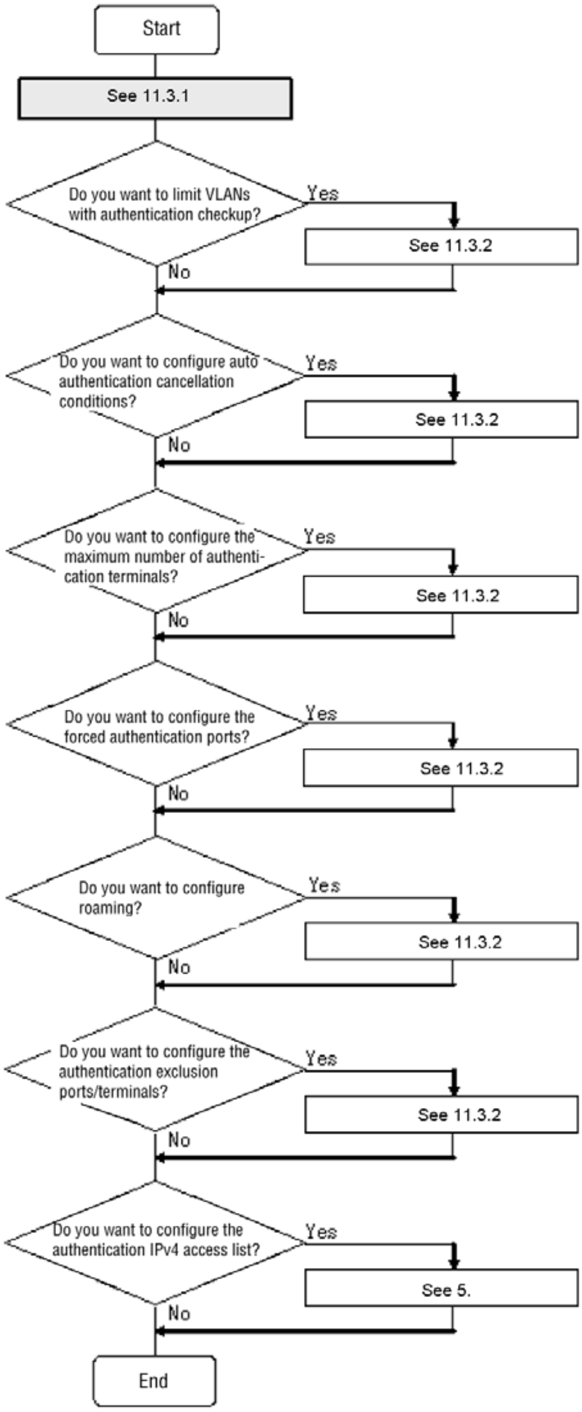
Notes

Specify this command after all settings for MAC-based authentication have been completed. If MAC-based authentication is enabled before configuration is complete, account logs might be collected for authentication failures.

11.3 Configuring fixed VLAN mode

Configure fixed VLAN mode according to the following flow chart after a configuration based on *11.1 MAC-based authentication configuration* and *11.2 Configuration common to all authentication modes.*

Figure 11-3 Configuration procedure for fixed VLAN mode

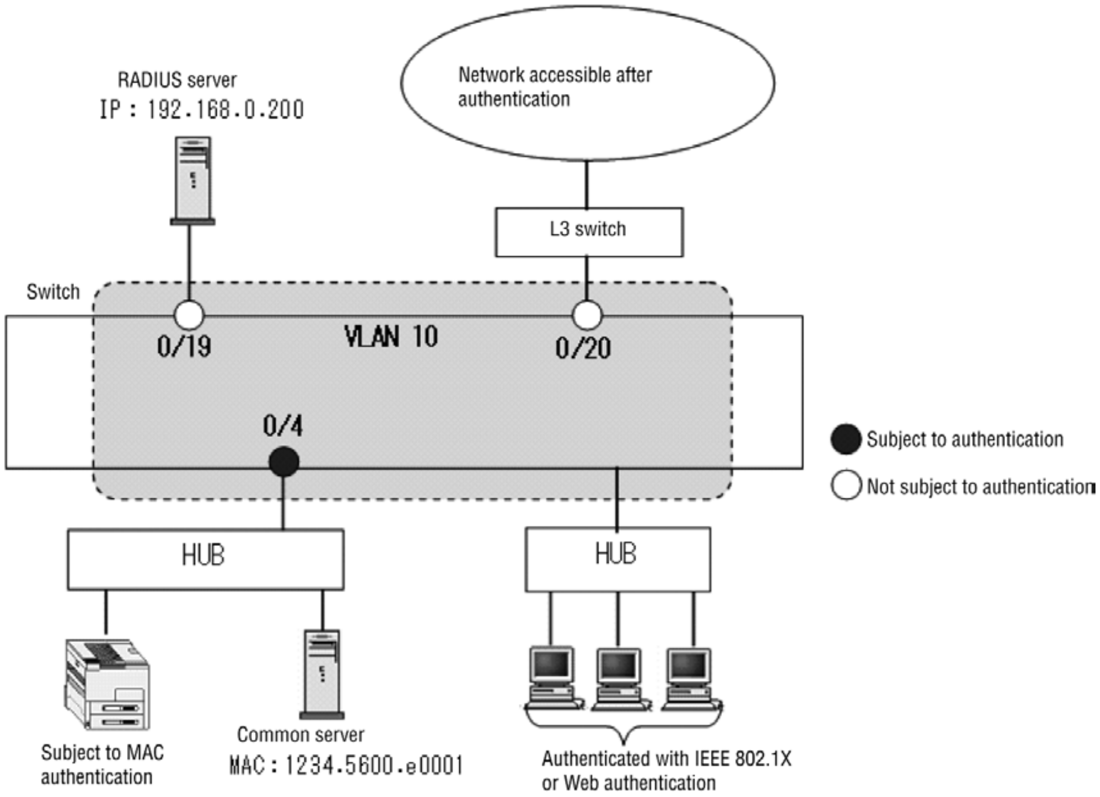


For details about the configuration, see the following:

1. Configuring fixed VLAN mode: *11.3.1 Configuring fixed VLAN mode*
2. Configuring VLAN restrictions when cross-checking authentication: *(1) Restrictions of VLAN when cross-checking authentication information* in *11.3.2 Configuration related to authentication processing*
3. Configuring automatic cancellation of authentication: *(2) Configuring the conditions for automatic cancellation of authentication* in *11.3.2 Configuration related to authentication processing*
4. Maximum number of authentication terminals: *(3) Maximum number of authentication terminals* in *11.3.2 Configuration related to authentication processing*
5. Configuring forced authentication ports: *(4) Forced authentication ports* in *11.3.2 Configuration related to authentication processing*
6. Configuring roaming: *(5) Setting roaming (allowing communication for moved ports of authenticated terminals)* in *11.3.2 Configuration related to authentication processing*
7. Configuring authentication exemption for ports or terminals: *(6) Authentication exemption* in *11.3.2 Configuration related to authentication processing*
8. Configuring the authentication IPv4 access list: *5.5.2 Configuring the authentication IPv4 access list*

11.3.1 Configuring fixed VLAN mode

Figure 11-4 Configuration example of fixed VLAN mode



(1) Configuring authentication ports and VLAN information for authentication

Points to note

Set fixed VLAN mode and VLAN information for authentication for ports used for fixed VLAN mode.

Command examples

1.
```
(config)# vlan 10
(config-vlan)# exit
```
Specifies VLAN ID 10.

2.
```
(config)# interface fastethernet 0/4
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
```
Sets port 0/4 as the access port to which terminals to be authenticated are connected, and sets VLAN 10 for authentication.

3.
```
(config-if)# mac-authentication port
(config-if)# exit
```
Sets fixed VLAN mode to port 0/4.

(2) Configuring authentication method list names for port-based authentication method

Points to note

Sets the name of an authentication method list for the port-based authentication method.

For details about the configuration of the authentication method list, see *(1) Configuring the authentication method group* in *11.2.1 Configuring the authentication method group and RADIUS server information.*

Command examples

1.
```
(config)# interface fastethernet 0/4
(config-if)# mac-authentication authentication MAC-list1
(config-if)# exit
```

Sets the authentication method list name `MAC-list1` to port 0/4.

Notes

- If this information has not been configured, authentication follows the Switch default as explained in *(1) Configuring the authentication method group* in *11.2.1 Configuring the authentication method group and RADIUS server information.*
- When a name of an authentication method list set for a port does not match the name of an authentication method list of an authentication method group or is not present in an authentication method group, authentication will be performed according to the device default.
- The setting cannot be specified concurrently with the authentication method by user ID in Web authentication or legacy mode. For details, see *5.2.2 Authentication method list.*

11.3.2 Configuration related to authentication processing

This subsection describes the settings for authentication processing for fixed VLAN mode.

(1) Restrictions of VLAN when cross-checking authentication information

Points to note

Set the VLAN ID to be cross-checked when cross-checking authentication terminals by local authentication or RADIUS authentication in fixed VLAN mode.

Command examples

1.
```
(config)# mac-authentication vlan-check key @VLAN
```

Authentication terminals are cross-checked in local authentication by MAC addresses and VLAN ID of the corresponding ports and in RADIUS authentication by MAC addresses, separated by the character string `@` and VLAN ID of the corresponding ports.

For RADIUS authentication, see *(1) Specifying the MAC address format when sending a request to the RADIUS server* and *(2) Specifying the password used for requests to the RADIUS server* in*11.2.4 Configuring* *authentication requests to the RADIUS server,* and set the MAC address format and password as necessary.

(2) Configuring the conditions for automatic cancellation of authentication

(a) Maximum connection time

This setting is common to all authentication modes in MAC-based authentication. See *11.2.3 Maximum connection time* in *11.2 Configuration common to all authentication modes.*

(b) Non-connection monitoring time for authentication terminals

Points to note

Set the non-connection monitoring time for authentication terminals. When no frames are received from target terminals after the specified time has elapsed, authentication of the terminals is automatically canceled.

Command examples

1. `(config)# mac-authentication auto-logout delay-time 600`

   Sets non-connection monitoring time for authentication terminals to `600` seconds (10 minutes).

   If MAC-based authentication is enabled, this functionality operates by default (delay-time: 3600 seconds).

   If `no mac-authentication auto-logout` is specified, authentication is not canceled.

Notes

- When the time for automatically canceling authentication and the time for periodic re-authentication requests to the RADIUS server (the `mac-authentication timeout reauth-period`) overlap, automatically canceling authentication will be given a higher priority.
- This setting is applied immediately. However, a delay of up to 60 seconds until actually applying the functionality occurs because non-connection monitoring time is a 60-second cycle. When the value of `mac-authentication auto-logout delay-time` is changed from the current time to a shorter time, and terminals with the elapsed changed non-connection monitoring time are detected, authentication is automatically canceled. In this case, a maximum delay of up to 60 seconds is again observed.

(3) Maximum number of authentication terminals

Points to note

Set the maximum number of terminals that can be authenticated in fixed VLAN mode.

For device settings, set this number by using global configuration mode, and to adjust the settings for ports, set this number by using the configuration mode corresponding to the ports.

Command examples

1.
```
(config)# interface fastethernet 0/4
(config-if)# mac-authentication static-vlan max-user 2
(config-if)# exit
```

Specifies that the maximum number of authentication terminals in port 0/4 is 2.

(4) Forced authentication ports

Points to note

Set ports that will be permitted for forced authentication in fixed VLAN mode.

Command examples

1.
```
(config)# interface fastethernet 0/4
(config-if)# mac-authentication static-vlan force-authorized
(config-if)# exit
```

Sets port 0/4 to a forced authentication port.

Notes

When using forced authentication, set only the RADIUS authentication method. Settings for forced authentication do not operate with the following settings:

- `aaa authentication mac-authentication default gourp radius local`
- `aaa authentication mac-authentication default local gourp radius`

(5) Setting roaming (allowing communication for moved ports of authenticated terminals)

Points to note

Set authentication terminals in fixed VLAN mode to be able to connect even if the terminals have been moved to other ports without linking down the port.

Command examples

1.
```
(config)# mac-authentication static-vlan roaming
```

Sets authentication terminals in fixed VLAN mode to be able to connect after moving to other ports.

Notes

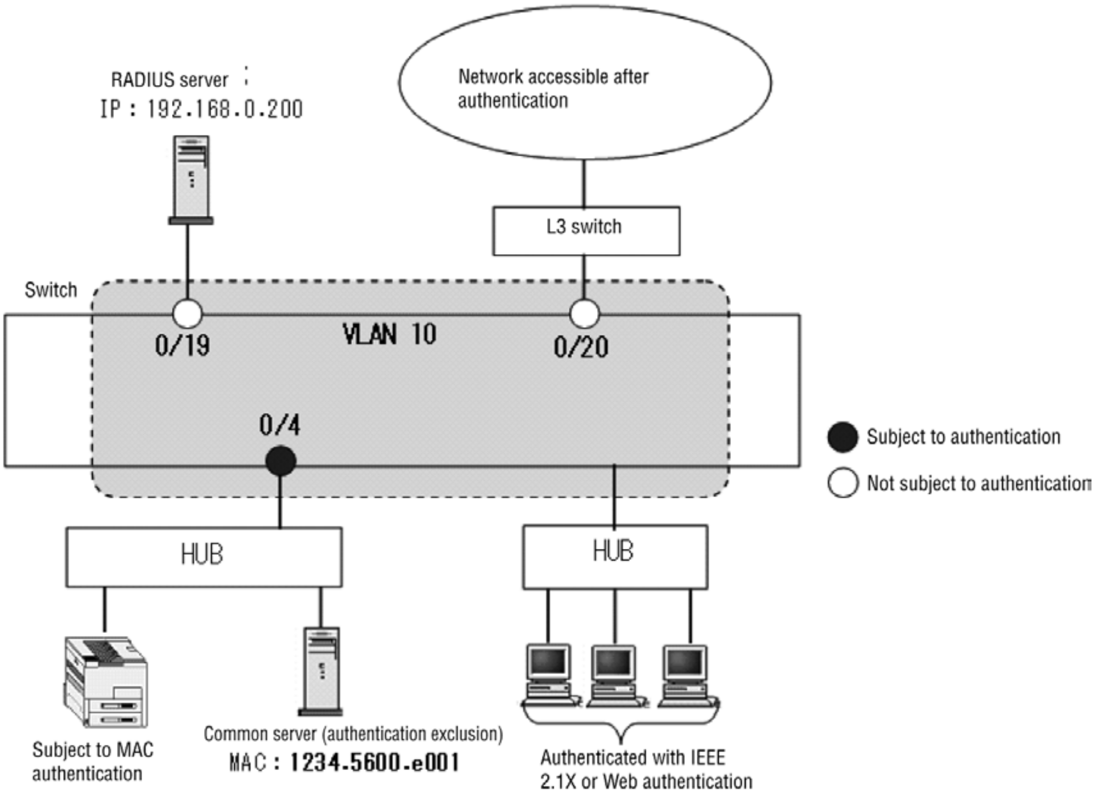
Roaming operates when the following conditions are met:

- Ports for fixed VLAN mode before and after moving
- The same VLAN before and after moving

(6) Authentication exemption

You can set ports and terminals in fixed VLAN mode to be excluded from authentication. In this example, ports 0/19, 0/20 and a shared server as illustrated in the following figure are set to be exempted from authentication.

Figure 11-5 Configuration example of authentication exemption in fixed VLAN mode



(a) Configuring ports exempted from authentication

Points to note

Prevent authentication mode from being set for ports exempted from authentication in fixed VLAN mode.

Command examples

1.
```
(config)# interface range fastethernet 0/19-20
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 10
(config-if-range)# exit
```

Sets ports 0/19 and 0/20 in VLAN ID 10 as access ports. No authentication mode is set (`mac-authentication port`).

(b) Terminals exempted from authentication

Points to note

Register MAC addresses into the MAC address table for MAC addresses of terminals exempted from authentication in fixed VLAN mode.

Command examples

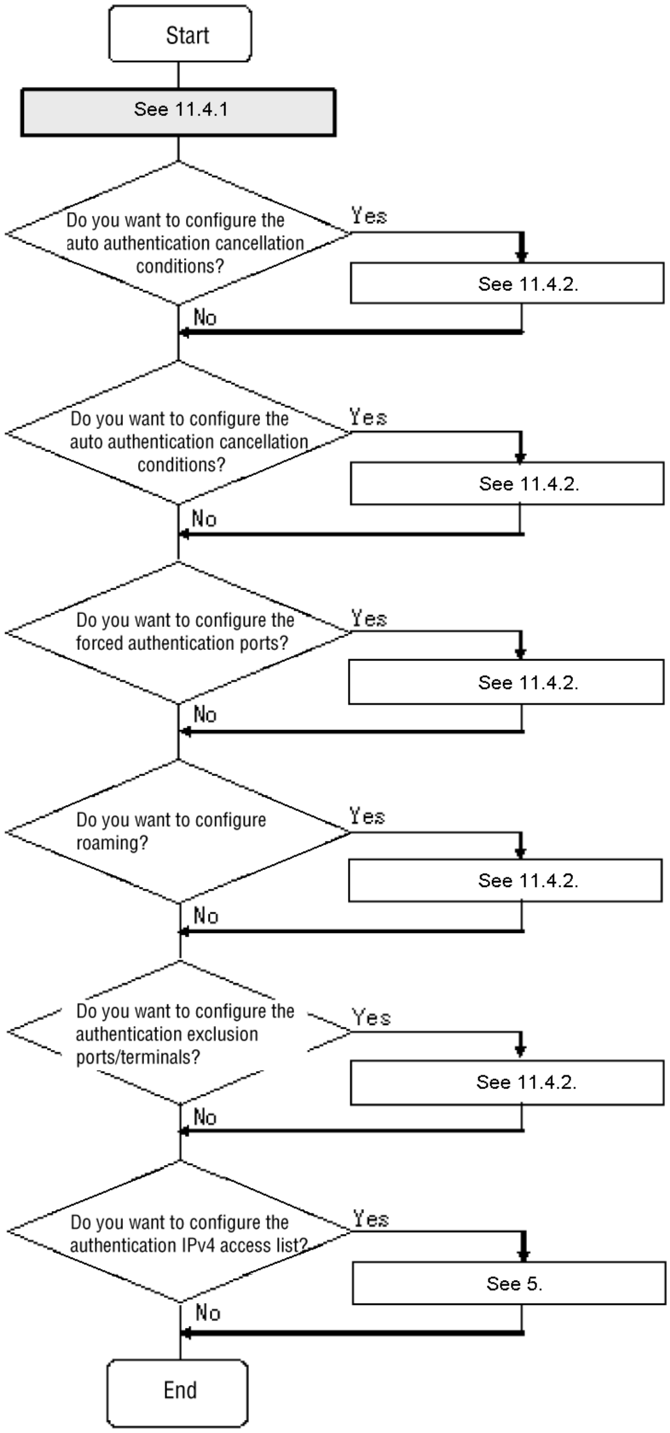
1.
```
(config)# mac-address-table static 1234.5600.e001 vlan 10
interface fastethernet 0/4
```

Sets the MAC address (MAC address of shared server: 1234.5600.e001 in the figure) of a terminal permitted to connect but exempt from authentication with port 0/4 in VLAN ID 10 to the MAC address table.

11.4 Configuring dynamic VLAN mode

Configure dynamic VLAN mode according to the following flow chart after a configuration based on *11.1 MAC-based authentication configuration* and *11.2 Configuration common to all authentication modes.*

Figure 11-6 Configuration procedure for dynamic VLAN mode

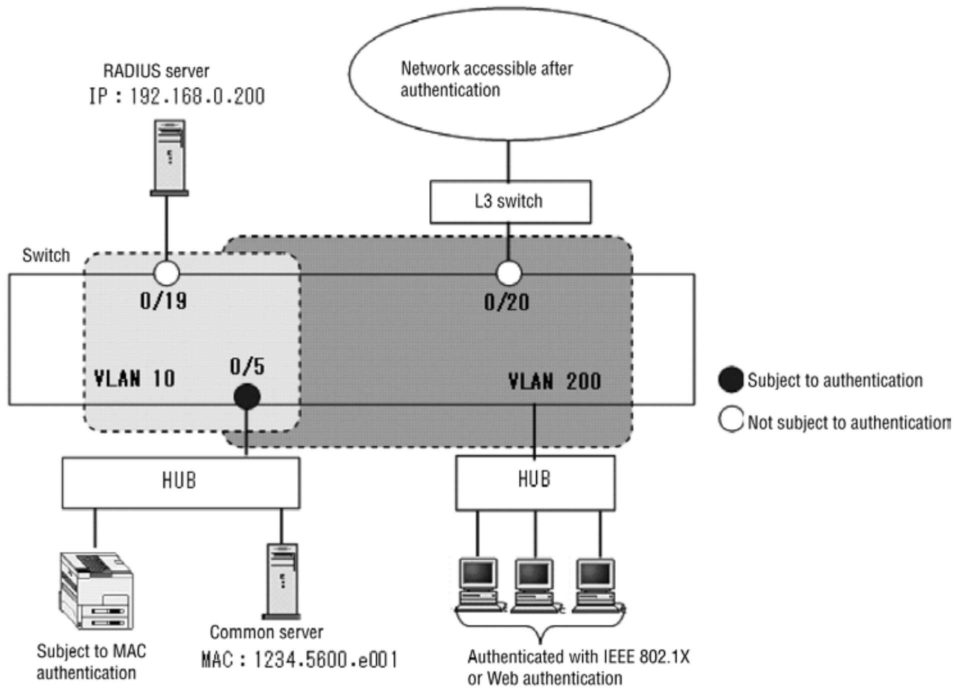


For details about the configuration, see the following:

1. Configuring dynamic VLAN mode: *11.4.1 Configuring dynamic VLAN mode*
2. Configuring automatic cancellation of authentication: *(1) Configuring the conditions for automatic cancellation of authentication* in *11.4.2 Configuration related to authentication processing*
3. Maximum number of authentication terminals: *(2) Maximum number of authentication terminals* in *11.4.2 Configuration related to authentication processing*
4. Configuring forced authentication ports*: (3) Forced authentication ports* in *11.4.2 Configuration related to authentication processing*
5. Configuring roaming: *(4) Setting roaming (allowing communication for moved ports of authenticated terminals)* in *11.4.2 Configuration related to authentication processing*
6. Configuring authentication exemption for ports or terminals: *(5) Authentication exemption* in *11.4.2 Configuration related to authentication processing*
7. Configuring the authentication IPv4 access list: *5.5.2 Configuring the authentication IPv4 access list*

11.4.1 Configuring dynamic VLAN mode

Figure 11-7 Configuration example of dynamic VLAN mode



(1) Configuring authentication ports and VLAN information for authentication

Points to note

Set dynamic VLAN mode and VLAN information for authentication for ports used for dynamic VLAN mode.

Command examples

1.
```
(config)# vlan 200 mac-based
(config-vlan)# exit
```
Configures VLAN ID 200 as a MAC VLAN.

2.
```
(config)# vlan 10
(config-vlan)# exit
```
Specifies VLAN ID 10.

3.
```
(config)# interface fastethernet 0/5
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 10
```
Sets port 0/5 where terminals for authentication are connected as a MAC port, and sets VLAN 10 for pre-authentication. (The post-authentication VLAN is assigned according to *5.4.3 Auto VLAN assignment for a MAC VLAN*.)

4.
```
(config-if)# mac-authentication port
(config-if)# exit
```
Sets port 0/5 to dynamic VLAN mode.

(2) Configuring authentication method list names for authentication method by port

Points to note

Sets the name of an authentication method list for the port-based authentication method.

For details about configuration of the authentication method list, see *(1) Configuring the authentication method group* in *11.2.1 Configuring the authentication method group and RADIUS server information.*

Command examples

1.
```
(config)# interface fastethernet 0/5
(config-if)# mac-authentication authentication MAC-list1
(config-if)# exit
```
Sets the authentication method list name `MAC-list1` to port 0/5.

Notes

- If this information has not been configured, authentication follows the Switch default as explained in *(1) Configuring the authentication method group* in *11.2.1 Configuring the authentication method group and RADIUS server information.*
- When a name of an authentication method list set for a port does not match the name of an authentication method list of an authentication

method group or is not present in an authentication method group, authentication will be performed according to the device default.

- The setting cannot be specified concurrently with the authentication method by user ID in Web authentication or legacy mode. For details, see *5.2.2 Authentication method list.*

11.4.2 Configuration related to authentication processing

The subsection describes settings concerning authentication processing for dynamic VLAN mode.

(1) Configuring the conditions for automatic cancellation of authentication

(a) Maximum connection time

This setting is common to all authentication modes in MAC-based authentication. See *11.2.3 Maximum connection time* in *11.2 Configuration common to all authentication modes.*

(b) Non-connection monitoring time for authentication terminals

Configuration is the same as for fixed VLAN mode. See *(b) Non-connection monitoring time for authentication terminals* in *(2) Configuring the conditions for automatic cancellation of authentication* in *11.3.2 Configuration related to authentication processing.*

(2) Maximum number of authentication terminals

Points to note

Set the maximum number of terminals that can be authenticated in dynamic VLAN mode.

For device settings, set this number by using global configuration mode, and to adjust the settings for ports, set this number by using the configuration mode corresponding to the ports.

Command examples

1.
```
(config)# interface fastethernet 0/5
(config-if)# mac-authentication max-user 2
(config-if)# exit
```

Specifies that the maximum number of authentication terminals for port 0/5 is 2.

(3) Forced authentication ports

Points to note

Allow forced authentication and assign a post-authentication VLAN to ports in dynamic VLAN mode.

Command examples

1.
```
(config)# interface fastethernet 0/5
(config-if)# mac-authentication force-authorized vlan 200
(config-if)# exit
```

Allows forced authentication at port 0/5 and specifies the VLAN ID of the post-authentication VLAN to be assigned.

Notes

1. By using the configuration command `vlan`, set the VLAN ID with the `mac-based` setting (MAC VLAN setting).
2. When using forced authentication, set only the RADIUS authentication method. Settings for forced authentication do not operate with the following settings:
   - `aaa authentication mac-authentication default gourp radius local`
   - `aaa authentication mac-authentication default local gourp radius`

(4) Setting roaming (allowing communication for moved ports of authenticated terminals)

Points to note

Set authentication terminals in dynamic VLAN mode to be able to connect even if the terminals have been moved to other ports without linking down the ports.

Command examples

1. `(config)# mac-authentication roaming`

   Sets authentication terminals in dynamic VLAN mode to be able to connect after moving to other ports.

Notes

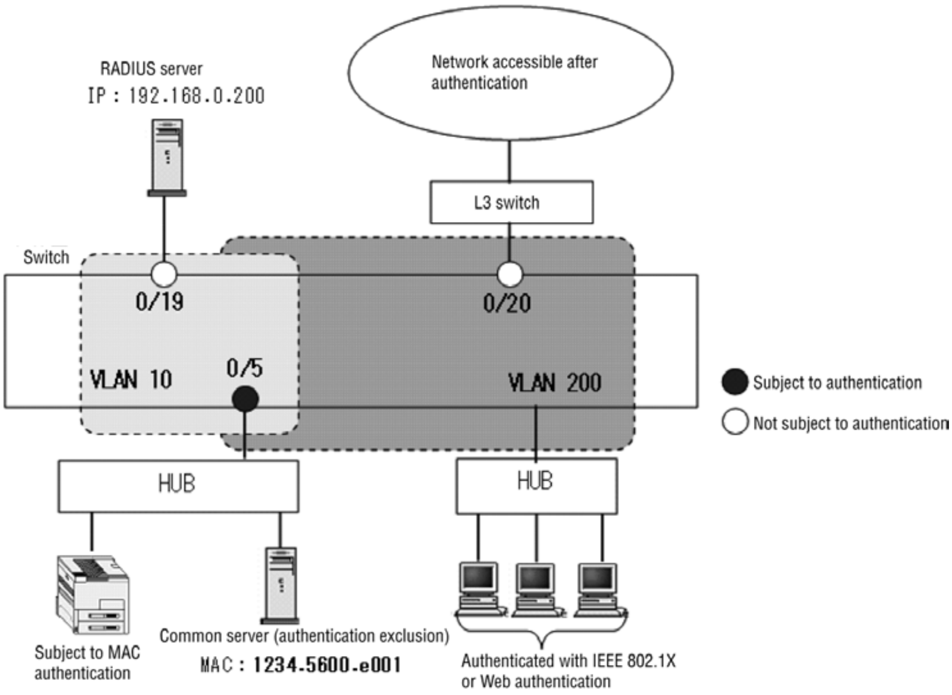
Roaming operates when the following conditions are met:

- Ports for dynamic VLAN mode before and after moving

(5) Authentication exemption

You can set ports and terminals in dynamic VLAN mode to be excluded from authentication. In this example, ports 0/19, 0/20 and a shared server as illustrated in the following figure are set to be exempted from authentication.

Figure 11-8 Configuration example of authentication exemption in dynamic VLAN mode



(a) Configuring ports exempted from authentication

Points to note

Set ports excluded from authentication as access ports. No authentication mode is specified.

Command examples

1.
```
(config)# interface fastethernet 0/19
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit
```
Sets port 0/19 in VLAN ID 10 as an access port. No authentication mode is set (`mac-authentication port`).

2.
```
(config)# interface fastethernet 0/20
(config-if)# switchport mode access
(config-if)# switchport access vlan 200
(config-if)# exit
```
Sets port 0/20 of MAC VLAN ID 200 as an access port. No authentication mode is set (`mac-authentication port`).

(b) Terminals exempted from authentication

Points to note

Register the MAC address of a terminal permitted to bypass authentication in a MAC VLAN and a MAC address table.

Command examples

1. `(config)# vlan 200 mac-based`

   `(config-vlan)# mac-address 1234.5600.e001`

   `(config-vlan)# exit`

   Sets a MAC address of a terminal exempted from authentication (MAC address of shared server: `1234.5600.e001` in the figure) to MAC VLAN ID 200.

2. `(config)# interface fastethernet 0/5`

   `(config-if)# switchport mode mac-vlan`

   `(config-if)# switchport mac vlan 200`

   `(config-if)# exit`

   Specifies MAC VLAN ID 200 to which the exempted terminal belongs for an authentication port.

3. `(config)# mac-address-table static 1234.5600.e001 vlan 200 interface fastethernet 0/5`

   Sets the MAC address (MAC address of shared server: `1234.5600.e001` in the figure) of a terminal permitted to connect but exempt from authentication with port 0/5 in MAC VLAN ID 200 to the MAC address table.

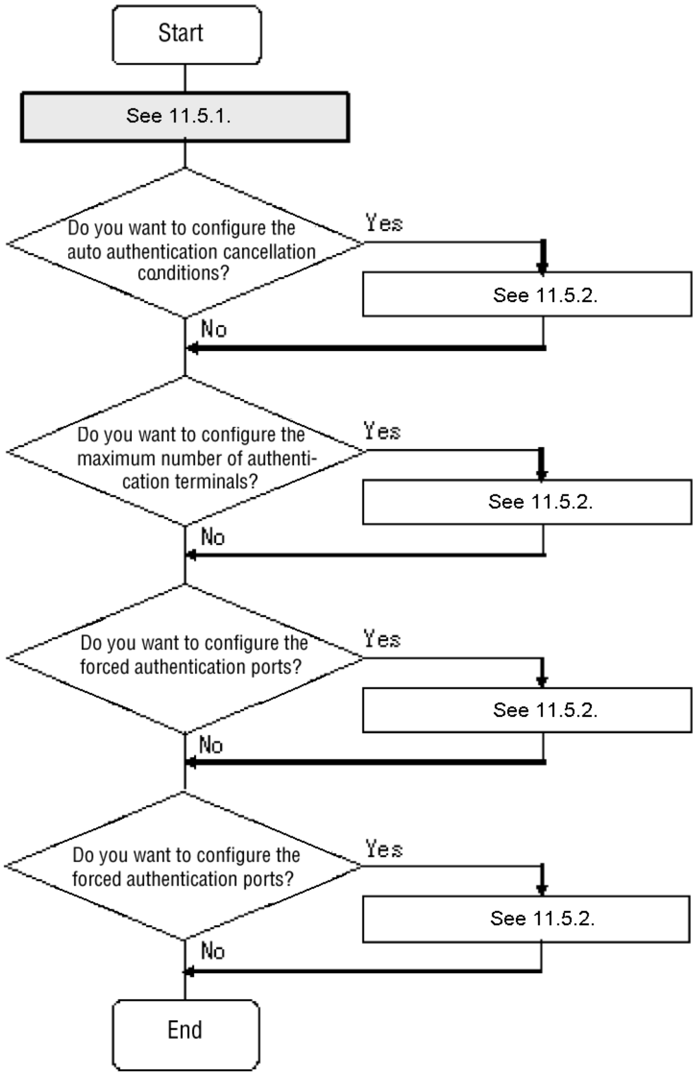
Notes

Before adding the MAC address of the terminal exempted from authentication to the MAC address table, set the VLAN ID of the MAC VLAN to the port to which the terminal belongs.

11.5 Configuring legacy mode

Configure legacy mode according to the following flow chart after a configuration based on *11.1 MAC-based authentication configuration* and *11.2 Configuration common to all authentication modes.*

Figure 11-9 Configuration procedure for legacy mode



For details about the configuration, see the following:

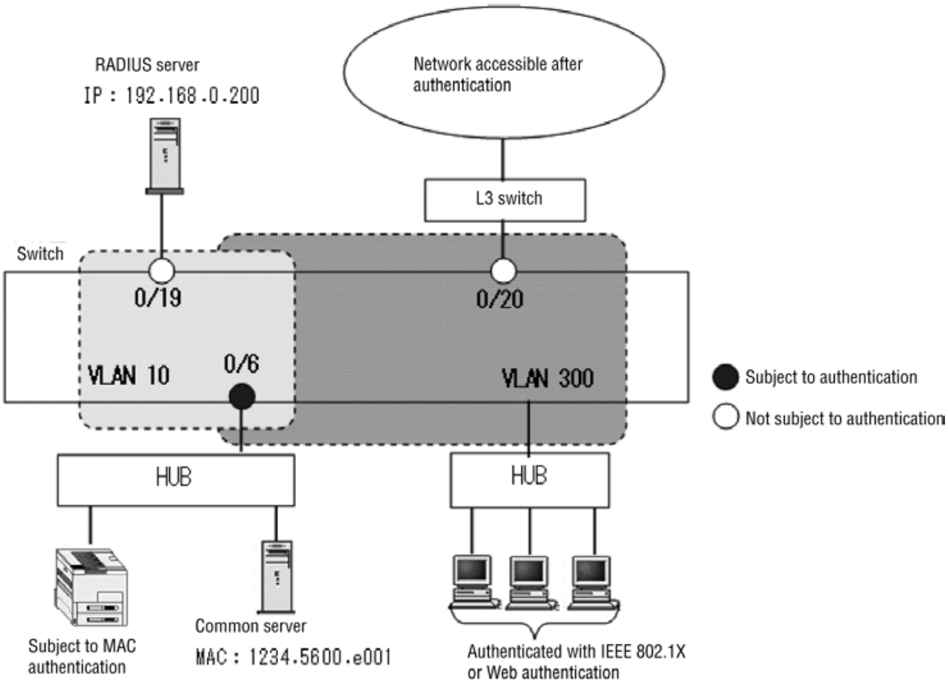
1. Configuring legacy mode: *11.5.1 Configuring legacy mode*
2. Configuring automatic cancellation of authentication: *(1) Configuring the conditions for automatic cancellation of authentication* in *11.5.2 Configuration related to authentication processing.*
3. Maximum number of authentication terminals: *(2) Maximum number of authentication terminals* in *11.5.2 Configuration related to authentication processing.*

4. Configuring forced authentication ports: *(3) Forced authentication ports* in *11.5.2 Configuration related to authentication processing.*

5. Configuring authentication exemption for ports or terminals: *(4) Authentication exemption* in *11.5.2 Configuration related to authentication processing.*

11.5.1 Configuring legacy mode

Figure 11-10 Configuration example for legacy mode



(1) Configuring ports for legacy mode

Points to note

Set the ports used for legacy mode.

Command examples

1. `(config)# mac-authentication interface fastethernet 0/6`

   Sets port 0/6 as a port for legacy mode.

(2) Configuring VLAN information for authentication ports

Points to note

Set VLAN information for authentication for the ports used for legacy mode.

Command examples

1. `(config)# vlan 300 mac-based`

   `(config-vlan)# exit`

   Configures VLAN ID 300 as a MAC VLAN.

2.
```
(config)# vlan 10
(config-vlan)# exit
```
Specifies VLAN ID 10.

3.
```
(config)# interface fastethernet 0/6
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 300
(config-if)# switchport mac native vlan 10
(config-if)# exit
```
Sets port 0/6 to which terminals for authentication are connected as a MAC port, and then sets the pre-authentication VLAN 10 and post-authentication VLAN 300.

(3) Configuring the post-authentication VLAN

Points to note

Set the post-authentication VLAN ID used for legacy mode. After authentication succeeds in legacy mode, the network is switched dynamically to the VLAN set by this command.

Command examples

1.
```
(config)# mac-authentication vlan 300
```
Sets the VLAN ID of the post-authentication VLAN of legacy mode.

Notes

When this information is not set, authentication in legacy mode fails. Set the target VLAN ID.

11.5.2 Configuration related to authentication processing

This subsection describes the settings for the authentication processing of legacy mode.

(1) Configuring the conditions for automatic cancellation of authentication

(a) Maximum connection time

This setting is common to all authentication modes in MAC-based authentication. See *11.2.3 Maximum connection time* in *11.2 Configuration common to all authentication modes.*

(b) Delay time between monitoring of MAC address aging and automatic cancellation of authentication

Points to note

For authentication terminals in legacy mode, set the delay time between when MAC address aging times out and automatic cancellation of authentication. The MAC address aging time is specified by the configuration command `mac-address-table aging-time`.

Command examples

1. `(config)# mac-authentication auto-logout delay-time 60`

   Sets the delay time between when MAC address aging times out and automatic cancellation of authentication to 60 seconds.

   If MAC-based authentication is enabled, this functionality operates by default (delay-time: 3600 seconds).

   If `no mac-authentication auto-logout` is specified, authentication is not canceled.

Notes

- When the time for automatic cancellation of authentication and the time for periodic re-authentication requests to the RADIUS server (`mac-authentication timeout reauth-period`) overlap, automatic cancellation of authentication is given higher priority.
- This setting is applied immediately. However, a delay of up to 60 seconds until the setting actually takes place occurs because monitoring of MAC address aging is on a 60-second cycle. When the value of `mac-authentication auto-logout delay-time` is changed from the current time to a shorter time, and terminals for which the changed delay time have elapsed are detected, automatic cancellation of authentication is executed. In this case, a delay of up to 60 seconds is again observed.

(2) Maximum number of authentication terminals

The configuration procedure is the same as for dynamic VLAN mode. See *(2) Maximum number of authentication terminals* in *11.4.2 Configuration related to authentication processing.*

(3) Forced authentication ports

Points to note

Allow forced authentication at a legacy mode port, and specify the post-authentication VLAN to be assigned.

Command examples

1. `(config)# interface fastethernet 0/6`

   `(config-if)# mac-authentication force-authorized vlan 300`

   `(config-if)# exit`

   Allows forced authentication at port 0/6 and specifies the VLAN ID of the post-authentication VLAN to be assigned.

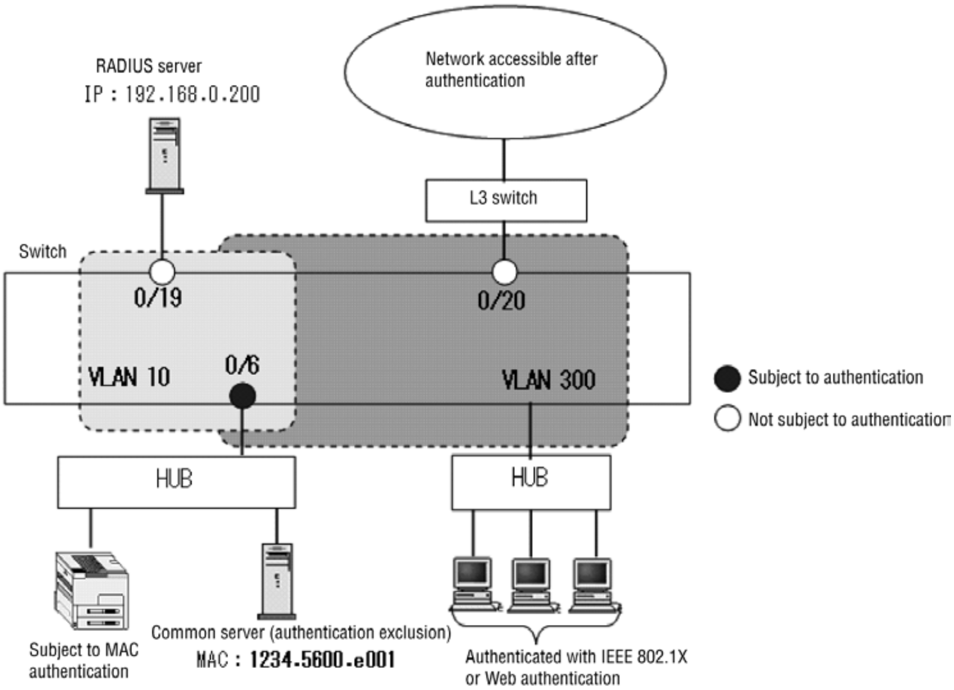
Notes

1. By using the configuration command `vlan`, set the VLAN ID with the `mac-based` setting (MAC VLAN setting).
2. When using forced authentication, set only the RADIUS authentication method. Settings for forced authentication do not operate with the following settings:
   - `aaa authentication mac-authentication default gourp radius local`
   - `aaa authentication mac-authentication default local gourp radius`

(4) Authentication exemption

You can set ports and terminals in legacy mode to be excluded from authentication. In this example, ports 0/19, 0/20 and a shared server as illustrated in the following figure are set to be exempted from authentication.

Figure 11-11 Configuration example of an authentication exemption in legacy mode



(a) Configuring ports exempted from authentication

Points to note

Designate the port where you wish to bypass authentication as an access port.

Command examples

1.
```
(config)# interface fastethernet 0/19
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit
```
Sets port 0/19 in VLAN ID 10 as an access port. No authentication mode is set (`mac-authentication port`).

2.
```
(config)# interface fastethernet 0/20
(config-if)# switchport mode access
(config-if)# switchport access vlan 300
(config-if)# exit
```
Sets port 0/20 in MAC VLAN ID 300 as an access port.

(b) Terminals exempted from authentication

Points to note

Register MAC addresses of terminals exempted from authentication to a MAC VLAN.

Command examples

1.
```
(config)# vlan 300 mac-based
(config-vlan)# mac-address 1234.5600.e001
(config-vlan)# exit
```

Sets a MAC address of a terminal exempted from authentication (MAC address of shared server: `1234.5600.e001` in the figure) in MAC VLAN ID 300.

11.6 MAC-based authentication operations

11.6.1 List of operation commands

The following table describes the operation commands for MAC-based authentication.

Table 11-3 List of operation commands

Command name	Description
`set mac-authentication mac-address`	Adds MAC addresses and information about post-authentication VLAN IDs for MAC-based authentication to the internal MAC-based authentication DB (edits MAC address information).
`remove mac-authentication mac-address`	Deletes MAC address information from the internal MAC-based authentication DB (edits MAC address information).
`commit mac-authentication`	Updates the internal MAC-based authentication DB with MAC address information that has been edited.
`store mac-authentication`	Backs up the internal MAC-based authentication DB to files.
`load mac-authentication`	Restores the internal MAC-based authentication DB from a backup file.
`show mac-authentication mac-address`	Displays the contents registered in the internal MAC-based authentication DB as well as any MAC address information that is being edited.
`show mac-authentication`	Displays the setting status of MAC-based authentication.
`show mac-authentication auth-state`	Displays the authentication status of MAC-based authentication
`show mac-authentication auth-state select-option`	Displays the authentication status of MAC-based authentication by selecting display options
`show mac-authentication auth-state summary`	Displays the number of authenticated terminals
`clear mac-authentication auth-state`	Forcibly cancels the authentication of authenticated MAC addresses.
`show mac-authentication login`	Displays the authentication status of MAC-based authentication (the displayed content is the same when specifying the operation command `show mac-authentication auth-state`).)

Command name	Description
show mac-authentication login select-option	Displays the authentication status of MAC-based authentication by selecting display options (The displayed content is the same as when specifying the operation command show mac-authentication auth-state select-option.)
show mac-authentication login summary	Displays the number of authenticated terminals (The displayed content is the same as when specifying the operation command show mac-authentication auth-state summary.)
show mac-authentication logging	Displays the operation log messages collected by MAC-based authentication.
clear mac-authentication logging	Clears the operation log messages collected by MAC-based authentication.
show mac-authentication statistics	Displays MAC-based authentication statistics.
clear mac-authentication statistics	Clears the MAC-based authentication statistics.

11.6.2 Registering an internal MAC-based authentication DB

You can register MAC address information (MAC addresses, post-authentication VLAN IDs) for authentication terminals used in the local authentication method to the internal MAC-based authentication DB. The procedure includes editing (adding and deleting) MAC address information and updating the internal MAC-based authentication DB. Shown below are examples of the registration.

Before adding MAC address information, you must finish setting up the environment for the MAC-based authentication system and configuration must be complete.

(1) Adding MAC address information

For each terminal to be authenticated, add MAC addresses and post-authentication VLAN IDs by using the operation command set mac-authentication mac-address. The following examples include a registration of only MAC addresses, and a registration of both MAC addresses and MAC masks.

Command entry (specifying MAC addresses)

```
# set mac-authentication mac-address 0012.e201.fff1 20
# set mac-authentication mac-address 0012.e202.fff1 30
```

Command entry (specifying both MAC addresses and MAC masks)

```
# set mac-authentication mac-address 0012.e201.0000 0000.0000.ffff 40
# set mac-authentication mac-address 0012.e202.0000 0000.0000.ffff 60
```

Command entry (specifying an any condition)

```
# set mac-authentication mac-address 0000.0000.0000 ffff.ffff.ffff 1
```

The above registration information is displayed as follows by using the operation command show mac-authentication mac-address. The information is displayed in ascending order by MAC address. However, registration of entries with only MAC addresses precedes registration of entries with MAC masks.

MAC address searches when using local authentication are executed by using the order given below.

Figure 11-12 Display of authentication status of internal MAC-based authentication DB

```
# show mac-authentication mac-address edit

Date 2008/11/13 17:40:02 UTC
 Total mac-address counts: 5
 mac-address     mac-mask         VLAN
 0012.e201.fff1  -                 20
 0012.e202.fff1  -                 30
 0012.e201.0000  0000.0000.ffff     40
 0012.e202.0000  0000.0000.ffff     60
 (any)          ffff.ffff.ffff      1

#
```

(2) Deleting MAC address information

Use the operation command `remove mac-authentication mac-address` to delete registered MAC address information. In the next example, information for a single user is deleted.

Command input

```
# remove mac-authentication mac-address 0012.e202.fff1 30
Remove mac-authentication mac-address.  Are you sure? (y/n): y

#
```

MAC address `0012.e202.fff1` and VLAN ID 30 are deleted.

(3) Updating the internal MAC-based authentication DB

Update the internal MAC-based authentication DB with edited MAC address information by using the operation command `commit mac-authentication`.

Command input

```
# commit mac-authentication
Commitment mac-authentication mac-address data.  Are you sure? (y/n): y

Commit complete.
#
```

11.6.3 Backing up and restoring the internal MAC-based authentication DB

The following example illustrates how to back up the internal MAC-based authentication DB and restore the database from the backup files.

(1) Backing up the internal MAC-based authentication DB

A backup file (`backupfile` in the following example) is created by using the operation command `store mac-authentication` from the internal MAC-based authentication DB.

Command input

```
# store mac-authentication ramdisk backupfile
Backup mac-authentication MAC address data.  Are you sure? (y/n): y
```

```
Backup complete.
#
```

Two files are automatically created (example when the file name is `backupfile`):

- `backupfile`: File that does not contain MAC mask information
- `backupfile.msk`: File that contains MAC mask information

(2) Restoring the internal MAC-based authentication DB

A backup file (`backupfile` in the following example) is restored by using the operation command `load mac-authentication` from the internal MAC-based authentication DB.

Command entry (restoring the internal MAC-based authentication DB that does not contain MAC mask information)

```
# load mac-authentication ramdisk backupfile
Restore mac-authentication MAC address data.  Are you sure? (y/n): y

Restore complete.
#
```

Command entry (restoring the internal MAC-based authentication DB that contains MAC mask information)

```
# load mac-authentication ramdisk backupfile.msk
Restore mac-authentication MAC address data.  Are you sure? (y/n): y

Restore complete.
#
```

11.6.4 Displaying setting status of MAC-based authentication

Use the operation command `show mac-authentication` to display the setting status of MAC-based authentication.

Figure 11-13 Displaying setting status of MAC-based authentication

```
# show mac-authentication

Date 2011/02/23 06:50:08 UTC
<<<MAC-Authentication mode status>>>
  Dynamic-VLAN     : Enable
  Static-VLAN      : Enable

<<<System configuration>>>
 * Authentication parameter
  Authentic-mode   : Dynamic-VLAN
  max-user        : 256
  id-format type   : xx-xx-xx-xx-xx-xx
  password        : Disable
  vlan-check      : -
  roaming         : Disable
  mac-authentication vlan :

 * AAA methods
  Authentication Default      : RADIUS
  Authentication port-list-BBB : RADIUS ra-group-2
  Authentication End-by-reject : Disable
```

```
 Accounting Default         : RADIUS

* Logout parameter
 max-timer       : infinity
 auto-logout     : 3600
 quiet-period    : 300
 reauth-period   : 3600

* Logging status
 [Syslog send]   : Disable
 [Traps]        : Disable

<Port configuration>
 Port Count          : 2

 Port               : 0/6
 VLAN ID            : 40
 Forceauth VLAN      : Disable
 Access-list-No      : L2-auth
 ARP relay          : Enable
 Max-user           : 256

 Port               : 0/22
 VLAN ID            : 40
 Forceauth VLAN      : Disable
 Access-list-No      : L2-auth
 ARP relay          : Enable
 Max-user           : 256
 Authentication method : port-list-BBB

<<<System configuration>>>
* Authentication parameter
 Authentic-mode   : Static-VLAN
 max-user        : 1024
 id-format type   : xx-xx-xx-xx-xx-xx
 password        : Disable
 vlan-check      : Disable
 roaming         : Disable
 mac-authentication vlan : -

* AAA methods
 Authentication Default      : RADIUS
 Authentication port-list-BBB : RADIUS ra-group-2
 Authentication End-by-reject : Disable
 Accounting Default         : RADIUS

* Logout parameter
 max-timer       : infinity
 auto-logout     : 3600
 quiet-period    : 300
 reauth-period   : 3600

* Logging status
 [Syslog send]   : Disable
 [Traps]        : Disable

<Port configuration>
 Port Count          : 3
```

```
  Port               : 0/5
  VLAN ID             : 4
  Forceauth VLAN       : Disable
  Access-list-No       : L2-auth
  ARP relay           : Enable
  Max-user            : 1024
  Authentication method : port-list-BBB

  Port               : 0/6
  VLAN ID             : 4
  Forceauth VLAN       : Disable
  Access-list-No       : L2-auth
  ARP relay           : Enable
  Max-user            : 1024

  Port               : 0/22
  VLAN ID             : 4
  Forceauth VLAN       : Disable
  Access-list-No       : L2-auth
  ARP relay           : Enable
  Max-user            : 1024
  Authentication method : port-list-BBB

#
```

11.6.5 Displaying status of MAC-based authentication

Use the operation command `show mac-authentication statistics` to display the status of MAC-based authentication and the status of communication with the RADIUS server.

Figure 11-14 Displaying MAC-based authentication statistics

```
# show mac-authentication statistics

Date 2009/10/28 09:12:44 UTC
MAC-Authentication Information:
  Authentication Request Total :       12
  Authentication Success Total :        6
  Authentication Fail Total    :       5
  Authentication Refuse Total  :        0
  Authentication Current Count :         1
  Authentication Current Fail  :        0

RADIUS MAC-Authentication Information:
[RADIUS frames]
  TxTotal   :       12  TxAccReq  :       11  TxError   :        1
  RxTotal   :       11  RxAccAccpt:       11  RxAccRejct:        0
                      RxAccChllg:       0  RxInvalid :        0
Account MAC-Authentication Information:
[Account frames]
  TxTotal   :       11  TxAccReq  :       11  TxError   :        0
  RxTotal   :       11  RxAccResp :       11  RxInvalid :        0

#
```

11.6.6 Displaying the status of MAC-based authentication sessions

(1) Displaying without specifying display options

Use the operation command `show mac-authentication auth-state` to display the authentication status of MAC-based authentication.

The same content can also be displayed by using the operation command `show mac-authentication login`.

Figure 11-15 Displaying the status of MAC-based authentication sessions

```
# show mac-authentication auth-state

Date 2009/03/24 17:14:56 UTC
 Dynamic VLAN mode total client counts(Login/Max):   1 / 256
  Authenticating client counts :    0
  Hold down client counts      :    0
  Port roaming : Disable
   No F MAC address     Port VLAN  Login time          Limit     Reauth
    1 * 00d0.5909.7121  0/20  200  2009/03/24 17:14:55   infinity    3598

 Static VLAN mode total client counts(Login/Max):    1 / 1024
  Authenticating client counts :    0
  Hold down client counts      :    0
  Port roaming : Disable
   No F MAC address     Port VLAN  Login time          Limit     Reauth
    1   0000.e28c.4add  0/10   10  2009/03/24 17:14:38   infinity    3582

#
```

(2) Displaying by specifying display options (specifying select-option)

Use the operation command `show mac-authentication auth-state select-option` to display the authentication status of MAC-based authentication with display option specified. The following example illustrates an implementation where an interface port number is specified.

The same content can also be displayed by using the operation command `show mac-authentication login select-option`.

Figure 11-16 Displaying information when specifying ports

```
# show mac-authentication auth-state select-option port 0/20

Date 2009/03/24 17:15:14 UTC
 Dynamic VLAN mode total client counts(Login/Max):   1 / 256
  Authenticating client counts :    0
  Hold down client counts      :    0
  Port roaming : Disable
   No F MAC address     Port VLAN  Login time          Limit     Reauth
    1 * 00d0.5909.7121  0/20  200  2009/03/24 17:14:55   infinity    3580

#
```

(3) Displaying only the number of authenticated terminals (summary display)

Use the operation command `show mac-authentication auth-state summary` to display the number of terminals authenticated by MAC-based authentication.

The same content can also be displayed by using the operation command `show mac-authentication login summary`.

Figure 11-17 Display of the number of authenticated terminals

```
# show mac-authentication auth-state summary port

Date 2009/03/24 17:16:56 UTC
 Dynamic VLAN mode total client counts(Login/Max):   1 / 256
  Authenticating client counts :    0
  Hold down client counts     :    0
  Port roaming : Disable
   No  Port  Login /  Max
    1  0/20     1 /  256

 Static VLAN mode total client counts(Login/Max):    1 / 1024
  Authenticating client counts :    1
  Hold down client counts     :    0
  Port roaming : Disable
   No  Port  Login /  Max
    1  0/10     1 / 1024

#
```

12. Multistep Authentication

The Switch supports multistep authentication, which performs terminal authentication and user authentication in two steps. This chapter describes multistep authentication.

12.1 Description

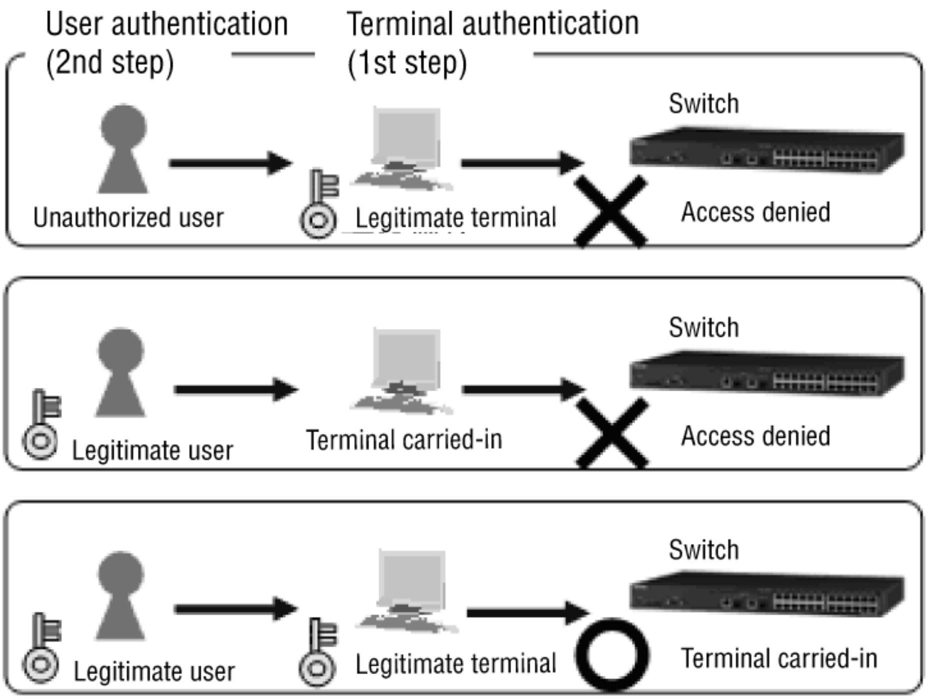
This functionality grants access only to registered users using legitimate terminals in two stages of authentication.

- Allows the user of the legitimate terminal who completes the first stage of authentication to complete the second stage of user authentication.
- Grants access to registered users who have completed the second stage of user authentication.

In this way, access by unauthenticated users or via a portable terminal is prevented.

The following figure shows an overview of multistep authentication.

Figure 12-1 Overview of multistep authentication



The Switch uses the following Layer 2 authentication methods for the first-step terminal authentication (hereinafter *terminal authentication*) and the second-step user authentication (hereinafter *user authentication*):

- Terminal authentication: MAC-based authentication, IEEE 802.1X
- User authentication: IEEE 802.1X, Web authentication

Although there is no functionality in setting up multistep authentication independently, the following functionality addresses terminals subject to authentication:

- Forced authentication: See *(8) Forced authentication* in *12.1.2 Authentication behavior.*
- Moving authenticated terminals between ports: See *(10) Roaming (moving authenticated terminals between ports)* in *12.1.2 Authentication behavior.*

- Displaying authentication status, accounting logs, and traps: See *(11) Displaying status, accounting logs, and traps* in *12.1.2 Authentication behavior.*

12.1.1 Scope of support

(1) Authentication modes

Multistep authentication is available only by using the RADIUS authentication method. The following table provides the authentication modes for multistep authentication.

Table 12-1 Authentication modes used in multistep authentication

Authentication type	Authentication method group#	Authentication mode
MAC-based authentication and IEEE 802.1X	Switch default Authentication method list	Fixed VLAN mode Dynamic VLAN mode
MAC-based authentication and Web authentication	Switch default Authentication method list	Fixed VLAN mode Dynamic VLAN mode
IEEE 802.1X and Web authentication	Switch default Authentication method list	Fixed VLAN mode Dynamic VLAN mode

#

If you set up either of the authentication method groups, they operate by RADIUS authentication.

Multistep authentication is not available in legacy mode. Therefore, the configuration for legacy mode in the following table cannot be set up with the configuration of multistep authentication at the same time.

Table 12-2 Legacy mode configurations that cannot be used with multistep authentication

Authentication type	Configuration command
IEEE802.1X	`dot1x vlan dynamic enable` `dot1x vlan dynamic radius-vlan`
Web authentication	`web-authentication vlan`
MAC-based authentication	`mac-authentication interface` `mac-authentication vlan`

(2) Expected user or terminal

This manual defines the expected users and terminals where connection to the multistep authentication port as follows.

Table 12-3 Definition of expected users and terminals

Expected user or terminal	Authentication required for communication	Authentication type
Printer	Terminal authentication only	Single authentication
Employee user	Terminal authentication and user authentication	Multistep authentication
Guest user	User authentication only	Single authentication

(3) Options for multistep authentication

Multistep authentication supports basic multistep authentication and the option categories that are shown in the following table.

Table 12-4 Option categories of multistep authentication

Terminal authentication	User authentication	Option categories of multistep authentication	Configuration	Remarks
MAC-based authentication	IEEE802.1X Web authentication	Basic multistep authentication	`authentication multi-step`	Users are authenticated after successful terminal authentication.
MAC-based authentication	IEEE802.1X Web authentication	Authorized user authentication option	`authentication multi-step permissive`	Users are authenticated even if terminal authentication fails.
IEEE802.1X MAC-based authentication	Web authentication	Terminal authentication dot1x option	`authentication multi-step dot1x`	Users are authenticated after successful terminal authentication. IEEE 802.1X is added to terminal authentication.

(a) Authorized user authentication option

The settings for user authentication for the Switch have the option for authorized user authentication. Basically, the user has the opportunity for authentication after successful terminal authentication, but an employee user and a guest user can coexist in a single multistep authentication port with these optional settings.

The table below shows the configuration of multistep authentication and whether terminal or user authentication are supported.

Table 12-5 Configuration of multistep authentication and availability of terminal or user authentication

Multistep authentication settings	Authorized user authentication option settings	Printer	Employee user	Guest user
Yes	No	S	M	N
	Yes	S	M#	S#
No	--	S	S	S

Legend

M: Multistep authentication

S: Single authentication

N: User authentication is unavailable.

--: Not applicable

#

The multistep authentication port can carry out user authentication even if terminal authentication fails. However, this depends on the `Filter-Id` RADIUS attribute, terminal authentication success is required for the specific user ID (an employee user), and authentication can be completed without terminal authentication for the specific user (a guest user).

(b) Terminal authentication dot1x option

This option adds IEEE 802.1X to terminal authentication. Basically, user authentication is allowed after successful MAC-based authentication, and user authentication (this case, only Web authentication) is allowed when terminal authentication IEEE 802.1X has succeeded by setting this option.

- The port is set up with this option, as a terminal authentication, and then executes MAC-based authentication and IEEE 802.1X at the same time.
- The port with this option is allowed user authentication when terminal authentication succeeds.
- This option and the authorized user authentication option cannot be set up on a single port.

(4) Authentication functionality behavior on a single port

The table below shows the behavior of authentication functionality on the same multistep authentication settings port.

Table 12-6 Behavior of authentication functionality on the same multistep authentication settings port

Multistep authentication port settings and option categories	Terminal authentication			User authentication			Expected user or terminal
	Filter-Id RADIUS attribute support	Permit MAC-based authentication	Permit IEEE 802.1X#	Filter-Id RADIUS attribute support	Permit IEEE 802.1X	Permit Web authentication	

Multistep authentication port settings and option categories	Terminal authentication			User authentication			Expected user or terminal
	Filter-Id RADIUS attribute support	Permit MAC-based authentication	Permit IEEE 802.1X#	Filter-Id RADIUS attribute support	Permit IEEE 802.1X	Permit Web authentication	
Basic multistep authentication port	No	S	--	--	--	--	Printer
	Yes	P	--	No	M	M	Employee user
				Yes	M	M	Employee user
Port with authorized user authentication option	No	S	--	--	--	--	Printer
	Yes	P	--	No	S	S	Guest user
				Yes	M	M	Employee user
Port with terminal authentication dot1x option	No	S	S	--	--	--	Printer
	Yes	P	P	No	--	M	Employee user
				Yes	--	M	Employee user
Port not set (single authentication)	--	S	--	--	S	S	--

Legend

M: Multistep authentication

S: Single authentication

P: Waits for the result of user authentication (pending)

--: Not applicable

#

For example, IEEE 802.1X computer authentication

12.1.2 Authentication behavior

(1) MAC-based authentication events

There is a difference in the frame that should be used for authentication in MAC-based authentication between the multistep authentication port and the single authentication port.

In the table below, multistep authentication of all of the frames, including EAPOL frames or HTTP/HTTPS frames, are MAC-based authentication with or without IEEE 802.1X settings and Web authentication configuration on the multistep authentication port.

On a single authentication port, EAPOL frames should use MAC-based authentication if IEEE 802.1X is not configured, and HTTP/HTTPS frames should use MAC-based authentication if Web authentication is not configured.

The following table provides the frame for the authentication in MAC-based authentication.

Table 12-7 Frame of the multistep authentication configuration and MAC-based authentication

Frame type	**EAPOL**		**HTTP/HTTPS**	
Prot settings	**IEEE 802.1X Yes**	**IEEE 802.1X No**	**Web authentication Yes**	**Web authentication No**
Multistep authentication configured	Y	Y	Y	Y
Multistep authentication not configured (Single authentication port)	N	Y	N	Y

Legend

Y: Subject to MAC-based authentication

N: Not subject to MAC-based authentication

(2) Determination of authentication behavior based on the Filter-Id RADIUS attribute

When the multistep authentication receives authentication success (`Accept`) from a RADIUS server, the Switch determines the authentication behavior of the next stage from the character string of the `Filter-Id` RADIUS attribute.

The table below provides the strings of the `Filter-Id` RADIUS attribute in multistep authentication.

Table 12-8 Character string of Filter-Id RADIUS attribute in multistep authentication

Character string of the Filter-Id RADIUS attribute	**Description**	**Authentication functionality to determine the character string of the Filter-Id RADIUS attribute**
`@@1X-Auth@@`	Authorizing the authentication behavior of IEEE 802.1X	MAC-based authentication
`@@Web-Auth@@`	Authorizing authentication behavior of Web authentication	IEEE 802.1X#1, MAC-based authentication
`@@MultiStep@@`	Authorizing authentication behavior of IEEE 802.1X and Web authentication (User executes either authentication)	IEEE 802.1X#1, #2, MAC-based authentication
`@@MAC-Auth@@`	MAC-based authentication is required.	IEEE 802.1X, Web authentication

#1

When terminal authentication dot1x option is configured

#2

When the terminal is authenticated by IEEE 802.1X, it uses only web authenticated user authentication even if `Filter-Id` is `@@MultiStep@@`.

(3) Behavior of basic multistep authenticated ports

Terminal authentication and user authentication can be performed by the following methods on the basic multistep authenticated port.

1. Terminal authentication waits for the next user authentication when terminal authentication succeeds with the character strings below of the `Filter-Id` RADIUS attribute. In this case, the MAC address of the target terminals is not registered as authentication entries in the MAC address table. (Ports without the character strings below are subject to single authentication, and then the MAC address of the target terminals are registered as authentication entries in the MAC address table.)
   - `@@1X-Auth@@`
   - `@@Web-Auth@@`
   - `@@MultiStep@@`
2. User authentication is permitted after successful terminal authentication. The authentication is completed after a successful user authentication that does not depend on the result of the `Filter-Id` RADIUS attribute. The terminal can access the Switch when the MAC address of the target terminal is registered as an authentication entry in the MAC address table.

   In addition, when an authentication functionality registers the MAC address as an authentication entry in the MAC address table, the `show mac-address table` operation command displays the following authentication functionality in the MAC address table entry.
   - IEEE 802.1X (`Dot1x`)
   - Web authentication (`WebAuth`)
   - MAC-based authentication (`MacAuth`)

   MAC address entries that show (`Static`) are entries that were registered by using the `mac-address-table static` configuration command.

   Terminals that have not finished authentication are shown as (`Dynamic`).
3. Available authentication functionality on this port

   The table below shows the authentication functionality available on a basic multistep authentication port.

Table 12-9 Authentication functionality available on basic multistep authentication ports

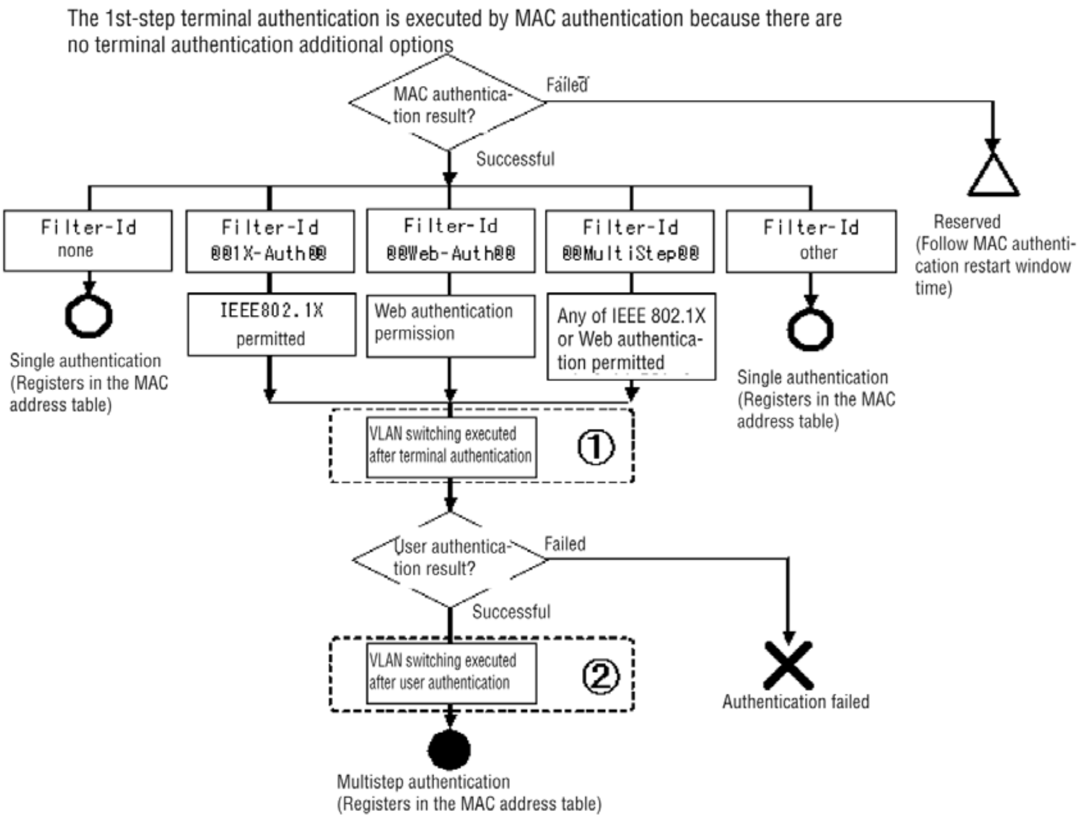
Terminal authentication	User authentication	Terminal management
MAC-based authentication: Success	No user authentication	Single authentication
MAC-based authentication: Success	IEEE 802.1X: Success	Multistep authentication

Terminal authentication	User authentication	Terminal management
MAC-based authentication: Success	Web authentication: Success	Multistep authentication

The Switch can only support the above combinations.

The following figure shows the behavior of the multistep authentication port.

Figure 12-2 Authentication behavior of basic multistep authenticated ports



In dynamic VLAN mode, when terminal or user authentication is successful, the terminal is assigned to the VLAN ((i) and (ii) in Figure 12-2).

Even if the user authentication failed, the status of the VLAN assigned at terminal authentication ((i) in Figure 12-2) is preserved.

The Switch monitors an authenticated terminal, and if the Switch consistently finds that there has been no access from the terminal, it cancels the authentication status, and the assigned VLAN reverts to the pre-authentication VLAN (native VLAN).

(4) Authentication behavior of ports with the authorized user authentication option

If employee users and guest users use the same port for multistep authentication, the `authentication multi-step` configuration command specifies `permissive` as the authorized user authentication option.

The port for which authorized user authentication is specified allows user authentication (IEEE 802.1X or Web authentication), even if terminal authentication

(MAC-based authentication) on the first stage has failed.

Then, user authentication can be performed when terminal authentication (MAC-based authentication) failed (retained entry). Therefore, specify more than 0 seconds for the re-authentication retry interval for MAC-based authentication (`mac-authentication timeout quiet-period`). (The default interval is 300 seconds.)

The following table shows the authentication functionality available on ports with the authorized user authentication option.

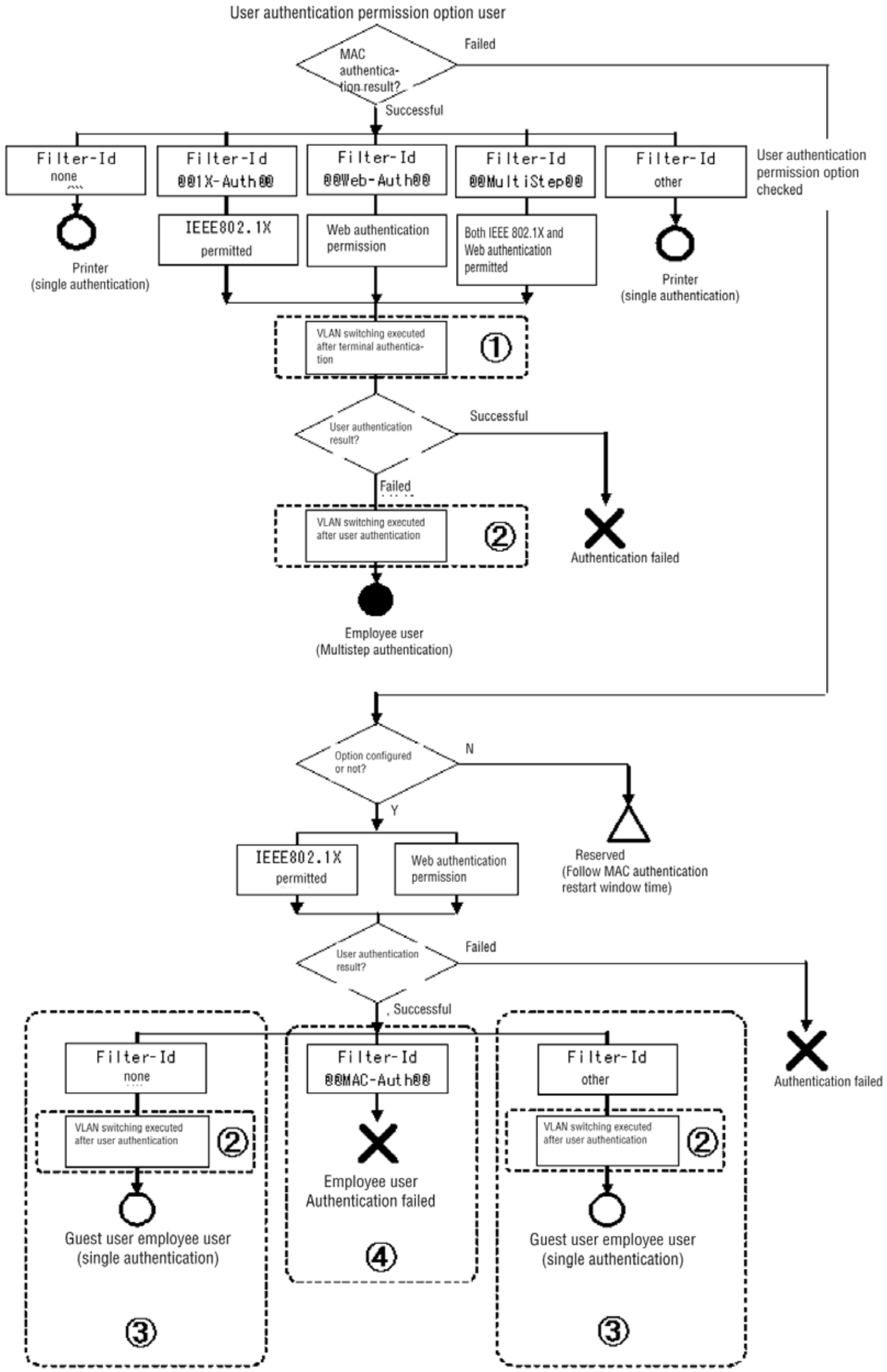
Table 12-10 Authentication functionality on ports with the authorized user authentication option

Terminal authentication	User authentication	Terminal management
MAC-based authentication: Success	No user authentication	Single authentication
MAC-based authentication: Success	IEEE 802.1X: Success	Multistep authentication
MAC-based authentication: Success	Web authentication: Success	Multistep authentication
MAC-based authentication: Failure	IEEE 802.1X: Success	Single authentication
MAC-based authentication: Failure	Web authentication: Success	Single authentication

The Switch can only support the above combinations.

The following figure shows the authentication behavior of ports with the authorized user authentication option.

Figure 12-3 Authentication behavior of the authorized user authentication option on a multistep authentication port



In dynamic VLAN mode, when terminal or user authentication is successful, the terminal is assigned to the VLAN ((i) and (ii) in Figure 12-2).

Even if the user authentication failed, the status of the VLAN assigned at terminal authentication ((i) in Figure 12-3) is preserved.

The Switch monitors an authenticated terminal, and if the Switch consistently finds that there has been no access from the terminal, it cancels the authentication status, and the assigned VLAN reverts to the pre-authentication VLAN (native VLAN).

If the Switch authenticates an employee user on the port that already has authorized user authentication, then the employee user is authenticated by user authentication ((iii) in Figure 12-3). In this case, configure `"@@MAC-Auth@@"` for the `Filter-Id` RADIUS attribute on the RADIUS server for user authentication. This will allow you to assign the authentication status of employee users to failed authentication ((iv) in Figure 12-3) when terminal authentication has failed on ports for which the authorized user authentication option is configured.

The table below shows the `Filter-Id` RADIUS attribute received on a port with the authorized user authentication option and the authentication behavior of user authentication.

Table 12-11 Authentication behavior of ports with the authorized user authentication option

Filter-Id RADIUS attribute received by user authentication	**Terminal authentication result**	**Authentication behavior of user authentication**	**Expected user**
No	--	Define the user not required MAC-based authentication: user authentication succeeds.	Guest user
`@@MAC-Auth@@`	succeeded	Define the user required MAC-based authentication. MAC-based authentication succeeds: user authentication succeeds.	Employee user
	failed	Define the user required MAC-based authentication. MAC-based authentication failed: user authentication failed.	Unauthorized user
All other cases	--	Define the user not required MAC-based authentication: user authentication succeeds.	Guest user

Legend

--: Not dependent on terminal authentication result

(5) Authentication behavior on a port with the terminal authentication dot1x option

Terminal authentication and user authentication can be performed with the following methods on ports with the terminal authentication dot1x option:

1. Terminal authentication waits for the next user authentication when terminal authentication succeeds with the character strings below of the `Filter-Id` RADIUS attribute. In this case, the MAC address of the target terminals is not registered as authentication entries in the MAC address table. (Ports without the character strings below are subject to single authentication, and then the

MAC address of the target terminals are registered as authentication entries in the MAC address table.)

- @@Web-Auth@@
- @@MultiStep@@

2. User authentication is permitted after successful terminal authentication. The authentication is completed after a successful user authentication that does not depend on the result of the Filter-Id RADIUS attribute. The terminal can access the Switch when the MAC address of the target terminal is registered as an authentication entry in the MAC address table.

   In addition, when an authentication functionality registers the MAC address as an authentication entry in the MAC address table, the show mac-address table operation command displays the following authentication functionality in the MAC address table entry.

   - IEEE 802.1X (Dot1x)
   - Web authentication (WebAuth)
   - MAC-based authentication (MacAuth)

   MAC address entries that show (Static) are entries that were registered by using the mac-address-table static configuration command.

   Terminals that have not finished authentication are shown as (Dynamic).

3. Available authentication functionality on this port

   The following table shows the authentication functionality on ports with the terminal authentication dot1x option.

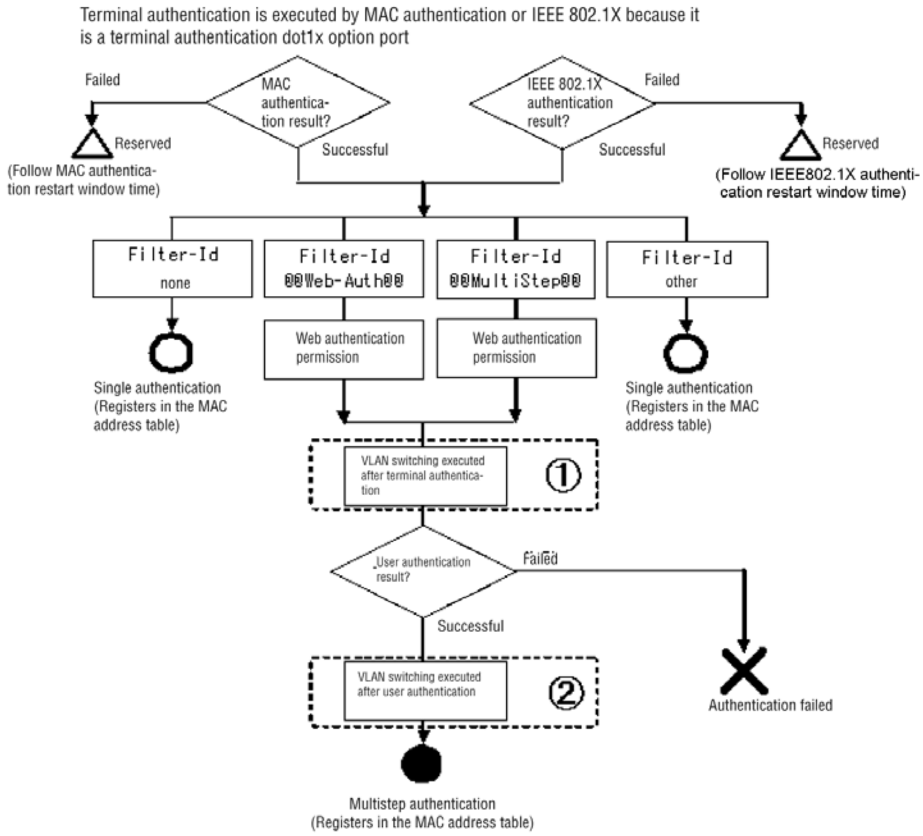
Table 12-12 Authentication functionality on ports with the terminal authentication dot1x option

Terminal authentication	**User authentication**	**Terminal management**
MAC-based authentication: Success	No user authentication	Single authentication
IEEE 802.1X: Success	No user authentication	Single authentication
MAC-based authentication: Success	Web authentication: Success	Multistep authentication
IEEE 802.1X: Success	Web authentication: Success	Multistep authentication

The Switch can only support the above combinations.

The following figure shows the authentication behavior of ports with the terminal authentication dot1x option.

Figure 12-4 Authentication behavior on a port with the terminal authentication dot1x option



In dynamic VLAN mode, when terminal or user authentication is successful, the terminal is assigned to the VLAN (① and ② in *Figure 12-4*).

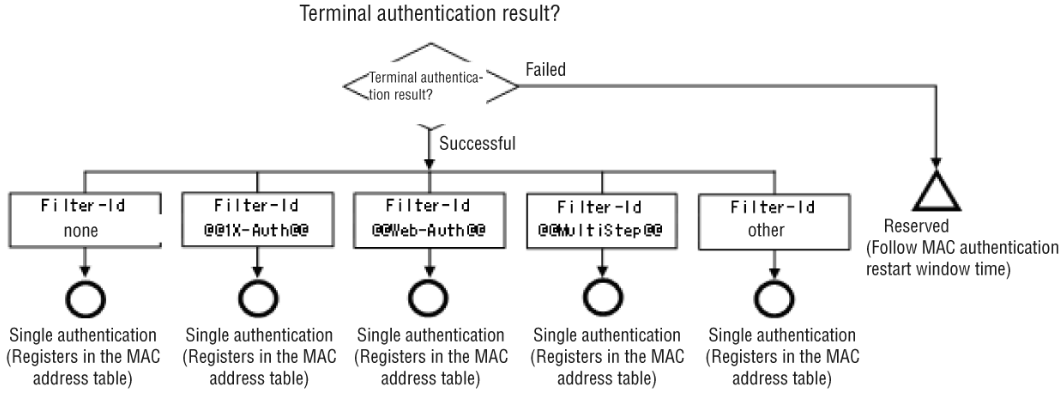
Even if the user authentication failed, the status of the VLAN assigned at terminal authentication (① in *Figure 12-4*) is preserved.

The Switch monitors an authenticated terminal, and if the Switch consistently finds that there has been no access from the terminal, it cancels the authentication status, and the assigned VLAN reverts to the pre-authentication VLAN (native VLAN).

(6) Authentication behavior of ports not configured for multistep authentication (single authentication ports)

The following figure shows the authentication behavior of a port not configured for multistep authentication.

Figure 12-5 Authentication behavior of a port not configured for multistep authentication



Even if one of the following character strings has been specified for `Filter-Id`, the port is handled with single authentication:

- `@@1X-Auth@@`
- `@@Web-Auth@@`
- `@@MultiStep@@`

(7) Post-authentication VLAN

In dynamic VLAN mode, when terminal or user authentication is successful, the terminal is assigned the VLAN sent by the RADIUS server for terminal and user authentication. For details about configuring the VLAN information to the RADIUS server, see *12.1.3 Preparation.*

(8) Forced authentication

The target terminals for which forced authentication is enabled use the following authentication.

Table 12-13 Authentication for target terminals with forced authentication

Multistep authentication port option	Forced authentication with terminal authentication	Forced authentication with user authentication
Basic multistep authentication	Single authentication	Multistep authentication
Authorized user authentication option	Single authentication	Single authentication
Terminal authentication dot1x option	Single authentication	Multistep authentication

The following VLANs are associated with forced authentication terminals.

Table 12-14 VLANs associated with target forced authentication terminals

Port type	Configuration VLAN for forced authentication	VLAN
Access port	n/a	Fixed VLAN

Port type	Configuration VLAN for forced authentication	VLAN
Trunk port	n/a	Fixed VLAN
MAC port	Yes	Depends on VLAN assigned by configuration.
	No	Native VLANs
MAC port (when `dot1q vlan` is configured)	n/a	Fixed VLAN

(9) Managing authenticated terminals and de-authentication

(a) Managing multistep authenticated terminals

The Switch manages the authenticated terminal according to the final authentication status. If the terminal has been authenticated by terminal authentication and is then authenticated by user authentication, the terminal is managed by user authentication. The Switch manages the terminal with the final authentication status when it has been authenticated by single authentication even for multistep authentication ports.

(b) De-authentication of multistep authenticated terminals

Canceling the authentication status on the multistep authenticated terminal depends on the de-authentication condition of user authentication. When the terminal is authenticated by single authentication on a multistep authentication port, it will be de-authenticated according to the de-authentication condition of the authentication functionality used. For details about the clearing authentication status, see the description of each authentication functionality.

If the Switch receives an EAPOL-Start frame on ports with the terminal authentication dot1x option, it forcibly cancels the Web authentication status of the authenticated terminal. (If the terminal is authenticated by MAC-based authentication, and Web authentication receives an EAPOL-Start frame on the same port, the terminal will be forcibly de-authenticated.)

(c) Monitoring non-communication of a multistep authenticated terminal

The following non-communication monitoring operations are applied to authenticated terminals on multistep authentication ports depending on their status:

- Authenticated terminals are monitored for non-communication.
- Terminals waiting to be authenticated are monitored for MAC address table aging.
- Entries of terminals that failed to authenticate are held for a period of time.

The table below shows the status of the terminal and monitoring methods for non-communication.

Table 12-15 Terminal status and monitoring methods for non-communication

Terminal status	Authentication status	MAC-based authentication	IEEE 802.1X	Web authentication
Authentication completed	Multistep authentication (user authentication completed)	--	Non-communication monitoring time	Non-communication monitoring time
	Single authentication	Non-communication monitoring time	Non-communication monitoring time	Non-communication monitoring time
Waiting for authentication	Terminal authentication succeeds[#1] (waits for user authentication to complete)	MAC address table aging monitoring time	MAC address table aging monitoring time	--
	Quarantined[#1, #2]	--	MAC address table aging monitoring time	--
Failed authentication	Failed authentication	Retry MAC-based authentication. Waits for a re-authentication interval	Retry IEEE 802.1X authentication. Waits for a re-authentication interval.	Delete entries immediately

Legend

--: Not applicable

#1

The MAC address of a target terminal is managed in the MAC address table as a `Dynamic` entry.

#2

Port-based authentication (static) only

(10) Roaming (moving authenticated terminals between ports)

Authenticated terminals that are moved between ports behave depending on the final authentication method. You do not have to set up roaming specifically for multistep authentication.

1. Final authentication method: IEEE 802.1X

   The terminal is de-authenticated when the terminal move is detected.

2. Final authentication method: Web authentication

   The behavior follows the configuration of the authentication policies and roaming for Web authentication.

   Authenticated terminals can be moved among ports that have the same authentication policy.

   If both the source and destination ports support single authentication, they follow the port movement conditions for Web authentication.

Authentication policy

Both source and destination ports must support the same combination of configurations as follows.

Table 12-16 Combination of configurations for the source and destination ports

Conditions		Remarks
Configured the `authentication multi-step` command on the source and destination ports		Ports not configured by the `authentication multi-step` command are processed by single authentication.
	Same status of authorized user authentication option	Checked when the `authentication multi-step` command is configured.
	Same status of terminal authentication dot1x option	Checked when the `authentication multi-step` command is configured.
Same combination as below		Checked when the `authentication multi-step` command is configured
	dot1x port-control	Checked when the `aaa authentication dot1x default` command is configured.
	web-authentication port	Checked when the `web-authentication system-auth-control` command is configured.
	mac-authentication port	Checked when the `mac-authentication system-auth-control` command is configured.

The authentication status of the port will be canceled if the combination does not match any listed above.

3. Final authentication method: MAC-based authentication

   The behavior follows the configuration of roaming for MAC-based authentication.

   Authenticated terminals can be moved among ports that have the same status of multistep authentication.

   If both source and destination ports support single authentication, they follow the port movement conditions for MAC-based authentication.

Table 12-17 Configuration of multistep authentication on the ports

Conditions		Remarks
Configured the `authentication multi-step` command on the source and destination ports		Ports not configured by the `authentication multi-step` command are processed by single authentication.
	Same status of authorized user authentication option	Checked when the `authentication multi-step` command is configured.
	Same status of terminal authentication	Checked when the `authentication`

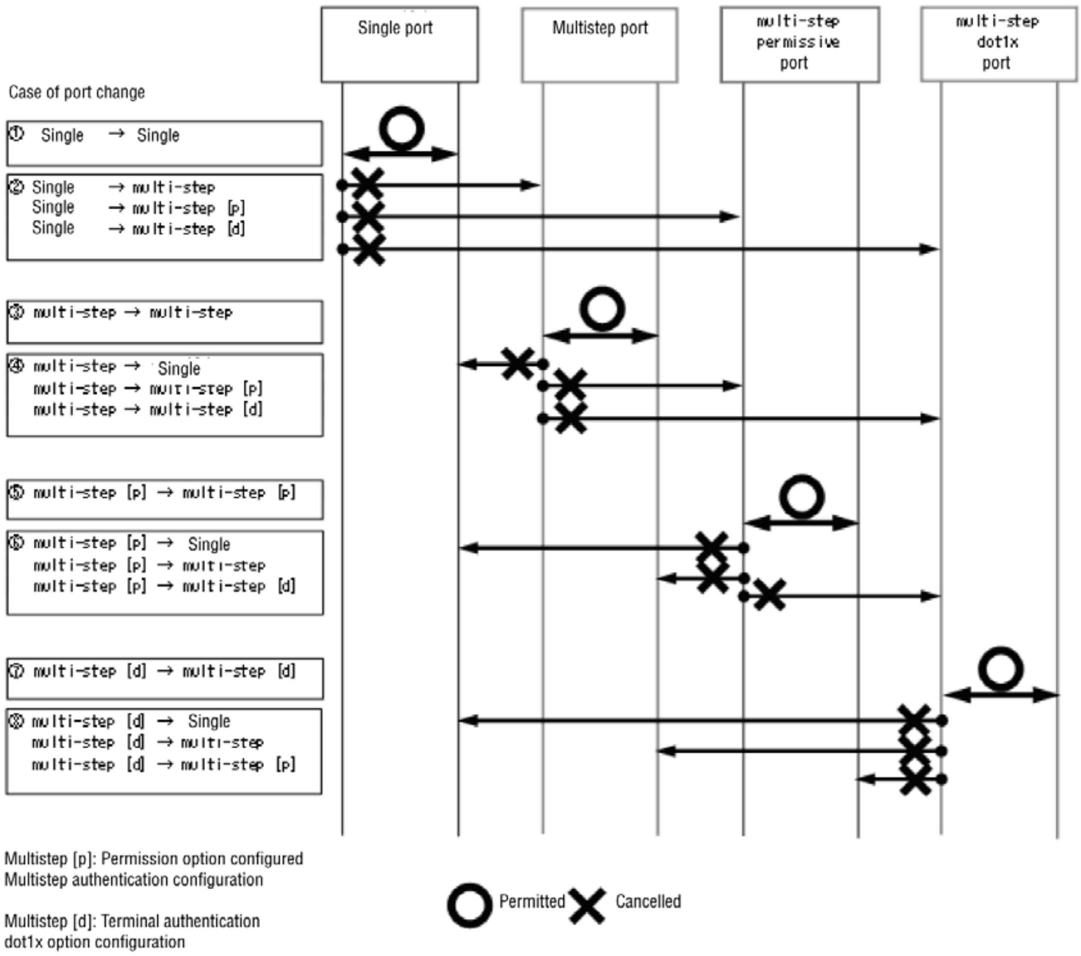
Conditions		Remarks
	dot1x option	`multi-step` command is configured.

The authentication status of the port will be canceled if the combination does not match any listed above.

For details about roaming for the Web authentication and MAC-based authentication, see *Roaming (moving authenticated terminals between ports)* in *8. Description of Web Authentication* and *10. Description of MAC-based Authentication.*

The figure below shows the transfer scenario and whether the multistep authenticated terminal can be transferred.

Figure 12-6 Port movement scenario and the multistep authenticated terminal movement conditions



The port (① in *Figure 12-6*) which supports single authentication follows the port movement conditions of Web authentication or MAC-based authentication.

The ports ③, ⑤, and ⑦ in *Figure 12-6* are the destination and source ports. The authenticated terminal is allowed to move between ports if it follows *Table 12-16*

Combination of configurations for the source and destination ports or *Table 12-17 Configuration of multistep authentication on the ports*.

Other ports that do not match the configuration for multistep authentication when moved will be de-authenticated.

The target terminal follows the final authentication method used to authenticate the terminal when the move among ports is detected. The behavior of the authentication method when the move is detected according to *Figure 12-6 Port movement scenario and the multistep authenticated terminal movement conditions* is described below.

1. Final authentication method: IEEE 802.1X

   When the movement of an IEEE 802.1X authenticated terminal is detected by receiving frames, no roaming settings exist. Therefore, the authentication is canceled in all scenarios.

2. Final authentication method: Web authentication

   The table below shows the behavior of Web-authenticated terminals when the movement is detected by receiving frames. For details about authentication policies, see *Table 12-16 Combination of configurations for the source and destination ports*.

Table 12-18 Behavior of Web-authenticated terminal port movement

Port movement scenario in *Figure 12-6*	**Roaming for Web authentication**		
	disable	**enable**	
		Authentication policy matches.	**Authentication policy does not match.**
①, ③, ⑤, ⑦	Authentication canceled.	Authentication information (move ports) is updated.	Authentication canceled
All other cases	Authentication canceled.	Authentication canceled.	Authentication canceled.

3. Final authentication method: MAC-based authentication

   The following table shows the behavior of a MAC-authenticated terminal when the transfer has been detected by receiving frames.

Table 12-19 Behavior of MAC-authenticated terminal port movement

Port movement scenario in *Figure 12-6*	**Roaming for MAC-based authentication**	
	disable	**enable**
(i), (iii), (v), (vii)	Authentication canceled.	Authentication information (move ports) is updated.
All other cases	Authentication canceled.	Authentication canceled.

(11) Displaying status, accounting logs, and traps

- Multistep authentication status

  To display the progress of multistep authentication per MAC address, use the `show authentication multi-step` operation command.

- Displaying accounting logs

  To display chronological accounting log information for each authentication functionality, use the `show authentication logging` operation command.

- Private traps

  Private traps are configured according to the authentication functionality. Multistep authentication does not have specific private traps.

12.1.3 Preparation

Multistep authentication supports only RADIUS authentication. When the port receives `Accept` from the RADIUS server, terminal authentication and user authentication determine the authentication behavior based on the character string of the `Filter-Id` RADIUS attribute.

Table 12-20 Attribute name (Access-Accept) on multistep authentication

Attribute name	Type value	Description
Filter-Id	11	Text character string. The Switch determines the authentication behavior when multistep authentication is performed.# ● `@@1X-Auth@@` ● `@@Web-Auth@@` ● `@@MultiStep@@` ● `@@MAC-Auth@@`
Tunnel-Private-Group-ID	81	A string identifying a VLAN. 1. RADIUS server for terminal authentication ■ User authentication uses IEEE 802.1X. Pre-authentication VLAN for IEEE 802.1X. ■ User authentication uses Web authentication. VLAN containing the IP address for accessing to the Web authentication login page. 2. RADIUS server for user authentication ■ Post-authentication VLAN

#

For details about the information for the authentication functionality and the behavior that defines the character string of `Filter-Id`, see *12.1.2 Authentication behavior.*

Other RADIUS attributes follow the proper authentication functionality. See the section on preparation in the description of each authentication functionality.

12.1.4 Notes on using multistep authentication

(1) Settings for authorized user authentication option and MAC-based authentication

The authorized user authentication option (`permissive`) is functionality authorized for the user if terminal authentication (MAC-based authentication) failed. When you configure a port with the authorized user authentication option, check the following configurations for MAC-based authentication to execute terminal authentication and user authentication.

1. Restricting MAC addresses to be authenticated

   Configure the MAC address of the terminal authorized by user authentication (IEEE 802.1X or Web authentication) as an authenticated MAC address by restricting the authentication target MAC addresses (`mac-authentication access-group` command).

   If you do not configure the MAC address as MAC-authenticated, MAC-based authentication will not start, and then user authentication will not be able to be performed.

   For details about restricting target MAC addresses, see *(2) Restricting MAC addresses to be authenticated* in *10.2.2 Authentication functionality* in *10. Description of MAC-based Authentication.*

2. Re-authentication delay timer

   Specify a re-authentication delay of more than 0 seconds (by using the `mac-authentication timeout quiet-period` configuration command). (The default interval is 300 seconds.)

   If you specify 0 seconds, the terminal cannot receive the failure information when MAC-based authentication is in progress. Therefore, user authentication cannot execute even if the authorized user authentication option is enabled.

   For details about the re-authentication interval timer, see *(3)* Re-authentication delay timer in *10.2.2 Authentication functionality* in *10. Description of MAC-based Authentication*.

(2) Using IEEE 802.1X

To use IEEE 802.1X on a multistep authenticated port, use the following configuration:

- Authentication sub mode: Terminal authentication mode (`dot1x multiple-authentication`)
- Terminal detection behavior toggle option: `auto` (`dot1x supplicant-detection auto`)

(3) Terminal authentication dot1x option

If you configure the terminal authentication dot1x option, the MAC-based authentication and IEEE 802.1X on terminal authentication are performed at the same time. If you use the authenticated terminal by setting IEEE 802.1X and Web authentication, do not define MAC-based authentication as a system requirement. (For example, do not assign a MAC-authenticated terminal to a RADIUS server.)

Do not configure a forced authentication on a MAC-based authentication.

(4) Multistep authentication and legacy mode

Multistep authentication is not available in legacy mode. If you use multistep authentication, confirm that the configuration shown in *Table 12-2 Legacy mode configurations that cannot be used with multistep authentication* is not set.

12.2 Configuration

12.2.1 List of configuration commands

The following table describes the commands used to configure multistep authentication.

Table 12-21 List of configuration commands for multistep authentication

Command	Description
`authentication multi-step`	Configures the port to support multistep authentication.

12.2.2 Structure of multistep authentication

This section describes the structure examples, configuration, and overview of multistep authentication.

The following table shows the structure of multistep authentication. All the scenarios obtain a terminal IP address from a DHCP server.

Table 12-22 Structure of multistep authentication

Multistep port type	Authentication mode	Port type	Authentication target type	Authentication type		Overview reference	Example reference
				Terminal	User		
Basic multistep authentication port	Dynamic VLAN	MAC	Employee user	MAC	Web	*12.2.3(1)(b) Scenario (i)*	*12.2.3(1)(d)*
			Printer	MAC	--	*12.2.3(1)(c) Scenario (ii)*	
	Fixed VLAN	Access Trunk MAC (Native)	Employee user	MAC	Web	*12.2.3(2)(b) Scenario (iii)*	*12.2.3(2)(d)*
			Printer	MAC	--	*12.2.3(2)(c) Scenario (iv)*	
Port with authorized user authentication option	Dynamic VLAN	MAC	Guest user	--	Web	*12.2.4(1)(b) Scenario (v)*	*12.2.4(1)(d)*
			Employee user	MAC	Web	*12.2.4(1)(c) Scenario (vi)*	
	Fixed VLAN	Access Trunk MAC (Native)	Guest user	--	Web	*12.2.4(2)(b) Scenario (vii)*	*12.2.4(2)(d)*
			Employee user	MAC	Web	*12.2.4(2)(c)*	

Multistep port type	Authentication mode	Port type	Authentication target type	Authentication type		Overview reference	Example reference
				Terminal	User		
						Scenario (viii)	
Port with terminal authentication dot1x option	Dynamic VLAN	MAC	Employee user	IEEE802.1X	Web	*12.2.5(1)(b)* *Scenario (ix)*	*12.2.5(1)(c)*
	Fixed VLAN	Access Trunk	Employee user	IEEE802.1X	Web	*12.2.5(2)(b)* *Scenario (x)*	*12.2.5(2)(c)*

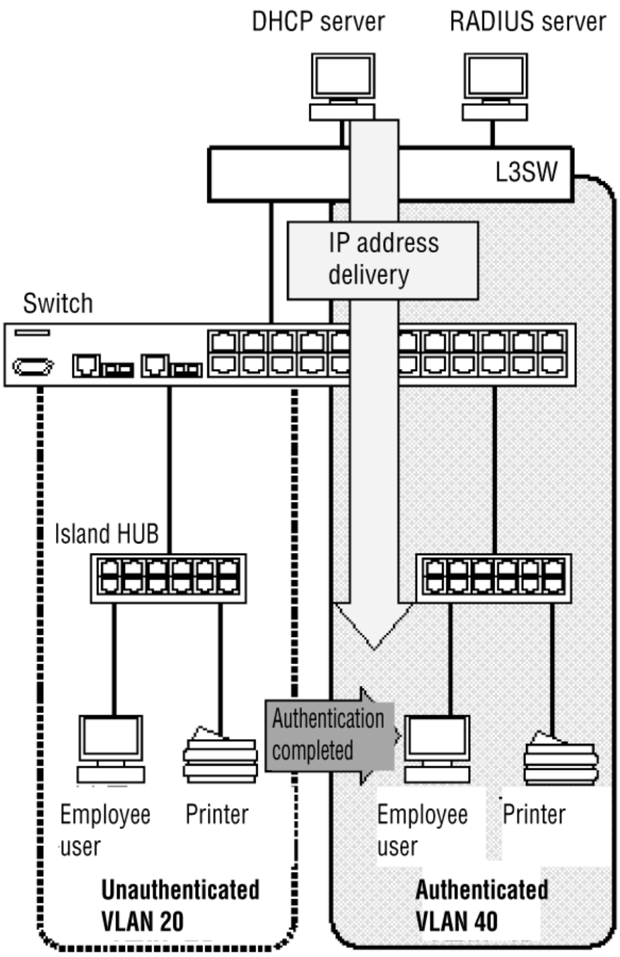
12.2.3 Configuring basic multistep authentication ports

(1) Dynamic VLAN mode

(a) Summary

The descriptions in this section assume that dynamic VLAN mode with basic multistep authentication ports assign employee users and printers to the same port, and then they obtain IP addresses after authentication.

Figure 12-7 Configuration example of a basic multistep authentication (dynamic VLAN mode)

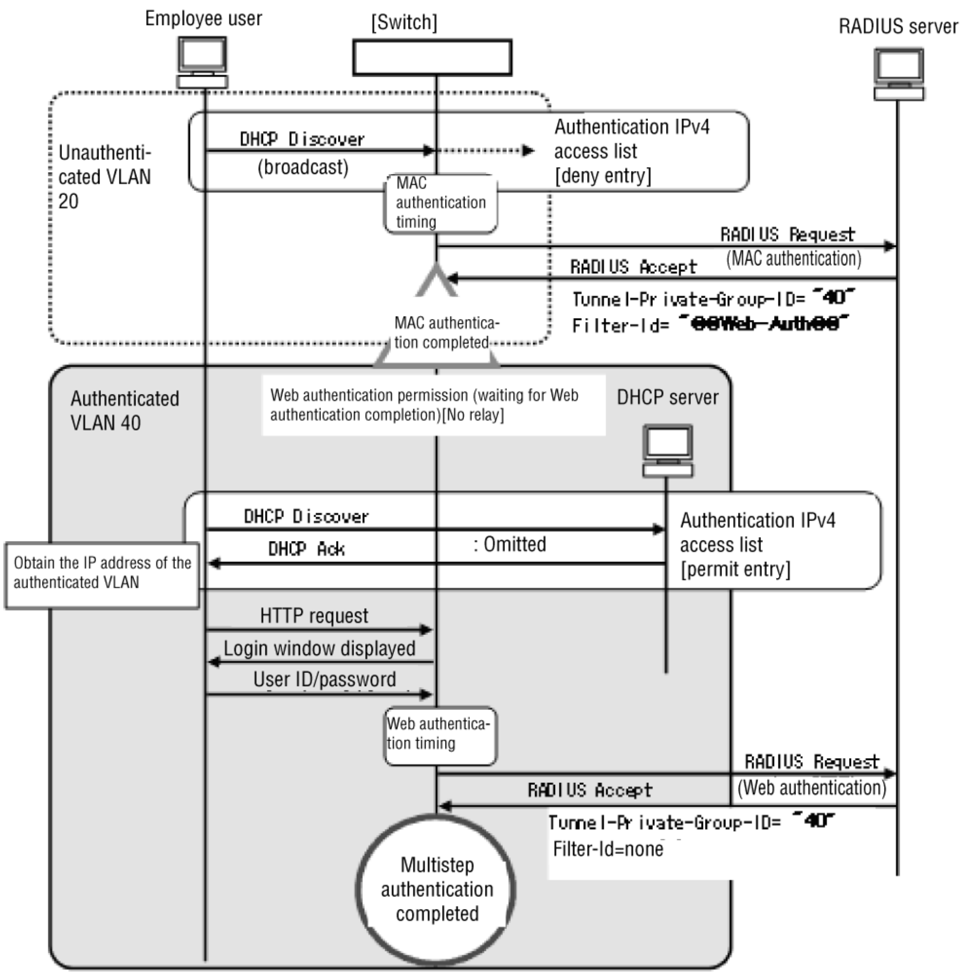


(b) Scenario (i): Employee user authentication overview

Authentication behavior

If you use basic multistep authentication, a terminal will be assigned to the post-authentication VLAN when the terminal is authenticated (MAC-based authentication), and then the terminal acquires an IP address from the authentication IPv4 access list. By executing user authentication (Web authentication), the terminal IP address is fixed both before and after Web authentication in dynamic VLAN mode.

Figure 12-8 Authentication behavior of employee users (dynamic VLAN mode)



Points to note

Table 12-23 Overview of employee users authentication (dynamic VLAN mode)

Configuration items	Requirements	Description		Remarks
Authentication IPv4 access list	Required	`deny`	`eq bootps vlan 20`	Discards DHCP frames in the pre-authentication VLAN.#
		`permit`	`eq bootps`	Forwards DHCP frames throughout the VLAN.
Internal DHCP server of the Switch	Not required	n/a		
External DHCP server	Required	`VLAN 40`		Sets to a post-authentication VLAN.

Configuration items	Requirements	Description		Remarks
RADIUS server	MAC-based authentication (authenticates MAC address of employee user terminal)	`Tunnel-Private-Group-ID`	"`40`"	Responds with post-authentication VLAN.
		`Filter-Id`	"`@@Web-Auth@@`"	Sends response `"@@Web-Auth@@"`. Waits for a user authentication (MAC-based authentication) when a terminal has been authenticated (Web authentication). Assigned to VLAN; however, traffic is prevented.
	Web authentication (authenticates employee user ID)	`Tunnel-Private-Group-ID`	"`40`"	Responds with post-authentication VLAN.
		`Filter-Id`	Not set	Responds without `Filter-Id`.

#

If you do not configure an internal DHCP server and then forward DHCP frames via an authentication IPv4 access list on the pre-authentication VLAN, the frames cannot start MAC-based authentication. Therefore, MAC-based authentication will not be able to start until the VLAN obtains an IP address and an ARP frame is sent.

In this scenario, if you do not set up a DHCP server on a pre-authentication VLAN, MAC-based authentication will never start.

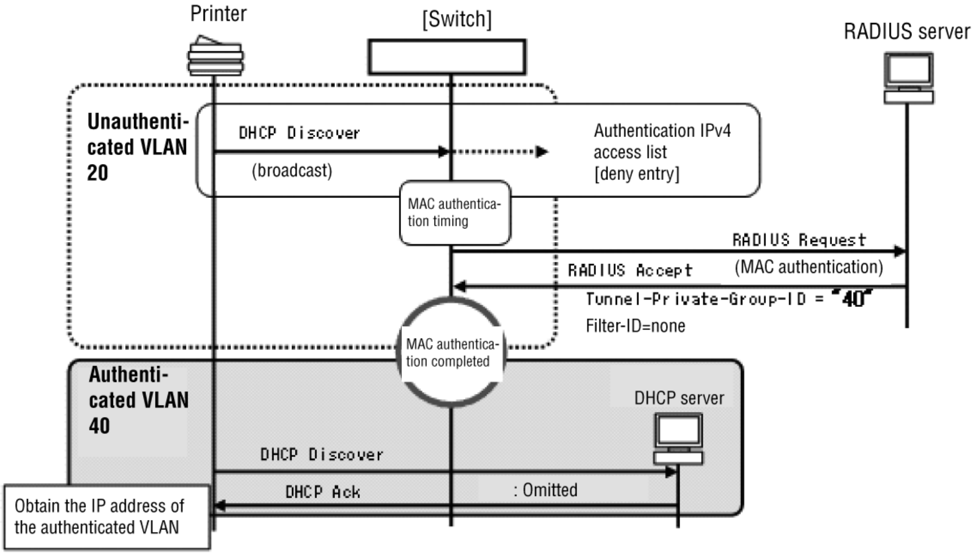
If you set up the DHCP frames to be discarded in the pre-authentication VLAN, MAC-based authentication will start by using DHCP frames when terminal authentication is completed.

(c) Scenario (ii): Printer authentication overview

Authentication behavior

If you configure a printer on the same port with an employee user in dynamic VLAN, authenticate it according to the following sequence.

Figure 12-9 Printer authentication behavior (dynamic VLAN mode)



Points to note

Table 12-24 Overview of printer authentication (dynamic VLAN mode)

Configuration items	Requirements	Description		Remarks
Authentication IPv4 access list	Not required	n/a		The access list is not required if the terminal only uses MAC-based authentication; however, if you configure the printer on the same port as the employee user, the same authentication IPv4 access list must be applied.
Internal DHCP server of the Switch	Not required	n/a		
External DHCP server	Required	VLAN 40		Sets to a post-authentication VLAN.
The RADIUS server	MAC-based authentication (authenticates printer MAC address)	`Tunnel-Private-Group-ID`	"`40`"	Responds with post-authentication VLAN.
		`Filter-Id`	Not set	Responds without `Filter-Id`. Access will be permitted when terminal authentication (MAC-based authentication) is completed.
	Web authentication	n/a		Settings are unnecessary.

Legend

n/a: Not applicable

(d) Configuring dynamic VLAN mode

The following describes the configuration for dynamic VLAN mode on a port for basic multistep authentication.

Overview

The example below shows how to set the following items at a port to be authenticated:

- VLANs
- Authentication method
- MAC port and native VLAN
- Terminal authentication (MAC-based authentication)
- User authentication (Web authentication)
- Multistep authentication port
- Authentication IPv4 access list

For details about the configuration for Web authentication, see *9. Web Authentication Configuration and Operation*, for the configuration for MAC-based authentication, see *11. MAC-based Authentication Configuration and Operation.*

Command examples

1.
```
(config)# vlan 40 mac-based
(config-vlan)# exit
```
Configures VLAN ID 40 as a MAC VLAN. (Assigns the VLAN ID to be the same as post-authentication VLAN ID which is sent from RADIUS server.)

2.
```
(config)# vlan 20
(config-vlan)# exit
```
Specifies VLAN ID 20.

3.
```
(config)# aaa authentication mac-authentication default group radius
(config)# aaa authentication web-authentication default group radius
```
Configures RADIUS authentication for both MAC and Web authentication.

4.
```
(config)# interface fastethernet 0/1
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 20
```
Specifies the port 0/1 for the MAC port. Assigns native VLAN 20 (pre-authentication VLAN) on a MAC port. (The post-authentication VLAN is assigned according to *5.4.3 Auto VLAN assignment for a MAC VLAN*.)

5. `(config-if)# web-authentication port`

   `(config-if)# mac-authentication port`

   `(config-if)# authentication multi-step`

   Configures the Web authentication, MAC-based authentication, multistep authentication (without the authorized user authentication option) to port 0/1.

6. `(config-if)# authentication ip access-group L2-AUTH`

   `(config-if)# authentication arp-relay`

   `(config-if)# exit`

   Configures an authentication IPv4 access list for frames sent from unauthenticated terminals to port 0/1. Configures the port to forward ARP frames sent from unauthenticated terminals.

7. `(config)# ip access-list extended L2-AUTH`

   `(config-ext-nacl)# deny udp any any eq bootps vlan 20`

   `(config-ext-nacl)# permit udp any any eq bootps`

   `(config-ext-nacl)# exit`

   Sets an authentication IPv4 access list to discard DHCP frames (`bootps`) in the pre-authentication VLAN and to allow the Switch to forward DHCP frames to another VLAN.

Notes

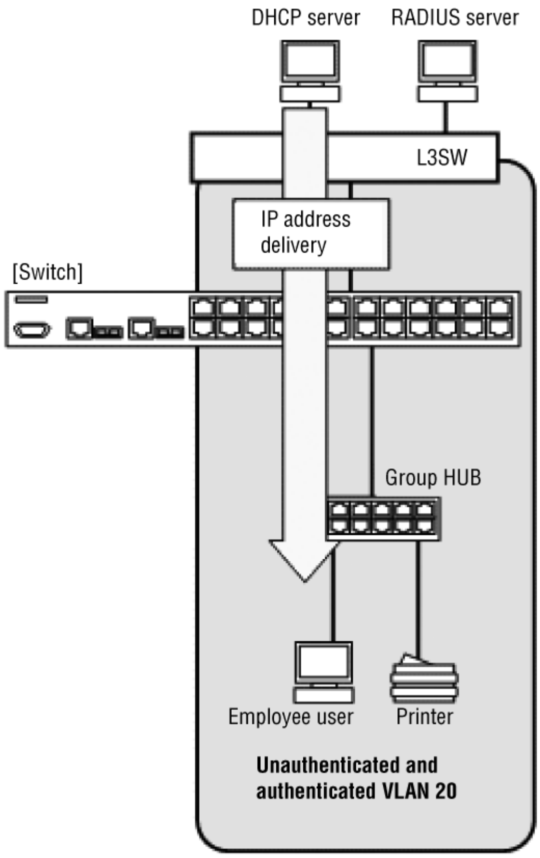
1. Configure the following parameter to the `Filter-Id` RADIUS attribute on the RADIUS server when multistep authentication is set up as above:
   - For a MAC-based authentication RADIUS server: "`@@Web-Auth@@`"
2. If you automatically assign the post-authentication VLAN in dynamic VLAN mode, assign the VLAN sent from the RADIUS server as a MAC VLAN in the `vlan` configuration command. (In this case, you do not have to assign the `switchport mac vlan` configuration command to the MAC port.)
3. If the Switch receives the response (`Accept`), which describes that authentication has succeeded and no information about the post-authentication VLAN is included, the authenticated terminal will be associated with native VLAN on the target MAC port. The terminal will be authenticated in fixed VLAN mode.

(2) Fixed VLAN mode

(a) Summary

The descriptions in this section assume that fixed VLAN mode with basic multistep authentication port assigns employee users and printers to the same port, and then they obtain IP addresses after authentication.

Figure 12-10 Configuration example of basic multistep authentication (fixed VLAN mode)



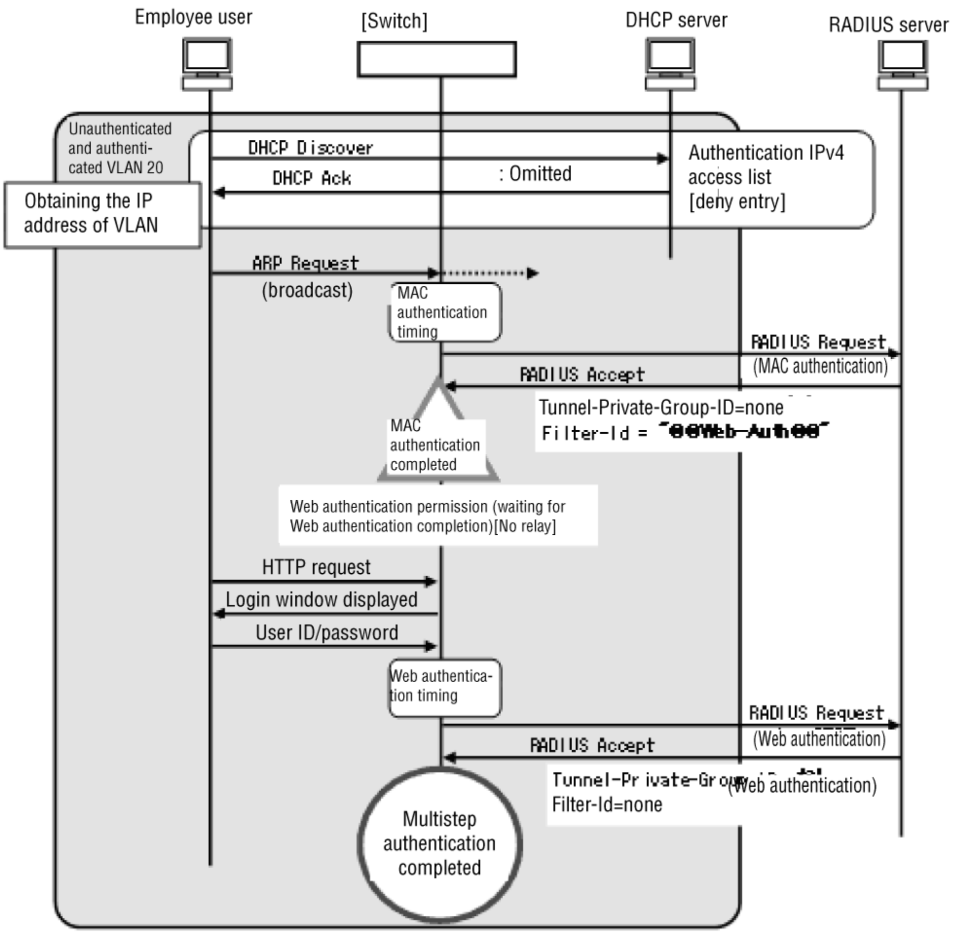
(b) Scenario (iii): Employee users authentication overview

Authentication behavior

First, an employee user authenticated by basic multistep authentication obtains an IP address from an authentication IPv4 access list and starts terminal authentication (MAC-based authentication) by using a frame such as an ARP frame.

This will lead the terminal to user authentication (Web authentication), and the traffic from the terminal will have full access after Web authentication.

Figure 12-11 Authentication of employee users (fixed VLAN mode)



Points to note

Table 12-25 Overview of employee users authentication (fixed VLAN mode)

Configuration items	Requirements	Description		Remarks
Authentication IPv4 access list	Required	`permit`	`eq bootps`	Forwards DHCP frames throughout the VLAN.
Internal DHCP server of the Switch	Not required	n/a		
External DHCP server	Required	`VLAN 20`		Sets to a post-authentication VLAN.
The RADIUS server	MAC-based authentication (authenticates	`Tunnel-Private-Group-ID`	Not set	Sends response without `Tunnel-Private-Group-ID`.

Configuration items	Requirements	Description		Remarks
	MAC address of employee user terminal)	`Filter-Id`	"`@@Web-Auth@@`"	Sends response "`@@Web-Auth@@`".
	Web authentication (authenticates employee user ID)	`Tunnel-Private-Group-ID`	Not set	Sends response without `Tunnel-Private-Group-ID`.
		`Filter-Id`	Not set	Responds without `Filter-Id`.

Legend

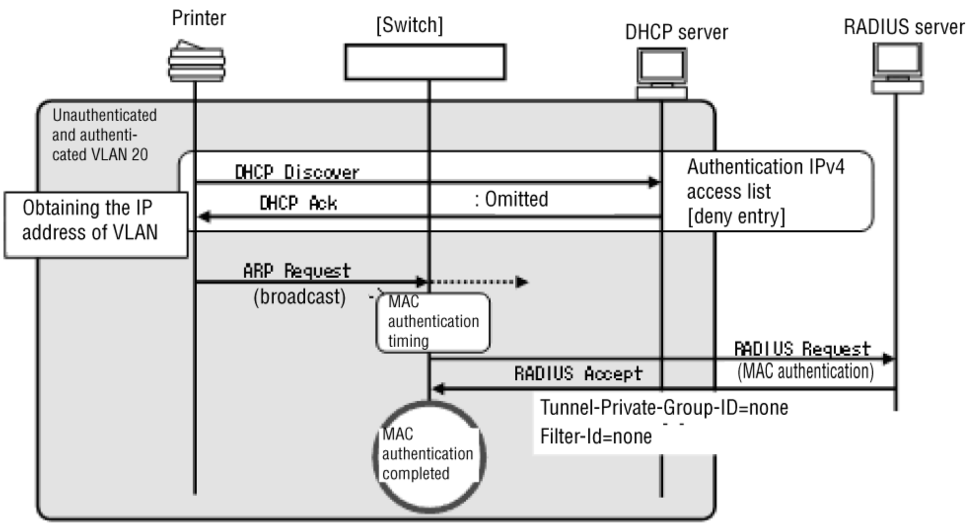
n/a: Not applicable

(c) Scenario (iv): Printer authentication overview

Authentication behavior

If you configure a printer on the same port with an employee user in fixed VLAN mode, authenticate it according to the following sequence.

Figure 12-12 Authentication behavior of printers (fixed VLAN mode)



Points to note

Table 12-26 Overview of printer authentication (fixed VLAN mode)

Configuration items	Requirements	Description	Remarks
Authentication IPv4 access list	Not required	n/a	The access list is not required if the terminal only uses MAC-based authentication; however, if you configure the printer on the same port as the

Configuration items	Requirements	Description		Remarks
				employee user, the same authentication IPv4 access list must be applied.
Internal DHCP server of the Switch	Not required	n/a		
External DHCP server	Required	`VLAN 20`		Sets to a post-authentication VLAN.
The RADIUS server	MAC-based authentication (authenticates printer MAC address)	`Tunnel-Private-Group-ID`	Not set	Sends response without `Tunnel-Private-Group-ID`.
		`Filter-Id`	Not set	Responds without `Filter-Id`. Access will be permitted when terminal authentication (MAC-based authentication) is completed.
	Web authentication	n/a		Settings are unnecessary.

Legend

n/a: Not applicable

(d) Configuring fixed VLAN mode

The following describes the configuration of fixed VLAN mode on a port for basic multistep authentication.

Overview

The example below shows how to set the following items at a port to be authenticated:

- VLAN
- Authentication method
- Access port and VLAN
- Terminal authentication (MAC-based authentication)
- User authentication (Web authentication)
- Multistep authentication port
- Authentication IPv4 access list

For details about the configuration for Web authentication, see *9. Web Authentication Configuration and Operation*, for the configuration for MAC-based authentication, see *11. MAC-based Authentication Configuration and Operation.*

Command examples

1.
```
(config)# vlan 20
(config-vlan)# exit
```

Specifies VLAN ID 20 to be accessed before and after authentication.

2. `(config)# aaa authentication mac-authentication default group radius`

   `(config)# aaa authentication web-authentication default group radius`

   Configures RADIUS authentication for both MAC-based and Web authentication.

3. `(config)# interface fastethernet 0/1`

   `(config-if)# switchport mode access`

   `(config-if)# switchport access vlan 20`

   Specifies the port 0/1 as the access port. Assigns VLAN 20 to the access port.

4. `(config-if)# web-authentication port`

   `(config-if)# mac-authentication port`

   `(config-if)# authentication multi-step`

   Configures the Web authentication, MAC-based authentication, multistep authentication (without the authorized user authentication option) to port 0/1.

5. `(config-if)# authentication ip access-group L2-AUTH`

   `(config-if)# authentication arp-relay`

   `(config-if)# exit`

   Configures an authentication IPv4 access list for frames sent from unauthenticated terminals to port 0/1. Configures the port to forward ARP frames sent from unauthenticated terminals.

6. `(config)# ip access-list extended L2-AUTH`

   `(config-ext-nacl)# permit udp any any eq bootps`

   `(config-ext-nacl)# exit`

   Configures an authentication IPv4 access list that forwards DHCP frames (`bootps`) sent from unauthenticated terminals.

Notes

1. Configure the following parameter to the `Filter-Id` RADIUS attribute on the RADIUS server when multistep authentication is set up as above:
   - For a MAC-based authentication RADIUS server: "`@@Web-Auth@@`"

12.2.4 Configuring ports for the authorized user authentication option

(1) Dynamic VLAN mode

(a) Summary

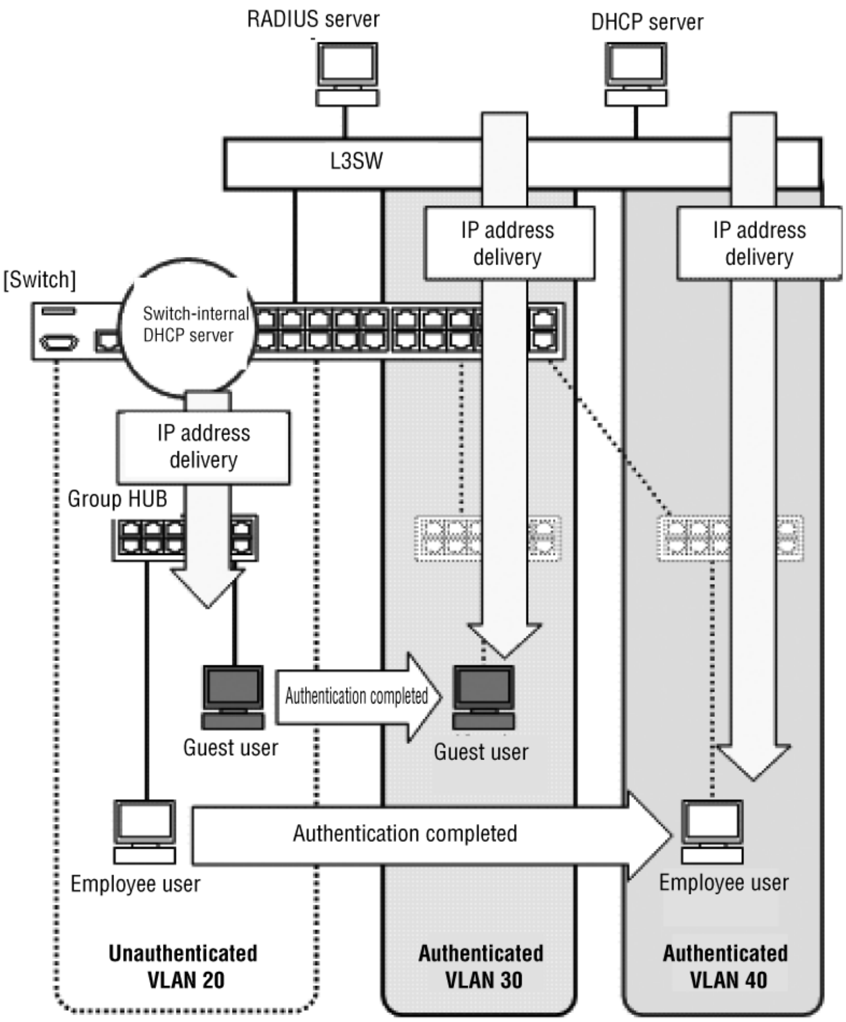
You can assign a guest user and an employee user to the same port in dynamic VLAN mode for ports with the authorized user authentication option.

The portable terminal for a guest user is authenticated by Web authentication, and the terminal will become a member of a VLAN that is accessible by the guest user.

The portable terminal for an employee user is not allowed to access a VLAN, and the terminal used by registered users must be associated with a VLAN.

The section describes how both types of users obtain an IP address in the different VLANs before and after authentication.

Figure 12-13 Configuration example of authorized user authentication option (dynamic VLAN mode)



(b) Scenario (v): Guest user authentication overview

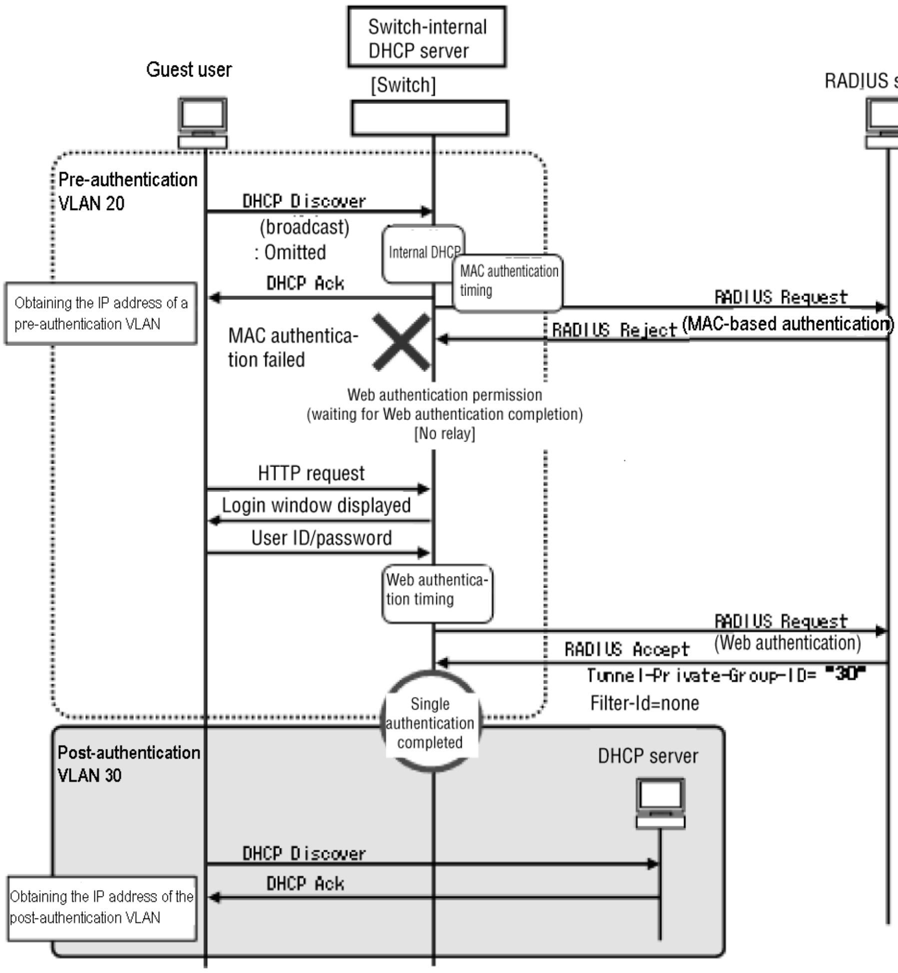
Authentication behavior

The authorized user authentication option assumes that a guest user and an employee user are assigned to the same port.

A guest user fails terminal authentication, and the user in dynamic VLAN mode cannot move to another VLAN. Therefore, the guest user has to obtain an IP address in the pre-authentication VLAN. To obtain the IP address in the pre-authentication VLAN, use the internal DHCP server of the Switch is used.

If you set up the internal DHCP server in the pre-authentication VLAN, DHCP frames will start MAC-based authentication even if the DHCP frames have been configured to be forwarded on the authentication IPv4 access list.

Figure 12-14 Authentication behavior of guest users (dynamic VLAN mode)



Points to note

Table 12-27 Overview of guest users authentication (dynamic VLAN mode)

Configuration items	Requirements	Description		Remarks
Authentication IPv4 access list	Required	`permit`	`eq bootps`	Forwards DHCP frames throughout the

Configuration items	Requirements	Description		Remarks
				VLAN.
Internal DHCP server of the Switch	Required	`VLAN 20`		Enabled on pre-authentication VLAN.
External DHCP server	Required	`VLAN 30, 40`		Sets to a post-authentication VLAN.
The RADIUS server	MAC-based authentication (authenticates MAC address of portable terminal)	n/a		Sends response Reject: Access-Reject.
	Web authentication (authenticates guest user ID)	`Tunnel-Private-Group-ID`	"30"	Assigns post-authentication VLAN.
		`Filter-Id`	Not set	Responds without `Filter-Id`.

Legend

n/a: Not applicable

(c) Scenario (vi): Employee user authentication overview

Authentication behavior

The behavior of employee user authentication is the same as that of basic multistep authentication when terminal authentication (MAC-based authentication) has succeeded. The internal server on this port is enabled in the pre-authentication VLAN for a guest user. In this case, an IP address that is not actually used is temporarily obtained in the pre-authentication VLAN.

An authentication IPv4 access list must be set up to obtain an IP address from the external DHCP in the post-authentication VLAN, because the terminal only moves from pre- to post-authentication VLAN when terminal authentication (MAC-based authentication) succeeds.

An employee user is not allowed to use a portable terminal; terminal authentication (MAC-based authentication) must be configured on the RADIUS server for Web authentication. The authentication process completes after either Web or MAC-based authentication.

Figure 12-15 Authentication behavior of employee users (dynamic VLAN mode)

Points to note

Table 12-28 Overview of employee users authentication (dynamic VLAN mode)

Configuration items	Requirements	Description		Remarks
Authentication IPv4 access list	Required	permit	eq bootps	Forwards DHCP frames throughout the VLAN.
Internal DHCP server of the Switch	Not required	n/a		The internal DHCP is not required for an employee user; however, it is required for a guest user in the pre-authentication VLAN.
External DHCP server	Required	VLAN 40		Sets to a post-authentication VLAN.
The RADIUS server	MAC-based authentication (authenticates MAC address of employee user terminal)	Tunnel-Private-Group-ID	"40"	Responds with post-authentication VLAN.
		Filter-Id	"@@Web-Auth@@"	Sends response "@@Web-Auth@@". Waits for a user authentication (MAC-based authentication) when a terminal has been authenticated (Web authentication). Assigned to VLAN; however, traffic is prevented.
	Web authentication (authenticates employee user ID)	Tunnel-Private-Group-ID	"40"	Responds with post-authentication VLAN.
		Filter-Id	"@@MAC-Auth@@"	"@@MAC-Auth@@" Only the terminal authenticated (MAC-based authentication) user is permitted successful authentication.

Legend

n/a: Not applicable

(d) Configuring dynamic VLAN mode

The following describes the configuration for dynamic VLAN mode on a port with the authorized user authentication option.

Overview

The example below shows how to set the following items at a port to be authenticated:

- VLANs
- Authentication method
- MAC port and native VLAN
- Terminal authentication (MAC-based authentication)
- User authentication (Web authentication)
- Multistep authentication port (with the authorized user authentication option)
- Authentication IPv4 access list
- Internal DHCP server of the Switch

For details about the configuration for Web authentication, see *9. Web Authentication Configuration and Operation*, for the configuration for MAC-based authentication, see *11. MAC-based Authentication Configuration and Operation.*

Command examples

1.
```
(config)# vlan 30 mac-based
(config-vlan)# exit
(config)# vlan 40 mac-based
(config-vlan)# exit
```
Assigns MAC VLAN to VLAN ID 30 and 40. (Assigns the VLAN ID to be the same as post-authentication VLAN ID which is sent from RADIUS server.)

2.
```
(config)# vlan 20
(config-vlan)# exit
```
Specifies VLAN ID 20.

3.
```
(config)# aaa authentication mac-authentication default group radius
(config)# aaa authentication web-authentication default group radius
```
Configures RADIUS authentication for both MAC and Web authentication.

4.
```
(config)# interface fastethernet 0/1
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 20
```
Specifies the port 0/1 for the MAC port. Assigns native VLAN 20 (pre-authentication VLAN) on a MAC port. (The post-authentication VLAN is assigned according to *5.4.3 Auto VLAN assignment for a MAC VLAN*.)

5.
```
(config-if)# web-authentication port
(config-if)# mac-authentication port
```

`(config-if)# authentication multi-step permissive`

Configures Web authentication, MAC-based authentication, and multistep authentication (with the authorized user authentication option) to the port 0/1.

6. `(config-if)# authentication ip access-group L2-AUTH`

   `(config-if)# authentication arp-relay`

   `(config-if)# exit`

   Configures an authentication IPv4 access list for frames sent from unauthenticated terminals to port 0/1. Configures the port to forward ARP frames sent from unauthenticated terminals.

7. `(config)# ip access-list extended L2-AUTH`

   `(config-ext-nacl)# permit udp any any eq bootps`

   `(config-ext-nacl)# exit`

   Configures an authentication IPv4 access list that forwards DHCP frames (`bootps`) sent from unauthenticated terminals.

8. `(config)# interface vlan 20`

   `(config-if)# ip address 192.168.20.254 255.255.255.0`

   `(config-if)# exit`

   `(config)# service dhcp vlan 20`

   `(config)# ip dhcp pool NativeVLAN`

   `(dhcp-config)# network 192.168.20.0/24`

   `(dhcp-config)# exit`

   Assigns IP addresses to pre-authentication VLANs. Enables the internal DHCP server on pre-authentication VLAN 20.

Notes

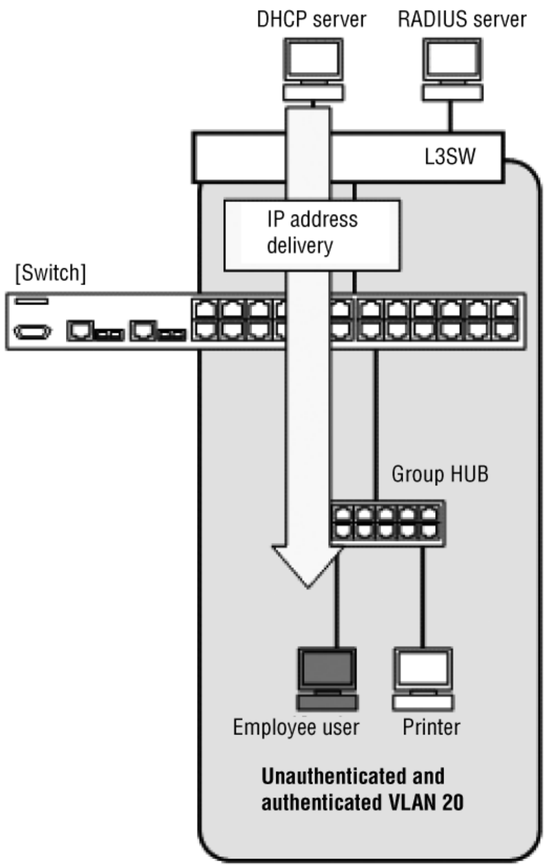
1. Configure the following parameter to the `Filter-Id` RADIUS attribute on the RADIUS server when multistep authentication is set up as above:
   - For a MAC-based authentication RADIUS server: "`@@Web-Auth@@`"
   - For a Web authentication RADIUS server: "`@@MAC-Auth@@`"
2. If you automatically assign the post-authentication VLAN in dynamic VLAN mode, assign the VLAN sent from the RADIUS server as a MAC VLAN in the `vlan` configuration command. (In this case, you do not have to assign the `switchport mac vlan` configuration command to the MAC port.)
3. If the Switch receives the response (`Accept`), which describes that authentication has succeeded and no information about the post-authentication VLAN is included, the authenticated terminal will be associated with native VLAN on the target MAC port. The terminal will be authenticated in fixed VLAN mode.

(2) Fixed VLAN mode

(a) Summary

The descriptions of this section assume that fixed VLAN mode on a port with the authorized user authentication option assigns guest users and employee user to the same port, and then they obtain IP addresses before authentication.

Figure 12-16 Configuration example of authorized user authentication option (fixed VLAN mode)



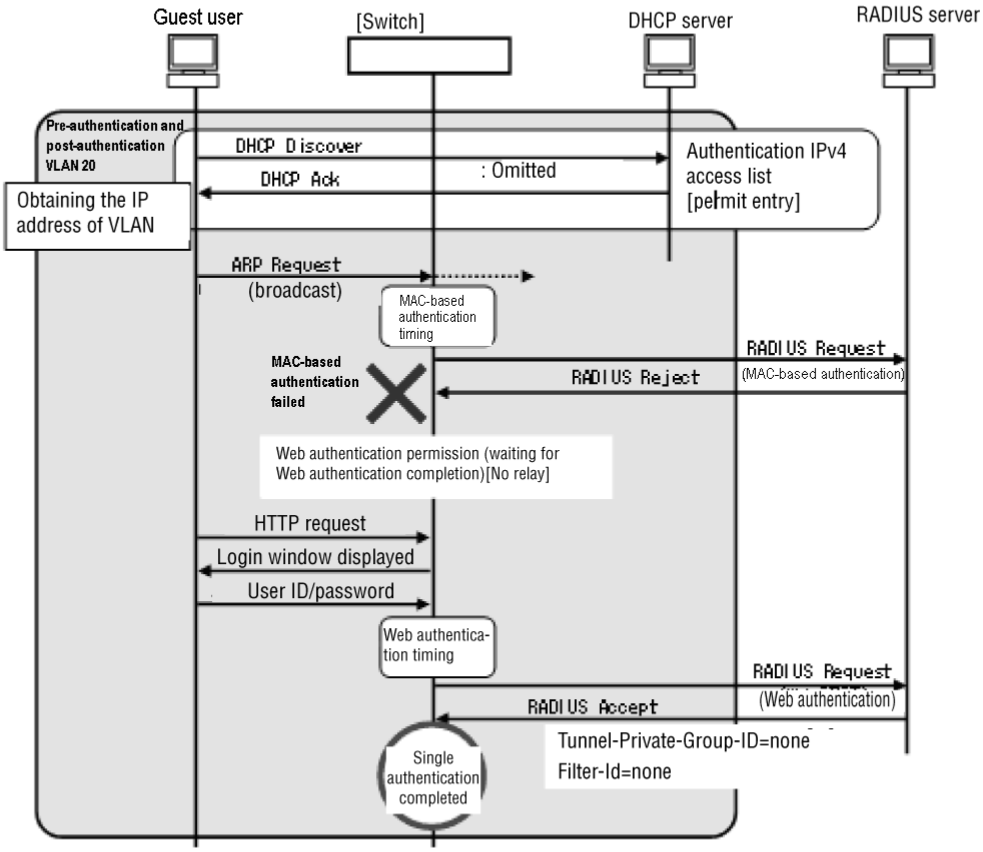
(b) Scenario (vii): Guest user authentication overview

Authentication behavior

First, the guest user on a port with the authorized user authentication option obtains an IP address from an authentication IPv4 access list and starts terminal authentication (MAC-based authentication) by using a frame such as an ARP frame. In this case, MAC-based authentication will fail because the MAC address of a portable terminal is not registered.

The port with the authorized user authentication option allows the terminal to execute user authentication (Web authentication) even if terminal authentication (MAC-based authentication) fails. The guest user will have full access after Web authentication.

Figure 12-17 Authentication behavior of guest users (fixed VLAN mode)



Points to note

Table 12-29 Overview of guest user authentication (fixed VLAN mode)

Configuration items	Requirements	Description	Remarks
Authentication IPv4 access list	Required	`permit` `eq bootps`	Forwards DHCP frames throughout the VLAN.
Internal DHCP server of the Switch	Not required	n/a	
External DHCP server	Required	`VLAN 20`	Sets to a post-authentication VLAN.
The RADIUS server	MAC-based authentication (authenticates MAC address of portable terminal)	n/a	Setting are unnecessary. Sends response Reject: `Access-Reject`.

Configuration items	Requirements	Description		Remarks
	Web authentication (authenticates guest user ID)	`Tunnel-Private-Group-ID`	Not set	Sends response without `Tunnel-Private-Group-ID`.
		`Filter-Id`	Not set	Responds without `Filter-Id`. The authentication will be completed regardless of the result of terminal authentication (MAC-based authentication).

Legend

n/a: Not applicable

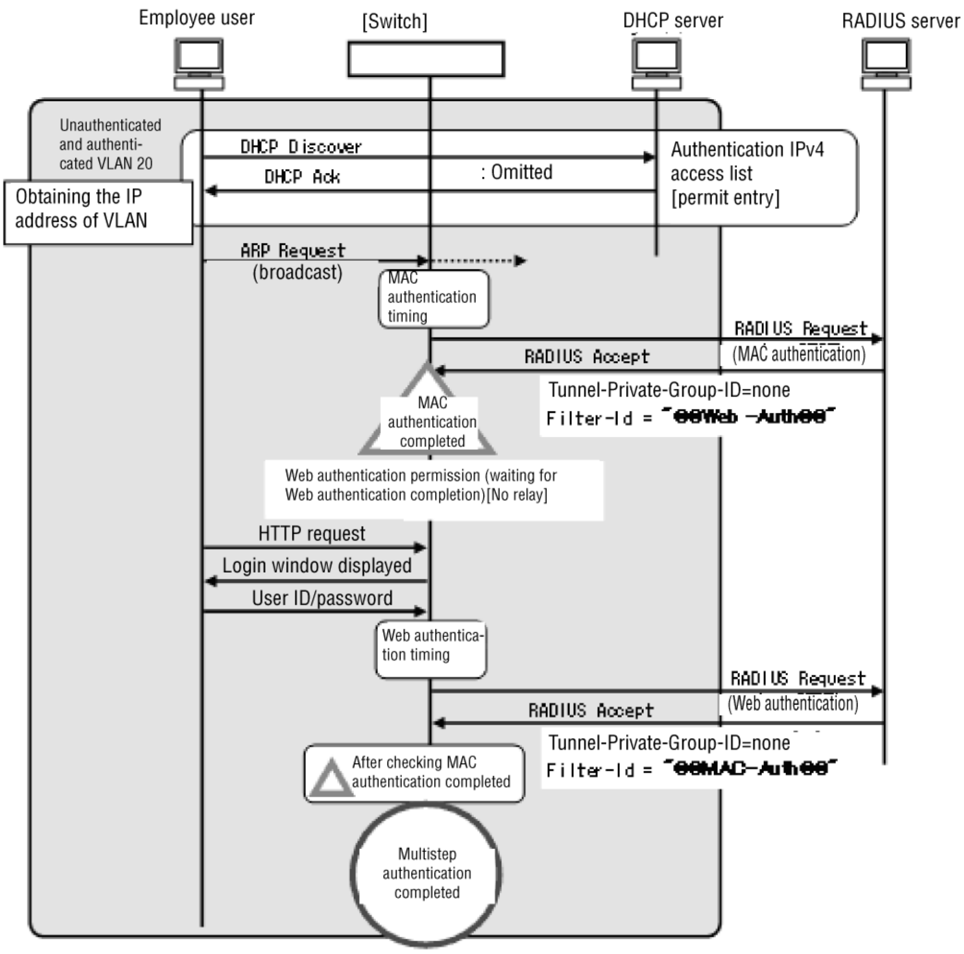
(c) Scenario (viii): Employee user authentication overview

Authentication behavior

First, the employee user on a port with the authorized user authentication option obtains an IP address from an authentication IPv4 access list and starts terminal authentication (MAC-based authentication) by using a frame such as an ARP frame.

This will lead the terminal to Web authentication and the traffic from the terminal will have full access after Web authentication.

Figure 12-18 Authentication behavior of employee users (fixed VLAN mode)



Points to note

Table 12-30 Overview of employee users authentication (fixed VLAN mode)

Configuration items	Requirements	Description		Remarks
Authentication IPv4 access list	Required	`permit`	`eq bootps`	Forwards DHCP frames throughout the VLAN.
Internal DHCP server of the Switch	Not required	n/a		
External DHCP server	Required	`VLAN 20`		Sets to a post-authentication VLAN.
The RADIUS server	MAC-based authentication	`Tunnel-Private-Group-ID`	Not set	Sends response without `Tunnel-Private-Group-ID`.

Configuration items	Requirements	Description		Remarks
	(authenticates MAC address of employee user terminal)	`Filter-Id`	"`@@Web-Auth@@`"	Sends response "`@@Web-Auth@@`". Waits for a user authentication when a terminal has been authenticated (MAC-based authentication). The traffic is prevented.
	Web authentication (authenticates employee user ID)	`Tunnel-Private-Group-ID`	Not set	Sends response without `Tunnel-Private-Group-ID`.
		`Filter-Id`	"`@@MAC-Auth@@`"	Responds with "`@@MAC-Auth@@`" Only the terminal authenticated (MAC-based authentication) user is permitted successful authentication.

Legend

n/a: Not applicable

(d) Configuring fixed VLAN mode

The following describes the configuration of fixed VLAN mode on a port with the authorized user authentication option.

Overview

The example below shows how to set the following items at a port to be authenticated:

- VLANs
- Authentication method
- Access port and VLAN
- Terminal authentication (MAC-based authentication)
- User authentication (Web authentication)
- Multistep authentication port (with the authorized user authentication option)
- Authentication IPv4 access list

For details about the configuration for Web authentication, see *9. Web Authentication Configuration and Operation*, for the configuration for MAC-based authentication, see *11. MAC-based Authentication Configuration and Operation.*

Command examples

1.
```
(config)# vlan 20
(config-vlan)# exit
```

Specifies VLAN ID 20 to be accessed before and after authentication.

2. `(config)# aaa authentication mac-authentication default group radius`

   `(config)# aaa authentication web-authentication default group radius`

   Configures RADIUS authentication for both MAC and Web authentication.

3. `(config)# interface fastethernet 0/1`

   `(config-if)# switchport mode access`

   `(config-if)# switchport access vlan 20`

   Specifies the port 0/1 as the access port. Assigns VLAN 20 to the access port.

4. `(config-if)# web-authentication port`

   `(config-if)# mac-authentication port`

   `(config-if)# authentication multi-step permissive`

   Configures Web authentication, MAC-based authentication, and multistep authentication (with the authorized user authentication option) to the port 0/1.

5. `(config-if)# authentication ip access-group L2-AUTH`

   `(config-if)# authentication arp-relay`

   `(config-if)# exit`

   Configures an authentication IPv4 access list for frames sent from unauthenticated terminals to port 0/1. Configures the port to forward ARP frames sent from unauthenticated terminals.

6. `(config)# ip access-list extended L2-AUTH`

   `(config-ext-nacl)# permit udp any any eq bootps`

   `(config-ext-nacl)# exit`

   Configures an authentication IPv4 access list that forwards DHCP frames (`bootps`) sent from unauthenticated terminals.

Notes

1. Configure the following parameter to the `Filter-Id` RADIUS attribute on the RADIUS server when multistep authentication is set up as above:
   - For a MAC-based authentication RADIUS server: "`@@Web-Auth@@`"
   - For a Web authentication RADIUS server:"`@@MAC-Auth@@`"

12.2.5 Configuring ports with the terminal authentication dot1x option

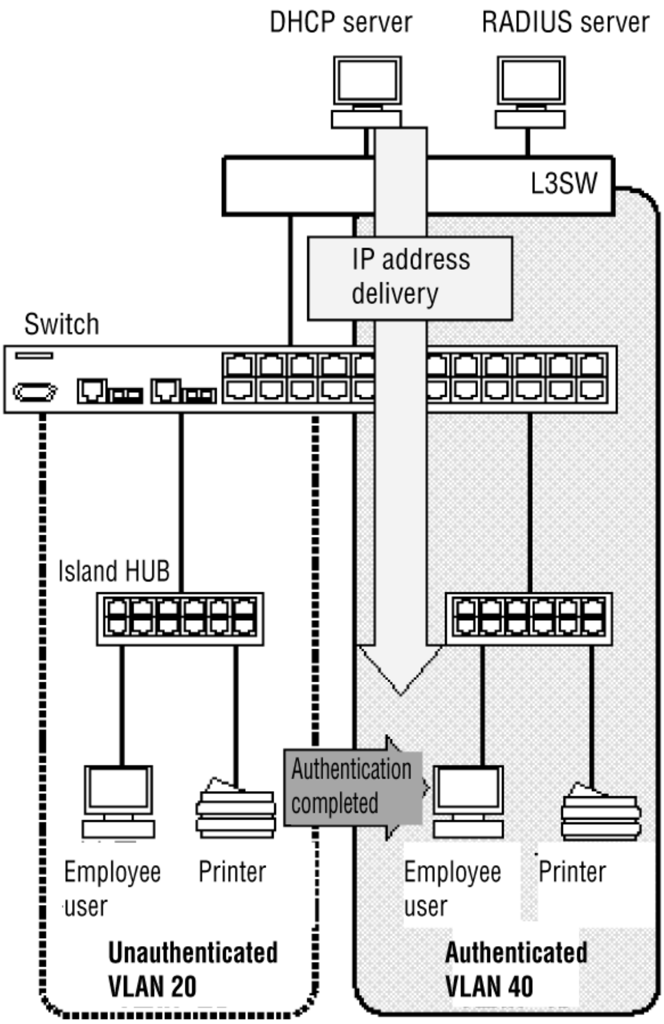
(1) Dynamic VLAN mode

(a) Summary

The descriptions in this section assume that dynamic VLAN mode for a port with the terminal authentication dot1x option assigns employee users and printers to the same port, and then they obtain IP addresses after authentication.

Printer authentication is configured in the same way as basic multistep authentication ports. See *12.2.3 Configuring basic multistep authentication ports.*

Figure 12-19 Configuration example of terminal authentication dot1x (dynamic VLAN mode)

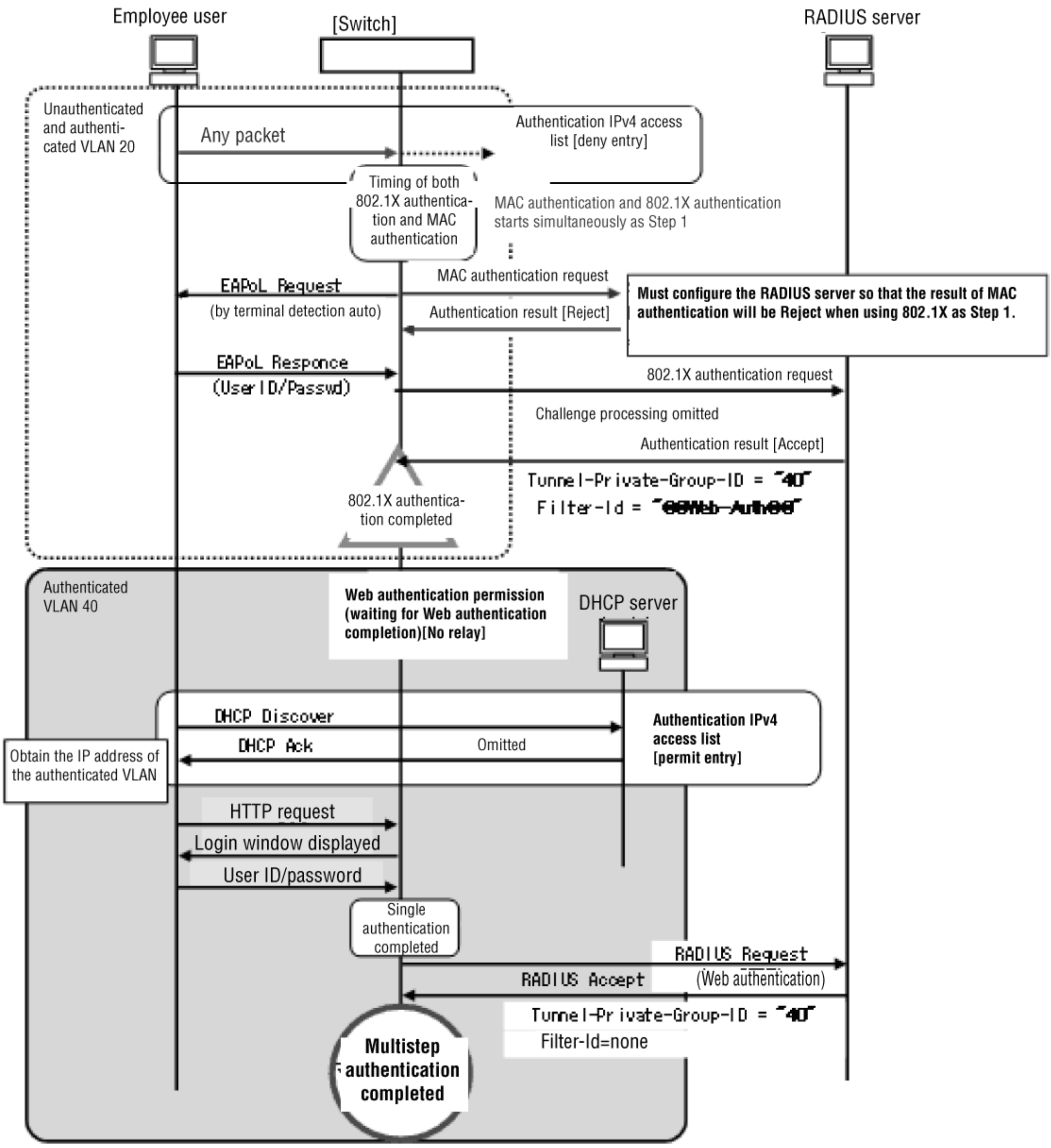


(b) Scenario (ix): Employee users authentication overview

Authentication behavior

If you use the terminal authentication dot1x option, a terminal will be assigned to the post-authentication VLAN when the terminal has authenticated (IEEE 802.1X authentication), and then it acquires an IP address from the authentication IPv4 access list. By executing user authentication (Web authentication), the terminal IP address is fixed both before and after Web authentication in dynamic VLAN mode.

Figure 12-20 Authentication behavior of employee users (dynamic VLAN mode)



Points to note

Table 12-31 Overview of employee users authentication (dynamic VLAN mode)

Configuration items	Requirements	Description		Remarks
Authentication IPv4 access list	Required	`deny`	`eq bootps vlan 20`	Discards DHCP frames in the pre-authentication VLAN#

Configuration items	Requirements	Description		Remarks
		permit	eq bootps	Forwards DHCP frames throughout the VLAN
Internal DHCP server of the Switch	Not required	n/a		
External DHCP server	Required	VLAN 40		Sets to a post-authentication VLAN
The RADIUS server	IEEE 802.1X (authenticates MAC address of employee user terminal)	Tunnel-Private-Group-ID	"40"	Responds with post-authentication VLAN
		Filter-Id	"@@Web-Auth@@"	Sends response "@@Web-Auth@@". Waits for a user authentication (Web authentication) when a terminal has been authenticated (IEEE 802.1X authentication). Assigned to VLAN; however, traffic is prevented.
	Web authentication (authenticates employee user ID)	Tunnel-Private-Group-ID	"40"	Responds with post-authentication VLAN
		Filter-Id	Not set	Responds without Filter-Id

#

If you do not configure an internal DHCP server and then forward DHCP frames via an authentication IPv4 access list on the pre-authentication VLAN, the frames cannot start MAC-based authentication. Therefore, MAC-based authentication will not be able to start until the VLAN obtains an IP address and an ARP frame is sent.

In this scenario, if you do not set up a DHCP server on a pre-authentication VLAN, MAC-based authentication will never start.

If you set up the DHCP frames to be discarded in the pre-authentication VLAN, MAC-based authentication will start by using DHCP frames when terminal authentication is completed.

(c) Configuring dynamic VLAN mode

The following describes the configurations of dynamic VLAN mode on a port with the terminal authentication dot1x option.

IEEE 802.1X and Web authentication must be configured for employee user authentication. MAC-based authentication must be configured for printer authentication.

Overview

The example below shows how to set the following items at a port to be authenticated:

- VLAN
- Authentication method
- MAC port and native VLAN
- Terminal authentication (IEEE 802.1X)
- User authentication (Web authentication)
- Terminal authentication (MAC-based authentication)
- Multistep authentication port (with terminal authentication dot1x option)
- Authentication IPv4 access list

For other configurations necessary for IEEE 802.1X, see *7. IEEE 802.1X Configuration and Operation*. For the configuration necessary for Web authentication, see *9. Web Authentication Configuration and Operation*, and for the configuration necessary for MAC-based authentication, see *11. MAC-based Authentication Configuration and Operation*.

Command examples

1.
```
(config)# vlan 40 mac-based
(config-vlan)# exit
```
Configures VLAN ID 40 as a MAC VLAN. (Assigns the VLAN ID to be the same as post-authentication VLAN ID which is sent from RADIUS server.)

2.
```
(config)# vlan 20
(config-vlan)# exit
```
Specifies VLAN ID 20.

3.
```
(config)# aaa authentication dot1x default group radius
(config)# aaa authentication web-authentication default group
radius
(config)# aaa authentication mac-authentication default group
radius
```
Configures RADIUS authentication for IEEE 802.1X, Web authentication, and MAC-based authentication.

4.
```
(config)# interface fastethernet 0/1
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 20
```
Specifies the port 0/1 for the MAC port. Assigns native VLAN 20 (pre-authentication VLAN) on a MAC port. (The post-authentication VLAN is assigned according to *5.4.3 Auto VLAN assignment for a MAC VLAN*.)

5. `(config-if)# dot1x port-control auto`
   `(config-if)# dot1x multiple-authentication`
   `(config-if)# dot1x supplicant-detection auto`
   `(config-if)# web-authentication port`
   `(config-if)# mac-authentication port`
   `(config-if)# authentication multi-step dot1x`

   Configures IEEE 802.1X, Web authentication, MAC-based authentication, and multistep authentication (with the terminal authentication dot1x option) to port 0/1.

6. `(config-if)# authentication ip access-group L2-AUTH`
   `(config-if)# authentication arp-relay`
   `(config-if)# exit`

   Configures an authentication IPv4 access list for frames sent from unauthenticated terminals to port 0/1. Configures the port to forward ARP frames sent from unauthenticated terminals.

7. `(config)# ip access-list extended L2-AUTH`
   `(config-ext-nacl)# deny udp any any eq bootps vlan 20`
   `(config-ext-nacl)# permit udp any any eq bootps`
   (config-ext-nacl)# exit

   Sets an authentication IPv4 access list to discard DHCP frames (`bootps`) in the pre-authentication VLAN and to allow the Switch to forward DHCP frames to another VLAN.

Notes

1. Configure the following parameter to the `Filter-Id` RADIUS attribute on the RADIUS server when multistep authentication is set up as above:
   - For an IEEE 802.1X authentication RADIUS server: "`@@Web-Auth@@`"

   Note that when the port is set up as shown above, MAC-based authentication and IEEE 802.1X operate simultaneously for terminal authentication. To use IEEE 802.1X to authenticate employee users, specify the configuration so that MAC-based authentication fails (for example, do not assign the terminal to the RADIUS server as a MAC-based authentication target).

2. If you automatically assign the post-authentication VLAN in dynamic VLAN mode, assign the VLAN sent from the RADIUS server as a MAC VLAN in the `vlan` configuration command. (In this case, you do not have to assign the `switchport mac vlan` configuration command to the MAC port.)

3. If the Switch receives the response (`Accept`), which describes that authentication has succeeded and no information about the post-authentication VLAN is included, the authenticated terminal will be associated with native VLAN on the target MAC port. The terminal

will be authenticated in fixed VLAN mode.

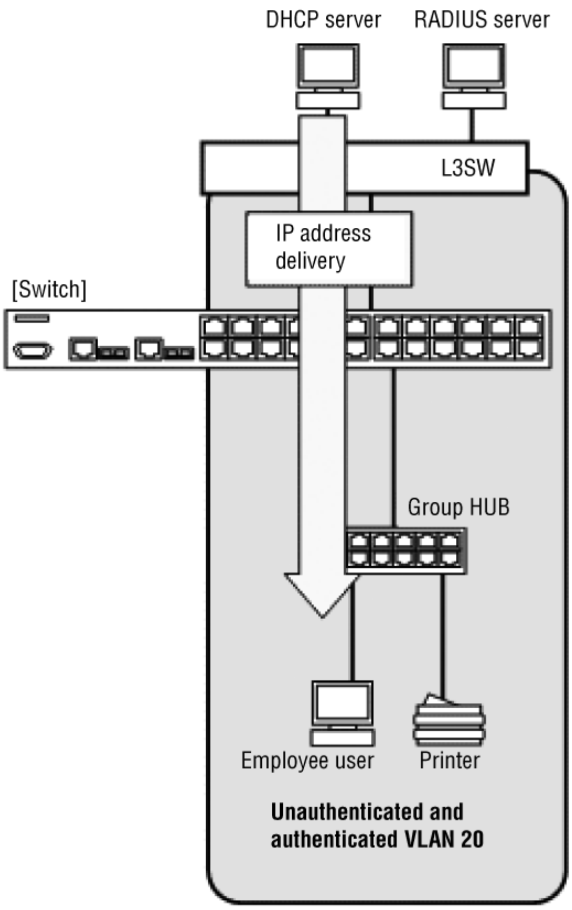
(2) Fixed VLAN mode

(a) Summary

The descriptions in this section assume that fixed VLAN mode with the terminal authentication dot1x option assigns employee users and printers to the same port, and then they obtain IP addresses after authentication.

Printer authentication is configured in the same way as basic multistep authentication ports. See *12.2.3 Configuring basic multistep authentication ports*.

Figure 12-21 Configuration example of terminal authentication dot1x option (fixed VLAN mode)

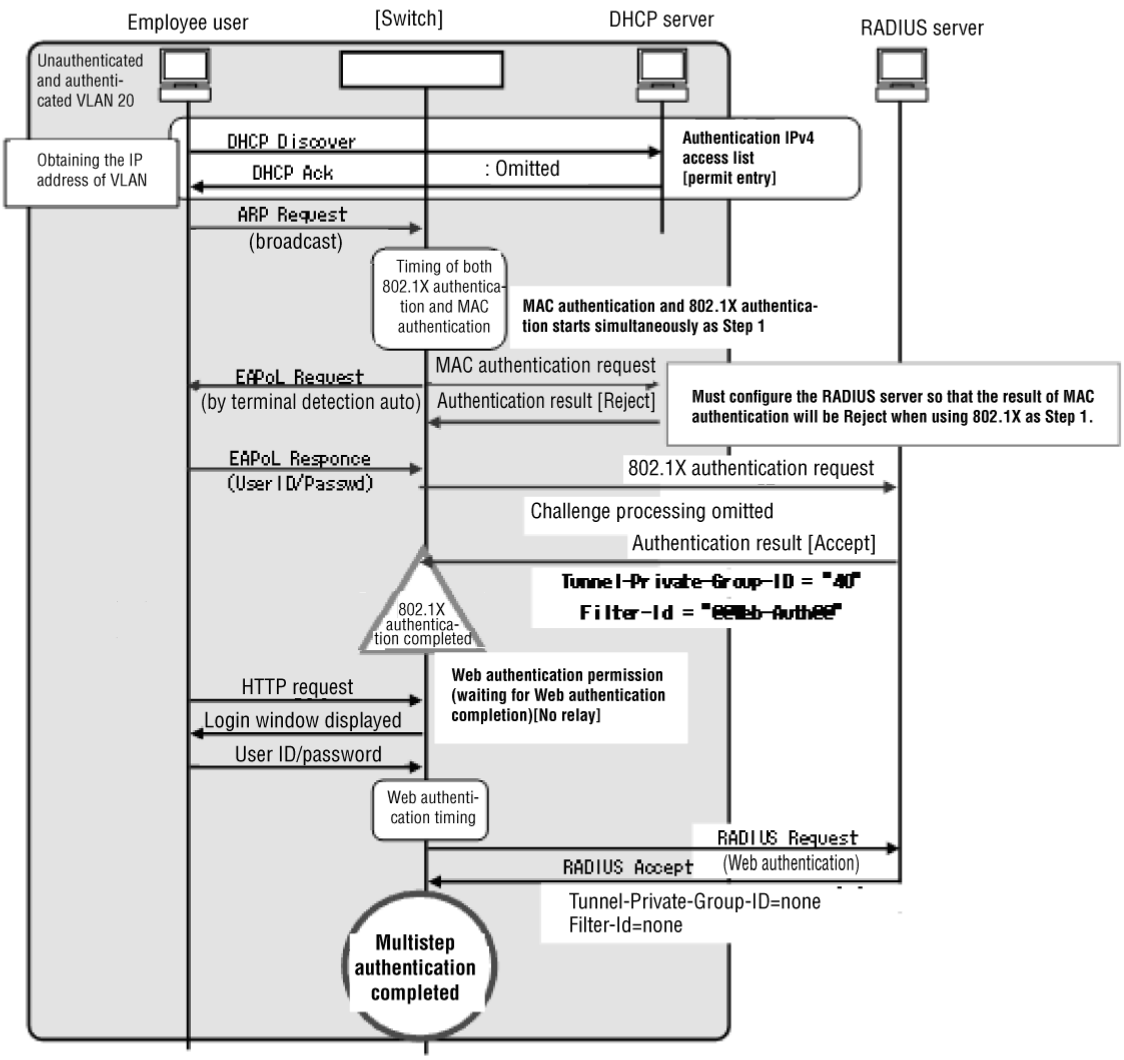


(b) Scenario (x): Employee user authentication overview

Authentication behavior

First, the employee user on a port with the terminal authentication dot1x option obtains an IP address from an authentication IPv4 access list and starts terminal authentication (IEEE 802.1X) by using a frame such as an ARP frame. This will lead the terminal to user authentication (Web authentication), and the traffic from the terminal will have full access after Web authentication.

Figure 12-22 Authentication behavior of employee users (fixed VLAN mode)



Points to note

Table 12-32 Overview of employee users authentication (fixed VLAN mode)

Configuration items	Requirements	Description		Remarks
Authentication IPv4 access list	Required	`permit`	`eq bootps`	Forwards DHCP frames throughout the VLAN
Internal DHCP server of the Switch	Not required	n/a		
External DHCP server	Required	`VLAN 20`		Sets to a post-authentication VLAN

Configuration items	Requirements	Description		Remarks
The RADIUS server	IEEE 802.1X (authenticates MAC address of employee user terminal)	`Tunnel-Private-Group-ID`	Not set	Sends response without `Tunnel-Private-Group-ID`
		`Filter-Id`	"`@@Web-Auth@@`"	Sends response "`@@Web-Auth@@`".
	Web authentication (authenticates employee user ID)	`Tunnel-Private-Group-ID`	Not set	Sends response without `Tunnel-Private-Group-ID`.
		`Filter-Id`	Not set	Responds without `Filter-Id`.

Legend

n/a: Not applicable

(c) Configuring fixed VLAN mode

The following describes the configuration of fixed VLAN mode on a port with the terminal authentication dot1x option.

IEEE 802.1X and Web authentication must be configured for employee user authentication. MAC-based authentication must be configured for printer authentication.

Overview

The example below shows how to set the following items at a port to be authenticated:

- VLAN
- Authentication method
- Access port and VLAN
- Terminal authentication (IEEE 802.1X)
- User authentication (Web authentication)
- Terminal authentication (MAC-based authentication)
- Multistep authentication port (with terminal authentication dot1x option)
- Authentication IPv4 access list

For other configurations necessary for IEEE 802.1X, see *7. IEEE 802.1X Configuration and Operation*. For the configuration necessary for Web authentication, see *9. Web Authentication Configuration and Operation*, and for the configuration necessary for MAC-based authentication, see *11. MAC-based Authentication Configuration and Operation*.

Command examples

1.
```
(config)# vlan 20
(config-vlan)# exit
```

Specifies VLAN ID 20 to be accessed before and after authentication.

2.
```
(config)# aaa authentication dot1x default group radius
(config)# aaa authentication web-authentication default group radius
(config)# aaa authentication mac-authentication default group radius
```
Configures RADIUS authentication for IEEE 802.1X, Web authentication, and MAC-based authentication.

3.
```
(config)# interface fastethernet 0/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 20
```
Specifies the port 0/1 as the access port. Assigns VLAN 20 to the access port.

4.
```
(config-if)# dot1x port-control auto
(config-if)# dot1x multiple-authentication
(config-if)# dot1x supplicant-detection auto
(config-if)# web-authentication port
(config-if)# mac-authentication port
(config-if)# authentication multi-step dot1x
```
Configures IEEE 802.1X, Web authentication, MAC-based authentication, and multistep authentication (with the terminal authentication dot1x option) to port 0/1.

5.
```
(config-if)# authentication ip access-group L2-AUTH
(config-if)# authentication arp-relay
(config-if)# exit
```
Configures an authentication IPv4 access list for frames sent from unauthenticated terminals to port 0/1. Configures the port to forward ARP frames sent from unauthenticated terminals.

6.
```
(config)# ip access-list extended L2-AUTH
(config-ext-nacl)# permit udp any any eq bootps
```
(config-ext-nacl)# exit

Configures an authentication IPv4 access list that forwards DHCP frames (`bootps`) sent from unauthenticated terminals.

Notes

1. Configure the following parameter to the `Filter-Id` RADIUS attribute on the RADIUS server when multistep authentication is set up as above:
   - For an IEEE 802.1X authentication RADIUS server: "`@@Web-Auth@@`"

Note that when the port is set up as shown above, MAC-based authentication and IEEE 802.1X operate simultaneously for terminal authentication. To use IEEE 802.1X to authenticate employee users, specify the configuration so that MAC-based authentication fails (for example, do not assign the terminal to the RADIUS server as a MAC-based authentication target).

12.3 Operation

12.3.1 List of operation commands

The following table describes the operation commands for multistep authentication.

Table 12-33 List of operation commands for multistep authentication

Command	Description
`show authentication multi-step`	Displays the information for authenticated terminals on a multistep authentication port per interface.
`show authentication logging`	Chronologically displays accounting log information for each Layer 2 authentication method starting from the newest entry.

12.3.2 Displaying the multistep authentication status

To display information for authenticated terminals on a multistep authentication port, use the `show authentication multi-step` operation command on the Switch.

Figure 12-23 Example of show authentication multi-step

```
# show authentication multi-step

Date 2009/10/29 06:58:27 UTC
Port 0/1  : multi-step dot1x
    <     Supplicant information     >  <Authentic method>
  No MAC address    State VLAN F Type    Last  (first step)
   1 000d.0b3a.e977 pass   100   multi   web   (dot1x)

Port 0/5  : multi-step
    <     Supplicant information     >  <Authentic method>
  No MAC address    State VLAN F Type    Last  (first step)
   1 0013.20a5.24ab pass    10 * single  mac   (-)

Port 0/22 : multi-step permissive
    <     Supplicant information     >  <Authentic method>
  No MAC address    State VLAN F Type    Last  (first step)
   1 000b.972f.e22b pass   100   single  dot1x (-)
#
```

13. Secure Wake-on-LAN [OP-WOL]

The secure Wake-on-LAN functionality allows you to access the Switch from home or outside the company by using a Web browser to turn on the power to a desktop PC. To turn off the PC, use its normal shutdown functionality.

This chapter describes the details and operation of Secure Wake-on-LAN.

A software option license is required to use this functionality.

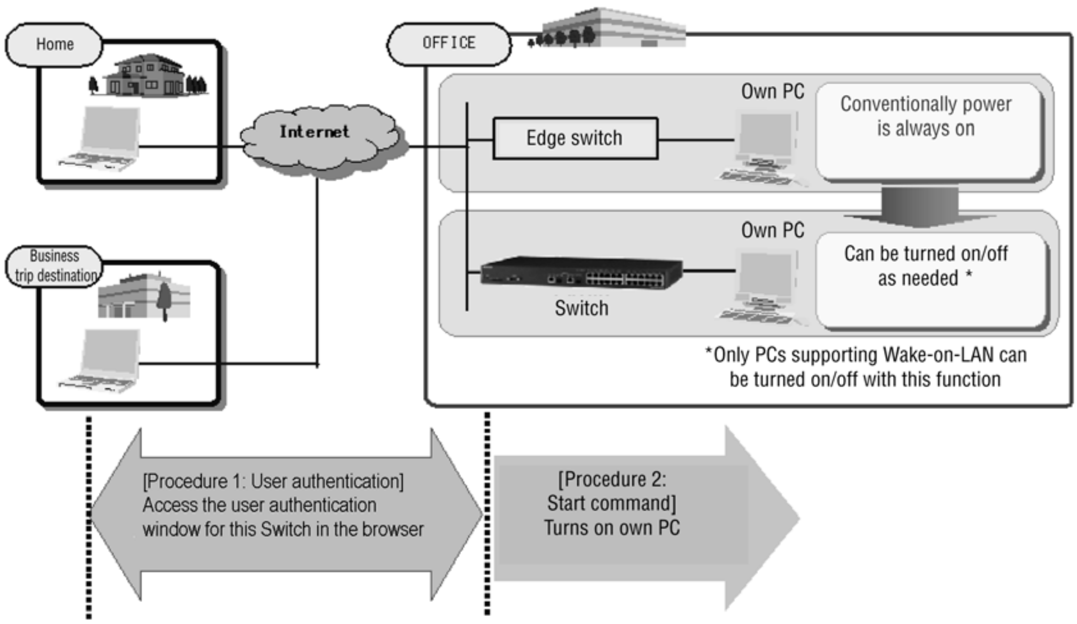
13.1 Overview

This functionality allows access to your PC from outside the company, whether you are at home or on a business trip. You can use a Web browser to access the Switch and, via the in-house network, turn on the power to a desktop PC within the company.

Users can open the user authentication page for the Secure Wake-on-LAN functionality on the Switch but only authenticated users have access to the functionality. Users are authenticated through the user information registered on the user database dedicated to the Secure Wake-on-LAN functionality on the Switch. For authenticated users, terminal information registered on the Switch is displayed in a Web browser, which enables the user to select the PC and send activation commands.

By introducing a remote desktop environment, users can turn desktop PCs on at their discretion, which results in saving energy for the whole system.

Figure 13-1 Overview of the Secure Wake-on-LAN functionality



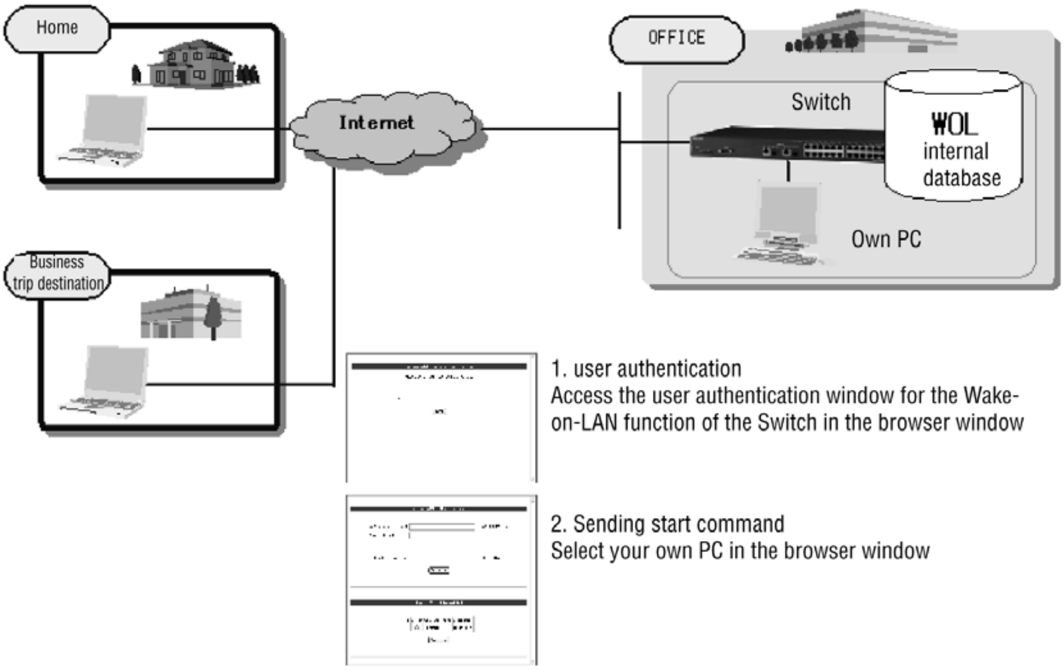
13.1.1 Preparation for using the Switch

With Secure Wake-on-LAN, users access the authentication page using a Web browser, select the target terminal, and send an activation command.

Two types of databases with built-in Wake-on-LAN (WOL) functionality need to be registered on the Switch before use; a database for registering the terminals to which activation commands are sent (hereafter called the *WOL Terminal DB*) and a database for user authentication (the *WOL User DB*).

The two types of databases with internal WOL are reflected on the Switch by entering (`set`) and registering (`commit`) them using the operation commands, as in the internal databases for Web authentication. The databases can be backed up (`store`) and restored (`load`) as well.

Figure 13-2 Example of selecting and sending commands on a Web browser



(1) IP address of the VLAN interface

To access the Secure Wake-on-LAN user authentication page, specify the IP address of the VLAN interface on the Switch. Use configuration commands to specify the IP address.

When specifying the URL to access the Secure Wake-on-LAN user authentication page, you can choose the language: English or Japanese.

- English: `https://`*IP-address-of-VLAN-interface*`/wol/en/wol_login.html`
- Japanese:
  `https://`*IP-address-of-VLAN-interface*`/wol/ja/wol_login.html`

As both pages in English and in Japanese have been registered on the Switch, there is no setting to switch the language. Use the URL above.

(2) Internal DB for registering terminals to which activation commands are sent (WOL Terminal DB)

On the WOL Terminal DB, register the information on the terminals to which activation commands are sent, using Secure Wake-on-LAN (MAC address, VLAN ID, terminal IP address, method for confirming the terminal is activated, and supplementary explanation of the terminal information).

If you register on the WOL Terminal DB such that the activation of the terminal can be confirmed, register the terminal IP address as well. The IP address is necessary because the activation is confirmed by using ping.

- For a terminal in a DHCP environment: Register DHCP.

  Set the DHCP snooping functionality of the Switch as well. When the target terminal is a DHCP client, the activation of the terminal can be confirmed by specifying the IP address distributed by the DHCP server using the DHCP snooping functionality.

For details of the DHCP snooping functionality, see *DHCP Snooping* in the manual *Configuration Guide Vol. 1*.

- For a terminal with a static IP address: Register the static IP address of the terminal.

Register the terminal name registered on the WOL Terminal DB as the name for identifying the terminal access permissions on the WOL User DB which will be described below.

The following table describes the information to register on the WOL Terminal DB

Table 13-1 Information registered on the WOL Terminal DB

<table>
<tr><th colspan="3">Item</th><th colspan="2">Information to be registered</th><th>Default</th><th>Scope of registration</th></tr>
<tr><td colspan="3">Terminal name</td><td colspan="2">Register the name of the terminal to which an activation command is sent in text format.</td><td>None</td><td>128 characters</td></tr>
<tr><td colspan="3">MAC address</td><td colspan="2">Register the MAC address of the terminal to which an activation command is sent.</td><td>None</td><td>In the format of xxxx.xxxx.xxxx</td></tr>
<tr><td colspan="3">VLAN ID</td><td colspan="2">Register the VLAN number of the terminal to which an activation command is sent.</td><td>None</td><td>1 to 4094</td></tr>
<tr><td colspan="3">Method to confirm the activation of the terminal</td><td colspan="2">Register the method for confirming that the terminal to which an activation command is sent is activated.</td><td rowspan="3">Confirmation required</td><td rowspan="3">• Confirmation required
• No confirmation required</td></tr>
<tr><td rowspan="5"></td><td colspan="2">No confirmation required</td><td colspan="2">Register when ping is not used to confirm that the terminal is activated</td></tr>
<tr><td colspan="2">Confirmation required</td><td colspan="2">Register when ping is used to confirm that the terminal is activated. The terminal IP address and the timeout duration for confirming the activation are also registered as shown below.</td></tr>
<tr><td rowspan="3"></td><td rowspan="2">Terminal IP address</td><td>DHCP</td><td>DHCP environment:
Register DHCP which identifies the IP address in liaison with DHCP snooping</td><td rowspan="2">DHCP</td><td rowspan="2">• DHCP
• IPv4 address:
1.0.0.0 to 126.255.255.255
128.0.0.0 to 223.255.255.255</td></tr>
<tr><td>IPv4 address</td><td>Static IP address environment:
Directly register the static IP address of the terminal.</td></tr>
<tr><td>Timeout</td><td colspan="2">Register the timeout duration to confirm that the terminal is activated by using ping..</td><td>120 seconds</td><td>60 to 600 seconds</td></tr>
</table>

Item	Information to be registered	Default	Scope of registration
Supplementary explanation	Register the supplementary explanation of the terminals to which the activation commands are sent in text (specify the user of the terminal, IP address of the static IP terminal, etc.).	None	128 characters

For the details of the device capacities of the WOL Terminal DB, see *3.2 Capacity limits* in the *Configuration Guide Vol. 1*.

(3) Internal DB for user authentication (WOL User DB)

Register the information of the Secure Wake-on-LAN users.

The following table describes the information to be registered.

Table 13-2 Information registered in the WOL User DB

Item	Information to be registered	Default	Scope of registration
User ID	Register the ID of the Secure Wake-on-LAN user.	None	128 letters
Password	Register the password of the Secure Wake-on-LAN user.	None	32 letters
Access permissions to the terminal	Register the access permissions to the terminal of the Secure Wake-on-LAN user.	None	● any ● manual ● Name of the terminal:128 characters
any	Register the access permissions to all terminals. (all terminals registered on the WOL Terminal DB)		
manual	Register the permissions to directly specify MAC address and VLAN ID.		
Terminal name	Register the access permissions to specific terminals. (Specify the terminal name registered on the WOL Terminal DB)		

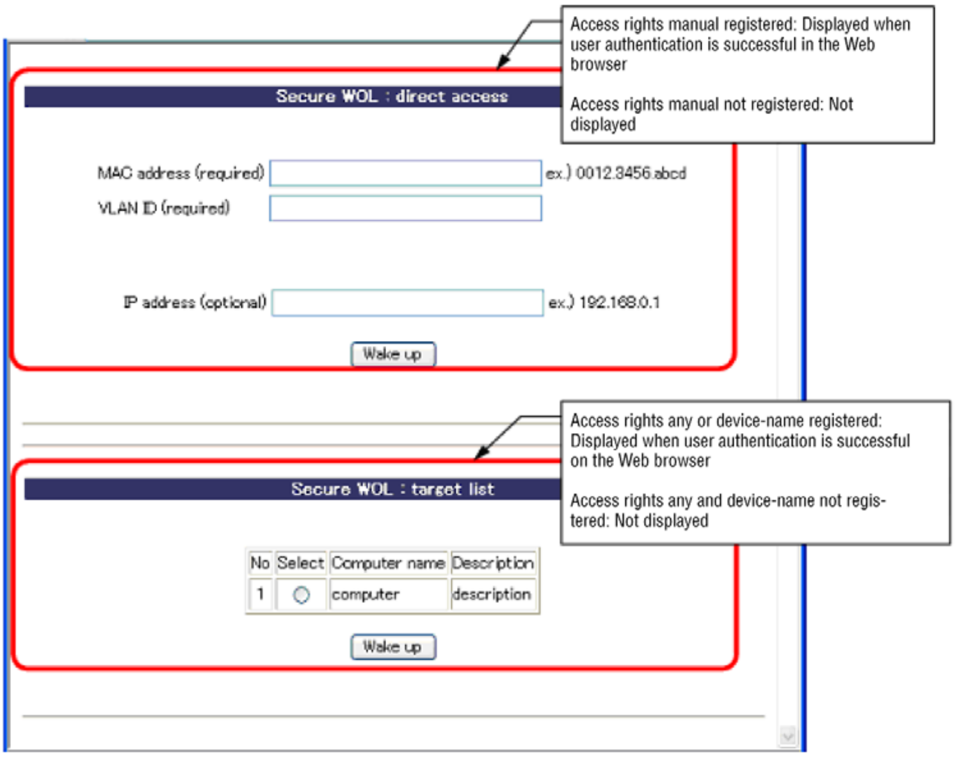
Note

The upper limit on the number of combinations of users and terminals is 300. For example, if you allowed one user to access 300 terminals, then no more access rights to other terminals can be set for the user. The settings of `any` and `manual` are excluded from this limit.

For details of the device capacities of the WOL User DB, see *3.2 Capacity limits* in the *Configuration Guide Vol. 1*.

How the Selecting Terminals and Sending Activation Commands page is displayed in the Web browser varies according to the access permissions registered on the WOL User DB. Shown below is an example of how the page looks like depending on the registered access permissions to the terminals.

Figure 13-3 Example of the Selecting Terminals and Sending Activation Commands page for registering access permissions to the terminal



For details, see *13.3.8 Procedure for selecting and sending commands in a Web browser.*

(4) Using HTTPS servers

To use HTTPS servers, register the server certification. For details, see the manual *Supplement: Web Authentication Manual - SSL Certification Operation*.

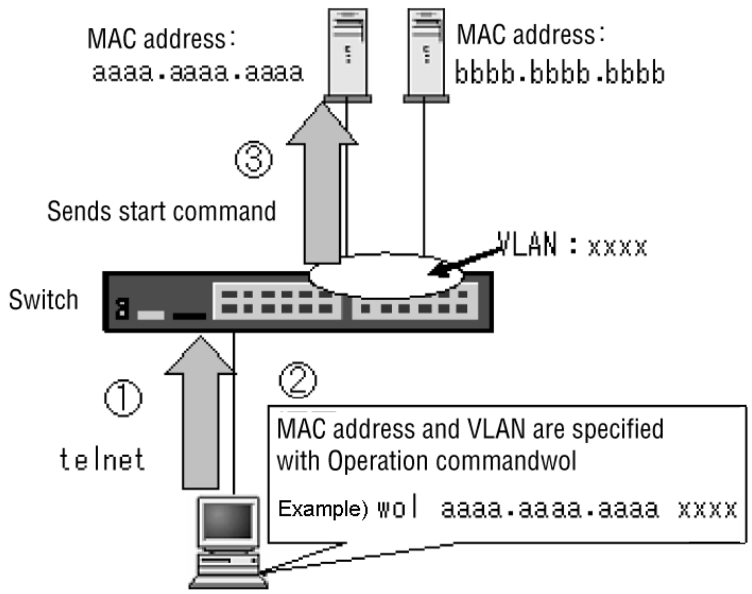
(5) Command direct sending functionality by using operation commands

The Switch supports the command direct sending functionality by using operation commands in addition to selecting andsending commands of a Web browser.

In the command direct sending functionality, specify the MAC address of the desktop PC and the VLAN using the operation command `wol` and send the activation command directly. In this case, the activation command can be sent, even if no IP address is assigned to the target VLAN interface.

Because this functionality allows remote login to the Switch using Telnet and operation commands, it is suitable for operation within the company.

Figure 13-4 Example of the use of the command direct sending functionality



13.1.2 Notes on using Secure Wake-on-LAN

(1) Setting terminals to which the activation command is sent

You can confirm that the terminal to which you sent an activation command is activated via the Switch by using ping, depending on settings in the WOL Terminal DB. When doing this, set `respond to ping` on the target terminal. Some terminals might be set to `do not respond to ping`.

(2) VLAN interface to which the activation command is sent

You can send the activation command, even if no IP address is assigned to the VLAN interface of the target terminal.

(3) Use with Layer 2 functionality

Do not set Layer 2 authentication functionality on the port that connects the Switch and the terminal to which the activation command is sent. If you do this, you might not be able to access your desktop PC remotely from outside the company even after turning on the PC, or you might be able to mistakenly access the user authentication page of the Secure Wake-on-LAN functionality from a terminal that has not yet been authenticated on the port where Web authentication is executed.

It can be used with the Layer 2 authentication functionality within a device. Use different ports for the connection of the terminals in the Secure Wake-on-LAN functionality and for Layer 2 authentication.

13.2 Configuration

13.2.1 List of configuration commands

The following table describes the commands used to configure the Secure Wake-on-LAN functionality.

Table 13-3 List of configuration commands

Command	Description
`http-server`	Enables the HTTP server functionality.

13.2.2 Enabling the HTTP server functionality

Points to note

The example below shows how to enable the HTTP server functionality when the Secure Wake-on-LAN functionality is used.

Command examples

1. `(config)# http-server`

   Enables the HTTP server functionality.

Notes

Configure this command to use the Secure Wake-on-LAN functionality.

13.3 Operation

13.3.1 List of operation commands

The following table describes operation commands for the Secure Wake-on-LAN functionality.

Table 13-4 List of operation commands

Command	Description
`set wol-device name`	Registers on the WOL Terminal DB the information of a new terminal to which the activation command is sent.
`set wol-device mac`	Changes the MAC address of the terminal information registered on the WOL Terminal DB.
`set wol-device vlan`	Changes the VLAN ID of the terminal information registered on the WOL Terminal DB.
`set wol-device ip`	Changes the IP address and method to identify IP address of the terminal information registered on the WOL Terminal DB.
`set wol-device alive`	Changes the method for confirming that the terminal is activated, that is registered as the terminal information on the WOL Terminal DB.
`set wol-device description`	Changes the supplementary explanation of the terminal information registered on the WOL Terminal DB.
`remove wol-device name`	Deletes the terminal information registered on the WOL Terminal DB.
`show wol-device name`	Displays the terminal information being edited or already registered on the WOL Terminal DB.
`commit wol-device`	Stores the terminal information edited on the WOL Terminal DB in a built-in flash memory and reflects it in the operation.
`store wol-device`	Creates a backup file of the WOL Terminal DB.
`load wol-device`	Restores the WOL Terminal DB from a backup file.
`set wol-authentication user`	Registers new user information (user ID, password, and access permissions to the terminal) on the WOL User DB.
`set wol-authentication password`	Changes the password of the user registered on the WOL User DB.
`set wol-authentication permit`	Changes (adds or deletes) the information of the terminals accessible from users registered on the WOL User DB.
`remove wol-authentication user`	Deletes the user information being edited on the WOL User DB.

Command	Description
`show wol-authentication user`	Displays user information being edited or already registered on the WOL User DB.
`commit wol-authentication`	Reflects the edited parts of on the WOL User DB on the operation.
`store wol-authentication ramdisk`	Creates a backup file of the WOL User DB.
`load wol-authentication ramdisk`	Restores the WOL User DB.
`wol`	Specifies the MAC address and VLAN of your desktop PC and directly sends the activation command.
`show wol`	Displays the information of the users currently using the Secure Wake-on-LAN functionality from Web browsers.

Legend:

WOL Terminal DB: Internal DB for registering terminals to which activation commands are sent

WOL User DB: Internal DB for user authentication

13.3.2 Registering, changing, and deleting on the WOL Terminal DB

Register data on the internal DB for registering terminals to which activation commands are sent (*WOL Terminal DB*), which is used with the Secure Wake-on-LAN functionality. Register on the WOL Terminal DB the name of the terminal to which activation commands are sent, MAC address, VLAN, and confirmation of the activation of the terminal. The procedure includes the change (addition, change, and deletion) of the WOL Terminal DB and the reflection of the revised data on the database. Shown below are examples of the registration.

(1) Registering new data on the WOL Terminal DB

For each user of the Secure Wake-on-LAN functionality, register the name of the terminal, MAC address, VLAN, and confirmation of the activation of the terminal using the `set wol-device name` operation command.

In the following example, data for three terminals are registered.

Command input

```
# set wol-device name PC01 1234.5600.6fd4 4094 ip 202.68.133.72 alive check
timeout 300 description change-user
# set wol-device name pc.20082001.abc 1234.5600.ff02 2000 ip 202.68.133.71
alive check
# set wol-device name pc.20082002.abc 1234.5600.ff03 2000 ip 202.68.133.75
alive nocheck description notePC
```

(2) Changing and deleting on the WOL Terminal DB

Follow the procedure below to change or delete the registered terminal information.

(a) Changing MAC address

To change the MAC address of a registered terminal, use the `set wol-device mac` operation command. The following example illustrates the change in the MAC address of the terminal (`pc.20082001.abc`).

Command input

```
# set wol-device mac pc.20082001.abc 1234.5600.ffe1
```
Changes the MAC address of the terminal (`pc.20082001.abc`) to 1234.5600.ffe1.

(b) Changing VLAN

To change the VLAN of the registered terminal, use the operation command `set wol-device vlan`.

The following example illustrates the change in the VLAN of the terminal (`pc.20082001.abc`).

Command input

```
# set wol-device vlan pc.20082001.abc 4000
```
Changes the VLAN of the terminal (`pc.20082001.abc`) to 4000.

(c) Deleting terminal information

To delete the information of a registered terminal, use the `remove wol-device name` operation command. The following example illustrates the deletion of the terminal (`pc.20082001.abc`).

Command input

```
# remove wol-device name pc.20082001.abc
Remove wol-device name.  Are you sure? (y/n): y

#
```
Deletes the information of the terminal (`pc.20082001.abc`).

(3) Displaying the WOL Terminal DB

To display the status of editing or registering the WOL Terminal DB, use the `show wol-device name` operation command.

Figure 13-5 Displaying the WOL Terminal DB

```
# show wol-device name edit

Date 2008/11/06 14:48:49 UTC
 Total device counts:   5
  No Device name   MAC           VLAN IP address     Alive    Description
   1 PC01         1234.5600.6fd4 4094 202.68.133.72   300      change-user
   2 PC02         00ee.16fd.a142  100 10.1.10.10     600     all-user-...
   3 PC03_High...  0022.fa12.34dd  10 dhcp           60      High_price
   4 PC04         04ff.d423.f145    5 dhcp          120
   5 PC05         0612.7faf.1fdd 2000 202.68.133.70   no-check notePC

#
```

(4) Reflecting data on the WOL Terminal DB

To reflect the edited terminal information on the WOL Terminal DB, use the `commit wol-device` operation command.

Command input

```
# commit wol-device
Commitment wol-device name data.  Are you sure? (y/n): y

Commit complete.
#
```

13.3.3 Backing up and restoring the WOL Terminal DB

The following are examples of creation of a backup file of the WOL Terminal DB and restoration of the database from the backup file.

(1) Baking up the WOL Terminal DB

Use the `store wol-device` operation command to create a backup file of the WOL Terminal DB (`backupfile` in the following example).

Command input

```
# store wol-device ramdisk backupfile
Backup wol-device name data.  Are You sure? (y/n): y

Backup complete.
#
```

(2) Restoring the WOL Terminal DB

Use the `load wol-device` operation command to restore the WOL Terminal DB from the backup file (`backupfile` in the following example).

Command input

```
# load wol-device ramdisk backupfile
Restore wol-device name data.  Are you sure? (y/n): y

Restore complete.
#
```

13.3.4 Registering, changing, and deleting on the WOL User DB

Register data on the internal DB for user authentication (hereinafter WOL User DB), which is used with the Secure Wake-on-LAN functionality. Register on the WOL User DB the ID of the Secure Wake-on-LAN, user, password, access permissions, and the names of the accessible terminals. The procedure includes the edit (addition, change and deletion) of the WOL User DB and the reflection of the edited data on the database. Shown below are examples of the registration.

(1) Registering new data on the WOL Terminal DB

For each user of the Secure Wake-on-LAN functionality, register user ID, password, access permissions to the terminal and the names of the accessible terminals, using the `set wol-authentication user` operation command.

In the following example, data for three terminals are registered.

Command input

```
# set wol-authentication user user01.example.abc.com pass01 permit
device-name pc.20082001.abc
# set wol-authentication user user02.example.abc.com pass02 permit
device-name pc.20082002.abc
```

```
# set wol-authentication user user03.example.abc.com pass03 permit
device-name pc.20082003.abc
```

(a) Checking consistency between the registered WOL Terminal DB and WOL User DB

When registering the name of an accessible terminal (`device-name`) on the WOL User DB, check the entry using the `show wol-authentication user` operation command. An asterisk (`*`) added to the entry means that the name of the target terminal is not registered on the WOL Terminal DB. (For an example of the display, see, *(3) Displaying the WOL User DB* below.)

After checking the terminal name with the operation command `show wol-device-name`, change the entry by referring to *(b) Changing (adding or deleting) the information of an accessible terminal* in *(2) Changing and deleting on the WOL User DB*. You cannot select the target terminal in the procedure for selecting and sending commands of a Web browser until the asterisk is hidden.

(2) Changing and deleting on the WOL User DB

Follow the procedure below to change or delete registered user information.

(a) Changing the password

To change the password of a registered user, use the `set wol-authentication password` operation command. The following example shows how to change the password of a user (ID: `user01.example.abc.com`).

Command input

```
# set wol-authentication password user01.example.abc.com pass01 pass1001
```

Changes the password of a user (ID: `user01.example.abc.com`) from `pass01` to `pass1001`.

(b) Changing (adding or deleting) the information of an accessible terminal

To change (add or delete) the information of the accessible terminal of a registered user, use the operation command `set wol-authentication permit`. The following example shows how to add the information of the terminal to which a user (ID: `user02.example.abc.com`) can access.

Command input

```
# set wol-authentication permit user02.example.abc.com add device-name
pc.20083002.abc
```

Adds `pc.20083002.abc` to the information of the terminal to which a user (ID: `user02.example.abc.com`) can access.

(c) Deleting user information

To delete the information of a registered user, use the `remove wol-authentication user` operation command. The following example shows how to delete the information of a user (ID:`user01.example.abc.com`).

The following example shows how to delete the information of a user (ID:`user01.example.abc.com`).

Command input

```
# remove wol-authentication user user01.example.abc.com
```

```
Remove wol-authentication user.  Are you sure? (y/n): y

#
```

Deletes the user (ID: `user01.example.abc.com`).

(3) Displaying the WOL User DB

To display the status of editing or registering the WOL User DB, use the `show wol-authentication user` operation command.

Figure 13-6 Displaying the WOL User DB

```
# show wol-authentication user edit

Date 2008/11/06 20:48:57 UTC
  Total user counts:   5
  Total device link:   7
   No any     manual  device  Username
    1 deny    deny        2  Mail-Address_of_USER04_of_The_Company...
    2 permit  permit      1  USER01
*   3 deny    permit      3  USER02
    4 permit  deny        0  USER03
*   5 permit  deny        1  USER05

#
```

An asterisk (`*`) added to the user means that the name of the user is not registered on the WOL Terminal DB. Select the `detail` option to display the names of the terminals registered for the user. Check which terminal has an asterisk (`*`).

Figure 13-7 Displaying the WOL User DB (with the detail option specified)

```
# show wol-authentication user edit detail

Date 2008/11/06 20:49:10 UTC
 No    1 : Mail-Address_of_USER04_of_The_Company@example.com
  permit : any=deny, manual=deny
   device-name
        1  : PC01
        2  : PC03_High-Speed_machine

 No    2 : USER01
  permit : any=permit, manual=permit
   device-name
        1  : PC01

 No    3 : USER02
  permit : any=deny, manual=permit
   device-name
    *   1  : PC02@
        2  : PC01
        3  : PC03_High-Speed_machine

 No    4 : USER03
  permit : any=permit, manual=deny

 No    5 : USER05
  permit : any=permit, manual=deny
   device-name
    *   1  : PC04@
```

```
#
```

(4) Reflecting data on the WOL User DB

To reflect the edited user information on the WOL User DB, use the `commit wol-authentication` operation command.

Command input

```
# commit wol-authentication
Commitment wol-authentication user data. Are you sure? (y/n): y

Commit complete.
#
```

13.3.5 Backing up and restoring the WOL User DB

The following are examples of creating a backup file for the WOL User DB and restoring the database from the backup file.

(1) Baking up the WOL User DB

Use the `store wol-authentication` operation command to create a backup file for the WOL User DB (`backupfile` in the following example).

Command input

```
# store wol-authentication ramdisk backupfile
Backup wol-authentication user data.  Are you sure? (y/n): y

Backup complete.
#
```

(2) Restoring the WOL Terminal DB

Use the `load wol-authentication` operation command to restore the WOL User DB from the backup file (`backupfile` in the following example).

Command input

```
# load wol-authentication ramdisk backupfile
Restore wol-authentication user data.  Are you sure? (y/n): y

Restore complete.
#
```

13.3.6 Displaying information of a user using the Secure Wake-on-LAN

Use the `show wol` operation command to display the information of a user using the Secure Wake-on-LAN. Check the status of sending the activation commands or accessing the terminal on the display.

Figure 13-8 Displaying the information of a user using the Secure Wake-on-LAN

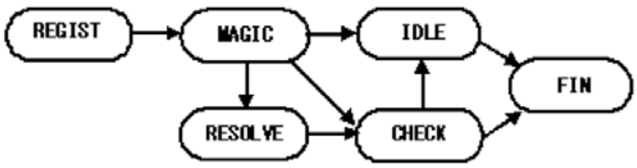
```
# show wol

Date 2008/11/06 17:32:25 UTC
 No User name                          Phase   Magic  Device IP      Target
  1 User-A                            IDLE    -      -             Timeout
  2 User-B                            CHECK   Sent   192.168.1.102   Waiting
  3 User-C                            IDLE    Sent   192.168.10.100  Alive
  4 User-D                            RESOLVE Failed Waiting         -
```

```
  5 User-E                          RESOLVE Sent   Waiting        -
  6 Mail-Address_of_USER04_of_The_Co... IDLE    Sent   202.68.133.72   Alive

#
```

Figure 13-9 Basic phase transition



REGIST: user authentication initial status

MAGIC: Start command can be issued while selected terminal has been information entered

RESOLVE: IP resolve monitoring status of a DHCP terminal

CHECK: Terminal monitoring status

IDLE: Reserved due to a series of processes completed or request timeout

FIN: The last update request completed or completing due to request timeout

The maximum number of users who can simultaneously use the Secure Wake-on-LAN functionality is 32. When the maximum of 32 has been reached, no more users are allowed to use the functionality. If you are unable to use it, verify that the number of users displayed by the command is 32.

13.3.7 Command direct sending functionality

Log in to the Switch and directly send the activation command to the terminal using operation command.

Command input

```
# wol 1234.5600.00fe 4000
The magic packet is sent.

#
```

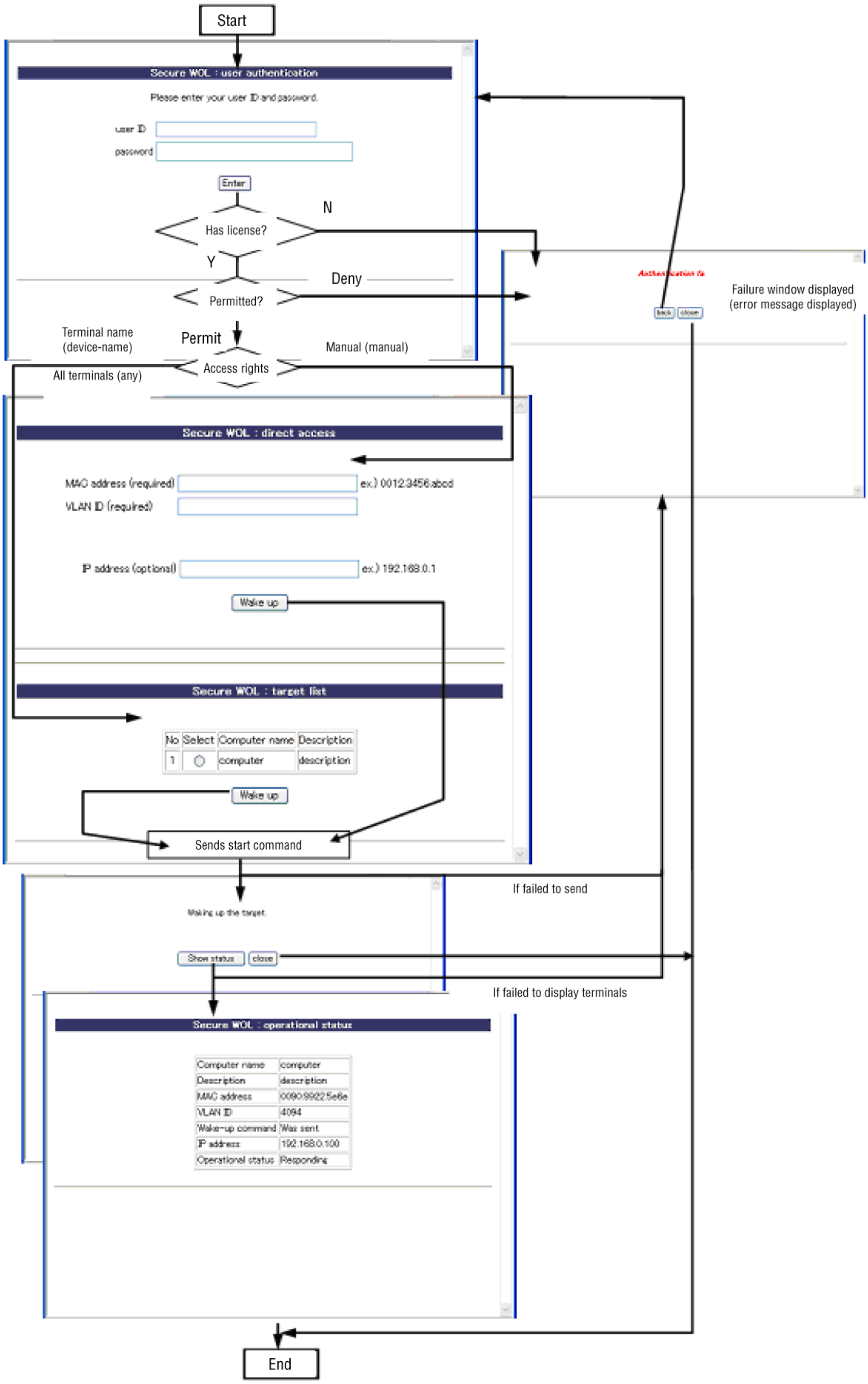
13.3.8 Procedure for selecting and sending commands in a Web browser

This section explains the procedure for executing the Secure Wake-on-LAN functionality from outside the company. After configuring the Switch as required for the Secure Wake-on-LAN functionality and setting the WOL User DB and the WOL Authentication DB, follow the procedure below.

The recommendation is to follow the procedure in SSL (HTTPS) for security reasons.

Choose either English or Japanese for the language used on the operation page. English is used in the examples in this section.

Figure 13-10 Page sequence of selecting and sending commands in a Web browser



(1) Accessing to the Secure Wake-on-LAN user authentication page

Before accessing the Secure Wake-on-LAN user authentication page, choose the language, either English or Japanese.

- English: `https://`*IP-address-of-VLAN-interface*`/wol/en/wol_login.html`
- Japanese: `https://`*IP-address-of-VLAN-interface*`/wol/ja/wol_login.html`

The Secure Wake-on-LAN user authentication page is displayed. Enter your use ID and password.

Figure 13-11 Secure Wake-on-LAN user authentication page

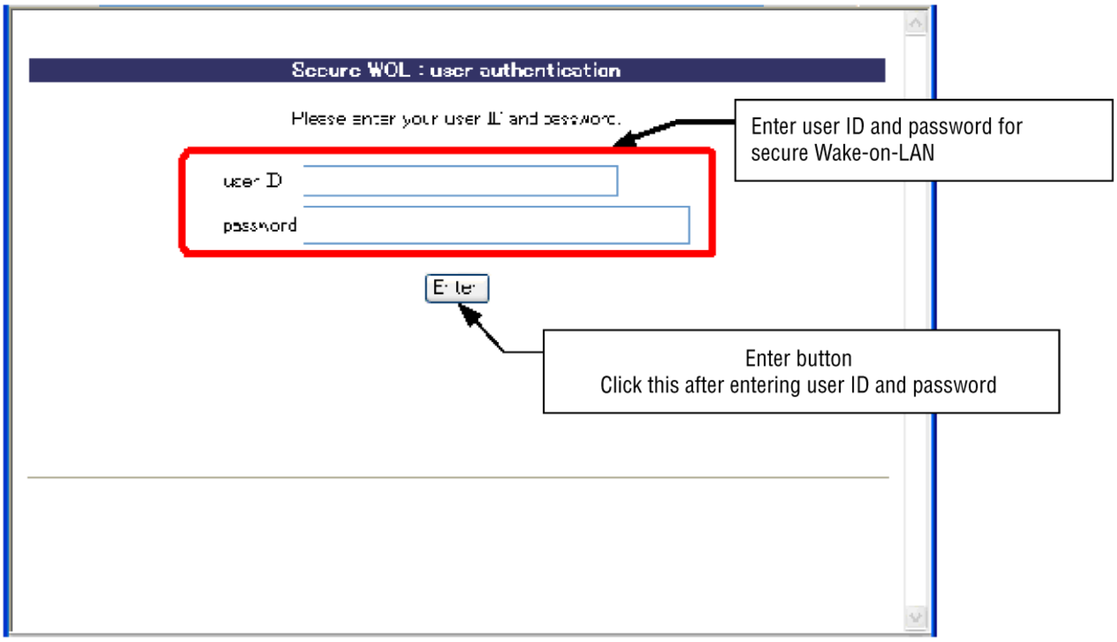


Table 13-5 Displays on the user authentication page

Displays in English	Displays in Japanese
`Secure WOL : user authentication`	セキュア WOL：ユーザ認証
`Please enter your user ID and password.`	ユーザ ID とパスワードを入力してください。
`user ID`	ユーザ ID
`password`	パスワード
`Enter`	実行

(2) Authenticating the user ID and password entered on the user authentication page

Verify that the entered user ID and password match the user information of the WOL User DB registered on the System.

When they are the same, the *Figure 13-13 Selecting Terminals and Sending Activation Commands page* is displayed.

When they are not the same, the *Figure 13-12 Failure in the Secure Wake on the LAN page* is displayed.

- Click the **back** button to restart from the user authentication page.
- Click the **close** button to terminate.

Figure 13-12 Failure in the Secure Wake on the LAN page

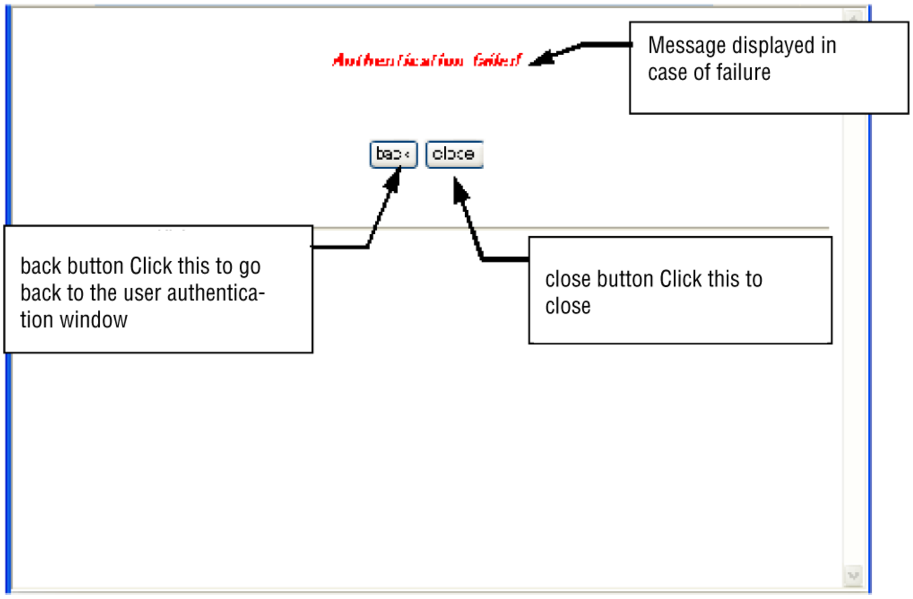


Table 13-6 Displays on the failure page

Displays in English	Displays in Japanese
See *Table 13-7 List of messages displayed on the failure page*.	
back	戻る
close	閉じる

Table 13-7 List of messages displayed on the failure page

No.	Displays in English	Displays in Japanese
①	License key is not installed.	セキュア WOL ソフトウェアオプションライセンスキーが未設定です。
②	Target not selected; redo from authentication.	端末が選択されていません。再度，ユーザ認証からやりなおしてください。
③	Session timeout.	セッションがタイムアウトしました。

No.	Displays in English	Displays in Japanese
④	`Invalid specification; redo from authentication.`	入力情報に誤りがあります。再度，ユーザ認証からやりなおしてください。
⑤	`WOL server busy; try again after a minute.`	セキュア WOL サーバがビジーです。少し待ってから再度実行してください。
⑥	`Authentication failed.`	認証が失敗しました。
⑦	`User engaged; try again after a minute.`	ユーザ ID が重複しています。少し待ってから再度実行してください。

Table 13-8 Details of messages or actions to be taken

No.	Description
①	The Secure Wake-on-LAN software option license key has not been set.
②	There is an error in the terminal information you entered. Check the problem and retry the operation. ● The terminal name you entered is not registered on the WOL Terminal DB. ● The terminal name was not selected.
③	The user information you entered has expired. Retry from the user authentication page.
④	There is an error in the information you entered. Check the problem and retry the operation. ● You have not entered all the required parameters. ● There is an error in the information you entered.
⑤	The number of users has reached the upper limit of the Secure Wake-on-LAN functionality. Retry the operation later.
⑥	You entered an incorrect user ID or password. Check the user ID and password and retry from the user authentication page.
⑦	The entered user ID has already been authenticated. The terminal is currently being activated.

(3) Selecting Terminals and Sending Activation Commands

After the user has successfully been authenticated on the user authentication page of the Secure Wake-on-LAN, the Selecting Terminals and Sending Activation Commands page is displayed.

Figure 13-13 Selecting Terminals and Sending Activation Commands page

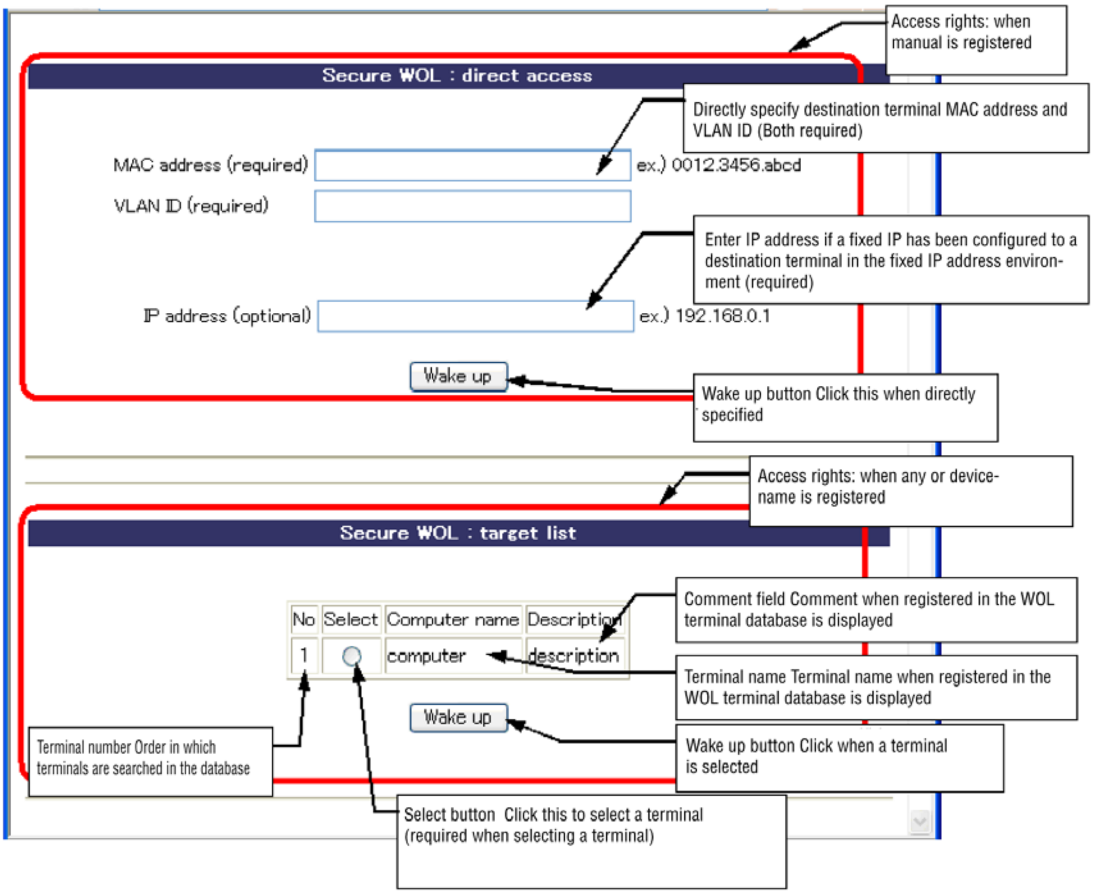


Table 13-9 Displays on the Directly Specifying Device Information page

Displays in English	Displays in Japanese
`Secure WOL : direct access`	セキュア WOL：機器情報直接指定
`MAC address (mandatory)`	MAC アドレス（入力必須）
`VLAN ID (mandatory)`	VLAN ID（入力必須）
`IP address (if known)`	IP アドレス（任意）
`Wake up`	起動開始

Table 13-10 Displays on the Selecting the Target Device page

Displays in English	Displays in Japanese
`Secure WOL : target list`	セキュア WOL：対象機器選択
`#`	No

Displays in English	Displays in Japanese
`Select`	選択
`Computer name`	機器名
`Description`	コメント
`Wake up`	起動開始

The Directly Specifying Device Information page and the Selecting the Target Device page are displayed on the Selecting Terminals and Sending Activation Commands page.

- The Directly Specifying Device Information page is displayed at the top of the page
- The Selecting the Target Device page is displayed at the bottom of the page

Enter the terminal information on either page, and then click the **Wake up** button. Then, a page that tells the completion of transmission is displayed. (See *Figure 13-15 Example of the page displayed after sending the activation command*.)

If the access permissions to the terminal (manual/any/device-name) are not registered, the message `Not available` is displayed. (See *Figure 13-14 Example of the Access Right to the Terminal Not Registered page.)*

(a) Directly Specifying Device Information page (Secure WOL: direct access)

The page is displayed when `manual` is specified for the access permissions to the terminal of the WOL User DB registered on the Switch. If `manual` is not registered, this page is not displayed.

On this page, directly specify the terminal MAC address and VLAN ID to send the activation command. After sending the command, the activation of the terminal to which the command is sent is confirmed.

When a static IP address is set on the terminal in a static IP address environment, specify the IP address.

(b) Selecting the Target Device page (Secure WOL: target list)

The page is displayed when `device-name` is registered for the right to access the terminal of the WOL User DB registered on the Switch. If `any` is registered, all terminal information registered on the WOL Terminal DB is displayed.

If neither of `device-name` nor `any` is registered, no page for terminal selection is displayed.

On this page, select a terminal from among the terminal information registered on the target user in the WOL User DB to send the activation command.

(c) Access Rights to the Terminal Not Registered page

If the right to access the terminal has not been registered, the pages below are displayed.

Figure 13-14 Example of the Access Right to the Terminal Not Registered page

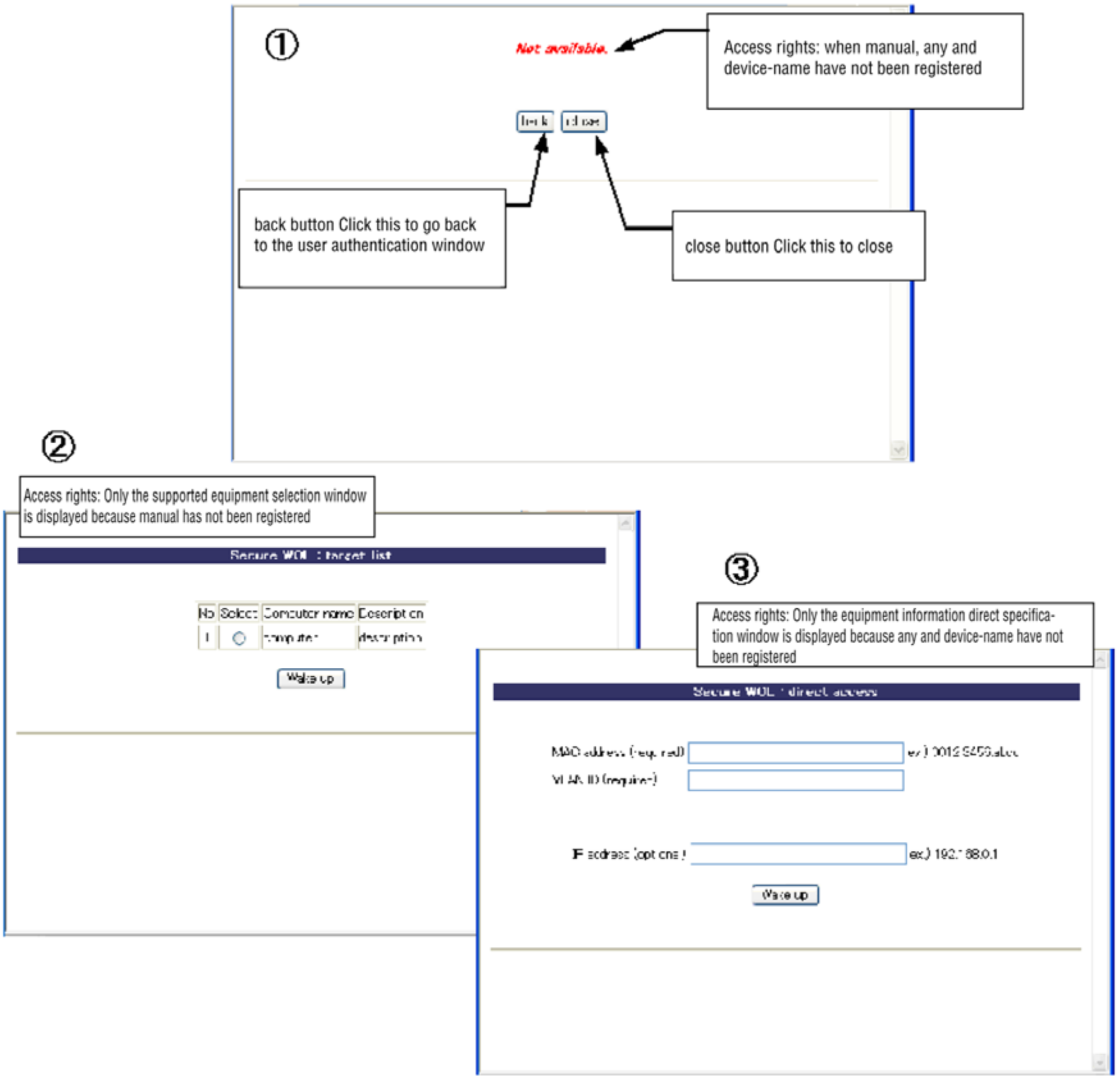


Table 13-11 Access Rights to the Terminal Not Registered page ((1) in the figure above)

Displays in English	Displays in Japanese
`Not available.`	実行できません。
`back`	戻る
`close`	閉じる

- Access rights in (2) of the figure above: Display of the page where `any` and `device-name` have not been registered

  See *Table 13-9 Displays on the Directly Specifying Device Information page.*

- Access rights in (3) of the figure above: Display of the page where `manual` has not been registered

See *Table 13-10 Displays on the Selecting the Target Device page.*

(d) Page displayed after sending the activation command

Click the **Wake up** button on the pages to directly specify or select terminals to display the page below.

Figure 13-15 Example of the page displayed after sending the activation command

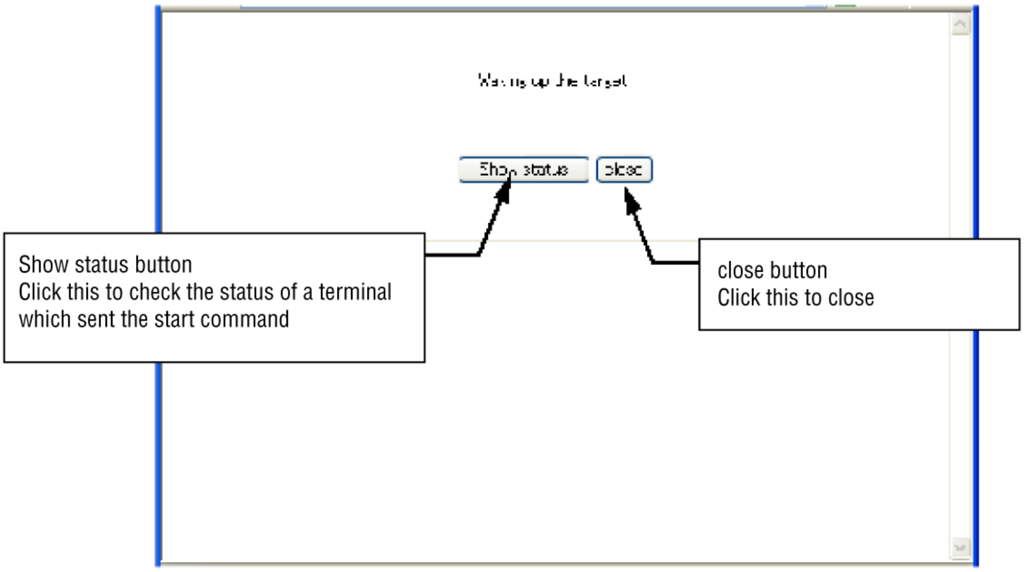


Table 13-12 Page displayed after sending the activation command

Displays in English	Displays in Japanese
`Waking up the target.`	起動処理中
`Show status`	状況確認
`close`	閉じる

- To check the activation status of the target terminal, click the **Show status** button. *Figure 13-16 Page to check the operation status of the terminal to which the activation command is sent* is displayed.
- Click the **close** button to terminate.

(4) Checking the operation status of the terminal to which the activation command is sent

It displays the operation status of the terminal to which the activation command is sent. The page is automatically updated every five seconds.

Figure 13-16 Page to check the operation status of the terminal to which the activation command is sent

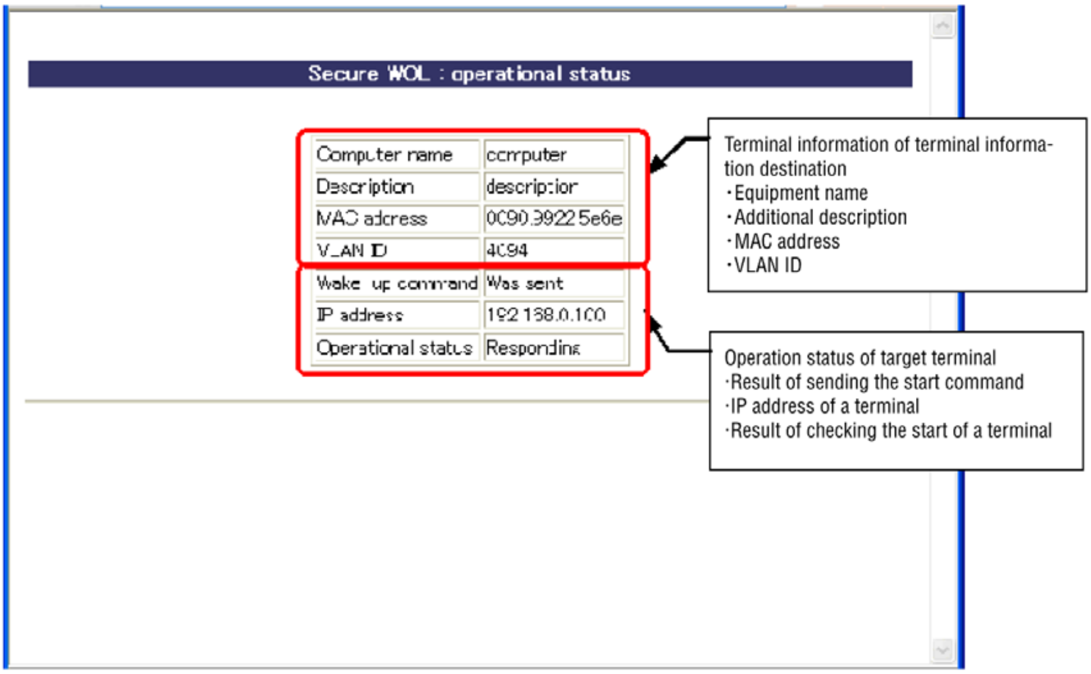


Table 13-13 Displays on the page to check the operation status of the terminal to which the activation command is sent

Displays in English	Displays in Japanese
`Secure WOL : operational status`	セキュア WOL：動作状態
`Computer name`	機器名
`Description`	コメント
`MAC address`	MAC address
`VLAN ID`	VLAN ID
`Wake-up command`	起動コマンド
`IP address`	IP アドレス
`Operational status`	動作状態

Table 13-14 Displays of the information of the terminal to which the activation command is sent

Item	Description
`Computer name`	Name of the terminal (name registered on the WOL Terminal DB)

Item	Description
`Description`	Supplementary explanation (of the terminal registered on the WOL Terminal DB)
`MAC address`	MAC address of the terminal (registered on the WOL Terminal DB)
`VLAN ID`	VLAN ID of the terminal (registered on the WOL Terminal DB)

Table 13-15 Display of the operation status of the target terminal

Item	Displays in English	Displays in Japanese	Meaning
Wake-up command	`Preparing`	準備中	Preparing the activation command for the target terminal
	`Sending`	送信中	Sending the activation command for the target terminal
	`Was sent`	送信済	The activation command has been sent to the target terminal.
IP address	--	--	The activation command has not been sent to the target terminal.
	`Sensing`	検出中	Detecting the IP address of the target terminal by the DHCP snooping functionality
	<IP address>	IP アドレス値	IP address of the target terminal
	`Unknown`	不明	● Suspended before identifying the IP address of the target terminal (timeout) ● The IP address of the target terminal unknown doe to the invalidity of the DHCP snooping functionality
Operational status	--	--	Have not configured the settings for confirming that the target terminal is activated in the WOL Terminal DB.
	`Sensing`	検出中	Processing of the IP address of the target terminal has not been completed.
	`Waiting for a response`	応答待ち	Waiting for a response from the target terminal
	`Responding`	応答あり	Received the response from the target terminal
	`Not responding`	応答なし	Have not received the response from the target terminal (time-out)

14. One-time Password Authentication [OP-OTP]

The Switch provides Web authentication and login authentication functionality, linking with RSA SecurID and using one-time password authentication functionality.

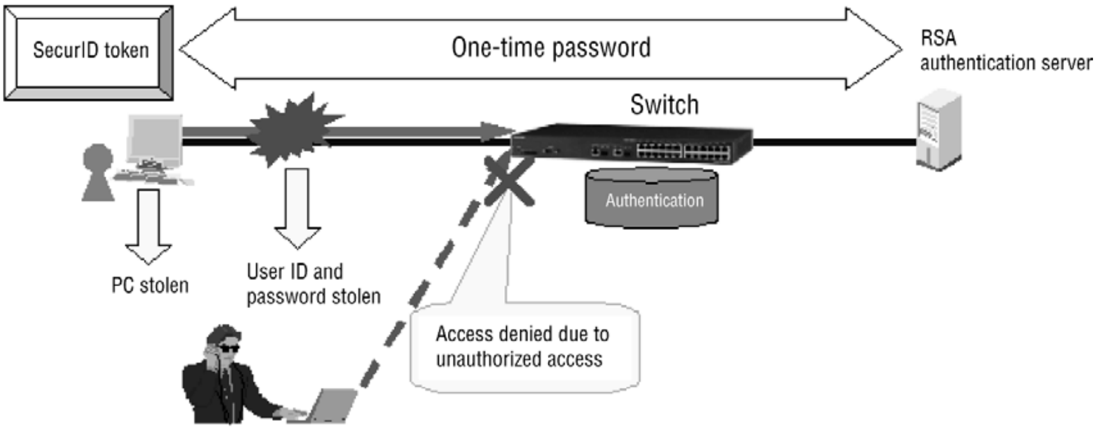
This chapter describes the operation of one-time password authentication.

A software option license is required to use this functionality.

14.1 Overview

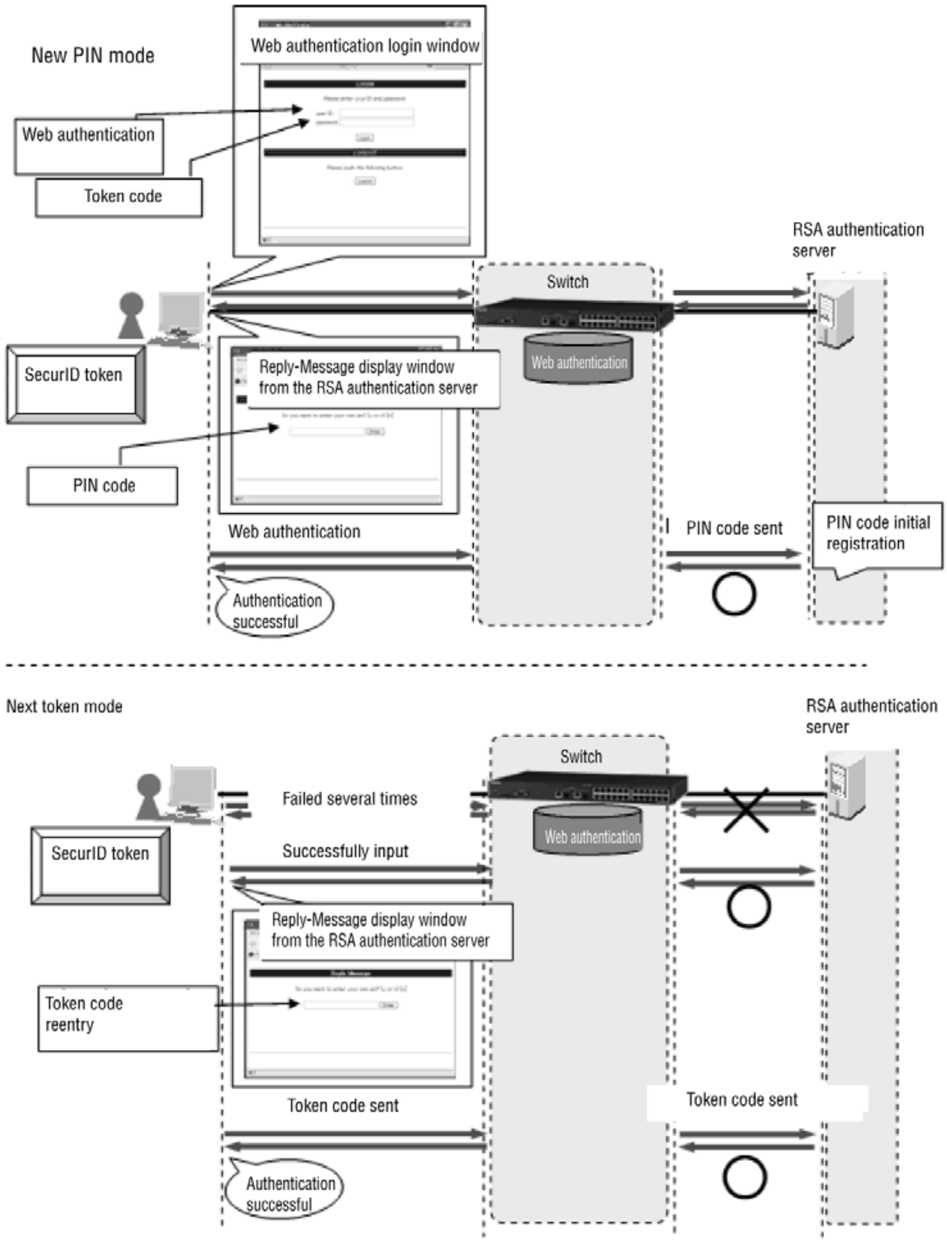
The Switch prevents unauthorized access through Web authentication or login authentication by using the one-time password authentication functionality of RSA SecurID.

Figure 14-1 Overview of one-time password authentication



When the software option license key that you purchased is registered, users are allowed to use the New PIN mode and Next Token mode.

Figure 14-2 When registering a software option license key



- New PIN mode

  Instead of registering a PIN code on the RSA authentication server beforehand, users can register the code during the first access.

- Next Token mode

  If users enter the correct user ID and password after several successive login failures, they can re-enter the token code.

Table 14-1 Scope of the support provided by the software option license

Item	Software option license registered	Software option license not registered
Token code and PIN code entry when logging in	Y	Y
New PIN mode	Y	N
Next Token mode	Y	N

Legend:

Y: Applicable; N: Not applicable

14.1.1 Applicability of authentication

(1) Applicability of one-time password authentication

On a Switch, one-time password authentication can be used for Web authentication and login authentication. The following tables describe the applicability to Web authentication and login authentication.

(a) Web Authentication

In Web authentication, the New PIN mode and Next Token mode can be used for any authentication mode.

Table 14-2 Applicability of one-time password authentication in Web authentication

Authentication mode	Local authentication	RADIUS authentication	One-time password authentication (applicability of New PIN mode and Next Token mode)
Fixed VLAN mode	Y	Y	Y
Dynamic VLAN mode	Y	Y	Y
Legacy mode	Y	Y	Y

Legend:

Y: Applicable

(b) Login authentication

In login authentication, the applications where New PIN mode and Next Token mode can be used are limited.

Table 14-3 Applicability of one-time password authentication in login authentication

Login method	Local authentication	RADIUS authentication	One-time password authentication (applicability of New PIN mode and Next Token mode)
Serial	Y	N	N

Login method	Local authentication	RADIUS authentication	One-time password authentication (applicability of New PIN mode and Next Token mode)
telnet	Y	Y	Y
ftp	Y	Y	N

Legend:

Y: Applicable; N: Not applicable

(2) Error messages displayed when using one-time password authentication

The following table describes the error messages displayed on the login failure screen when using one-time password authentication for Web authentication. (For details about error messages other than those described below, see *8.7 Authentication error messages* in *8 Description of Web Authentication*.)

Table 14-4 Error messages displayed when using one-time password authentication

Error message	Error no.	Cause
`Invalid sequence. Please retry again.`	91	Authentication failed because the response to the PIN code from the RSA authentication server was not received within the designated waiting time.
	92	Authentication failed for the following reasons: ● The terminal connection information of the user who sent the result of the response of a PIN code changed. ● The Switch and the session code of the user are inconsistent.
	93	Authentication failed because the user is invalid due to failure in receiving the response to the PIN code from the RSA authentication server.

14.1.2 Screen files displaying Reply-Message

This functionality uses authentication-in-progress screen files (`loginProcess.html` files) in addition to the Web authentication page files shown in section *8.10 Procedure for creating Web authentication pages* in *8. Description of Web Authentication*.

The authentication-in-progress screen file is an HTML file used to display the Reply-Message in the Access-Challenge sent from the RADIUS server and received by the Switch, and to send the entered PIN code.

(1) Authentication-in-progress screen file (loginProcess.html)

(a) Condition for setting

To create an HTML file for the authentication-in-progress screen, include all tags listed in the following table.

Table 14-5 Settings required for the authentication-in-progress screen

Code	Description
<form name="Process" method="post" action="/cgi-bin/Process.cgi"></form>	This tag directs the sending of a PIN code and other information for Web authentication. Do not modify this code.
<input name="pcode" size="40" maxlength="32" autocomplete="OFF" type="password">	This tag specifies the PIN code and other information. Do not change any attributes except size and maxlength. Place this code inside the <form></form> tags.
<input value="Enter" type="submit">	This tag sends the PIN code and other information for Web authentication. Do not modify this code. Place this code inside the <form></form> tags.

Note

If you want to associate another file with the loginProcess.html file, add a slash (/) to the beginning of the name of the other file.

Example: <img src="/image_file.gif">

(b) Sample code

An example of the source code of the authentication-in-progress screen (loginProcess.html) is shown below.

Figure 14-3 Example source code of the authentication-in-progress screen (loginProcess.html)

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">

<head>
 <meta http-equiv="Pragma" content="no-cache">
 <meta http-equiv="Cache-Control" content="no-cache">
 <meta http-equiv="Expires" content="Thu, 01 Dec 1994 16:00:00 GMT">
 <title> </title>
</head>

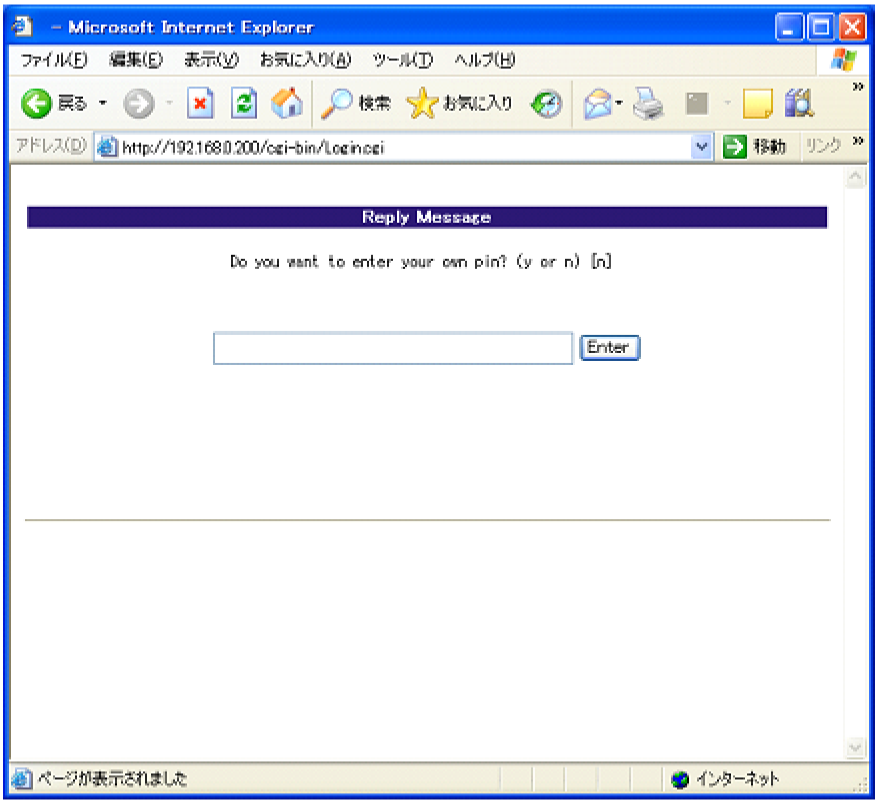
<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
<br>
<table width="100%">
 <tbody>
 <tr>
  <td align="center" bgColor="#2b1872">
  <font color="#ffffff"><b>Reply Message</b></font></td>
 </tr>
 </tbody>
</table>
<br>
<table align="center" border="0">
 <tbody>
 <tr>
 <td align="left" nowrap="nowrap"><!-- Reply_Message --></td>
 </tr>                  Description to display Reply-Message on the under authentication window
 </tbody>
</table>
<br>                    Description to display Reply-Message on the under authentication window

<form name="Process" method="post" action="/cgi-bin/Process.cgi">
<input name="scode" type="hidden" value="<!-- Session_Code -->">
<table align="center" border="0">
<tbody>                 Tag for session identification by user
 <tr>
 <td align="left"><input name="pcode" size="40" maxlength="32" autocomplete="OFF" type="password"></td>
 <td align="left"><input value="Enter" type="submit"></td>      Description to specify PIN codes
 </tr>
 </tbody>          Description to send PIN codes to Web authentication
</table>
</form>
<br>
<br>
<br>
<br>
<br>
<br>
</center>
<!-- ===== Footer ===== -->
<hr>
<div align="right"></div>
</body>
</html>
```

(c) Example of the authentication-in-progress screen

An example of the authentication-in-progress screen is shown below.

Figure 14-4 Example of the authentication-in-progress screen



(2) Adding authentication error message files

The authentication error message file (`webauth.msg`) contains the messages presented to the user when an attempt to log in or out of Web authentication fails.

If you want to replace the default authentication error message, create an authentication error message file that contains the message shown below after the 9 lines of messages indicated in section *8.10.3 Authentication error message file (webauth.msg)* in *8. Description of Web Authentication.*

Table 14-6 Contents of the authentication error message file by line

Line number	Description
10	Message displayed when a PIN code is sent: Default message: "`Invalid sequence.  Please retry again.`"

(a) Condition for setting

- If a line contains only a line break, the switch outputs the default error message for that line.
- When saving the file, specify CR+LF or LF as the line break code.
- Each line can contain a maximum of 512 single-byte characters, including HTML markup and the line break tag `<BR>`. Any excess characters are ignored.
- If the authentication error message file has 11 or more lines, the messages

after the 10th line are ignored.

(b) Key points regarding error message file creation

- The text in the authentication error message file is handled as HTML text without any modifications. If you include HTML markup in an error message, the message is formatted accordingly.
- Each message must occupy one line in the file. If you want to insert a line break in an error message, use the HTML line break tag `<BR>`.

(c) Sample code

The following figure shows an example of the source code for the authentication error message file (`webauth.msg`).

Figure 14-5 Example of source code for authentication error message file (webauth.msg)

```
Invalid user ID or password
Invalid password
No authentication server found<BR>Contact your system administrator.
Error in system configuration<BR>Contact your system administrator.
System failure occurred (minor)<BR>Retry later.
System failure occurred (major)<BR>Contact your system administrator.
System failure occurred (critical)<BR>Contact your system administrator.
System heavily loaded<BR>Retry later.
You have not logged in
Invalid sequence<BR>Retry later.
```

(3) Tags dedicated to Web authentication used with this functionality

The authentication-in-progress screen file can be rewritten using the Web authentication page replacement functionality as with other Web authentication page files.

If you insert the following tags dedicated to Web authentication, the file can be substituted for user-specific Web authentication page files.

(a) Adding tags dedicated to Web authentication

By inserting tags dedicated to Web authentication in the HTML file of the Web authentication screen, the portion where the tag is written is converted into the intended information.

If you insert an appropriate tag in the HTML file, you can display the login time or an error message on the authentication screen, or recognize the information through an application operating in the Web browser.

Table 14-7 Tags dedicated to Web authentication and converted information

Tags specific to Web authentication	Example of the text after conversion	Meaning of the converted information
`<!-- Session_Code -->`	`123456`	Session identification code per user (screen)
`<!-- Reply_Message -->`	`Do you want to enter your...`	Reply-Message to Access-Challenge received from RADIUS server

The dedicated tag that is converted into the session identification code (`<!-- Session_Code -->`) is embedded in the default HTML file as described below. It is not displayed in a Web browser.

- HTML inserted into the authentication-in-progress screen by default (`loginProcess.html`)

  ```
  <input name="scode" type="hidden" value="<!-- Session_Code -->">
  ```

  Note: As the type of the input tag is hidden, it is not displayed in typical Web browsers.

If you want to display the identification code of the session under authentication in a Web browser, create an authentication-in-progress screen file (`loginProcess.html` file). Register it on the Switch as described in subsection *8.9.1 Replacing Web authentication pages* to display it on the authentication-in-progress screen.

The following table describes which combination of tags dedicated to Web authentication and the screens are valid for the conversion of information.

Table 14-8 Combinations of the tags dedicated to Web authentication and the screens that are valid for the conversion of information

Tags specific to Web authentication	Types of screens (to be converted)						
	Login page	**Authentication-in-progress**	**Logout page**	**Login success page**	**Login failed page**	**Logout completed page**	**Logout failed page**
`<!-- Session_Code -->`	--	Y	--	--	--	--	--
`<!-- Reply_Message -->`	--	Y	--	--	--	--	--

Legend:

Y: If the tag dedicated to Web authentication is included in the HTML file, it is converted into the intended information.

--: Even if the tag dedicated to Web authentication is included in the HTML file, it is not converted into the intended information.

14.1.3 Using with other Web authentication functionality

All other Web authentication functionality, including URL Redirect, IP address dedicated for authentication, and passage before authentication, can be used with the one-time password authentication functionality.

14.2 Configuration

No configuration to enable one-time password authentication functionality is set on the Switch. See the following to specify the configuration required for Web authentication and login authentication.

- Web authentication: *8. Description of Web Authentication* and *9. Web Authentication Configuration and Operation*
- Login authentication: *8. Login Security and RADIUS* in the *Configuration Guide Vol. 1*

14.3 Operation

14.3.1 List of operation commands

The following table describes the operation commands for one-time password authentication.

Table 14-9 List of operation commands

Command name	Description
`set web-authentication html-files`	Registers the specified Web authentication page files.
`clear web-authentication html-files`	Deletes the Web authentication page files you registered.
`show web-authentication html-files`	Displays the file names and sizes of the Web authentication page files, as well as the date and time of their registration.
`store web-authentication html-files`	Take the Web authentication page file currently in operation and stores it in a directory on the RAMDISK.

For usage examples, see *9. Web Authentication Configuration and Operation.*

Part 4: High Reliability Based on Redundant Configurations

15. GSRP Aware Functionality

GSRP aware functionality clears internal MAC address table entries by receiving a frame from a GSRP switch. This chapter provides an overview of the GSRP aware functionality.

15.1 Overview of GSRP

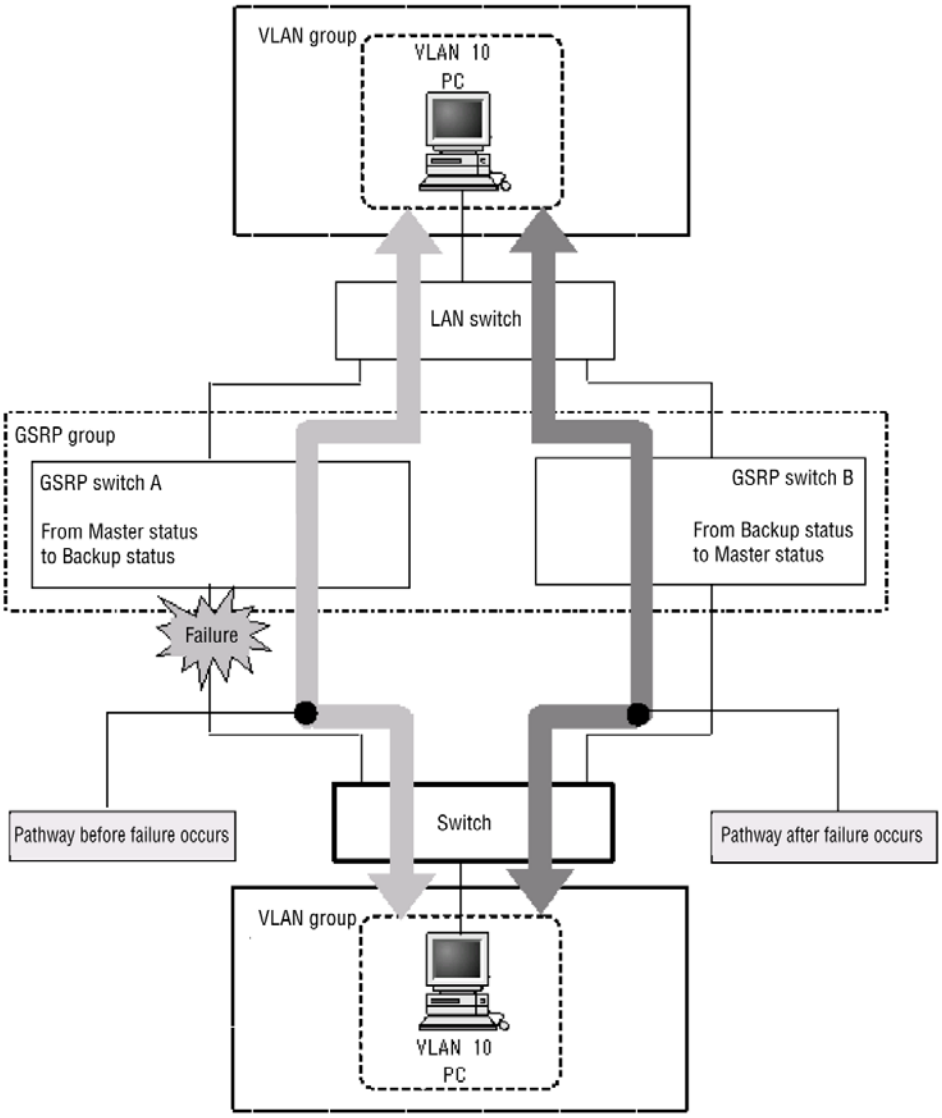
15.1.1 Overview

Gigabit Switch Redundancy Protocol (GSRP) provides redundancy for switches by securing a communication path via another switch in the same network even if the primary switch has failed.

Another functionality that can provide redundancy on a network is Spanning Tree Protocols. Because the paired switches exchange control frames to check each other's status with GSRP, the switchover from one switch to another is faster than using Spanning Tree Protocols. GSRP is also suitable for large-scale configurations in which core switches are used in multiple stages on a network. On the other hand, Spanning Tree Protocols are standard protocols and suitable for building a network consisting of switches and routers manufactured by different vendors.

The following figure provides an overview of redundancy in Layer 2 provided by GSRP.

Figure 15-1 Overview of GSRP



15.1.2 Supported specifications

The Switch supports GSRP aware only. For details, see *15.2 GSRP switchover control.*

(1) Use with other functionality

(a) When used with the Layer 2 switch functionality

For details, see *15.3 Compatibility between Layer 2 switch functionality and other functionality* in the *Configuration Guide Vol. 1*.

(b) When used with the Layer 2 authentication functionality

See *5.9.3 Interoperability of the Layer 2 authentication functionality and other functionality.*

15.2 GSRP switchover control

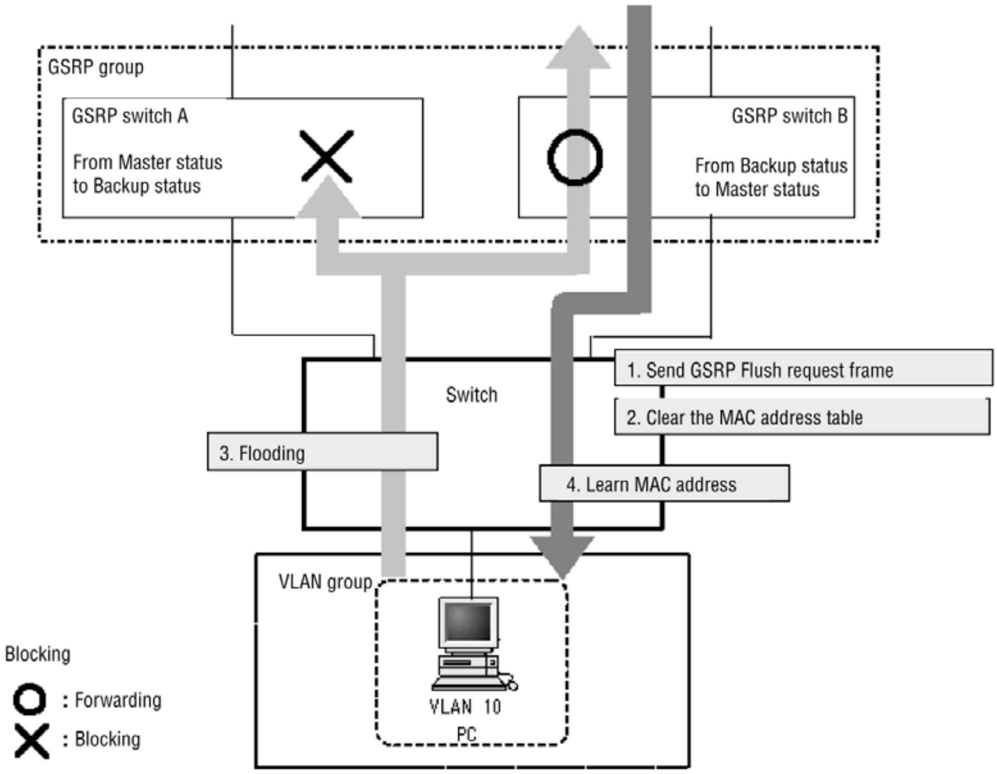
When the backup GSRP switch takes over as the master switch, the backup switch assumes the forwarding and blocking responsibility for frames. However, that is not enough to immediately resume end-to-end communication, because the MAC address entries in the MAC address tables in the adjacent switches are still registered for the previous master GSRP switch. To immediately resume communication, the MAC address table entries on the adjacent switches need to be cleared when the GSRP switches change.

GSRP supports the following methods for clearing the MAC address table entries in the adjacent switches.

(1) Sending GSRP Flush request frames

When the GSRP backup switch takes over as the master switch, the backup switch sends a control frame called a GSRP Flush request frame to the adjacent switches to request the clearing of the MAC address table entries. A switch that can receive this GSRP Flush request frame and clear the internal MAC address table is GSRP aware. GSRP-aware switches flood GSRP Flush request frames. The Switch is constantly GSRP aware. The following figure provides an overview of clearing MAC address table entries by using GSRP Flush request frames.

Figure 15-2 Overview of clearing MAC address table entries by using GSRP Flush request frames



1. GSRP switch B takes over from GSRP switch A. GSRP switch B sends a GSRP Flush request frame to the Switch.
2. The Switch receives the GSRP Flush request frame, and clears the internal

MAC address table.

3. As a result, the Switch floods a MAC address request on the port to which the PC is connected until the MAC address of the PC is learned from the frames sent from the PC.

   The frames sent from the PC are forwarded to the destination via the master switch (GSRP switch B).

4. When a frame returns to the PC as a response, the Switch learns the MAC address of the PC.

   Thereafter, the Switch forwards the frames from the PC only to GSRP switch B.

15.3 Configuration

The Switch supports GSRP awareness only. There is no configuration.

15.4 Operation

15.4.1 List of operation commands

The following table describes the operation commands for GSRP.

Table 15-1 List of operation commands

Command name	Description
show gsrp aware	Displays GSRP aware information.

15.4.2 Confirming GSRP aware information

The Switch displays the GSRP aware information by the information command show gsrp aware.

Figure 15-3 An example of executing the show gsrp detail command

```
> show gsrp aware

Date 2008/11/14 14:34:40 UTC
Last mac_address_table Flush Time : 2008/11/14 14:34:35
GSRP Flush Request Parameters :
 GSRP ID : 10     VLAN Group ID : 6   Port : 0/16
 Source MAC Address : 0012.e208.2096
>
```

16. Uplink Redundancy

With uplink redundancy, a redundant configuration can be built without using Spanning Tree Protocols.

This chapter describes uplink redundancy and its use.

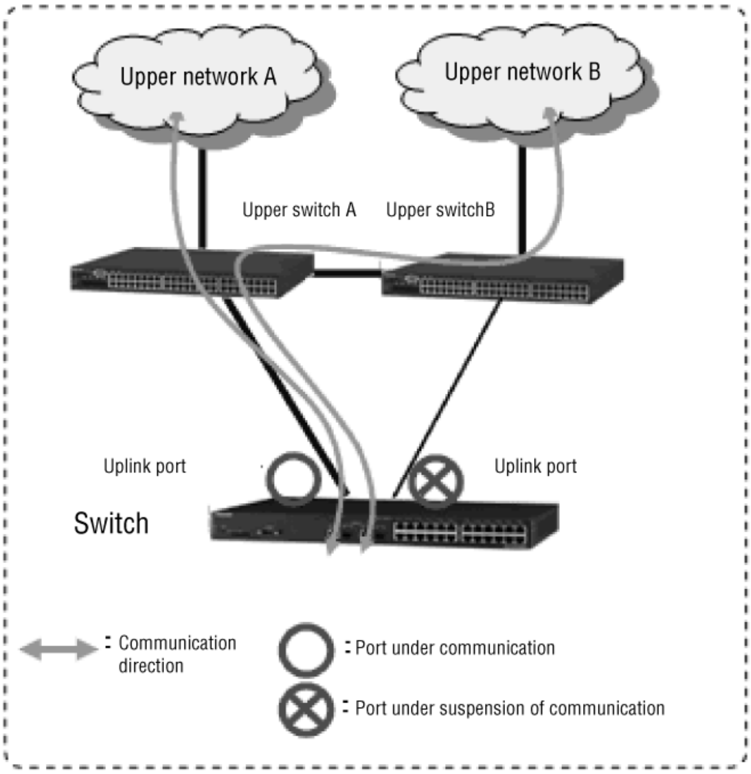
16.1 Description

Uplink redundancy duplicates uplink ports on the Switch. If a failure occurs, the backup port takes over for the current port to continue communication with upstream switches. By using uplink redundancy, you can create redundant uplink ports without using protocols such as the Spanning Tree Protocol. A pair of redundant ports is called an uplink port.

- Connect Layer 2 switches in a V-shape and the lower-level switch conducts switching.
- The lower-level switch duplicates the uplink port by pairing the Layer 2 interface (Ethernet or port channel).

The following figure shows a basic configuration of uplink redundancy.

Figure 16-1 Overview of uplink redundancy



When you use uplink redundancy in this configuration, if the link between the Switch and upstream switch A fails, the link between the Switch and upstream switch B can take over to continue communication.

The following table shows functionality details and gives cross-references to explanations.

Table 16-1 Functionality supported by uplink redundancy

Functionality	Item	Functionality reference	Settings reference
Basic	Uplink redundancy operation	See *16.1.1*.	--
	Applicable interfaces for uplink ports	See *16.1.1*.	See *16.2.2*.
	Number of uplink ports	See *16.1.1*.	--
	Switchover and switch-back between primary and secondary ports	See *16.1.2*.	--
	Switch-back when recovering from a failure	See *16.1.2*.	See *16.2.2*.
	Port control	See *16.1.2*.	--
Extended	Functionality for sending and receiving flush control frames	See *16.1.3*.	See *16.2.3*.
	Functionality for updating MAC addresses	See *16.1.4*.	See *16.2.4*.
	Active port locking at switch startup	See *16.1.5*.	--

16.1.1 Uplink redundancy operation

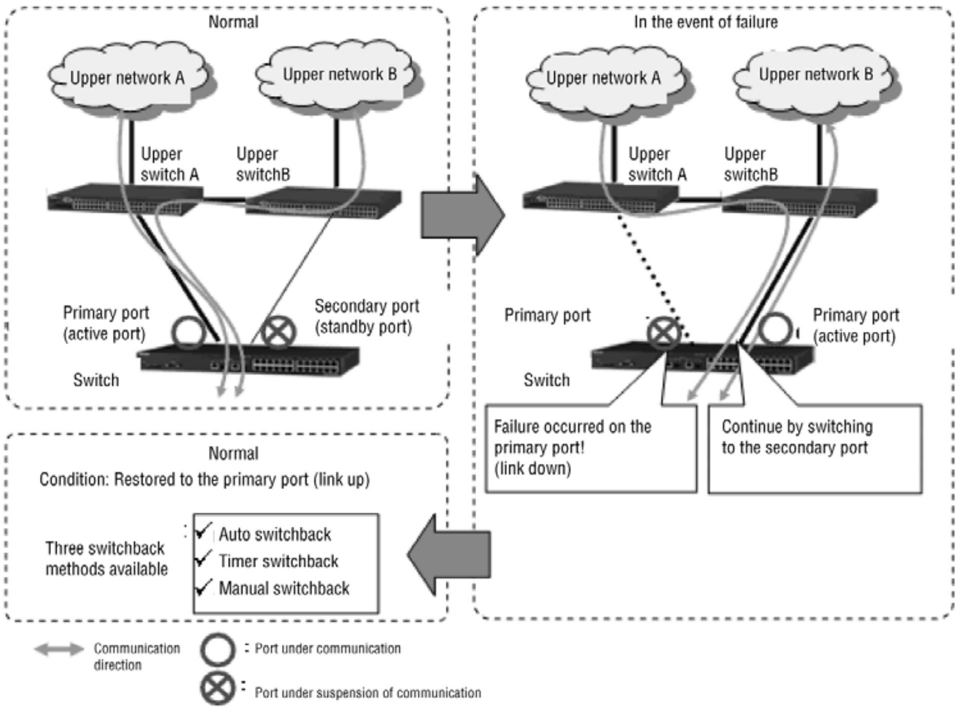
Uplink redundancy provides redundancy by using a pair of ports or bundles of ports (aggregated link ports). This pair of ports is called an uplink port. An uplink port consists of a primary port that performs communication during normal operation and a secondary port that takes over as the primary port in case of a failure. You can configure these ports by using configuration commands.

In the uplink port, the port that is currently performing communication is called the active port. The other port is called the standby port, and it stands ready to take over as the active port if the active port fails so that communication can continue.

The ports of the uplink port must belong to the same VLAN and have the same settings. In addition, the ports used for an uplink port cannot be used as another uplink port.

The following figure provides an overview of uplink redundancy operation.

Figure 16-2 Overview of uplink redundancy operation



Normal operation

Communication between the primary port on the Switch and the upstream switch A is possible. The secondary port on the Switch is not communicating.

If the primary port fails

If the primary port link goes down, the Switch switches the active port over to the secondary port and uses it to continue communication with upstream switches. This action is called a switchover.

When the primary port is restored

When the primary port link is re-enabled and the port is standing by, you can use Switch functionality such as automatic switch-back (using a timer) or manual switch-back to switch the active port to the primary port. This action is called a *switch-back*.

When the active port is switched over, from the new active port you send the flush control frames that require, due to the configuration, an upstream switch to clear the MAC address table

(1) Applicable interfaces for uplink ports

An Ethernet interface or a port-channel interface can be specified as an uplink port. A combination of an Ethernet interface and a port-channel interface can also be set as the pair of primary and secondary ports, as shown in the table below.

Table 16-2 Range and combination of primary and secondary ports

Model	Interface type	Range of port numbers	Combination of primary and secondary ports
AX2230S-24T AX2230S-24P	Ethernet	gigabitethernet 0/1-0/28	Combination is supported for any interface.
	Port channel	port-channel 1-8	
AX1250S-24T2C AX1240S-24T2C	Ethernet	fastethernet 0/1-0/24	Combination is supported for any interface.
		gigabitethernet 0/25-0/26	
	Port channel	port-channel 1-8	
AX1240S-24P2C	Ethernet	fastethernet 0/1-0/24	Combination is supported for any interface.
		gigabitethernet 0/25-0/26	
	Port channel	port-channel 1-8	
AX1240S-48T2C	Ethernet	fastethernet 0/1-0/48	Combination is supported for any interface.
		gigabitethernet 0/49-0/50	
	Port channel	port-channel 1-8	

(2) Number of uplink ports

In this functionality, the combination of a primary port and a secondary port is set as an uplink port. The following table describes the number of uplink ports that can be set in a Switch.

Table 16-3 Maximum number of uplink ports that can be set

Model	Maximum number of settings
AX2230S-24T AX2230S-24P	14
AX1250S-24T2C AX1240S-24T2C AX1240S-24P2C	13
AX1240S-48T2C	25

16.1.2 Switchover and switch-back between primary and secondary ports

Switchovers and switch-backs automatically change the active port or manually change the active port using operation commands when a failure occurs on the port that performs communication. For switchovers or switch-backs, the partner port of the active port needs to be the standby port.

(1) Switchover in case of failure

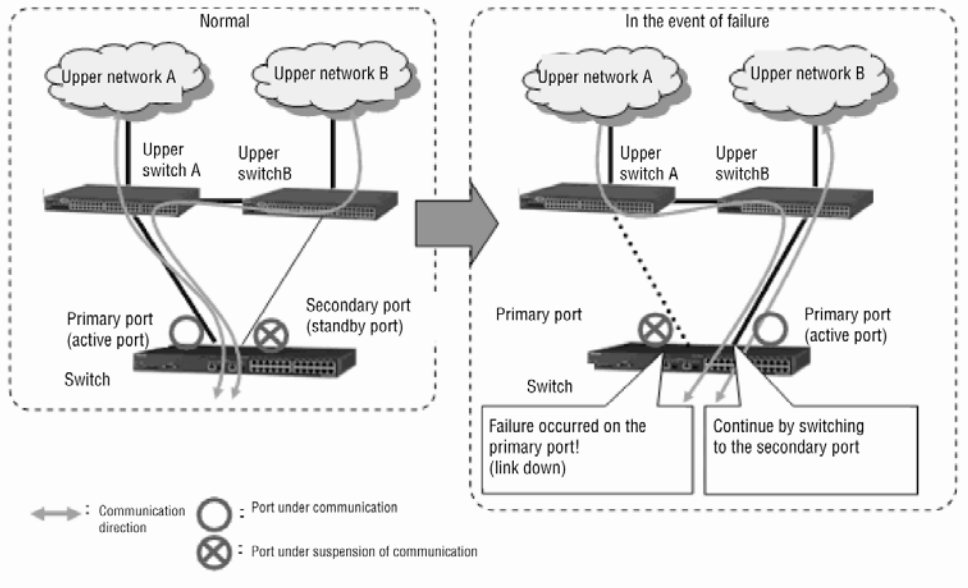
Configure a primary port and a secondary port on the Switch beforehand.

During normal operation, communication is performed via the primary port. When a link down is detected on the primary port, the active port is switched to the secondary port.

The MAC address table in the Switch is not deleted, and the port number is switched from the primary port to the secondary port.

The new active port sends a flush control frame, which clears the MAC address table, to the upstream switch of the uplink port. Alternatively, it sends a MAC address update frame, which requests that the MAC address table be updated. Either frame signifies that a switchover has occurred.

Figure 16-3 Overview of the switchover of the primary and secondary



(2) Switch-back when recovering from a failure

When the port recovers from a failure, a switch-back occurs due to an automatic switch-back, a timer switch-back, or a manual switch-back.

(a) Automatic switch-back

When the uplink redundancy is in effect, an automatic switch-back is executed by setting the configuration switch-back time to 0 seconds.

When a link-up occurs on the primary port, the port is switched back automatically and immediately. For details about automatic switch-backs by a timer, see *(b) Timer switch-back.*

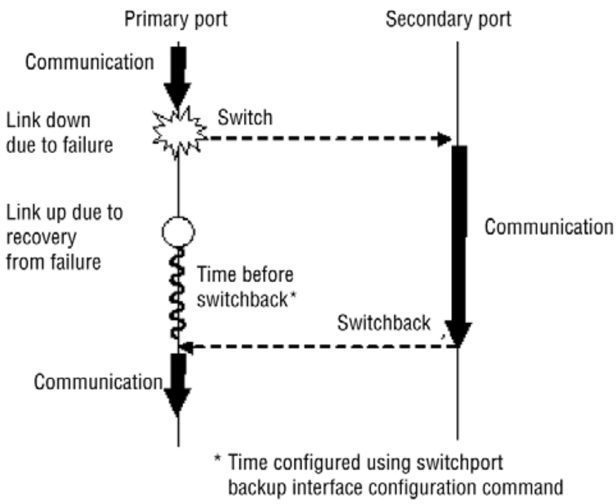
(b) Timer switch-back

When the uplink redundancy is in effect, a timer switch-back is executed automatically by setting the configuration switch-back time to 1 to 300 seconds.

The port is switched back, if the link-up status on the primary port continues longer than the timer switch-back wait time set by the `switchport backup interface` configuration command.

When a link-down occurs on the primary port before the timer switch-back wait time is completed, the time measurement is reset to zero. The following figure shows an outline of a timer switch-back.

Figure 16-4 Overview of a timer switch-back



(c) Manual switch-back

When the uplink redundancy is in effect, the secondary port continues to be active even after a link-up occurs on the primary port due to recovery from a failure. To switch the active port from the second port to the primary after the primary port is recovered, use the `select switchport backup interface` operation command.

The operation command is executable, when a link-up occurs on the port to be specified as active.

(3) Port control

Port control in the uplink redundancy functionality is control for blocking (status in which communication is not possible) or forwarding (status in which communication is possible). Execute the port control shown in the table below.

Table 16-4 Port control in the uplink redundancy functionality

Status of the port (setting of primary/secondary and physical condition)			**Port control in the uplink redundancy functionality**		
Status	**Setting**	**Physical condition**	**Operation**	**Frame reception**	**Frame sending**
Normal condition	Primary	link-up	Forwarding	Y	Y
	Secondary	link-up	Blocking	N	N#
When the link-down state is detected on the primary port	Primary	link-down	Blocking	N	N
	Secondary	link-up	Forwarding	Y	Y
When the primary port is recovered and in the link-up	Primary	link-up	Blocking	N	N#

Status of the port (setting of primary/secondary and physical condition)			Port control in the uplink redundancy functionality		
Status	**Setting**	**Physical condition**	**Operation**	**Frame reception**	**Frame sending**
state, and the condition is any of the following: ● Before automatic switch-back is executed ● Before timer switch-back is executed ● Waiting for manual switch-back	Secondary	link-up	Forwarding	Y	Y
When the link-down state is detected on the secondary port	Primary	link-up	Forwarding	Y	Y
	Secondary	link-down	Blocking	N	N
When the link-down state is detected on both primary and secondary ports	Primary	link-down	Blocking	N	N
	Secondary	link-down	Blocking	N	N

Legend:

Y: To be sent; N: Not to be sent

#

Frames such as LACP can be sent or received even during blocking.

16.1.3 Functionality for sending and receiving flush control frames

Sending a flush control frame clears the MAC address table on an upstream switch. **Upstream switches need to support the clearing of MAC address tables** triggered **by flush control frames.**

(1) Sending operation

If a flush control frame that requests clearing the MAC address table is configured to be sent, a flush control frame is sent when the active port is switched.

The Switch sends frames from the new active port immediately after the switched primary and secondary ports are enabled.

The same frame is sent three times at intervals of one second when the active port is switched. The following table describes the destination VLANs.

Table 16-5 VLAN to which flush control frames are sent

Settings of sending flush control frames in the configuration	Types of ports that send frames	Destination VLAN
Destination VLAN is not specified	Access port	Sent to access VLAN
	Trunk port	Sent to native VLAN
	MAC port	Sent to native VLAN

Settings of sending flush control frames in the configuration	Types of ports that send frames	Destination VLAN
	Protocol port	Sent to native VLAN
Destination VLAN is specified	Access port	Sent to access VLAN
	Trunk port	Sent to designated VLAN
	MAC port	Sent to native VLAN
	Protocol port	Sent to native VLAN

(2) Receiving operation

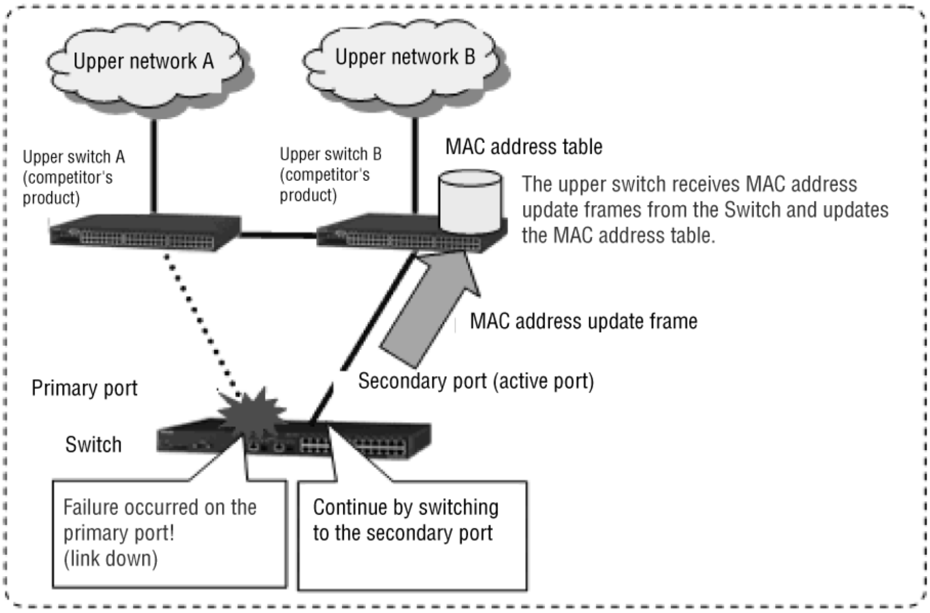
By receiving the flush control frame, the MAC address table is cleared. All entries are cleared, every time one frame is received.

There is no configuration for receiving frames.

16.1.4 Functionality for updating MAC addresses

This functionality updates the MAC address table of an upstream switch. Use it instead of a flush control frame if the upstream switch cannot receive flush control frames (for example, when it is another company's product).

Figure 16-5 Overview of the address update functionality



(1) Sending operation

If the MAC address update functionality that requests updating of the MAC address table is configured, a MAC address update frame is sent when the active port is switched.

The Switch sends frames from the new active port immediately after the switched primary and secondary ports are enabled. If switchover is not successful, no frame is sent.

A maximum of 1,024 MAC addresses, which were taken from the MAC address table when the active port was switched, can be sent. If more than 1,024 addresses were taken, the 1,025th address and thereafter are not sent and operation log data is collected instead. Among all addresses in the registered MAC address, only the ones that meet the following conditions are sent:

- Learnt at a non-uplink port
- The VLAN of the learnt MAC address is included in the uplink port.
- Addresses that are registered as static, dynamic, or authentication (dot1x, WebAuth and MacAuth) (Snoop MAC address update frames are not sent.)
- Not included in the exempted VLANs designated by the configuration

  For details, see *(b) Target and exempted VLANs of the MAC address update functionality.*

The following figure shows an example of MAC addresses to be sent.

Figure 16-6 Example of MAC addresses to be sent

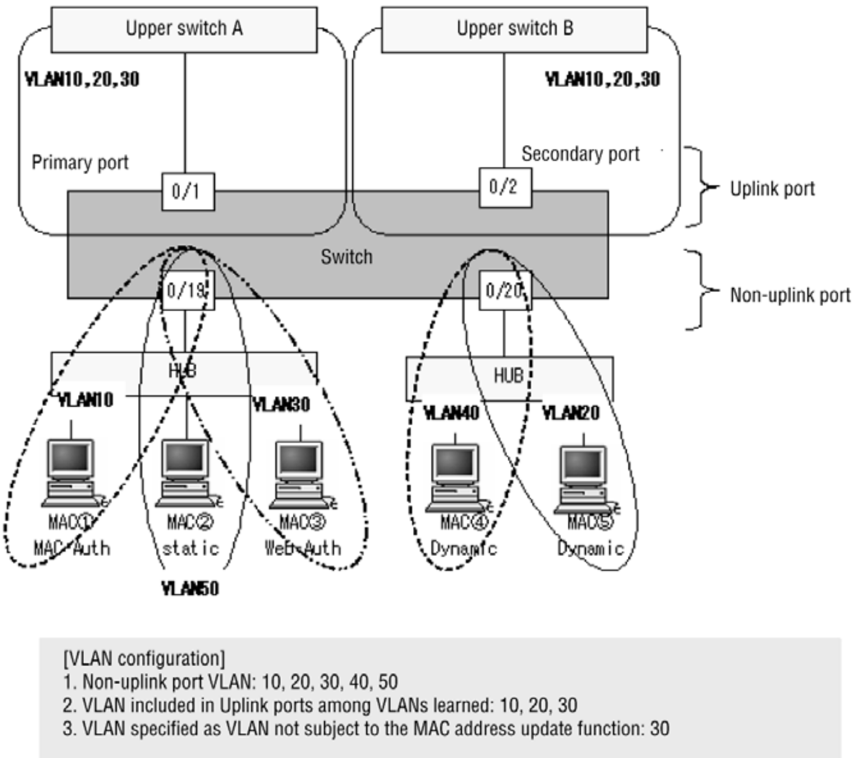


Table 16-6 MAC addresses to be sent

MAC address	VLAN	State of learning	Port	Destination
MAC (1)	10	MacAuth	0/19	Y
MAC (2)	50	Static	0/19	N

MAC address	VLAN	State of learning	Port	Destination
MAC (3)	30	WebAuth	0/19	N
MAC (4)	40	Dynamic	0/20	N
MAC (5)	20	Dynamic	0/20	Y

Legend:

Y: To be sent; N:Not to be sent

(a) Number of frame re-transmissions

A maximum of three re-transmissions can be set in the configuration. At retransmission time the MAC address table is not obtained again, and the same frames as the first transmission are sent.

(b) Target and exempted VLANs of the MAC address update functionality

- Target VLANs

  Among the VLANs learnt at the non-uplink port, all VLANS included in the uplink port are targets.

  The MAC address update functionality sends all MAC addresses included in the above VLANs.

- Exempted VLANs

  If you have any MAC addresses you do not want to send in the MAC address update functionality, exclude them in units of VLANs. Specify such a VLAN and exclude it from the target VLANs defined above. The MAC addresses learnt at an exempted VLAN are not sent by the MAC address update functionality.

(c) Using with the functionality for sending and receiving flush control frames

This functionality and the functionality for sending and receiving flush control frames can be set on the same port. In this case, send the flush control frames first, and send the MAC address update frames later.

(2) Receiving operation

When the MAC address update frames are received, the MAC addresses are learnt as usual and the MAC address table is updated.

There is no configuration for receiving frames.

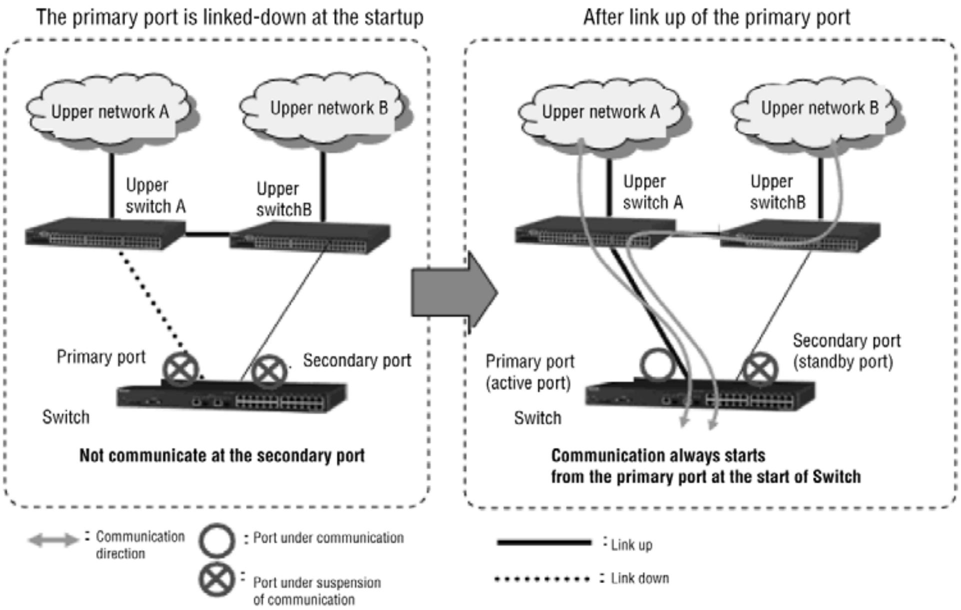
16.1.5 Active port locking at switch startup

Use active port locking at Switch startup if you want to always start communication on the primary port when the Switch starts. When this functionality is enabled on a Switch, communication via the uplink port does not start even if the secondary port is enabled at startup. Instead, communication starts only when the primary port is enabled.

Operation proceeds as usual when communication has started on the primary port. If the primary port fails or a user executes the appropriate operation command, the secondary port takes over for the primary port. If the primary port link is disabled at switch startup because, for example, an upstream switch on the primary port side has failed, execute the appropriate `switchport backup interface` operation command to use the secondary port to start communication.

The following figure shows operation when active port locking at switch startup is enabled.

Figure 16-7 Operation when the active port locking functionality is enabled at switch startup



16.1.6 Operation logs, MIBs and traps

(1) Collecting operation logs

The following operations conducted in this functionality are logged as Switch events: switchovers and switch-backs between primary and secondary ports, clearing of the MAC address table when the flush control frames are received, and excessive detection of MAC addresses when MAC address update frames are sent. The operation logs can be seen by using the `show logging` operation command.

If the functionality to output logs to the syslog server is set, the collected operation logs are sent to the syslog server.

(2) Private MIB/Trap

This functionality supports private MIB and private traps. For details of private MIBs, see the manual *MIB Reference*.

Use the `snmp-server host` configuration command to determine whether a private trap is issued or not.

16.1.7 Notes on use with other functionality

For interoperability with other functionality, the behavior is described in the following table.

Table 16-7 Operations when used with other functionality

Other functionality	Compatibility	Actions when used at the same time
Link aggregation	Supported	Can operate using an aggregated link.
Spanning Tree Protocol	Not supported (Ports are not compatible)	Spanning trees are forcibly disabled at uplink ports (port by port).
Ring Protocol	Supported (Partial)	Uplink redundancy cannot be used with a ring port.
L2 loop detection	Supported	Operates as set in the configuration. However, L2 loop detection frames are not received at the blocking port by uplink redundancy.
GSRP aware	Supported	Operates as normal. However, GSRP Flush request frames are not received at the blocking port by uplink redundancy.
OAN	Supported	Operates as set in the configuration.
Authentication	Not supported (Ports are not compatible)	Use this functionality and the following functionality only on the same device: ● IEEE 802.1X ● Web Authentication ● MAC-based Authentication ● DHCP snooping Use with the above-mentioned functionality at an uplink port is not recommended.
MAC address table static definition	Not supported (Ports are not compatible)	Can be configured. However, they actually cannot be used together, as the MAC address table static definition port is disabled by the switchover of the primary and secondary ports.
Other functionality	Supported	Can be operated only at the port where either primary or secondary is in the forwarding state. How the functionality operates depends on the setting of each primary or secondary port. Therefore, if different functionality is set on primary and secondary ports, how the functionality operates depends on the setting of the currently operating port. No identity check is conducted on the configuration setting of primary and secondary ports.

16.1.8 Notes on using uplink redundancy

(1) Use with L2 loop detection

If only send is set on an L2 loop detection port, loops are detected but no switchover between primary and secondary ports occurs.

If L2 loop detection is conducted on the secondary port as well after having switched to the secondary port, a loop will be detected again unless the cause of the loop is systematically eliminated.

If you use a port as the primary or secondary port and as a L2 loop detection (`send-inact`) port, the `send-inact` port is disabled when an incoming L2 loop detection frame from another port is received.

(2) Pairing a port with an uplink port

Set the same VLAN for the port that is paired with a primary or secondary port.

(3) Timer switch-back wait time setting when spanning trees are used at a higher-level switch

When spanning trees are used at the higher-level switch, the status will be `listening` or `learning` after recovering from the link-down state and communication cannot be restored immediately. In this case, we recommend that you set the timer switch-back wait time to 30 seconds or longer.

(4) Using the functionality for sending and receiving flush control frames

- Check whether the upstream switches support the reception of flush control frames sent by uplink redundancy.

  The MAC address table will not be cleared, even if the Switch sends flush control frames to a switch that does not support the functionality. In this case, use the MAC address update functionality.
- If a VLAN Tag value is set here, the flush control frames are sent in the form of tagged frames even if the target port is an access port.
- On the primary port, specify the settings to send the flush control frames.

(5) Using the MAC address update functionality

Specify the MAC address update functionality on the primary port.

(6) Changing the setting in a loop structure

The uplink redundancy functionality is used in the network that forms a loop.

When changing the setting of uplink redundancy, shut down the target port of uplink redundancy beforehand and cancel the shutdown after changing the setting. If you change the setting without shutting down, a loop might be formed.

16.2 Configuration

16.2.1 List of configuration commands

The following table describes the commands used to configure uplink redundancy.

Table 16-8 List of configuration commands

Command name	Description
`switchport backup interface`	Specifies primary and secondary ports and an automatic or timer switch-back wait time.
`switchport backup flush request transmit`	Enables the sending of flush control frames to request that the upstream switches clear their MAC address tables.
`switchport backup mac-address-table update transmit`	Enables the sending of MAC address update frames to request that the upstream switches update their MAC address tables.
`switchport backup mac-address-table update exclude-vlan`	Sets the VLAN to be excluded when sending MAC address update frames.
`switchport backup mac-address-table update retransmit`	Specifies the number of re-transmissions of MAC address update frames.
`switchport-backup startup-active-port-selection`	Enables active port locking at Switch startup.

16.2.2 Specifying the primary and secondary ports and timer switch-back wait time

Points to note

The example below shows how to configure Ethernet port 0/1 as the primary port and Ethernet port 0/20 as the secondary port. The example specifies the timer switch-back wait time when the primary port is restored.

Command examples

1.
```
(config)# interface fastethernet 0/1
(config-if)# switchport backup interface fastethernet 0/20
preemption delay 10
(config-if)# exit
```

Enters configuration mode for port 0/1, which is the primary port. Sets port 0/20 as the secondary port and 10 seconds as the timer switch-back wait time. After having switched to the secondary port and when 10 seconds or more have passed since the restoration of the primary port, the primary port becomes the active port.

Notes

When Spanning Tree Protocols are used at the higher-level switch, the status will be `listening` or `learning` after recovering from the link-down state and communication cannot be restored immediately. In this case, we recommend that you set the timer switch-back wait time to 30 seconds or longer.

16.2.3 Setting the functionality to send/receive flush control frames to upstream switches

Points to note

The example below shows how to configure Ethernet port 0/1 as the primary port and specifies the sending of flush control frames. Also, the example specifies the VLAN Tag value to be added to the flush control frames. No setting is required for reception.

Command examples

1.
```
(config)# vlan 10,50
(config-vlan)# exit
```
Configures VLANs 10 and 50.

2.
```
(config)# interface fastethernet 0/1
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 10,50
(config-if)# switchport trunk native vlan 10
```
Configures the port 0/1 as a trunk port, and configures VLANs 10 and 50. Sets the native VLAN to 10.

3.
```
(config-if)# switchport backup flush request transmit vlan 50
(config-if)# exit
```
Sets the VLAN Tag value to be added to the flush control frames to 50.

Notes

1. When the VLAN Tag value is set here, the flush control frames are sent in the form of tagged frames even if the target port is an access port.
2. Configure the above settings for the primary port.

16.2.4 Setting the MAC address update functionality to upstream switches

Points to note

The example below shows how to configure Ethernet port 0/1 as the primary port and specifies the following:

- Configures the trunk port; VLAN 10, 20, 30, and 50; and native VLAN 10
- Enables the MAC address update functionality
- VLANs that are not subject to the MAC address update functionality
- Configures the number of update frame re-transmissions

The example sets Ethernet port 0/20 as the secondary port and configure the same VLAN as the primary port. No setting is required for reception.

Command examples

1. `(config)# vlan 10,20,30,50`

   `(config-vlan)# exit`

   Configures VLAN 10, 20, 30 and 50.

2. `(config)# interface fastethernet 0/1`

   `(config-if)# switchport mode trunk`

   `(config-if)# switchport trunk allowed vlan 10,20,30,50`

   `(config-if)# switchport trunk native vlan 10`

   Configures the port 0/1 as a trunk port, and configures VLANs 10, 20, 30, and 50. Sets the native VLAN to 10.

3. `(config-if)# switchport backup mac-address-table update transmit`

   Enables the MAC address update functionality.

4. `(config-if)# switchport backup mac-address-table update exclude-vlan 20`

   Configures VLAN 20 to be excluded.

5. `(config-if)# switchport backup mac-address-table update retransmit 3`

   `(config-if)# exit`

   Sets the number of update frame re-transmissions to 3.

6. `(config)# interface fastethernet 0/20`

   `(config-if)# switchport mode trunk`

   `(config-if)# switchport trunk allowed vlan 10,20,30,50`

   `(config-if)# switchport trunk native vlan 10`

   `(config-if)# exit`

   Configures the port 0/20 as a trunk port, and configures VLANs 10, 20, 30, and 50. Sets the native VLAN to 10.

Notes

1. Configure the above settings for the primary port.

16.3 Operation

16.3.1 List of operation commands

The following table describes the operation commands for uplink redundancy.

Table 16-9 List of operation commands

Command name	Description
show switchport backup	Displays information about uplink redundancy.
show switchport backup statistics	Displays statistics related to flush control frames.
clear switchport backup statistics	Clears statistics related to flush control frames.
select switchport backup interface	Specifies the interface that performs a manual switch-back.
show switchport backup mac-address-table update	Displays information about MAC address update frames.
show switchport backup mac-address-table update statistics	Displays statistics related to MAC address update frames.
clear switchport backup mac-address-table update statistics	Clears the statistics related to MAC address update frames.

16.3.2 Displaying the status of uplink redundancy

(1) Displaying the switchover status and the destination VLANs for flush control frames

You can display the switchover status of the primary and secondary ports, the remaining time of automatic or timer switch-back, and destination VLANs.

The following figure shows the result of executing the show switchport backup operation command.

Figure 16-8 Results of executing show switchport backup

```
> show switchport backup

Date 2010/01/08 16:48:07 UTC
Startup active port selection: primary only
Switchport backup pairs                      Preemption    Flush
 Primary    Status      Secondary  Status      Delay Limit   VLAN
 Port 0/1   Blocking    Port 0/25  Forwarding     -     -    4094
 Port 0/10  Blocking    ChGr 4     Forwarding   100    98     10
*Port 0/11  Down        Port 0/15  Down           -     -      -
 Port 0/26  Blocking    ChGr 1     Forwarding    30    25   untag
 ChGr 8     Blocking    Port 0/24  Forwarding   300   297    100

>
```

Notes

In the following case, no information about a primary or secondary pair is displayed:

- When there is no configuration of the port channel interface designated in the secondary port

(2) Displaying statistics about the flush control frames

You can display statistics including the number of sending/receiving flush control frames and of the frames that cleared the MAC address table.

The following figure shows the result of executing the `show switchport backup statistics` operation command.

Figure 16-9 Results of executing show switchport backup statistics

```
> show switchport backup statistics

Date 2008/11/04 17:34:51 UTC
System ID : 00ed.f009.0001
Port 0/1  Transmit : on
        Transmit Total packets      :         3
        Receive  Total packets      :         0
               Valid packets      :         0
               Unknown version    :         0
               Self-transmitted   :         0
               Duplicate sequence :         0
  Last change time   : 2008/11/04 16:52:21 UTC (00:42:30 ago)
  Last transmit time : 2008/11/04 16:52:22 UTC (00:42:29 ago)
  Last receive time  : -
   Sender system ID  : 0000.0000.0000
             :
             :

>
```

(3) Displaying the switchover status and the target VLANs for MAC address update frames

Display the switchover status of the primary and secondary ports, the remaining time of an automatic or timer switch-back and the lists target VLANs and exempted VLANs.

The following figure shows the result of executing the `show switchport backup mac-address-table update` operation command.

Figure 16-10 Result of executing show switchport backup mac-address-table update

```
> show switchport backup mac-address-table update

Date 2010/01/08 18:02:40 UTC
Startup active port selection: primary only
Switchport backup pairs                   Preemption   Retransmit
 Primary    Status     Secondary  Status     Delay Limit
 Port 0/1   Down       Port 0/2   Forwarding    0     -           -
  VLAN          : 1,101-149,151-200,2001-2049,2051-2100,4040-4049,4051-4094
  Exclude-VLAN    : 50,150,1050,2050,3050,4050

Switchport backup pairs                   Preemption   Retransmit
 Primary    Status     Secondary  Status     Delay Limit
 Port 0/25  Down       Port 0/26  Forwarding    0     -           3
  VLAN          : 1,101-149,151-200,2001-2049,2051-2100,4040-4049,4051-4094
  Exclude-VLAN    : 50,150,1050,2050,3050,4050
```

```
Switchport backup pairs                    Preemption   Retransmit
 Primary    Status     Secondary  Status     Delay Limit
 ChGr 1     Down       ChGr 2     Forwarding     0    -          3
  VLAN          : 1,101-149,151-200,2001-2049,2051-2100,4040-4049,4051-4094
  Exclude-VLAN    : 50,150,1050,2050,3050,4050

>
```

Notes

In the following case, no information about a primary or secondary pair is displayed:

- When there is no configuration of the port channel interface designated in the secondary port

(4) Displaying statistics about the MAC address update frames

You can display statistics including the number of re-transmissions of MAC address update frames and of the switchovers that occurred.

The following figure shows the result of executing the `show switchport backup mac-address-table update statistics` operation command.

Figure 16-11 Results of executing show switchport backup mac-address-table update statistics

```
> show switchport backup mac-address-table update statistics

Date 2009/03/20 18:04:33 UTC
System ID : 0012.e244.0000
Port 0/1  Transition count                :     20094
        Update transmit total packets    :        0
        Transmission over flows         :        0
  Last change time   : 2009/03/20 16:25:55 UTC (01:38:38 ago)
  Last transmit time : -

Port 0/2  Transition count                :     20094
        Update transmit total packets    :      294
        Transmission over flows         :        0
  Last change time   : 2009/03/20 16:25:59 UTC (01:38:34 ago)
  Last transmit time : 2009/03/20 16:26:07 UTC (01:38:26 ago)

Port 0/25 Transition count                :     18743
        Update transmit total packets    :    325020
        Transmission over flows         :      9224
  Last change time   : 2009/03/20 18:01:31 UTC (00:03:02 ago)
  Last transmit time : 2009/03/20 18:01:36 UTC (00:02:57 ago)

Port 0/26 Transition count                :     18743
        Update transmit total packets    :   4098830
        Transmission over flows         :     10569
  Last change time   : 2009/03/20 18:01:37 UTC (00:02:56 ago)
  Last transmit time : 2009/03/20 18:04:22 UTC (00:00:11 ago)

ChGr 1    Transition count                :       511
        Update transmit total packets    :     30553
        Transmission over flows         :       480
  Last change time   : 2009/03/20 18:01:29 UTC (00:03:04 ago)
  Last transmit time : 2009/03/20 18:01:19 UTC (00:03:14 ago)

ChGr 2    Transition count                :       512
        Update transmit total packets    :    128844
```

```
        Transmission over flows         :       480
  Last change time   : 2009/03/20 18:01:33 UTC (00:03:00 ago)
  Last transmit time : 2009/03/20 18:04:32 UTC (00:00:01 ago)

>
```

Notes

In the following case, no information about a primary or secondary pair is displayed:

- When there is no configuration of the port channel interface designated in the secondary port

16.3.3 Manually switching over the primary and secondary ports

You can switch ports manually.

The following figure shows the results of executing the `select switchport backup interface` operation command.

Figure 16-12 Results of executing select switchport backup interface

```
# select switchport backup interface port-channel 8

#
```

Part 5: High Reliability Based on Network Failure Detection

17. Storm Control

Storm control functionality limits the number of flooding frames that are forwarded.
This chapter describes storm control and its use.

17.1 Description

17.1.1 Overview of storm control

If a loop exists in a Layer 2 network, broadcast frames are forwarded without limit between switches, severely increasing network load and the load on connected devices. This condition is called a broadcast storm and is a problem that must be avoided in Layer 2 networks. Additionally, multicast storms, in which an unlimited number of multicast frames are forwarded, and unicast storms, in which an unlimited number of unicast frames are forwarded, must be avoided.

Storm control refers to functionality that limits the number of flooded frames that are forwarded by a switch, to control the impact of storms on the network and connected devices.

For the Switch, the maximum number of frames that are received per second can be specified as a storm detection threshold (upper threshold) for each Ethernet interface so that frames exceeding that threshold are discarded. You can specify three separate threshold values, one each for broadcast frames, multicast frames, and unicast frames.

If the number of received frames exceeds the threshold, the port can be blocked, a private trap can be sent, or a log message can be output.

17.1.2 Functionality to limit flow rate

The Switch can automatically stop the traffic or limit the flow rate when a storm is detected, and cancel the limit.

The Switch blocks the frames or limits the flow rate to the designated level, if the number of frames of a specific type (broadcast, multicast or unicast) exceeds the storm detection threshold. If the number of frames of the designated type received per second exceeds the storm detection threshold (upper threshold), the Switch limits the flow rate to the threshold (lower threshold). By setting the detection threshold to zero, you can stop the traffic after detecting the storm.

If this functionality has maintained the flow rate under the recovery-from-storm threshold for a specified period of time, the functionality will be automatically canceled (monitoring time for canceling the flow rate limit). After canceling the limit, the storm will be monitored with the recovery-from-storm threshold.

The following chart describes the operations to limit flow rate.

Figure 17-1 Operations to limit flow rate

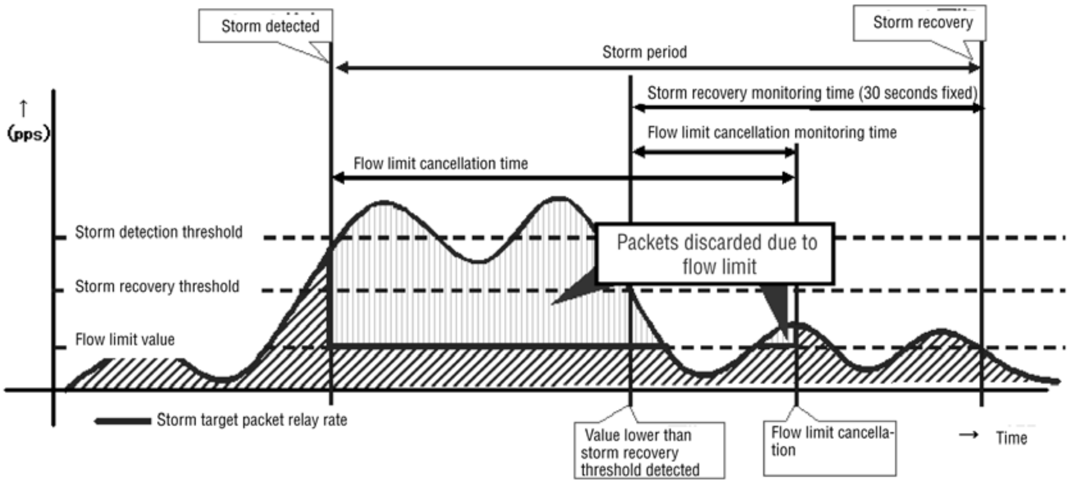


Table 17-1 Explanation of the actions and period of time in the figure

Operation	Description
Storm detection	Position to detect the storm control. Starts the action specified with the `action` command.
Recovery from the storm	Position to detect the recovery from storm control. The `action log` command and the `action trap` command are recovered.
Duration of the storm	Duration when the storm control is effective. In the `action log` command and the `action trap` command, this duration is determined as the period of storm.
Storm detection threshold	Threshold to detect a storm. A storm is detected when the number of frames exceeds the value (pps) designated in the configuration. The frames exceeding the threshold on the hardware are discarded (upper threshold). If no recovery-from-storm threshold is set, it is regarded as same as the storm detection threshold.
Recovery-from-storm threshold	Threshold to determine recovery from the storm. If the number of frames falls below the value (pps) designated in the configuration, it is determined that the Switch has recovered from the storm.
Flow rate limit value	Value specified in the configuration that limits the flow rate (pps) after a storm is detected (lower threshold).
Duration of flow rate limitation	The time period when the flow rate is limited.
Monitoring time for determining recovery from the storm	When the number of frames drops below the recovery-from-storm threshold (pps) and remains there for 30 seconds, the Switch is considered to have recovered from the storm.
Monitoring time for canceling the flow rate limit	When the number of frames drops below the recovery-from-storm threshold (pps) and remains there for the period of time specified in the configuration, the flow rate limit is canceled.

17.1.3 Notes on using storm control functionality

(1) Handling unicast frames

For the Switch, unicast storm detection and the frames to be discarded are not the same. A unicast storm is detected by counting all unicast frames received by the Switch, whereas frames that are to be discarded are determined by counting only the flooded unicast frames, which are those without a destination MAC address registered in the MAC address table.

(2) Detecting storms and recovery

The Switch determines that a storm has occurred when the number of frames received in one second exceeds the threshold specified in the configuration section. After a storm, if the number of frames received per second drops below the threshold value and remains there for 30 seconds, the Switch is considered to have recovered from the storm. (See *Figure 17-1 Operations to limit flow rate*.)

(3) Checking recovery from a storm when a port is blocked

If a port is blocked when a storm occurs, recovery from a storm cannot be detected because the port is no longer receiving any frames. If you set that a port is to be blocked when a storm occurs, make sure that port recovery is performed by a method that uses a network monitoring device or other device instead of by using the Switch.

17.2 Configuration

17.2.1 List of configuration commands

The following table describes the commands used to configure storm control

Table 17-2 List of configuration commands

Command name	Description
`storm-control`	Sets the threshold value for storm control. In addition, operations that can be performed when a storm is detected can be specified.

17.2.2 Basic settings

- Suppressing broadcast frames

  To prevent broadcast storms, specify a threshold for the number of broadcast frames received through the Ethernet interface. Specify a value that allows some margin after determining the number of frames used for normal operations. This is because the broadcast frames include frames required for communication such as ARP packets.

- Suppressing multicast frames

  To prevent multicast storms, specify a threshold for the number of multicast frames received through the Ethernet interface. Specify a value that allows some margin after determining the number of frames used for normal operations. This is because multicast frames include frames required for communication such as control multicast frame like BPDU and control packets for IPv4 multicast packets.

- Suppressing unicast storms

  To prevent unicast storms, specify a threshold for the number of unicast frames received through an Ethernet interface. Specify a value that allows some margin after determining the number of frames used for normal operations.

  Although the Switch uses the total number of received unicast frames for the detection of unicast frames, only flooded unicast frames are counted as frames to be discarded instead of being forwarded because their destination MAC addresses are not registered in the MAC address table. In particular, if you want to block a port when a storm is detected, specify a threshold value with enough margin so that a storm is not detected from normal-operation frames.

- Operations when a storm is detected

  Specify the Switch operations to be performed when a storm is detected. Select any combination of blocking a port, sending a private trap, and outputting a log message for each port.

  - Blocking a port

    When a storm is detected on a port, deactivate the port. Use the `activate` command to activate the port again after recovery from the storm.

  - Sending a private trap

When a storm has been detected, after recovery is detected, a private trap is sent as a notification.

- Outputting a log message

  When a storm has been detected, after recovery is detected, a log message is output as a notification. Note that a message must be output if a port is blocked.

Points to note

The interfaces that can be set are Ethernet interfaces.

If a storm occurs on a port, the port is blocked.

Command examples

1. `(config)# interface fastethernet 0/10`

   `(config-if)# storm-control broadcast level pps 50`

   Sets the threshold for detecting a storm of broadcast frames to 50 pps.

2. `(config-if)# storm-control multicast level pps 500`

   Sets the threshold for detecting a storm of multicast frames to 500 pps.

3. `(config-if)# storm-control unicast level pps 1000`

   Sets the threshold for detecting a storm of unicast frames to 1000 pps.

4. `(config-if)# storm-control action inactivate`

   `(config-if)# exit`

   Deactivates a port when a storm is detected on the port.

17.2.3 Extended setting:Limiting flow rate

The storm detection threshold is the same as the basic setting. It limits the flow rate to the level designated per frame type instead of blocking the ports.

Points to note

The example below shows how to configure the Switch so that the flow rate is lowered when a storm occurs and the number of received frames exceeds the storm detection threshold.

Set the monitoring time for canceling the flow rate limit automatically when the flow rate is back on or below the threshold.

Configure the Switch to output operation log data in case of storm detection and recovery from the storm.

Command examples

1. `(config)# interface fastethernet 0/20`

   `(config-if)# storm-control broadcast level pps 50 40`

   Sets the threshold for the recovery from the storm of broadcast frames to 40 pps in addition to the basic setting in port 0/20.

2. `(config-if)# storm-control multicast level pps 500 400`

Sets the threshold for the recovery from the storm of multicast frames to 400 pps in addition to the basic setting.

3. `(config-if)# storm-control unicast level pps 1000 800`

   Sets the threshold for the recovery from the storm of unicast frames to 800 pps in addition to the basic setting.

4. `(config-if)# storm-control action filter`

   Enables the setting for limiting the flow rate.

5. `(config-if)# storm-control filter-broadcast 30`

   Sets the flow rate limit of broadcast frames to 30 pps.

6. `(config-if)# storm-control filter-multicast 300`

   Sets the flow rate limit of multicast frames to 300 pps.

7. `(config-if)# storm-control filter-unicast 700`

   Sets the flow rate limit of unicast frames to 700 pps.

8. `(config-if)# storm-control filter-recovery-time 15`

   Sets the monitoring time for canceling the flow rate limitation to 15 seconds.

9. `(config-if)# storm-control action log`

   `(config-if)# exit`

   Sets to output the operation logs in case of storm detection and recovery from the storm.

17.3 Operation

17.3.1 List of operation commands

The following table describes operation commands for storm control.

Table 17-3 List of operation commands

Command name	Description
`show storm-control`	Displays the status of storm control.

17.3.2 Checking the status of storm control

Use the `show storm-control` command to check the settings and the operating status of storm control.

Confirm the storm detection threshold, recovery-from-storm threshold, flow rate limit value (lower threshold), the status of storm detection, as well as the number of storm detections, if any, and the time when the last storm was detected.

Specify the detail parameter to display the actions when a storm was detected, length of time of monitoring flow limit and its remaining time.

The following figure shows the result of executing the `show storm-control` operation command:

Figure 17-2 Result of executing the `show storm-control` command

```
> show storm-control

Date 2009/03/24 10:46:35 UTC
<Broadcast>
 Port    Detect Recovery   Filter  State          Count Last detect
 0/1       200      100     100  Filtering          1 2009/03/24 10:46:25
 0/2       200      100       -  Forwarding         0 ----/--/-- --:--:--

<Unicast>
 Port    Detect Recovery   Filter  State          Count Last detect
 0/1      10000     5000    5000  Filtering          1 2009/03/24 10:45:52
 0/2      10000     5000       -  Forwarding         0 ----/--/-- --:--:--

>
```

Figure 17-3 Result of executing `show storm-control detail` (port 0/1 broadcast detail displayed)

```
> show storm-control port 0/1 broadcast detail

Date 2009/03/24 10:48:20 UTC
<Broadcast>
 Port 0/1
  Detect rate : 200        Recover rate : 100       Filter rate : 100
  Action : Filter,Trap,Log
  Filter recovery time : 30
  <Status>
  State : Filtering         Filter recovery remaining time : 30
  Current rate :       189  Current filter rate    :       100
```

```
  Detect count :         1  Last detect          : 2009/03/24 10:46:25
>
```

18. IEEE 802.3ah/UDLD

The IEEE 802.3ah/UDLD functionality detects unidirectional link failures to prevent related network failures.

This chapter describes the IEEE 802.3ah/UDLD functionality and its use.

18.1 Description

18.1.1 Overview

UDLD (Unidirectional Link Detection) functionality detects unidirectional link failures.

When a unidirectional link failure occurs, one switch is able to send data but cannot receive data, while the other switch is able to receive data but cannot send data. Furthermore, a malfunction occurs in an upper protocol, and various other failures occur throughout the network. Some of the known failures are loops in the Spanning Tree Protocol and frame losses caused by link aggregation. These failures can be prevented by deactivating the applicable port when a unidirectional link failure is detected.

The OAM (Operations, Administration, and Maintenance) protocol, which functions as a part of the `slow` protocol in IEEE 802.3ah (Ethernet in the First Mile) and will be referred to hereafter as *IEEE 802.3ah/OAM*, describes the following method. OAM status information is regularly exchanged between the local switch and the partner switch by using control frames and checking frame-arrival capability at a remote device to monitor the bidirectional link status. The Switch uses the IEEE 802.3ah/OAM functionality to monitor the bidirectional link status. If the status cannot be checked in this case, UDLD functionality is used to detect unidirectional link failures.

The IEEE 802.3ah/OAM protocol also includes the concept of active and passive modes. The sending of a control frame starts at the active-mode switch and the passive-mode switch does not send any control frames until it has received a control frame. Because the factory default setting of the Switch enables IEEE 802.3ah/OAM functionality, all ports operate in passive mode.

Unidirectional link failures are detected by executing the `efmoam active udld` configuration command to configure the ports of both switches connected by an Ethernet cable. If a unidirectional link failure is detected on a port configured with the `efmoam active udld` command, the port is deactivated and a link failure is detected on the port of the partner switch. As a result, operation of the two target ports on the connected switches is stopped.

18.1.2 Supported specifications

IEEE 802.3ah/UDLD functionality supports IEEE 802.3ah/OAM functionality as described in the following table.

Table 18-1 IEEE 802.3ah OAMPDUs supported by IEEE 802.3ah/UDLD functionality

Item	Description	Supported
Information	Sends OAM status information to a remote device.	Y
Event Notification	Sends a link event warning to a remote device.	N
Variable Request	Asks a remote device for the MIB variable.	N
Variable Response	Sends the requested MIB variable.	N

Item	Description	Supported
Loopback Control	Controls the loopback status of a remote device.	N
Organization Specific	Used for functionality expansion	N

Legend: Y: Supported, N: Not supported

18.1.3 Notes on using IEEE 802.3ah/UDLD

(1) When a switch that does not support IEEE 802.3ah/OAM functionality is connected between switches configured with IEEE 802.3ah/UDLD functionality

Because a standard switch does not forward control frames used by IEEE 802.3ah/OAM functionality, information cannot be transmitted between switches, and a unidirectional link failure is detected on a port configured with the `efmoam active udld` configuration command. Accordingly, IEEE 802.3ah/UDLD functionality cannot be used.

(2) When a media converter or other relay device is connected between switches configured with IEEE 802.3ah/UDLD functionality

If a media converter that does not automatically disconnect the link when the other link is disconnected is installed between switches, recognition of the link status varies between the switches. Accordingly, a unidirectional link failure is detected even if the remote device is not operating on a port configured with the `efmoam active udld` command. When you attempt recovery from a failure, you must synchronize both switches, making operation more difficult. Use a media converter that automatically disconnects the link status if the other link is disconnected.

(3) Connecting to the UDLD functionality of another manufacturer's switch

The IEEE 802.3ah/UDLD functionality of the Switch and the UDLD functionality of other manufacturers' switches cannot be connected because UDLD functionality specifications differ by manufacturer.

(4) Use with other functionality

(a) When used with Layer 2 authentication

See *5.9.3 Interoperability of the Layer 2 authentication functionality and other functionality.*

18.2 Configuration

18.2.1 List of configuration commands

The following table describes the commands used to configure IEEE 802.3ah/UDLD.

Table 18-2 List of configuration commands

Command name	Description
`efmoam active`	Activates IEEE 802.3ah/OAM functionality on a physical port.
`efmoam disable`	Disables IEEE 802.3ah/OAM functionality.
`efmoam udld-detection-count`	Specifies the counter value for determining a unidirectional link failure.

18.2.2 Configuring IEEE 802.3ah/UDLD

(1) Configuring IEEE 802.3ah/UDLD functionality

Points to note

To use IEEE 802.3ah/UDLD functionality, you must first enable IEEE 802.3ah/OAM functionality for the entire switch. As the factory default setting, IEEE 802.3ah/OAM functionality is enabled for the Switch (all ports are set to passive mode). Next, configure active mode with the `UDLD` parameter added for the ports on which you want to activate unidirectional link failure detection functionality.

In this subsection, IEEE 802.3ah/UDLD functionality is used for `fastethernet 0/1`.

Command examples

1. `(config)# interface fastethernet 0/1`

   Switches to the Ethernet interface configuration mode for port 0/1.

2. `(config-if)# efmoam active udld`

   `(config-if)# exit`

   Sets active mode for the IEEE 802.3ah/OAM functionality port 0/1 to initiate the detection of unidirectional link failures.

(2) Setting the unidirectional link failure detection count

Points to note

A unidirectional link failure is detected if the number of successive failures for checking the bidirectional link status resulting from a timeout of information sent from the link origination reaches the predetermined number. This predetermined number is the *unidirectional link failure detection count*. The bidirectional link status is checked once every second.

By changing the bidirectional link failure detection count, you can adjust the length of time between the actual occurrence of a unidirectional link failure and the time at which it is detected. If you decrease the count value, failures can be detected nearer the time of occurrence, but a greater risk of false detection. Normally, you do not change this setting.

The following is the approximate time from the occurrence of a unidirectional link failure and its detection (note that a maximum deviation of 10% is possible):

5 + unidirectional-link-failure-detection-count seconds

Command examples

1. `(config)# efmoam udld-detection-count 60`

   Sets to 60 the maximum number of successive timeouts allowed for information sent from the other switch before detecting a unidirectional link failure.

18.3 Operation

18.3.1 List of operation commands

The following table describes the operation commands for IEEE 802.3ah/OAM functionality.

Table 18-3 List of operation commands

Command name	Description
show efmoam	Displays the IEEE 802.3ah/OAM configuration information and port setting information.
show efmoam statistics	Displays statistics regarding IEEE 802.3ah/OAM.
clear efmoam statistics	Clears statistics regarding IEEE 802.3ah/OAM.

18.3.2 Displaying IEEE 802.3ah/OAM information

To display IEEE 802.3ah/OAM information, use the show efmoam operation command. The show efmoam command displays the IEEE 802.3ah/OAM configuration information and information about the ports in active mode. The show efmoam statistics operation command displays the status of failures detected by the IEEE 802.3ah/UDLD functionality in addition to IEEE 802.3ah/OAM protocol statistics.

Figure 18-1 Results of executing the show efmoam command

```
> show efmoam

Date 2008/11/13 17:36:11 UTC
Port    Status              Dest MAC
0/1     Forced Down (UDLD)  0012.e214.ffae
0/2     Mutually Seen       0012.e214.ffaf
0/3     Partner Seen        0012.e214.ffb0
0/4     Down                unknown
0/5     Down                unknown

>
```

Figure 18-2 Result of executing the show efmoam statistics command

```
> show efmoam statistics

Date 2008/11/13 17:35:25 UTC
Port 0/1 [Forced Down (UDLD)]
  OAMPDUs:Tx     :       133  Rx       :        57
         Invalid:          0  Unrecogn. :         0
  Expirings      :         1  Thrashings:         0  Blockings:         1
Port 0/2 [Mutually Seen]
  OAMPDUs:Tx     :       771  Rx       :       750
         Invalid:          0  Unrecogn. :         0
  Expirings      :         0  Thrashings:         0  Blockings:         0
Port 0/3 [Partner Seen]
  OAMPDUs:Tx     :       631  Rx       :       593
```

```
        Invalid:         0  Unrecogn. :        0
 Expirings     :         0  Thrashings:        0  Blockings:        0
>
```

19. L2 Loop Detection

L2 loop detection is functionality that detects a loop failure in a Layer 2 network and corrects the loop failure by blocking the port causing the loop.

This chapter describes L2 loop detection and its use.

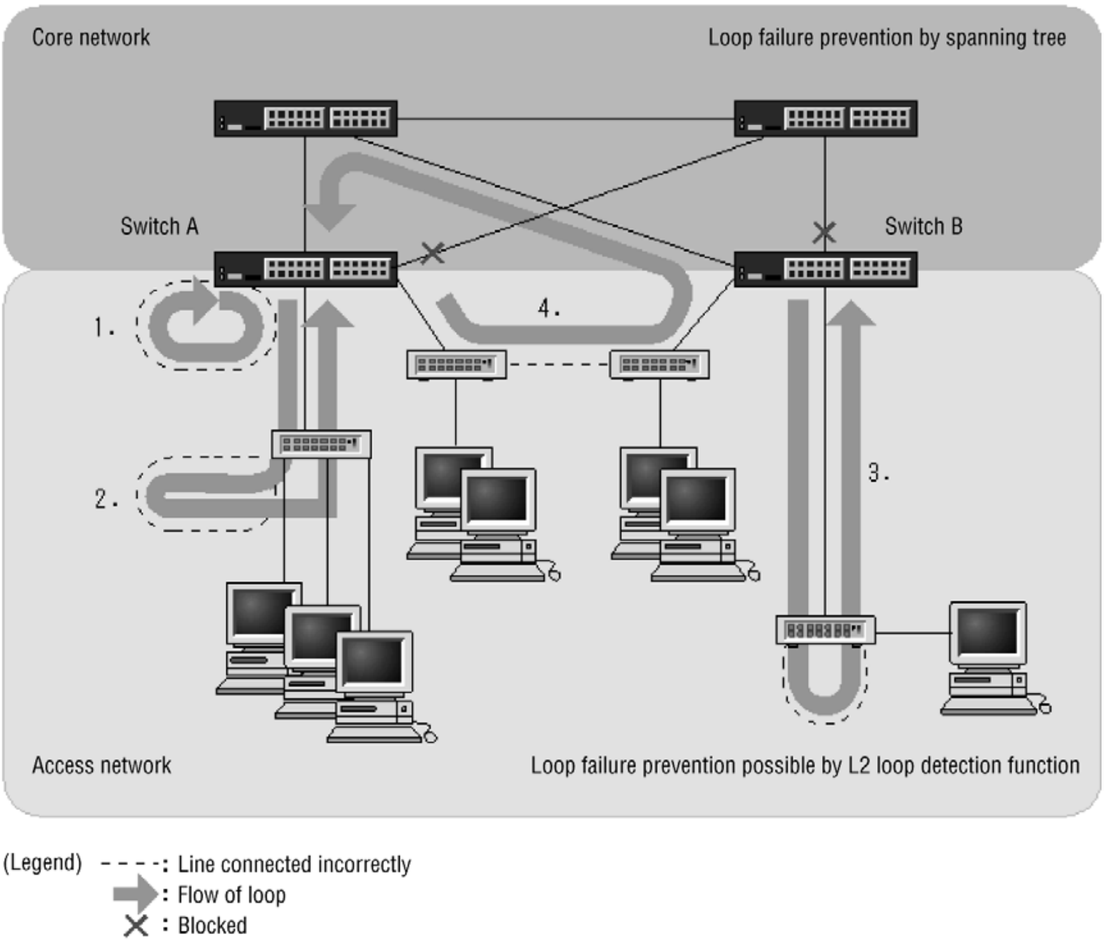
19.1 Description

19.1.1 Overview

If a loop failure occurs in a Layer 2 network, MAC address learning becomes unstable, or normal communication cannot continue because of the load on the switch. Protocols such as Spanning Tree are provided to avoid such states. Generally, the L2 loop detection functionality corrects loop failures in a non-redundant access network, but not in the core network in which these protocols are used.

When an L2 loop failure that occurred under the control of the Switch is detected, the L2 loop detection functionality deactivates (makes it `inactive`) the port on which the failure was detected to isolate the failure cause from the network. Isolation is necessary to prevent the loop failure from spreading throughout the entire network.

Figure 19-1 Examples of loop failures



Loop failure 1.

A line is connected incorrectly to the Switch A resulting in a loop failure.

Loop failure 2 & 3.

A line is connected incorrectly from the Switch A or B to a lower-level switch or to an L2 switch resulting in a loop failure.

Loop failure 4.

A line is connected to a lower-level switch incorrectly resulting in a loop failure that spreads to the core network.

As described above, the L2 loop detection functionality can detect loop failures in various locations, including those with incorrect connections to the Switch or to other switches.

19.1.2 Operational overview

In L2 loop detection, a control frame for detecting an L2 loop (an *L2 loop detection frame*) is sent regularly from the port (a physical port or a channel group) specified in the configuration section. If the L2 loop detection frame sent from the Switch is received on a port on which the L2 loop detection functionality is enabled, a loop failure is determined, and the port on which the frame is received or the port originating the frame is deactivated (`inactive`).

After the cause of the loop failure has been corrected, an operation command can be used to activate the inactive port. If the automatic-restoration functionality has been configured, the deactivated port can be activated automatically.

(1) Types and actions of ports used by the L2 loop detection functionality

Listed below are the types of ports used by the L2 loop detection functionality. The types of ports are set using the configuration command `loop-detection`.

- Detecting port

  The default position when the L2 loop detection functionality is enabled (status where the configuration command `loop-detection` has not been set)

- Detecting and blocking port (`send-inact-port`)

  The L2 loop detection functionality is enabled. The port is deactivated when the L2 loop detection frame sent from a local switch is received.

- Detecting and sending port (`send-port`)

  The L2 loop detection functionality is enabled. The port is not deactivated, even when the L2 loop detection frame sent from a local switch is received.

- Uplink port (`uplink-port`)

  The port connected to a higher-level network or a key port that enables the L2 loop detection functionality

- Out-of-scope port (`exception-port`)

  The port is where the L2 loop detection functionality is disabled.

The following table describes the actions of ports.

Table 19-1 Types and actions of ports

Port type	L2 loop detection functionality	Sending L2 loop detection frames	Actions when receiving the L2 loop detection frames from a local switch		
			Deactivating the port	Collecting operation logs	Sending traps

Port type	L2 loop detection functionality	Sending L2 loop detection frames	Actions when receiving the L2 loop detection frames from a local switch		
			Deactivating the port	Collecting operation logs	Sending traps
Detecting port	Enabled	--	--	Y	Y
send-inact-port	Enabled	Y	Y	Y	Y
send-port	Enabled	Y	--	Y	Y
uplink-port	Enabled	--	#	Y	Y
exception-port	Disabled	--	--	--	--

Legend:

Y: Performed --: Not performed

#

The behavior is as follows when a loop is detected in the uplink port:

- The uplink port is not deactivated.
- If the L2 loop detection frame is sent from the `send-inact-port`, the port is deactivated.
- If the L2 loop detection frame is sent from the `send-port`, the port is not deactivated.

(2) Sending L2 loop detection frames

(a) Tagged frame

The same number of L2 loop detection frames for `switchport trunk allowed vlan` of a trunk port and `switchport mac dot1q vlan` of a MAC port as the number of relevant VLANs is sent in the form of tagged frames.

L2 loop detection frames for `switchport trunk native vlan` of a trunk port are sent in the form of untagged frames.

(b) Untagged frame

- Access port

  L2 loop detection frames of VLANs that belong to the relevant port are sent in the form of untagged frames.

- Protocol port and MAC port

  When VLANs are multiplexed, L2 loop detection frames are aggregated and sent in the form of untagged frames. (The frames for the redundant VLANs are not sent.)

(c) Ports to which frames are sent

- `interface fastethernet`
- `interface gigabitethernet`
- `interface port-channel` (sent not based on physical ports but on logical ports)

The number of L2 loop detection frames sent from each port varies depending on the type of a port (access, trunk, protocol, or MAC) and the number of VLANs accommodated.

(d) Interval for sending frames

An L2 loop detection frame is sent from all VLANs belonging to the detecting and blocking port and the detecting and sending port within the interval specified in the configuration section.

An L2 loop detection frame sending interval can be set with the configuration command `loop-detection interval`.

(e) Sending rate and the number of frames sent

L2 loop detection frames are sent from the available port or VLAN that fall within the range of device capacities. No frame exceeding the capacities is sent. A port or VLAN that cannot send frames cannot detect loop failures.

For details of capacity limit, see *3.2 Capacity limits* in the *Configuration Guide Vol. 1*.

(3) Receiving the L2 loop detection frames and deactivating ports

(a) Setting the threshold number of L2 loop detection frames received before deactivating ports

The threshold for the number of L2 loop detection frames that can be received before deactivating ports is set with the configuration command `loop-detection threshold`.

If this command is omitted, the port is deactivated when the first L2 loop detection frame is received. Setting this command is effective when you want to avoid deactivating the detecting and blocking port by the detection of a temporary L2 loop failure.

(b) Retaining the number of L2 loop detections

The number of received L2 loop detection frames from a local switch is calculated for each port. The number is retained until the port is deactivated and is cleared immediately after the port is deactivated.

The length of time for retaining the number of L2 loop detection frames can be set with the configuration command `loop-detection hold-time`. The number of the received frames is retained for the period specified with this command. If no frame is received during the specified retention time, the number is cleared.

(c) Blocking a port

Ports are deactivated in units of physical ports.

If any port that belongs to a channel group goes down, `inactivate` is issued to all physical ports that belong to the same channel group, deactivating them. It does the same for any standby port using the standby link functionality (link-down /no-link-down)

(4) Restoring the deactivated ports

There are two ways to restore the port deactivated by the L2 loop detection functionality: manual restoration and automatic restoration.

(a) Manual restoration

The port deactivated by the L2 loop detection functionality can be restored in units of physical ports by using the operation command `activate`. The ports in a channel group are also restored in a unit of physical port. When one physical port in the channel group deactivated by the L2 loop detection functionality is linked up, the whole channel group is restored.

(b) Automatic restoration

This functionality automatically restores the port deactivated by the L2 loop detection after a specified period of time. This functionality is enabled by using the configuration command `loop-detection auto-restore-time`.

If the ports in a channel group have been deactivated, an `activate` command is issued to all physical ports that belong to the same group. The same command is automatically issued for any standby port using the standby link functionality (link-down /no-link-down)

19.1.3 Use with other functionality

The following table shows how the L2 loop detection functionality can be used simultaneously with other functionality.

Table 19-2 Use of L2 loop detection functionality with other functionality

Functionality	Item	Use in the same switch	Use in the same port	Actions when used at the same time
Link aggregation	IEEE802.3ad	Yes	Yes	When the physical ports belonging to the channel group where the ports are deactivated by the L2 loop detection functionality are linked, then the channel group is restored.
MAC Address Table	MAC address learning	Yes	Yes	The L2 loop detection frames are excluded from learning.
Port VLAN	port-based VLAN	Yes	Yes	Sending in a form of untagged frame
Protocol VLAN	protocol-based VLAN	Yes	Yes	If VLANs are multiple, L2 loop detection frames are aggregated and sent.
MAC VLAN	mac VLAN	Yes	Yes	
Spanning Tree Protocol	IEEE 802.1d IEEE802.1w IEEE802.1s PVST+	Yes	Yes[#]	Sending/receiving L2 loop detection frames becomes possible only when forwarding.
DHCP snooping	Terminal filtering	Yes	Yes	The L2 loop detection frames are excluded from DHCP snooping.
Filters	permit/deny	Yes	Yes	The L2 loop detection frames are excluded from filtering.

Functionality	Item	Use in the same switch	Use in the same port	Actions when used at the same time
QoS	Change in priority	Yes	Yes	The L2 loop detection frames are excluded from QoS flow.
Priority of the outgoing frames	Setting user-priority	Yes	Yes	The L2 loop detection frames are excluded from priority setting of the outgoing frames.
Layer 2 Authentication	IEEE802.1X Web Authentication MAC-based Authentication	Yes	Yes	Sending/receiving L2 loop detection frames becomes possible even before authentication.

#

When used in the same port and the port deactivated by the L2 loop detection functionality is inactive, the topology of the spanning tree changes.

19.1.4 Operation logs and traps

(1) Collecting operation logs

This functionality collects two types of logs: received frame logs and loop detection/deactivation event logs.

(a) Received frame logs

This functionality collects 1,000 received L2 loop detection frames, which were sent from the Switch. It collects such information as frame sending/receiving ports, VLAN number, and port actions. The received frame logs can be checked by the operation command `show loop-detection logging`.

The received frame logs are not sent to the syslog server.

(b) Loop detection/deactivation event logs

The logs collect such information as loop failures detected by the L2 loop detection functionality and the operations such as deactivation and restoration on ports in the operation log as device events. The operation logs can be seen by the operation command `show logging`.

The loop detection/deactivation event logs are sent to the syslog server.

(2) Private MIB/Trap

This functionality supports private MIB and private traps.

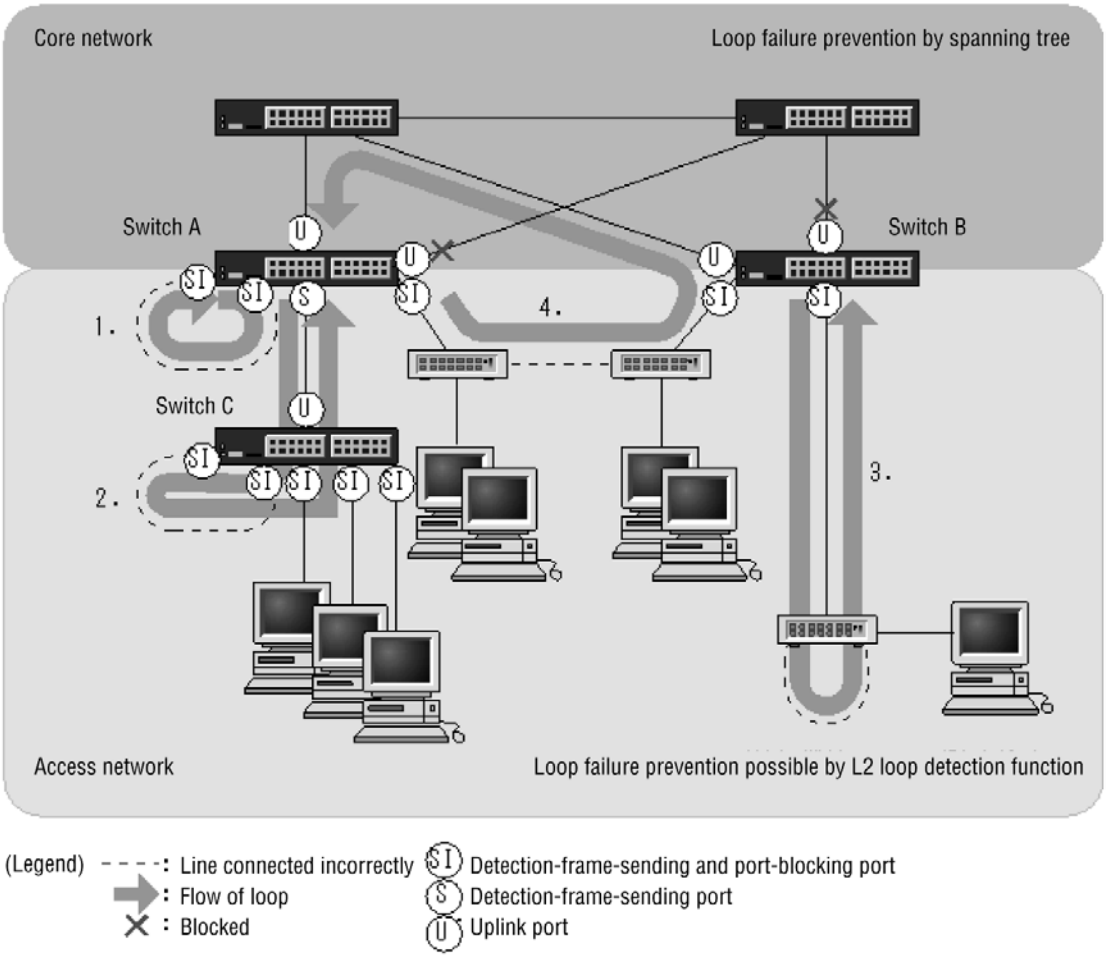
For details of private MIBs, see the manual *MIB Reference*.

Use the configuration command `snmp-server host` to determine whether a private trap is issued or not.

19.1.5 Application example

The following figure shows a network configuration in which the L2 loop detection functionality is used.

Figure 19-2 An example of a network configuration in which the L2 loop detection functionality is used



(1) Using detecting and blocking ports

This port type is generally specified for L2 loop detection. As shown by the Switches A and B in the figure, specifying lower-level ports as detecting and blocking ports is effective for failures caused by incorrect lower-level connections (see 1, 2, and 3 in the figure).

(2) Using detecting and sending ports

This port type is effective for minimizing the extent of a loop failure when L1 loop detection is used on a switch at the lowest possible level. When a switch is connected to multiple layers (see Switches A and C in the figure), if a port on the Switch A side is deactivated due to an incorrect connection (2 in the figure), none of the terminals unrelated to the loop failure occurring on Switch C can connect to a higher-level network. This is the reason that using the L2 loop detection functionality in a lower-level switch (Switch C in the figure) is recommended.

For such cases, specify a port on Switch A side as the detecting and sending port. This setting allows Switch C to detect loop failures during normal operation, but if Switch C is unable to detect loop failures because L2 loop detection is configured incorrectly, Switch A can detect loop failures. (In this case, it does not deactivate the port.)

(3) Using uplink ports

Specify an uplink port for ports connected to a higher-level network or for ports that will connect to the core network. If an incorrect connection, such as item 4 in the figure, is found, this setting allows connection to the core network to be reserved because Switch A source port has been deactivated.

19.1.6 Notes on using the L2 loop detection functionality

(1) Operation on a protocol VLAN or MAC VLAN

An L2 loop detection frame is an untagged frame with its own format. Because the L2 loop detection frame is transferred as a native VLAN on a protocol port or a MAC port, a loop failure across switches might not be detected if the following conditions are met:

- A port on the core network side is specified as an uplink port.
- No native VLANs are specified on the core network side.

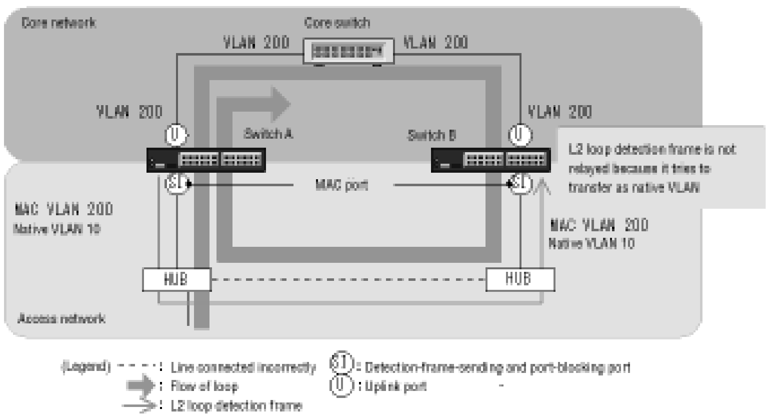
In such cases, if a port on the core network side specified as an uplink port is specified as the detecting and sending port, loop failures can be detected. The following are specific configuration examples.

(a) Example configuration in which loop detection is restricted

In the configuration shown in the figure below, if the connection between hubs under the Switch is incorrect, a loop across switches occurs.

In the figure, Switch A sends an L2 loop detection frame from the detecting and blocking port on the hub side, but the frame is not sent from the uplink port on the core switch side. Because Switch B tries to transfer the L2 loop detection frame received on the MAC port as a native VLAN, the L2 loop detection frame is not forwarded to the core switch side. In such cases, loop failures cannot be detected because the L2 loop detection frame is not returned to Switch A.

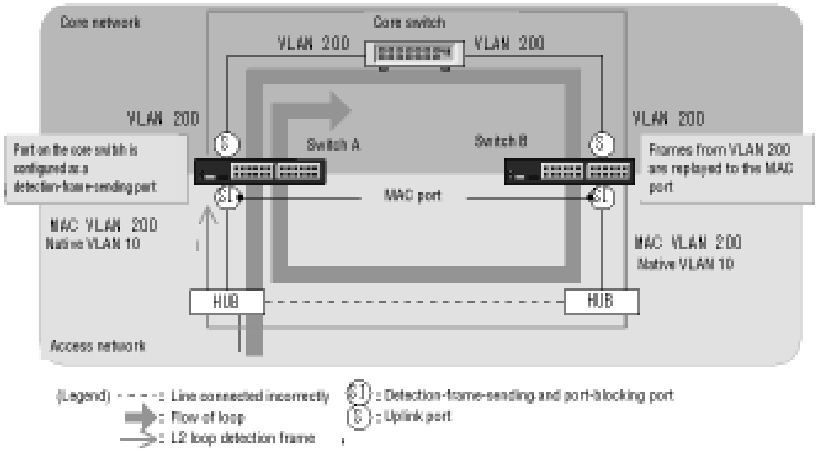
Figure 19-3 Configuration in which loop detection is restricted



(b) Example configuration in which loops can be detected

If a port on the core switch side of Switch A is specified as a detecting and sending port, Switch A can detect loop failures because Switch B forwards the L2 loop detection frame received from the port on the core switch side to the MAC port.

Figure 19-4 Configuration in which loops can be detected



(2) Operation when the tag translation functionality is used on other devices

If the tag of an L2 loop detection frame sent from the Switch was translated on another device and received as another VLAN of the Switch, it is determined that a loop failure has occurred.

(3) Operating environment for L2 loop detection

When the L2 loop detection functionality is used, if a switch that does not support the functionality is installed on the same network and receives a loop detection frame, it discards the frame. Therefore, if a loop failure occurs on the path containing these switches, the failure is not detected.

(4) Functionality that activates a deactivated port automatically (automatic-restoration functionality)

Note the following if you use the automatic-restoration functionality in static link aggregation:

- If you use the auto-negotiation functionality for connection, specify a line speed. If you do not specify a line speed, the line speed might temporarily vary due to degradation of the line quality, in which case the low-speed line might be withdrawn from the applicable channel group. If a loop is detected in this state, the automatic-restoration functionality might not operate in the applicable channel group.

If the automatic-restoration functionality does not operate, correct the cause of the loop, and then use the `activate` operation command to activate the port.

19.2 Configuration

19.2.1 List of configuration commands

The following table describes the commands used to configure L2 loop detection.

Table 19-3 List of configuration commands

Command name	Description
`loop-detection`	Sets the port type for the L2 loop detection functionality.
`loop-detection auto-restore-time`	Sets the time until a deactivated port is activated automatically.
`loop-detection enable`	Enables L2 loop detection.
`loop-detection hold-time`	Sets the time for holding the number of L2 loop detections before a port is blocked.
`loop-detection interval-time`	Sets the interval for sending L2 loop detection frames.
`loop-detection threshold`	Sets the number of L2 loop detections before a port is blocked.

19.2.2 Configuring the L2 loop detection functionality

(1) Enabling L2 loop detection and specifying the type of port for L2 loop detection

Points to note

The example below shows how to set up the L2 loop detection configuration to enable L2 loop detection for the entire switch, and to specify which ports actually detect L2 loop failures and which are L2 loop detection out-of-scope ports.

Command examples

1.

```
(config)# loop-detection enable
```

Enables L2 loop detection.

2.

```
(config)# interface fastethernet 0/2
(config-if)# loop-detection send-inact-port
(config-if)# exit
```

Sets ports 0/2 as detecting and blocking ports.

3.

```
(config)# interface fastethernet 0/4
(config-if)# loop-detection send-port
(config-if)# exit
```

Sets ports 0/4 as detecting and sending ports.

4. `(config)# interface gigabitethernet 0/25`
   `(config-if)# loop-detection uplink-port`
   `(config-if)# exit`

   Sets ports 0/25 as uplink ports.

5. `(config)# interface fastethernet 0/1`
   `(config-if)# loop-detection exception-port`
   `(config-if)# exit`

   Sets ports 0/1 as an L2 loop detection out-of-scope ports.

(2) Setting the interval for sending L2 loop detection frames

Points to note

Frames that exceed the transmission rate of L2 loop detection frames are not sent. In addition, loop failures will no longer be able to be detected on ports or the VLANs from which the frames could not be sent. If the maximum transmission rate of L2 loop detection frames is exceeded, specify a longer interval so that no frames will exceed the transmission rate.

Command examples

1. `(config)# loop-detection interval-time 60`

   Sets the L2 loop detection frame sending interval to 60 seconds.

(3) Specifying the conditions for deactivating ports

Points to note

If no command is specified, a port is deactivated when a loop failure is detected once (initial value). To avoid port deactivation due to a momentary loop, specify the number of L2 loop detection frames to be received before the port is deactivated.

Command examples

1. `(config)# loop-detection threshold 100`

   Sets the number of L2 loop detection frames to be received before the port is deactivated to 100, and deactivates the port when 100 frames have been received.

2. `(config)# loop-detection hold-time 60`

   Holds the number of received L2 loop detection frames for 60 seconds after the last frame was received. Clears the number when 60 seconds passes without receiving the frame again.

(4) Setting the automatic-restoration time after the port deactivation

Points to note

The following example shows how to specify the time to automatically activate the ports deactivated by the L2 loop detection functionality.

Command examples

1. `(config)# loop-detection auto-restore-time 360`

   Sets the ports deactivated by the L2 loop detection functionality to automatically activate in 360 seconds.

19.3 Operation

19.3.1 List of operation commands

The following table describes operation commands for the L2 loop detection functionality.

Table 19-4 List of operation commands

Command name	Description
`show loop-detection`	Displays L2 loop detection information.
`show loop-detection statistics`	Displays L2 loop detection statistics.
`clear loop-detection statistics`	Clears L2 loop detection statistics.
`show loop-detection logging`	Displays the logs of the received L2 loop detection frames.
`clear loop-detection logging`	Clears the logs of the received L2 loop detection frames.

19.3.2 Checking the L2 loop detection status

Use the `show loop-detection` operation command to check the L2 loop detection settings and the operating status.

You can check for ports that are unable to send frames because the rate for sending L2 loop detection frames on the port has exceeded the maximum value. If the configuration of VLAN port counts does not exceed the capacity, there is no problem.

Also, check for ports that have been deactivated due to a loop failure in the status section of the port information section.

Figure 19-5 Result of executing the `show loop-detection` operation command

```
> show loop-detection

Date 2008/11/12 16:22:28 UTC
Interval Time          :10
Output Rate            :20pps
Threshold              :200
Hold Time              :300
Auto Restore Time      :3600
VLAN Port Counts
   Configuration       :6       Capacity      :200
Port Information
  Port    Status     Type       DetectCnt RestoringTimer  SourcePort  Vlan
  0/1     Down       trap             0             -  -
  0/2     Down       trap             0             -  -
  0/3     Down       trap             0             -  -
  0/4     Down(loop) send-inact       200           3569  0/6           1
  0/5     Up         exception        0             -  0/7           1
  0/6     Down       send           200             -  0/4           1
  0/7     Up         send-inact       0             -  -
  0/8     Down(loop) send-inact       200           3569  ChGr:8(U)     1
```

```
                 :
                 :
  0/22    Down      uplink           -            -  -
  0/24    Down      trap             0            -  -
  0/25    Down      trap             0            -  -
  0/26    Down      trap             0            -  -
  ChGr:1  Down(loop) send-inact       200          3569  ChGr:2        1
  ChGr:2  Down(loop) send-inact       200          3569  ChGr:1        1
  ChGr:5  Down      trap             0            -  -
  ChGr:8  Down      uplink           -             -  0/8         1

>
```

20. CFM

CFM (Connectivity Fault Management) verifies the connectivity between bridges at the Layer 2 level and confirms routes; in other words, it is functionality for managing and maintaining wide-area Ethernet networks.

This chapter describes CFM and its operations.

20.1 Description

20.1.1 Overview

In addition to enterprise LANs, Ethernet is also starting to be used for wide area networks. As a result, maintenance and management functionality on par with SONET and ATM is required for Ethernet.

The CFM functionality uses the following types of functionality to maintain and manage Layer 2 networks:

1. Continuity check

   This functionality always monitors whether information is delivered correctly to the destination (accessibility and continuity) between management points.

2. Loopback

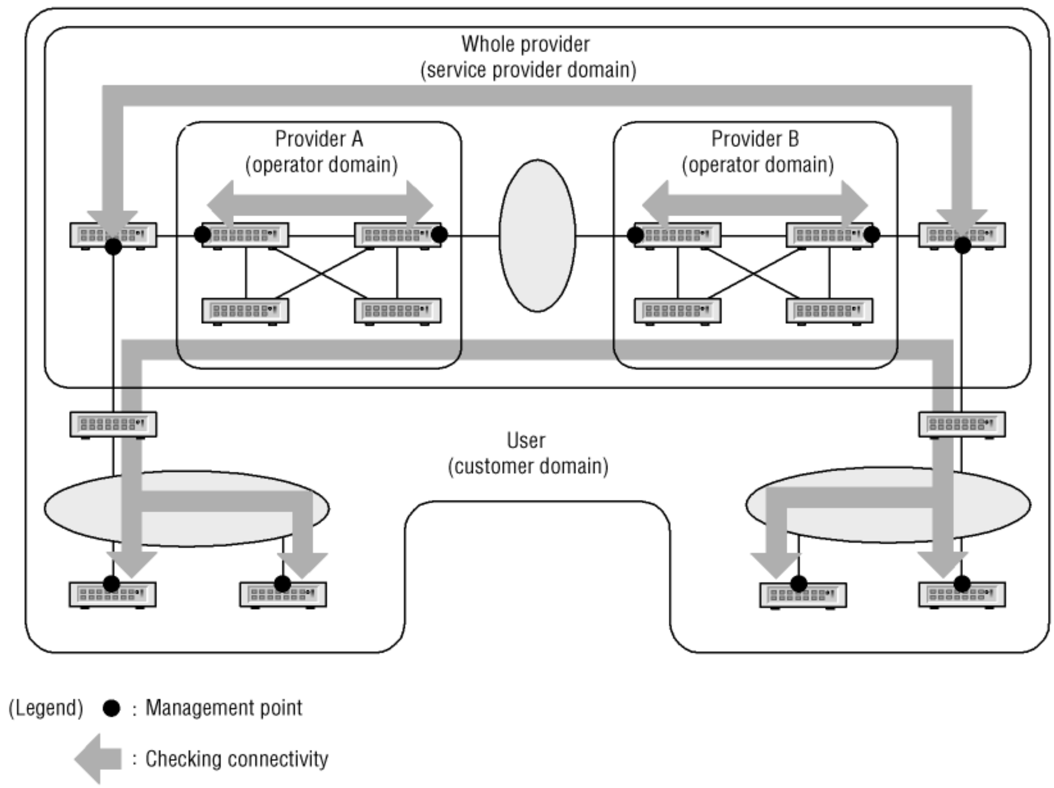
   This functionality identifies how far loopback reaches on the route after detecting a failure. (It performs a loopback test.)

3. Linktrace

   After a failure is detected, the linktrace functionality verifies the route to a management point (route searching within a Layer 2 network).

The following figure shows a configuration example of CFM.

Figure 20-1 CFM configuration example



(1) CFM functionality

CFM is defined by `IEEE 802.1ag` and has the functionality described in the table below. The Switch supports all of this functionality.

Table 20-1 CFM functionality

Name	Description
Continuity check (CC)	Continuously monitors accessibility between management points.
Loopback	Loopback test. Executes ping-equivalent functionality in Layer 2.
Linktrace	Route search. Executes traceroute-equivalent functionality in Layer 2.

(2) CFM configuration

The table below describes the CFM components. The scope of CFM operation is maintenance and management for domains, MAs, MEPs, and MIPs.

Table 20-2 CFM components

Name	Description
Domain (Maintenance Domain)	A management group on the network for which CFM is applied.
MA (Maintenance Association)	A group of VLANs used to subdivide a domain for management.
MEP (Maintenance association End Point)	A management termination point. A MEP is a port on the boundary of a domain and is set for each MA. In addition, MEPs execute CFM functionality.
MIP (Maintenance domain Intermediate Point)	A management intermediate point. This management point is located inside a domain.
MP (Maintenance Point)	A management point. A general term for MEP and MIP.

20.1.2 CFM components

(1) Domain

CFM manages a network hierarchically on a domain-by-domain basis, and maintains and manages the network by sending and receiving CFM PDUs within a domain. Domains are classified into eight levels from 0 to 7 (domain level), with larger value indicating a higher level.

Higher-level domains discard CFM PDUs from lower-level domains. Lower-level domains forward CFM PDUs from higher-level domains without processing them. Therefore, CFM PDUs from lower-level domains cannot be passed to the higher-level domains; each domain can independently execute maintenance and management.

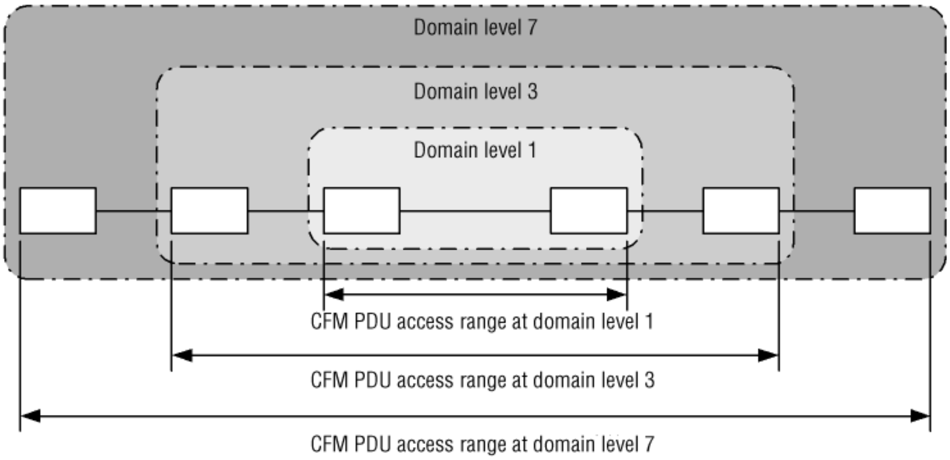
Domain levels are specified in the standard to be used according to classes. Domain levels assigned to classes are shown in the following table.

Table 20-3 Domain levels assigned to classes

Domain level	Class
7	Customer (user)
6	
5	
4	Service provider (overall business unit)
3	
2	Operator (business unit)
1	
0	

Domains can be set hierarchically. To hierarchically configure domains, place lower-level domains inside and higher-level domains outside. The following figure shows a configuration example of hierarchical domains.

Figure 20-2 Configuration example of hierarchical domains



(2) MA

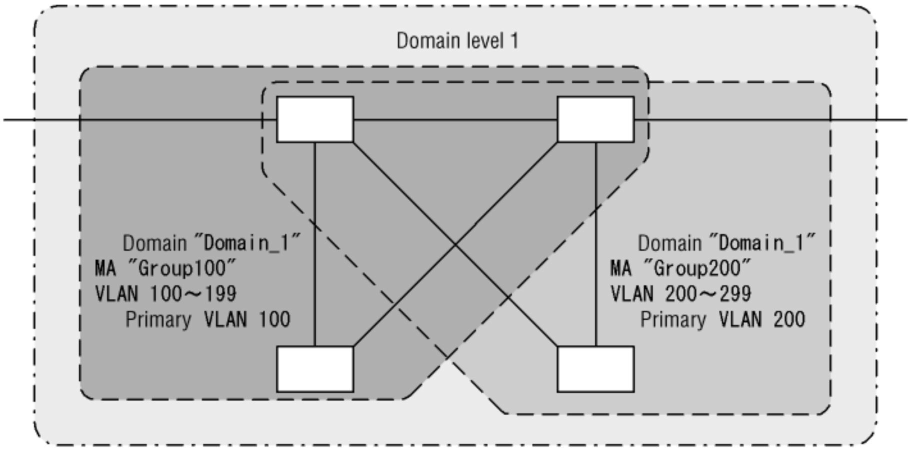
An MA is used to manage a domain by subdividing it into VLAN groups. A domain must have at least one MA.

Since CFM operates within MAs, the setting of MAs allows the management area to be controlled in detail.

MAs are identified by a domain name and an MA name. Accordingly, for the switches used in the same MA, the same domain name and the same MA name must be specified.

The following figure shows an example of the scope of MA management.

Figure 20-3 Example of the MA management scope



The same settings must be used for the VLAN that sends and receives CFM PDUs within the same MA (the primary VLAN).

As the initial setting, the VLAN with the smallest VLAN ID within an MA is the primary VLAN. By using the `ma vlan-group` configuration command, you can explicitly set any VLAN as the primary VLAN.

By setting the primary VLAN so that it is the same VLAN as that for forwarding data, you can monitor actual accessibility.

(3) MEP

An MEP is a management point on a domain boundary, and is specified for an MA. An MEP is identified by a MEP ID, which is unique within the MA.

The CFM functionality is executed at a MEP. When CFM PDUs are sent and received between MEPs (that is, at domain boundaries), the CFM functionality is able to check the connectivity of the applicable network.

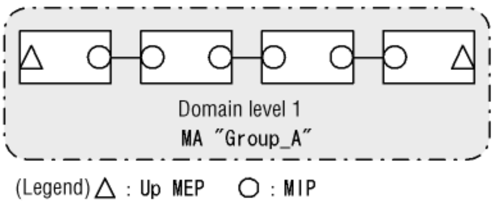
There are two types of MEPs:

- *Up MEP*

  This MEP is set on the forwarding side. The up MEP itself does not send or receive CFM PDUs. Instead, it sends and receives the PDUs through a MIP or a port in the same MA.

  The following figure shows a configuration example of up MEPs.

Figure 20-4 Configuration example of up MEPs

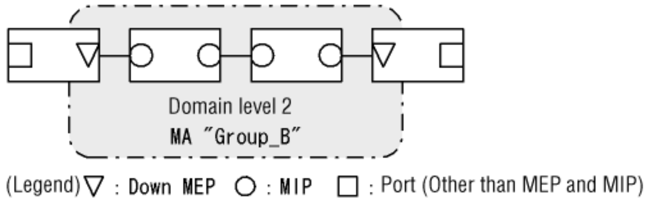


- *Down MEP*

  This MEP is set on the line side. The down MEP sends and receives CFM PDUs itself.

  The following figure shows a configuration example of down MEPs.

Figure 20-5 Configuration example of down MEPs



The following figures explain how CFM PDFs are sent from the down MEP and the up MEP and received at the down MEP and the up MEP.

Figure 20-6 Sending CFM PDFs from the down MEP or the up MEP

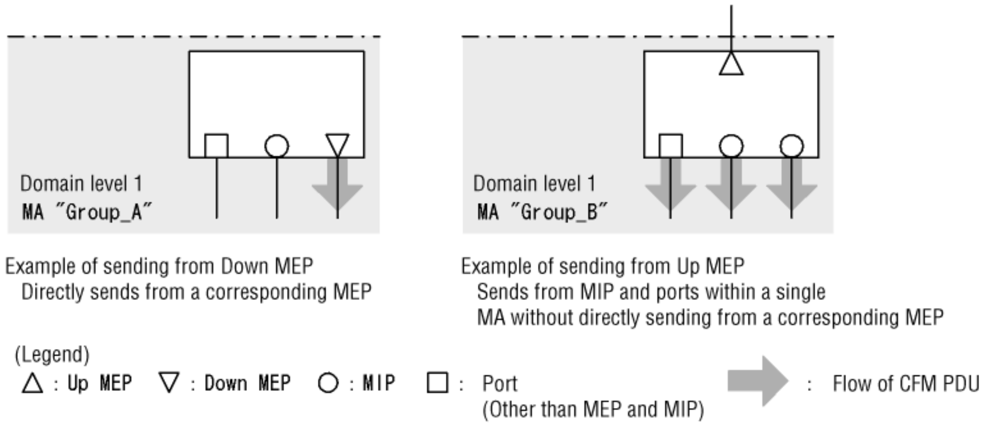
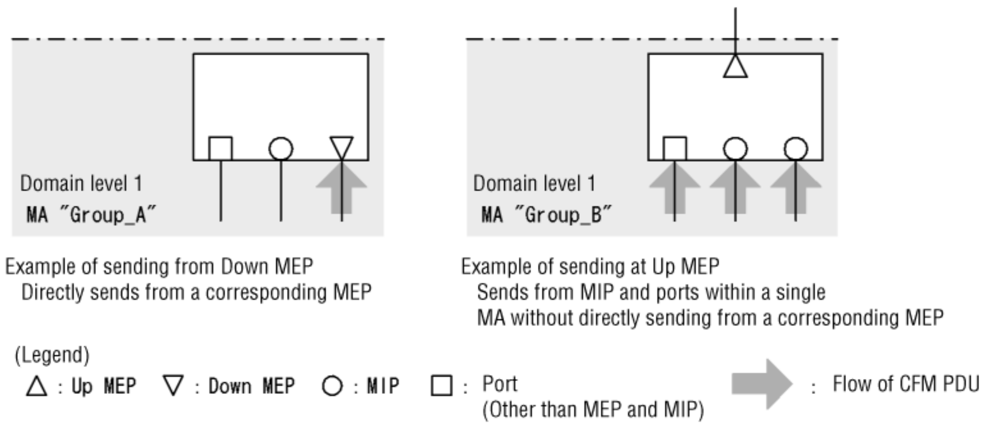
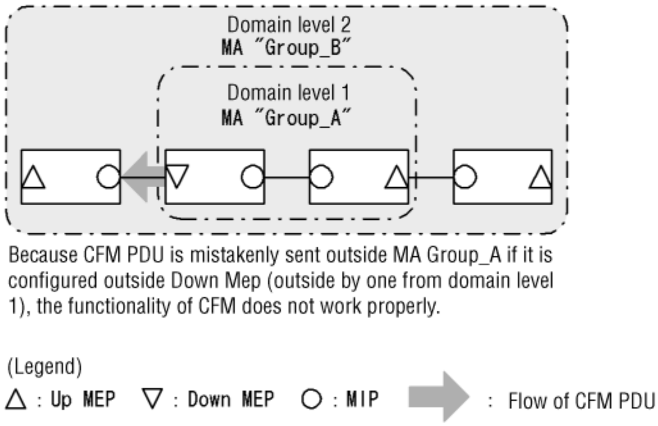


Figure 20-7 Receiving CFM PDFs at the down MEP or up MEP



Set the down MEP and the up MEP at the correct locations. For example, a down MEP must be set on the line side (inside an MA). If you place a down MEP on the forwarding side (outside an MA), CFM does not function correctly because CFM PDUs are sent outside the MA. The following figure shows an example of an incorrectly set down MEP.

Figure 20-8 Example of an incorrectly set down MEP



(4) MIP

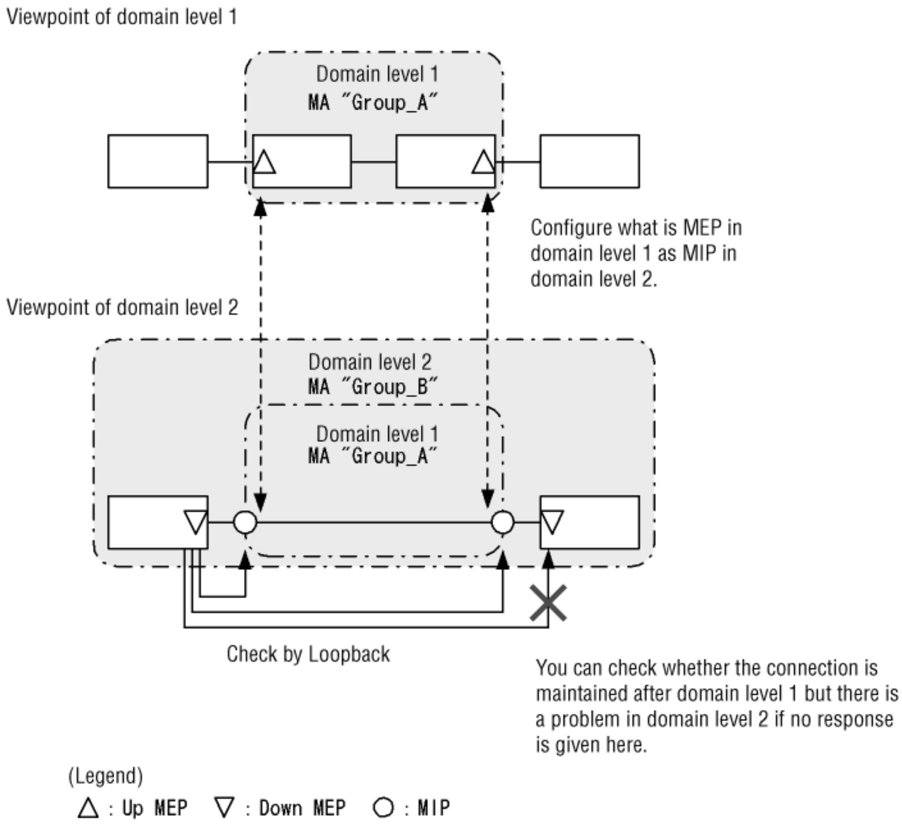
An MIP is a management point set inside a domain, and is specified for each domain (and is shared by all MAs inside a domain). For a hierarchical configuration, set a MIP at the point where a higher-level domain and a lower-level domain overlap. In addition, because MIPs respond to the loopback functionality and the linktrace functionality, set a MIP inside a domain at the point where you want maintenance and management to occur.

(a) When setting a MIP at the point where domains overlap

If you set a MIP at the point where domains overlap, you can manage these domains in a state in which a higher domain recognizes a lower domain, but in which the higher domain is unaware of the configuration of the lower domain.

The following figure shows an example of a hierarchical structure configured for domain levels 1 and 2.

Figure 20-9 Example of a hierarchical structure with domain levels 1 and 2



When designing domain level 2, specify a port set as a MEP in an MA of domain level 1 as a MIP in domain level 2. By doing so, you can manage domain level 2 without being aware of domain level 1 during operation, even if domain level 2 recognizes the domain level 1's range.

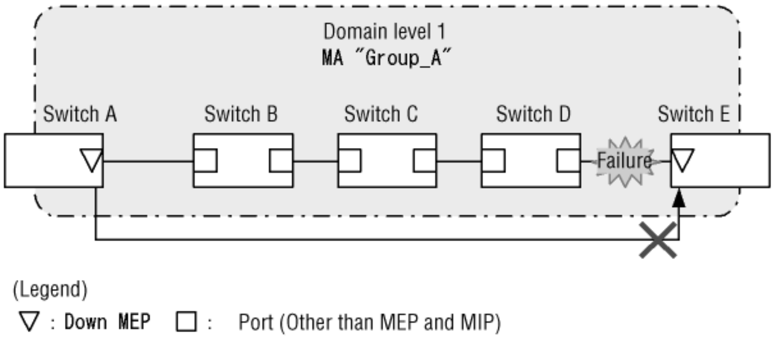
If a failure occurs, you can narrow down the scope of the investigation because you are able to isolate the cause of the failure to domain level 1 or domain level 2.

(b) When setting a MIP at the point where you want maintenance and management to occur

The more MIPs you specify in a domain, the more precisely you can maintain and manage the domain.

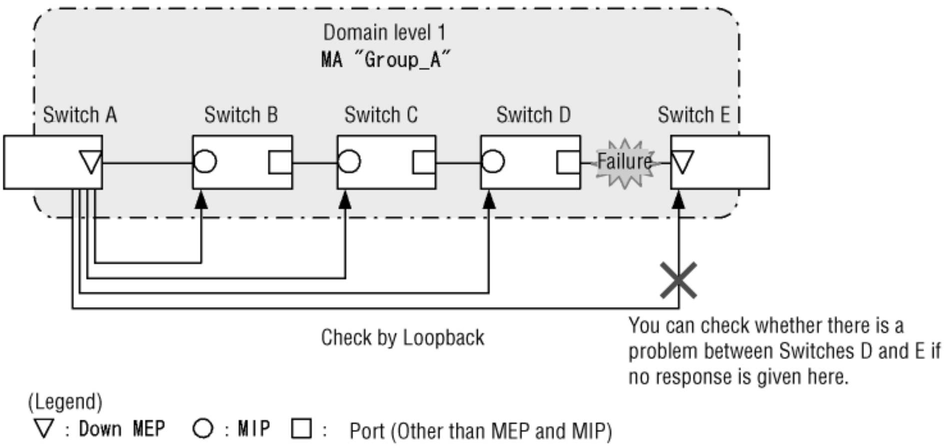
The figure below shows an example configuration where no MIPs are set in a domain. In this example, if a network failure occurs, you can confirm that the MEP of switch A cannot communicate with the MEP of switch E, but you cannot identify the point at which the failure occurred.

Figure 20-10 Example configuration in which no MIPs are set in a domain



The figure below shows an example configuration in which MIPs are set in a domain. In this example, you can determine the point at which a failure occurs because the MIPs in the domain make it possible for each switch to respond to the loopback or linktrace functionality.

Figure 20-11 Example configuration where MIPs are set in a domain



20.1.3 Designing domains

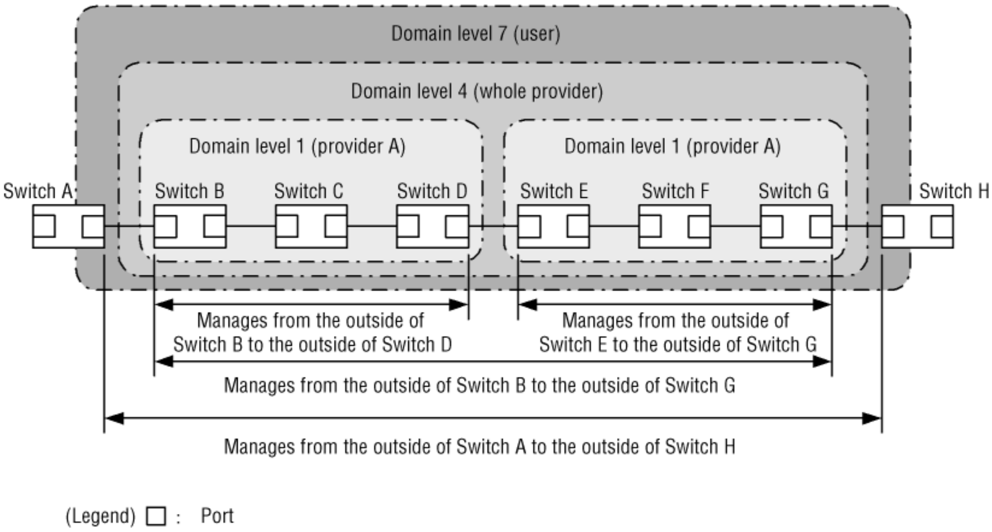
To use the CFM functionality, design the domains first. Then design the domain configurations and their hierarchies, and finally design the details of each domain.

When you design a domain, you must configure the domain level, MAs, MEPs, and MIPs.

(1) Designing the domain configuration and its hierarchy

Set an MA port (for which the MA is the boundary between domains) as a MEP and set a port that overlaps with the lower domain as a MIP. The procedure for designing the domain configuration and the hierarchy is described below according to the configuration example shown in the following figure.

Figure 20-12 Configuration example



Design the domain as units, such as business unit A, business unit B, the overall business unit, and user, and then specify the domain level appropriate for the class. Also, the following items are assumed:

- Business unit A, business unit B, and the overall business unit manage connectivity, including the ports to be provided to users, in order to ensure the availability of lines that need to be provided to users.
- Users manage the connectivity of the line provided by a business unit in order to monitor the availability of that line.

Design a domain from the lowest level up as described below.

■ Configuring domain levels 1 and 2

1. In domain level 1, configure MA "Group_A".

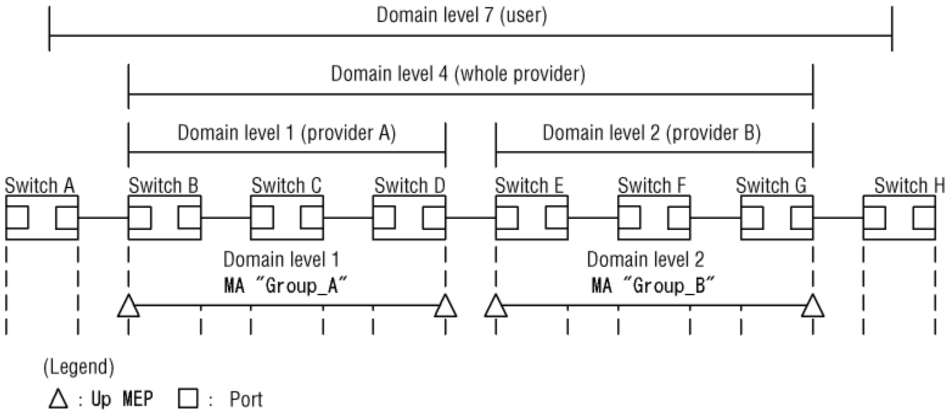
   In this example, one domain is managed by one MA. If you want to manage the domain more precisely by subdividing it into VLAN groups, set an MA for each management unit.

2. Set an MA port as a MEP on switches B and D, which are on the domain boundary.

   The business unit configures the up MEPs in order to manage the connectivity, including the ports to be provided to users.

3. Set an MA for domain level 2 as well, and configure an up MEP on switches E and G.

Figure 20-13 Configuring domain levels 1 and 2



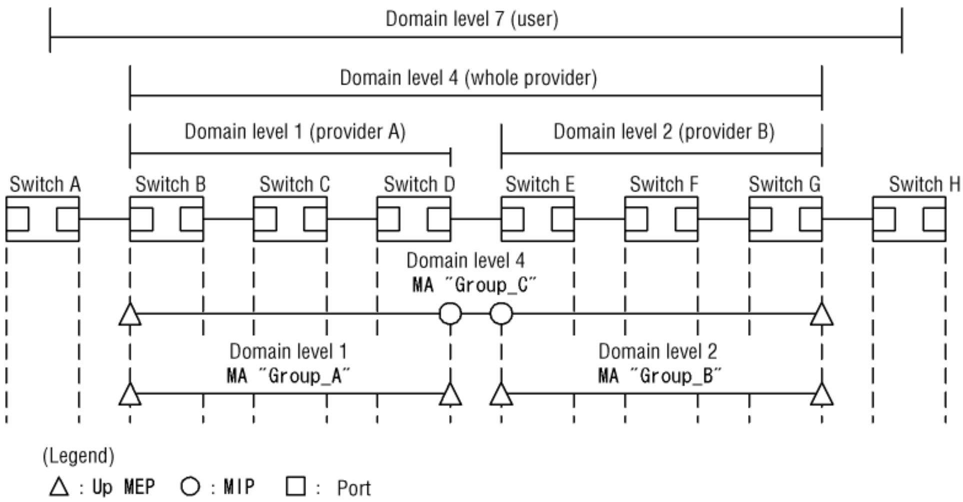
■ Configuring domain level 4

1. In domain level 4, configure MA "Group_C".
2. Set an MA port as a MEP on switches B and G, which are on the boundary of domain level 4.

   The business unit configures the up MEPs in order to manage the connectivity, including the ports to be provided to users.
3. Because domain level 4 contains domain levels 1 and 2, configure MIPs on switches D and E, which are the relay points of each domain level.

   If you set a MEP of a lower domain as a MIP in a higher domain, you can identify the scope of investigation more easily because you can use the loopback or linktrace functionality to determine if the problem has occurred in the domain you manage or in a lower-level domain.

Figure 20-14 Configuring domain level 4



■ Configuring domain level 7

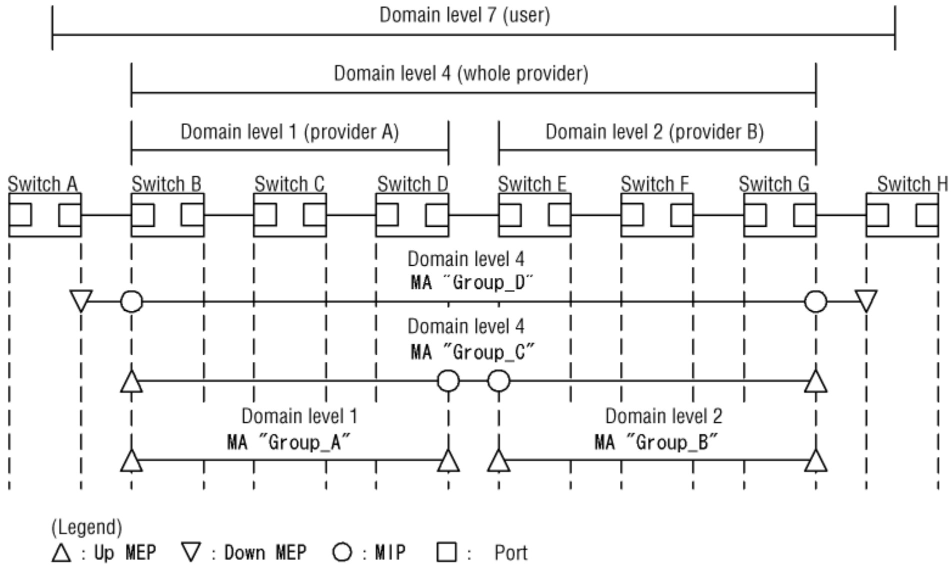
1. In domain level 7, specify MA "Group_D".
2. Set an MA port as a MEP on switches A and H, which are on the boundary of domain level 7.

   In order to manage the connectivity of the lines provided by business units, users configure the down MEP.

3. Because domain level 7 contains domain level 4, configure MIPs on switches B and D, which are relay points.

   Because domain levels 1 and 2 are specified as relay points of domain level 4, it is not necessary to configure domain levels 1 and 2 in domain level 7.

Figure 20-15 Configuring domain level 7



(2) Detailed design of each domain

For the detailed design, configure, as MIPs, the points to which you want to apply the loopback functionality and the linktrace functionality.

The following figure shows configuration examples before and after MIPs are set.

Figure 20-16 Configuration example before MIPs are set

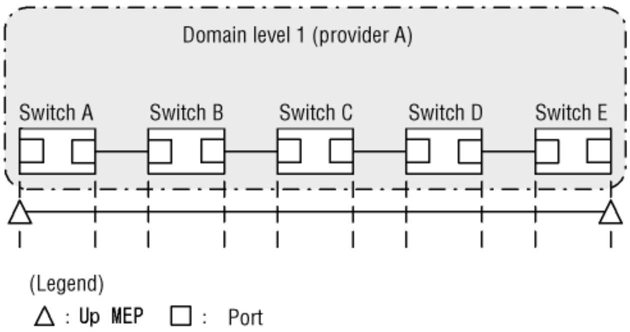
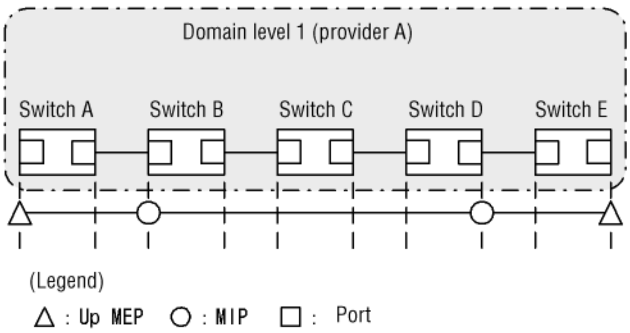


Figure 20-17 Configuration example after MIPs are set



Inside the domain, specify, as MIPs, the ports to be configured as the destination of the loopback functionality and the linktrace functionality. In this example, MIPs are set on switches B and D. With this configuration, you can perform loopback and linktrace for the MIPs on switches B and D. In addition, route information of the linktrace functionality is returned as a response.

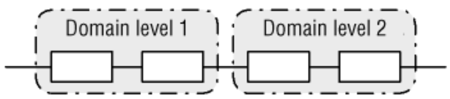
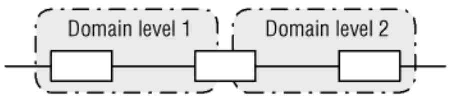
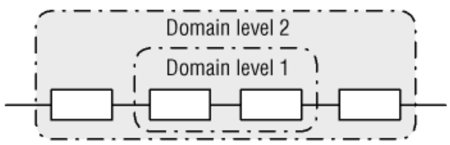
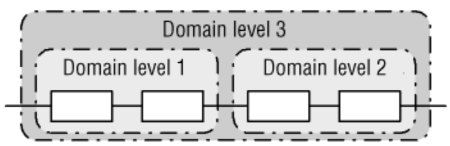
You cannot specify switch C as the destination for loopback and linktrace because no MIPs are configured on switch C. In addition, because switch C does not respond to the linktrace functionality, information about switch C is not contained in route information.

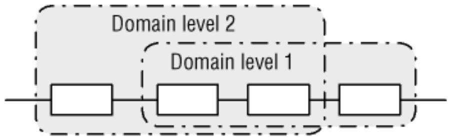
(3) Domain configuration examples

Domains can be configured hierarchically. The inner part of the hierarchy must be configured as lower-level domains and the outer part as higher-level domains.

The following table provides configuration examples and states whether they are possible or not.

Table 20-4 Example of possible and impossible domain configurations

Configuration status	**Configuration example**	**Whether configurable**
Adjacent domains		Yes
Touching domains		Yes
Nested domains		Yes
Combination of adjacent domains and nested domains		Yes

Configuration status	Configuration example	Whether configurable
Overlapping domains		No

20.1.4 Continuity check

The continuity check (CC) is functionality that continuously monitors the connectivity between MEPs. All MEPs in an MA exchange CCMs (continuity check messages, which is a kind of CFM PDU) with each other to learn the MEPs in the MA. What the MEPs learn is used for the loopback functionality and the linktrace functionality.

If a switch on which the CC functionality is used does not receive CCMs or a port on the applicable switch in an MA cannot communicate, a failure is determined to have occurred. When this happens, a CCM with a failure detection flag is sent to notify MEPs in the MA of the failure.

The table below describes the failures detectable by the CC functionality. There are multiple failure levels. The configuration of the Switch can change the failure level detected. By default, failures of level 2 or higher are detected.

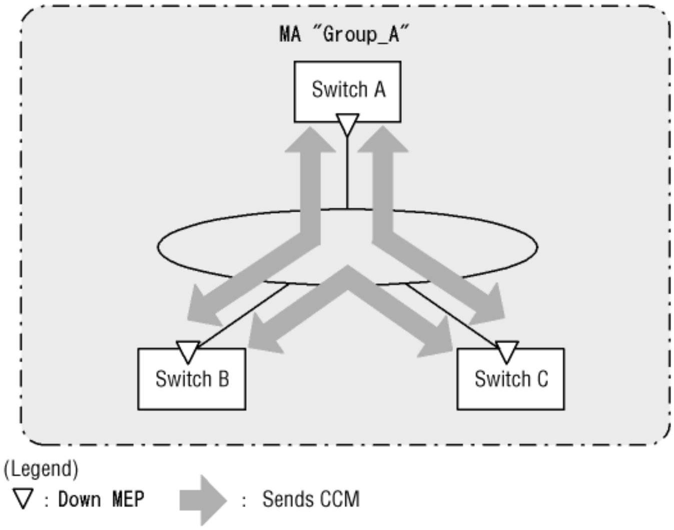
Table 20-5 Levels detected by CC and failure descriptions

Failure level	Failure description	Initial state
5	A domain and the MA received different CCMs.	Detected
4	A CCM with an incorrect MEP ID or an incorrect sending interval was received.	
3	CCMs are no longer received.	
2	A port on the applicable switch has entered a state in which it is unable to communicate.	
1	A CCM reporting failure detection was received. Remote Defect Indication	Not detected
0	No failure detected	

CC functionality behavior will be described using switch B in the following figures as an example.

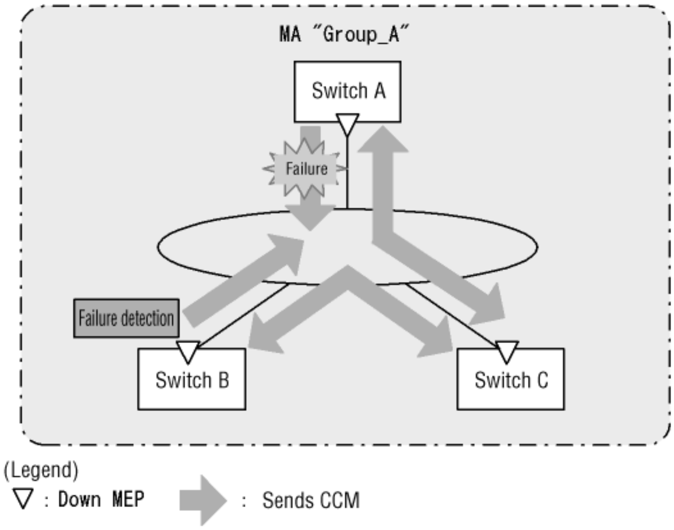
Each MEP uses multicast to send CCMs inside the MA at one-minute intervals. Because CCMs are received from each MEP regularly, connectivity is always monitored. In addition, the configuration of the Switch can change the intervals of CCM transmissions.

Figure 20-18 Continuous monitoring of the connectivity by using the CC functionality



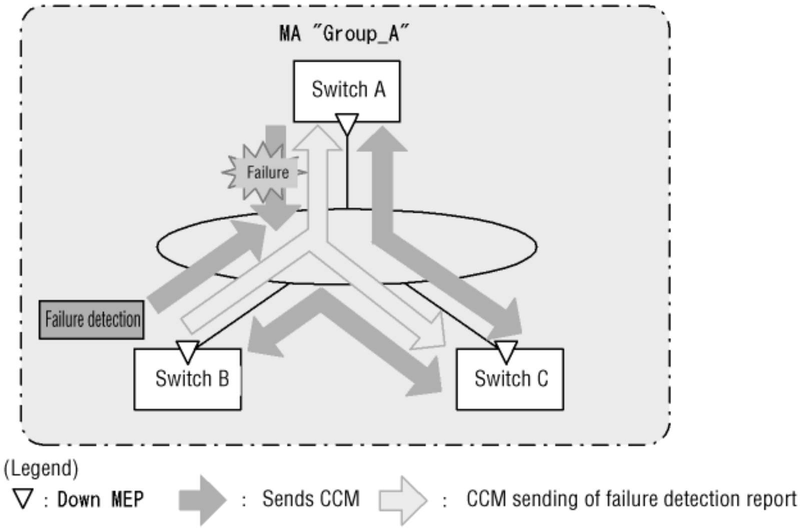
If a CCM from switch A cannot be delivered to switch B because of a switch failure or a network failure, switch B determines that the state is a network failure between switches A and B.

Figure 20-19 Detecting a failure by using the CC functionality



When switch B detects a failure, switch B notifies all MEPs in the MA that a failure has been detected.

Figure 20-20 Reporting failures to all MEPs



The MEPs that received the CCM indicating a detected failure acknowledge that a failure has occurred somewhere in the MA. If loopback and linktrace are performed on each switch, the switches can determine the route inside the MA on which the failure occurred.

(1) Failure detection and trap notification

When CC detects a failure, the trap is reported. Note that the configuration can be used to restrict trap notification for a specified time after a failure is detected. The following table shows time types to be set via the configuration.

Table 20-6 Trap notification time when CC detects a failure

Time type	Description	Setting range
Failure detection start time (trap notification time after failure detection)	Time after failure detection until trap notification. After the time set by configuration elapses after failure detection, trap is notified.	From 2,500 to 10,000 ms
Failure re-detection time (continuous trap notification restricted time)	Time during which continuous failure detection is regarded as re-detection. Even if a failure is detected within the time specified by configuration after failure detection, it is regarded as re-detection and no trap is notified. (However, if a higher level failure than current level is detected during re-detection time, trap is notified.)	From 2,500 to 10,000 ms

20.1.5 Loopback

The loopback functionality can be used at the Layer 2 level, and is equivalent to pinging. The loopback function verifies the connectivity between MEPs or between a MEP and a MIP in the same MA.

The CC functionality verifies the connectivity between MEPs. The loopback functionality can additionally verify the connectivity between a MEP and a MIP, with the result that it can check the connectivity in an MA in greater detail.

Connectivity is verified by sending a loopback message (a kind of CFM PDU) from the MEP to the destination and confirming that the destination responds to the message.

The MIP or MEP responds directly to the loopback functionality. If, for example, multiple MIPs are configured on a switch, connectivity can be verified for each MIP.

The following figure shows an example of executing the loopback for MIPs and MEPs.

Figure 20-21 Example of executing loopback for MIPs

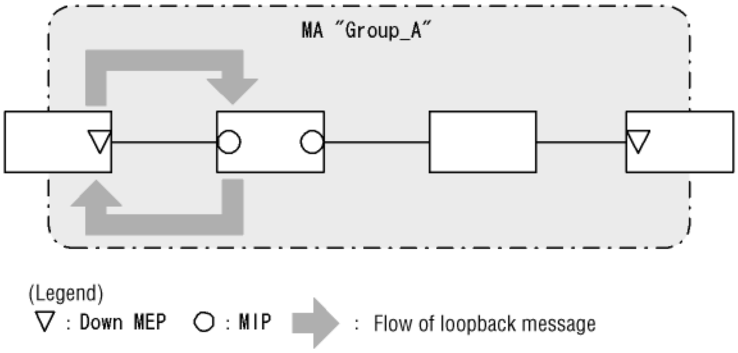
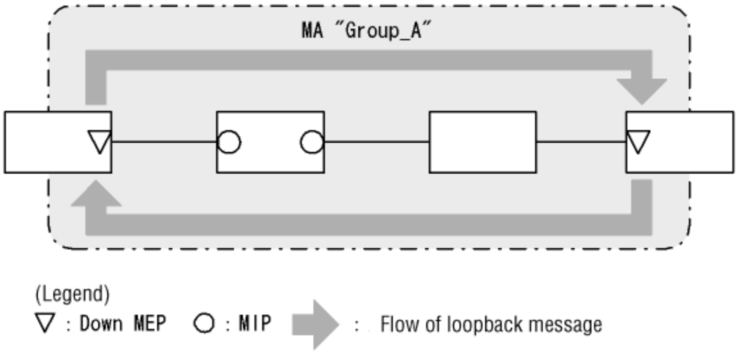


Figure 20-22 Example of executing loopback for MEPs



Because the loopback functionality uses what the CC functionality learns, the CC functionality must be started beforehand. If you configure a MIP on the destination switch, you must note the MAC address of the port used as the MIP beforehand.

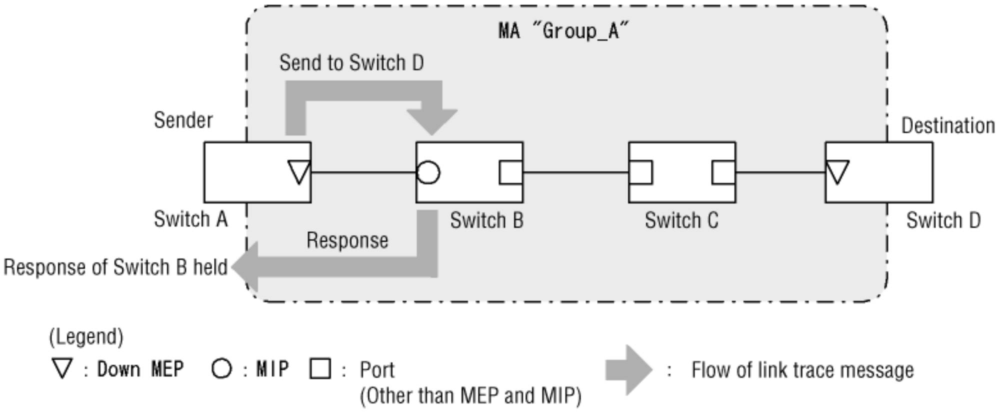
20.1.6 Linktrace

The linktrace functionality can be used at the Layer 2 level, and is equivalent to traceroute. The linktrace functionality collects information about switches that pass traffic between MEPs or between a MEP and a MIP of the same MA, and outputs route information.

The linktrace functionality sends a linktrace message (a kind of CFM PDU) and collects the returned responses as routing information.

The following figure shows an example of sending a linktrace message to a destination.

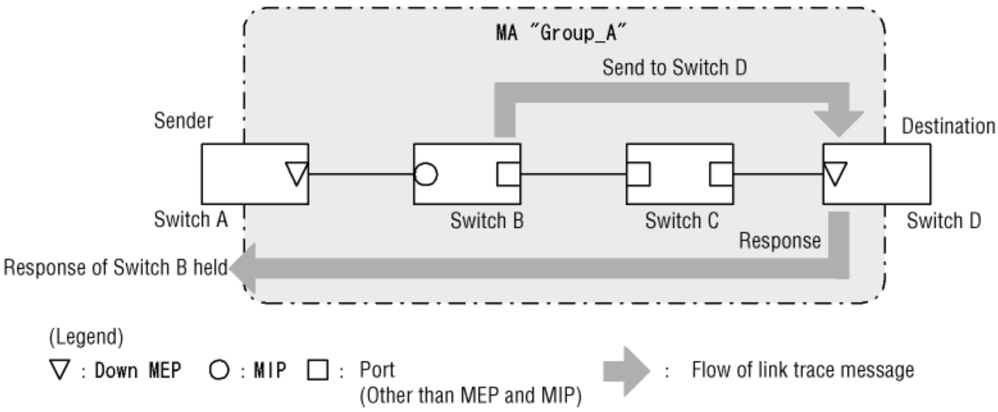
Figure 20-23 Example of sending a linktrace message to a destination



A linktrace message is forwarded to the destination via MIPs. An MIP sends back information about the port of the local switch used to receive the MIP and the ports used to forward the MIP. The switch from which the message was sent (the source switch) keeps the information sent by the MIPs as route information.

The following figure shows an example of forwarding a linktrace message to the destination.

Figure 20-24 Example of forwarding a linktrace message to the destination



The MIP that sent back the information forwards the linktrace message to the destination. However, switch C in the above figure does not send back the information because MEPs or MIPs are not configured on switch C. At least one MIP must be configured on a switch in order to send back information.

When a linktrace message reaches the MEP or the MIP at the destination, a message containing information about the MEP or MIP at the destination to which the linktrace message was delivered and the port through which the message was received is delivered to the source switch.

The source switch outputs the information it has retained as route information that can be used to check the route to the destination.

The linktrace functionality provides information for each switch. For example, whether one or multiple MIPs are configured on a switch, the linktrace functionality provides information about the port used to receive the message and the port used to forward the message.

Because the linktrace functionality uses what the CC functionality learns, the CC functionality must be started beforehand. If you configure a MIP on the destination switch, you must note the MAC address of the port used as the MIP beforehand.

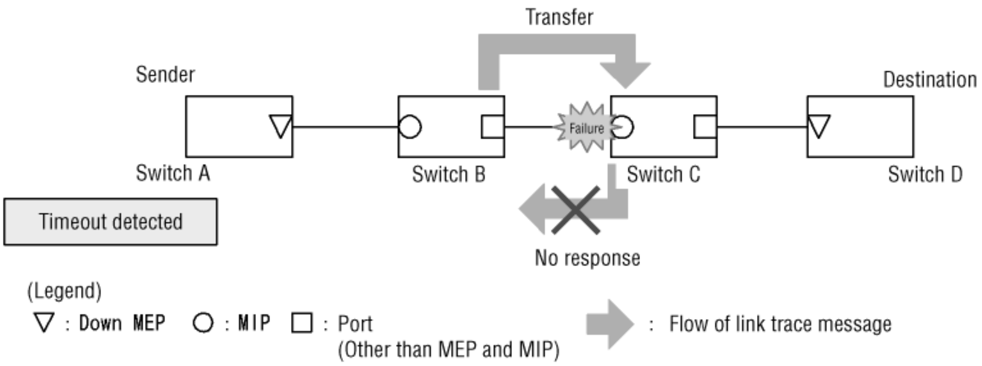
(a) Using the linktrace functionality to isolate failures

You can use the execution results of the linktrace functionality to isolate the switch or port on which a failure has occurred.

■ *When a timeout is detected*

The following figure shows an example of timeout detection by the linktrace functionality.

Figure 20-25 Example timeout detection by the linktrace functionality

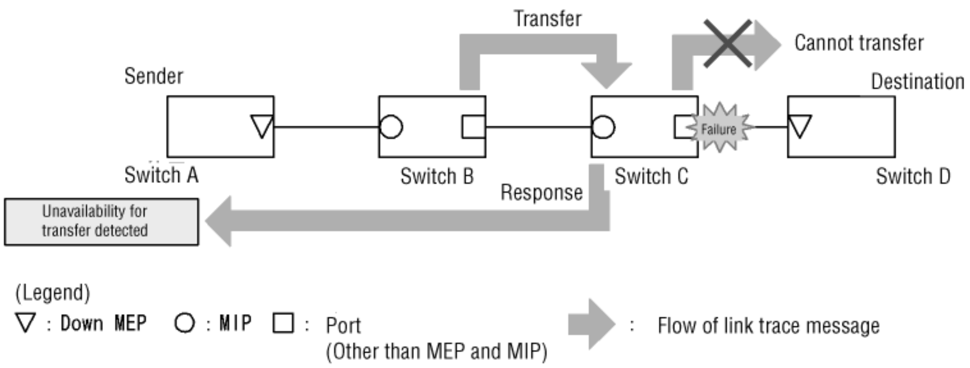


In this example, when switch A detects a timeout by using the linktrace functionality, a receiving port on the network might not be able to communicate. A linktrace message is forwarded from switch B to switch C, but because switch C cannot communicate and cannot return a response, a timeout occurs.

■ *When a forwarding failure is detected*

The following figure shows an example of a communication failure detected by the linktrace functionality.

Figure 20-26 Example of detection of a communication failure by the linktrace functionality



If switch A detects a forwarding failure by using the linktrace functionality, a sending port on the network might not be able to communicate. This is because a response is returned to Switch A indicating that the port on the sending side cannot communicate if Switch C cannot forward the linktrace message to Switch D (destination).

(b) Linktrace response

Linktrace messages are multicast frames.

When forwarding linktrace messages between switches on which CFM is used, the port used for forwarding is determined by referring to the MIP CCM database and the MAC address table.

Switches on which CFM is not used flood linktrace messages. As a result, if there is a switch on the network on which CFM is not used, responses are returned from switches that are not on the route to the destination.

20.1.7 Specifications for common operations

(1) Behavior for a blocked port

The following tables describe the behavior of each type of CFM functionality for a blocked port.

Table 20-7 When an up MEP is blocked

Functionality	Operation
CC	● Sends and receives a CCM and sets Blocked as the status of the port from which the CCM was sent.
Loopback	● Can execute the `l2ping` operation command. ● Responds to loopback messages sent to the local switch.
Linktrace	● Can execute the `l2traceroute` operation command. ● Responds to link trace messages. The Egress Port is set to Blocked in response to linktrace messages.

Table 20-8 When a down MEP is blocked

Functionality	Operation
CC	● CCM is not sent.
Loopback	● The `l2ping` operation command cannot be executed. ● Does not respond to loopback messages sent to the local switch.
Linktrace	● The `l2traceroute` operation command cannot be executed. ● Does not respond to linktrace messages.

Table 20-9 When an MIP is blocked

Functionality	Operation
CC	● Does not transmit CCMs.
Loopback	● Does not respond to a loopback message received from the line side and sent to the local switch. ● Responds to a loopback message received from the forwarding and sent to the local switch. ● Does not transmit loopback messages.

Functionality	Operation
Linktrace	● Does not respond to a linktrace message received from the line side ● Responds to a linktrace message received from the forwarding side. The Egress Port is set to Blocked in response to linktrace messages. ● Does not transmit linktrace messages

Table 20-10 When ports other than MEP and MIP ports are blocked

Functionality	Operation
CC	● Does not transmit CCMs.
Loopback	● Does not transmit loopback messages.
Linktrace	● Does not transmit linktrace messages

20.1.8 Databases used for the CFM functionality

The following table describes the databases used by the CFM functionality.

Table 20-11 Databases used for the CFM functionality

Database	Description	Command for checking its contents
MEP CCM database	A database maintained by each MEP. Information about MEPs in the same MA. The CC functionality uses this database to continuously monitor connectivity in CC. The database holds the following information: ● MEP ID ● MAC addresses corresponding to the MEP ID ● Information about failures occurring at the applicable MEP.	`show cfm remote-mep`
MIP CCM database	A database maintained by switches. Information about MEPs in the same MA. This database is used to determine the port used for forwarding a linktrace message. The database holds the following information: ● MEP MAC address ● VLAN and the port on which CCMs of the applicable MEP were received	None
Linktrace database	A database holding the execution results of the linktrace functionality. The database holds the following information: ● The MEPs and the destinations where the linktrace functionality was executed ● TTL ● Information about switches that sent back	`show cfm l2traceroute-db`

Database	Description	Command for checking its contents
	responses ● Information about ports on which linktrace messages were received ● Information about ports from which linktrace messages were forwarded	

(1) MEP CCM database

The MEP CCM database holds information about the types of MEPs that are in the same MA. It also holds information about the failures occurring at the applicable MEPs.

Although you can specify the destination by using the MEP ID for the loopback functionality and the linktrace functionality, the MEP ID that are not registered in the MEP CCM database cannot be specified. You can use the `show cfm remote-mep` operation command to check if a MEP ID is registered in the database.

An entry in this database is created when a MEP receives a CCM while the CC functionality is running.

(2) MIP CCM database

The MIP CCM database is used to determine the port from which a linktrace message was forwarded.

When a linktrace message is forwarded, if the MAC address of the destination MEP is not registered in the MIP CCM database, the port for forwarding is determined by referring to the MAC address table.

If the MAC address is not found in the MAC address table, a response indicating that the message could not be forwarded is sent to the source without forwarding the linktrace message.

An entry for this database is created when a MIP transfers a CCM while the CC functionality is running.

(3) Linktrace database

The linktrace database holds the execution results of the linktrace functionality.

You can use the `show cfm l2traceroute-db` operation command to see the results of executing the linktrace functionality in the past.

(a) Number of routes that can be held

Responses for a maximum of 256 switches per route can be stored for a total of 1024 switches.

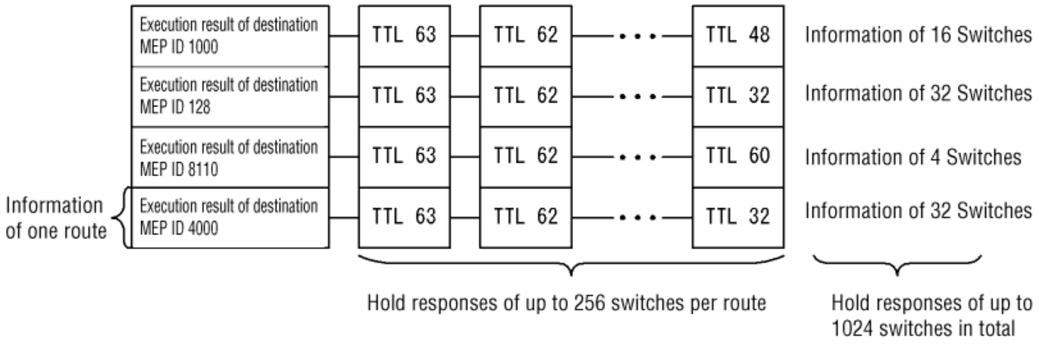
The number of routes that can be retained is determined by the number of switches per route. If you want to retain responses for 256 switches per route, you can have four routes. If you want to retain responses for 16 switches per route, you can have 64 routes.

If the number of responses exceeds for the number of responses allowed for 1024 switches, information about an old route is deleted, and information about the new route is saved.

When the linktrace functionality is executed at a destination that is registered in the linktrace database, the route information up to the target destination is deleted from the linktrace database, and a new linktrace response is stored.

The following figures show entries in the linktrace database.

Figure 20-27 Linktrace database



An entry in this database is created when a MEP receives a response while the linktrace functionality is running.

20.1.9 Notes on using the CFM functionality

(1) About switches on which the CFM functionality is not used

When you use the CFM functionality, you do not need to use it on all the switches in a domain. However, CFM PDUs must be transparent on the switches on which the functionality is not used.

Except for the Switch, you need to configure the switches on which the CFM functionality is not used so that the frames described in the following table are transparent.

Table 20-12 Frames that need to be transparent

Frame type	Destination MAC address
Multicast	`0180.c200.0030` to `0180.c200.003f`

If the CFM functionality is not used, the Switch makes all CFM PDUs transparent.

(2) Use with other functionality

For interoperability with other functionality, the behavior is described in the following table.

Table 20-13 Interoperability with other functionality of the Switch

Functionality		Availability	Remarks
Port type	Access port	Y	
	Trunk port	Y	
	Protocol port	N	CFM frames cannot join the port on the left (cannot be forwarded in VLAN).

Functionality		Availability	Remarks
	MAC port	N	CFM frames cannot join the port on the left (cannot be forwarded in VLAN).
VLAN	Relay blocking between ports	N	Relay-blocking functionality between ports is invalid for CFM frames.
Link aggregation		Y	CFM operates on each channel.
Spanning Tree Protocol		Y	
GSRP aware		Y	
Ring Protocol		Y	
IGMP/MLD snooping		Y	
DHCP Snooping		Y	
	Terminal filtering	N	CFM frames cannot be received.
	Dynamic ARP inspection	Y	
The L2 loop detection functionality		Y	
LLDP		N	
UDLD		Y	
Filters		N	For MAC access list specification, implicit discard is performed.
QoS		N	No effect on forwarding. Priority of frames originated by the device can be changed.
IEEE 802.1X authentication		N	Since CFM frames might not be received, do not set the authentication port on the forwarding route of CFM.
Web authentication (including one-time password authentication)		N	
MAC-based Authentication		N	
Multistep authentication		N	
Secure Wake-on-LAN		N	
Uplink redundancy		Y	
Storm Control		Y	If multicast is specified, CFM is also discarded.

Functionality	Availability	Remarks
Port Mirroring	N	Monitor port setting is invalid. In addition, frames originated by the device and software-forwarded frames cannot be mirrored.

Legend:

Y: Available

N: Not available

(3) About burst reception of CFM PDUs

When there are 48 or more remote MEPs to be monitored continuously by the CC functionality, the Switch might receive CFM PDUs in a burst if the timing for sending CFM PDUs from remote MEPs is accidentally the same. In such case, the Switch might discard CFM PDUs and might detect a failure incorrectly.

If this problem occurs often, adjust the timing for sending CFM PDUs on all switches so that there is no timing overlap.

(4) About the MEP settings in MAs in which the same primary VLAN is configured in the same domain

For MAs (including the same MA) that sets the same primary VLAN in the same domain, do not set multiple MEPs for the same port. If you do so, the CFM functionality does not operate correctly on the applicable MEPs.

(5) About collecting route information by using the linktrace functionality

The linktrace functionality determines the destination port for forwarding linktrace messages by referencing the MIP CCM database or the MAC address table. However, correct route information cannot be collected because the destination port cannot be determined until the CC functionality sends or receives a CCM when link-up is detected (including a second link-up after a link failure) or after a change of the route when the Spanning Tree Protocol is used.

(6) When a MIP on a blocked port does not respond to the loopback functionality and linktrace functionality

If you configure a MIP on a blocked port and perform one of the following operations for the port, the MIP might not respond to the loopback functionality and the linktrace functionality.

- Operation of the loop guard functionality by using a Spanning Tree Protocol (PVST+ or Single Spanning Tree)
- When the Spanning Tree Protocol (MSTP) is used, configuring the access VLAN or the native VLAN as the primary VLAN
- Operation of Ring Protocol
- Operation of uplink redundancy

(7) Behavior of the CC functionality in a redundant configuration

When the CC functionality is used in a network configured redundantly, such as when the Spanning Tree Protocol is used, if a communication route is switched, in rare cases, a CCM sent from the MEP of the local switch might be received and an ErrorCCM might be detected. This failure is corrected after the communication route becomes stable.

20.2 Configuration

20.2.1 List of configuration commands

The following table describes the commands used to configure the CFM functionality.

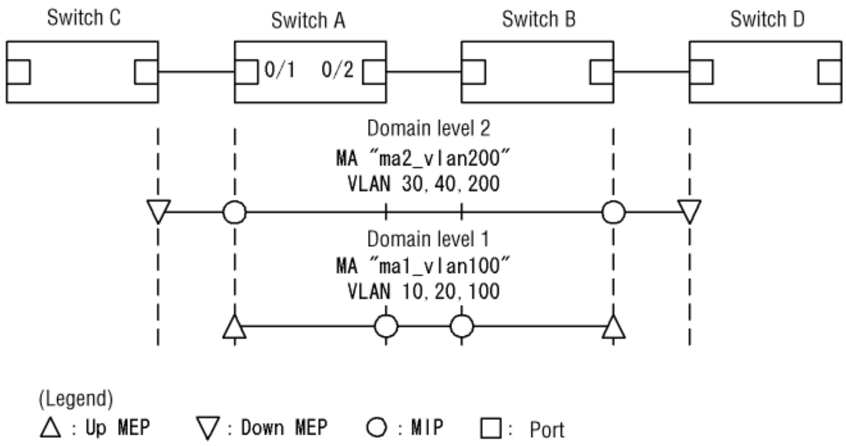
Table 20-14 List of configuration commands

Command name	Description
`domain name`	Sets the name used for the applicable domain.
`ethernet cfm cc alarm-priority`	Sets the failure level to be detected by CC.
`ethernet cfm cc alarm-reset-time`	Sets the time interval for identifying re-detection when CC repeatedly detects failures.
`ethernet cfm cc alarm-start-time`	Sets the time after CC detects a failure until a trap is sent.
`ethernet cfm cc interval`	Sets the CCM transmission interval for a target MA.
`ethernet cfm cc enable`	Sets in a domain an MA in which the CC functionality is used.
`ethernet cfm domain`	Sets a domain.
`ethernet cfm enable (global)`	Starts CFM.
`ethernet cfm enable (interface)`	Stops CFM when `no ethernet cfm enable` is set.
`ethernet cfm mep`	Sets a MEP used by the CFM functionality.
`ethernet cfm mip`	Sets a MIP used by the CFM functionality.
`ma name`	Sets the name of an MA to be used in the applicable domain.
`ma vlan-group`	Sets the VLAN belonging to the MA used in the applicable domain.

20.2.2 Configuring CFM (multiple domains)

This section describes the procedure for configuring multiple domains by using switch A in the following figure as an example.

Figure 20-28 Configuring CFM (multiple domains)



(1) Setting an MA for multiple domains and for each domain

Points to note

When there are multiple domains, configure the lowest-level domain first. When you configure an MA, the domain level, MA identification number, domain name, and MA name settings of the switch must match those of the partner switch. If these settings are different, the Switch and the partner switch are not regarded as one MA.

For the primary VLAN of the MA, set the VLAN that receives CFM PDUs from the Switch MEP.

If the `primary-vlan` parameter is not set, the VLAN with the smallest VLAN ID of the VLANs set by using the `vlan-group` parameter is selected to be the primary VLAN.

Command examples

1.
```
(config)# ethernet cfm domain level 1 direction-up
(config-ether-cfm)# domain name str operator_1
```
Sets the initial state of the domain level 1 and the MEP as an up MEP, switches to configuration Ethernet CFM mode, and sets the domain name.

2.
```
(config-ether-cfm)# ma 1 name str ma1_vlan100
(config-ether-cfm)# ma 1 vlan-group 10,20,100 primary-vlan 100
(config-ether-cfm)# exit
```
Sets the MA name, the VLANs belonging to the MA, and the primary VLAN in MA1.

3.
```
(config)# ethernet cfm domain level 2
(config-ether-cfm)# domain name str operator_2
(config-ether-cfm)# ma 2 name str ma2_vlan200
(config-ether-cfm)# ma 2 vlan-group 30,40,200 primary-vlan 200
(config-ether-cfm)# exit
```
Sets the initial state of domain level 2 and the MEP as a down MEP.

The sequence then sets the MA name, the VLANs belonging to the MA, and the primary VLAN in MA2.

(2) Configuring MEPs and MIPs

Points to note

Set no more MEPs and MIPs than the number defined in the capacity limits.

To start operation of the MEPs and MIPs you specified, enable the CFM functionality of the switch.

Command examples

1.
```
(config)# interface fastethernet 0/1
(config-if)# ethernet cfm mep level 1 ma 1 mep-id 101
(config-if)# ethernet cfm mip level 2
(config-if)# exit
(config)# interface fastethernet 0/2
(config-if)# ethernet cfm mip level 1
(config-if)# exit
```
Sets MEPs belonging to domain level 1 and MA1 for port 0/1. Also, configures a MIP in domain level 2. Set MIPs for domain level 1 to port 0/2.

2.
```
(config)# ethernet cfm enable
```
Initiates operation of the CFM functionality on the Switch.

(3) Stopping the CFM functionality on a port

Points to note

This setting is required if you want to temporarily stop the CFM functionality on a port.

Command examples

1.
```
(config)# interface fastethernet 0/1
(config-if)# no ethernet cfm enable
(config-if)# exit
```
Stops CFM on port 0/1.

(4) Configuring the CC functionality

Points to note

The CC functionality starts operation as soon as the `ethernet cfm cc enable` configuration command is set.

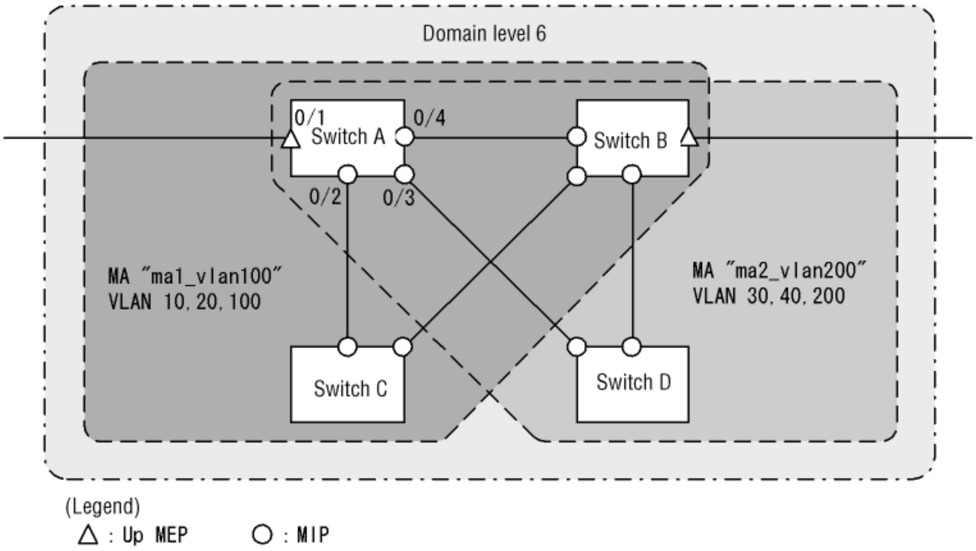
Command examples

1.
```
(config)# ethernet cfm cc level 1 ma 1 enable
```
Starts execution of CC for domain level 1 and MA1.

20.2.3 Configuring the CFM functionality (same domain, multiple MAs)

This section describes the procedure for setting multiple MAs in a single domain by using switch A in the following figure as an example.

Figure 20-29 Setting example of CFM (same domain, multiple MAs)



(1) Setting multiple MAs in the same domain

Points to note

When you set multiple MAs in the same domain, make sure that there is no duplication of MA identification numbers and MA names. For the basics of setting domains and MAs, see *20.2.2 Configuring CFM (multiple domains).*

Command examples

1.
```
(config)# ethernet cfm domain level 6 direction-up
(config-ether-cfm)# domain name str customer_6
```
Sets the initial state of the domain level and the MEPs as up MEPs, switches to configuration Ethernet CFM mode, and sets the domain name.

2.
```
(config-ether-cfm)# ma 1 name str ma1_vlan100
(config-ether-cfm)# ma 1 vlan-group 10,20,100 primary-vlan 100
(config-ether-cfm)# ma 2 name str ma2_vlan200
(config-ether-cfm)# ma 2 vlan-group 30,40,200 primary-vlan 200
(config-ether-cfm)# exit
```
Sets the MA identification number, the MA name, the VLANs belonging to the MA, and the primary VLAN.

(2) Configuring MEPs and MIPs

Points to note

MEPs must be set for each MA. An MIP is shared by the MAs, and one MEP is set for each port. For the basics of setting MEPs and MIPs, see *20.2.2*

Configuring CFM (multiple domains).

Command examples

1. `(config)# interface fastethernet 0/1`

   `(config-if)# ethernet cfm mep level 6 ma 1 mep-id 101`

   `(config-if)# ethernet cfm mep level 6 ma 2 mep-id 201`

   `(config-if)# exit`

   `(config)# interface range fastethernet 0/2-4`

   `(config-if-range)# ethernet cfm mip level 6`

   `(config-if-range)# exit`

   Sets MEPs belonging to domain level 6 and MA1 for port 0/1. Also, sets a MEP belonging to MA2. Sets MIPs of domain level 6 to port 0/2 to 0/4.

2. `(config)# ethernet cfm enable`

   Initiates operation of the CFM functionality on the Switch.

20.3 Operation

20.3.1 List of operation commands

The following table describes the list of operation commands for CFM.

Table 20-15 List of operation commands

Command name	Description
`l2ping`	Executes the CFM loopback functionality and verifies the connectivity between the specified MPs.
`l2traceroute`	Executes the CFM linktrace functionality and verifies the routing between the specified MPs.
`show cfm`	Displays information about a CFM domain.
`show cfm remote-mep`	Displays information about a CFM remote MEP.
`show cfm fault`	Displays CFM failure information.
`show cfm l2traceroute-db`	Displays route information obtained by using the `l2traceroute` operation command.
`show cfm statistics`	Displays CFM statistics.
`clear cfm remote-mep`	Clears remote information about a CFM MEP.
`clear cfm fault`	Clears CFM failure information.
`clear cfm l2traceroute-db`	Clears route information obtained by using the `l2traceroute` operation command.
`clear cfm statistics`	Clears CFM statistics.

20.3.2 Verifying connectivity between MPs

You can use the `l2ping` operation command to verify the connectivity between the specified MPs and to display the results. For the command, you can specify the number of verifications and the time to wait for a response. By default, the number of verifications is set to five, and the time to wait for a response is set to five seconds. When a verification result is returned or the time to wait for a response has elapsed, another verification attempt is started.

Figure 20-30 Results of executing the l2ping command

```
> l2ping remote-mep 1010 domain-level 7 ma 1000 mep 1020 count 3
L2ping to MP:1010(0012.e254.dc01) on Level:7  MA:1000  MEP:1020  VLAN:20
Time:2009/10/28 06:59:50
1: L2ping Reply from 0012.e254.dc01  64bytes  Time=   20 ms
2: L2ping Reply from 0012.e254.dc01  64bytes  Time=   10 ms
3: L2ping Reply from 0012.e254.dc01  64bytes  Time=   10 ms

--- L2ping Statistics ---
```

```
  Tx L2ping Request :   3  Rx L2ping Reply :   3  Lost Frame  :   0%
  Round-trip Min/Avg/Max : 10/13/20 ms
>
```

20.3.3 Verifying the route between MPs

You can use the `l2traceroute` operation command to obtain route information about the route between the specified MPs and to display the results. You can specify the time to wait for a response and a TTL value for the command. By default, the time to wait for a response is set to five seconds, and the TTL value is set to 64.

The word `Hit` confirms that a response from the MP specified as the destination was received.

Figure 20-31 Results of executing the l2traceroute command

```
> l2traceroute remote-mep 1010 domain-level 7 ma 1000 mep 1020 ttl 64
L2traceroute to MP:1010(0012.e254.dc01) on Level:7  MA:1000  MEP:1020  VLAN:20
Time:2009/10/28 08:27:44
 63  00ed.f205.0115  Forwarded
 62  0012.e2a8.f8d0  Forwarded
 61  0012.e254.dc01  NotForwarded  Hit
>
```

20.3.4 Checking the status of MPs on a route

You can use the `show cfm l2traceroute-db detail` operation command to check detailed information about the route to the destination MP and the MPs on the route. If the `NotForwarded` message is displayed, you can check the reason that the linktrace message was not forwarded in the `Action` section on the `Ingress Port` and the `Egress Port` lines.

Figure 20-32 Results of executing the show cfm l2traceroute-db detail command

```
> show cfm l2traceroute-db detail

Date 29.10.09 08:45:32 AM UTC
L2traceroute to MP:302(0012.e254.dc09) on Level:3  MA:300   MEP:300  VLAN:300
Time:2009/10/29 08:35:02
63   00ed.f205.0111  Forwarded
  Last Egress : 00ed.f205.0001  Next Egress : 00ed.f205.0001
  Relay Action: MacAdrTbl
  Chassis ID    Type: MAC      Info: 00ed.f205.0001
  Ingress Port  Type: LOCAL     Info: Port 0/1
    MP Address: 00ed.f205.0101  Action: OK
  Egress Port   Type: LOCAL     Info: Port 0/17
    MP Address: 00ed.f205.0111  Action: OK
62   0012.e254.dc09  NotForwarded  Hit
  Last Egress : 00ed.f205.0001  Next Egress : 0012.e254.dbf0
  Relay Action: RlyHit
  Chassis ID    Type: MAC      Info: 0012.e254.dbf0
  Ingress Port  Type: LOCAL     Info: Port 0/17
    MP Address: 0012.e254.dc01  Action: OK
  Egress Port   Type: LOCAL     Info: Port 0/25
    MP Address: 0012.e254.dc09  Action: OK
>
```

20.3.5 Checking the CFM status

You can use the `show cfm` operation command to display the CFM settings and the status of detected failures. If the CC functionality has detected failures, in the `Status` section, you can check the type of the failure that has the highest failure level of all the detected failures.

Figure 20-33 Results of executing the show cfm command

```
> show cfm

Date 28.10.09 09:31:33 AM UTC
Domain Level 3 Name(str): ProviderDomain_3
  MA 300   Name(str) : Tokyo_to_Osaka
    Primary VLAN:300   VLAN:10-20,300
    CC:Enable   Interval:1min
    Alarm Priority:2  Start Time: 2500ms  Reset Time:10000ms
    MEP Information
      ID:8012  UpMEP    CH1 (Up)    Enable   MAC:00ed.f205.0101  Status:-
  MA 400   Name(str) : Tokyo_to_Nagoya
    Primary VLAN:400   VLAN:30-40,400
    CC:Enable   Interval:10min
    Alarm Priority:0  Start Time: 7500ms  Reset Time: 5000ms
    MEP Information
      ID:8014  DownMEP  0/21(Up)    Disable  MAC:00ed.f205.0115  Status:-
  MIP Information
      0/12(Up)    Enable   MAC:00ed.f205.010c
      0/22(Down)  Enable   MAC:-
Domain Level 4 Name(str): ProviderDomain_4
  MIP Information
      CH8 (Up)    Enable   MAC:00ed.f205.0108
>
```

20.3.6 Checking detailed information of failures

You can use the `show cfm fault detail` operation command to display the status of failure detection and the CCM information. This information is an aid for detecting failures of each failure type. The remote MEP that sent the CCM can be checked in the `RMEP`, `MAC`, and `VLAN` sections.

Figure 20-34 Results of executing the show cfm fault detail command

```
> show cfm fault domain-level 7 detail

Date 2009/10/29 07:28:32 UTC
MD:7  MA:1000  MEP:1000  Fault
  OtherCCM : -  RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:2009/10/29 07:18:44
  ErrorCCM : On RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:2009/10/29 07:27:45
  Timeout  : On RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:2009/10/29 07:27:20
  PortState: -
  RDI      : -  RMEP:1001 MAC:0012.e254.dbff VLAN:1000 Time:2009/10/29 07:23:45

>
```

21. Using SNMP to Manage Networks

This chapter describes the SNMP agent functionality, with a focus on supported specifications.

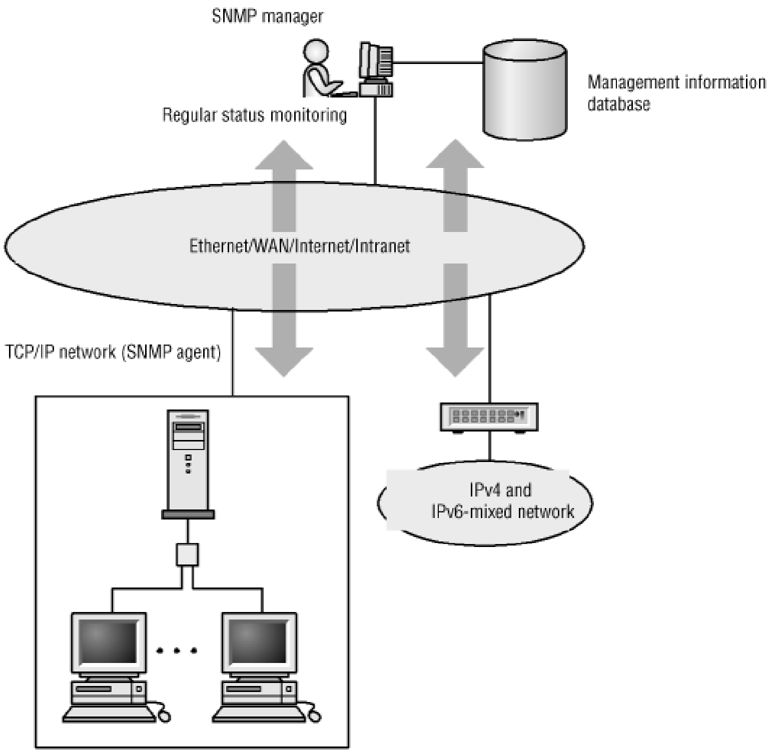
21.1 Description

21.1.1 SNMP overview

(1) Network management

Maintaining the operating environment and performance of a network system requires high-level network management. The *Simple Network Management Protocol (SNMP)* is an industry-standard network management protocol with which you can manage a multi-vendor network consisting of network devices that support SNMP. A server that manages a network by collecting management information is called an *SNMP manager*, and a network device that is managed is called an *SNMP agent*. The following figure provides an overview of network management.

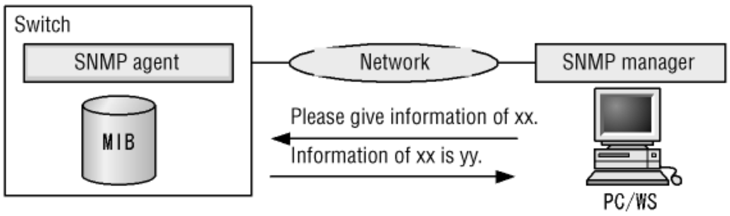
Figure 21-1 Overview of network management



(2) SNMP agent functionality

SNMP agent for the Switch is a program included on a switch on a network. An SNMP agent has functionality that provides the SNMP manager with information internal to the switch. This information is called the management information base (MIB). SNMP manager is software that retrieves the information on a switch, edits and processes it, and provides it to the network administrator for management of the network. The following figure shows an example of MIB retrieval.

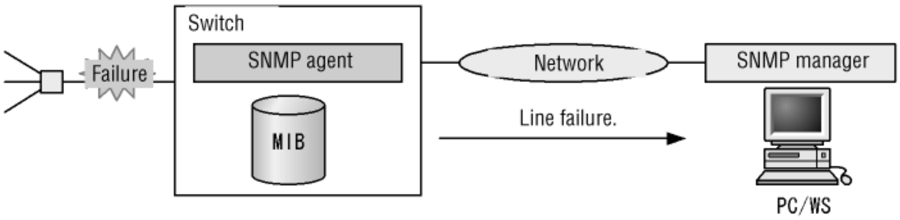
Figure 21-2 Example of MIB retrieval



This Switch supports SNMPv1 (RFC 1157) and SNMPv2C (RFC 1901). When managing the network with an SNMP manager, use the SNMPv1 and SNMPv2C protocols. Note that SNMPv1 and SNMPv2C can be used simultaneously.

In addition, an SNMP agent has a functionality called a *trap* for reporting events (mainly failure information). The SNMP manager can learn about changes by receiving traps without regularly monitoring changes to the switch status. Note, however, that the SNMP manager cannot verify whether a trap has arrived from a switch because traps use UDP. Accordingly, some traps might not arrive at the SNMP manager due to network congestion. The following figure shows an example of a trap.

Figure 21-3 Example of a trap



21.1.2 MIB overview

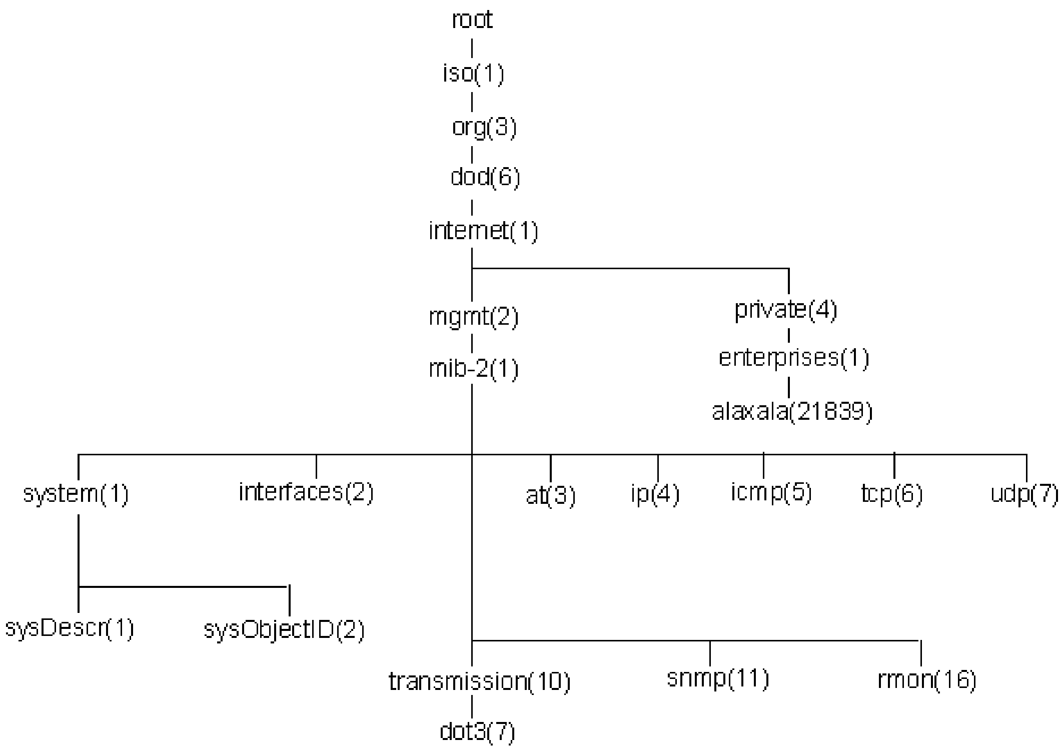
A switch manages and provides SNMP managers with the following two types of MIBs: One is defined in an RFC, and the other is information prepared by the vendor who developed the switch.

A MIB defined in an RFC is called a *standard MIB*. Because standard MIBs are standardized, there are no differences in the information provided. A MIB provided independently by a switch vendor is called a *private MIB*, and its contents vary depending on the switch. Note, however, that MIB operations, including the retrieval and specification of information, are common to both standard and private MIBs. An operation consists of specifying a switch and the target MIB information. Specify the switch by using an IP address and specify the MIB information by using an object ID.

(1) Structure of a MIB

Because a MIB has a tree structure, each node is identified by a number. Each item of MIB information is uniquely identified by assigning a sequential number to each node starting from the root. This sequential number is called the *object ID* and is assigned by adding, from the root, lower-level object group numbers by using dot notation. For example, the `sysDescr` MIB in the figure below is expressed by its object ID 1.3.6.1.2.1.1.1. The following figure shows an example of a MIB tree structure.

Figure 21-4 MIB tree structure



(2) Expressing MIB objects

An object ID consists of numbers in dot notation (for example, 1.3.6.1.2.1.1.1). Because a number-only ID is not easy to understand, some managers use mnemonics such as `sysDescr` for specification. If you specify a MIB by using a mnemonic, you must ascertain beforehand the MIB mnemonics the SNMP manager can use.

(3) Index

When an object ID is used to specify a MIB, some MIBs have one meaning and some MIBs have multiple sets of information. An index is used to identify each MIB. The index is expressed by adding a number to the end of the object ID, which corresponds to some information.

When a MIB has only one meaning, add ".0" to the object ID of the MIB. If a MIB contains multiple information items, add a number to the end of the object ID to indicate the order of information. For example, specify `ifType` (1.3.6.1.2.1.2.2.1.2) for a MIB indicating an interface type. This switch has multiple interfaces. To check a specific interface type, you must specify the type specifically as "type of the second interface". When specifying the type by using a MIB, add the index `.2` to the end of the MIB to indicate the second item as shown in `ifType.2` (1.3.6.1.2.1.2.2.1.2.2).

How an index is expressed depends on the MIB. A MIB entry expressed as `INDEX {`*`xxxxx`*`,`*`yyyyy`*`,`*`zzzzzz`*`}` in the MIB definition section of the RFC has *xxxxx* and *yyyyy* and *zzzzzz* as indexes. Check the index for each MIB before performing MIB operations.

(4) MIBs supported by the Switch

This Switch provides the MIBs necessary for managing networks, such as those for device statuses, interface statistics, and device information about the Switch. Note that the definition file of private MIBs (ASN.1) is provided with the software.

For details about MIBs, see the *MIB Reference*.

21.1.3 SNMPv1 and SNMPv2C operations

For the collection or setting of management data, SNMP provides the following four operations:

- `GetRequest`: Extracts information of the specified MIB.
- `GetNextRequest`: Extracts information of the MIB next to the specified MIB.
- `GetBulkRequest`: Extended version of `GetNextRequest`.
- `SetRequest`: Sets a value for the specified MIB.

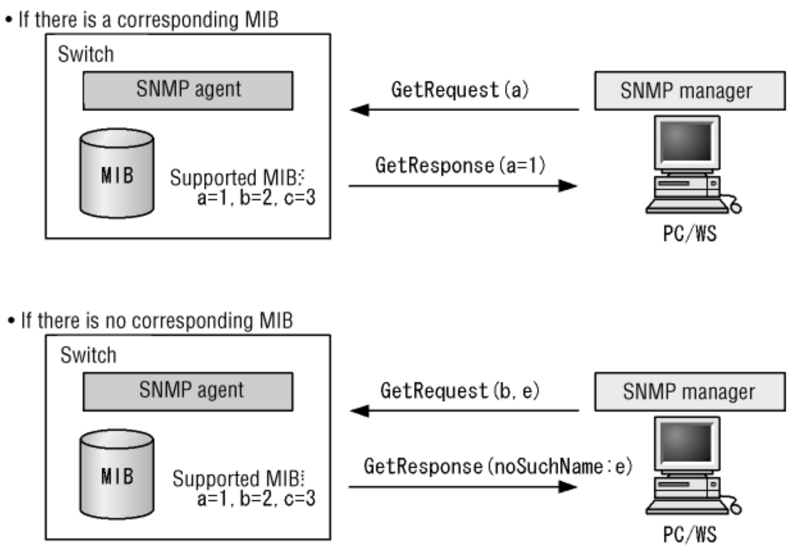
The above operations are performed for a switch (SNMP agent) from the SNMP manager. Each operation is described below.

(1) GetRequest operation

The `GetRequest` operation is used when an SNMP manager extracts MIB information from a switch (agent functionality). One or more MIBs can be specified for this operation.

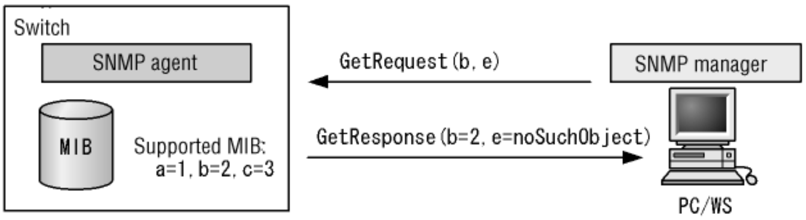
If the switch holds the applicable MIB, the `GetResponse` operation returns the MIB information. If the switch does not hold the applicable MIB, the `GetResponse` operation returns `noSuchName`. The following figure illustrates the `GetRequest` operation.

Figure 21-5 GetRequest operation



In SNMPv2C, if the switch does not hold the applicable MIB, the `GetResponse` operation returns `noSuchObject` as the MIB value. The following figure illustrates the `GetRequest` operation for SNMPv2C.

Figure 21-6 GetRequest operation for SNMPv2C

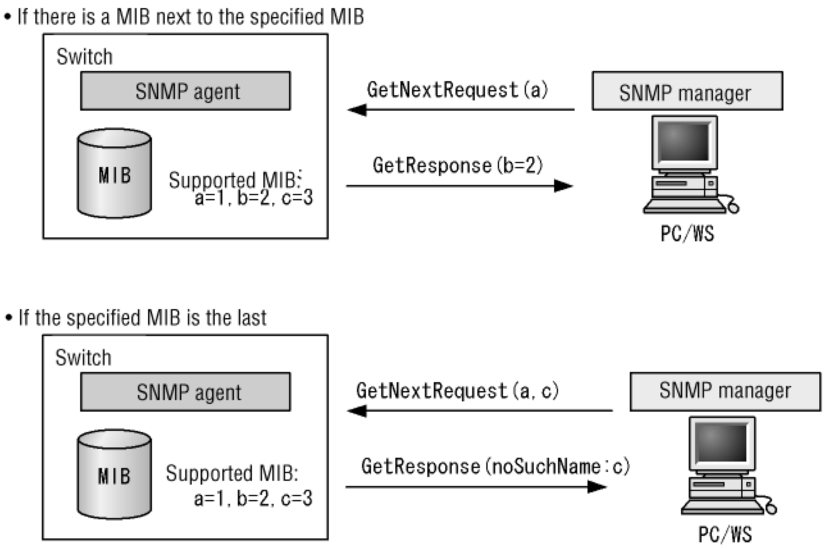


(2) GetNextRequest operation

The `GetNextRequest` operation is similar to the `GetRequest` operation. Whereas the `GetRequest` operation is used for reading the specified MIB, the `GetNextRequest` operation is used to extract the MIB after the specified MIB. One or more MIBs can be specified for this operation.

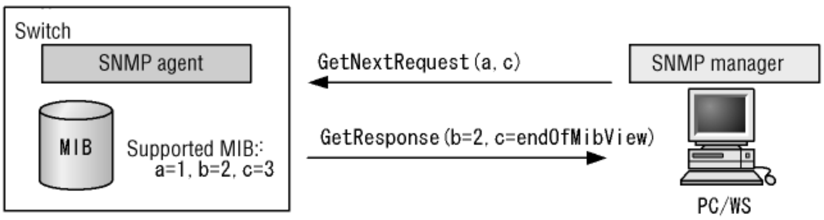
If the switch holds the MIB following the specified one, the `GetResponse` operation returns the MIB. If the specified MIB is the last MIB, the `GetResponse` operation returns `noSuchName`. The following figure illustrates the `GetNextRequest` operation.

Figure 21-7 GetNextRequest operation



In SNMPv2C, if the specified MIB is the last MIB, the `GetResponse` operation returns `endOfMibView` as the MIB value. The following figure illustrates the `GetNextRequest` operation for SNMPv2C.

Figure 21-8 GetNextRequest operation for SNMPv2C



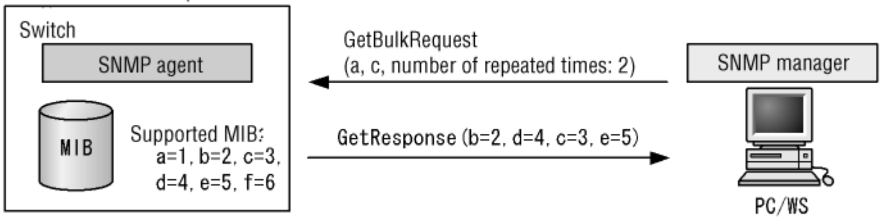
(3) GetBulkRequest operation

The `GetBulkRequest` operation is an extended `GetNextRequest` operation. By using the `GetNextRequest` operation, you can set a number of repetitions. You can extract from the items next to the specified MIB as many MIBs as the specified number of repetitions. One or more MIBs can be specified for this operation.

If a switch has many MIBs as the specified number of repetitions from the item next to the specified MIB, the `GetResponse` operation returns the MIB. If the specified MIB is the last MIB, or the last MIB is retrieved before the specified number of repetitions, the `GetResponse` operation returns `endOfMibView` as the MIB value. The following figure illustrates the `GetBulkRequest` operation.

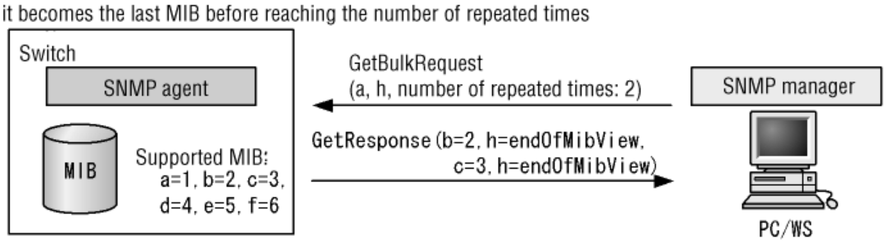
Figure 21-9 GetBulkRequest operation

• If there is the next MIB specified



In the above figure, MIBs `a` and `c` are specified with 2 as the number of repetitions. As a result, MIBs `b` (the next MIB after MIB `a`) and `d` (the next MIB after MIB `c`), and then MIBs `c` (the next MIB after MIB `b`) and `e` (the next MIB after MIB `d`) can be retrieved.

• If it becomes the last MIB before reaching the number of repeated times



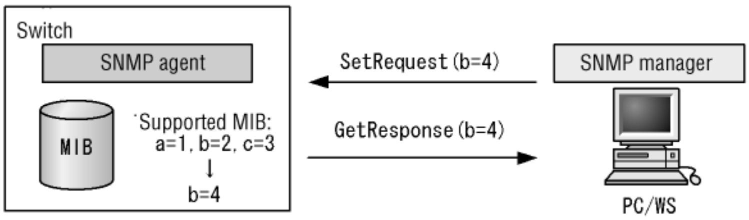
In the above figure, MIBs `a` and `h` are specified with 2 as the number of repetitions. Because `h` is the last MIB, the `GetBulkRequest` operation will return `endOfMibView`.

(4) SetRequest operation

The `SetRequest` operation is similar to the `GetRequest`, `GetNextRequest`, and `GetBulkRequest` operations because it is performed for a switch (agent functionality) from the SNMP manager, but the method for setting a value for the `SetRequest` operation is different from that of the other operations.

The `SetRequest` operation specifies both a value to be set and a MIB. When a value is specified, the `GetResponse` operation returns the MIB and the setting value. The following figure illustrates the `SetRequest` operation.

Figure 21-10 SetRequest operation



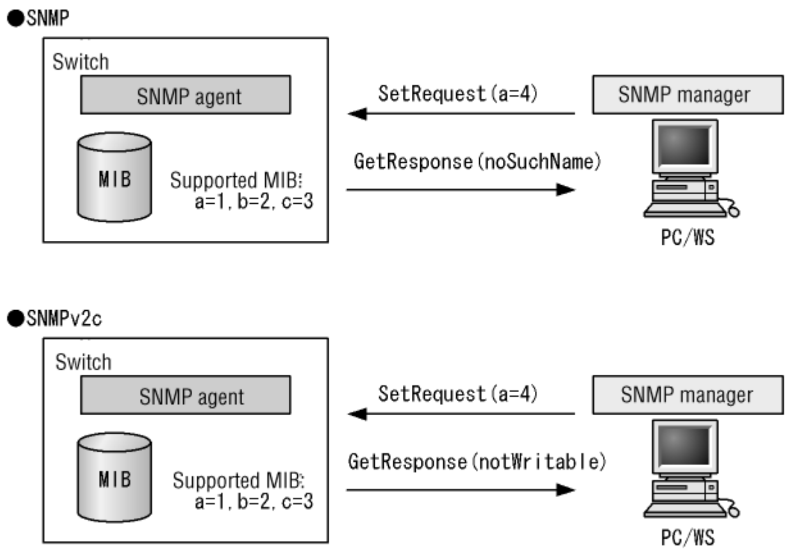
(a) Response when a MIB cannot be configured

The following are three cases when a MIB cannot be configured:

- The MIB is read-only (includes managers that belong to read-only communities).
- The setting value is not correct.
- Configuration cannot be performed because of the status of the switch.

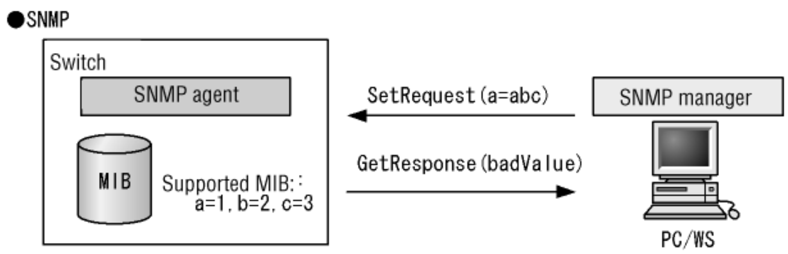
Each case returns a different response. If the MIB is read-only, `noSuchName` is returned by the `GetResponse` operation. In SNMPv2C, if the MIB is read-only, the `GetResponse` operation returns `notWritable`. The following figure illustrates the `SetRequest` operation when the MIB is read-only.

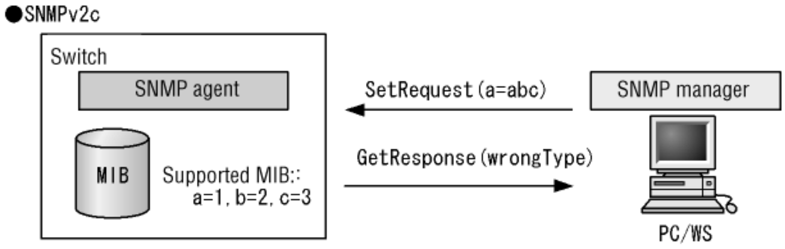
Figure 21-11 SetRequest operation when the MIB variable is read-only



If the type of the setting value is not correct, the `GetResponse` operation returns `badValue`. In SNMPv2C, if the type of the setting value is not correct, the `GetResponse` operation returns `wrongType`. The following figure illustrates the `SetRequest` operation when the type of the setting value is not correct.

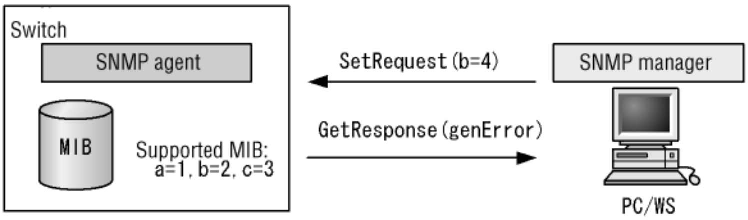
Figure 21-12 Example of the SetRequest operation when the setting value type is not correct





If settings are not possible because of the status of the switch, `genError` is returned. For example, when an attempt is made to set a value on a switch, if a setting timeout is detected on the switch, `genError` is returned. The following figure illustrates the `SetRequest` operation when settings are not possible because of the status of the switch.

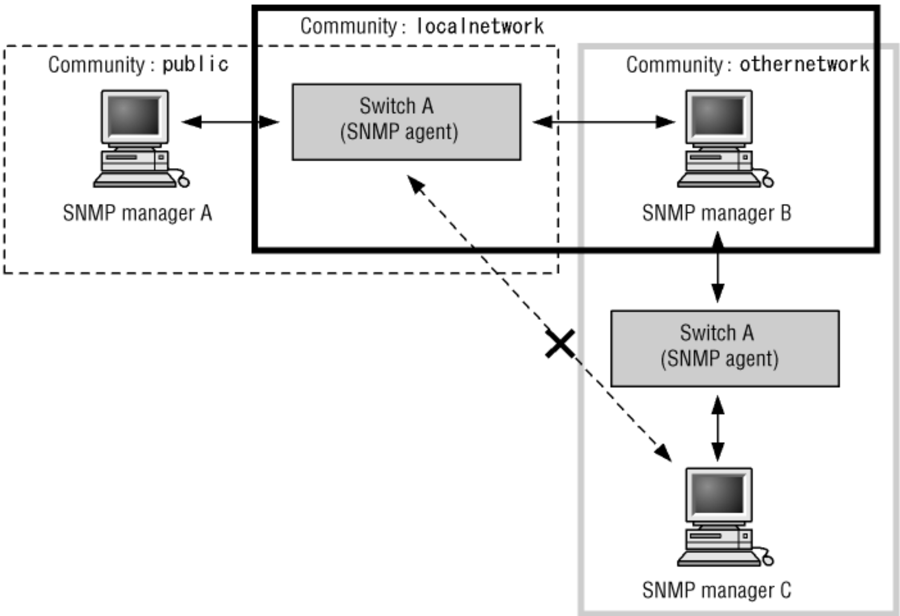
Figure 21-13 SetRequest operation when settings are not possible because of the status of the switch



(5) Operational restrictions applying to communities

In SNMPv1 and SNMPv2C, restrictions can be applied to SNMP managers that perform operations under the community concept. A *community* is the allocation of an SNMP manager that performs operations and an SNMP agent to a group. To perform MIB operations, the SNMP manager and the SNMP agent must belong to the same group (community). The following figure illustrates the operation of a community.

Figure 21-14 Operation of a community



Switch A belongs to the `public` community and the `localnetwork` community, but it does not belong to the `othernetwork` community. In this case, switch A accepts MIB operations requested by SNMP manager A in the `public` community and SNMP manager B in the `localnetwork` community, but it does not accept operations requested by SNMP manager C in the `othernetwork` community.

(6) Operational restrictions applying to IP addresses

In consideration of security risks, the Switch can be configured so that they do not accept MIB operations if the combination of community and IP address of the SNMP manager does not match an access list. To use SNMPv1 and SNMPv2C on the Switch, you must register communities by using a configuration command. A community is specified by using a character string. In addition, `public` is generally used for a community name.

(7) Error status codes for SNMP operations

If an error occurs during an operation, the SNMP agent assigns an error code for the error status and returns a response in the `GetResponse` operation. The response contains the number of the MIB information where the error occurred set as the error location number. If the result of the operation is normal, a code indicating no errors is set as the error status and a response in the `GetResponse` operation that contains the MIB information of the operations actually performed is returned. The following table describes the error status codes.

Table 21-1 SNMPv1 error status codes

Error status	Code	Occurrence condition
`noError`	0	Normal
`tooBig`	1	The length of the response message exceeded 2048 bytes.
`noSuchName`	2	● The object specified by the `Get` or `Set` operation does not exist. ● The object specified by the `Set` operation is implemented as `read-only`. ● The community for the `Set` operation is defined as `ro`. ● The `GetNext` operation reached the end. (`snmpwalk` ended.)
`badValue`	3	An invalid value was specified for the `Set` operation (including an invalid type).
`readOnly`	4	Not used.
`genError`	5	The number of entries for the `Set` operation, such as RMON, exceeded the maximum. (This includes cases where resources are insufficient.)

If the community name is not set, no response is returned. (No error codes are returned.)

Table 21-2 SNMPv2C error status codes

Error status	Code	Occurrence condition
noError	0	Normal
tooBig	1	The length of the response message exceeded 2048 bytes.
noSuchName	2	Not used.
badValue	3	Not used.
readOnly	4	Not used.
genError	5	An error for which no other error status is applicable.
noAccess	6	The community for the Set operation is defined as ro.
wrongType	7	An invalid value was specified for the Set operation. (The type does not match.)
wrongLength	8	An invalid value was specified for the Set operation. (The character string length is out of range.)
wrongEncoding	9	The encoding for the value specified for the Set operation is invalid. (This code is not used on the Switch.)
wrongValue	10	An invalid value was specified for the Set operation.
noCreation	11	• The ifTable column (ifIndex) specified for the Set operation does not exist. • The column number of the table type object specified for the Set operation is out of range.
inconsistentValue	12	The value specified for the Set operation cannot be set because the procedure for accessing the entry is not correct.
resourceUnavailable	13	The number of entries for the Set operation, such as RMON, exceeded the maximum. (This includes the case where resources are insufficient.)
commitFailed	14	Configuration processing failed. (This code is not used on the Switch.)
undoFailed	15	Undo processing failed. (This code is not used on the Switch.)
authorizationError	16	Not used
notWritable	17	• The object specified by the Set operation is not implemented. • The object specified by the Set operation is implemented as read-only.
inconsistentName	18	The column for the table type object specified for the Set operation cannot be created because the procedure for accessing the entry is not correct.

If the community name is not set, no response is returned. (No error codes are returned.)

Table 21-3 SNMPv2C status codes for each object

Status	Code	Occurrence condition
`noSuchObject`	[0]	The object specified by the `Get` operation does not exist.
`noSuchInstance`	[1]	The column for the table type object specified for the `Get` operation does not exist.
`endOfMibView`	[2]	The `GetNext` operation reached the end. (`snmpwalk` ended.)

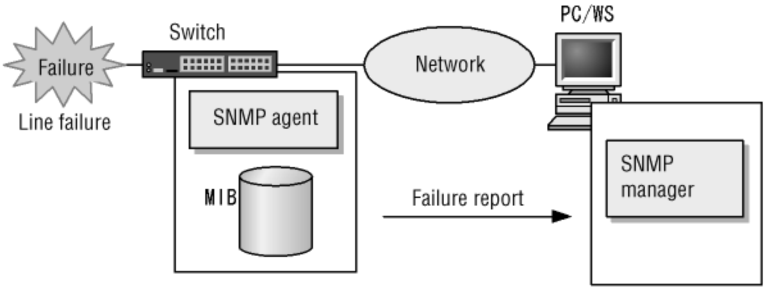
21.1.4 Traps

(1) Overview of traps

SNMP agents have a function called a *trap* for event notification (mainly information about failures or log information). Traps are used to report important events asynchronously to an SNMP manager from an SNMP agent. The SNMP manager can regularly detect changes to the switch status by receiving traps. Based on such notification, the SNMP manager can extract the MIBs on switches to obtain more detailed information.

Note, however, that the SNMP manager cannot verify whether a trap has arrived from a switch because traps use UDP. Accordingly, some traps might not arrive at the SNMP manager due to network congestion. The following figure shows an example of a trap.

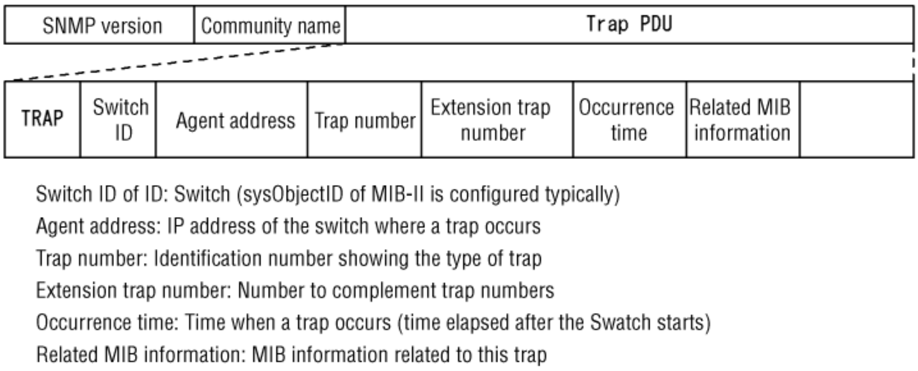
Figure 21-15 Example of a trap



(2) Trap format

A trap frame contains the IP address of a switch, and information about what has occurred in the switch and when it occurred. The following figure shows the trap format.

Figure 21-16 Trap format



21.1.5 RMON MIB

RMON (Remote Network Monitoring) functionality includes the provision of Ethernet statistics, generation of an event from the checking of threshold values in the collected statistics, and the capture of packets. RMON is defined in RFC 1757.

This section provides an overview for the statistics, history, alarm, and event groups of the RMON MIBs.

(1) Statistics group

The statistics group collects basic statistics about monitored subnetworks. For example, it collects the total number of packets in a subnetwork, the number of packets for each packet type such as broadcast packets, and the number of errors, which includes CRC errors and collision errors. The statistics group provides statistics about subnetwork traffic conditions and line status.

(2) History group

The history group samples statistics that are almost the same as the information collected by the statistics group, and retains the sampled information as history information.

A history group has a control table named `historyControlTable` and a data table named `etherHistoryTable`. `historyControlTable` is a MIB used to set the sampling interval and the number of history records.

`etherHistoryTable` is a MIB of history information about the sampled statistics. The history group retains statistics on the switch for a certain period of time. Compared to regular polling by an SNMP manager to collect statistics, network load is lower and continuous statistical information for a certain period can be obtained.

(3) Alarm group

The alarm group is a MIB that configures the interval for checking monitored MIBs and the threshold values for logging when the MIB reaches the threshold value and for issuing a trap to an SNMP manager.

For example, the alarm group can log information or issue a trap to the SNMP manager if it detects that no packets can be received successively ten times or more within a five-minute period set as a sampling period. When you use the alarm group, you must configure the event group.

(4) Event group

The event group consists of the `eventTable` group MIB, which specifies the behavior when a MIB threshold value set in the alarm group is exceeded, and the `logTable` group MIB, which logs information when a threshold value is exceeded.

The `eventTable` group MIB is used to set, when a threshold value is reached, whether information is to be logged or a trap is to be issued to an SNMP manager, or whether both actions or neither action is required.

The `logTable` group MIB logs information on the switch when logging is specified by the eventTable group MIB. Because the number of log entries on a switch is fixed, if the limit is exceeded, new information replaces old information in the log. Note that if you do not save log information regularly to the SNMP manager, some logged information might be lost.

21.1.6 Notes on connecting to an SNMP manager

(1) Tuning the cycle for collecting MIB information

To detect a new device on a network or to monitor traffic conditions, an SNMP manager extracts MIBs regularly from devices supported by the SNMP agent. If the interval for extracting MIBs is too short, the load on the network device or network itself increases. In addition, depending on the switch status or the configuration, a timeout might occur on the SNMP manager when it extracts a MIB. In particular, the possibility of a response timeout is high in the following cases:

- When too many SNMP managers are connected

  When many SNMP managers are connected to a Switch and the operations for collecting MIB information result in congestion

- When many SNMP events occur simultaneously

  In this case, because a large number of traps are issued from a Switch, a response might time out if MIBs are extracted or MIBs are extracted in parallel according to the trap issued from a Switch.

If responses time out often, adjust the polling cycle or the value of the response monitoring timer for the SNMP manager. The following are the major SMNP manager tuning parameters:

- Polling interval
- Response monitoring timer
- Number of retries when a response monitoring timeout occurs

21.2 Configuration

21.2.1 List of configuration commands

The following table describes the commands used to configure SNMP/RMON.

Table 21-4 List of configuration commands

Command name	Description
`hostname`	Sets the host name of a Switch. This setting is equivalent to `sysName` defined in RFC 1213.
`rmon alarm`	Sets the control information of the RMON (RFC 1757) alarm group.
`rmon collection history`	Sets the control information for the statistical history for RMON (RFC 1757) Ethernet.
`rmon event`	Sets the control information for an RMON (RFC 1757) event group.
`snmp-server community`	Sets the access list for the SNMP community.
`snmp-server contact`	Sets the contact information of the Switch. This setting is equivalent to `sysContact` defined in RFC 1213.
`snmp-server host`	Registers the network management switch (SNMP manager) to which traps are sent.
`snmp-server location`	Sets the name of the location where the Switch is installed. This setting is equivalent to `sysLocation` defined in RFC 1213.
`snmp-server traps`	Sets the timing for issuing a trap.
`snmp trap link-status`	If a link-up failure or link-down failure occurs on a line when `no snmp trap link-status` is set, this command suppresses the sending of traps (SNMP link-down and link-up traps).

21.2.2 Configuring MIB access permissions in SNMPv1 and SNMPv2C

Points to note

Configures access to the MIB of the Switch from the SNMP manager.

When allowing only a specific SNMP manager to access the Switch, it is necessary to register the IP address of the terminal in advance to give access permission by means of the configuration command `ip access-list standard`. In addition, note that one access list can be specified for one community.

Command examples

1.
```
(config)# ip access-list standard SNMPMNG
(config-std-nacl)# permit host 128.1.1.2
(config-std-nacl)# exit
```

Configures the access list to allow access from IP address 128.1.1.2.

2. `(config)# snmp-server community "NETWORK" ro SNMPMNG`

   Configures the MIB access mode for the community of an SNMP manager and the applicable access list.

   - Community name: `NETWORK`
   - Access list: `SNMPMNG`
   - Access mode: `read only`

Notes

- An access list for use by the Switch does not depend on the settings of the flow detection mode.
- An IP address meeting a permit condition is subject to access permission.

  An IP address meeting a deny condition is subject to access rejection.

  An implicit deny condition for all IP addresses is set at the end of the IP access list.

  In this example of the setting, the permit condition is defined in one line. When this permit condition is not met, access is rejected because it is assumed that the implicit deny condition has been met.

21.2.3 Configuring the sending of traps in SNMPv1 and SNMPv2C

Points to note

Registers the SNMP manager that issues a trap.

Command examples

1. `(config)# snmp-server host 128.1.1.2 traps "NETWORK" version 1 snmp`

   Configures an SNMP manager to issue standard traps.

   - Community name: `NETWORK`
   - IP address of the SNMP manager: 128.1.1.2
   - Traps to be issued: standard traps

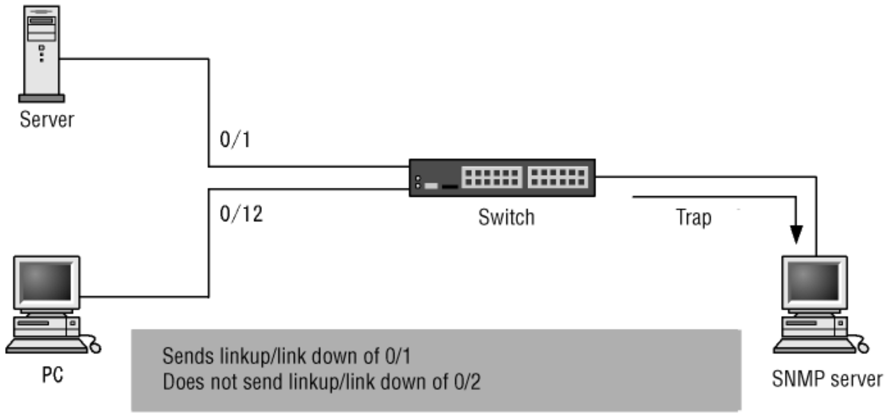
21.2.4 Suppressing link traps

The Switch issues an SNMP trap by default when a link-up or a link-down occurs on an Ethernet interface. You can suppress the sending of link traps for each Ethernet interface by specifying suppression through the configuration. For example, by sending traps only about important lines such as a line connecting to a server, and suppressing link traps about another line, you can eliminate unnecessary processing by Switches, networks, and SNMP managers.

Points to note

Determine the link trap configuration based on the operation policies of the entire network.

Figure 21-17 Link trap configuration



As seen from the above figure, no configuration is required for port 0/1 because traps are sent. In contrast, port 0/12 need be configured so that no traps are sent.

Command examples

1. `(config)# interface fastethernet 0/12`

   `(config-if)# no snmp trap link-status`

   `(config-if)# exit`

   Configures the Switch so that traps are sent when a link-up or link-down occurs.

21.2.5 Configuring control information for the RMON Ethernet history group

Points to note

Configures the control information for the RMON (RFC 1757) Ethernet statistics history. The command can configure up to 32 entries. You must register an SNMP manager beforehand.

Command examples

1. `(config)# interface fastethernet 0/5`

   Moves to the interface mode for port 0/5.

2. `(config-if)# rmon collection history controlEntry 33 owner "NET-MANAGER" buckets 10`

   `(config-if)# exit`

   Sets the information identification number of the control information for statistics history information, the identification information of the person responsible for configuration, and the number of history entries for storing statistical information.

   - Information identification number: 33
   - Number of entries obtained for history information: 10
   - Identification information about the person responsible for the configuration: `NET-MANAGER`

21.2.6 Threshold check for specific MIB values by RMON

Points to note

Configures a switch to be used to regularly check the threshold value for a specific MIB value, and to notify the SNMP manager of an event if the threshold value is exceeded.

If you specify trap as an event execution method, you must configure the SNMP trap mode beforehand.

Command examples

1. `(config)# rmon event 3 log trap public`

   Configures an event to be executed when an alarm is generated.

   - Information identification number: 3
   - Event execution method: `log` or `trap`
   - Trap-sending community name: `public`

2. `(config)# rmon alarm 12 "ifOutDiscards.13"  256111 delta rising-threshold 400000 rising-event-index 3 falling-threshold 100  falling-event-index 3 owner "NET-MANAGER"`

   Configures control information for the RMON alarm group according to the following conditions:

   - Control information identification number for the RMON alarm group: 12
   - Object identifier for the MIB used for checking the threshold: ifOutDiscards.13
   - Time interval for checking the threshold: 256111 seconds
   - Method for checking the threshold: difference value check (delta)
   - Upper threshold value: 400000
   - Identification number of the method for generating an event if the upper threshold is exceeded: 3
   - Lower threshold value: 100
   - Identification number of the method for generating an event if the lower threshold is exceeded: 3

   Identification information for the person responsible for configuration: `NET-MANAGER`

21.2.7 Verifying communication with SNMP managers

When you manage networks using the SNMP protocol by configuring the SNMP agent functionality on the Switch, verify the following:

- The Switch can retrieve MIBs from an SNMP manager on a network.
- An SNMP trap is sent from the Switch to an SNMP manager on a network.

To carry out the check, do the following. For details about the MIBs that can be obtained from the Switch, see *1. Overview of Supported MIBs* in the manual *MIB Reference*. For details about traps that are sent from the Switch, see *4.2 Supported Trap-PDU parameters* in the manual *MIB Reference*.

1. Execute the operation command `ping` by specifying the IP address of the SNMP manager to confirm that IP communication with the SNMP manager

can be made from the Switch. If communication has not been established, see the *Troubleshooting Guide*.

2. Make sure that the Switch can retrieve MIBs from an SNMP manager. If the MIB cannot be retrieved, see the *Troubleshooting Guide*.

22. Log Data Output Functionality

This chapter describes the log output functionality for the Switch.

22.1 Description

This Switch logs information on operation and failures into an operation log. The operation log is stored on the Switch, and use of the information allows management of the operation status of the device, and the monitoring of failures.

The operation log records the events that occur during operation of the device in the order they occurred. The following information is saved as an operation log:

- User command operations and response messages
- Operation information output by the switch
- Device failure logs

This data is logged in text format inside the switch. To view the entries, use the `show logging` operation command. In addition, device failure logs can be checked via the operation command `show critical-logging`.

Log information collected on a Switch can be sent[#1] to other devices (such as UNIX workstations) with the syslog functionality on the network by using the syslog interface[#2].

#1

Functionality to receive syslog messages from other devices is not supported.

#2

For syslog messages generated by this Switch, the `HOSTNAME` and `TIMESTAMP` columns in HEADER defined by RFC 3164 are not set. To add `HOSTNAME` and `TIMESTAMP`, use the configuration command `logging syslog-header`. The following diagram shows the syslog server output format when this command is set.

Figure 22-1 Format of output to the syslog server

```
Fac Mon Date Time hostname [number]:AUT Mon/Date/Time Web log message body
|(1)|---(2) ---|--(3)---|--(4)-|(5)|----(6)---|(7)|------------(8)-------------|
```

(1) Facility
(2) Date and time output in TIMESTAMP: syslog
(3) Identification name of HOSTNAME: Switch
(4) Function number
(5) Log type representing authentication function
(6) Event occurrence time
(7) Authentication function type representing Web authentication
(8) Message body

By setting the configuration command `logging syslog-header`, (2) to (4) are added. In addition, when the `hostname` configuration command is set, the character string shown in the following table is added to the (3) `HOSTNAME` column.

Table 22-1 HOSTNAME column when the hostname configuration command is set

Model	Whether the hostname configuration command is set		Remarks
	No	Yes	
AX2200S	"AX2200S"	Setting character string	If the setting character string includes a space, AX2200S is used.
AX1250S AX1240S	"AX1200S"	Setting character string	If the setting character string includes a space, AX1200S is used.

For details of (5) to (8) in the diagram, see the manual *Message and Log Reference*. However, since the message indicating AUT in (5) in the diagram indicates the account log of the Layer 2 authentication functionality, see the manual *Operation Command Reference*.

In addition, the use of the operation command trace-monitor allows the operation log to appear on the monitor of the operation terminal (console). For details on the monitor display, see *10. Device Management* in the *Configuration Guide Vol. 1*.

22.2 Configuration

22.2.1 List of configuration commands

The following table describes the commands used to configure log output functionality.

Table 22-2 List of configuration commands (configuration related to syslog output)

Command name	Description
`logging event-kind`	Sets the event type of the log information to be sent to the syslog server.
`logging facility`	Sets a facility to which log information is output via the syslog interface.
`logging host`	Sets the output destination for log information.
`logging syslog-header`	Adds `HOSTNAME`, `TIMESTAMP`, and a functionality number to the message to be sent to the syslog server.
`logging trap`	Sets the level of importance for log information to be sent to the syslog server.

22.2.2 Configuring the output of log information to syslog

Points to note

Configures a switch so that it uses the syslog output functionality to send the log information to the syslog server.

Command examples

1. `(config)# logging host 192.168.101.254`

   Sets up the log so that log data is generated for the IP address 192.168.101.254

22.2.3 Configuring addition of the HEADER part to log data output to syslog

Points to note

The example below shows how to add `HOSTNAME`, `TIMESTAMP`, and a functionality number to the HEADER part of a syslog message.

Command examples

1. `(config)# logging syslog-header`

   Adds `HOSTNAME`, `TIMESTAMP`, and a functionality number to the HEADER part of a syslog message.

Part 7: Management of Neighboring Device Information

23. LLDP

The Link Layer Discovery Protocol (LLDP) is functionality that collects information about the devices that are neighbors of the Switch. This chapter describes LLDP and its use.

23.1 Description

23.1.1 Overview

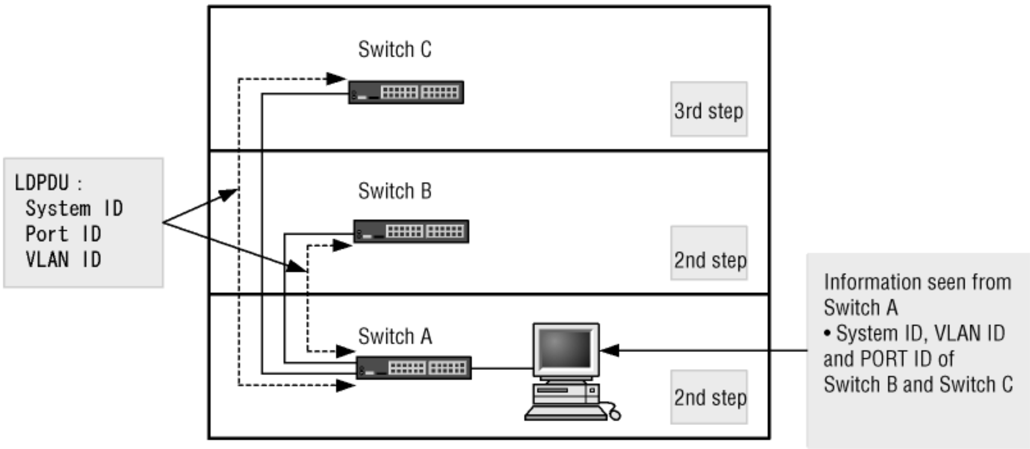
LLDP (*Link Layer Discovery Protocol*) is a protocol to collect information about neighboring devices. The purpose of the functionality provided by the protocol is to make the examination of information about connected devices easier during operation and maintenance.

(1) Example of using LLDP

The LLDP functionality sends information about the Switch and about the target port to each port connected to neighboring devices. Managing the information about neighboring devices received at the target port allows you to understand the connection status between the Switch and neighboring devices.

The figure below shows an example of using LLDP. In this example, the operator of Switch A installed on the 1st floor of a building can check the status of connections to other Switches installed on other floors of the building.

Figure 23-1 Example of using LLDP



23.1.2 Supported specifications

The information that the Switch sends to neighboring devices over LLDP is not limited to the information prescribed in IEEE 802.1AB Draft 6, but also includes extended vendor-specific information. The following table describes the information items that can be sent via LLDP.

Table 23-1 Information that can be sent by using LLDP

#	Name	Description
1	End Of LDPDU	LDPDU terminal identifier
2	Time-to-Live	Information retention period
3	Chassis ID	Device identifier

#		Name	Description
4		Port ID	Port identifier
5		Port description	Port type
6		System name	Device name
7		System description	Device type
8	n/a	Organizationally defined TLV extensions	TLV information uniquely added by the vendor or organization
	a	VLAN ID	VLAN ID that has been set
	b	VLAN Address	IP address associated with the VLAN

Legend n/a: Not applicable

The following subsections describe the above information in detail.

For details on MIB, see the *MIB Reference*.

(1) Time-to-Live (the time information is retained)

`Time-to-Live` indicates how long the destination device will retain the received information.

Although you can change the retention time in configuration mode, we recommend that you do not change the initial value.

(2) Chassis ID (device identifier)

`Chassis ID` is information that identifies the device. This information has a subtype, and the value to be sent changes according to the subtype. The following table describes subtypes and the values to be sent.

Table 23-2 List of Chassis ID subtypes

subtype	Type	Value to be sent
1	Chassis component	The same value as `entPhysicalAlias` of the Entity MIB
2	Chassis interface	The same value as `ifAlias` of the Interface MIB
3	Port	The same value as `portEntPhysicalAlias` of the Entity MIB
4	Backplane component	The same value as `backplaneEntPhysicalAlias` of the Entity MIB
5	MAC address	The same value as `macAddress` of the LLDP MIB
6	Network address	The same value as `networkAddress` of the LLDP MIB

subtype	Type	Value to be sent
7	Locally assigned	The same value as `local` of the LLDP MIB

The following are the sending and reception conditions for `Chassis ID`:

- Sending: Only `subtype = 5` is sent. The MAC address of the device is sent.
- Reception: All subtypes shown above can be received.
- Maximum length for received data: 255 bytes

(3) Port ID (port identifier)

`Port ID` is information that identifies the port. This information has a subtype, and the value to be sent changes according to the subtype. The following table describes subtypes and the values to be sent.

Table 23-3 List of Port ID subtypes

subtype	Type	Value to be sent
1	Port	The same value as `ifAlias` of the Interface MIB
2	Port component	The same value as `portEntPhysicalAlias` of the Entity MIB
3	Backplane component	The same value as `backplaneEntPhysicalAlias` of the Entity MIB
4	MAC address	The same value as `macAddr` of the LLDP MIB
5	Network address	The same value as `networkAddr` of the LLDP MIB
6	Locally assigned	The same value as `local` of the LLDP MIB

The following are the sending and reception conditions for `Port ID`:

- Sending: Only `subtype = 4` is sent. The MAC address of a target port is sent.
- Reception: All subtypes shown above can be received.
- Maximum length for received data: 255 bytes

(4) Port description (port type)

`Port Description` is information that indicates the type of the port. This information does not have a subtype.

The value to be sent and the reception condition are as follows:

- Value to be sent: The same value as `ifDescr` of the Interface MIB
- Maximum length for received data: 255 bytes

(5) System name (device name)

`System Name` is information that indicates the name of the device. This information does not have a subtype.

The value to be sent and the reception condition are as follows:

- Value to be sent: The same value as `sysName` of the System MIB
- Maximum length for received data: 255 bytes

(6) System description (device type)

`System Description` is information that indicates the type of the device. This information does not have a subtype.

The value to be sent and the reception condition are as follows:

- Value to be sent: The same value as `sysDescr` of the System MIB
- Maximum length for received data: 255 bytes

(7) Organizationally defined TLV extensions

The organizationally defined TLV extensions supported uniquely by the Switch are as follows.

(a) VLAN ID

`VLAN ID` indicates the VLAN tag used by the port. Note that `VLAN ID` is information that is effective on only trunk ports.

(b) VLAN Address

If there is VLAN for which IP addresses are set, this information indicates the VLAN ID and one of the IP addresses.

23.1.3 Notes on using LLDP

(1) If another device that does not support this functionality is connected between devices for which this functionality is set

If the configuration is one of the following, it is difficult to correctly grasp the connection status with neighboring devices.

- If the connection is made through a switch, the switch forwards the LLDP distribution information. Therefore, since the distribution information can be received as neighboring information between devices not connected directly, the information cannot be distinguished from information between directly connected devices.
- If a connection is made through a router, the LLDP distribution information is discarded at the router, so the information cannot be received by a device for which the LLDP functionality is set.

(2) Connection to other company devices

Interconnection with the Link Layer Discovery Protocol# supported uniquely by other companies cannot be made.

#

Cisco Systems: CDP (Cisco Discovery Protocol)

Extreme Networks: EDP (Extreme Discovery Protocol)

Foundry Networks: FDP (Foundry Discovery Protocol)

(3) Connection with the IEEE 802.1AB standard

The LLDP of the Switch is original functionality whose support is based on IEEE 802.1AB Draft 6. There is no connectivity with IEEE 802.1AB standards.

(4) Maximum number of neighboring devices

The Switch can handle information for no more than the number of neighboring devices indicated in *3.2 Capacity limits* in the *Configuration Guide Vol. 1*. If the maximum is exceeded, the distributed information is discarded when received. To ensure the time needed to delete the received neighboring device information because of a timeout, the discard state continues for a set period. The time is the same as the retention time for neighboring device information when the threshold of maximum accommodation is exceeded.

(1) Use with other functionality

(a) Use with Layer 2 functionality

See *5.9.3 Interoperability of the Layer 2 authentication functionality and other functionality.*

(b) Use with CFM

See *20.1.9 Notes on using the CFM functionality.*

23.2 Configuration

23.2.1 List of configuration commands

The following table describes the commands used to configure LLDP.

Table 23-4 List of configuration commands

Command name	Description
`lldp enable`	Starts operation of LLDP on the port.
`lldp hold-count`	Specifies the time for a neighboring device to retain LLDP frame sent by this Switch.
`lldp interval-time`	Specifies the transmission interval between LLDP frames sent by this Switch.
`lldp run`	Activates LLDP functionality for the entire device.

23.2.2 Configuring LLDP

(1) Configuring LLDP

Points to note

Configuration of LLDP requires enabling of LLDP for the entire device, and then enabling of LLDP for the port for which it will be used.

In this example, the LLDP functionality operates in the status of `fastethernet 0/1`.

Command examples

1. `(config)# lldp run`

   Enables LLDP for the entire device.

2. `(config)# interface fastethernet 0/1`

   Moves to the Ethernet interface configuration mode of port 0/1.

3. `(config-if)# lldp enable`

   `(config-if)# exit`

   Starts operation of LLDP functionality at port 0/1.

(2) Setting the sending interval and retention time of LLDP frames

Points to note

How often neighboring device information is updated can be adjusted by changing the interval for sending LLDP frames. If the interval is decreased, the information is updated more often. If the interval is increased, the information is updated less often.

Command examples

1. `(config)# lldp interval-time 60`

Sets 60 seconds as the interval for sending LLDP frames.

2. `(config)# lldp hold-count 3`

   Sets the time for neighboring devices to retain the information sent by this Switch. The retention time is determined by the sending interval time multiplied by the number of sending intervals specified here. In this example, the retention time is 180 seconds (60 seconds x 3).

23.3 Operation

23.3.1 List of operation commands

The following table describes the operation commands for LLDP.

Table 23-5 List of operation commands

Command name	Description
`show lldp`	Displays LLDP configuration information and neighboring device information.
`show lldp statistics`	Displays LLDP statistics.
`clear lldp`	Clears the LLDP information for neighboring devices.
`clear lldp statistics`	Clears LLDP statistics.

23.3.2 Displaying LLDP information

LLDP information can be displayed by using the `show lldp` operation command. The operation command `show lldp` displays the LLDP setting information and the number of neighboring devices for each port. The operation command `show lldp detail` displays the detailed information on neighboring devices.

Figure 23-2 Execution results of show lldp

```
>show lldp

Date 2011/09/15 13:32:41 UTC
Status: Enabled  Chassis ID: Type=MAC      Info=0012.e204.0001
Interval Time: 30   Hold Count: 4  TTL: 120
Port Counts=5
  0/5(CH:1)   Link: Up    Neighbor Counts: 1
  0/6(CH:1)   Link: Up    Neighbor Counts: 1
  0/18        Link: Up    Neighbor Counts: 1
  0/23        Link: Down  Neighbor Counts: 0
  0/24        Link: Up    Neighbor Counts: 1

>
```

Figure 23-3 Execution results of show lldp detail

```
> show lldp detail

Date 2011/09/15 13:33:18 UTC
Status: Enabled  Chassis ID: Type=MAC    Info=0012.e204.0001
Interval Time: 30  Hold Count: 4  TTL: 120
System Description: ALAXALA AX1240 AX-1240-24T2C [AX1240S-24T2C] Switching
software Ver. 2.3.B OS-LT2
Total Neighbor Counts=4
Port Counts=5
Port 0/5(CH:1)    Link: Up   Neighbor Counts: 1
```

```
 Port ID: Type=MAC    Info=0012.e204.0105
 Port Description: FastEther 0/5
 Tag ID: Tagged=10,100,4094
 IPv4 Address: Tagged: 10   192.168.10.2
 1  TTL:92 Chassis ID: Type=MAC    Info=0012.e284.0001
    System Description: ALAXALA AX1240 AX-1240-24T2C [AX1240S-24T2C] Switching
software Ver. 2.3.B OS-LT2
    Port ID: Type=MAC    Info=0012.e284.0105
    Port Description: FastEther 0/5
    Tag ID: Tagged=10
    IPv4 Address: Tagged: 10   192.168.10.1
             :
             :

>
```

Part 8: Port Mirroring

24. Port Mirroring

Port mirroring is functionality that sends a copy of sent or received frames to the specified physical port. This chapter describes port mirroring and its use.

24.1 Description

24.1.1 Overview of port mirroring

Port mirroring is functionality that sends a copy of sent or received frames to the specified physical port. The copying of frames is called *mirroring*. By using an analyzer to receive the forwarded mirror frames, you can monitor or analyze traffic.

The following figures show the flow of received frames and sent frames when mirroring is used.

Figure 24-1 Mirroring of received frames

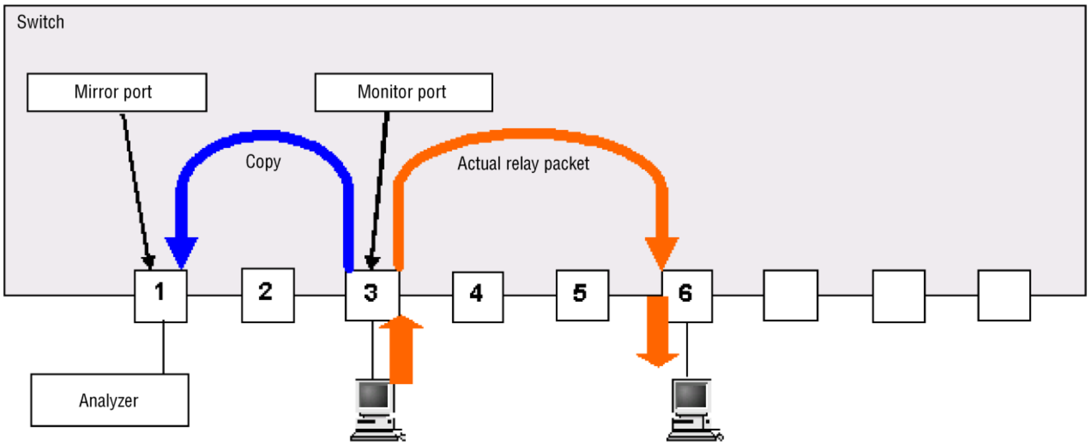
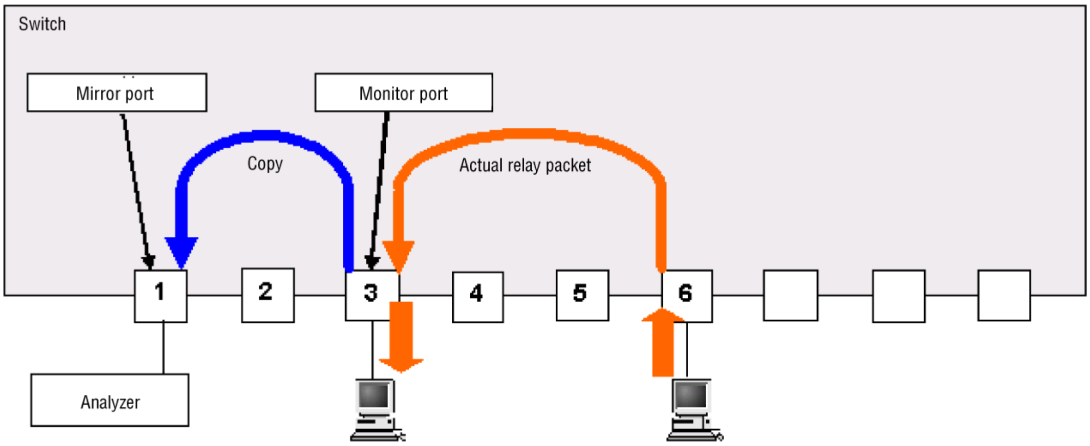


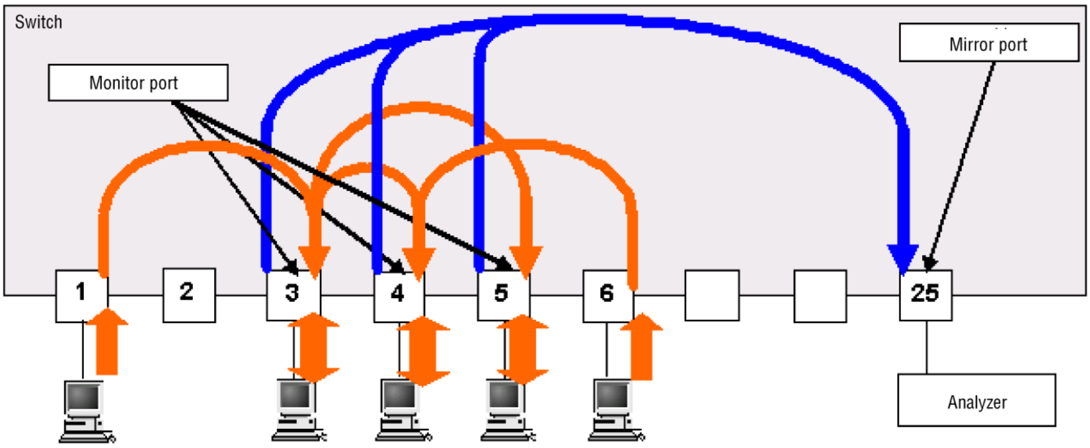
Figure 24-2 Mirroring of sent frames



As indicated in the above figures, a physical port whose traffic is monitored is called a *monitored port*, and the physical port to which the frames copied for mirroring are sent is called a *mirror port*.

Also note that the monitored and mirror ports can be in a multipoint-to-point relationship. That is, copies of frames received by multiple monitored ports can be sent to one mirror port. It is not possible to send copied frames to multiple mirror ports.

Figure 24-3 Mirroring of frames on multiple ports



There are no operation commands for port mirroring. Use the analyzer connected to the mirror port to confirm that frames are mirrored.

24.1.2 Notes applying when port mirroring is used

(1) Notes on use with other functionality

- On the mirror port, VLANs are unavailable when port mirroring is used. The Spanning Tree Protocol, the Ring Protocol, and IGMP or MLD snooping, which are based on VLAN functionality, are also unavailable.
- On monitor ports, other functionality can operate without restrictions.

(2) Notes applying when port mirroring is used

1. The monitor port cannot output more mirror frames than the mirror port's bandwidth allows.
2. If the FCS of a received frame is incorrect, the target frame is not mirrored.
3. Filter control can be used for the monitored port, but this does not affect port mirroring.
4. For the mirroring of sent frames, the Switch mirrors the frames that are forwarded by hardware. Frames originated by the device are mirrored, but the following sent frames are not.(Also see *Table 24-1 Availability of mirroring for sent frames.)*
    - L2 frames originated by the device (for example, LLDP, UDLD)
    - DHCP frames (when DHCP snooping is enabled)
    - ARP frames (when dynamic ARP inspection is enabled)
    - IGMP frames (when IGMP snooping is enabled)
    - MLD frames (when MLD snooping is enabled)
    - Pre-authentication frames (when Layer 2 authentication is enabled)
    - GSRP aware frames (only for transmission when the frames are being forwarded)
    - Uplink-redundant flash control frames originated by the device (when flash control frame sending is enabled)

- Uplink-redundant MAC address update frames originated by the device (when MAC address updating is enabled)
- L2 loop detection frames originated by the device (when L2 loop detection is enabled)
- CFM forwarded frames (when CFM is enabled)
- Sent frames for CCM, loopbacks (messages and response), linktraces (messages and response) (when CFM is enabled)

When received frames are mirrored, all received frames, including the incoming frames, are mirrored.

5. When sent frames are mirrored, if multiple monitored ports are used, and frames are flooded to some or all of the ports, frames are mirrored as follows:
   - If the applicable ports are members of either the group consisting of ports 0/1 to 0/24, 0/49, and 0/50 or the group consisting of ports 0/25 to 0/48, two frames are mirrored.
   - If the monitored ports are members of groups other than the above two groups, one frame is mirrored.
6. When sent frames are mirrored, even if untagged frames are sent, tagged frames that have the tag of VLAN for the sent frames are mirrored.
7. When frames are mirrored, only one session can be set.
8. When the following functionality is enabled on the mirror ports, the mirror ports send control frames:
   - LLDP: LLDP frames
   - IEEE 802.3ah/UDLD: UDLD frames
   - Spanning Tree Protocol: BPDU frames

     The spanning tree protocol is enabled by default. To stop sending BPDU frames, set the `spanning-tree disable` configuration command, or set BPDU filtering on the mirror ports (`spanning-tree bpdufilter` configuration command).
9. When an outgoing frame is mirrored, the frame transmission order might differ from the order sent from the monitor port.

Table 24-1 Availability of mirroring for sent frames

Frame type	Availability of mirroring	Type	Remarks
ICMP	Yes	Originated	Includes the confirmation of Secure Wake-on-LAN terminal startup.
FTP	Yes	Originated	
telnet	Yes	Originated	
SNMP	Yes	Originated	
SNMP TRAP	Yes	Originated	
syslog	Yes	Originated	

Frame type	Availability of mirroring	Type	Remarks
RADIUS	Yes	Originated	
NTP	Yes	Originated	
IGMP	Available/ unavailable	Forward	Unavailable only when IGMP snooping is enabled.
MLD	Available/ unavailable	Forward	Unavailable only when MLD snooping is enabled.
DHCP	Available/ unavailable	Forward	Unavailable only when DHCP snooping is enabled.
ARP	Available/ unavailable	Forward	Unavailable only when dynamic ARP inspection is enabled.
Startup command	Yes	Originated	Secure Wake-on-LAN
Pre-authentication	Available/ unavailable	Forward	• Unavailable when Layer 2 authentication is enabled. • Partly unavailable when IPv4 access list exclusively for authentication is configured.#
LLDP	No	Originated	
UDLD	No	Originated	
LACP	No	Originated	
EAPOL	No	Originated	
BPDU	No	Originated	
L2 Loop Detection	No	Originated	
Flush control frame	No	Originated	Uplink redundancy
MAC address update frames	No	Originated	Uplink redundancy
GSRP aware	No	Forward	Unavailable only for transmission when the frames are being forwarded.
CFM	No	Originated	
		Forward	Unavailable only when CFM is enabled.

#

The frames that meet the conditions in the table below are not mirrored even if IPv4 access list exclusively for authentication is configured.

Table 24-2 Exceptions for IPv4 access list exclusively for authentication for port mirroring

Conditions	Frame type
IGMP snooping is enabled.	IGMP
MLD snooping is enabled.	MLD
DHCP snooping is enabled.	DHCP
Dynamic ARP inspection is enabled.	ARP

24.2 Configuration

24.2.1 List of configuration commands

The following table describes the commands used to configure port mirroring.

Table 24-3 List of configuration commands

Command name	Description
`monitor session`	Configures port mirroring.

24.2.2 Configuring port mirroring

When port mirroring is configured, a combination of monitored ports and a mirror port is defined as a *monitored session*. A maximum of one monitored session can be defined for the Switch.

Ports used for normal data communication are specified as monitored ports. A port to which an analyzer is connected for monitoring or analyzing the traffic is specified as a mirror port.

(1) Mirroring of received frames

Points to note

The mirroring of sent or received frames can be defined for Ethernet interfaces. Specify separate Ethernet interfaces even if link aggregation is used. Make sure that no VLANs belong to the port to be used as a mirror port.

Command examples

1.

```
(config)# monitor session 1 source interface 0/1 rx destination
interface fastethernet 0/5
```

Sets that an analyzer is connected to port 0/5, and that the frames received on port 0/1 are mirrored. Note that the number of the monitored session is fixed to 1.

(2) Mirroring of sent frames

Points to note

The mirroring of sent or received frames can be defined for Ethernet interfaces. Specify separate Ethernet interfaces even if link aggregation is used. Make sure that no VLANs belong to the port to be used as a mirror port. Note that the number of the monitored session is fixed to 1.

Command examples

1.

```
(config)# monitor session 1 source interface 0/2 tx destination
interface fastethernet 0/6
```

Sets that an analyzer is connected to port 0/6, and that the frames sent on port 0/2 are mirrored. Note that the number of the monitored session is fixed to 1.

(3) Mirroring of sent or received frames

Points to note

The mirroring of sent or received frames can be defined for Ethernet interfaces. Specify separate Ethernet interfaces even if link aggregation is used. Make sure that no VLANs belong to the port to be used as a mirror port. Note that the number of the monitored session is fixed to 1.

Command examples

1. `(config)# monitor session 1 source interface 0/3 both destination interface fastethernet 0/11`

   Sets that an analyzer is connected to port 0/11, and that the frames sent and received on port 0/3 are mirrored. Note that the number of the monitored session is fixed to 1.

(4) Mirroring of frames on multiple monitor ports

Points to note

You can set multiple monitor ports in the form of a list. Make sure that no VLANs belong to the port to be used as a mirror port. Note that the number of the monitored session is fixed to 1.

Command examples

1. `(config)# monitor session 1 source interface 0/3-5 both destination interface gigabitethernet 0/25`

   Sets that an analyzer is connected to port 0/25, and that the frames sent and received on port 0/3 to 0/5 are mirrored. Note that the number of the monitored session is fixed to 1.

Appendix

A. Relevant standards

A.1 IEEE802.1X

Table A-1 Relevant standards and recommendations for IEEE 802.1X

Name (month and year issued)	Title
IEEE802.1X (June 2001)	Port-Based Network Access Control
RFC 2865 (June 2000)	Remote Authentication Dial In User Service (RADIUS)
RFC 2866 (June 2000)	RADIUS Accounting
RFC 2868 (June 2000)	RADIUS Attributes for Tunnel Protocol Support
RFC 2869 (June 2000)	RADIUS Extensions
RFC 3579 (September 2003)	RADIUS Support For Extensible Authentication Protocol (EAP)
RFC 3580 (September 2003)	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
RFC 3748 (June 2004)	Extensible Authentication Protocol (EAP)

A.2 Web Authentication

Table A-2 Relevant standards and recommendations for Web authentication

Name (month and year issued)	Title
RFC 2865 (June 2000)	Remote Authentication Dial In User Service (RADIUS)
RFC 2866 (June 2000)	RADIUS Accounting

A.3 DHCP Server Functionality

Table A-3 Relevant standards for the DHCP server functionality

Name (month and year issued)	Title
RFC 2131 (March 1997)	Dynamic Host Configuration Protocol
RFC 2132 (March 1997)	DHCP Options and BOOTP Vendor Extensions

A.4 MAC-based Authentication

Table A-4 Relevant standards and recommendations for MAC-based authentication

Name (month and year issued)	Title
RFC 2865 (June 2000)	Remote Authentication Dial In User Service (RADIUS)
RFC 2866 (June 2000)	RADIUS Accounting

A.5 IEEE 802.3ah/UDLD

Table A-5 Relevant standards and recommendations for IEEE 802.3ah/UDLD

Name (month and year issued)	Title
IEEE802.3ah (September 2004)	Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks

A.6 CFM

Table A-6 Relevant standards and recommendations for CFM

Name (month and year issued)	Title
IEEE802.1ag-2007 (December 2007)	Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management

A.7 SNMP

Table A-7 Relevant standards and recommendations for SNMP

Name (month and year issued)	Title
RFC 1155 (May 1990)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157 (May 1990)	A Simple Network Management Protocol (SNMP)
RFC 1213 (March 1991)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1493 (June 1993)	Definitions of Managed Objects for Bridges[#]
RFC 1643 (July 1994)	Definitions of Managed Objects for the Ethernet-like Interface Types[#]

Name (month and year issued)	Title
RFC 1757 (February 1995)	Remote Network Monitoring Management Information Base
RFC 1901 (January 1996)	Introduction to Community-based SNMPv2
RFC 1902 (January 1996)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1903 (January 1996)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1904 (January 1996)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1905 (January 1996)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1906 (January 1996)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1907 (January 1996)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1908 (January 1996)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC 2233 (November 1997)	The Interfaces Group MIB using SMIv2
RFC 2863 (June 2000)	The Interfaces Group MIB[#]
RFC 3621 (December 2003)	Power Ethernet MIB

#
Only a part of MIBs are subject to the relevant standard. For more details, see the manual *MIB Reference*.

A.8 SYSLOG

Table A-8 Relevant standards and recommendations for SYSLOG

Name (month and year issued)	Title
RFC 3164 (August 2001)	The BSD Syslog Protocol

A.9 LLDP

Table A-9 Relevant standards and recommendations for LLDP

Name (month and year issued)	Title
IEEE802.1AB/D6.0 (October 2003)	Draft Standard for Local and Metropolitan Networks: Station and Media Access Control - Connectivity Discovery

Index

M

N

O

P