AX3660S Software Manual

Configuration Guide Vol.2

For Version 12.1 Rev.11

AX38S-S011X-C0

AlaxalA

■ Relevant products

This manual applies to the models in the AX3660S series of switches. It also describes the function of OS-L3M version 12.1 of the software.

■ Precautions in exporting

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. If you require more information, please contact an Alaxala sales representative.

■ Trademarks

■ Reading and storing this manual

Before you use the device, 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.

■ Note

Information in this document is subject to change without notice.

■ Editions history

December 2023 (Edition 1) AX38S-S011X-C0

■ Copyright

Preface

■ Applicable products and software versions

This manual applies to the models in the AX3660S series of switches. It also describes the function of OS-L3M version 12.1 of the software. The described function is that supported by the software license and by optional licenses.

Before you operate the Switch, 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 functions common to both the SL-L3A and SL-L3L software licenses. Functions that are not common are indicated as follows.

[SL-L3A]:

The description applies to the SL-L3A software 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:

https://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 a switch.

● **To learn how to unpack the switch and the basic settings for initial installation**

Quick Start Guide (AX36S-Q002X)

● **To check the hardware equipment conditions and how to handle the hardware**

Hardware Instruction Manual (AX36S-H002X)

Transceiver Hardware Instruction Manual (AX-COM-H001X)

● **To learn the software functions, configuration settings, and use of operation commands**

Configuration Guide Vol.1 (AX38S-S010X)
Vol.2 (AX38S-S011X)
Vol.3 (AX38S-S012X)

● **To learn the entry syntax of configuration commands and the details of command parameters**

Configuration Command Reference Vol.1 (AX38S-S013X)
Vol.2 (AX38S-S014X)

● **To learn the entry syntax of operation commands and the details of command parameters**

Operation Command Reference Vol.1 (AX38S-S015X)
Vol.2 (AX38S-S016X)

● **To check messages and logs**

Message Log Reference (AX38S-S017X)

● **To learn how to troubleshoot a problem**

Troubleshooting Guide (AX36S-T002X)

■ Conventions: The terms "Switch" and "switch"

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

- AX3660S 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.

■ Abbreviations used in the manual

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
ALG	Application Level Gateway

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
BFD	Bidirectional Forwarding Detection
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
CA	Certificate Authority
CBC	Cipher Block Chaining
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
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DNSSL	Domain Name System Search List
DR	Designated Router
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DSS	Digital Signature Standard
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECDHE	Elliptic Curve Diffie-Hellman key exchange, Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
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
GCM	Galois/Counter Mode
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
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
MLD	Multicast Listener Discovery
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission 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
PGP	Pretty Good Privacy
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
PMTU	Path Maximum Transmission Unit
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PTP	Precision Time Protocol
QoS	Quality of Service
QSFP+	Quad Small Form factor Pluggable Plus
QSFP28	28Gbps Quad Small Form factor Pluggable

RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
RDNSS	Recursive Domain Name System Server
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
RSA	Rivest, Shamir, Adleman
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
SFP+	enhanced Small Form-factor Pluggable
SHA	Secure Hash Algorithm
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
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
Sync-E	Synchronous Ethernet
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLS	Transport Layer Security
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
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VLAN	Virtual LAN
VNI	VXLAN Network Identifier
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
VTEP	VXLAN Tunnel End Point
VXLAN	Virtual eXtensible Local Area Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web

■ 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.

Contents

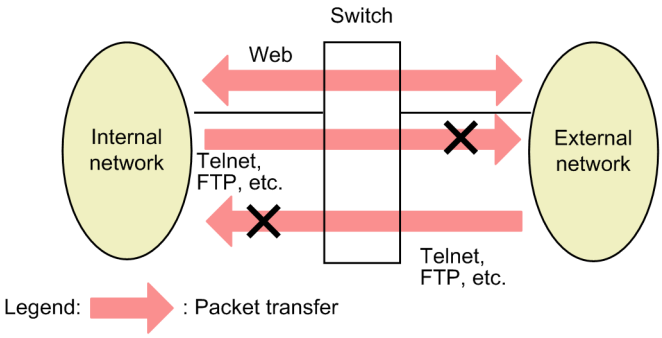
1 Filters

Filtering is a function used for forwarding and discarding certain types of frames. This chapter provides an overview of the filter function and describes its use.

1.1 Description

Filtering is a function used to forward and discard certain types of 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. Doing so allows you to prevent unauthorized access from the external network and prevent information leaks to the external network from the internal network. The following figure shows an example of network configuration that uses filters.

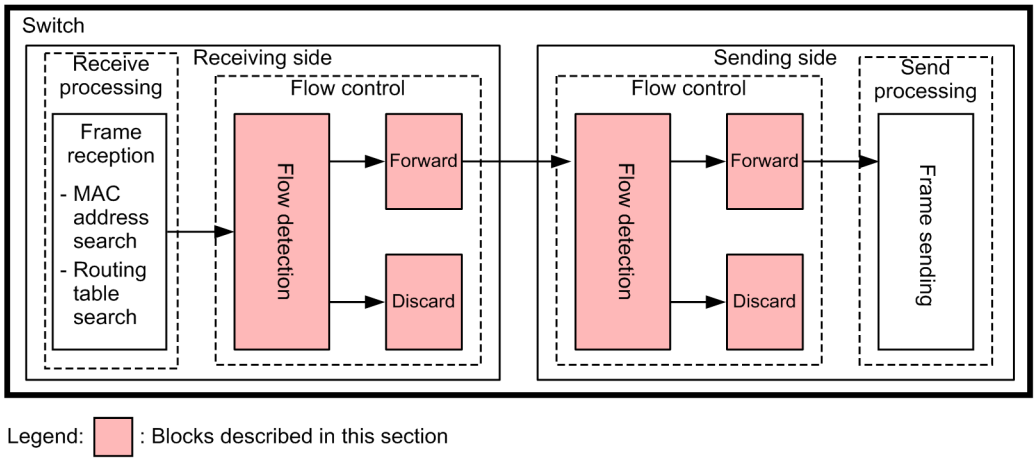
Figure 1-1: Example of network configuration that uses filters



1.1.1 Overview of filters

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

Figure 1-2: Functional blocks for filters



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

Table 1-1: Overview of functional blocks for filters

Section and functional blocks		Function overview
Flow control section	Flow detection	This block detects a flow (specific frames) that matches a condition, such as MAC address, protocol type, IP address, TCP/UDP port number, or ICMP header.
	Forwarding and discarding	These blocks forward and discard frames found by the flow detection block.

To use a filter on a Switch, you need to create a filter entry that defines a combination of flow detection condition (such as MAC address, protocol type, IP address, TCP/UDP port number, or ICMP header) and a behavior (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 ends when a filter entry matching the frame is found.
3. Whether the frame is forwarded or discarded is determined according to the behavior specified for the filter entry.
4. If the frame does not match any filter entry, the frame is discarded. For details on discarding, see "1.1.7 Implicit discard".

Notes

If a frame is discarded on the receiving-side interface, the sending-side interface does not perform flow detection.

Also, filters cannot be used on the stack port.

1.1.2 Flow detection

The flow detection function detects a flow, which is a sequence of frames, based on conditions, such as the MAC header, IP header, TCP header, and ICMP header. Settings are configured in access lists. For details about access lists, see "1.1.6 Access lists".

In the Switch, an access list can be set for the Ethernet interface and the VLAN interface. The Switch is able to perform flow detection for Ethernet V2 format frames and IEEE 802.3 SNAP/RFC 1042 format frames on both the Ethernet interfaces and VLAN interfaces with an access list set.

If flow detection is specified for the receiving-side interface, flow detection is performed at the point of reception on the Ethernet interface for both the Ethernet interface and the VLAN interface. Note that the frames received by the Switch are also subject to the flow detection.

If flow detection is specified for the sending-side interface, flow detection is performed at the point of sending on the Ethernet interface for both the Ethernet interface and the VLAN interface. Therefore, frames relayed from other VLANs to the target VLAN can be detected by the sender of the target VLAN interface. Note that the frames spontaneously sent by the Switch are also subject to the flow detection performed on the sending side.

1.1.3 Receiving-side flow detection mode

The Switch provides receiving-side flow detection modes for network configuration and an operation mode. The receiving-side flow detection modes determine the distribution pattern of filter entries and QoS entries for the receiving-side interface. For the entry distribution, refer to "Configuration Guide Vol. 1, 3 Capacity Limit", and select the mode according to your operating requirements.

Use the "flow detection mode" command to specify the receiving-side flow detection mode. The selected receiving-side flow detection mode applies to both filters and QoS. To change the receiving-side flow detection mode, delete all the following commands set for the receiving-side and sending-side interfaces and the "ip verify source" command of DHCP snooping.

- mac access-group
- ip access-group
- ipv6 traffic-filter

- mac qos-flow-group
- ip qos-flow-group
- ipv6 qos-flow-group

Furthermore, if you change the receiving-side flow detection mode to the receiving-side flow detection mode that does not support policy-based routing, you must delete the following commands in addition to these commands.

- policy-list
- policy-list default-aging-interval
- policy-list default-init-interval

If the IP unset VLAN suppression mode of the receiving-side flow detection mode is set, it controls IP packets (including ARP) in VLANs where the "ip address" configuration command is not set, and IPv6 packets in VLANs where the "ipv6 enable" configuration command is not set, so that they are not transferred to the CPU. However, when using any of the following functions, IP packets that need to be controlled by the target function are transferred to the CPU.

- VXLAN PMTU function
- IGMP snooping
- MLD snooping
- Layer 2 authentication
- DHCP snooping (However, dynamic ARP inspection cannot be used along with the IP unset VLAN suppression mode.)

Note that if you do not specify the receiving-side flow detection mode, layer3-2 is set as the default mode.

The following table describes the relationship between the receiving-side flow detection modes and flow performances.

Table 1-2: Flow detection modes for the receiving side and flow performances

Receiving-side flow Detection mode name	Purpose	Flow performance
layer3-1	• To perform flow control for IP packets and other frames • To perform flow control specialized for IPv4 packets	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-2	• To perform flow control specialized for IPv4 packets	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-6	• To perform flow control specialized for IPv4 or IPv6 packets • To use the policy-based routing	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.

Receiving-side flow Detection mode name	Purpose	Flow performance
layer3-dhcp-1	• To perform flow control specialized for IPv4 packets and to use the terminal filter of DHCP snooping	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-mirror-1	• To use flow control and policy-based mirroring of IP packets and other frames • To perform flow control and policy-based mirroring specialized for IPv4 packets	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-mirror-2	• To perform flow control and policy-based mirroring specialized for IPv4 packets	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-mirror-3	• To use flow control specialized for IPv4 or IPv6 packets • To use policy-based mirroring of IP packets and other frames • To perform policy-based mirroring specialized for IPv4 packets • To use the policy-based routing	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-mirror-4	• To perform flow control specialized for IPv4 or IPv6 packets • To use policy-based mirroring specialized for IPv6 packets • To use the policy-based routing	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-mirror-5	• To perform flow control specialized for IPv4 or IPv6 packets • To use policy-based mirroring of IP packets and other frames • To use policy-based mirroring for IPv4 and IPv6 packets • To use the policy-based routing	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-suppress-1	• To use the IP unset VLAN suppression mode • To perform flow control for IP packets and other frames • To perform flow control specialized for IPv4 packets	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.

Receiving-side flow Detection mode name	Purpose	Flow performance
layer3-suppress-2	• To use the IP unset VLAN suppression mode • To perform flow control specialized for IPv4 or IPv6 packets • To use the policy-based routing	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-suppress-dhcp-1	• To use the IP unset VLAN suppression mode • To perform flow control specialized for IPv4 packets and to use the terminal filter of DHCP snooping	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-suppress-mirror-1	• To use the IP unset VLAN suppression mode • To use flow control and policy-based mirroring of IP packets and other frames • To perform flow control and policy-based mirroring specialized for IPv4 packets	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-suppress-mirror-2	• To use the IP unset VLAN suppression mode • To use filters for IPv4 and IPv6 packets • To use policy-based mirroring of IPv4 and IPv6 packets • To use the policy-based routing	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
custom	Use this mode to select the functions listed below, assign the function to each entry block in the hardware table, and set the accommodation conditions flexibly. • IP unset VLAN suppression mode • Flow control for IPv4 or IPv6 packets and other frames • Policy-based mirroring for IPv4 or IPv6 packets and other frames • Policy-based routing • Terminal filter of DHCP snooping	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.

1.1.4 Sending-side flow detection mode

The Switch provides sending-side flow detection modes for network configuration and an operation mode. The sending-side flow detection modes determine the distribution pattern of filter entries for the sending-side interface. For the entry distribution, refer to "Configuration Guide Vol. 1, 3 Capacity Limit", and select the mode according to your operating requirements.

Use the "flow detection out mode" command to specify the sending-side flow detection mode. The selected sending-side flow detection mode takes effect on the filter. To change the sending-side flow detection mode, you need to delete all the following commands set for the receiving-side and sending-side interfaces:

- mac access-group
- ip access-group

- ipv6 traffic-filter

If you do not specify the sending-side flow detection mode, layer3-1-out is set as the default mode.

The following table describes the relationship between the sending-side flow detection modes and flow performances.

Table 1-3: Flow detection modes for the sending side and flow performances

Sending-side flow Detection mode name	Purpose	Flow performance
layer3-1-out	• To perform flow control specialized for IPv4 packets	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-2-out	• To perform flow control for IPv4 or IPv6 packets and other frames	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IP packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.

1.1.5 Flow detection conditions

To perform flow detection, specify the conditions for identifying the flow in the configuration. The following describes the flow detection conditions for the receiving-side and sending-side interfaces.

(1) Flow detection conditions for the receiving-side interface

The following table describes the flow detection conditions that can be specified for the receiving-side interface.

Table 1-4: Flow detection conditions that can be specified for the receiving-side interface

Type		Configuration items
MAC conditions	Configuration	VLAN ID[#1]
	MAC headers	Source MAC address
		Destination MAC address
		Ethernet type
		User priority[#2]
IPv4 conditions	Configuration	VLAN ID[#1]
	MAC header	User priority[#2]
	IPv4 header[#3]	Upper layer protocol
		Source IP address
		Destination IP address
		ToS
		DSCP
		Precedence

Type		Configuration items	
	IPv4-TCP header	Source port number	Single specification (eq)
			Range specification (range)[#4]
		Destination port number	Single specification (eq)
			Range specification (range)[#4]
		TCP control flag[#5]	
	IPv4-UDP header	Source port number	Single specification (eq)
			Range specification (range)[#4]
		Destination port number	Single specification (eq)
			Range specification (range)[#4]
	IPv4-ICMP header	ICMP type value	
		ICMP code value	
IPv6 conditions	Configuration	VLAN ID[#1]	
	MAC header	User priority[#2]	
	IPv6 header[#6]	Upper layer protocol	
		Source IP address	
		Destination IP address	
		Traffic class	
		DSCP	
	IPv6-TCP header	Source port number	Single specification (eq)
			Range specification (range)[#4]
		Destination port number	Single specification (eq)
			Range specification (range)[#4]
		TCP control flag[#5]	
	IPv6-UDP header	Source port number	Single specification (eq)
			Range specification (range)[#4]
		Destination port number	Single specification (eq)
			Range specification (range)[#4]

Type		Configuration items
	IPv6-ICMP header	ICMP type value
		ICMP code value

#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

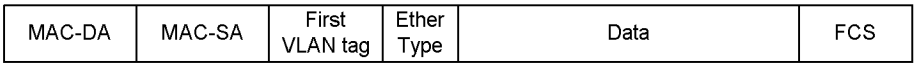
The user priority cannot be detected for the following frames. Therefore, user priority "3" is always detected.

- Frames that do not have a VLAN tag

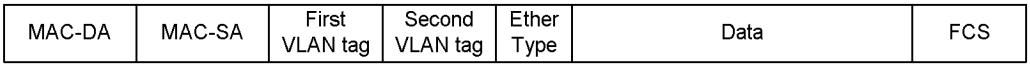
- Frames received on ports on which VLAN tunneling is set

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.

(i) Format of a frame with a single VLAN tag



(ii) Format of a frame with two VLAN tags

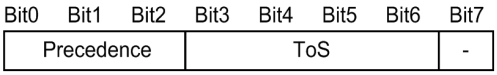


#3

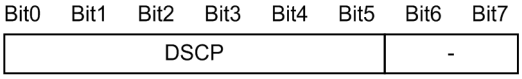
Supplementary note for the ToS field specification

ToS: Value of bits 3 to 6 in the ToS field.

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



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



#4

For details about capacity limits of the TCP/UDP port number detection pattern, see "Configuration Guide Vol. 1, 3.5 Filters, QoS, and policy-based mirroring".

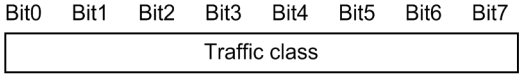
#5

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

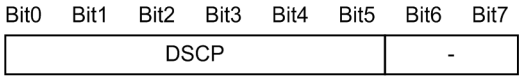
#6

Supplementary note for the traffic class field specification

Traffic class: The value of the traffic class field.



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



(2) Flow detection conditions for the sending-side interface

The following table describes the flow detection conditions that can be specified for the sending-side interface. However, filter entries cannot be applied to VLAN interfaces for which the tag translation has been set for any of the Ethernet interfaces that belong to the target VLAN.

Table 1-5: Flow detection conditions that can be specified for the sending-side interface

Type		Configuration items	
MAC conditions	Configuration	VLAN ID[#1]	
	MAC headers	Source MAC address	
		Destination MAC address	
		Ethernet type	
		User priority[#2]	
IPv4 conditions	Configuration	VLAN ID[#1]	
	MAC header	User priority[#2]	
	IPv4 header[#3]	Upper layer protocol	
		Source IP address	
		Destination IP address	
		ToS	
		DSCP	
		Precedence	
	IPv4-TCP header	Source port number	Single specification (eq)
		Destination port number	Single specification (eq)
		TCP control flag[#4]	
	IPv4-UDP header	Source port number	Single specification (eq)
		Destination port number	Single specification (eq)
	IPv4-ICMP header	ICMP type value	
		ICMP code value	
IPv6 conditions	Configuration	VLAN ID[#1]	
	MAC header	User priority[#2]	
	IPv6 header	Upper layer protocol	
		Source IP address	

Type		Configuration items	
		Destination IP address	
		Traffic class	
		DSCP	
	IPv6-TCP header	Source port number	Single specification (eq)
		Destination port number	Single specification (eq)
		TCP control flag#4	
	IPv6-UDP header	Source port number	Single specification (eq)
		Destination port number	Single specification (eq)
	IPv6-ICMP header	ICMP type value	
		ICMP code value	

#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 the outgoing frames belong will be detected.

You cannot specify a VLAN ID for either of the following interfaces:

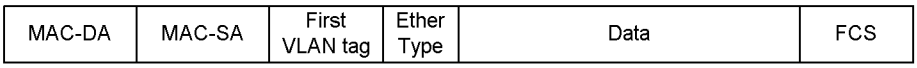
- Ethernet interfaces for which tag translation is set

- Ethernet interfaces for which VLAN tunneling is set

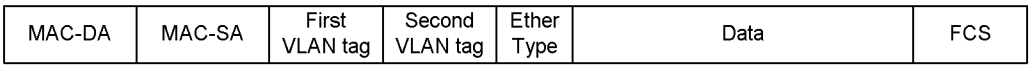
#2

The user priority set in the VLAN tag of the send frame is 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.

(i) Format of a frame with a single VLAN tag



(ii) Format of a frame with two VLAN tags



For the sending-side interface, the user priority for a frame without a VLAN tag is also detected. The following table describes the details of user priority detection.

Table 1-6: User priority detection on the sending-side interface

Ports from which frames are sent	Sending frame	Flow detection behavior for detecting the user priority
Ports for which VLAN tunneling is not set	—	If the marker function is used on the receiving side, the user priority after marking is performed is detected. If the marker function is not used on the receiving side and frames without VLAN tag are received, user priority 3 is detected. If the marker function is not used on the receiving side and frames with VLAN tag are received, the user priority that exists when the frames are received is detected. Note, however, that user priority 3 is detected for the following frames: • Frames received on ports on which VLAN tunneling is set

Ports from which frames are sent	Sending frame	Flow detection behavior for detecting the user priority
Ports for which VLAN tunneling is set	Without VLAN tag	Same as above
	With VLAN tag	The user priority for send frames is detected as follows, regardless of whether the marker function is used on the receiving side. The following user priority is detected for the outgoing frames: • For frames received on a port for which VLAN tunneling is set, the user priority that exists when the frames are received is detected. • For frames received on a port for which VLAN tunneling is not set, the user priority that exists when VLAN tags are removed from the receive frames is detected.

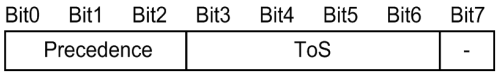
Legend: —: With or without a VLAN tag

#3

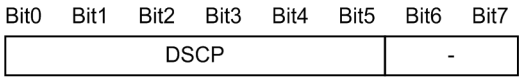
Supplementary note for the ToS field specification

ToS: Value of bits 3 to 6 in the ToS field.

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



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



When the marker function is used to rewrite a DSCP on the receiving-side interface, the values of ToS, DSCP, and Precedence for the sending-side interface are detected for the frames after the DSCP is rewritten.

#4

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

1.1.6 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 1-7: Relationship between the access lists for flow detection conditions and detectable frame types

Specifiable flow detection conditions	Access lists	Receiving-side flow detection mode	Sending-side flow detection mode	Detectable frame type		
				Non-IP	IPv4	IPv6
MAC conditions	mac access-list	layer3-1, layer3-mirror-1, layer3-mirror-3, layer3-mirror-5, layer3-suppress-1, layer3-suppress-mirror-1, custom	layer3-2-out	Y	Y	Y

Specifiable flow detection conditions	Access lists	Receiving-side flow detection mode	Sending-side flow detection mode	Detectable frame type		
				Non-IP	IPv4	IPv6
IPv4 conditions	access-list ip access-list	layer3-1, layer3-2, layer3-6, layer3-dhcp-1, layer3-mirror-1, layer3-mirror-2, layer3-mirror-3, layer3-mirror-4, layer3-mirror-5, layer3-suppress-1, layer3-suppress-2, layer3-suppress-dhcp-1, layer3-suppress-mirror-1, layer3-suppress-mirror-2, custom	layer3-1-out, layer3-2-out	—	Y	—
IPv6 conditions	ipv6 access-list	layer3-6, layer3-mirror-3, layer3-mirror-4, layer3-mirror-5, layer3-suppress-2, layer3-suppress-mirror-2, custom	layer3-2-out	—	—	Y

Legend: Y: Can be detected; —: Cannot be detected

The order in which filter entries are applied is determined by the sequence number specified as a parameter of an access list.

(1) Behavior when multiple flow detection conditions are simultaneously set

If filtering is performed for outgoing and incoming frames of the interface when multiple flow detection conditions are set, frames are detected in the order shown in the below table. Multiple filter entries are not matched.

Table 1-8: Flow detection order

Flow detection order	Access lists	Interface
1	mac access-list	Ethernet
2		VLAN
3	access-list ip access-list	Ethernet
4		VLAN
5	ipv6 access-list	Ethernet
6		VLAN

(2) Frames that cannot be discarded

The following frames on the receiving-side interface cannot be discarded regardless of whether filtering is enabled.

The following frames received by the Switch:

- Incoming frames for which the learned source MAC addresses are determined to have been moved

Of the frames received by the Switch by Layer 3 forwarding, the following packets and frames:

- IPv4 and IPv6 packets exceeding the MTU
- Frames whose TTL is set to 1
- Frames whose hop limit is set to 1
- Frames with an IP option
- Frames with an IPv6 extension header
- IPv4 or IPv6 packets with an unknown receiver address

1.1.7 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.

1.1.8 Notes on using the filter

(1) Filtering of frames with VLAN tags

You cannot filter frames with three or more VLAN tags by using an Ethernet type for a MAC condition, an IPv4 condition, or an IPv6 condition specified as a flow detection condition.

Either of the following conditions must be satisfied to filter the frames with two VLAN tags on the receiving side by an Ethernet type for a MAC condition, an IPv4 condition, or an IPv6 condition as a flow detection condition:

- The VLAN tunneling function is not active on the Switch.
- The VLAN tunneling function is active on the Switch, but frames were received by a trunk port.

(2) Filtering of fragmented IPv4 packets

If you filter by using a TCP/UDP header or ICMP 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 and ICMP header are not in those packets. To filter frames that include fragmented packets, specify the MAC header or IP header in the flow detection conditions.

(3) Filtering IPv6 packets that have an extension header

You cannot filter IPv6 packets that have an IPv6 extension header by using a TCP/UDP header or ICMP header as a flow detection condition. To filter packets that have an extension header, specify the MAC header or IPv6 header in the flow detection conditions.

(4) IPv4 protocol detection

The protocol name ah or the protocol number 51 cannot be detected as a filter condition.

(5) Behavior when filter entries are applied

When filter entries are applied to the interfaces on the Switch#, packets may be detected by other filter entries including an implicit discard entry until the specified filter entries are applied. In this case, statistics for the filter entries including the implicit discard entry that detected the packets 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 to add an entry

- When a filter entry is applied when the switch is started, the "copy" operation command is executed, or the "restart vlan" operation command is executed

(6) Behavior 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.

(7) Concurrent behavior with other functions

(a) Statistics of frames discarded due to specific conditions

Frames are discarded when one of the conditions listed below is satisfied. However, if a frame matches a filter entry specified for the receiving-side 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 by the inter-port forwarding block function.
- 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 access, protocol or MAC ports.
- Frames are discarded by the MAC address learning function.
- Frames are discarded by the Layer 2 forwarding block function.
- Frames are discarded by the Layer 2 authentication function.
- When a frame is discarded due to an invalid Layer 2 protocol
- Frames are discarded by IGMP snooping or MLD snooping.
- Frames are discarded by DHCP snooping.
- Fames are discarded by QoS control.
- Frames are discarded by storm control.
- Packets are discarded by IP layer or IPv6 layer forwarding.

(b) Storm detection when using filters

If discards due to filter detection and discards due to storm detection occur at the same time, more frames may be discarded, including frames that should have been relayed.

1.2 Configuration

1.2.1 List of configuration commands

The following table describes the list of configuration commands that are used by filters.

Table 1-9: List of configuration commands

Command name	Description
access-list	Sets an access list used as an IPv4 filter.
deny	Specifies the condition by which the filter discards access.
ip access-group	Applies an IPv4 filter to an Ethernet interface or VLAN interface and enables the IPv4 filter function.
ip access-list extended	Sets an access list used as an IPv4 packet filter.
ip access-list resequence	Re-sequences the sequence numbers that determine the order in which the IPv4 address filter and IPv4 packet filter apply filter conditions.
ip access-list standard	Sets an access list used as an IPv4 address filter.
ipv6 access-list	Sets an access list used as an IPv6 filter.
ipv6 access-list resequence	Re-sequences the sequence numbers that determine the order in which the IPv6 filter applies filter conditions.
ipv6 traffic-filter	Applies an IPv6 filter to an Ethernet interface or VLAN interface and enables the IPv6 filter function.
mac access-group	Applies a MAC filter to an Ethernet interface or VLAN interface and enables the MAC filter function.
mac access-list extended	Sets an access list used as a MAC filter.
mac access-list resequence	Re-sequences the sequence numbers that determine the order in which the MAC filter applies filter conditions.
permit	Specifies the condition by which the filter forwards access.
remark	Specifies supplementary information for the filter.
flow detection mode#	Sets the receiving-side flow detection mode for the filter and QoS control.
flow detection out mode#	Sets the sending-side flow detection mode for the filter.

#

See "Configuration Command Reference Vol. 1, 24. Flow Detection Modes/Flow Performance".

1.2.2 Configuring the receiving-side flow detection mode

The following shows an example of specifying the receiving-side flow detection mode for filtering.

Points to note

You must first set the receiving-side flow detection mode to determine the basic running conditions of the hardware.

Command examples

1. `(config)# flow detection mode layer3-1`

   Enables receiving-side flow detection mode layer3-1.

1.2.3 Configuring the sending-side flow detection mode

The following shows an example of specifying the sending-side flow detection mode for filtering.

Points to note

You must first set the sending-side flow detection mode to determine the basic running conditions of the hardware.

Command examples

1. `(config)# flow detection out mode layer3-2-out`

   Enables sending-side flow detection mode layer3-2-out.

1.2.4 Configuring frame forwarding and discarding by MAC header

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). When this list is created, the command 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 gigabitethernet 1/0/1`

   Switches to the interface mode for port 1/0/1.

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

   Enables the MAC filtering on the receiving side.

1.2.5 Configuring frame forwarding and discarding by IP header and TCP/UDP header

(1) 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 source 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). When this list is created, the command switches to IPv4 address filter 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 source IP address 192.168.0.0/24 network.

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

   Returns to global configuration mode from IPv4 address filtering mode.

4. `(config)# interface vlan 10`

   Switches to the interface mode for VLAN10.

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

   Enables IPv4 filtering on the receiving side.

(2) 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). When this list is created, the command 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`

   Sets an IPv4 packet filter that forwards all frames.

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

   Returns to global configuration mode from IPv4 address filtering mode.

5. `(config)# interface vlan 10`

   Switches to the interface mode for VLAN10.

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

   Enables IPv4 filtering on the receiving side.

(3) Using a range of TCP/UDP port numbers as a flow detection condition

The following shows an example of specifying frame forwarding and discarding based on specification of a range of UDP port numbers as the flow detection condition.

Points to note

When frames are received, flow detection is performed based on the range of destination port numbers in the UDP header, and the frames that match the filter entry are discarded.

Command examples

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

   Creates ip access-list (PORT_RANGE_DENY). When this list is created, the command switches to IPv4 packet filtering mode.

2. `(config-ext-nacl)# deny udp any any range 10 20`

   Sets an IPv4 packet filter that discards packets whose destination port number in the UDP header is in the range from 10 to 20.

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

   Sets an IPv4 packet filter that forwards all frames.

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

   Returns to global configuration mode from IPv4 address filtering mode.

5. `(config)# interface vlan 10`

   Switches to the interface mode for VLAN10.

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

   Enables IPv4 filtering on the receiving side.

(4) Using IPv6 packet as the flow detection condition

The following shows an example of specifying frame forwarding and discarding based on specification of IPv6 packet as the flow detection condition.

Points to note

When frames are received, flow detection is performed based on IP address, and 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)# ipv6 access-list FLOOR_B_PERMIT`

   Creates ipv6 access-list (FLOOR_B_PERMIT). When this list is created, the command switches to IPv6 packet filtering mode.

2. `(config-ipv6-acl)# permit ipv6 2001:100::1/64 any`

   Sets an IPv6 packet filter that forwards frames from source IP address 2001:100::1/64.

3. `(config-ipv6-acl)# exit`

   Returns to global configuration mode from IPv6 packet filtering mode.

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

   Switches to the interface mode for port 1/0/1.

5. `(config-if)# ipv6 traffic-filter FLOOR_B_PERMIT in`

   Enables IPv6 filtering on the receiving side.

1.2.6 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)# access-list 10 permit host 192.168.0.1`

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

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

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

3. `(config-if-range)# ip access-group 10 in`

   Enables IPv4 filtering on the receiving side.

1.3 Operation

Use the "show access-filter" command to make sure that the information you have set is applied.

1.3.1 List of operation commands

The table below describes the list of operation commands that are used by filters.

Table 1-10: List of operation commands

Command name	Description
show access-filter	Shows statistics on the access lists (mac access-list, access-list, ip access-list, and ipv6 access-list) set by the "access group" commands (mac access-group, ip access-group, and ipv6 traffic-filter).
clear access-filter	Clears statistics on the access lists (mac access-list, access-list, ip access-list, and ipv6 access-list) set by the "access group" commands (mac access-group, ip access-group, and ipv6 traffic-filter).

1.3.2 Checking filters

(1) Checking the entries set for an Ethernet interface

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

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

```
> show access-filter 1/0/1 IPX_DENY
Date 20XX/12/01 12:00:00 UTC
Using Port:1/0/1 in
Extended MAC access-list:IPX_DENY
      remark "deny only ipx"
      10 deny any any ipx
         matched packets       :   74699826
      20 permit any any
         matched packets       :     264176
      implicitly denied packets:          0
```

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 behavior when a filter is set for a VLAN interface.

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

```
> show access-filter interface vlan 10 FLOOR_A_PERMIT
Date 20XX/12/01 12:00:00 UTC
Using Interface:vlan 10 in
Standard IP access-list:FLOOR_A_PERMIT
      remark "permit only Floor-A"
      10 permit 192.168.0.0 0.0.0.255 any
         matched packets       :  74699826
      implicitly denied packets:      2698
```

Make sure that "Standard IP access-list" is displayed for the filter for the specified VLAN.

2 Overview of QoS Control

The QoS control function provides bandwidth monitoring, marker, determination of priority, and bandwidth control as 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.

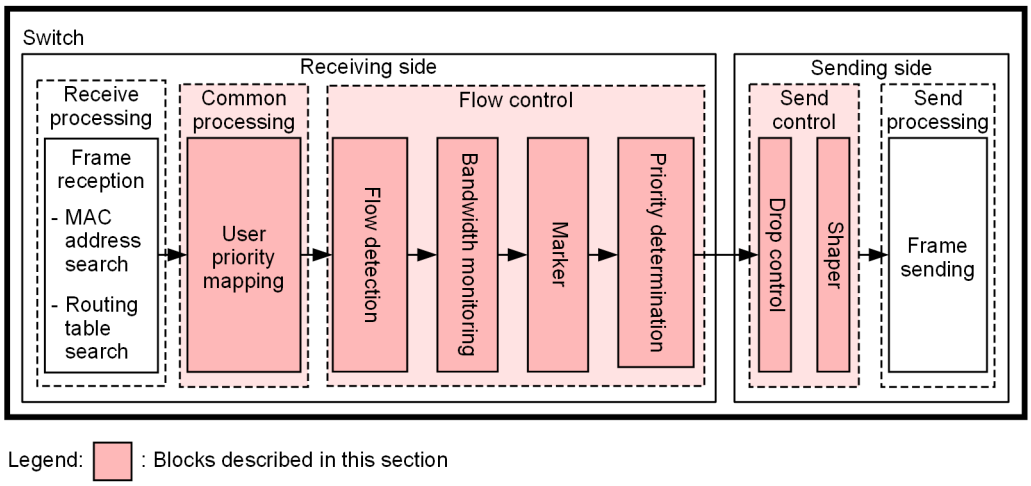
2.1 Structure of QoS control

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 switches



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

Table 2-1: Overview of the functional blocks for QoS control

Section and functional blocks		Function overview
Receive processing section	Frame reception	Receives frames and searches the MAC address table and routing 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 frame that matches a condition, such as MAC address, protocol type, IP address, TCP/UDP port number, or ICMP header.
	Bandwidth monitoring	Monitors the bandwidth of frame flow and assigns a penalty to frames that exceed the bandwidth.
	Marker	Updates the user priority in the DSCP or VLAN tag in the IP header.
	Priority determination	Determines the priority of frames and the queuing priority, which indicates how easily a frame can be discarded.
Send control section	Drop control	Controls whether frames can be queued or dropped according to the packet priority and queue status.
	Shaper	Controls the output order of frames from queues and the output bandwidth.

Section and functional blocks		Function 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 priority over user priority mapping. You can also use flow control to employ bandwidth monitoring and marker in addition to priority determination. Bandwidth monitoring, marker, and priority determination can run concurrently for the frames detected by flow detection.

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

Notes

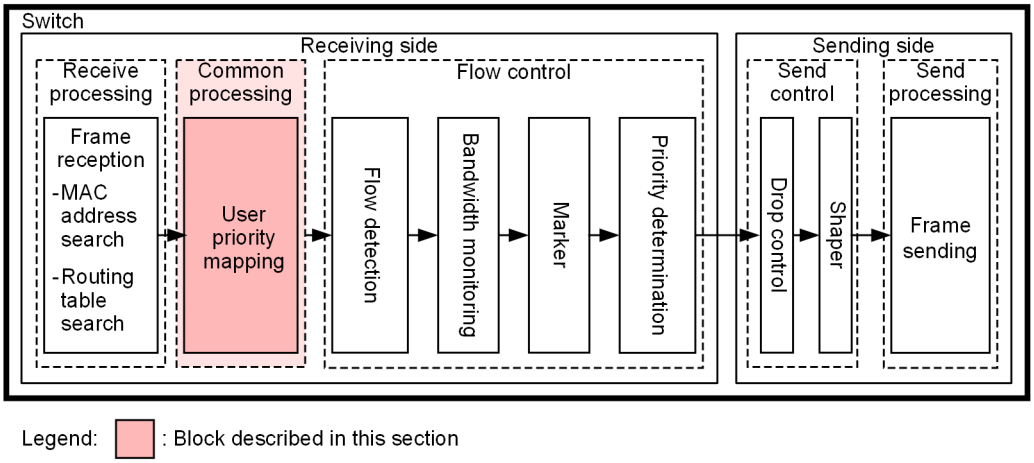
Keep the following in mind when using the QoS control.

- If the packets processing performance is exceeded for the AX3660S-48XT4QW, AX-3660S-24X4QW, and AX3660S-48X4QW, the packets may be discarded regardless of the setting of flow detection.
- Flow control or send control cannot be set on a stack port.

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 function 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 unicast frames. For broadcast frames and multicast frames, the CoS value determined by priority determination is used because user priority mapping is not performed.

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 "3.10.3 CoS mapping function".

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 priority over user priority mapping.

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

Frame type		Mapped CoS values
VLAN tag	User priority value	
Without VLAN tag	—	3
With VLAN tag#	0	0
	1	1
	2	2
	3	3
	4	4
	5	5

Frame type		Mapped CoS values
VLAN tag	User priority value	
	6	6
	7	7

Legend: —: Not applicable

#: In the following case, mapping is always performed with a CoS value of 3 regardless of the user priority value that is set when the frame was received.

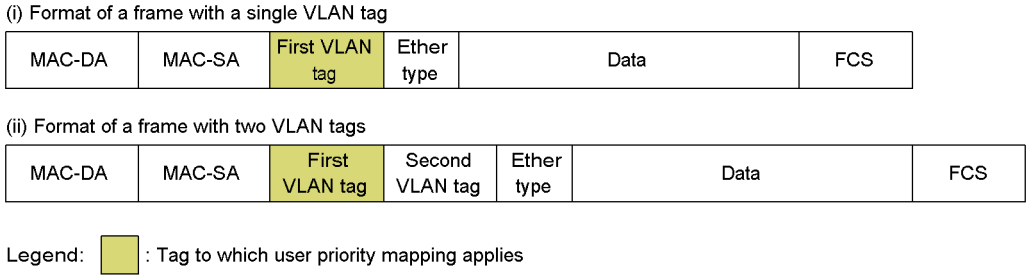
- Frames received on ports on which VLAN tunneling is set

2.2.2 Note on user priority mapping

(1) Applicability of user priority mapping

When a Switch performs Layer 3 forwarding, user priority mapping is in effect for frames that have two or fewer VLAN tags. If a frame that has three or more VLANs tag is received, the frame is discarded. The following figure shows the VLAN tag to which user priority mapping applies.

Figure 2-3: Tag to which user priority mapping applies



2.3 Configuration common to QoS control

2.3.1 List of configuration commands

The following table describes the configuration commands for QoS control.

Table 2-3: List of configuration commands

Command name	Description
ip qos-flow-group	Applies an IPv4 QoS flow list to an Ethernet interface or VLAN 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.
ipv6 qos-flow-group	Applies an IPv6 QoS flow list to an Ethernet interface or VLAN and enables IPv6 QoS control.
ipv6 qos-flow-list	Sets the QoS flow list used for IPv6 QoS flow detection.
ipv6 qos-flow-list resequence	Resets the sequence number for the order in which the conditions in the IPv6 QoS flow list are applied.
mac qos-flow-group	Applies a MAC QoS flow list to an Ethernet interface or VLAN 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 behavior 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-shape rate	Sets port bandwidth control for an Ethernet interface.
flow action-change arp-discard-class#	Changes the queuing priority of ARP broadcast frames.
flow action-change arp-reply-cos#	Changes the CoS value of ARP reply broadcast frames.
flow action-change cos#	Sets the function for changing which frames are subject to priority determination of the QoS function.
flow detection mode#	Sets the receiving-side flow detection mode for the filter and QoS control.

#
See "Configuration Command Reference Vol. 1, 24. Flow Detection Modes/Flow Performance".

2.4 Operations common to QoS control

2.4.1 List of operation commands

The following table describes the list of operation commands for QoS control.

Table 2-4: List of operation commands

Command name	Description
show qos-flow	Shows statistics on the QoS flow lists (mac qos-flow-list, ip qos-flow-list, and ipv6, qos-flow-list) set by the QoS flow group commands (mac qos-flow-group, ip qos-flow-group, and ipv6 qos-flow-group).
clear qos-flow	Clears statistics on the QoS flow lists (mac qos-flow-list, ip qos-flow-list, and ipv6, qos-flow-list) set by the QoS flow group commands (mac qos-flow-group, ip qos-flow-group, and ipv6 qos-flow-group).
show qos queueing	Shows 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, bandwidth monitoring, marker, and priority determination) for the Switch.

3.1 Description of flow detection

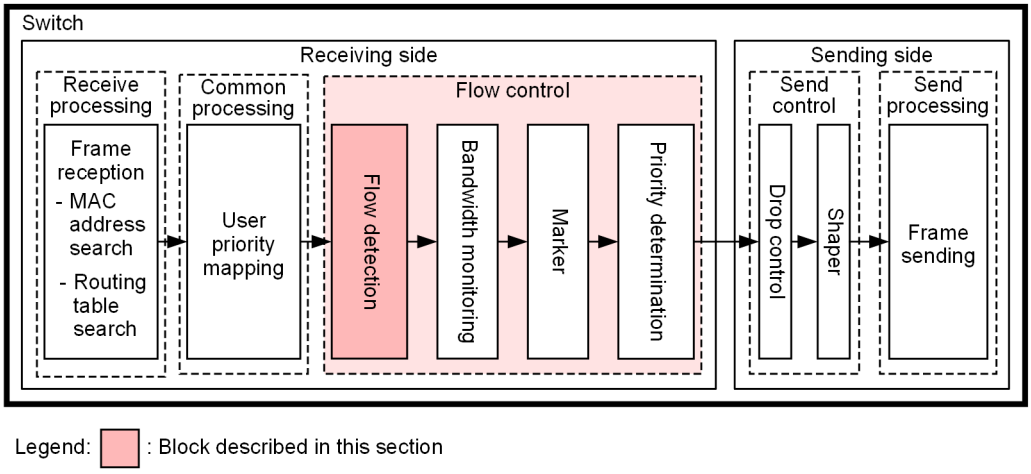
The flow detection function detects a flow, which is a sequence of frames, based on conditions, such as the MAC header, IP header, TCP header, and ICMP header. QoS flow lists are used to set up flow detection. For details about the QoS flow lists, see "3.1.3 QoS flow lists".

Enables the QoS function by applying an IPv6 QoS flow list to an Ethernet interface or a VLAN interface. For AX3640S series switches, the Switch is able to perform flow detection for Ethernet V2 format and IEEE 802.3 SNAP/RFC 1042 format frames on the sending-side Ethernet interface and VLAN interface.

If flow detection is specified for the receiving-side interface, flow detection is performed at the point of reception on the Ethernet interface for both the Ethernet interface and the VLAN interface. Note that the frames received by the Switch are also subject to the flow detection.

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 Receiving-side flow detection mode

The Switch provides receiving-side flow detection modes for network configuration and an operation mode. The receiving-side flow detection modes determine the distribution pattern of filter entries and QoS entries for the receiving-side interface. For the entry distribution, refer to "Configuration Guide Vol. 1, 3 Capacity Limit", and select the mode according to your operating requirements.

Use the "flow detection mode" command to specify the receiving-side flow detection mode. The selected receiving-side flow detection mode applies to both filters and QoS. To change the receiving-side flow detection mode, delete all the following commands set for the receiving-side and sending-side interfaces and the "ip verify source" command of DHCP snooping.

- mac access-group
- ip access-group
- ipv6 traffic-filter
- mac qos-flow-group
- ip qos-flow-group
- ipv6 qos-flow-group

Furthermore, if you change the receiving-side flow detection mode to the receiving-side flow detection mode that does not support policy-based routing, you must delete the following commands in addition to these commands.

- policy-list

- policy-list default-aging-interval
- policy-list default-init-interval

If the IP unset VLAN suppression mode of the receiving-side flow detection mode is set, it controls IP packets (including ARP) in VLANs where the "ip address" configuration command is not set, and IPv6 packets in VLANs where the "ipv6 enable" configuration command is not set, so that they are not transferred to the CPU. However, when using any of the following functions, IP packets that need to be controlled by the target function are transferred to the CPU.

- VXLAN PMTU function
- IGMP snooping
- MLD snooping
- Layer 2 authentication
- DHCP snooping (However, dynamic ARP inspection cannot be used along with the IP unset VLAN suppression mode.)

Note that if you do not specify the receiving-side flow detection mode, layer3-2 is set as the default mode.

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

Table 3-1: Flow detection modes for the receiving side and flow behaviors

Receiving-side flow Detection mode name	Purpose	Flow operations
layer3-1	• To perform flow control for IP packets and other frames • To perform flow control specialized for IPv4 packets	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-2	• To perform flow control specialized for IPv4 packets	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-6	• To perform flow control specialized for IPv4 or IPv6 packets • To use the policy-based routing	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-dhcp-1	• To perform flow control specialized for IPv4 packets and use the terminal filters of DHCP snooping	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-mirror-1	• To use flow control and policy-based mirroring of IP packets and other frames • To perform flow control and policy-based mirroring specialized for IPv4 packets	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.

Receiving-side flow Detection mode name	Purpose	Flow operations
layer3-mirror-2	• To perform flow control and policy-based mirroring specialized for IPv4 packets	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-mirror-3	• To use flow control specialized for IPv4 or IPv6 packets • To use policy-based mirroring of IP packets and other frames • To perform policy-based mirroring specialized for IPv4 packets • To use the policy-based routing	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-mirror-4	• To use flow control specialized for IPv4 or IPv6 packets • To use policy-based mirroring specialized for IPv6 packets • To use the policy-based routing	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-mirror-5	• To use flow control specialized for IPv4 or IPv6 packets • To use policy-based mirroring of IP packets and other frames • To use policy-based mirroring of IPv4 and IPv6 packets • To use the policy-based routing	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-suppress-1	• To use the IP unset VLAN suppression mode • To perform flow control for IP packets and other frames • To perform flow control specialized for IPv4 packets	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-suppress-2	• To use the IP unset VLAN suppression mode • To perform flow control specialized for IPv4 or IPv6 packets • To use the policy-based routing	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.

Receiving-side flow Detection mode name	Purpose	Flow operations
layer3-suppress-dhcp-1	• To use the IP unset VLAN suppression mode • To perform flow control specialized for IPv4 packets and use the terminal filter of DHCP snooping	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-suppress-mirror-1	• To use the IP unset VLAN suppression mode • To use flow control and policy-based mirroring of IP packets and other frames • To perform flow control and policy-based mirroring specialized for IPv4 packets	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
layer3-suppress-mirror-2	• To use the IP unset VLAN suppression mode • To use filters for IPv4 and IPv6 packets • To use policy-based mirroring of IPv4 and IPv6 packets • To use the policy-based routing	For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.
custom	Use this mode to select the functions listed below, assign the function to each entry block in the hardware table, and set the accommodation conditions flexibly • IP unset VLAN suppression mode • Flow control for IPv4 or IPv6 packets and other frames • Policy-based mirroring for IPv4 or IPv6 packets and other frames • Policy-based routing • Terminal filter of DHCP snooping	Frames are detected based on the MAC header, which contains a MAC address and Ethernet type. For IPv4 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header. For IPv6 packets, frames are detected based on the IP header, TCP/UDP header, and ICMP header.

3.1.2 Flow detection conditions

To perform flow detection, specify the conditions for identifying the flow in the configuration. The following describes the flow detection conditions for the receiving-side interface.

(1) Flow detection conditions for the receiving-side interface

The following table describes the flow detection conditions that can be specified for the receiving-side interface.

Table 3-2: Flow detection conditions that can be specified for the receiving-side interface

Type		Configuration items	
MAC conditions	Configuration	VLAN ID[#1]	
	MAC headers	Source MAC address	
		Destination MAC address	
		Ethernet type	
		User priority[#2]	
IPv4 conditions	Configuration	VLAN ID[#1]	
	MAC header	User priority[#2]	
	IPv4 header[#3]	Upper layer protocol	
		Source IP address	
		Destination IP address	
		ToS	
		DSCP	
		Precedence	
	IPv4-TCP header	Source port number	Single specification (eq)
			Range specification (range)[#4]
		Destination port number	Single specification (eq)
			Range specification (range)[#4]
		TCP control flag[#5]	
	IPv4-UDP header	Source port number	Single specification (eq)
			Range specification (range)[#4]
		Destination port number	Single specification (eq)
			Range specification (range)[#4]
	IPv4-ICMP header	ICMP type value	
		ICMP code value	
IPv6 conditions	Configuration	VLAN ID[#1]	
	MAC header	User priority[#2]	
	IPv6 header[#6]	Upper layer protocol	
		Source IP address	
		Destination IP address	
		Traffic class	
		DSCP	

Type		Configuration items	
	IPv6-TCP header	Source port number	Single specification (eq)
			Range specification (range)#4
		Destination port number	Single specification (eq)
			Range specification (range)#4
		TCP control flag#5	
	IPv6-UDP header	Source port number	Single specification (eq)
			Range specification (range)#4
		Destination port number	Single specification (eq)
			Range specification (range)#4
	IPv6-ICMP header	ICMP type value	
		ICMP code value	

#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.

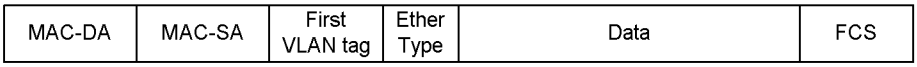
#2

The user priority cannot be detected for the following frames. Therefore, user priority "3" is always detected.

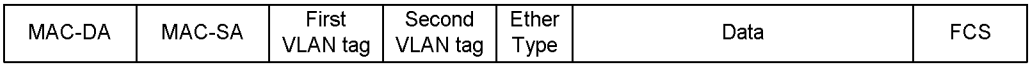
- Frames that do not have a VLAN tag
- Frames received on ports on which VLAN tunneling is set

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.

(i) Format of a frame with a single VLAN tag



(ii) Format of a frame with two VLAN tags

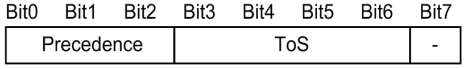


#3

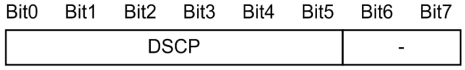
Supplementary note for the ToS field specification

ToS: Value of bits 3 to 6 in the ToS field.

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



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



#4

For details about capacity limits of the TCP/UDP port number detection pattern, see "Configuration Guide Vol. 1, 3.5 Filters, QoS, and policy-based mirroring".

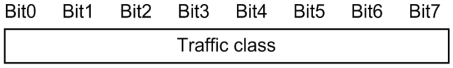
#5

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

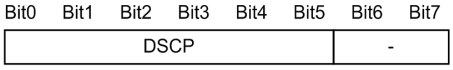
#6

Supplementary note for the traffic class field specification

Traffic class: The value of the traffic class field.



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



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 conditions	QoS flow list	Receiving-side flow detection mode	Detectable frame type		
			Non-IP	IPv4	IPv6
MAC conditions	mac qos-flow-list	layer3-1, layer3-mirror-1, layer3-suppress-1, layer3-suppress-mirror-1, custom	Y	Y	Y
IPv4 conditions	ip qos-flow-list	layer3-1, layer3-2, layer3-6, layer3-dhcp-1, layer3-mirror-1, layer3-mirror-2, layer3-mirror-3, layer3-mirror-4, layer3-mirror-5, layer3-suppress-1, layer3-suppress-2, layer3-suppress-dhcp-1, layer3-suppress-mirror-1, custom	—	Y	—

Flow detection conditions	QoS flow list	Receiving-side flow detection mode	Detectable frame type		
			Non-IP	IPv4	IPv6
IPv6 conditions	ipv6 qos-flow-list	layer3-6, layer3-mirror-3, layer3-mirror-4, layer3-suppress-2, custom	—	—	Y

Legend: Y: Can be detected; —: Cannot be detected

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) Behavior when multiple flow detection conditions are simultaneously set

If QoS flow detection is performed for incoming frames of the interface when multiple flow detection conditions are set, frames are detected in the order shown in the below table. Multiple QoS entries are not matched.

Table 3-4: Flow detection order

Flow detection order	QoS flow list	Interface
1	mac qos-flow-list	Ethernet
2		VLAN
3	ip qos-flow-list	Ethernet
4		VLAN
5	ipv6 qos-flow-list	Ethernet
6		VLAN

3.1.4 Notes on using flow detection

(1) QoS flow detection for frames with VLAN tags

You cannot perform QoS flow detection for frames with three or more VLAN tags by using an Ethernet type for a MAC condition, an IPv4 condition, or an IPv6 condition specified as a flow detection condition.

Either of the following conditions must be satisfied to perform QoS flow detection on the receiving side by an Ethernet type for a MAC condition, an IPv4 condition, or an IPv6 condition specified as the flow detection condition for a frame that has two VLAN tags:

- The VLAN tunneling function is not active on the Switch.
- The VLAN tunneling function is active on the Switch, but frames were received by a trunk port.

(2) QoS flow detection for fragmented IPv4 packets

If you perform QoS flow detection by using a TCP/UDP header or ICMP 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 and ICMP header are 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.

(3) QoS flow detection for IPv6 packets that have an extension header

You cannot perform QoS flow detection for IPv6 packets that have an IPv6 extension header by using a TCP/UDP header or ICMP header as a flow detection condition. To perform QoS flow detection for such packets, specify the MAC header or IPv6 header in the flow detection conditions.

(4) IPv4 protocol detection

The protocol name ah or the protocol number 51 cannot be detected as flow conditions.

(5) Behavior when a QoS entry is applied

When QoS entries are applied to the interfaces on the Switch#, packets may be detected by other QoS entries until the specified Qos entries are applied. In this case, statistics for the QoS entries that detected packets are collected.

#

- When a QoS list containing one or more entries is applied to the interface by using the QoS flow group command
- When a QoS flow list is applied by using the QoS flow group command to add an entry
- When a QoS entry is applied when the switch is started, the "copy" operation command is executed, or the "restart vlan" operation command is executed

(6) Behavior 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.

(7) Concurrent behavior with other functions

Frames are discarded when one of the conditions listed below is satisfied. However, if a frame matches a QoS entry specified for the receiving-side 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 by the inter-port forwarding block function.
- 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 access, protocol or MAC ports.
- Frames that match a filter entry specifying discard (including an implicit discard entry) are received.
- Frames are discarded by the MAC address learning function.
- Frames are discarded by the Layer 2 forwarding block function.
- Frames are discarded by the Layer 2 authentication function.
- When a frame is 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.
- Packets are discarded by IP layer or IPv6 layer forwarding.

3.2 Flow detection configuration

3.2.1 Configuring the receiving-side flow detection mode

The following shows an example of specifying the receiving-side flow detection mode for QoS control.

Points to note

You must first set the receiving-side flow detection mode to determine the basic operating conditions of the hardware.

Command examples

1. `(config)# flow detection mode layer3-1`

   Enables receiving-side flow detection mode layer3-1.

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). When this list is created, control 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 gigabitethernet 1/0/1-4`

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

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

   Enables the IPv4 QoS flow list on the receiving side.

3.2.3 Configuring a range of TCP/UDP port numbers for QoS control

The following shows an example of setting QoS control based on specification of a range of UDP port numbers as the flow detection condition.

Points to note

When frames are received, flow detection for QoS control is performed based on the range of destination port numbers in the UDP header.

Command examples

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

   Creates an IPv4 QoS flow list (QOS-LIST1). When this list is created, control switches to IPv4 QoS flow list mode.

2. `(config-ip-qos)# qos udp any any range 10 20 action cos 6`

   Sets the range of destination port numbers from 10 to 20 as the flow detection condition in the UDP header, and then sets the CoS value to 6 in the QoS flow list.

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

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

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

   Switches to interface mode for port 1/0/1.

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

   Enables the IPv4 QoS flow list on the receiving side.

3.3 Flow detection operation

To check whether the information you have set is applied, use the "show qos-flow" command.

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

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

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

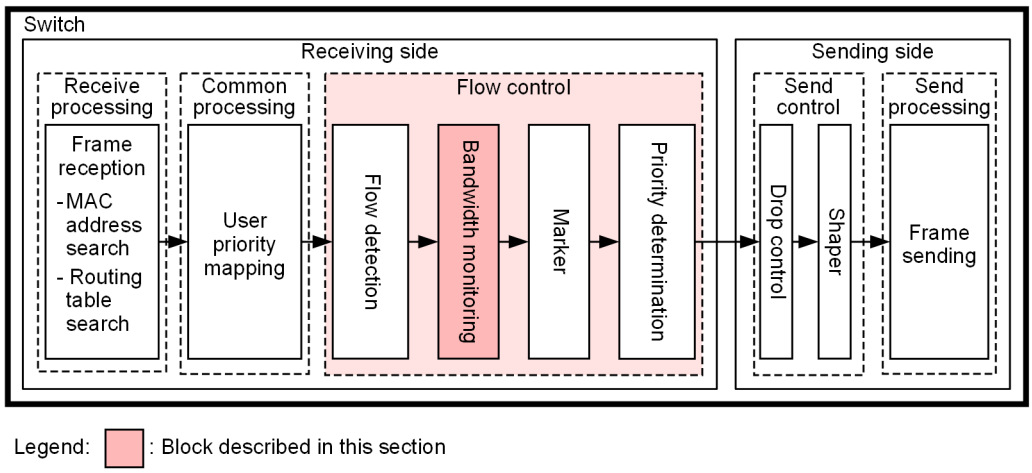
```
> show qos-flow 1/0/1
Date 20XX/12/01 12:00:00 UTC
Using Port:1/0/1 in
IP qos-flow-list:QOS-LIST1
      10 ip any host 192.168.100.10 action replace-user-priority 6
         matched packets       :  74699826
```

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

3.4 Description of bandwidth monitoring

Bandwidth monitoring is the function used to monitor the bandwidth of the traffic flows subject to flow detection. The following figure shows the positioning of the bandwidth monitoring block described in this section.

Figure 3-3: Positioning of the bandwidth monitoring block



3.4.1 Bandwidth monitoring

The bandwidth monitoring function monitors bandwidth based on the frame length (from the MAC address to the FCS) or the number of frames detected by flow detection. Frames that are forwarded as being within the specified monitoring bandwidth are referred to as compliant frames. Frames penalized for exceeding the monitoring bandwidth are referred to as non-compliant frames.

The compliance of frames detected by flow detection with the monitoring bandwidth limit is determined by using the Token Bucket algorithm.

Burst size is the maximum frame capacity that allows burst traffic to be transferred as compliant frame. The following table describes the characteristics of the burst size.

Table 3-5: Burst size characteristics

Burst size	Features
Smaller	The dropping of burst traffic is relatively easy. If traffic is sent while communication is not being performed, the send bandwidth fluctuations are relatively small.
Larger	The dropping of burst traffic is relatively difficult. If traffic is sent while communication is not being performed, the send bandwidth fluctuations are relatively large.

The bandwidth monitoring function consists of minimum bandwidth monitoring and maximum bandwidth control. The following table describes the types of penalties that can be used for minimum bandwidth monitoring and maximum bandwidth control.

Table 3-6: Types of penalties that can be used for minimum bandwidth monitoring and maximum bandwidth control

Penalty for non-compliant frames	Type of bandwidth monitoring	
	Minimum bandwidth monitoring	Maximum bandwidth controls
Discard	—	Y

Penalty for non-compliant frames	Type of bandwidth monitoring	
	Minimum bandwidth monitoring	Maximum bandwidth controls
Queuing priority change	Y	—
DSCP rewrite	Y	—

Legend: Y: The penalty can be used; —: The penalty cannot be used.

Penalties for rewriting DSCP do not work for the following frames:

- IPv4 and IPv6 packets exceeding the MTU
- Frames whose TTL is set to 1
- Frames whose hop limit is set to 1
- Frames with an IP option
- Frames with an IPv6 extension header
- IPv4 or IPv6 packets with an unknown receiver address

● Bandwidth monitoring when stack is configured

In a stack configuration, the support status of bandwidth monitoring varies depending on the interface type. The following table describes interface types and their corresponding bandwidth monitoring.

Table 3-7: Interface types and their bandwidth monitoring

Interface type	Bandwidth monitoring
Ethernet interface	Y
VLAN interface within a member switch	Y
VLAN interface across different member switches	—

Legend: Y: Supported; —: Not supported

● Bandwidth monitoring for multiple flows (summarized bandwidth monitoring)

Summarized bandwidth monitoring collects frames detected by multiple flow detections into a single bandwidth and monitors the bandwidth.

The flows targeted for summarized bandwidth monitoring are combinations of all interface types (Ethernet interface, VLAN interface) and all flow detection conditions (MAC conditions, IPv4 conditions, IPv6 conditions). However, in a stack configuration, a combination of interfaces belonging only to the same switch is supported.

3.4.2 Bandwidth non-compliance notification

Bandwidth non-compliance notification is the function that periodically monitors increases in the number of bandwidth non-compliance frames (maximum bandwidth non-compliance or minimum bandwidth non-compliance) for QoS entries that monitor bandwidth, and outputs operation messages and sends SNMP notifications. Describes the bandwidth status and monitoring cycle of the target QoS entry.

(1) Bandwidth status

Bandwidth non-compliance notification periodically monitors the number of bandwidth non-compliance frames for each QoS entry targeted for bandwidth non-compliance notification and determines the bandwidth status. The bandwidth status includes bandwidth compliance status and bandwidth non-compliance status, and the initial status is bandwidth compliance status.

Also, the QoS entry whose bandwidth status has changed notifies the change of bandwidth status.

(a) Transition from bandwidth compliance status to bandwidth non-compliance status

The transition from bandwidth compliance status to bandwidth non-compliance status is performed based on the bandwidth non-compliance count and monitoring count set by the configuration command.

The target QoS entry is periodically monitored, and if the number of times the number of bandwidth non-compliance frames increases from the time of the previous monitoring (bandwidth non-compliance count) reaches the set bandwidth non-compliance count, it transitions to bandwidth non-compliance status. If the status does not transition to bandwidth non-compliance status by the set number of monitoring times, the bandwidth compliance status continues, and the bandwidth non-compliance count and monitoring count are reset to the initial values and restarted.

(b) Transition from bandwidth non-compliance status to bandwidth compliance status

The transition from bandwidth non-compliance status to bandwidth compliance status is performed based on the bandwidth compliance count and monitoring count set by the configuration command.

The target QoS entry is periodically monitored, and if the number of times the number of bandwidth non-compliance frames has not changed since the previous monitoring (bandwidth compliance count) reaches the set bandwidth compliance count, it transitions to bandwidth compliance status. If the status does not change to bandwidth compliance status by the set monitoring count, bandwidth non-compliance status continues, and the bandwidth compliance count and monitoring count are reset to the initial values and restarted.

(2) Monitoring interval of bandwidth non-compliance notification

The monitoring interval of bandwidth non-compliance notification is specified by a configuration command. The QoS entries targeted for bandwidth non-compliance notification are monitored for the number of entries set by the configuration command per second.

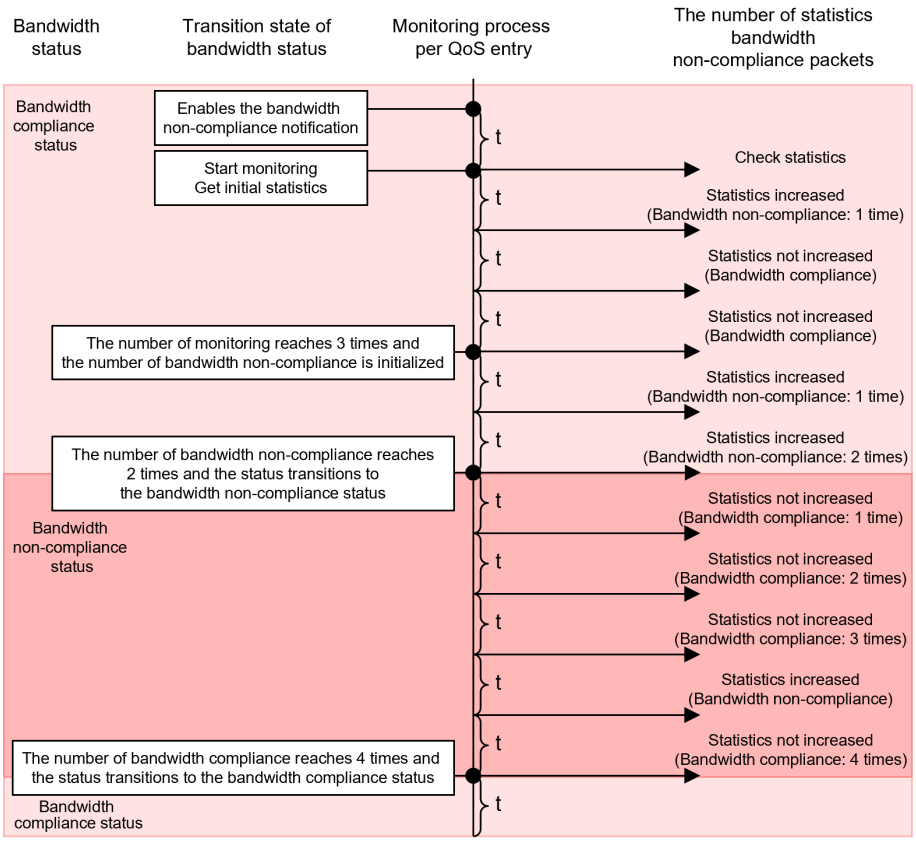
For example, if the configuration command sets the number of entries to 100 and the number of QoS entries targeted for bandwidth non-compliance notification is 110, 100 entries are monitored in the first second, and the remaining 10 entries are monitored in the second.

In a stack configuration, each member switch monitors the target QoS entries for bandwidth non-compliance notification for each member switch.

(3) Example of transition in bandwidth status

The following figure shows the sequence when the bandwidth status transitions. In this example, bandwidth status transitions from bandwidth compliance status to bandwidth non-compliance status, and then from bandwidth non-compliance status to bandwidth compliance status. The bandwidth non-compliance count in bandwidth compliance status is 2 times, the monitoring count is 3 times, the bandwidth compliance count in bandwidth non-compliance status is 4 times, and the monitoring count is 5 times.

Figure 3-4: Transition sequence in bandwidth status



Legend: t : Monitoring cycle

3.4.3 Statistics that can be collected when bandwidth monitoring is used

The statistics that can be collected depend on the type of bandwidth monitoring, as described in the following table.

Table 3-8: Statistics that can be collected for bandwidth monitoring

Type of bandwidth monitoring	Statistics collection			
	Maximum bandwidth non-compliance	Maximum bandwidth compliance	Minimum bandwidth non-compliance	Minimum bandwidth compliance
Minimum bandwidth monitoring	—	—	Y	Y
Maximum bandwidth controls	Y	Y	—	—
Combined minimum bandwidth monitoring and maximum bandwidth controls	Y	Y	—	—

Legend: Y: Can be collected; —: Cannot be collected

3.4.4 Notes on using bandwidth monitoring

(1) Relationship between bandwidth monitoring and transmission Ethernet interface/ transmission queue

Compliant frames may be discarded on the transmission Ethernet interface or the transmission queue in the following cases:

- When the monitoring bandwidth value specified for bandwidth monitoring is set to a value greater than the bandwidth value of the transmission Ethernet interface or transmission queue of the target flow
- When a flow that does not use bandwidth monitoring and a flow that uses bandwidth monitoring are sent to the same transmission Ethernet interface or transmission queue

In particular, when using multiple bandwidth monitoring for multiple flows, pay attention to the total monitoring bandwidth value for each bandwidth monitoring.

(2) Bandwidth monitoring for protocol control frames

Protocol control frames are also subject to bandwidth monitoring on the Switch. Therefore, because a protocol control frame might also be discarded as a non-compliant frame in maximum bandwidth control, allocate the maximum bandwidth only after reviewing whether the protocol control frames will be sent to the Switch.

(3) Using maximum bandwidth control for TCP frames

When you use maximum bandwidth control, repeated slow startup of TCP might result in an extremely slow data transfer rate.

To avoid this problem, use minimum bandwidth monitoring to specify a behavior that lowers the queuing priority so that frames can be discarded more easily. This setting ensures that frames that exceed the contracted bandwidth will not be discarded immediately, but will be discarded only when the output line is congested.

(4) Concurrent behavior with other functions

- If frames that match a filter entry specifying discard (including an implicit discard entry) are received, they are discarded but are still subject to bandwidth monitoring
- If a bandwidth monitoring violation and a storm detection occur simultaneously, more frames may be discarded, including frames that should have been relayed.

3.5 Configuration of bandwidth monitoring

3.5.1 Configuring maximum bandwidth control

Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then bandwidth monitoring using maximum bandwidth control is performed.

Command examples

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

   Creates an IPv4 QoS flow list (QOS-LIST1). When this list is created, control switches to IPv4 QoS flow list mode.

2. `(config-ip-qos)# qos ip any host 192.168.100.10 action max-rate 5M max-rate-burst 512`

   Configures the IPv4 QoS flow list for flows whose destination IP address is 192.168.100.10. The command sets for maximum bandwidth control a monitoring bandwidth of 5 Mbit/s and a burst size of 512 KB.

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

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

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

   Switches to interface mode for port 1/0/1.

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

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

3.5.2 Configuring the queuing priority for non-compliance in minimum bandwidth monitoring

Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then minimum bandwidth monitoring is performed. The queuing priority of any non-compliant frames found during minimum bandwidth monitoring is changed.

Command examples

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

   Creates an IPv4 QoS flow list (QOS-LIST2). When this list is created, control switches to IPv4 QoS flow list mode.

2. `(config-ip-qos)# qos ip any host 192.168.110.10 action min-rate 1M min-rate-burst 64 penalty-discard-class 1`

   Configures the IPv4 QoS flow list for flows whose destination IP address is 192.168.110.10. The command sets a minimum monitoring bandwidth of 1 Mbit/s, a minimum-monitoring-bandwidth burst size of 64 KB, and a queuing priority of 1 for non-compliant frames in minimum bandwidth monitoring.

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

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

4. `(config)# interface gigabitethernet 1/0/3`

   Switches to interface mode for port 1/0/3.

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

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

3.5.3 Configuring DSCP rewrite for non-compliant minimum bandwidth monitoring in units of the number of frames

The following describes how to perform minimum bandwidth monitoring in units of the number of frames (changing the DSCP for non-compliant frames) 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 bandwidth monitoring using a minimum bandwidth (min-pps-rate) in units of the number of frames is performed. The DSCP value of a frame that does not comply is changed.

Command examples

1. `(config)# ip qos-flow-list QOS-LIST3`

   Creates an IPv4 QoS flow list (QOS-LIST3). When this list is created, control switches to IPv4 QoS flow list mode.

2. `(config-ip-qos)# qos ip any host 192.168.120.10 action min-pps-rate 10000 min-packet-burst 64 penalty-dscp 8`

   Configures the IPv4 QoS flow list for flows whose destination IP address is 192.168.120.10. The command sets a minimum monitoring bandwidth of 10000packet/s, a minimum-monitoring-bandwidth burst size of 64 packets, and DSCP value of 8 for non-compliant frames in minimum bandwidth monitoring.

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

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

4. `(config)# interface gigabitethernet 1/0/5`

   Switches to interface mode for port 1/0/5.

5. `(config-if)# ip qos-flow-group QOS-LIST3 in`

   Enables the IPv4 QoS flow list (QOS-LIST3) on the receiving side.

3.5.4 Configuring the combined use of maximum bandwidth control and minimum bandwidth monitoring

The following describes how to perform maximum bandwidth control and minimum bandwidth monitoring (updating the DSCP value of non-compliant frames) on certain types of flows.

Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then bandwidth monitoring using maximum bandwidth control and minimum bandwidth monitoring is performed. The DSCP value of any non-compliant frames found during minimum bandwidth monitoring is changed.

Command examples

1. `(config)# ip qos-flow-list QOS-LIST4`

   Creates an IPv4 QoS flow list (QOS-LIST4). When this list is created, control switches to IPv4 QoS flow list mode.

2. `(config-ip-qos)# qos ip any host 192.168.130.10 action max-rate 5M max-rate-burst 512 min-rate 1M min-rate-burst 64 penalty-dscp 8`

   Configures the IPv4 QoS flow list for flows whose destination IP address is 192.168.130.10. The command sets a monitoring bandwidth for maximum bandwidth control of 5 Mbit/s, a maximum-bandwidth-control burst size of 512 KB, a minimum monitoring bandwidth of 1 Mbit/s, a minimum-monitoring-bandwidth burst size of 64 KB, and a DSCP value of 8 for non-compliant frames in minimum bandwidth monitoring.

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

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

4. `(config)# interface gigabitethernet 1/0/7`

   Switches to interface mode for port 1/0/7.

5. `(config-if)# ip qos-flow-group QOS-LIST4 in`

   Enables the IPv4 QoS flow list (QOS-LIST4) on the receiving side.

3.5.5 Configuring the summarized bandwidth monitoring

Set the summarized bandwidth monitoring when you want to collectively monitor multiple flows in one bandwidth.

Points to note

Sets a summarized bandwidth monitoring that performs maximum bandwidth control and minimum bandwidth monitoring, and set a summarized bandwidth monitoring that performs flow detection for multiple destination IP addresses when a frame is received. The DSCP value of any non-compliant frames found during minimum bandwidth monitoring is changed.

Command examples

1. `(config)# aggregate-policer POLICER-LIST4 in max-rate 5M max-rate-burst 512 min-rate 1M min-rate-burst 64 penalty-dscp 8`

   Creates a summarized bandwidth monitoring list (POLICER-LIST4) with a monitoring bandwidth for maximum bandwidth control of 5 Mbit/s, a maximum-bandwidth-control burst size of 512 KB, a minimum monitoring bandwidth of 1 Mbit/s, a minimum-monitoring-bandwidth burst size of 64 KB, and a DSCP value of 8 for non-compliant frames in minimum bandwidth monitoring. By creating this list, you can specify the summarized bandwidth monitoring list (POLICER-LIST4) in the action parameter of the QoS flow list.

2. `(config)# ip qos-flow-list QOS-LIST4`

   Creates an IPv4 QoS flow list (QOS-LIST4). When this list is created, control switches to IPv4 QoS flow list mode.

3. `(config-ip-qos)# qos ip any host 192.168.130.10 action aggregate-policer POLICER-LIST4`

   Sets an IPv4 QoS flow list that specifies the summarized bandwidth monitoring list (POLICER-LIST4) for the flow with the destination IP address of 192.168.130.10.

4. `(config-ip-qos)# qos ip any host 192.168.131.10 action aggregate-policer POLICER-LIST4`

   Sets an IPv4 QoS flow list that specifies the summarized bandwidth monitoring list (POLICER-LIST4) for the flow with the destination IP address of 192.168.131.10.

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

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

6. `(config)# interface gigabitethernet 1/0/7`

   Switches to interface mode for port 1/0/7.

7. `(config-if)# ip qos-flow-group QOS-LIST4 in`

   Enables the IPv4 QoS flow list (QOS-LIST4) on the receiving side.

3.5.6 Configuring the bandwidth non-compliance notification

Set the maximum bandwidth control for a specific flow to output an operation message and send an SNMP notification when there is a bandwidth non-compliance.

Points to note

When frames are received, first flow detection is performed based on the destination IP address, and then bandwidth monitoring using maximum bandwidth control and bandwidth non-compliance notification are performed.

Command examples

1. `(config)# ip qos-flow-list QOS-LIST4`

   Creates an IPv4 QoS flow list (QOS-LIST4). When this list is created, control switches to IPv4 QoS flow list mode.

2. `(config-ip-qos)# qos ip any host 192.168.130.10 action max-rate 5M max-rate-burst 512 log trap`

   For a flow whose destination IP address is 192.168.130.10, the command sets for maximum bandwidth control a monitoring bandwidth of 5 Mbit/s and a burst size of 512 KB, and sets an output of operation message and the sending of SNMP notification as a bandwidth non-compliance notification.

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

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

4. `(config)# flow rate-alarm exceed-count 3 100`

   Enables the bandwidth non-compliance notification. Sets the bandwidth non-compliance count to 3 times and the monitoring count in the bandwidth compliance status to 100 times.

5. `(config)# interface gigabitethernet 1/0/7`

   Switches to interface mode for port 1/0/7.

6. `(config-if)# ip qos-flow-group QOS-LIST4 in`

   Enables the IPv4 QoS flow list (QOS-LIST4) on the receiving side.

3.6 Operation for bandwidth monitoring

To check whether the information you have set is applied, use the "show qos-flow" command.

3.6.1 Checking maximum bandwidth control

The following figure shows how to check maximum bandwidth control.

Figure 3-5: Checking maximum bandwidth control

```
> show qos-flow 1/0/1
Date 20XX/12/01 13:00:00 UTC
Using Port:1/0/1 in
IP qos-flow-list:QOS-LIST1
      10 ip any host 192.168.100.10 action max-rate 5M max-rate-burst 512
         matched packets(max-rate over) :         7
         matched packets(max-rate under):        28
>
```

Make sure that the monitoring bandwidth for maximum bandwidth control (max-rate 5M) and the burst size for maximum bandwidth control (max-rate-burst 512) are displayed in the information for QOS-LIST1.

3.6.2 Checking the queuing priority when non-compliance occurs in minimum bandwidth monitoring

The following figure shows how to check the queuing priority when non-compliance in minimum bandwidth monitoring occurs.

Figure 3-6: Checking the queuing priority when non-compliance in minimum bandwidth monitoring occurs

```
> show qos-flow 1/0/3
Date 20XX/12/01 13:00:00 UTC
Using Port:1/0/3 in
IP qos-flow-list:QOS-LIST2
      10 ip any host 192.168.110.10 action min-rate 1M min-rate-burst 64 penalty-discard-class 1
         matched packets(min-rate over) :      9826
         matched packets(min-rate under):  74699826
>
```

Make sure that the minimum monitoring bandwidth (min-rate 1M), the burst size of the minimum monitoring bandwidth (min-rate-burst 64), and the queuing priority of non-compliant frames (penalty-discard-class 1) are displayed in the information for QOS-LIST2.

3.6.3 Checking DSCP rewrite when non-compliance occurs in minimum monitoring bandwidth in units of the number of frames

The following figure shows how to check DSCP rewrite when a minimum monitoring bandwidth non-compliance occurs in units of the number of frames.

Figure 3-7: Checking DSCP rewrite when a minimum monitoring bandwidth non-compliance occurs

```
> show qos-flow 1/0/5
Date 20XX/12/01 13:00:00 UTC
Using Port:1/0/5 in
IP qos-flow-list:QOS-LIST3
      10 ip any host 192.168.110.10 action min-pps-rate 10000 min-packet-burst 64 penalty-dscp cs1
        matched packets(min-rate over) :        28
        matched packets(min-rate under):         7
>
```

Make sure that the minimum monitoring bandwidth (min-pps-rate 10000), the burst size of the minimum monitoring bandwidth (min-packet-burst 64), and the DSCP name (cs1) for non-compliant frames are displayed in the information for QOS-LIST3.

3.6.4 Checking the combined use of maximum bandwidth control and minimum bandwidth monitoring

The following figure shows how to check the combined use of maximum bandwidth control and minimum bandwidth monitoring.

Figure 3-8: Checking the combined use of maximum bandwidth control and minimum bandwidth monitoring

```
> show qos-flow 1/0/7
Date 20XX/12/01 13:00:00 UTC
Using Port:1/0/7 in
IP qos-flow-list:QOS-LIST4
      10 ip any host 192.168.130.10 action max-rate 5M max-rate-burst 512 min-rate 1M
min-rate-burst 64 penalty-dscp cs1
         matched packets(max-rate over) :  74699826
         matched packets(max-rate under):        28
>
```

Make sure that the monitoring bandwidth for maximum bandwidth control (max-rate 5M), the burst size for maximum bandwidth control (max-rate-burst 512), the minimum monitoring bandwidth (min-rate 1M), the burst size of the minimum monitoring bandwidth (min-rate-burst 64), and the DSCP name (cs1) for non-compliant frames are displayed in the information for QOS-LIST4.

3.6.5 Checking the summarized bandwidth monitoring

The following figure shows how to check summarized bandwidth monitoring.

Figure 3-9: Checking summarized bandwidth monitoring

```
> show qos-flow 1/0/7
Date 20XX/12/01 13:00:00 UTC
Using Port:1/0/7 in
IP qos-flow-list:QOS-LIST4
      10 ip any host 192.168.130.10 action aggregate-policer POLICER-LIST4
         matched packets(max-rate over) :  74699826
         matched packets(max-rate under):        28
      20 ip any host 192.168.131.10 action aggregate-policer POLICER-LIST4
         matched packets(max-rate over) :       241
         matched packets(max-rate under):    145834
>
```

Make sure that the summarized bandwidth monitoring (aggregate-policer POLICER-LIST4) is displayed in the information for QOS-LIST4.

3.6.6 Checking bandwidth non-compliance notification

The following figure shows how to check bandwidth non-compliance notification.

Figure 3-10: Checking bandwidth non-compliance notification

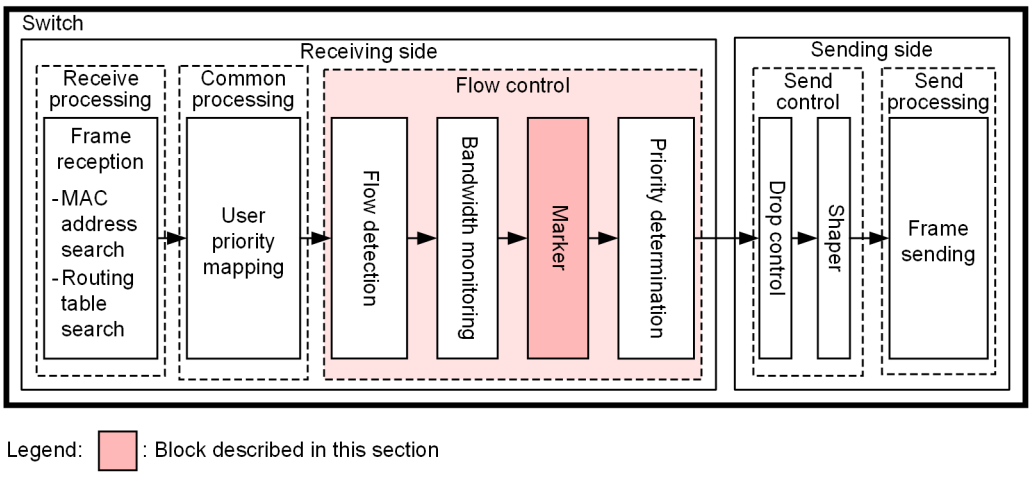
```
> show qos-flow 1/0/7
Date 20XX/12/01 13:00:00 UTC
Using Port:1/0/7 in
IP qos-flow-list:QOS-LIST4
      10 ip any host 192.168.130.10 action max-rate 5M max-rate-burst 512 log trap
         matched packets(max-rate over) :       826
         matched packets(max-rate under):   4385728
         rate-alarm
              state: conform
              count:    1/  65
              total exceed-count/total conform-count:        154/      7295
>
```

Checks that "operation message output of bandwidth non-compliance notification (log)" and "SNMP notification (trap)" are displayed in the information for QOS-LIST4. Checks that the "bandwidth status (state:)", "status (count:)", and "total number of bandwidth non-compliances and compliances (total exceed-count/total conform-count:)" are displayed in the bandwidth non-compliance notification information.

3.7 Description of marker

Marker is the function 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 marker block described in this section.

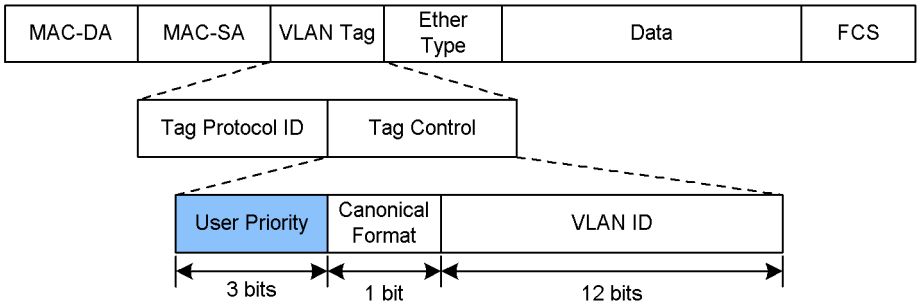
Figure 3-11: Positioning of marker



3.7.1 User priority rewriting

User priority rewriting is the function 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 3-12: 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. The following figure shows an example of a frame that has multiple VLAN tags.

Figure 3-13: Overview of the format of a frame that has multiple VLAN tags

(i) Format of a frame with a single VLAN tag

MAC-DA	MAC-SA	First VLAN tag	Ether Type	Data	FCS

(ii) Format of a frame with two VLAN tags

MAC-DA	MAC-SA	First VLAN tag	Second VLAN tag	Ether Type	Data	FCS

You cannot update the user priority for the following frames:

- Frames sent from a port for which VLAN tunneling is set
- IPv4 and IPv6 packets exceeding the MTU
- Frames whose TTL is set to 1
- Frames whose hop limit is set to 1
- Frames with an IP option
- Frames with an IPv6 extension header
- IPv4 or IPv6 packets with an unknown receiver address

You cannot specify user priority rewriting and user priority inheritance at the same time.

If neither user priority rewriting nor user priority inheritance is used, the user priority is set as described in the following table.

Table 3-9: User priority when frames are sent

User priority for frames to be sent	Applicable frames
3	• Frames received without a VLAN tag and sent with a VLAN tag • Frames forwarded from the access line to the backbone line by VLAN tunneling
User priority of received frames	• Frames with a VLAN tag that are forwarded from the access line to the backbone line by VLAN tunneling • Frames received with a VLAN tag on a port for which neither tag translation nor VLAN tunneling is configured, and sent with a VLAN tag

3.7.2 User priority inheritance

When you use VLAN tunneling to add a VLAN tag to frames from the access line and forward them to the backbone line, you can use the user priority inheritance function. This function inherits the user priority of a frame detected by flow detection as the user priority of the backbone line (user priority in the added VLAN tag) and the CoS values for priority determination. This function uses the following frames:

- Frames forwarded by the Switch
- Frames sent to the Switch

You can set user priority inheritance on a receiving-side Ethernet interface for which VLAN tunneling is configured.

The following table describes the values set when user priority inheritance is set.

Table 3-10: Values set when user priority inheritance is set

User priority of frames detected by flow detection	Outgoing frames	
	User priority	CoS value
Without VLAN tag	0	0
0	0	0
1	1	1
2	2	2

User priority of frames detected by flow detection	Outgoing frames	
	User priority	CoS value
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

You cannot set user priority inheritance concurrently with user priority rewriting and priority determination (CoS value specification).

For details about the CoS values when user priority inheritance is not set, see "3.10.2 CoS values and queuing priority". For details about the user priority, see "3.7.1 User priority rewriting".

3.7.3 DSCP rewrite

DSCP rewriting is the function that is used to update the DSCP, which is the six highest-order bits of the TOS field in the IPv4 header or the traffic class field in the IPv6 header. The following figures show the formats of the TOS and traffic class fields.

Figure 3-14: Format of the TOS field

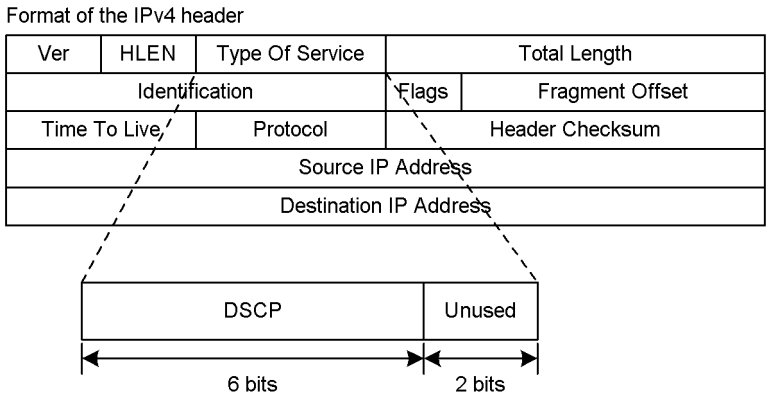
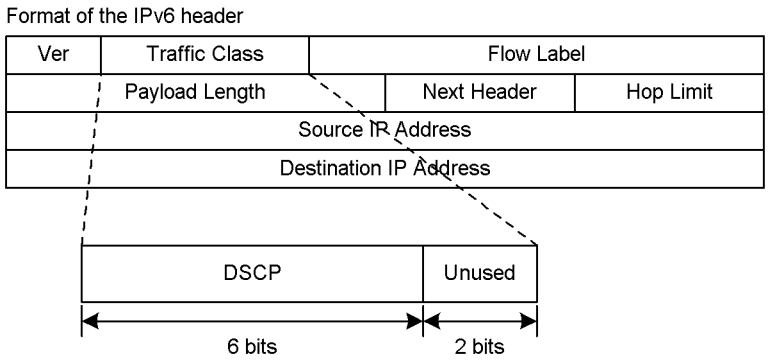


Figure 3-15: Format of the Traffic class field



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

You can also use DSCP rewriting to update the DSCP of a frame that exceeds the minimum monitoring bandwidth on instruction from the bandwidth monitoring function. For example, you can set the DSCP value to 0 for frames that exceed the minimum monitoring bandwidth.

For handling of non-compliant frames when DSCP rewriting and minimum bandwidth monitoring are specified at the same time, the penalty behavior specified for non-compliance has priority.

You cannot update the DSCP for the following frames:

- IPv4 and IPv6 packets exceeding the MTU
- Frames whose TTL is set to 1
- Frames whose hop limit is set to 1
- Frames with an IP option
- Frames with an IPv6 extension header
- IPv4 or IPv6 packets with an unknown receiver address

3.8 Marker configuration

3.8.1 Configuring user priority rewriting

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). When this list is created, control 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 gigabitethernet 1/0/1`

   Switches to interface mode for port 1/0/1.

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

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

3.8.2 Configuring user priority inheritance

The following describes the configuration when the user priority is to be inherited 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 inherited.

Command examples

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

   Creates an IPv4 QoS flow list (QOS-LIST2). When this list is created, control switches to IPv4 QoS flow list mode.

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

   Configures the IPv4 QoS flow list for destination IP address 192.168.100.10, and the sets that the user priority is to be inherited.

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

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

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

   Switches to interface mode for port 1/0/1.

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

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

3.8.3 Configuring DSCP rewrite

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-LIST3`

   Creates an IPv4 QoS flow list (QOS-LIST3). When this list is created, control 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 gigabitethernet 1/0/3`

   Switches to interface mode for port 1/0/3.

5. `(config-if)# ip qos-flow-group QOS-LIST3 in`

   Enables the IPv4 QoS flow list (QOS-LIST3) on the receiving side.

3.9 Marker operation

To check whether the information you have set is applied, use the "show qos-flow" command.

3.9.1 Checking user priority rewriting

The following figure shows how to check user priority rewriting.

Figure 3-16: Checking user priority rewriting

```
> show qos-flow 1/0/1
Date 20XX/12/01 13:00:00 UTC
Using Port:1/0/1 in
IP qos-flow-list:QOS-LIST1
      10 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-LIST1.

3.9.2 Checking user priority inheritance

The following figure shows how to check user priority inheritance.

Figure 3-17: Checking user priority inheritance

```
> show qos-flow 1/0/1
Date 20XX/03/01 13:00:00 UTC
Using Port:1/0/1 in
IP qos-flow-list:QOS-LIST2
      10 ip any host 192.168.100.10 action copy-user-priority
         matched packets                    :       0
>
```

Make sure that copy-user-priority is displayed in the information for QOS-LIST2.

3.9.3 Checking DSCP rewrite

The following figure shows how to check the DSCP rewriting.

Figure 3-18: Checking DSCP rewriting

```
> show qos-flow 1/0/3
Date 20XX/12/01 13:00:00 UTC
Using Port:1/0/3 in
IP qos-flow-list:QOS-LIST3
      10 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-LIST3.

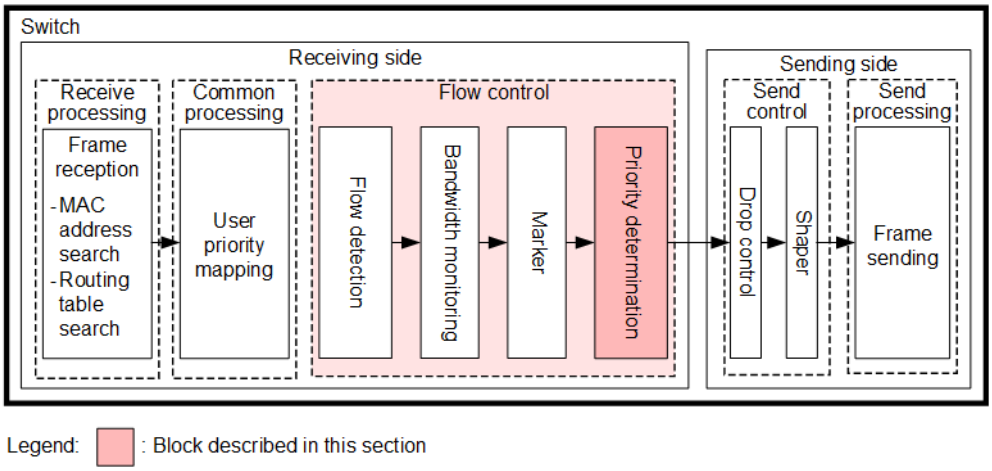
3.10 Description of priority determination

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

Frames to which this function applies differ depending on the switch configuration and the setting for changing which frames are subject to priority determination. For details, see "3.10.1 Frames subject to priority determination".

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

Figure 3-19: Positioning of the priority determination block



3.10.1 Frames subject to priority determination

The function for changing which frames are subject to priority determination is used to make the frames that are sent to the Switch and are not subject to priority determination subject to priority determination. By default, only frames forwarded by the Switch are subject to priority determination. The table below describes switch configurations, the setting for changing which frames are subject to priority determination, and the corresponding frames subject to priority determination.

Table 3-11: Switch configuration and frames subject to priority determination

Device configuration	Setting for changing which frames are subject to priority determination	Frame type	
		Frames sent to the Switch	Frames forwarded by the Switch
All models (in standalone mode)	Not set	N	Y
	Set	Y	Y
All models (in stack mode)	Not set	Y	Y
	Set	Y	Y

Legend: Y: Becomes subject to priority determination; N: Does not become subject to priority determination

3.10.2 CoS values and queuing priority

CoS values are used as an index for showing the priority of frames on the Switch. The queuing priority indicates how easily a frame can be discarded for each queue.

The following table describes the specifiable range of CoS values and queuing priority values.

Table 3-12: Specifiable range of CoS values and queuing priority values

Item	Range
CoS value	0 to 7
Queuing priority	1 to 3

You cannot specify a CoS value and user priority inheritance at the same time.

For frames where neither priority determination nor user priority inheritance is set for flow control, the default CoS values and queuing priority are used. The following table describes the default CoS values and queuing priority values for each frame type.

Table 3-13: Default CoS values and queuing priority for each frame type

Frame type	Default	
	CoS value	Queuing priority
Unicast frame	Conforms to the result of user priority mapping	3
Broadcast frame	0	
Multicast frame		

In addition, mirrored frames conform to the CoS value and queuing priority of the copy source frame.

Note that the correspondence between the CoS values and the determined queuing priority is fixed for the frames indicated in the table below regardless of whether priority determination and user priority inheritance for flow control are set.

The following table indicates the frames whose values cannot be changed by either priority determination or user priority inheritance.

Table 3-14: Frames whose values cannot be changed by priority determination

Frame type	CoS value	Queuing priority
Frames spontaneously sent by the Switch	7	3
The following frames received by the Switch: • ARP frame[#1#2] • Frames used for line test	5	—
The following frames received by the Switch: • Incoming frames for which the learned source MAC addresses are determined to have been moved	2	—
Of the frames received by the Switch by Layer 3 forwarding, the following packets and frames: • IPv4 and IPv6 packets exceeding the MTU • Frames whose TTL is set to 1 • Frames whose hop limit is set to 1 • Frames with an IP option • Frames with an IPv6 extension header	2	—

Frame type	CoS value	Queuing priority
Of the frames received on the Switch by Layer 3 forwarding, the following packets: • IPv4 or IPv6 packets with an unknown receiver address	2	—
The following frames for which the Switch perform Layer 3 forwarding: • Fragmented frames on the Switch • Frames with an IP option • Frames with an IPv6 extension header • Forwarding frames that are temporarily retained on the Switch due to unresolved ARP or NDP	3	—

Legend: —: Can be changed according to the priority determination for flow control.

#1

The "flow action-change arp-discard-class" configuration command can be used to change the queuing priority of ARP broadcast frame from 3 to 2.

#2

The "flow action-change arp-reply-cos" configuration command can be used to change the CoS value of ARP reply frames received by the Switch and whose destination MAC address is the broadcast address from 5 to 0.

3.10.3 CoS mapping function

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

(1) Mapping of CoS values and send queues for ports

There are eight sending queues per port for unicast frames with already-learned MAC addresses (UC queues), and four queues for unicast frames with unlearned MAC addresses, multicast frames, broadcast frames, and mirrored frames (MC queues). The following table describes the mapping of CoS values to send queues per port.

Table 3-15: Mapping of CoS values to send queues for ports (UC queues)

CoS value	Queue number for sending	
	Send queue length: 2880	Send queue length: 24272
0	1	2
1	2	2
2	4	2
3	5	2
4	6	2
5	8	2
6	10	2
7	12	4

Table 3-16: Mapping of CoS values to send queues for ports (MC queues)

CoS value	Queue number for sending	
	Send queue length: 2880	Send queue length: 24272
0	3	1
1	3	1
2	3	1
3	3	1
4	7	1
5	7	1
6	9	1
7	11	3

(2) Mapping of CoS values to CPU-addressed sending queues

The CPU-addressed sending queue differs from the port sending queue in that there are eight common sending queues for all frame types. The following table describes the mapping of CoS values to send queues.

Table 3-17: Mapping of CoS values to CPU-addressed sending queues

CoS value	Queue number for sending
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

3.10.4 Note on using priority determination

(1) Priority determination for frames

If a behavior that raises the priority of the frame is specified, communication might be disabled because protocol control frames sent to the Switch cannot be received, or frames originated by the Switch cannot be sent. In particular, IP multicast packets are packets sent to the Switch and also are frames to be relayed. Therefore, be careful when raising the priority of the frames. If such a problem occurs, perform the following:

- When the stack is configured, if communication with protocol control frames sent to the Switch is disconnected, lower the priority of the frames.

- In a standalone configuration, if communication with protocol control frames sent to the Switch is disconnected, specify the setting for changing which frames are subject to priority determination.
- If communication with frames originated by the Switch is disconnected, lower the priority of the frames.

3.11 Priority determination configuration

3.11.1 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). When this list is created, control 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 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 gigabitethernet 1/0/1`

   Switches to interface mode for port 1/0/1.

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

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

3.12 Priority operation

3.12.1 Checking the priority

When traffic (frames whose destination IP address is 192.168.100.10) flows into a line, use the "show qos queuing" command to check the queue number. In this example, the applicable Ethernet interface is port 1/0/2.

Figure 3-20: Checking the priority

```
> show qos queueing 1/0/2
Date 20XX/03/01 13:00:00 UTC
Switch1/NIF0/Port2 (outbound)
 Max_Queue=12, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop
  Queue  1: Qlen=     0, Limit_Qlen= 2880, HOL1=          0
  Queue  2: Qlen=     0, Limit_Qlen= 2880, HOL1=          0
  Queue  3: Qlen=     0, Limit_Qlen= 2880, HOL1=          0
  Queue  4: Qlen=     0, Limit_Qlen= 2880, HOL1=          0
  Queue  5: Qlen=     0, Limit_Qlen= 2880, HOL1=          0
  Queue  6: Qlen=     1, Limit_Qlen= 2880, HOL1=          0 … 1
  Queue  7: Qlen=     0, Limit_Qlen= 2880, HOL1=          0
  Queue  8: Qlen=     0, Limit_Qlen= 2880, HOL1=          0
  Queue  9: Qlen=     0, Limit_Qlen= 2880, HOL1=          0
  Queue 10: Qlen=     0, Limit_Qlen= 2880, HOL1=          0
  Queue 11: Qlen=     0, Limit_Qlen= 2880, HOL1=          0
  Queue 12: Qlen=     0, Limit_Qlen= 2880, HOL1=          0
 Tail_drop=          0
```

1.Make sure that the Qlen value for Queue6 has a count value.

4 Send Control

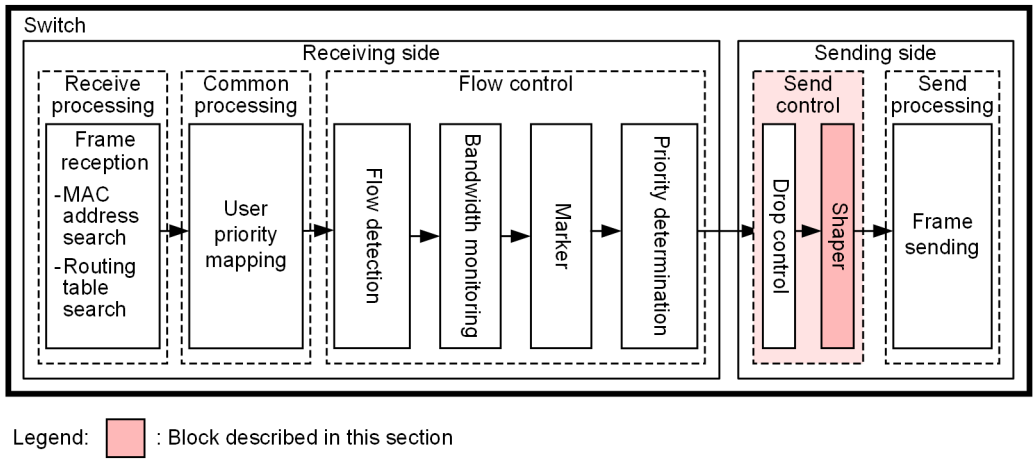
This chapter describes send control (shaper and drop control) used on the Switch.

4.1 Description of shaper

4.1.1 Overview of the legacy shaper

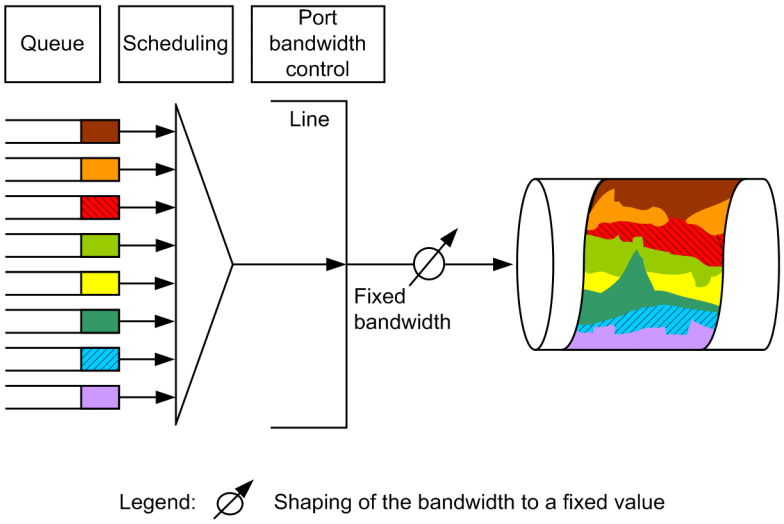
The shaper function is used to control the output order of frames from each queue and the output order and output bandwidth for each port. The following figure shows the positioning of the shaper block described in this section.

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. This 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. The number of frames that can be queued in a queue is called the send queue length. If a frame is stored in multiple buffers, the first buffer can contain up to 144 bytes, and the second and subsequent buffers can contain up to 208 bytes. One buffer can contain only one frame. To change the send queue length, 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 queue length of 2880 is used.

Table 4-1: Send queue lengths and their purposes

Send queue length	Purpose
2880	When the load on each queue is equal, specify this value to enable send control.
24272#	Specify this value to reduce queue overflows caused by burst traffic.

#

When you specify a send queue length of 24272, the queue length is assigned to only queues 1 to 4, resulting in the following scheduling behaviors:

PQ: Queues 1 to 4 run with PQ specified

4PQ+8RR: Queues 1 to 4 run with RR specified

4PQ+8ERR: Queues 1 to 4 run with ERR specified

4PQ+8WRR: Queues 1 to 4 run with WRR specified

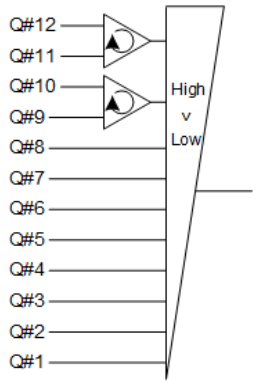
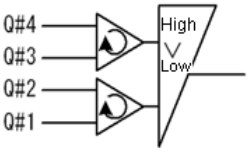
4PQ+8WFQ: Queues 1 to 4 run with WFQ specified

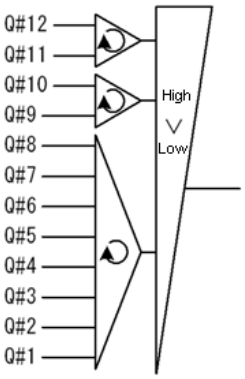
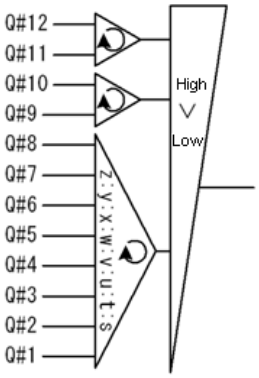
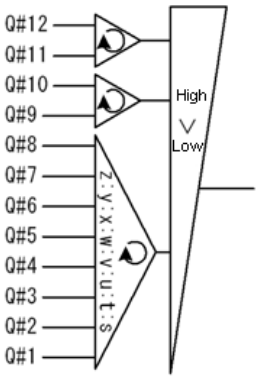
4.1.3 Scheduling

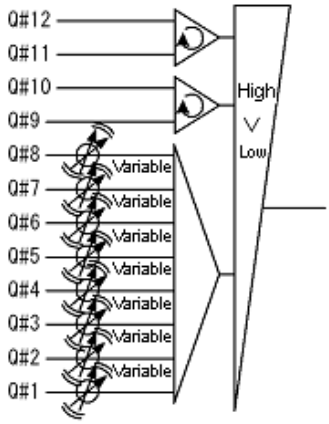
Scheduling is the function that controls the order in which the frames in each queue will be sent.

The Switch provides the five scheduling types below. The following table describes the scheduling behaviors:

Table 4-2: Scheduling behavior descriptions

Scheduling type	Conceptual diagram	Description	Application example
PQ		Complete priority queuing. 12 queues per port. When there are frames in multiple queues, the frames in a higher-priority queue are always sent first. However, queues 12 (Q#12), 11 (Q#11), 10 (Q#10), and 9 (Q#9) are controlled such that each queue has an equal number of frames to be sent.	When traffic priority must be strictly observed
		Complete priority queuing. 4 queues per port. Queues 4 (Q#4) and 3 (Q#3) are controlled such that each queue has an equal number of frames to be sent. When there are frames in queue 4 or 3, the frames in a higher-priority queue are always sent first. When there is no frame in queue 4 or queue 3, queues 2 (Q#2) and 1 (Q#1) are controlled such that each queue has an equal number of frames to be sent.	

Scheduling type	Conceptual diagram	Description	Application example
4PQ+8RR		Round robin with top-priority queues. 12 queues per port. When there are frames in multiple queues, the frames in a higher-priority queue are always sent first. However, queues 12 (Q#12), 11 (Q#11), 10 (Q#10), and 9 (Q#9) are controlled such that each queue has an equal number of frames to be sent. When there is no frame in queues 12-9, queues 8-1 (Q#8 to Q#1) are controlled such that each queue has an equal number of frames to be sent regardless of the frame length.	When the only traffic is data traffic
4PQ+8ERR		Top-priority queues and weighted (ratio based on the byte count) round robin. 12 queues per port. When there are frames in multiple queues, the frames in a higher-priority queue are always sent first. However, queues 12 (Q#12), 11 (Q#11), 10 (Q#10), and 9 (Q#9) are controlled such that each queue has an equal number of frames to be sent. When there is no frame in queues 12-9, the frames in queues 8-1 (Q#8 to Q#1) are sent according to the ratio (z:y:x:w:v:u:t:s) determined based on the number of bytes set for each queue.	When the top-priority queues are used for video and audio data, and the ERR queue is used for data traffic
4PQ+8WRR		Top-priority queues and weighted (number of frames) round robin. 12 queues per port. When there are frames in multiple queues, the frames in a higher-priority queue are always sent first. However, queues 12 (Q#12), 11 (Q#11), 10 (Q#10), and 9 (Q#9) are controlled such that each queue has an equal number of frames to be sent. When there is no frame in queues 12-9, the frames in queues 8-1 (Q#8 to Q#1) are sent based on the number of frames (z, y, x, w, v, u , t, or s) set to each queue. If queues 8-1 are evenly weighted, a round-robin behavior is performed.	When the top-priority queues are used for video and audio data, and the WRR queue is used for data traffic

Scheduling type	Conceptual diagram	Description	Application example
4PQ+8WFQ		Top-priority queues and weighted fair queuing. 12 queues per port. When there are frames in multiple queues, the frames in a higher-priority queue are always sent first. Queues 12 (Q#12), 11 (Q#11), 10 (Q#10), and 9 (Q#9) are controlled such that each queue has an equal number of frames to be sent. When there is no frame in queues 12-9, a minimum number of the frames in queues 8-1 (Q#8 to Q#1) are sent according to the weight (minimum guaranteed bandwidth) set to each queue. After sending all queues, a round-robin operation will be performed.	When the top-priority queues are used for video and audio data, and the WFQ queue is used for data traffic

The following table describes the scheduling specifications.

Table 4-3: Scheduling specifications

Item		Specifications
Number of queues		12 queues
4PQ+8ERR	Setting range of the weights for queues 1 to 8	1 to 127
4PQ+8WRR	Setting range of the weights for queues 1 to 8	1 to 15
4PQ+8WFQ	Setting range of the weights for queues 1 to 8	See "(1) Setting range for WFQ". 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

(1) Setting range for WFQ

The tables below show the setting ranges for WFQ.

Table 4-4: Setting range for WFQ (10BASE-T, 100BASE-TX, 1000BASE-T, and 1000BASE-X)

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

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.

#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).

Table 4-5: Setting range for WFQ (10GBASE-R, 10GBASE-T)

Setting unit[#1]	Setting range	Increment
Gbit/s	1G to 10G	1 Gbit/s
Mbit/s	1 M to 10000 M	1 Mbit/s
kbit/s	1000 to 10000000	100 kbit/s[#2]
	64 to 960	64 kbit/s[#3]

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.
#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).

Table 4-6: Setting range for WFQ (40GBASE-R)

Setting unit[#1]	Setting range	Increment
Gbit/s	1G to 40G	1 Gbit/s
Mbit/s	1M to 40000M	1 Mbit/s
kbit/s	1000 to 40000000	500 kbit/s[#2]
	256 to 768	256 kbit/s[#3]

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.
#2: To set a value of 1000 kbit/s or more, specify the value in units of 500 kbit/s (1000, 1500, 2000...40000000).
#3: When setting a value less than 1000 kbit/s, specify the value in units of 256 kbit/s (256, 512, and 768).

Table 4-7: Setting range for WFQ (100GBASE-R)

Setting unit[#1]	Setting range	Increment
Gbit/s	1G to 100G	1 Gbit/s
Mbit/s	1M to 100000M	1 Mbit/s
kbit/s	1000 to 100000000	500 kbit/s[#2]
	512	512 kbit/s[#3]

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.
#2: To set a value of 1000 kbit/s or more, specify the value in units of 500 kbit/s (1000, 1500, 2000...100000000).
#3: To set a value less than 1000 kbit/s, specify 512 only.

4.1.4 Port bandwidth control

The port bandwidth control function 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.

Port bandwidth control uses the leaky bucket algorithm, which is based on the model of a bucket that has a hole in the bottom.

The setting ranges for port bandwidth control are shown below. Set the bandwidth so that it is equal to or smaller than the line speed. If setting is not possible, the operation log is displayed, and the port bandwidth control setting is disabled.

Table 4-8: Setting range for port bandwidth control (10BASE-T, 100BASE-TX, 1000BASE-T, and 1000BASE-X)

Setting unit#1	Setting range	Increment
Gbit/s	1 G	1 Gbit/s
Mbit/s	1 M to 1000 M	1 Mbit/s
kbit/s	1000 to 1000000	100 kbit/s#2
	64 to 960	64 kbit/s#3

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.
#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).

Table 4-9: Setting range for port bandwidth control (10GBASE-R, 10GBASE-T)

Setting unit#1	Setting range	Increment
Gbit/s	1 G to 10 G	1 Gbit/s
Mbit/s	1M to 10000M	1 Mbit/s
kbit/s	1000 to 10000000	100 kbit/s#2
	64 to 960	64 kbit/s#3

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.
#2: To set a value of 1000 kbit/s or more, specify the value in units of 100 kbit/s (1000, 1100, 1200...10000000).
#3: To set a value less than 1000 kbit/s, specify the value in units of 64 kbit/s (64, 128, 192...960).

Table 4-10: Setting range for port bandwidth control (40GBASE-R)

Setting unit#1	Setting range	Increment
Gbit/s	1 G to 40 G	1 Gbit/s
Mbit/s	1 M to 40000 M	1 Mbit/s
kbit/s	1000 to 40000000	500 kbit/s#2
	256 to 768	256 kbit/s#3

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.
#2: To set a value of 1000 kbit/s or more, specify the value in units of 500 kbit/s (1000, 1500, 2000...40000000).
#3: When setting a value less than 1000 kbit/s, specify the value in units of 256 kbit/s (256, 512, and 768).

Table 4-11: Setting range for port bandwidth control (100GBASE-R)

Setting unit[#1]	Setting range	Increment
Gbit/s	1G to 100G	1 Gbit/s
Mbit/s	1M to 100000M	1 Mbit/s
kbit/s	1000 to 100000000	500 kbit/s[#2]
	512	512 kbit/s[#3]

#1: 1 G is treated as 1000000000, 1 M is treated as 1000000, and 1 k is treated as 1000.
#2: To set a value of 1000 kbit/s or more, specify the value in units of 500 kbit/s (1000, 1500, 2000...100000000).
#3: To set a value less than 1000 kbit/s, specify 512 only.

The following table describes the setting range for the burst size.

Table 4-12: Setting range for the burst size

Line type	Setting range	Default value when no value is specified
10BASE-T 100BASE-TX 1000BASE-T 1000BASE-X 10GBASE-R 10GBASE-T	4, 8, 16, 32 KB	32kbyte
40GBASE-R	8, 16, 32, 64 KB	64kbyte
100GBASE-R	16, 32, 64, 128 kbytes	128kbyte

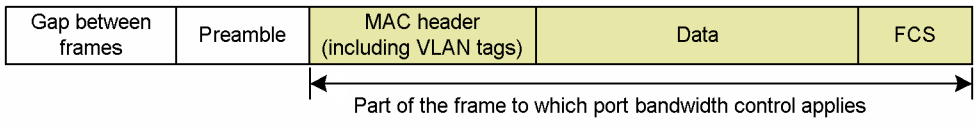
The following table describes the burst size characteristics based on the properties of the leaky bucket algorithm.

Table 4-13: Burst size characteristics

Burst size	Features
Smaller	The dropping of burst traffic is relatively easy. If traffic is sent while communication is not being performed, the send bandwidth fluctuations are relatively small.
Larger	The dropping of burst traffic is relatively difficult. If traffic is sent while communication is not being performed, the send bandwidth fluctuations are relatively large.

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 Note on using the shaper

(1) 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 for depletion, use the "show qos queueing" command to check whether the HOL1 counter has been incremented.

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

4.2 Shaper configuration

4.2.1 Configuring scheduling

Points to note

Sets scheduling in the QoS queue list information and sets the relevant port.

Command examples

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

   Sets scheduling (PQ) in the QoS queue list information (QLIST-PQ).

2. `(config)# interface gigabitethernet 1/0/1`

   Moves to port 1/0/1 interface mode.

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

   Specifies the QoS queue list name in the QoS queue interface information and enables the QoS queue list information.

4.2.2 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 bandwidth (20 Mbit/s) and the burst size (4 KB) are set in port bandwidth control for the relevant port (100 Mbit/s).

Command examples

1. `(config)# interface gigabitethernet 1/0/13`

   Moves to port 1/0/13 interface mode.

2. `(config-if)# speed 100`

   `(config-if)# duplex full`

   Sets the line speed of the port to 100 Mbit/s.

3. `(config-if)# traffic-shape rate 20M 4`

   Sets the port bandwidth to 20 Mbit/s and the burst size to 4 KB.

4.3 Shaper operation

Use the "show qos queueing" command to check the information about the legacy shaper set for the Ethernet interface.

4.3.1 Checking the scheduling

The following shows how to check the scheduling.

Figure 4-4: Checking scheduling

```
> show qos queueing 1/0/1
Date 20XX/03/01 13:00:00 UTC
Switch1/NIF0/Port1 (outbound)
 Max_Queue=12, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop …1
  Queue  1: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  2: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  3: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  4: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  5: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  6: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  7: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  8: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  9: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue 10: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue 11: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue 12: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
 Tail_drop=         0
```

1. Make sure that the information for the Qmode parameter is the same as that set for scheduling (in this example, 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

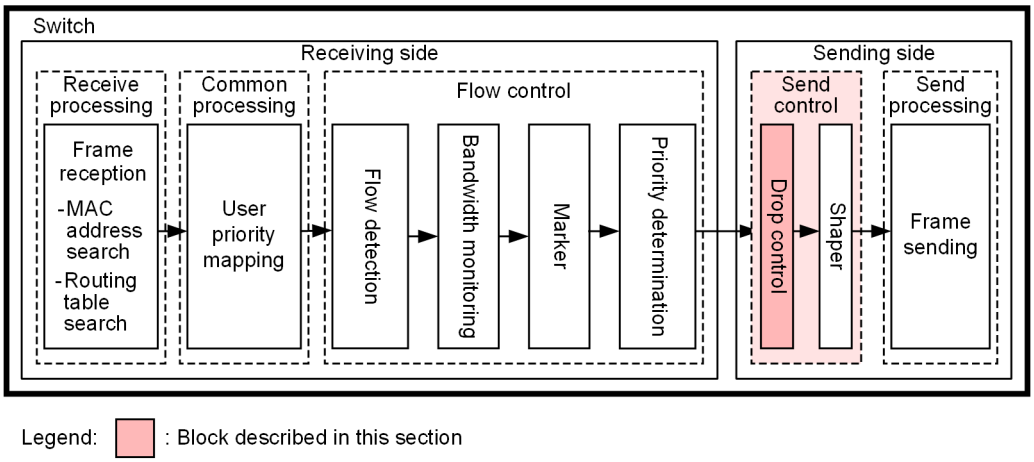
```
> show qos queueing 1/0/13
Date 20XX/03/01 13:00:00 UTC
Switch1/NIF0/Port13 (outbound)
 Max_Queue=12, Rate_limit=20Mbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop …1,2
  Queue  1: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  2: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  3: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  4: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  5: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  6: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  7: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  8: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue  9: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue 10: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue 11: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
  Queue 12: Qlen=    0, Limit_Qlen= 2880, HOL1=          0
 Tail_drop=         0
```

1. Make sure that the information for the Rate_limit parameter is the same as the configured bandwidth value (in this example, 20 Mbit/s).
2. Make sure that the information for the Burst_size parameter is the same as the configured burst size (in this example, 4 KB).

4.4 Description of drop control

The following figure shows the positioning of the drop control block described in this section.

Figure 4-6: Positioning of the drop control block



4.4.1 Drop control

Drop control is the function that controls the queuing priority, which indicates how easily a frame can be dropped from a queue, and that controls whether the frame can be queued or dropped according to the number of retained frames.

If frames remain in a queue, you can implement more detailed QoS by changing the queuing priority.

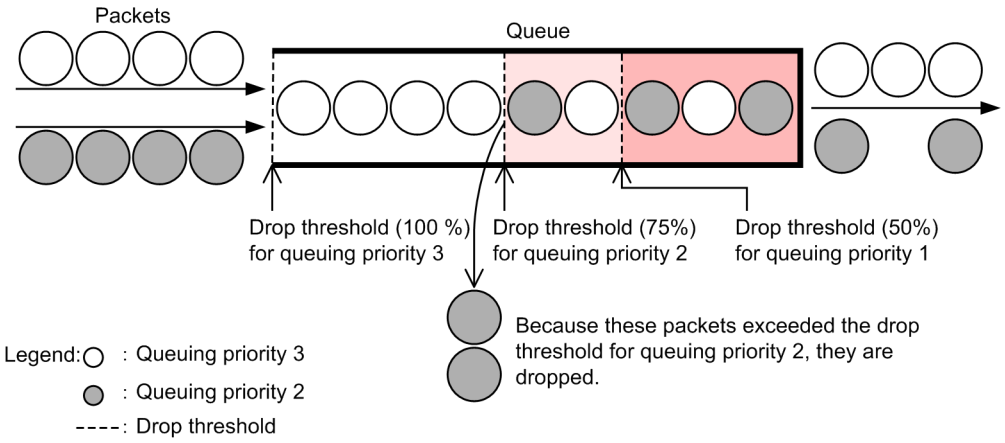
The number of frames than can be queued in a queue is called the queue length.

The Switch uses the tail drop method for drop control.

(1) Tail drop

The tail drop function drops frames if the queue length exceeds the drop threshold. The drop threshold varies depending on the queuing priority. Frames in a queue that has a higher queuing priority are more difficult to drop. The following figure shows an overview of the tail drop method. When the drop threshold for queuing priority 2 is exceeded, the queuing priority 2 frames are all dropped.

Figure 4-7: Overview of the tail drop method



The following table describes the queuing priorities and corresponding drop thresholds for the tail drop function. The drop threshold indicates the percentage of frames remaining in the queue to the queue length.

Table 4-14: Drop threshold for the tail drop method

Queuing priority	Drop threshold (%)
1	50
2	75
3	100

4.5 Drop control configuration

4.5.1 Configuring the queuing priority

Set the queuing priority 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 queuing priority is set.

Command examples

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

   Creates an IPv4 QoS flow list (QOS-LIST2). When this list is created, control switches to IPv4 QoS flow list mode.

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

   Sets the IPv4 QoS flow list for destination IP address 192.168.100.10, and then sets the queuing priority to 2.

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

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

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

   Switches to interface mode for port 1/0/1.

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

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

4.6 Drop control operation

Use the "show qos queueing" command to check the number of the queue that is holding the queued packets and the number of discarded packets.

4.6.1 Checking the queuing priority

The figure below shows how to check the queuing priority.

In this example, the applicable Ethernet interface is port 1/0/2.

The queuing priority is checked under the condition that traffic remaining in Queue 6 with Qlen of about 2880 flows into a line.

Figure 4-8: Checking the queuing priority

```
> show qos queueing 1/0/2
Date 20XX/03/01 13:00:00 UTC
Switch1/NIF0/Port2 (outbound)
 Max_Queue=12, Rate_limit=20Mbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop
  Queue  1: Qlen=    0, Limit_Qlen= 2880, HOL1=         0
  Queue  2: Qlen=    0, Limit_Qlen= 2880, HOL1=         0
  Queue  3: Qlen=    0, Limit_Qlen= 2880, HOL1=         0
  Queue  4: Qlen=    0, Limit_Qlen= 2880, HOL1=         0
  Queue  5: Qlen=    0, Limit_Qlen= 2880, HOL1=         0
  Queue  6: Qlen= 2160, Limit_Qlen= 2880, HOL1=        18   …1,2
  Queue  7: Qlen=    0, Limit_Qlen= 2880, HOL1=         0
  Queue  8: Qlen=    0, Limit_Qlen= 2880, HOL1=         0
  Queue  9: Qlen=    0, Limit_Qlen= 2880, HOL1=         0
  Queue 10: Qlen=    0, Limit_Qlen= 2880, HOL1=         0
  Queue 11: Qlen=    0, Limit_Qlen= 2880, HOL1=         0
  Queue 12: Qlen=    0, Limit_Qlen= 2880, HOL1=         0
 Tail_drop=         18                                    …2
```

1. Make sure that the Qlen value for Queue6 has a count value.
2. Make sure that the Qlen value is 75 % of the Limit_Qlen value and that the Tail_drop counter for dropped packets has been incremented.

5 Layer 2 Authentication

This chapter provides an overview of Layer 2 authentication functions in the Switch.

5.1 Overview

5.1.1 Types of Layer 2 authentication

The Switch supports the following functions for authentication at the Layer 2 level:

- IEEE 802.1X

  Provides user authentication conforming to the IEEE 802.1X standard. IEEE 802.1X authenticates terminals based on the successful exchange of EAPOL packets.

- Web authentication

  Web authentication is a function that authenticates users by using an ordinary Web browser. Authenticates users on terminals that can run an ordinary Web browser.

- MAC-based authentication

  Authenticates devices such as printers that are not capable of providing user-initiated logons.

Several authentication modes are used in Layer 2 authentication. The table below provides an overview of Layer 2 authentication functions by authentication mode.

Although some types of authentication functions will work with other networking functions, other types will not. For details about which functions will work with other types, see "5.2 Interoperability of Layer 2 authentication with other functions".

Table 5-1: Authentication functions supported at the layer 2 level

Layer 2 authentication	Authentication mode	Overview
IEEE 802.1X	Port-based authentication	Port-based authentication controls authentication at the physical port or channel group level, with a port or group serving as the unit of authentication. This mode incorporates the three submodes below, each of which presents a different authentication behavior: 1. Single mode In this mode, only one terminal is authenticated and connected per authentication unit. When an authentication request arrives from another terminal on the same port, the port reverts to the unauthorized state. 2. Multi-mode This mode allows multiple terminals to connect to the physical port or channel group. In this mode, only one of the attached terminals needs to be authenticated. 3. Terminal authentication mode This mode allows multiple terminals to connect to the physical port or channel group. Each terminal is subject to authentication.
	VLAN-based authentication (static)	This mode controls authentication on a VLAN basis. Multiple terminals are allowed to connect to the VLAN. Each terminal is subject to authentication. Successfully authenticated terminals are permitted access to the VLAN.
	VLAN-based authentication (dynamic)	This mode controls authentication for terminals that attach to a MAC VLAN. Multiple terminals are allowed to connect to the VLAN. Successfully authenticated terminals are permitted access to the VLAN associated with its MAC VLAN.
Web authentication	Fixed VLAN mode	A terminal is permitted access to the VLAN after successful user authentication.
	Dynamic VLAN mode	After successful user authentication, the terminal is permitted access to the VLAN associated with its MAC VLAN. Authorization is enabled on the physical port where the MAC VLAN is configured.

Layer 2 authentication	Authentication mode	Overview
	Legacy mode	After successful user authentication, the terminal is permitted access to the VLAN associated with its MAC VLAN. Authorization is enabled for access to the MAC VLAN.
MAC-based authentication	Fixed VLAN mode	A terminal is permitted access to the VLAN after successful user authentication.
	Dynamic VLAN mode	After successful authentication, a terminal is permitted access to the VLAN assigned to its MAC VLAN.

5.1.2 Authentication method

Layer 2 authentication provides local authentication and RADIUS authentication method. For the local authentication method, the authentication data in the Switch is used. For the RADIUS authentication method, a RADIUS server is used. The following table describes the authentication methods that work with each type of Layer 2 authentication.

Table 5-2: Authentication methods used in layer 2 authentication

Layer 2 authentication	Authentication mode	Local authentication method	RADIUS authentication method
IEEE 802.1X	Port-based authentication	N	Y
	VLAN-based authentication (static)	N	Y
	VLAN-based authentication (dynamic)	N	Y
Web authentication	Fixed VLAN mode	Y	Y
	Dynamic VLAN mode	Y	Y
	Legacy mode	Y	Y
MAC-based authentication	Fixed VLAN mode	Y	Y
	Dynamic VLAN mode	Y	Y

Legend: Y: Supported; N: Not supported

5.1.3 Using dynamically assigned MAC VLANs with Layer 2 authentication

The Switch uses the Layer 2 authentication functions and modes described in the table below to dynamically configure the post-authentication VLAN to which authenticated terminals connect via an authenticating port on a MAC VLAN. At the point when no authenticated terminals are attached to an authenticating port, the dynamically assigned VLAN is deleted.

Table 5-3: Layer 2 authentication functions and authentication modes that permit dynamic VLAN assignment

Layer 2 authentication function	Authentication mode
IEEE 802.1X	VLAN-based authentication (dynamic)
Web authentication	Dynamic VLAN mode
MAC-based authentication	Dynamic VLAN mode

Note that a port configured as a MAC-based authentication port by the "switchport mac vlan" configuration command cannot perform VLAN switching to a post-authentication VLAN that is not specified in the command. Moreover, if the "switchport mac vlan" configuration command is applied to a MAC-based authentication port with a dynamically assigned VLAN, the authentication status is reset for all terminals attached to the VLAN dynamically assigned as the port's post-authentication VLAN.

5.2 Interoperability of Layer 2 authentication with other functions

This section describes the interoperability of Layer 2 authentication with other functions.

5.2.1 Using Layer 2 authentication with other functions

The following table describes the specifications for interoperability between Layer 2 authentication and other functions.

Table 5-4: Interoperability with other functions

Layer 2 authentication function	Function name		Interoperability
IEEE 802.1X	Link aggregation		Cannot coexist with Link Aggregation Control Protocol (LACP) channel groups.
	MAC address learning suppression		A VLAN and a port configured with that VLAN cannot be used at the same time.
	VLAN	Port VLAN	Can be used in port-based authentication and VLAN-based authentication (static).
		Protocol VLAN	Cannot coexist on the same device.
		MAC VLAN	Can be used in VLAN-based authentication (dynamic).
	Default VLAN		Can be used in port-based authentication and VLAN-based authentication (static). Can also be used as the pre-authentication VLAN in VLAN-based authentication (dynamic).
	VLAN extended function	VLAN tunneling	Cannot coexist on the same device.
		EAPOL forwarding	Cannot coexist on the same device.
	VXLAN [SL-L3A]		Do not configure port-based authentication or VLAN-based authentication (static) for VXLAN Network ports and VXLAN Access ports.
	Spanning Tree Protocol		Do not configure port-based authentication or VLAN-based authentication (static) for a port subject to a Spanning Tree Protocol.
	Ring Protocol		Do not configure port-based authentication or VLAN-based authentication (static) for a ring port subject to the Ring Protocol.
	IGMP snooping		• Cannot coexist on the same device for the port-based authentication. • Cannot coexist on the same device for the VLAN-based authentication (static). • For VLAN-based authentication (dynamic), pre-authentication VLAN and post-authentication VLAN cannot be used at the same time.

Layer 2 authentication function	Function name		Interoperability
	GSRP		Cannot coexist on the same device.
	VRRP		Can authenticate terminals except those attached to a VLAN configured with VRRP or the ports associated with that VLAN. IEEE 802.1X authentication cannot take place in the following contexts: • Port-based authentication for ports configured in a VLAN running VRRP • VLAN-based authentication (static) on a VLAN running VRRP • VLAN-based authentication (dynamic) on a VLAN running VRRP using an authentication default VLAN or MAC VLAN
	Uplink redundancy		Cannot be used for uplink port pairs
	IEEE 802.3ah/UDLD		Do not use on a port configured for port-based authentication or VLAN-based authentication (static).
	CFM		Cannot be used at the same time on the port where CFM is set.
	OADP, CDP		The Switch does not forward OADP or CDP traffic.
	PTP		Cannot coexist on the same device.
	VRF		Cannot coexist on the same device.
Web authentication	Link aggregation		Ports in a channel group cannot be used as an authentication port in fixed VLAN or dynamic VLAN mode.
	MAC address learning suppression		A VLAN and a port configured with that VLAN cannot be used at the same time.
	VLAN	Port VLAN	Can be used in fixed VLAN mode.
		Protocol VLAN	Cannot coexist on the same device.
		MAC VLAN	Can be used in dynamic VLAN mode and legacy mode.
	Default VLAN		Can be used in fixed VLAN mode. Can also be used as the pre-authentication VLAN in dynamic VLAN mode and legacy mode.
	VLAN extended function	VLAN tunneling	Cannot coexist on the same device.
		EAPOL forwarding	Can be used on the same device.
	VXLAN [SL-L3A]		Do not set fixed VLAN mode or dynamic VLAN mode to VXLAN Network ports and VXLAN Access ports.

Layer 2 authentication function	Function name		Interoperability
	Spanning Tree Protocol		Do not configure fixed VLAN mode or dynamic VLAN mode for a port subject to a Spanning Tree Protocol.
	Ring Protocol		Do not configure fixed VLAN mode or dynamic VLAN mode for a ring port subject to the Ring Protocol.
	IGMP snooping#		Cannot coexist on the same device.
	DHCP snooping		Cannot be used with a port assigned a VLAN ID with legacy mode specified.
	VRRP		Can authenticate terminals except those attached to a VLAN configured with VRRP or the ports associated with that VLAN. Do not configure MAC-based authentication in the following contexts: • In fixed VLAN mode on a port associated with a VLAN running VRRP • A port in dynamic VLAN mode configured on a VLAN (pre- or post-authentication VLAN) running VRRP • Authentication in legacy mode using a pre- or post-authentication VLAN running VRRP
	Uplink redundancy		Cannot be used for uplink port pairs
	IEEE 802.3ah/UDLD		Do not use on a port configured in fixed VLAN mode or dynamic VLAN mode.
	CFM		Cannot be used at the same time on the port where CFM is set.
	PTP		Cannot coexist on the same device.
	VRF		Cannot coexist on the same device.
MAC-based authentication	Link aggregation		Ports in a channel group cannot be used as an authentication port in fixed VLAN or dynamic VLAN mode.
	MAC address learning suppression		A VLAN and a port configured with that VLAN cannot be used at the same time.
	VLAN	Port VLAN	Can be used in fixed VLAN mode.
		Protocol VLAN	Cannot coexist on the same device.
		MAC VLAN	Can be used in dynamic VLAN mode.
	Default VLAN		Can be used in fixed VLAN mode. Can also be used as the pre-authentication VLAN in dynamic VLAN mode.

Layer 2 authentication function	Function name		Interoperability
	VLAN extended function	VLAN tunneling	Cannot coexist on the same device.
		EAPOL forwarding	Can be used on the same device.
	VXLAN [SL-L3A]		Do not configure MAC-based authentication for VXLAN Network ports and VXLAN Access ports.
	Spanning Tree Protocol		Do not configure MAC-based authentication for a port subject to a Spanning Tree Protocol.
	Ring Protocol		Do not configure MAC-based authentication for a link port subject to the Ring Protocol.
	IGMP snooping		Cannot coexist on the same device.
	VRRP		Can authenticate terminals except those attached to a VLAN configured with VRRP or the ports associated with that VLAN. Do not configure MAC-based authentication in the following contexts: • In fixed VLAN mode on a port associated with a VLAN running VRRP • A port in dynamic VLAN mode configured on a VLAN (pre- or post-authentication VLAN) running VRRP
	Uplink redundancy		Cannot be used for uplink port pairs
	IEEE 802.3ah/UDLD		Do not use IEEE 802.3ah/UDLD on a port configured for MAC-based authentication.
	CFM		Cannot be used at the same time on the port where CFM is set.
	PTP		Cannot coexist on the same device.
	VRF		Cannot coexist on the same device.

#: Web authentication is compatible with IGMP snooping in legacy mode.

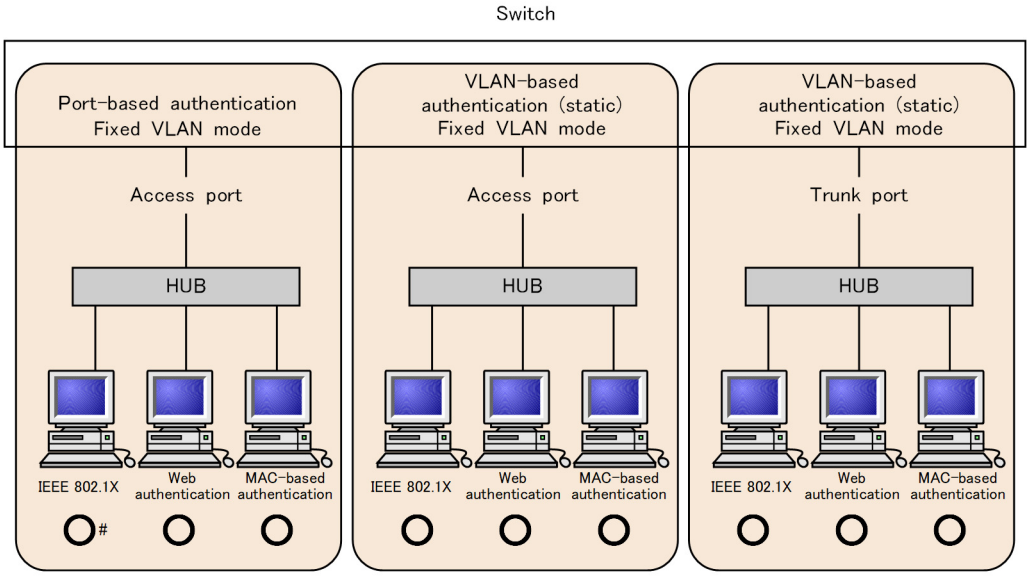
5.2.2 Using multiple authentication types on the same port

This section describes, for the following categories, the combinations of authentication mode that the Switch supports when using multiple Layer 2 authentication strategies simultaneously on the same port:

- Fixed VLAN mode
- Dynamic VLAN mode
- Fixed VLAN mode and dynamic VLAN mode
- Legacy mode

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

Figure 5-1: Interoperability of fixed VLAN modes on the same port



Legend: ○: Supported

#: Specify terminal authentication mode if you set up IEEE 802.1X port-based authentication at a port configured for Web or MAC-based authentication. Do not use single or multiple mode.

The following configuration commands are prohibited:
dot1x force-authorized-port
dot1x port-control force-authorized
dot1x port-control force-unauthorized
dot1x multiple-hosts

Table 5-5: Interoperability of fixed VLAN modes on the same port

Port type	IEEE 802.1X		Web authentication (Fixed VLAN mode)	MAC-based authentication (Fixed VLAN mode)
	Port-based authentication	VLAN-based authentication (static)		
Access port	Y#1	—	Y	Y
	—	Y	Y	Y
Channel group port (access port)	Y	N	—	—
	—	Y	—	—
Trunk port	—	Y#2	Y	Y
Channel group port (trunk port)	—	Y#2	—	—
Other	—	—	—	—

Legend:
Y: Supported
N: Not supported, but can be specified in the device configuration
—: Cannot be specified in the device configuration

#1

You must use terminal authentication mode if you set up IEEE 802.1X port-based authentication for a port that has Web authentication and MAC-based authentication configured. (Do not use single mode or multi-mode.)

Omit the following configuration commands:

dot1x force-authorized-port

dot1x port-control force-authorized

dot1x port-control force-unauthorized

dot1x multiple-hosts

#2

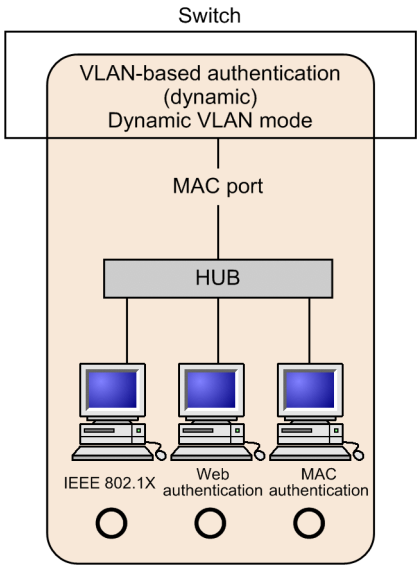
When VLANs that do and do not require authentication are assigned to the same port, terminals connected to that port will be unable to access the non-authenticating VLANs. You can overcome this limitation by using the authentication-exempted port option.

Example of interpreting interoperability tables:

When the connection target is an access port, you can use IEEE 802.1X port-based authentication, Web authentication (fixed VLAN mode), and MAC-based authentication (fixed VLAN mode) concurrently on the same port. Alternatively, you can use IEEE 802.1X VLAN-based authentication (static), Web authentication (fixed VLAN mode), and MAC-based authentication (fixed VLAN mode) on the same port.

(2) Dynamic VLAN mode interoperability on the same port

Figure 5-2: Interoperability of dynamic VLAN modes on the same port



Legend: ○: Supported

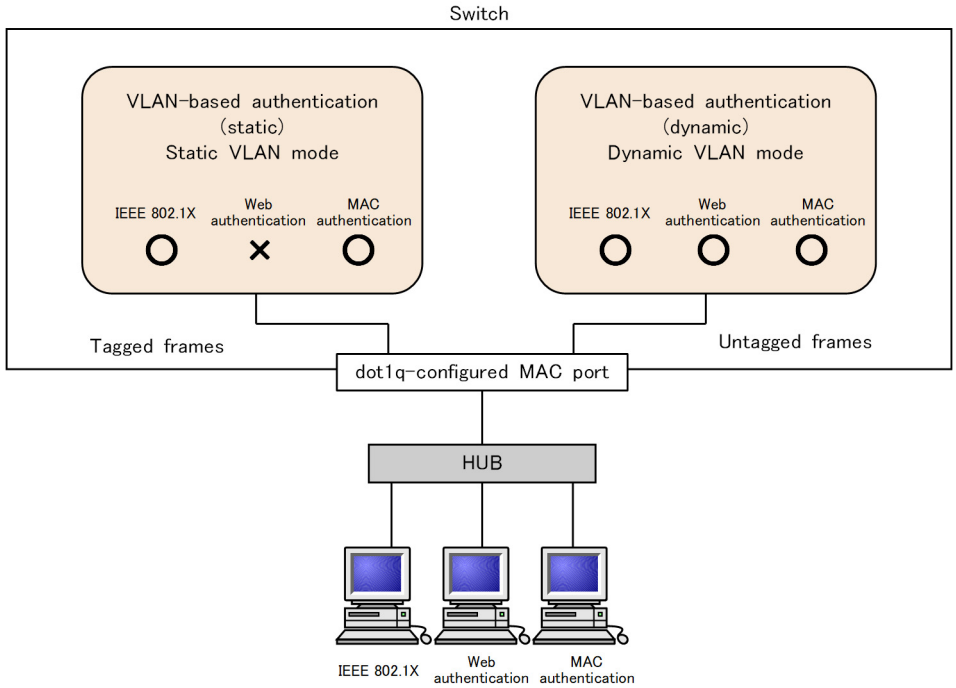
Table 5-6: Interoperability of dynamic VLAN modes on the same port

Port type	IEEE 802.1X VLAN-based authentication (dynamic)	Web authentication (Dynamic VLAN mode)	MAC-based authentication (Dynamic VLAN mode)
MAC port	Y	Y	Y
Other	N	N	N

Legend: Y: Operable; N: Inoperable

(3) Dynamic and fixed VLAN mode interoperability on the same port

Figure 5-3: Interoperability of dynamic and fixed VLAN modes on the same port



Legend: ○: Supported ×: Not supported

Table 5-7: Interoperability of dynamic and fixed VLAN modes on the same port

Port type	Type of received frames	IEEE 802.1X		Web authentication		MAC-based authentication	
		VLAN-based authentication (static)	VLAN-based authentication (dynamic)	Fixed VLAN mode	Dynamic VLAN mode	Fixed VLAN mode	Dynamic VLAN mode
MAC port configured with dot1q	Tagged frame	Y#1	N	N	N	Y	N
	Untagged frame	N	Y	Y#2	Y	Y#2	Y

Legend: Y: Operable; N: Inoperable

#1

When VLANs that do and do not require authentication are assigned to the same port, terminals connected to that port will be unable to access the non-authenticating VLANs. You can overcome this limitation by using the authentication-exempted port option.

#2

When using RADIUS authentication method, if the RADIUS server does not indicate which VLAN a terminal should attach to after authentication, the terminal attaches to the native VLAN as a member of a fixed VLAN. However, when a terminal is moved to a different port, the destination port runs in dynamic VLAN mode.

(4) Legacy mode interoperability on the same port

Table 5-8: Interoperability of legacy modes on the same port

Port type	IEEE 802.1X VLAN-based authentication (dynamic)	Web authentication (legacy mode)	MAC-based authentication (all modes)
MAC port	Y	Y	N
Other	N	N	N

Legend: Y: Operable; N: Inoperable

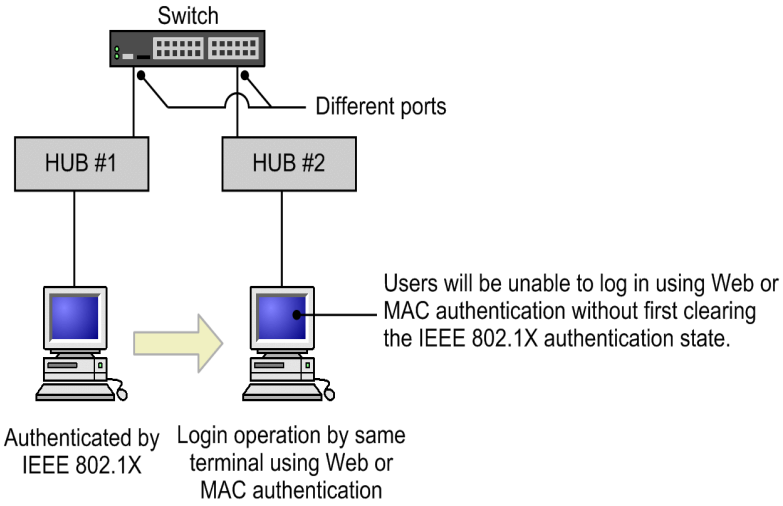
5.2.3 Priority of Layer 2 authentication types

(1) Priority of IEEE 802.1X relative to Web or MAC-based authentication

If a terminal that has undergone successful Web or MAC-based authentication later completes IEEE 802.1X port-based or VLAN-based (static) authentication, the result of the IEEE 802.1X process takes priority. In this case, the terminal loses the authentication status it gained by Web or MAC-based authentication. Users who performed Web authentication will not be presented with a logout page.

The figure below illustrates a situation where an IEEE 802.1X-authenticated terminal (having undergone port-based authentication in terminal authentication mode or VLAN-based authentication in static mode) is moved from one hub (HUB#1) to another hub (HUB#2) attached to a different port. Here, the user will be unable to log in using Web or MAC-based authentication (in fixed VLAN mode) without first canceling the IEEE 802.1X authentication status. To do so, use the "clear dot1x auth-state" command.

Figure 5-4: Using Web or MAC-based authentication after moving an IEEE 802.1X-authenticated terminal between ports



If this same terminal successfully undergoes Web authentication (dynamic VLAN mode or legacy mode) or MAC-based authentication (dynamic VLAN mode), and then later completes IEEE 802.1X VLAN-based authentication (dynamic), the result of the IEEE 802.1X process takes priority. In this case, the terminal will be attached to the VLAN specified in the IEEE 802.1X configuration, and lose the authentication status it gained by Web or MAC-based authentication. Users who performed Web authentication will not be presented with a logout page.

(2) Relative priority of Web and MAC-based authentication

If a terminal that has successfully undergone MAC-based authentication then attempts Web authentication, the Web authentication will fail. Similarly, if a Web-authenticated terminal subsequently attempts MAC-based authentication, the authentication process will end in an error and the Web authentication status will remain in effect.

5.3 Function common to all Layer 2 authentication modes

This section describes the function used in common by all modes of Layer 2 authentication, and the prerequisites for their configuration.

- Configuring the unit of authentication
- Permitting communication by unauthenticated terminals
- Limited number of authentications
- Forced authentication
- Moving authenticated terminals between ports
- Dead-interval function of RADIUS server communication
- Behavior with dot1q configured at a MAC port

5.3.1 Setting the unit of authentication

Layer 2 authentication can be configured on the basis of physical ports or VLANs. The unit of authentication depends on the Layer 2 authentication function and authentication mode you select.

The following table describes the combinations of Layer 2 authentication function and authentication modes applicable to each unit of authentication.

Table 5-9: Layer 2 authentication function and authentication modes by authentication unit

Authentication unit	Layer 2 authentication function and mode
Physical ports	• IEEE 802.1X (port-based authentication) • Web authentication (fixed VLAN mode) • Web authentication (dynamic VLAN mode) • MAC-based authentication (fixed VLAN mode) • MAC-based authentication (dynamic VLAN mode)
VLAN	• IEEE 802.1X (VLAN-based authentication (static)) • IEEE 802.1X (VLAN-based authentication (dynamic)) • Web authentication (legacy mode)

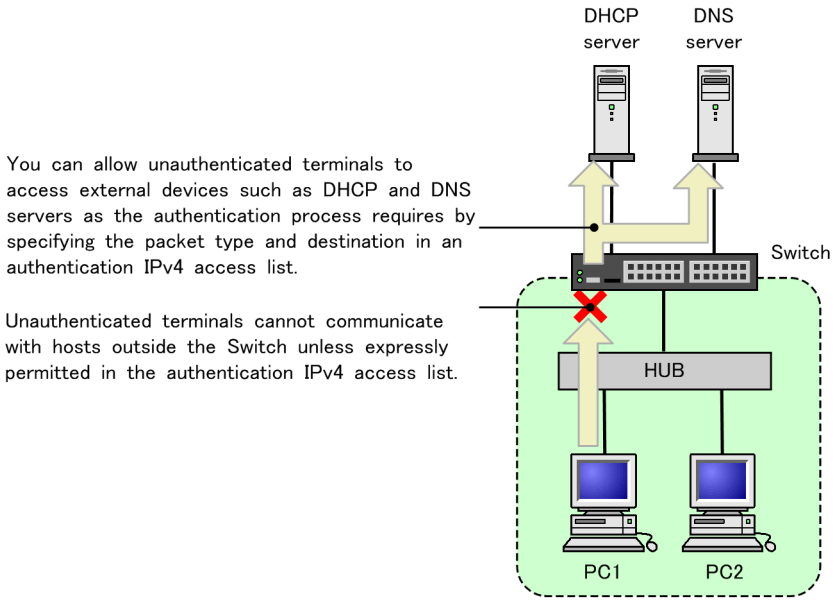
5.3.2 Permitting communication by unauthenticated terminals

(1) Authentication IPv4 access list

Unauthenticated terminals must be able to communicate with the DHCP server and DNS server to obtain distributed IP addresses and perform name resolution.

You can allow an unauthenticated terminal to access devices beyond the Switch (such as DHCP and DNS servers) by configuring an IPv4 access list (also referred to as the authentication IPv4 access list) for the pre-authentication VLAN.

Figure 5-5: Communication with authentication IPv4 access list applied



The authentication IPv4 access list differs from standard access lists (such as those configured by the "ip access-group" configuration command) in that the filter conditions no longer apply after authentication has taken place. Note that the filter conditions defined in standard access lists take priority over those in the authentication IPv4 access list. If you configure a standard access list and an authentication IPv4 access list for an authenticating port, the filter conditions in the standard access list will apply before and after authentication. For this reason, make sure that you include the filter conditions of the authentication IPv4 access list in the standard access list.

Before an unauthenticated terminal can obtain an IP address distributed 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 filter conditions like the following in the access list:

Example of filter 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 authentication IPv4 access list contains more than the maximum number of filter conditions, the configuration command ignores the excess conditions.
- Even if the following filter conditions are specified, they will not be applied by the "permit" or "deny" configuration command:
  - TCP port range specification
  - UDP port range specification

- user-priority
- vlan

- Authentication programs implicitly discard all packets that are not expressly permitted. This does not count in the number of filtering conditions.
- If you use the "permit ip host <ip address>" configuration command to add the IP address of a terminal to the authentication IPv4 access list as a filtering condition, the Switch will relay ARP packets from that terminal regardless of its authentication status without an "authentication arp-relay" command.
- Because Web authentication IP addresses are excluded from the destination IP addresses of filter conditions for an authentication IPv4 access list, the login operation can be performed with a Web authentication IP address even if a Web authentication IP address is included as a destination IP addresses.

(2) ARP packet relay function

The Switch does not normally forward ARP packets from unauthorized terminals to external devices. However, you can configure the Switch to forward such packets by using the "authentication arp-relay" configuration command.

(3) Function support by Layer 2 authentication type

The following table describes which Layer 2 authentication types support authentication IPv4 access list and ARP packet relay function.

Table 5-10: Support for authentication IPv4 access list and ARP packet relay function by Layer 2 authentication type

Function	IEEE 802.1X			Web authentication			MAC-based authentication	
	Port-based authentication	VLAN-based authentication (static)	VLAN-based authentication (dynamic)	Fixed VLAN mode	Dynamic VLAN mode	Legacy mode	Fixed VLAN mode	Dynamic VLAN mode
Authentication IPv4 access list	Y	Y	Y	Y	Y	N	Y	Y
ARP packet relay function	Y	Y	Y	Y	Y	N	Y	Y

Legend: Y: Operable; N: Inoperable

(4) Note on DHCP snooping

If DHCP snooping deems an authenticating port to be an untrusted port, DHCP packets sent from that port will be subject to DHCP snooping even if bootps or bootpc is specified as the protocol name in the authentication IPv4 access list. In this situation, the Switch will only forward DHCP packets allowed by DHCP snooping.

Because the ARP packets sent from the terminal will also be subject to DHCP snooping, the Switches will only forward ARP packets as DHCP snooping permits.

5.3.3 Limited number of authentications

You can limit the number of authenticated users across all Layer 2 authentication types.

Authenticated users can be limited:

- Per port
- Per switch

(1) Limited number of port-based authentication

You can use the "authentication max-user" command to set the maximum number of authentication sessions allowed on a port. An authentication error occurs when the number of users authenticated by Layer 2 authentication exceeds the maximum number set for the port.

(2) Limited number of switch-based authentication

You can use the "authentication max-user" command to set the maximum number of authenticated users allowed on a Switch. An authentication error occurs when the total number of authenticated by Layer 2 authentication exceeds the maximum number set for the Switch.

(3) Support for limiting authenticated users by Layer 2 authentication type

The following table describes which Layer 2 authentication types support port-level and switch-level restrictions on the number of authenticated users.

Table 5-11: Support for limiting authenticated users by layer 2 authentication type

Function	IEEE 802.1X			Web authentication			MAC-based authentication	
	Port-based authentication	VLAN-based authentication (static)	VLAN-based authentication (dynamic)	Fixed VLAN mode	Dynamic VLAN mode	Legacy mode	Fixed VLAN mode	Dynamic VLAN mode
Limited number of port-based authentication	Y#1	Y#1	Y#2	Y	Y	N	Y	Y
Limited number of switch-based authentication	Y#1	Y#1	Y#2	Y	Y	N	Y	Y

Legend: Y: Supported; N: Not supported

#1

Does not apply to terminals whose communication is restricted. For details, see "6.2.9 Blocking traffic from authenticated terminals".

#2

These modes might be subject to limits on the number of authenticated users depending on how the Switch is configured. For details, see "6.2.8 VLAN-based authentication (dynamic) behavior modes".

5.3.4 Forced authentication

Ports for which the "authentication force-authorized enable" command is configured consider all login requests to be successful in the following circumstances:

- RADIUS authentication method is specified but there is no response from the designated RADIUS server
- Local authentication method is specified, but no authentication data exists on the device:
  - For Web authentication, this means that no users are registered in the internal Web authentication DB.

- For MAC-based authentication, this means that no MAC addresses are registered in the internal MAC-based authentication database.

Users subject to forced authentication are treated the same as normal authenticated users for the duration of the authentication session. The following table describes the authentication modes that support forced authentication:

Table 5-12: Support for forced authentication by authentication mode

Function	IEEE 802.1X			Web authentication			MAC-based authentication	
	Port-based authentication	VLAN-based authentication (static)	VLAN-based authentication (dynamic)	Fixed VLAN mode	Dynamic VLAN mode	Legacy mode	Fixed VLAN mode	Dynamic VLAN mode
Forced authentication	N	N	N	Y	Y#	N	Y	Y#

Legend: Y: Operable; N: Inoperable

#:

In dynamic VLAN mode, the "authentication force-authorized vlan" configuration command specifies the VLAN ID assigned to the forcibly authenticated client. If you omit the "authentication force-authorized vlan" configuration command, the client is attached to the native VLAN.

Notes on configuring forced authentication:

Because forced authentication can pose a security risk, consider the implications carefully before using it.

Example: When using a RADIUS server for MAC-based authentication

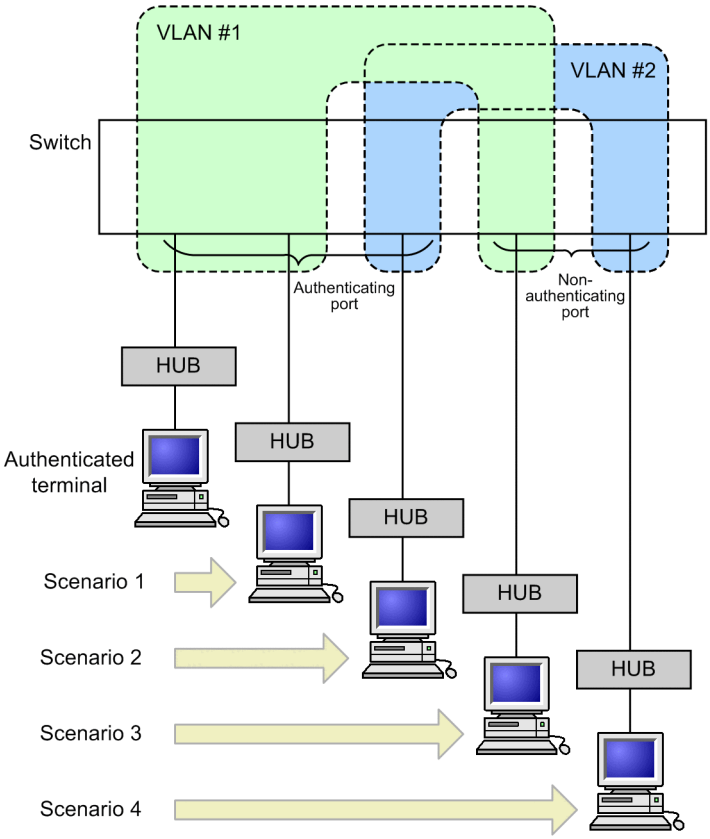
When Web authentication and MAC-based authentication are both configured for a port in force-authorized mode and a RADIUS server is set up for MAC-based authentication, if communication with the RADIUS server fails for some reason, forced authentication comes into behavior. In this case, terminals subject to Web authentication will be permitted access without going through the Web authentication process.

5.3.5 Moving authenticated terminals between ports

This section describes how the port status and authentication status are affected when you move a terminal that has undergone Layer 2 authentication to a different port.

The figure below depicts the four scenarios for moving an authenticated terminal between ports.

Figure 5-6: Examples of moving authenticated terminals between ports



When using a MAC VLAN, scenario 1 and scenario 2 work as follows:

Scenario 1:

The terminal will retain the same VLAN membership if either of the following conditions is applied at the destination port:

- The same VLAN ID is configured in the "switchport mac vlan" configuration command.
- The same VLAN ID has already been registered dynamically by a Layer 2 authentication process.

If MAC VLAN IDs are not dynamically registered, the ID of a VLAN to which a terminal belongs is created when the terminal authenticated by Web or MAC authentication moves. For this reason, this is regarded as a move to the same VLAN.

Scenario 2:

The terminal will change VLAN membership if the following conditions are satisfied at the destination port:

- A different VLAN ID is configured in the "switchport mac vlan" configuration command.

If MAC VLAN IDs are not dynamically created and a terminal of IEEE 802.1X moves, it is regarded as a move to another VLAN.

The behavior of the switch in the four scenarios is described below for each type of Layer 2 authentication.

(1) Behavior when moving IEEE 802.1X-authenticated terminals between ports

The tables below describe, for each authentication mode, what happens in terms of the port status and authentication status when you move an IEEE 802.1X-authenticated terminal to another port.

Table 5-13: Behavior when moving IEEE 802.1X-authenticated terminals between ports (port-based authentication)

Scenario	Destination port	VLAN	User authentication status	MAC address table of source port	Authentication status of source port	Ability to communicate after movement
1	Authenticating port	Same VLAN	Undergoes re-authentication at destination port	Port information updated	Existing authentication canceled	Cannot communicate until re-authenticated
2	Authenticating port	Different VLAN	Undergoes re-authentication at destination port	Not updated	Authorized status remains	Cannot communicate until re-authenticated
3	Non-authenticating port	Same VLAN	Authorized status remains	Not updated	Authorized status remains	Cannot communicate
4	Non-authenticating port	Different VLAN	Authorized status remains	Not updated	Authorized status remains	Can communicate

Table 5-14: Behavior when moving IEEE 802.1X-authenticated terminals between ports (VLAN-based authentication (static))

Scenario	Destination port	VLAN	User authentication status	MAC address table of source port	Authentication status of source port	Ability to communicate after movement
1	Authenticating port	Same VLAN	Authorization continues	Port information updated	Continues	Can communicate
2	Authenticating port	Different VLAN	Undergoes re-authentication at destination port	Not updated	Authorized status remains	Cannot communicate until re-authenticated
3	Non-authenticating port	Same VLAN	—	—	—	—
4	Non-authenticating port	Different VLAN	Authorized status remains	Not updated	Authorized status remains	Can communicate

Legend:

—: Because VLAN-based authentication (static) takes place at the VLAN level, the VLAN will not contain any non-authenticating ports.

Table 5-15: Behavior when moving IEEE 802.1X-authenticated terminals between ports (VLAN-based authentication (dynamic))

Scenario	Destination port	VLAN	User authentication status	MAC address table of source port	Authentication status of source port	Ability to communicate after movement
1	Authenticating port	Same VLAN	Authorization continues	Port information updated	Continues	Can communicate

Scenario	Destination port	VLAN	User authentication status	MAC address table of source port	Authentication status of source port	Ability to communicate after movement
2	Authenticating port	Different VLAN	Undergoes re-authentication at destination port	Deleted	Existing authentication canceled	Cannot communicate until re-authenticated
3	Non-authenticating port	Same VLAN	—	—	—	—
4	Non-authenticating port	Different VLAN	Authorized status remains	Not updated	Authorized status remains	Can communicate

Legend:

—: Because VLAN-based authentication (dynamic) takes place at the VLAN level, the VLAN will not contain any non-authenticating ports.

(2) Behavior when moving Web-authenticated terminals between ports

The tables below describe, for each authentication mode, what happens in terms of the port status and authentication status when you move a Web-authenticated terminal to another port.

Table 5-16: Behavior when moving Web-authenticated terminals between ports (fixed VLAN mode)

Scenario	Destination port	VLAN	User authentication status	MAC address table of source port	Authentication status of source port	Ability to communicate after movement
1	Authenticating port	Same VLAN	Authorization continues	Port information updated	Continues	Can communicate
2	Authenticating port	Different VLAN	Authorized status remains	Not updated	Authorized status remains	Cannot communicate until re-authenticated
3	Non-authenticating port	Same VLAN	Authorized status remains	Not updated	Authorized status remains	Cannot communicate
4	Non-authenticating port	Different VLAN	Authorized status remains	Not updated	Authorized status remains	Can communicate

Table 5-17: Behavior when moving Web-authenticated terminals between ports (dynamic VLAN mode)

Scenario	Destination port	VLAN	User authentication status	MAC address table of source port	Authentication status of source port	Ability to communicate after movement
1	Authenticating port	Same VLAN	Authorization continues	Port information updated	Continues	Can communicate

Scenario	Destination port	VLAN	User authentication status	MAC address table of source port	Authentication status of source port	Ability to communicate after movement
2	Authenticating port	Different VLAN	Authorized status remains	Not updated	Authorized status remains	Cannot communicate
3	Non-authenticating port	Same VLAN	Authorized status remains	Not updated	Authorized status remains	Cannot communicate
4	Non-authenticating port	Different VLAN	Authorized status remains	Not updated	Authorized status remains	Can communicate

Table 5-18: Behavior when moving Web-authenticated terminals between ports (legacy mode)

Scenario	Destination port	VLAN	User authentication status	MAC address table of source port	Authentication status of source port	Ability to communicate after movement
1	Authenticating port	Same VLAN	Authorization continues	Port information updated	Continues	Can communicate
2	Authenticating port	Different VLAN	Authorized status remains	Not updated	Authorized status remains	Cannot communicate
3	Non-authenticating port	Same VLAN	—	—	—	—
4	Non-authenticating port	Different VLAN	Authorized status remains	Not updated	Authorized status remains	Can communicate

Legend:

—: Because Web authentication (legacy mode) takes place at the VLAN level, the VLAN will not contain any non-authenticating ports.

(3) Behavior when moving MAC-authenticated terminals between ports

The tables below describe, for each authentication mode, what happens in terms of the port status and authentication status when you move a MAC-authenticated terminal to another port.

Table 5-19: Behavior when moving MAC-authenticated terminals between ports (fixed VLAN mode)

Scenario	Destination port	VLAN	User authentication status	MAC address table of source port	Authentication status of source port	Ability to communicate after movement
1	Authenticating port	Same VLAN	Authorization continues	Port information updated	Continues	Can communicate
2	Authenticating port	Different VLAN	Undergoes re-authentication#	Deleted#	Existing authentication canceled#	Cannot communicate until re-authenticated#

Scenario	Destination port	VLAN	User authentication status	MAC address table of source port	Authentication status of source port	Ability to communicate after movement
3	Non-authenticating port	Same VLAN	Authorized status remains	Not updated	Authorized status remains	Cannot communicate
4	Non-authenticating port	Different VLAN	Authorized status remains	Not updated	Authorized status remains	Can communicate

#

This behavior is performed when broadcast ARP packets are sent after a port is moved from an authenticated terminal. The authenticated status remains without being canceled for packets other than the broadcast ARP packets.

Table 5-20: Behavior when moving MAC-authenticated terminals between ports (dynamic VLAN mode)

Scenario	Destination port	VLAN	User authentication status	MAC address table of source port	Authentication status of source port	Ability to communicate after movement
1	Authenticating port	Same VLAN	Authorization continues	Port information updated	Continues	Can communicate
2	Authenticating port	Different VLAN	Authentication status canceled[#]	Deleted[#]	Existing authentication canceled[#]	Cannot communicate until re-authenticated[#]
3	Non-authenticating port	Same VLAN	Authorized status remains	Not updated	Authorized status remains	Cannot communicate
4	Non-authenticating port	Different VLAN	Authorized status remains	Not updated	Authorized status remains	Can communicate

#

This operation is performed when broadcast ARP packets are sent after a port is moved from an authenticated terminal. The authenticated status remains without being canceled for packets other than the broadcast ARP packets.

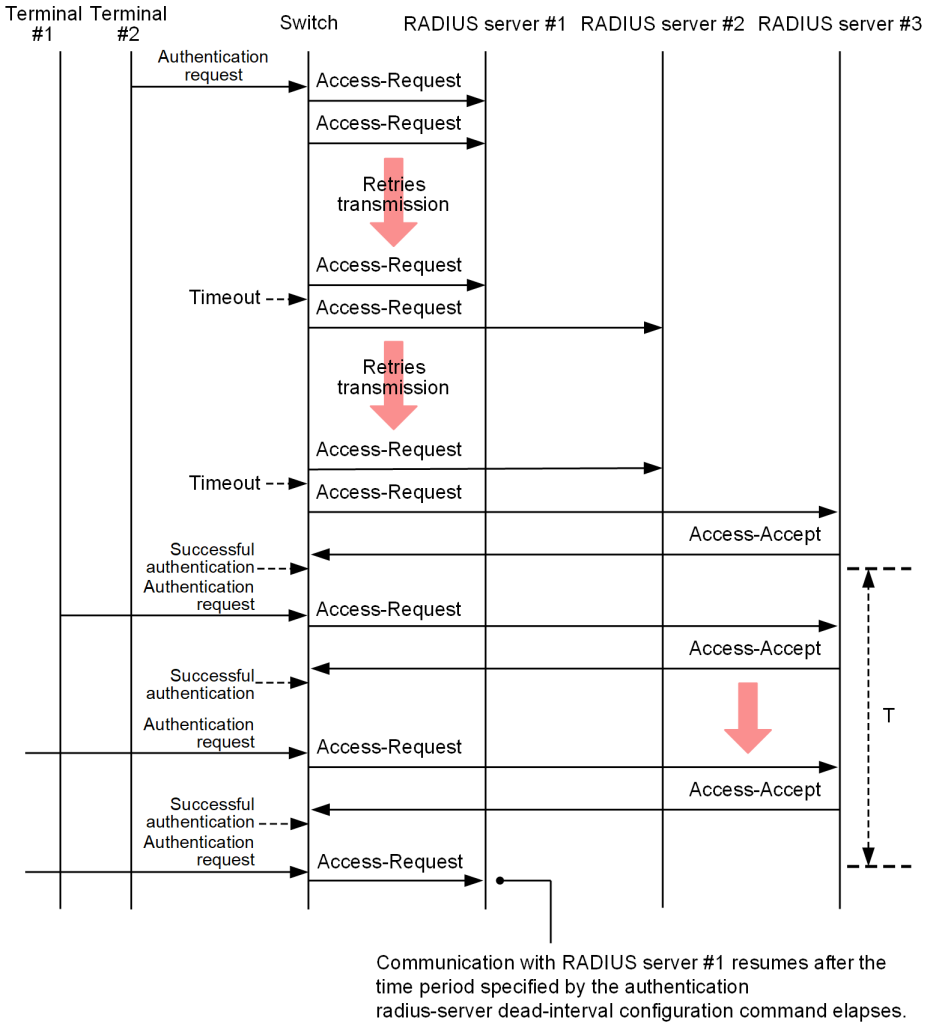
5.3.6 Dead-interval function of RADIUS server communication

If the switch does not receive a response from a RADIUS server, it will use other RADIUS servers for a period specified by the "authentication radius-server dead-interval" configuration command. The initial RADIUS server resumes authentication after this interval. If all RADIUS servers are unresponsive, authentication will fail for the duration of the period specified by the "authentication radius-server dead-interval" configuration command, even if communication is restored within the dead interval. To restore the RADIUS servers to active status, execute the following operation commands:

- Web authentication: clear web-authentication dead-interval-timer
- MAC-based authentication: clear mac-authentication dead-interval-timer

The figure below illustrates how the dead interval function works with RADIUS servers.

Figure 5-7: Dead-interval function of RADIUS server communication



T: The time specified by the authentication radius-server dead-interval configuration command

The following table describes which Layer 2 authentication types support the use of a dead interval with RADIUS servers.

Table 5-21: Support for RADIUS server dead interval by Layer 2 authentication type

Function	IEEE 802.1X			Web authentication			MAC-based authentication	
	Port-based authentication	VLAN-based authentication (static)	VLAN-based authentication (dynamic)	Fixed VLAN mode	Dynamic VLAN mode	Legacy mode	Fixed VLAN mode	Dynamic VLAN mode
Dead-interval function of RADIUS server communication	N	N	N	Y	Y	N	Y	Y

Legend: Y: Supported; N: Not supported

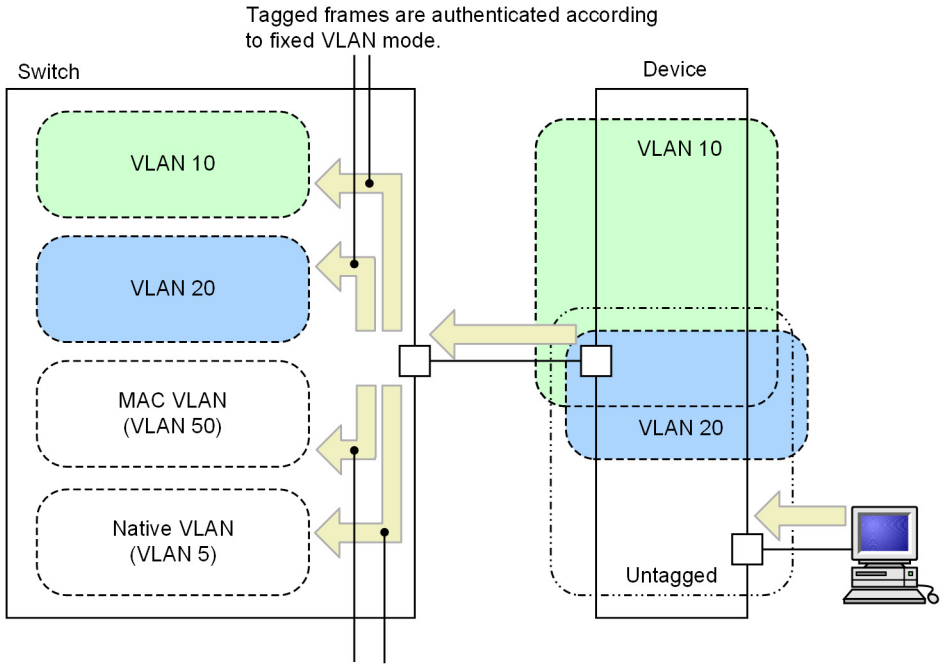
5.3.7 Behavior with dot1q configured at a MAC port

If you use the "switchport mac dot1q vlan" configuration command to configure dot1q at a MAC port, tagged frames entering that port are authenticated according to fixed VLAN mode.

Untagged frames are authenticated according to dynamic VLAN mode. Note that untagged frames are associated with the native VLAN prior to authentication and with the designated VLAN ID after successful authentication.

The following figure describes the behavior of the MAC port with dot1q configured:

Figure 5-8: Behavior of MAC port with dot1q configured



Untagged frames are authenticated according to dynamic VLAN mode.
Note that untagged frames are associated with the native VLAN prior to authentication, and with the MAC VLAN after successful authentication.

If the "mac-authentication dot1q-vlan force-authorized" configuration command is applied to the MAC port, the switch will forward tagged frames from that port without requiring it to undergo MAC-based authentication.

Because a terminal thus exempted from authentication is treated as an authenticated MAC terminal, keep the following in mind:

- Authentication-exempted terminals (MAC addresses) count against the maximum number of authenticated users allowed on a port.
- After you cancel terminal's authentication-exempted status, a logout message appears in the action log. Because authentication-exempted status is canceled when a terminal is moved to another port, the same message will appear in the action log after you move an authentication-exempted terminal between ports.
- The following triggers cancel the authentication-exempted status of a terminal:
  - An operation command is used to cancel authentication-exempted status.

    The authentication-exempted status of a terminal will be canceled if you specify its MAC address in the "clear mac-authentication auth-state" operation command.

    It also cancels its exempted status if you specify the option of the "clear mac-authentication auth-state" operation command that cancels the authentication status for all MAC-authenticated terminals.

- The port to which an authentication-exempted terminal is connected is in link-down status.

  When the switch detects that a port is in link-down status, the terminals attached to the port will lose their authentication-exempted status.

- An authentication-exempted terminal is aged out from the MAC address table.

  If there is no communication from an authentication-exempted terminal for a period of approximately 10 minutes after the aging time of the MAC address table has elapsed, the authentication-exempted status is canceled.

- The VLAN configuration changes.

  The authentication-exempted status of a terminal will be canceled if you use a configuration command to change the configuration of the VLAN to which the terminal belongs.

  The following configuration changes trigger a logout:

  - Deletion of the VLAN
  - Suspension of the VLAN

- The authentication mode changes.

  The authentication-exempted status of a terminal will be canceled if the "copy" command is used to change authentication modes.

- MAC-based authentication is deleted.

  The authentication-exempted status of a terminal will be canceled if the "no mac-authentication system-auth-control" configuration command is used to delete MAC-based authentication.

The following table describes the behavior of Layer 2 authentication with dot1q configured at a MAC port:

Table 5-22: Behavior of Layer 2 authentication with dot1q configured at a MAC port

Received frames	IEEE 802.1X	Web authentication	MAC-based authentication
Untagged frame	Subject to VLAN-based authentication (dynamic)	Subject to authentication in dynamic VLAN mode	Subject to authentication in dynamic VLAN mode
Tagged frame	Subject to VLAN-based authentication (static)	Cannot be authenticated	Subject to authentication in fixed VLAN mode

5.4 Notes on using Layer 2 authentication

5.4.1 Notes on changing the Switch configuration and status

(1) Notes on using the set clock command

The duration of an authentication session is managed using the internal clock of the Switch. Keep in mind that using the "set clock" operation command to change the system and time has a flow-on effect on the duration of authentication sessions.

For example, if you advance the clock by three hours, sessions will appear to be in progress for three hours longer than they actually have. Conversely, if you set the clock back by three hours, authentication sessions will be extended by three hours.

(2) Notes on changing the authentication mode

To change the authentication mode while Web authentication or MAC-based authentication is enabled, execute the "shutdown" configuration command for all ports to be authenticated so that they are disconnected from the authentication terminal, wait at least 60 seconds, and then change the authentication mode. After changing the authentication mode, execute the "no shutdown" command for all the ports to be authenticated.

If you changed the authentication mode while the authentication terminal is connected, use the restart web-authentication or "restart mac-authentication" operation command to restart the Web authentication program or MAC-based authentication program.

(3) Note on authentication ports and MAC VLAN configuration

If any of the operations below are performed when the value obtained from the following formula exceeds approximately 1600, the time period until authentication starts or until communication of the authenticated terminal is restored become longer because of the time period required for initial setup of the MAC manager program: the total number of authentication ports set for IEEE 802.1X (VLAN-based authentication (dynamic)), Web authentication (dynamic VLAN mode), and MAC-based authentication (dynamic VLAN mode) x the value set for the "vlan <vlan id list> mac-based" configuration command

- Start procedures
- Executing the "reload" operation command
- Executing the "copy" operation command
- Execution of the "restart vlan" operation command
- Executing the "restart vlan" operation command with the mac-manager parameter specified

5.4.2 Notes on using RADIUS server

(1) Notes on specifying RADIUS servers by host name

If you specify a RADIUS server by its host name, the following issues might occur if, for example, the switch is unable to connect to the DNS server to perform name resolution:

- When executing an operation command:
  - Command execution results are slow to appear.
  - Command output stops midstream, and then resumes following a brief pause.
  - The message Connection failed to 802.1X program. appears during IEEE 802.1X authentication.

- The message Can't execute. appears during MAC-based or Web authentication.

- When executing a configuration command:
  - It might take some time to save the new configuration or for configuration changes to take effect.
- When an SNMP manager acquires MIB information for IEEE 802.1X:
  - Response times might be slow, or SNMP might time out while waiting for a response.

To avoid these issues, we recommend that you specify the RADIUS server by its IP address in IPv4 or IPv6 format. If you must specify a host name, make sure that the DNS server is available to respond to requests from the switch.

(2) Notes for IEEE 802.1X when connectivity to the RADIUS server is lost

With IEEE 802.1X, if the switch cannot communicate with the RADIUS server, or the RADIUS server specified by the "radius-server host" configuration command does not exist, each login request takes a long time to process. That is, the duration of a single login attempt will be equivalent to the timeout value specified by the "radius-server timeout" configuration command multiplied by the number of retries specified by the "radius-server retransmit" configuration command.

If you use multiple "radius-server host" configuration commands to specify multiple RADIUS servers, login requests will still take a long time to process when connectivity with the first configured RADIUS server is lost. This is because the terminal will always send requests to hosts in the order you specify them.

If such a situation occurs, halt the login process, and then use the "radius-server host" configuration command to configure a working RADIUS server. You can then resume the login process.

5.5 Configuration common to all Layer 2 authentication modes

5.5.1 List of configuration commands

The following table describes the list of configuration commands for Layer 2 authentication.

Table 5-23: List of configuration commands

Command name	Description	Applicable Layer 2 authentication types		
		IEEE 802.1X	Web authentication#	MAC-based authentication
authentication arp-relay	Specify this command if you want the Switch to forward ARP packets from unauthenticated terminals to destinations outside the Switch.	Y	Y	Y
authentication force-authorized enable	Enables forced authentication.	—	Y	Y
authentication force-authorized vlan	Specifies the VLAN ID to be assigned to force-authorized users in dynamic VLAN mode.	—	Y	Y
authentication ip access-group	If you want the switch to forward packets from unauthenticated terminals to destinations outside the Switch, use this command to specify which types of packets to forward by means of an IPv4 access list.	Y	Y	Y
authentication max-user (global)	Specifies the maximum number of authenticated users permitted on the device.	Y	Y	Y
authentication max-user (Ethernet interface)	Specifies the maximum number of authenticated users permitted on each port.	Y	Y	Y
authentication radius-server dead-interval	Specifies how long to wait before attempting to access the highest-priority RADIUS server again after it stops responding.	—	Y	Y

Legend: Y: Can be used; —: Cannot be used

#: For Web authentication, the commands apply in fixed and dynamic VLAN modes.

5.5.2 Configuring common parameter for Layer 2 authentication

(1) Configuring whether ARP packets from unauthenticated terminals are forwarded outside the Switch

Points to note

Configures the Switch to forward ARP packets received from unauthorized terminals to a destination outside the Switch.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/10
(config-if)# web-authentication port
(config-if)# mac-authentication port
(config-if)# authentication arp-relay
(config-if)# exit
```

Configures the switch to forward ARP packets through port 1/0/10, which is subject to Web and MAC-based authentication.

(2) Setting the authentication IPv4 access list

Points to note

Configure an authentication IPv4 access list that allows traffic from unauthenticated terminals to reach destinations outside the Switch.

Command examples

1.
```
(config)# ip access-list extended 100
(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 gigabitethernet 1/0/10
(config-if)# web-authentication port
(config-if)# mac-authentication port
(config-if)# authentication ip access-group 100
(config-if)# exit
```

Configures an authentication IPv4 access list that permits unauthorized terminals to broadcast DHCP packets and to access IP address 10.0.0.1 (the DNS server).

(3) Configuring forced authentication

Points to note

Forcibly authenticate terminals when there is no response from the RADIUS server. For MAC or Web authentication, this configuration forcibly authenticates terminals when no data is in the internal MAC-based authentication DB or Web authentication DB.

Command examples

1.
```
(config)# authentication force-authorized enable
```

Enables forced authentication.

(4) Setting the VLAN ID used after forced authentication

Points to note

Configures the VLAN ID the switch assigns to a terminal that undergoes forced authentication in dynamic VLAN mode.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/5
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 100,200
```

```
(config-if)# web-authentication port
(config-if)# mac-authentication port
(config-if)# authentication force-authorized vlan 100
(config-if)# exit
```

Specifies that VLAN ID 100 is assigned to terminals that undergo forced authentication while attached to port 1/0/5, which is configured for Web and MAC-based authentication in dynamic VLAN mode.

(5) Setting the limited number of switch-based authentication

Points to note

Sets the maximum number of Layer 2 authenticated users allowed across the entire switch.

Command examples

1. `(config)# authentication max-user 512`

   Limits the total number of Layer 2 authenticated users to 512.

(6) Setting the limited number of port-based authentication

Points to note

Sets the maximum number of Layer 2 authenticated users allowed on a specific port.

Command examples

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

```
(config-if)# switchport mode access
(config-if)# switchport vlan 10
(config-if)# web-authentication port
(config-if)# mac-authentication port
(config-if)# authentication max-user 64
(config-if)# exit
```

Limits the number of authenticated users at the authenticating port 1/0/5 to 64.

(7) Setting a dead interval for RADIUS server access

Points to note

Specify a dead interval for RADIUS server access. When there is no response from the RADIUS server with the highest priority, the Switch starts using the RADIUS server with the next highest priority. This procedure specifies how long the Switch waits before trying the highest-priority RADIUS server again.

Command examples

1. `(config)# authentication radius-server dead-interval 20`

   Specifies a dead interval of 20 minutes for RADIUS servers.

6 Description of the IEEE 802.1X Interface

IEEE 802.1X function authenticates Layer 2 of the OSI layer model. This chapter provides an overview of IEEE 802.1X.

6.1 Overview of IEEE 802.1X

The IEEE 802.1X authentication function 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.

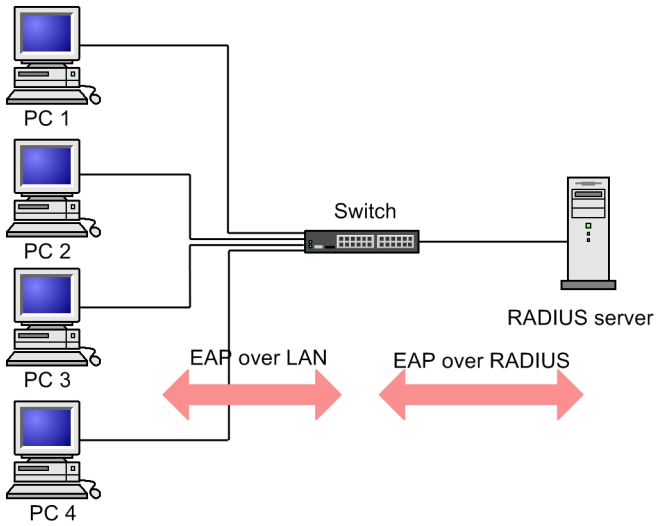
The following table describes the entities involved in IEEE 802.1X authentication, and how they interact.

Table 6-1: Entities in IEEE 802.1X and their roles

Parameters	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 function.
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.

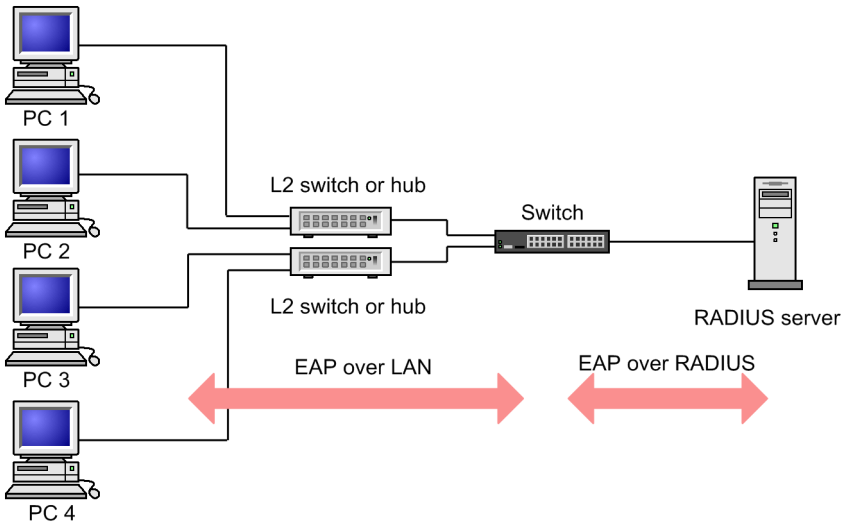
In a standard IEEE 802.1X configuration, terminals are connected directly to the ports of the Switch. The following figure describes the basic configuration of IEEE 802.1X authentication using a Switch.

Figure 6-1: IEEE 802.1X basic configuration



The Switch also supports the authentication of multiple terminals attached to a single port (via multi-mode and 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 switch placed between terminals



6.1.1 Supported function

This section lists the function supported by the Switch.

(1) PAE mode

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

The Switch supports authentication using a RADIUS server. 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.

"Table 6-2: Attributes used for authentication (Part 1: Access-Request)" to "Table 6-5: Attributes used for authentication (Part 4: Access-Reject)" list the RADIUS attribute name used by this device.

Table 6-2: Attributes used for authentication (Part 1: Access-Request)

Attribute name	Type value	Description
User-Name	1	The user name to be authenticated.
NAS-IP-Address	4	The IP address of the authenticator (the Switch) that is requesting authentication of the user. This attribute contains the local address of the Switch, or the IP address of the sending interface if no local address is set.
NAS-Port	5	The IfIndex of the interface that is authenticating the supplicant.
Service-Type	6	The type of service to be provided. Fixed as Framed(2).
Framed-MTU	12	The maximum size of a frame that may be transmitted between the supplicant and the authenticator. Fixed at (1466).
State	24	Allows state information to be maintained between the authenticator and the RADIUS server.

Attribute name	Type value	Description
Called-Station-Id	30	The MAC address of the bridge or access point. The MAC address of the Switch (as a hyphen-punctuated ASCII string).
Calling-Station-Id	31	The MAC address of the supplicant (as a hyphen-punctuated ASCII string).
NAS-Identifier	32	A string identifying the authenticator (by host name).
NAS-Port-Type	61	The type of physical port the authenticator is using to authenticate the user. Fixed as Ethernet (15).
Connect-Info	77	A string characterizing the connection with the supplicant. Port-based authentication: Physical port ("CONNECT Ethernet") CH port ("CONNECT Port-Channel ") VLAN-based authentication (static):("CONNECT VLAN") VLAN-based authentication (dynamic):("CONNECT DVLAN")
EAP-Message	79	Encapsulates EAP packets.
Message-Authenticator	80	Provides protection for RADIUS/EAP packets.
NAS-Port-Id	87	A string identifying the port of the authenticator that is authenticating the supplicant. Port-based authentication:"Port x/y", "ChGr x" VLAN-based authentication (static):"VLAN x" VLAN-based authentication (dynamic):"DVLAN x" (x and y take numerical values)
NAS-IPv6-Address	95	The IPv6 address of the authenticator that is requesting authentication of the user (in this case the Switch). This attribute contains the local address of the Switch, or the IP address (IPv6) of the sending interface if no local address is set. Note that when communication takes place using IPv6 link-local addresses, this attribute will contain the IPv6 link-local addresses of the sending interface regardless of whether local addresses are set.

Table 6-3: Attributes used in authentication (Part 2: Access-Challenge)

Attribute name	Type value	Description
Reply-Message	18	A message that may be displayed to a user.
State	24	Allows state information to be maintained between the authenticator and the RADIUS server.
Session-Timeout	27	The length of time to wait for a supplicant to respond to an EAP-Request.
EAP-Message	79	Encapsulates EAP packets.
Message-Authenticator	80	Provides protection for RADIUS/EAP packets.

Table 6-4: 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	The name of the filter list to be applied to the supplicant's session. This attribute is meaningful only in the context of VLAN-based authentication (static), or port-based authentication in terminal authentication mode. The authentication IPv4 access list, being the only applicable filter, takes effect when the Filter-Id is non-zero.
Reply-Message	18	A message that may be displayed to a user.
Session-Timeout	27	The time between supplicant re-authentication attempts.#
Termination-Action	29	Indicates what action the Switch should take following expiry of the re-authentication timer.#
Tunnel-Type	64	Indicates the tunneling protocol used. It is meaningful only in the context of VLAN-based authentication (dynamic). Fixed as VLAN (13).
Tunnel-Medium-Type	65	Indicates the protocol to use to create a tunnel. It is meaningful only in the context of VLAN-based authentication (dynamic). Fixed as IEEE 802 (6).
EAP-Message	79	Encapsulates EAP packets.
Message-Authenticator	80	Provides protection for RADIUS/EAP packets.
Tunnel-Private-Group-ID	81	A string identifying a VLAN. In an Access-Accept packet, this attribute indicates the VLAN to be assigned to the authenticated supplicant. It is meaningful only in the context of VLAN-based authentication (dynamic). The strings can be formatted as follows: (1) As a string indicating a VLAN ID (2) As a string containing the word "VLAN" followed by a VLAN ID (3) As a string indicating a VLAN name as specified by the "name" configuration command. The string cannot contain spaces. If it does, VLAN assignment will fail. Examples For VLAN10 series switches: Format (1): "10" Format (2): "VLAN10" Format (3): "business-office"
Acct-Interim-Interval	85	The number of seconds between interim packets. Interim packets will be sent if this attribute has a value of 60 or greater, but not for values less than 60. When using this attribute, we recommend that you specify a value of 600 or greater. Due to the potential for increased network traffic, caution is required when assigning values less than 600.

#

If the RADIUS server returns the value Radius-Request(1) for the Termination-Action attribute in an Access-Accept packet, the Switch performs re-authentication after the value specified for the Session-Timeout attribute (as a time in seconds) configured in the same packet has elapsed. The Switch exhibits the following behavior depending on the Session-Timeout value:

0: Re-authentication is disabled.

1 to 60: Re-authentication is triggered using a 60-second timer.

61 to 65535: Re-authentication is triggered after the specified number of seconds.

Table 6-5: Attributes used for authentication (Part 4: Access-Reject)

Attribute name	Type value	Description
Reply-Message	18	A message that may be displayed to a user.
EAP-Message	79	Encapsulates EAP packets.
Message-Authenticator	80	Provides protection for RADIUS/EAP packets.

(3) Authentication algorithm

The following table describes the supported authentication algorithms.

Table 6-6: 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. Supports the following two types of authentication methods. • PEAP-MS-CHAP V2: Authentication method with password-based credentials • PEAP-TLS: Authentication method based on a certificate authentication mechanism
EAP-TTLS	Performs authentication using an authentication algorithm of an existing protocol (such as EAP, PAP, or CHAP) encapsulated within an EAP-TLS tunnel.

(4) RADIUS accounting function

The Switch supports RADIUS accounting function. This function generates user accounting information whenever service delivery to an IEEE 802.1X-authenticated terminal starts or finishes. An administrator can use this information to track network usage. You can set up separate servers for RADIUS authentication and accounting services to distribute the RADIUS workload.

The following table describes the information that the RADIUS accounting function sends to the RADIUS server.

Table 6-7: Attributes used by RADIUS accounting

Attribute name	Type value	Description	Transmission by accounting request type		
			start	stop	Interim-Update
User-Name	1	The user name to be authenticated.	Y	Y	Y
NAS-IP-Address	4	The IP address of the authenticator (the Switch) that is requesting authentication of the user. This attribute contains the local address of the Switch, or the IP address of the sending interface if no local address is set.	Y	Y	Y

Attribute name	Type value	Description	Transmission by accounting request type		
			start	stop	Interim-Update
NAS-Port	5	The IfIndex of the interface that is authenticating the supplicant.	Y	Y	Y
Service-Type	6	The type of service to be provided. Fixed as Framed(2).	Y	Y	Y
Calling-Station-Id	31	The MAC address of the supplicant (as a hyphen-punctuated ASCII string).	Y	Y	Y
NAS-Identifier	32	A string identifying the authenticator (by host name).	Y	Y	Y
Acct-Status-Type	40	Accounting request type Start (1), Stop (2), or Interim-Update (3)	Y	Y	Y
Acct-Delay-Time	41	The delay (in seconds) between the event occurring and transmission to the server.	Y	Y	Y
Acct-Input-Octets	42	Accounting information (number of octets received). Fixed at (0).	—	Y	Y
Acct-Output-Octets	43	Accounting information (number of octets sent) Fixed at (0).	—	Y	Y
Acct-Session-Id	44	An ID for identifying the accounting information (This value is the same at authentication and authentication cancellation).	Y	Y	Y
Acct-Authentic	45	Indicates how the user was authenticated (RADIUS (1), Local (2), or Remote (3)).	Y	Y	Y
Acct-Session-Time	46	Accounting information (session length).	—	Y	Y
Acct-Input-Packets	47	Accounting information (number of received packets). Fixed at (0).	—	Y	Y
Acct-Output-Packets	48	Accounting information (number of send packets). Fixed at (0).	—	Y	Y
Acct-Terminate-Cause	49	Accounting information (reason for session termination). For details, see "Table 6-8: Termination causes returned by Acct-Terminate-Cause". User Request (1), Lost Carrier (2), Admin Reset (6), Reauthentication Failure (20), Port Reinitialized (21)	—	Y	—

Attribute name	Type value	Description	Transmission by accounting request type		
			start	stop	Interim-Update
NAS-Port-Type	61	The type of physical port the authenticator is using to authenticate the user. Fixed as Ethernet (15).	Y	Y	Y
NAS-Port-Id	87	A string identifying the port of the authenticator that is authenticating the supplicant. NAS-Port-Id differs from NAS-Port in that it is a string of variable length whereas NAS-Port is a 4-octet integer value. Port-based authentication:"Port x/y", "ChGr x" VLAN-based authentication (static):"VLAN x" VLAN-based authentication (dynamic):"DVLAN x" (x and y take numerical values)	Y	Y	Y
NAS-IPv6-Address	95	The IPv6 address of the authenticator that is requesting authentication of the user (in this case the Switch). This attribute contains the local address of the Switch, or the IP address (IPv6) of the sending interface if no local address is set. Note that when communication takes place using IPv6 link-local addresses, this attribute will contain the IPv6 link-local addresses of the sending interface regardless of whether local addresses are set.	Y	Y	Y

Legend: Y: Transmitted; —:Not transmitted.

Table 6-8: Termination causes returned by Acct-Terminate-Cause

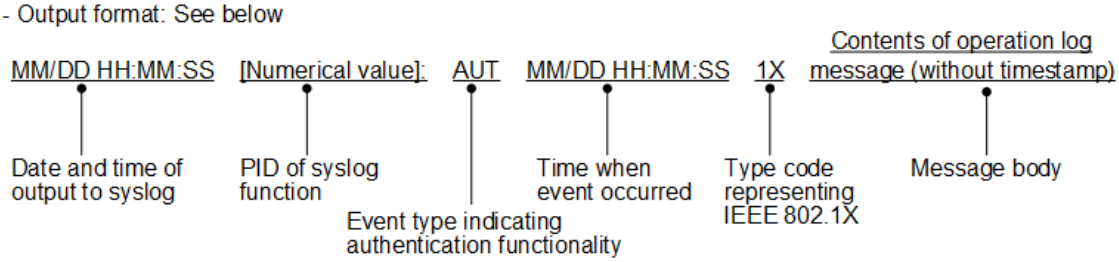
Termination cause	Code	Description
User Request	1	The session was terminated at the request of the supplicant. • A logoff request was received from the authenticated terminal
Lost Carrier	2	The modem dropped the carrier signal. • Internal error
Admin Reset	6	Action by the administrator caused the session to terminate. • The administrator deleted the interface configuration • force-authorized was configured • force-unauthorized was configured • force-authorized-port was configured
Reauthentication Failure	20	Re-authentication failed.
Port Reinitialized	21	The port's MAC address has been reinitialized. • A link went down • clear dot1x auth-state was executed

(5) Writing action logs to a syslog server

You can output the internal logs for the IEEE 802.1X function to a syslog server. In this case, the items that are output to the server are the same as those that appear in the internal log. The following figure shows the format of log output to the syslog server.

Figure 6-3: Format of output to syslog server

- Event type: AUT
- Output format: See below



You can use the "dot1x logging enable" and "logging event-kind" configuration commands to start and stop the logging of IEEE 802.1X authentication sessions.

6.2 Overview of extended function

The Switch extends the function of the standard IEEE 802.1X. An overview of the extended function is given below.

6.2.1 Authentication mode

On the Switch, IEEE 802.1X defines three basic authentication modes and a further three submodes. The basic authentication mode dictates the level at which authentication is controlled, and the submode specifies the manner in which authentication takes place. The Switch also provides options that can be configured for basic authentication modes and submodes. The following table describes the association between authentication modes and options.

Table 6-9: Relationship between authentication modes and options

Basic authentication modes	Authentication sub-modes	Authentication option
Port-based authentication	Single mode	—
	Multi-mode	—
	Terminal authentication mode	Authentication-exempted terminal option
		The option for restricting the number of terminals to be authenticated
VLAN-based authentication (static)	Terminal authentication mode	Authentication-exempted terminal option
		Authentication-exempted port option
		The option for restricting the number of terminals to be authenticated
VLAN-based authentication (dynamic)	Terminal authentication mode	Authentication-exempted terminal option
		The option for restricting the number of terminals to be authenticated
		Authentication default VLAN

Legend: —: Not applicable

IEEE 802.1X as implemented on the Switch treats a channel group as a single aggregate port. In describing this function, the term port includes normal ports and channel groups.

(1) Basic authentication modes

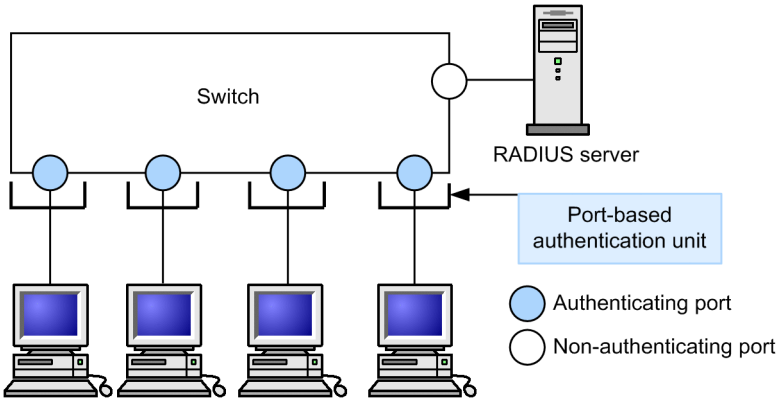
This subsection describes the basic authentication modes supported on the Switch.

(a) Port-based authentication

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. In this mode, the Switch cannot process EAPOL frames that use IEEE 802.1Q VLAN tagging and will discard any such frames it receives.

The following figure describes an example of a topology using port-based authentication:

Figure 6-4: Example configuration using port-based authentication

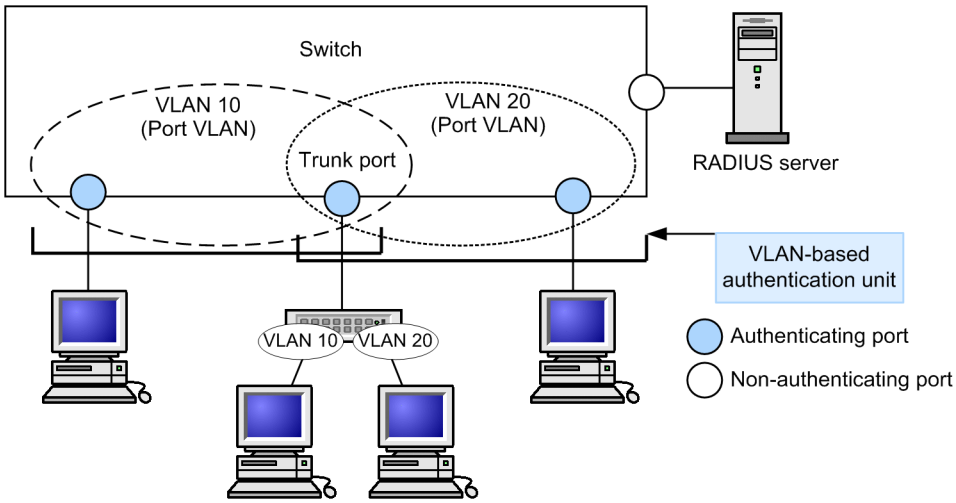


(b) VLAN-based authentication (static)

In this mode, IEEE 802.1X controls authentication at the VLAN level. The Switch can process EAPOL frames that use IEEE 802.1Q VLAN tagging. Use this mode in configurations where an L2 switch that uses IEEE 802.1Q VLAN tagging to encapsulate frames is connected between the terminal and a Switch. Untagged EAPOL frames are assumed to belong to the native VLAN of the port.

The following figure describes an example of a topology using VLAN-based authentication (static):

Figure 6-5: Example configuration using VLAN-based authentication (static)



(c) VLAN-based authentication (dynamic)

In this mode, IEEE 802.1X controls authentication at the level of terminals associated with a MAC VLAN. In this mode, the Switch cannot process EAPOL frames that use IEEE 802.1Q VLAN tagging and will process any such frames it receives in VLAN-based authentication (static) mode.

The specified trunk port or access port in the MAC VLAN is treated as an authentication-exempted port.

When a terminal is successfully authenticated, the Switch dynamically assigns a VLAN based on the VLAN information (the VLAN ID of a MAC VLAN) received from the RADIUS server.

The figures below describe an example of a configuration using VLAN-based authentication (dynamic), and illustrate its behavior.

Figure 6-6: Example configuration using VLAN-based authentication (dynamic)

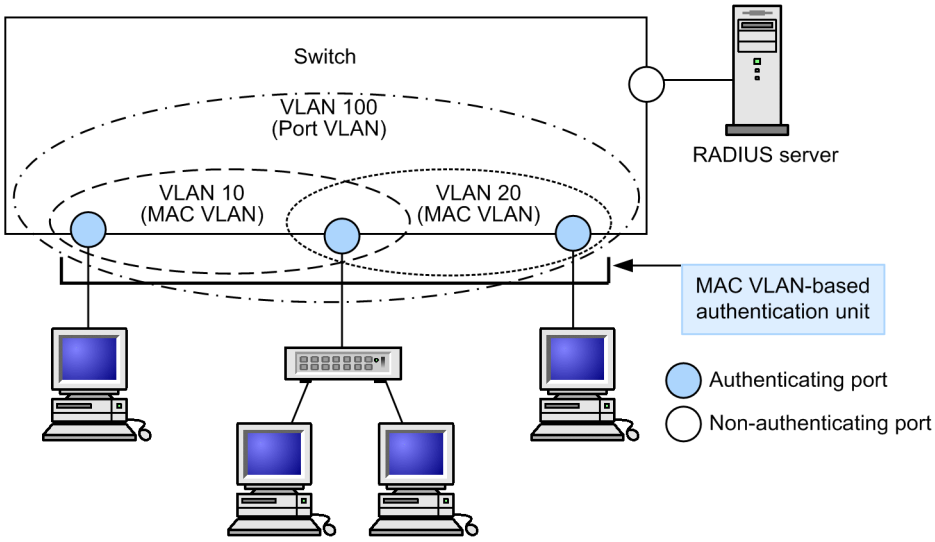
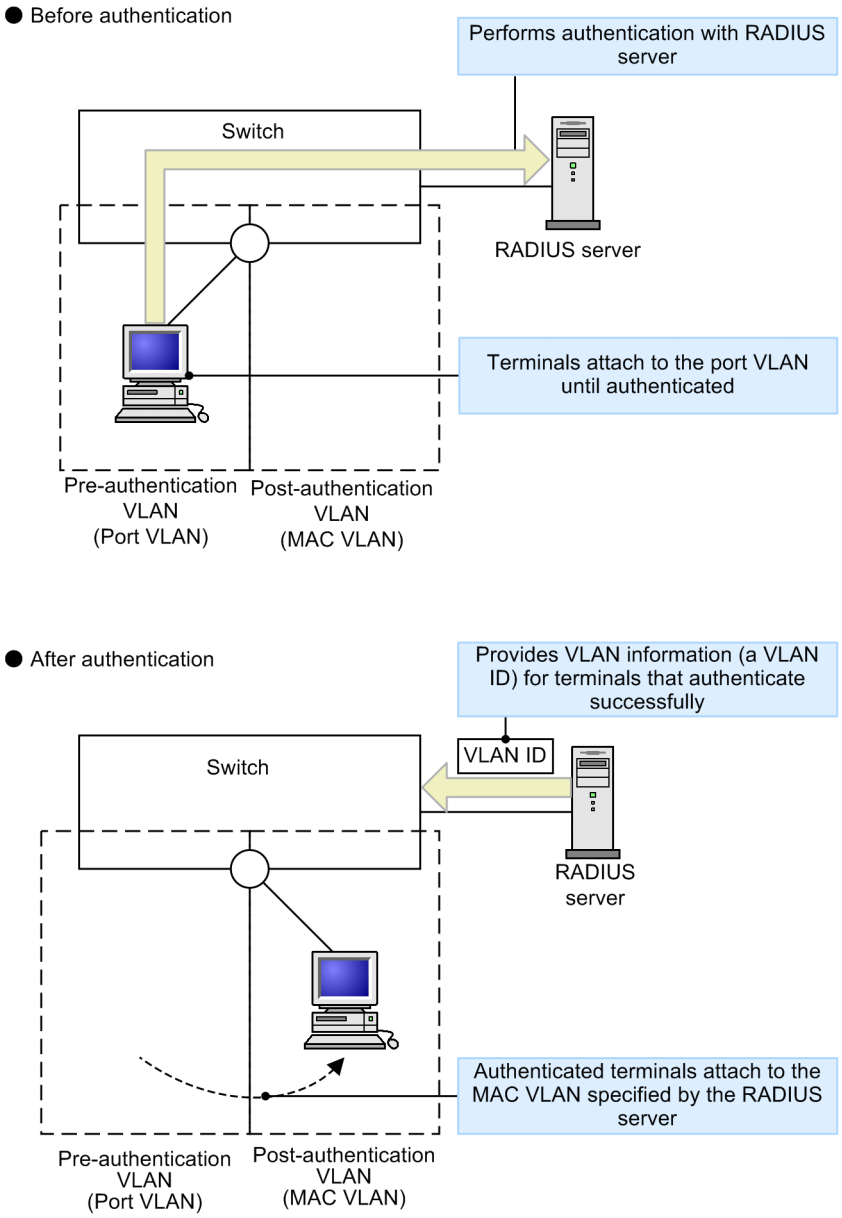


Figure 6-7: Behavior of VLAN-based authentication (dynamic) authentication



(2) Authentication submodes

The submodes that you can apply to basic authentication modes are described below.

(a) Single mode

In single-terminal mode, only one terminal can be authenticated at a given interface. This is the default mode for IEEE 802.1X. If the Switch receives an EAP packet from another terminal, the port returns to the unauthorized state. The authentication sequence then resumes after the time period specified by the configuration command elapses.

(b) Multi-mode

In multiple-terminal mode, you can attach multiple terminals to a single interface. However, only one of the attached terminals needs to be authenticated for all to be granted access. The Switch will ignore any EAP packets it receives from other terminals after the first terminal is authenticated.

(c) Terminal authentication mode

Terminal authentication mode allows you to attach multiple terminals to a single interface, but requires that each terminal (identified by source MAC address) be authenticated. In this mode, the Switch starts a new authentication sequence when it receives an EAP packet from a new terminal.

(3) Authentication mode options

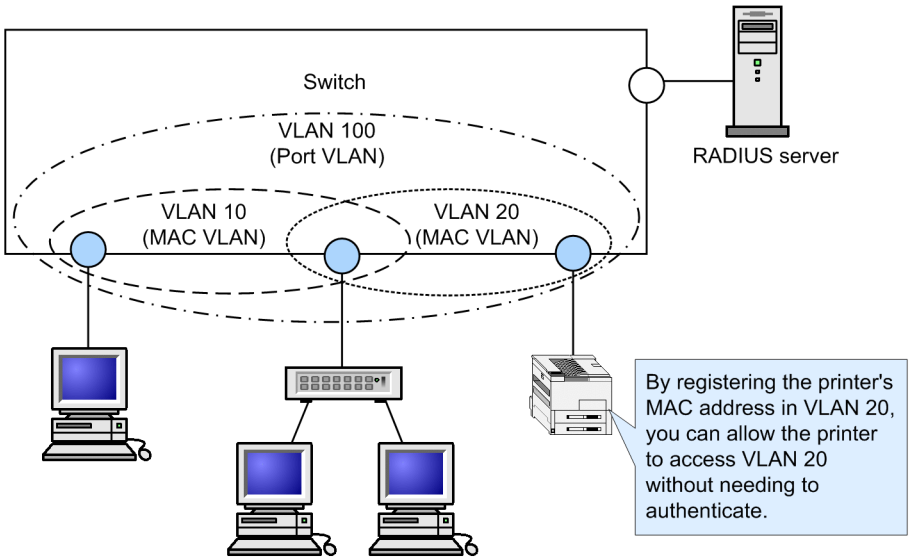
This subsection describes the options you can configure for authentication modes and submodes.

(a) Authentication-exempted terminal option

This option permits communication without authentication for the terminals whose MAC addresses have been configured by the static MAC address learning function and the MAC VLAN function. You can use this option to authorize devices such as printers that cannot operate as a supplicant function, and specific terminals such as servers that do not need to be authenticated. This option is available only in terminal authentication mode.

The figure below describes an example of a VLAN-based authentication-exempted terminal (dynamic).

Figure 6-8: VLAN-based authentication-exempted terminal (dynamic)



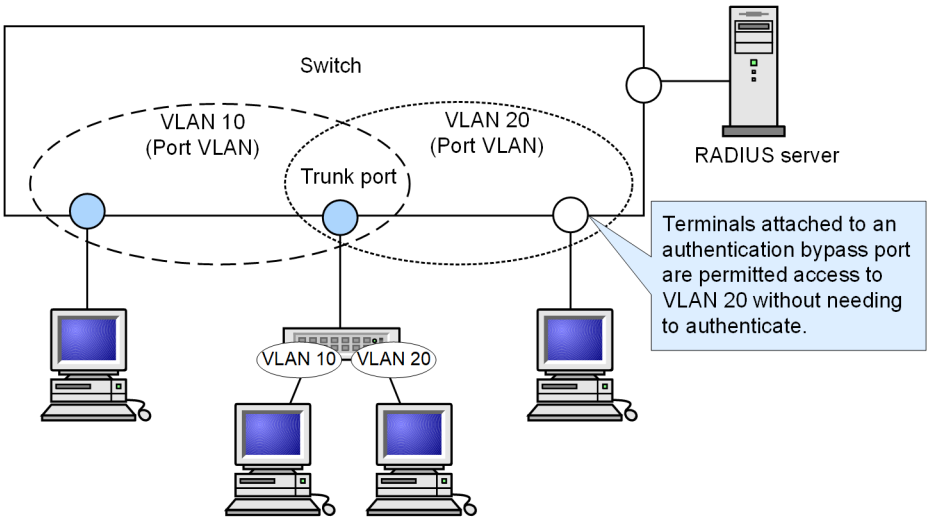
(b) Authentication-exempted port option

This option permits communication without authentication for the terminals attached to specific physical ports or channel groups. You can use this option with VLAN-based authentication (static) to designate a non-authenticating port in an authenticating VLAN.

When multiple VLANs are set up at a port configured for VLAN-based authentication (static), the specified port will act as an authentication-exempted port for all of the VLANs.

The figure below describes an example of a VLAN-based authentication-exempted port (static).

Figure 6-9: VLAN-based authentication-exempted port (static)



(c) The option for restricting the number of terminals to be authenticated

This option allows you to restrict the maximum number of terminals that can be authenticated at a given authentication unit. It applies only in terminal authentication mode. The following table describes the values you can set for each authentication mode.

Table 6-10: Option for restricting the number of terminals to be authenticated

Authentication mode	Initial value	Minimum	Maximum
Port-based authentication	64	1	64
VLAN-based authentication (static)	256	1	256
VLAN-based authentication (dynamic)	1024	1	1024

(d) Authentication default VLAN function

This function assigns a port 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 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

6.2.2 Terminal detection behavior switching option

The Switch sends EAP-Request/Identity packets to the multicast address at the interval specified by the "tx-period" command to detect unauthenticated terminals if no authenticated terminal exists. If the authentication submode is terminal authentication mode, authenticated terminals and unauthenticated terminals coexist, so terminals must be detected even if there are authenticated terminals. However, when EAP-Request/Identity packets are sent to the multicast address, authenticated terminals are also received, causing problems such as re-authentication for the authenticated terminals.

In the Switch, only in terminal authentication mode, you can select one of four methods for terminal detection behavior when an authenticated terminal exists. Understand features of each method and select an appropriate terminal detection behavior. You can specify this behavior by using the "supplicant-detection" command. If not specified, shortcut will be used.

This section describes the behaviors of each method.

(1) auto

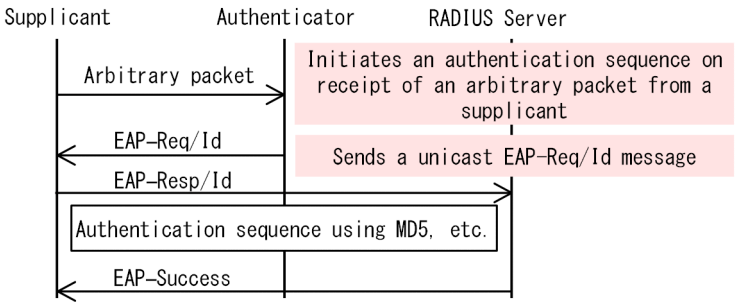
If an authenticated terminal exists, the switch does not send an EAP-Request/Identity message to the multicast address. By receiving arbitrary frames sent by unauthenticated terminals, unauthenticated terminals are detected and authentication is started.

With this method, the EAP-Request/Identity does not reach the authenticated terminals, so there is no load due to re-authentication of the authenticated terminals. We recommend that you use this method because there are no problems with detection or load.

Terminals connected to a channel group cannot be detected by arbitrary receive frames. In this case, the only trigger for terminal detection is the reception of EAPOL-Start sent by the unauthenticated terminals (same behavior as "disable"). If you cannot connect a terminal to a channel group and send EAPOL-Start to the Supplicant, specify "full" or "shortcut" for the terminal detection behavior of the Switch.

The following figure shows the EAP-Request/Identity sequence when "auto" is specified.

Figure 6-10: EAP-Request/Identity sequence when "auto" is specified



(2) disable

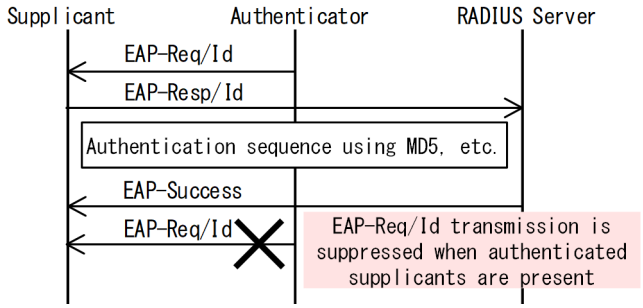
If an authenticated terminal exists, the switch does not send an EAP-Request/Identity message to the multicast address. By receiving EAPOL-Start sent by the unauthenticated terminals, the unauthenticated terminals are detected and authentication is started.

For this reason, if you use the Supplicant software that cannot send EAPOL-Start spontaneously, unauthenticated terminals cannot be detected. In such a case, either set to send EAPOL-Start to the Supplicant, or specify "auto" for the terminal detection behavior of the Switch.

With this method, the EAP-Request/Identity does not reach the authenticated terminals, so there is no load due to re-authentication of the authenticated terminals.

The following figure shows the EAP-Request/Identity sequence when "disable" is specified.

Figure 6-11: EAP-Request/Identity sequence when "disable" is specified



(3) full

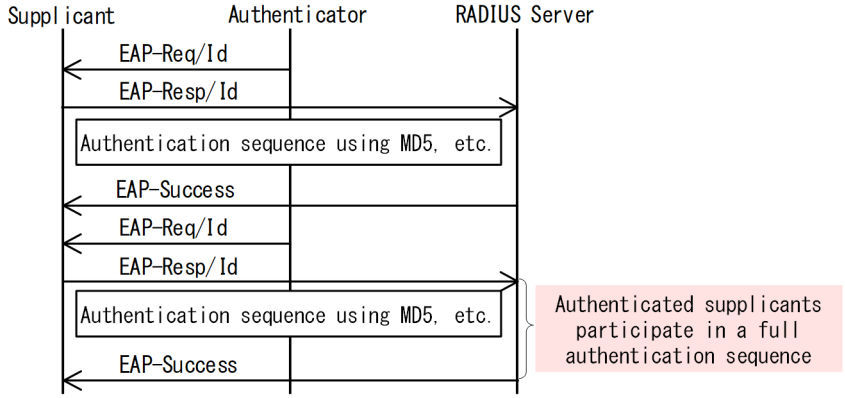
This mode sends EAP-Request/Identity packets to the multicast address even when authenticated terminals are present. Authentication starts when the unauthenticated terminals receive this frame and respond to it.

The authenticated terminals also start re-authentication by receiving this frame. With this method, when authenticated terminals start re-authentication, the authentication sequence is not skipped.

Since authenticated terminals periodically re-authenticate, a load proportional to the number of terminals is applied. To avoid the impact of load, limit the number of terminals per authentication to 20 or less.

The following figure shows the EAP-Request/Identity sequence when "full" is specified.

Figure 6-12: EAP-Request/Identity sequence when "full" is specified



(4) shortcut

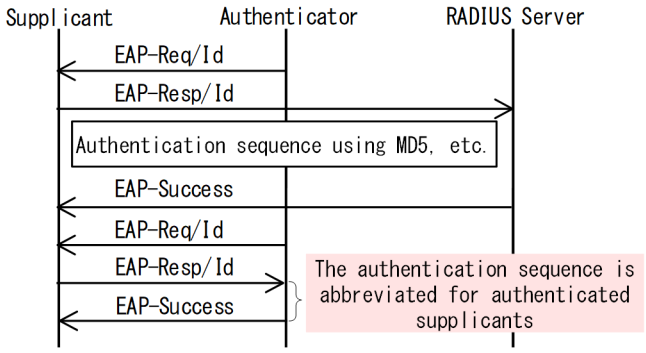
This mode sends EAP-Request/Identity packets to the multicast address even when authenticated terminals are present. Authentication starts when the unauthenticated terminals receive this frame and respond to it.

The authenticated terminals also start re-authentication by receiving this frame. With this method, when authenticated terminals start re-authentication, the load is reduced by omitting the authentication sequence and immediately sending EAP-Success.

However, some Supplicant software regards sending EAP-Success immediately as an authentication failure. As a result, communication may be interrupted immediately after authentication, communication may be interrupted several minutes to several tens of minutes after authentication, or the load may increase due to repeated re-authentication.

The following figure shows the EAP-Request/Identity sequence when "shortcut" is specified.

Figure 6-13: EAP-Request/Identity sequence when "shortcut" is specified (default)



6.2.3 Terminal re-authentication request suppression

This function prevents terminals from using EAPOL-Start messages to initiate re-authentication. This prevents a situation where a large number of requests received over a short period imposes a heavy load on the Switch. If you enable this function, the Switch performs re-authentication processing at an interval specified in the switch configuration.

6.2.4 RADIUS server connection function

(1) Connecting with a RADIUS+ server

You can specify a maximum of four RADIUS servers. Although you can specify a RADIUS server by IPv4 address, IPv6 address, or host name, in the context of IEEE 802.1X we recommend that you use an IPv4 address or IPv6 address. If you use a host name, keep the information in "5.4.2 Notes on using RADIUS server" in mind and exercise caution. If the host name resolves to multiple addresses, the switch uses the IP address with the highest priority. For more information about order of priority, see "Configuration Guide Vol. 1, 13.1 Description". You must use a non-authenticating port for the connection between the Switch and the RADIUS server.

If the connection to the RADIUS server fails, the switch will try the next RADIUS server listed in the configuration. If no RADIUS servers are accessible, the switch sends an EAP-Failure response to the terminal and terminates the authentication sequence.

If a timeout occurs at some point during the authentication sequence after connecting to the RADIUS server, the switch sends an EAP-Failure response to the terminal and terminates the authentication sequence.

(2) Settings for dynamically assigning VLANs in VLAN-based authentication (dynamic)

The Switch supports authentication in VLAN-based authentication (dynamic) mode. However, you must configure the following RADIUS server attributes before you can implement dynamic VLAN assignment on the Switch. For details about attributes, see "Table 6-4: Attributes used in authentication (Part 3: Access-Accept)".

- Tunnel-Type
- Tunnel-Medium-Type
- Tunnel-Private-Group-Id

(3) Configuration for applying filters to authenticated terminals in port-based authentication (terminal authentication mode) and VLAN-based authentication (static)

The Switch supports the filtering of terminals that undergo port-based authentication (in terminal authentication mode) and VLAN-based authentication (static). However, you must configure the following RADIUS server attribute before you can apply a filter. For details about attributes, see "Table 6-4: Attributes used in authentication (Part 3: Access-Accept)".

- Filter-Id

(4) Configuration for identifying the Switch on the RADIUS server

The RADIUS protocol stipulates that the RADIUS server must use the source IP address of the request packet to identify the RADIUS client (NAS). In the Switch, the addresses below are used as the source IP address of a request packet:

- If a local address is set, the local address is used as the source IP address
- If no local address is set, the IP address of the sending interface is used as the source IP address

If a local address is assigned to the Switch, specify the IP address configured as the local address when you register the Switch in the RADIUS server. This allows the RADIUS server to identify the IP address of the Switch from the local address even if you cannot identify the physical interface.

6.2.5 EAPOL forwarding function

You can use the EAPOL forwarding function to relay EAPOL frames when IEEE 802.1X authentication is disabled. The Switch normally does not relay EAPOL packets because their destination MAC address is a reserved address in IEEE 802.1D. However, you can use this function to relay EAPOL frames when IEEE 802.1X is disabled. Configure EAPOL forwarding when using the Switch as an L2 switch between a terminal and another authenticator.

For a configuration example of this function, see "Configuration Guide Vol. 1, 25.6 Configuration of the L2 protocol frame transparency function".

6.2.6 Limited number of authentications

You can limit the number of authenticated users at the device level and at the port level. For details, see "5.3 Function common to all Layer 2 authentication modes".

6.2.7 Moving authenticated terminals between ports

For details about how the switch behaves when you move an authenticated terminal between ports, see "5.3 Function common to all Layer 2 authentication modes".

6.2.8 VLAN-based authentication (dynamic) behavior modes

Terminals authenticated by VLAN-based authentication (dynamic) do not count against the maximum number of authenticated users. However, when a port that performs VLAN-based authentication (dynamic) authentication has any of the characteristics listed below, terminals attached to that port count against the maximum number of authenticated users, and can no longer use the authentication default VLAN. For details about authentication session limits, see "5.3.3 Limited number of authentications".

- Web authentication (dynamic VLAN mode) is configured
- MAC-based authentication is configured

- Dot1q is configured in a VLAN with a VLAN-based authentication (static) policy
- An authentication IPv4 access list is specified
- The port is configured to relay ARP packets from unauthenticated terminals
- auto is specified as the terminal detection behavior switching option (affects all ports)

6.2.9 Blocking traffic from authenticated terminals

With port-based authentication (in terminal authentication mode) or VLAN-based authentication (static), you can apply a filter that blocks the traffic generated by an authenticated terminal. For details about how to configure this function, see "6.2.4 RADIUS server connection function".

Note that the blocked terminal does not count against the maximum number of authenticated users. For details about authentication session limits, see "5.3.3 Limited number of authentications".

6.3 Notes on using IEEE 802.1X

(1) Notes on use with other functions

For details about how IEEE 802.1X interacts with other functions, see "5.2 Interoperability of Layer 2 authentication with other functions".

(2) Note when a MAC VLAN is specified as an access port

- Although you can configure port-based authentication for an interface specified as an access port in a MAC VLAN, IEEE 802.1X cannot operate in such a configuration.

(3) Note on the sending interval of interim packets

If you use interim packets with RADIUS Accounting, we recommend that you specify a value of 600 or higher as the sending interval for RADIUS packets in the Acct-Interim-Interval attribute. Because the switch sends interim packets for every authenticated terminal, exercise caution when assigning values less than 600 because this may place a heavy load on the network and the RADIUS server.

(4) Note on interoperability of VLAN-based authentication (dynamic) mode with MAC addresses registered as static entries

If you use the "mac-address-table static" command to register a static entry in the MAC address table of an interface that runs in MAC VLAN mode in a VLAN subject to VLAN-based authentication (dynamic), the associated terminal will be unable to perform authentication processing properly.

(5) Aging time settings for MAC address learning in VLAN-based authentication (dynamic) mode

When using VLAN-based authentication (dynamic), do not specify 0 (unlimited) as the aging time for MAC address entries in a port VLAN that is specified as the authentication default VLAN and the MAC VLAN for which you use VLAN-based authentication (dynamic). If you specify 0 (unlimited), 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. To clear the MAC address table of entries associated with the former VLAN, use the "clear mac-address-table" command.

(6) 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. To apply the change immediately, execute the "clear dot1x auth-state" command to clear the authentication status.

(7) Notes on placing L2 switches between terminals and the Switch

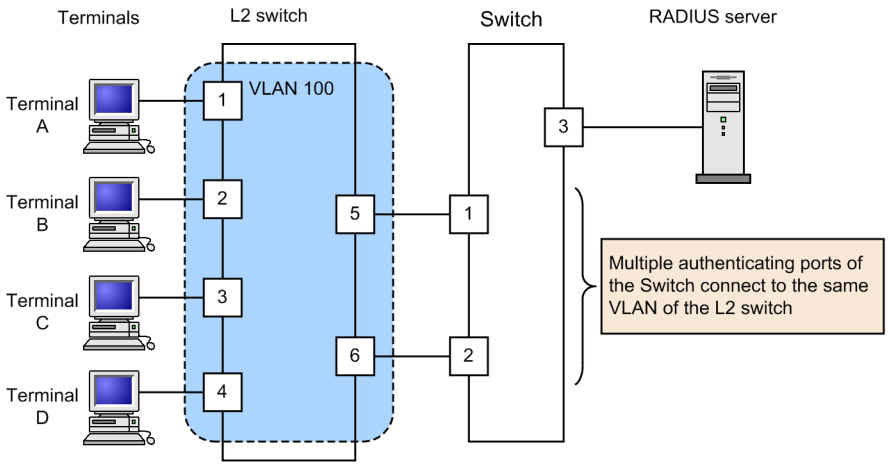
Responses from terminals are typically multicast. Therefore, if you connect an L2 switch between the terminal and the Switch, EAPOL frames that encapsulate responses from the terminal are forwarded to every port in the same VLAN on the L2 switch. If the L2 switch VLAN is configured in the manner described below, EAPOL frames from a given terminal arrive at more than one port on the Switch, creating a situation in which multiple ports are attempting to authenticate the same terminal. This affects the stability of the authentication process, and may 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.

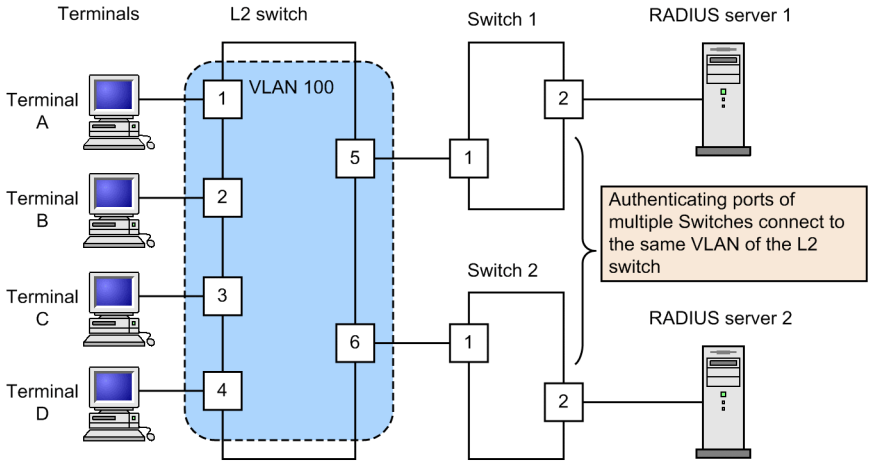
Figure 6-14: Examples of prohibited configurations

- Example in which multiple authenticating ports connect to the same VLAN of the L2 switch



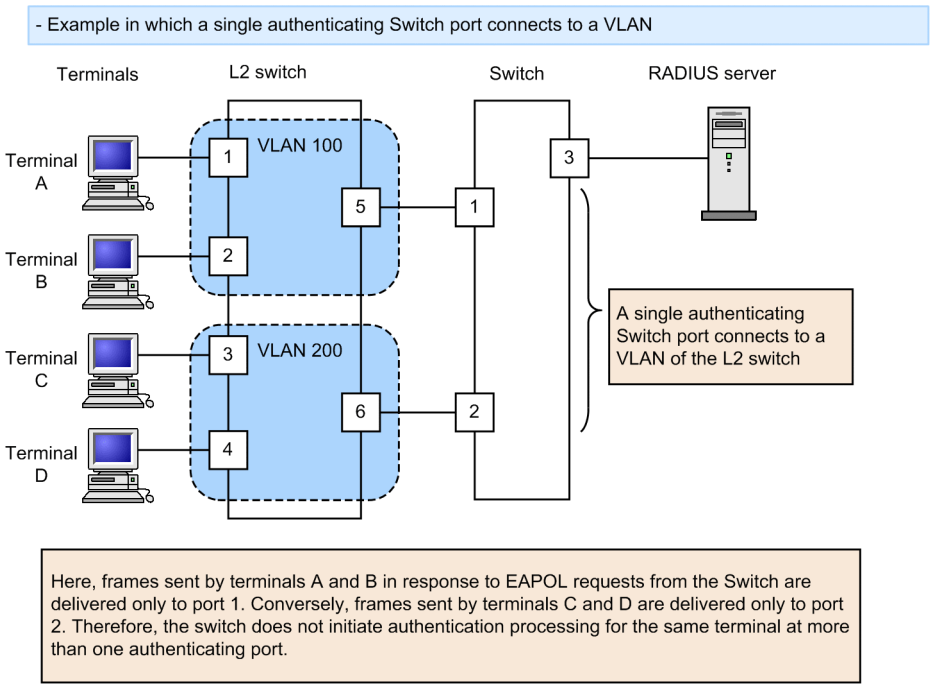
Here, frames sent by terminals A, B, C, and D in response to EAPOL requests from the Switch are forwarded to authenticating ports 1 and 2. This means that both ports begin authentication processing for the same terminal. If one of the ports discovers that the terminal is authenticated at the other, it cancels the authentication status of the terminal at the other port and begins its own authentication process. As a result, the terminal loses its ability to access the network.

- Example in which authenticating ports in more than one Switch connect to the same VLAN of the L2 switch



Here, EAPOL-Start frames from a terminal seeking authentication are delivered via multicast to Switch 1 and Switch 2. Both these switches then initiate authentication processing, which can result in a single terminal gaining authenticated status at Switch 1 and Switch 2.

Figure 6-15: Example of correct configuration



7 Settings and Operation for IEEE 802.1X

IEEE 802.1X function authenticates Layer 2 of the OSI layer model. This chapter describes IEEE 802.1X operations.

7.1 Configuration of the IEEE 802.1X interface

7.1.1 List of configuration commands

The following table describes the list of configuration commands for IEEE 802.1X.

Table 7-1: List of configuration commands

Command name	Description
aaa accounting dot1x default	Enables the collection of accounting information by the RADIUS server.
aaa authentication dot1x default	Configures the switch to use the RADIUS server for IEEE 802.1X user authentication.
aaa authorization network default	Enables VLAN-based authentication (dynamic) using VLAN information provided by the RADIUS server.
dot1x force-authorized-port	In the context of VLAN-based authentication (static), configures a port or channel group to transmit traffic without requiring authentication.
dot1x ignore-eapol-start dot1x vlan ignore-eapol-start 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.
dot1x logging enable	Enables the output of IEEE 802.1X action log information to a syslog server.
dot1x loglevel	Specifies the message level to write to the action log.
dot1x max-req dot1x vlan max-req 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.
dot1x max-supplicant dot1x vlan max-supplicant dot1x vlan dynamic max-supplicant	Specifies the maximum number of authenticated users permitted per authentication unit.
dot1x multiple-hosts dot1x multiple-authentication	Applies an authentication submode to port-based authentication.
dot1x port-control	Enables port-based authentication.
dot1x reauthentication dot1x vlan reauthentication dot1x vlan dynamic reauthentication	Enables or disables periodic re-authentication of authenticated terminals.
dot1x supplicant-detection dot1x vlan supplicant-detection dot1x vlan dynamic supplicant-detection	Configures how terminal detection is performed when terminal authentication mode is specified as the authentication submode.
dot1x system-auth-control	Enables IEEE 802.1X.

Command name	Description
dot1x timeout keep-unauth	In the context of port-based authentication in single mode, this command configures how long the port blocks traffic after receiving authentication requests from multiple terminals.
dot1x timeout quiet-period dot1x vlan timeout quiet-period 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.
dot1x timeout reauth-period dot1x vlan timeout reauth-period dot1x vlan dynamic timeout reauth-period	Specifies the interval between re-authentication attempts for authenticated terminals.
dot1x timeout server-timeout dot1x vlan timeout server-timeout dot1x vlan dynamic timeout server-timeout	Specifies how long the switch waits for a response from the authentication server.
dot1x timeout supp-timeout dot1x vlan timeout supp-timeout dot1x vlan dynamic timeout supp-timeout	Configures how long the switch waits for a supplicant to respond to an EAP-Request/Identity packet.
dot1x timeout tx-period dot1x vlan timeout tx-period dot1x vlan dynamic timeout tx-period	Specifies the sending interval for EAP-Request/Identity packets.
dot1x vlan enable	Enables VLAN-based authentication (static).
dot1x vlan dynamic enable	Enables VLAN-based authentication (dynamic).
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.

7.1.2 Configuring basic IEEE 802.1X settings

This section describes how to configure the basic IEEE 802.1X authentication modes.

(1) Enabling IEEE 802.1X

Points to note

Enable 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.

(2) Setting port-based authentication

This step designates a physical port or channel group as an authenticating port.

Points to note

Configure a port as an access port, and then enables port-based authentication for the port. You then specify the authentication submode. If you omit the authentication submode setting, the port will operate in single mode.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# switchport mode access
```
Places port 1/0/1 in access mode.
2.
```
(config-if)# dot1x multiple-authentication
```
Specifies terminal authentication mode as the authentication submode.
3.
```
(config-if)# dot1x port-control auto
```
Enables port-based authentication.

(3) Setting VLAN-based authentication (static)

This step designates a port VLAN as an authenticating VLAN.

Points to note

Set up a port VLAN, and then enable VLAN-based authentication (static) for that VLAN.

Command examples

1.
```
(config)# vlan 10
(config-vlan)# state active
(config-vlan)# exit
```
Configures VLAN ID 10 as a port VLAN.
2.
```
(config)# dot1x vlan 10 enable
```
Enables VLAN-based authentication (static) for VLAN ID 10.

(4) Setting VLAN-based authentication (dynamic)

This step designates a MAC VLAN as an authenticating VLAN.

Points to note

Configure a MAC VLAN, and then enable VLAN-based authentication (dynamic) for that VLAN.

Terminals that successfully undergo VLAN-based authentication (dynamic) obtain their VLAN membership via information sent by the RADIUS server. The "aaa authorization network default" configuration command must be configured for this process to work.

Command examples

1.
```
(config)# vlan 100 mac-based
(config-vlan)# name MACVLAN100
(config-vlan)# state active
(config-vlan)# exit
```
Configures VLAN ID 100 as a MAC VLAN.
2.
```
(config)# dot1x vlan dynamic radius-vlan 100
```
Specifies VLAN ID 100 as subject to VLAN-based authentication (dynamic).

3. `(config)# dot1x vlan dynamic enable`

   Enables VLAN-based authentication (dynamic).

7.1.3 Configuring authentication mode options

This section describes how to configure authentication mode options and parameters.

(1) Setting the authentication-exempted terminal option

This step specifies the terminals which are exempted from authentication (for example, terminals that do not support IEEE 802.1X), by their MAC addresses.

Points to note

For port-based authentication or VLAN-based authentication (static), this procedure registers a static entry in the MAC address table. For VLAN-based authentication (dynamic), registers a MAC address in a MAC VLAN.

Command examples (port-based authentication)

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# dot1x multiple-authentication
(config-if)# dot1x port-control auto
(config-if)# exit
```

   Assigns port 1/0/1 to VLAN ID 10, and then configures port-based authentication at the port that specifies terminal authentication mode as the authentication submode.

2. `(config)# mac-address-table static 0012.e200.0001 vlan 10 interface gigabitethernet 1/0/1`

   Adds a static entry for the MAC address (0012.e200.0001) for which you want to permit unauthenticated access to VLAN ID 10 from port 1/0/1.

Command examples (VLAN-based authentication (dynamic))

1.
```
(config)# vlan 100 mac-based
(config-vlan)# mac-address 0012.e200.0001
(config-vlan)# exit
```

   Specifies the MAC address of a terminal to be permitted access to the MAC VLAN assigned VLAN ID 100. The terminal will be able to access VLAN ID 100 without first undergoing IEEE 802.1X authentication.

2.
```
(config)# dot1x vlan dynamic radius-vlan 100
(config)# dot1x vlan dynamic enable
```

   Enables VLAN-based authentication (dynamic) for VLAN ID 100.

(2) Setting the authentication-exempted port option

Points to note

In a VLAN configured for VLAN-based authentication (static), configure a port to permit network access by unauthenticated devices. If the port belongs to multiple VLANs, devices attached to the port can access all those VLANs.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# dot1x force-authorized-port
```

Configures port 1/0/1 to allow access by unauthenticated devices. Here, port 1/0/1 is a member of a VLAN configured for VLAN-based authentication (static).

Notes

If you add a VLAN configured for VLAN-based authentication (static) to an authentication-exempted port, the port's network connection might be temporarily lost.

(3) Limiting the number of authenticated users

Points to note

Limit the maximum number of authenticated users per authentication unit. For port-based authentication, this setting takes effect when terminal authentication mode is the authentication submode.

Command examples (port-based authentication)

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# dot1x multiple-authentication
(config-if)# dot1x port-control auto
(config-if)# dot1x max-supplicant 50
```

Specifies 50 as the maximum number of authenticated users permitted at port 1/0/1.

Command examples (VLAN-based authentication (static))

1.
```
(config)# dot1x vlan 10 max-supplicant 50
```

Specifies 50 as the maximum number of authenticated users permitted at VLAN ID 10 (configured for VLAN-based authentication (static)).

Command examples (VLAN-based authentication (dynamic))

1.
```
(config)# dot1x vlan dynamic max-supplicant 50
```

Specifies 50 as the maximum number of authenticated users permitted by VLAN-based authentication (dynamic).

(4) 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 action 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 in an environment where authenticated terminals are present. full mode is intended for environments where supplicants that cannot cope with an abbreviated authentication sequence attempt authentication. Note that full mode places a higher burden on the switch and must be used with caution. In auto mode, the switch does not send an EAP-Request/Identity message to the multicast address. Instead, the switch sends EAP-Request/Identity messages only to terminals from which it receives an arbitrary packet.

Command examples (port-based authentication)

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# dot1x multiple-authentication
(config-if)# dot1x port-control auto
(config-if)# dot1x supplicant-detection disable
```

Configures the switch to stop transmitting EAP-Request/Identity messages when an authenticated terminal is present at port 1/0/1.

Command examples (VLAN-based authentication (static))

1. `(config)# dot1x vlan 10 supplicant-detection shortcut`

   Configures the switch to skip re-authentication and consider authentication successful when the switch receives EAP-Response/Identity messages from authenticated terminals in VLAN ID 10 which is configured for VLAN-based authentication (static).

Command examples (VLAN-based authentication (dynamic))

1. `(config)# dot1x vlan dynamic supplicant-detection full`

   Configures the switch to perform the authentication sequence and send requests to the authentication server when the switch receives EAP-Response/Identity messages from terminals authenticated by VLAN-based authentication (dynamic).

7.1.4 Configuring settings related to authentication processing

(1) Configuring the function for requesting terminal re-authentication

If you remove a terminal from the network without sending a logoff message to the Switch, the Switch will not have a chance to clear the authentication status of the terminal. This configuration solves the problem by clearing the authentication status of authenticated terminals that do not respond to re-authentication requests.

Points to note

Configure 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 (port-based authentication)

1. ```
   (config)# interface gigabitethernet 1/0/1
   (config-if)# dot1x reauthentication
   (config-if)# dot1x timeout reauth-period 360
   ```

   Enables the re-authentication request function at port 1/0/1, and then sets the re-authentication interval to 360 seconds.

Command examples (VLAN-based authentication (static))

1. ```
   (config)# dot1x vlan 10 reauthentication
   (config)# dot1x vlan 10 timeout reauth-period 360
   ```

   Enables the re-authentication function at VLAN ID 10 (configured for VLAN-based authentication (static)), and then sets the re-authentication interval to 360 seconds.

Command examples (VLAN-based authentication (dynamic))

1. ```
   (config)# dot1x vlan dynamic reauthentication
   (config)# dot1x vlan dynamic timeout reauth-period 360
   ```

   Enables the re-authentication function for terminals subject to VLAN-based authentication (dynamic), and then sets the re-authentication interval to 360 seconds.

(2) Configuring the retransmission of EAP-Request frames to terminals

This step 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 (port-based authentication)

1. `(config)# interface gigabitethernet 1/0/1`

   `(config-if)# dot1x timeout supp-timeout 60`

   Specifies a retransmission period of 60 seconds for EAP-Request frames at port 1/0/1.

2. `(config-if)# dot1x max-req 3`

   Specifies that EAP-Request frames be retransmitted a maximum of three times at port 1/0/1.

Command examples (VLAN-based authentication (static))

1. `(config)# dot1x vlan 10 timeout supp-timeout 60`

   Specifies a retransmission period for EAP-Request frames of 60 seconds at VLAN ID 10 (configured for VLAN-based authentication (static)).

2. `(config)# dot1x vlan 10 max-req 3`

   Specifies that EAP-Request frames are retransmitted a maximum of three times for members of VLAN ID 10 (configured for VLAN-based authentication (static)).

Command examples (VLAN-based authentication (dynamic))

1. `(config)# dot1x vlan dynamic timeout supp-timeout 60`

   Specifies a retransmission period for EAP-Request frames of 60 seconds for terminals subject to VLAN-based authentication (dynamic).

2. `(config)# dot1x vlan dynamic max-req 3`

   Specifies that EAP-Request frames are retransmitted a maximum of three times to terminals subject to VLAN-based authentication (dynamic).

(3) Configuring the function for suppressing authentication requests from terminals

This step prevents terminals from using EAP-Start frames to initiate an authentication sequence. With this function 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 function 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 (port-based authentication)

1. `(config)# interface gigabitethernet 1/0/1`

   `(config-if)# dot1x reauthentication`

   `(config-if)# dot1x ignore-eapol-start`

   Prevents authentication processing from being initiated in response to EAP-Start frames received at port 1/0/1.

Command examples (VLAN-based authentication (static))

1. `(config)# dot1x vlan 10 reauthentication`

   `(config)# dot1x vlan 10 ignore-eapol-start`

   Prevents authentication processing from being initiated in response to EAP-Start frames received from VLAN ID 10 (configured for VLAN-based authentication (static)).

Command examples (VLAN-based authentication (dynamic))

1. `(config)# dot1x vlan dynamic reauthentication`

   `(config)# dot1x vlan dynamic ignore-eapol-start`

   Prevents authentication processing from being initiated in response to EAP-Start frames received from terminals subject to VLAN-based authentication (dynamic).

(4) Configuring the idle period for terminals that fail authentication

This step 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 ID or password.

Command examples (port-based authentication)

1. `(config)# interface gigabitethernet 1/0/1`

   `(config-if)# dot1x timeout quiet-period 300`

   Specifies an idle period of 300 seconds before terminals attached to port 1/0/1 configured for port-based authentication can retry the authentication process.

Command examples (VLAN-based authentication (static))

1. `(config)# dot1x vlan 10 timeout quiet-period 300`

   Specifies an idle period of 300 seconds before terminals associated with VLAN ID 10 (configured for VLAN-based authentication (static)) can retry the authentication process.

Command examples (VLAN-based authentication (dynamic))

1. `(config)# dot1x vlan dynamic timeout quiet-period 300`

   Specifies an idle period of 300 seconds before terminals subject to VLAN-based authentication (dynamic) VLAN can retry the authentication process.

(5) Configuring the sending interval for EAP-Request/Identity frames

This configuration specifies the interval at which the Switch transmits EAP-Request/Identity packets to provide terminals that do not issue EAP-Start packets with an opportunity to initiate an authentication sequence.

Points to note

This function 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 authenticated by the Switch / 20) x 2

The default value of tx-period is 30 seconds. Therefore, in an environment where the switch authenticates more than 300 terminals, you will need to change the value of the tx-period timer.

Command examples (port-based authentication)

1. `(config)# interface gigabitethernet 1/0/1`

   `(config-if)# dot1x timeout tx-period 300`

   Specifies a 300 second interval for the transmission of EAP-Request/Identity frames to port 1/0/1 configured for port-based authentication.

Command examples (VLAN-based authentication (static))

1. `(config)# dot1x vlan 10 timeout tx-period 300`

Specifies a 300 second interval for the transmission of EAP-Request/Identity frames to VLAN ID 10 (configured for VLAN-based authentication (static)).

Command examples (VLAN-based authentication (dynamic))

1. `(config)# dot1x vlan dynamic timeout tx-period 300`

   Specifies a sending interval of 300 seconds for EAP-Request/Identity frames in VLAN-based authentication (dynamic).

(6) Setting a timeout period for responses from the authentication server

This step 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 following times: the time specified in the commands below, or the total time including retransmissions specified by the attributes of the "radius-server" command.

Points to note

When multiple RADIUS servers are configured in the "radius-server" 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 is able to send requests to all the authentication servers. If you want the notification to wait until the switch has failed to get a response from all of the authentication servers, make sure that these commands specify a longer value.

Command examples (port-based authentication)

1. ```
   (config)# interface gigabitethernet 1/0/1
   (config-if)# dot1x timeout server-timeout 300
   ```

   Specifies a 300-second timeout period for responses from the authentication server at port 1/0/1 configured for port-based authentication.

Command examples (VLAN-based authentication (static))

1. `(config)# dot1x vlan 10 timeout server-timeout 300`

   Specifies a 300-second timeout period for responses from the authentication server in VLAN ID 10 configured for VLAN-based authentication (static).

Command examples (VLAN-based authentication (dynamic))

1. `(config)# dot1x vlan dynamic timeout server-timeout 300`

   Specifies a 300-second timeout period for responses from the authentication server at terminals subject to VLAN-based authentication (dynamic).

(7) Configuring traffic blocking in response to authentication requests from multiple terminals

This step specifies how long to block traffic at a port configured for port-based authentication in single mode in the event that the port receives authentication requests from multiple terminals.

Points to note

Specify the length of time required to remove the surplus terminal from the port.

Command examples

1. ```
   (config)# interface gigabitethernet 1/0/1
   (config-if)# dot1x timeout keep-unauth 1800
   ```

   Specifies that port 1/0/1 configured for port-based authentication blocks traffic for 1800 seconds.

(8) Configuring output to the syslog server

This step configures the output of action logs on the syslog server.

Points to note

Configure the output of action logs that record information about IEEE 802.1X authentication and action to the syslog server.

Command examples

1. `(config)# dot1x logging enable`
   `(config)# logging event-kind aut`

   Configure output of action logs to the syslog server.

7.1.5 Configuring settings related to RADIUS servers

(1) Configuring accounting

Points to note

Set up the collection of RADIUS accounting information at a specified server.

Command examples

1. `(config)# aaa accounting dot1x default start-stop group radius`

   Specifies that accounting information be collected by the RADIUS server.

(2) Configuring RADIUS server authentication

Points to note

Enable user authentication via the RADIUS server.

Command examples

1. `(config)# aaa authentication dot1x default group radius`

   Specifies that user authentication takes place using a RADIUS server.

(3) Configuration when using VLAN-based authentication (dynamic)

Points to note

Authorize the switch to assign VLAN membership based on information received from the RADIUS server when using VLAN-based authentication (dynamic).

Command examples

1. `(config)# aaa authorization network default group radius`

   Directs the switch to associate clients with the VLAN specified by the RADIUS server.

7.2 IEEE 802.1X operation

7.2.1 List of operation commands

The following table describes the list of operation commands you can use to check the status of IEEE 802.1X.

Table 7-2: List of operation commands

Command name	Description
show dot1x	Shows the status of each authentication unit and information about authenticated supplicants.
show dot1x logging	Shows the action log messages output by the IEEE 802.1X software.
show dot1x statistics	Shows statistics about IEEE 802.1X authentication.
clear dot1x auth-state	Clears information related to authenticated terminals.
clear dot1x logging	Clears the action log messages output by the IEEE 802.1X software.
clear dot1x statistics	Resets IEEE 802.1X-related statistics to 0.
reauthenticate dot1x	Re-authenticates the status of IEEE 802.1X authentication.
restart dot1x	Restarts the IEEE 802.1X program.
dump protocols dot1x	Outputs the control table information and statistics gathered by the IEEE 802.1X software to a file.

7.2.2 Displaying the status of IEEE 802.1X

(1) Displaying authentication statuses

Use the "show dot1x" command to display the status of IEEE 802.1X authentication.

(a) Displaying general status information

Execute the "show dot1x" command to display the status of IEEE 802.1X authentication on the Switch.

Figure 7-1: Output of show dot1x command

```
> show dot1x
Date 20XX/10/20 10:52:40 UTC
System 802.1X : Enable

Port/ChGr/VLAN    AccessControl    PortControl         Status       Supplicants
Port  0/1         ---              Auto                Authorized   1
Port  0/2         Multiple-Hosts   Auto                Unauthorized 0
Port  0/3         Multiple-Auth    Auto                ---          0
ChGr  32          Multiple-Auth    Auto                ---          1
VLAN 10           Multiple-Auth    Auto                ---          1
VLAN 11           Multiple-Auth    Auto                ---          0
VLAN 12           Multiple-Auth    Auto                ---          0
VLAN(Dynamic)     Multiple-Auth    Auto                ---          1
```

(b) Displaying the status of port-based authentication

To display the individual status of ports subject to port-based authentication, use the "show dot1x port" command. To view the status of a channel group, use the "show dot1x channel-group-number" command.

If you specify a port number, the command outputs status information for the specified port.

Specify the detail parameter to include information about terminals authenticated in the VLAN.

Figure 7-2: Results of executing the show dot1x port command (with detail parameter specified)

```
> show dot1x port 0/1 detail
Date 20XX/10/20 10:52:48 UTC
Port  0/1
AccessControl  :  ---                  PortControl    :  Auto
Status         :  Authorized           Last EAPOL     :  0012.e200.0021
Supplicants    :  1 / 1                ReAuthMode     :  Enable
TxTimer(s)     :  9     / 30           ReAuthTimer(s) :  3585  / 3600
ReAuthSuccess  :  0                    ReAuthFail     :  0
KeepUnauth(s)  :  ---   / 3600

 Supplicants MAC     Status         AuthState     BackEndState  ReAuthSuccess
                     SessionTime(s) Date/Time
 0012.e200.0021      Authorized     Authenticated Idle          0
                     15             20XX/10/20 10:52:32
```

(c) Displaying the status of VLAN-based authentication (static)

Use the "show dot1x vlan" command to display the individual status of VLANs subject to VLAN-based authentication (static). If you specify a VLAN ID, the command outputs status information for the specified VLAN. Specify the detail parameter to include information about terminals authenticated in the VLAN.

Figure 7-3: Results of executing the show dot1x vlan command (with detail parameter specified)

```
> show dot1x vlan 20 detail
Date 20XX/10/20 10:52:48 UTC
VLAN 20
AccessControl  : Multiple-Auth             PortControl   : Auto
Status         : ---                       Last EAPOL    : 0012.e200.0003
Supplicants    : 2 / 2 / 256               ReAuthMode    : Enable
TxTimer(s)     : 3518  / 3600              ReAuthTimer(s): 3548  / 3600
ReAuthSuccess  : 0                         ReAuthFail    : 0
SuppDetection  : Shortcut
Port(s): 0/1-10, ChGr  1-5
Force-Authorized Port(s): 0/4,8-10, ChGr  1-5

 Supplicants MAC     Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 [Port 0/1]
 0012.e200.0003      Authorized     Authenticated  Idle           0
                     84             20XX/10/20 10:51:24
 [Port 0/3]
 0012.e200.0004      Authorized     Authenticated  Idle           0
                     5              20XX/10/20 10:51:03
```

(d) Displaying the status of VLAN-based authentication (dynamic)

Use the "show dot1x vlan dynamic" command to display the individual status of VLANs subject to 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 information about terminals authenticated in the VLAN.

Figure 7-4: Results of executing the show dot1x vlan dynamic command (with detail parameter specified)

```
> show dot1x vlan dynamic detail
Date 20XX/10/20 10:52:48 UTC
VLAN(Dynamic)
AccessControl  : Multiple-Auth             PortControl   : Auto
Status         : ---                       Last EAPOL    : 0012.e200.0005
Supplicants    : 1 / 1 / 256               ReAuthMode    : Disable
TxTimer(s)     : 3556  / 3600              ReAuthTimer(s): 3586  / 3600
ReAuthSuccess  : 0                         ReAuthFail    : 0
SuppDetection  : Shortcut
VLAN(s): 20

 Supplicants MAC     Status         AuthState      BackEndState   ReAuthSuccess
```

```
                    SessionTime(s) Date/Time
[VLAN 20]           VLAN(Dynamic) Supplicants : 1
0012.e200.0005      Authorized     Authenticated  Idle           0
                    44             20XX/10/20 10:52:03
```

7.2.3 Changing IEEE 802.1X authentication statuses

(1) Initializing authentication statuses

To initialize the authentication status of connected devices, use the "clear dot1x auth-state" command. 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 7-5: Example of initializing all IEEE 802.1X authentication information in the device

```
> clear dot1x auth-state
Initialize all 802.1X Authentication Information. Are you sure? (y/n) :y
```

(2) Forcing re-authentication

To force re-authentication for connected devices, use the "reauthenticate dot1x" command. 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 7-6: Example of forcing re-authentication for all IEEE 802.1X-authenticated ports and VLANs in the device

```
> reauthenticate dot1x
Reauthenticate all 802.1X ports and vlans. Are you sure? (y/n) :y
```

8 Description of Web Authentication

This chapter explains the Web authentication feature, which controls VLAN access at the user level based on credentials supplied from an ordinary Web browser.

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 Switch grants successfully authenticated terminals access to the post-authentication network on the basis of their MAC addresses.

Web authentication allows users to perform authentication using only their Web browser, without the need to install any special software on the terminal.

(1) Authentication mode

The Switch supports the following authentication modes:

- Fixed VLAN mode

  In this mode, successfully authenticated terminals have their MAC addresses entered in the MAC address table and are permitted access to the VLAN. To allow terminals to log in to an authentication network, you can use the URL redirection function offered in the Switch or specify the Web authentication IP address.

- Dynamic VLAN mode

  Successfully authenticated terminals have their MAC addresses entered in a MAC address table and registered in a MAC VLAN. Terminals are given access to different VLANs before and after authentication. To allow terminals to log in to an authentication network, you can use the URL redirection function offered in the Switch or specify the Web authentication IP address.

- Legacy mode

  Successfully authenticated terminals have their MAC addresses registered in a MAC VLAN. Terminals are given access to different VLANs before and after authentication. Unlike dynamic VLAN mode, terminals log in using the IP address of the pre-authentication VLAN interface.

In the description of dynamic VLAN mode and legacy mode, the VLAN to which an unauthenticated terminal belongs is called Pre-authentication VLAN. The VLAN after authentication is called Post-authentication VLAN.

(2) Authentication method

Users of the Switch can choose to perform local authentication or RADIUS authentication method. Fixed VLAN mode, dynamic VLAN mode, and legacy mode each support both variations.

- Local authentication method

  The Switch stores user information locally in what is known as an Internal Web authentication DB. Authentication is successful when a user supplies credentials that match those in the database. This method is suited to small-scale networks that lack a RADIUS server.

- RADIUS authentication method

  Authentication is performed by using a RADIUS server deployed on the network. This method is suited to larger networks.

(3) Authentication networks

In the Switch, Web authentication controls authentication on the IPv4 network. For this reason, terminals seeking authentication must attach to a VLAN interface that has an IPv4 address. Note that you can use an IPv4 or IPv6 address to specify a RADIUS server.

8.2 System configuration examples

This section illustrates sample configurations of networks that use local and RADIUS authentication method in fixed VLAN mode, dynamic VLAN mode, and legacy mode.

Also shown are network configurations that illustrate the different methods of assigning IP addresses to terminals.

8.2.1 Fixed VLAN mode

In fixed VLAN mode, prior to authentication, a terminal does not appear in the MAC address table and is unable to access the VLAN associated with the interface to which it is attached. If authentication succeeds, the switch adds the terminal's MAC address to the MAC address table, thus permitting access to the VLAN.

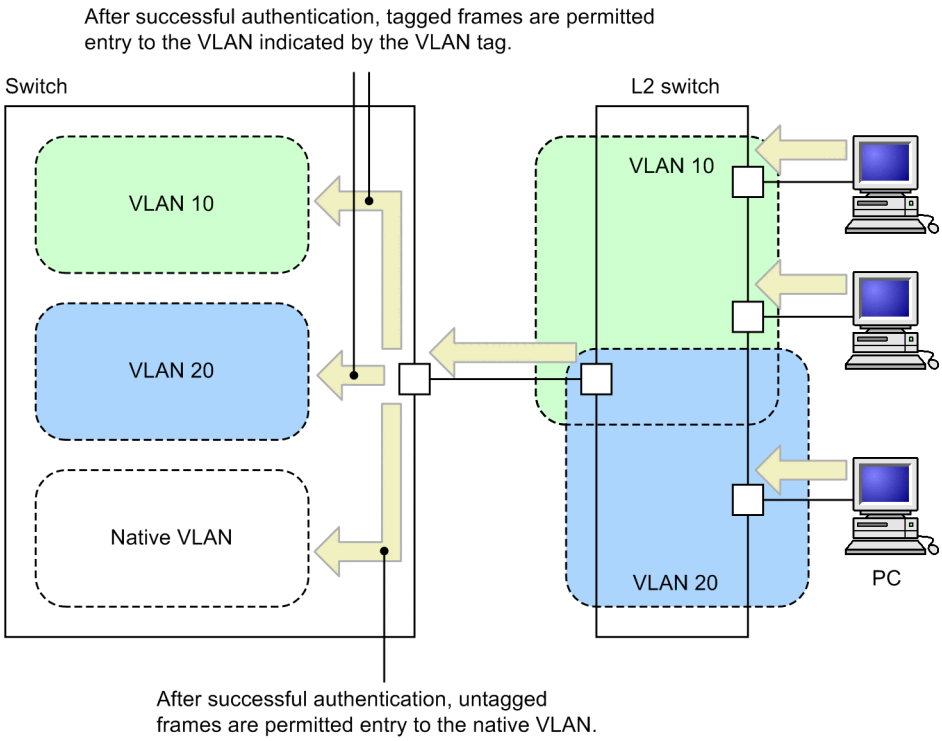
In the Switch, you can configure authentication at the following ports:

- Access port
- Trunk port

Tagged and untagged frames that enter a trunk port are handled as follows:

- Tagged frames are forwarded to the VLAN indicated by the VLAN tag after successful authentication
- Untagged frames are forwarded to the native VLAN after successful authentication

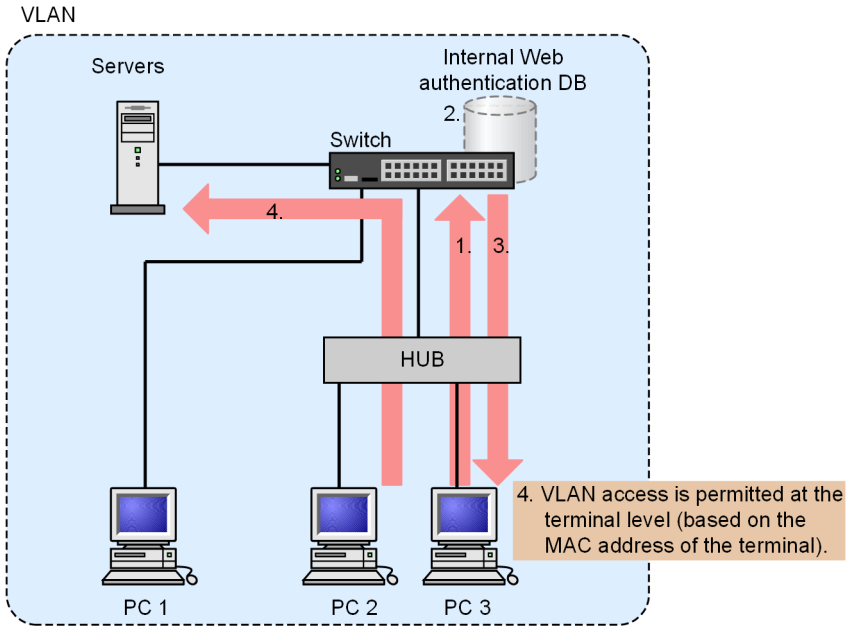
Figure 8-1: Frame handling at a trunk port



(1) Local authentication method

The figure below describes local authentication method using an internal Web authentication DB.

Figure 8-2: Local authentication method in fixed VLAN mode

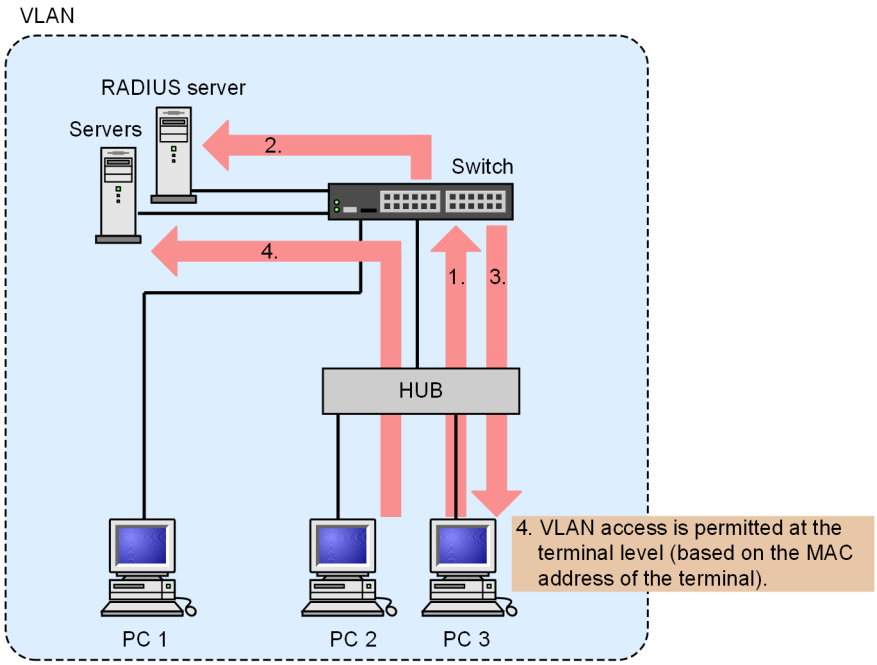


1. A user of a PC connected via a hub opens a Web browser and accesses the Switch.
2. The Switch compares the user ID and password entered by the user against the user information in the internal Web authentication DB.
3. If authentication succeeds, a page appears on the PC indicating that authentication was successful.
4. The authenticated PC is able to access servers in the VLAN associated with the port.

(2) RADIUS authentication method

The figure below describes RADIUS authentication method using a RADIUS server.

Figure 8-3: RADIUS authentication method in fixed VLAN mode



1. A user of a PC connected via a hub opens a Web browser and accesses the Switch.
2. Authentication takes place by comparing the user ID and password entered by the user against the user information registered on the RADIUS server.
3. If authentication succeeds, a page appears on the PC indicating that authentication was successful.
4. The authenticated PC is able to access servers in the VLAN associated with the port.

8.2.2 Dynamic VLAN mode

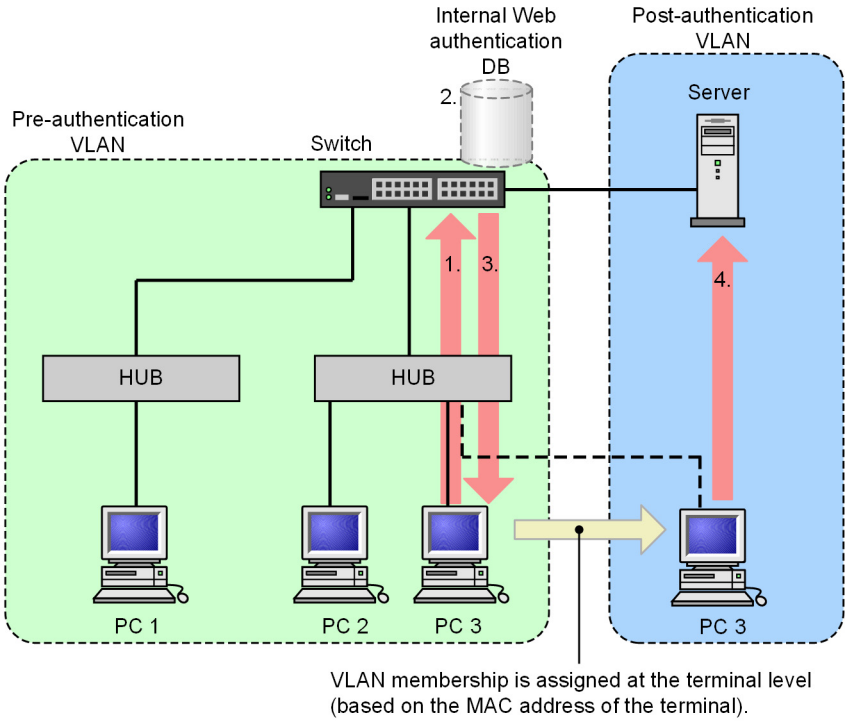
When a terminal with membership to the pre-authentication VLAN undergoes successful authentication in dynamic VLAN mode, the switch registers the terminal in a MAC VLAN and enters it in a MAC address table based on the VLAN ID provided by the internal Web authentication DB or the RADIUS server. As a result, the terminal gains access to the post-authentication VLAN. For this to work, the following configuration is required:

- The ports in the MAC VLAN must be configured as authentication ports
- An access list must be configured that prohibits unnecessary communication between the pre-authentication and post-authentication VLANs

(1) Local authentication method

The figure below describes local authentication method using an internal Web authentication DB.

Figure 8-4: Configuring Local Authentication Method for Dynamic VLAN Mode

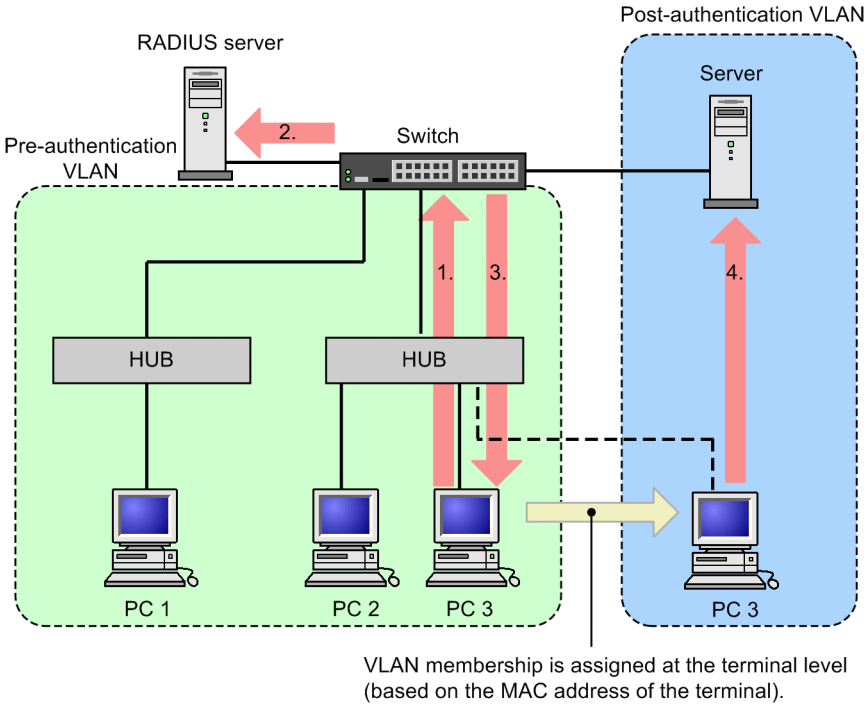


1. A user of a PC connected via a hub opens a Web browser and accesses the Switch.
2. The Switch compares the user ID and password entered by the user against the user information in the internal Web authentication DB.
3. If authentication succeeds, a page appears on the PC indicating that authentication was successful, and the PC gains membership to the post-authentication VLAN.
4. The authenticated PC is able to access servers in the post-authentication VLAN.

(2) RADIUS authentication method

The figure below describes RADIUS authentication method using a RADIUS server.

Figure 8-5: RADIUS authentication method in dynamic VLAN mode



1. A user of a PC connected via a hub opens a Web browser and accesses the Switch.
2. Authentication takes place by comparing the user ID and password entered by the user against the user information registered on the RADIUS server.
3. If authentication succeeds, a page appears on the PC indicating that authentication was successful, and the PC gains membership to the post-authentication VLAN.
4. The authenticated PC is able to access servers in the post-authentication VLAN.

8.2.3 Legacy mode

This mode is a running mode provided under the name of dynamic VLAN mode in versions prior to Ver.10.7 of the AX6000S series, AX3630S, and AX2430S. Use this when applying the Switch to a network configured using the Web authentication function prior to Ver.10.7.

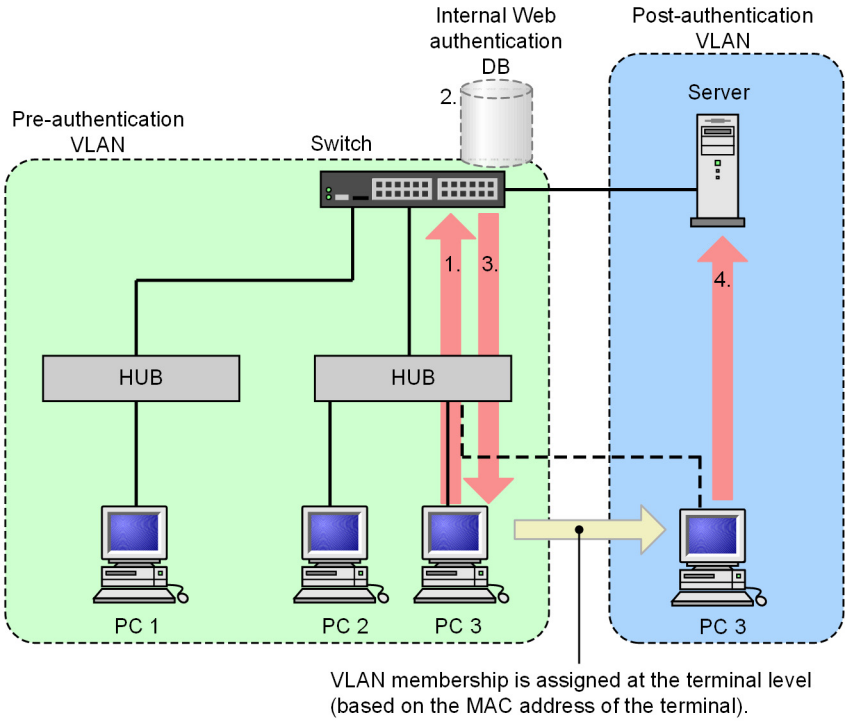
In this mode, the native VLAN is designated as the pre-authentication VLAN, and a MAC VLAN is designated as the post-authentication VLAN. Prior to authentication, the MAC address of the terminal is associated with the pre-authentication VLAN. If authentication succeeds, the switch associates the MAC address with the post-authentication VLAN. For this to work, the following configuration is required:

- A MAC VLAN must be configured as the post-authentication VLAN
- An access list must be configured that prohibits unnecessary communication between the pre-authentication and post-authentication VLANs

(1) Local authentication method

The figure below describes local authentication method using an internal Web authentication DB.

Figure 8-6: Web authentication system (local authentication method)

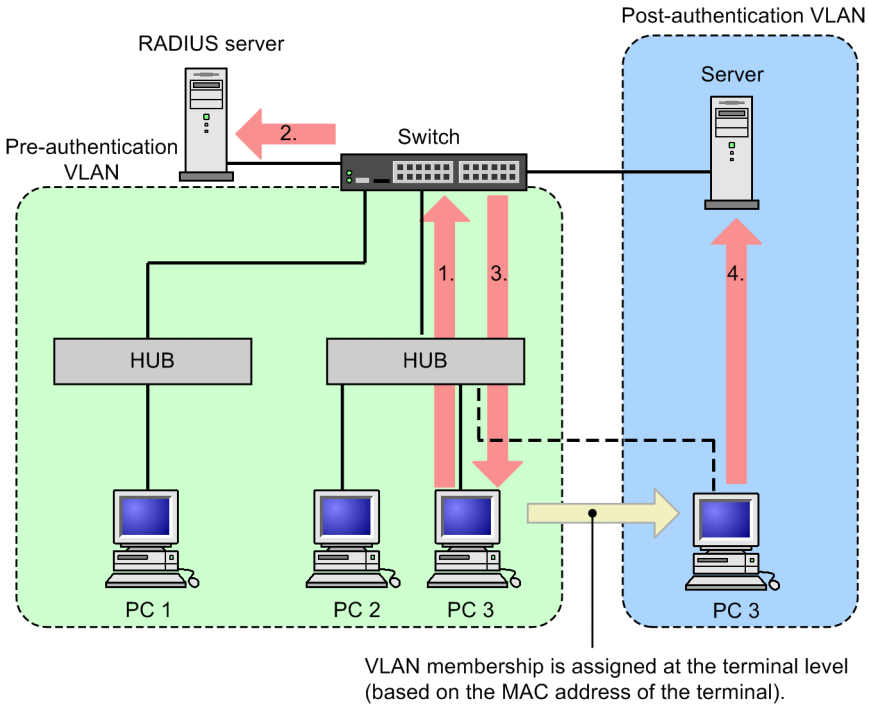


1. A user of a PC connected via a hub opens a Web browser and accesses the Switch.
2. The Switch compares the user ID and password entered by the user against the user information in the internal Web authentication DB.
3. If authentication succeeds, a page appears on the PC indicating that authentication was successful, and the PC gains membership to the post-authentication VLAN.
4. The authenticated PC is able to access servers in the post-authentication VLAN.

(2) RADIUS authentication method

The figure below describes RADIUS authentication method using a RADIUS server.

Figure 8-7: Web authentication system (RADIUS authentication method)



1. A user of a PC connected via a hub opens a Web browser and accesses the Switch.
2. Authentication takes place by comparing the user ID and password entered by the user against the user information registered on the RADIUS server.
3. If authentication succeeds, a page appears on the PC indicating that authentication was successful, and the PC gains membership to the post-authentication VLAN.
4. The authenticated PC is able to access servers in the post-authentication VLAN.

8.2.4 Configuration examples by IP address assignment method

A terminal attempting Web authentication can obtain an IP address in the three ways given below. Because Web authentication operates on the IPv4 network, the descriptions here relate to IPv4 addresses.

- IP address distribution using the Switch's internal DHCP server function
- IP address distribution using an external DHCP server
- Manual distribution of IP addresses

In fixed VLAN mode, there is no need for the terminal to change IP address after authentication. In dynamic VLAN mode and legacy mode, however, the terminal will belong to a different IP subnet after its membership changes to the post-authentication VLAN. This requires that the terminal gain a new IP address.

The following describes the system configuration for each method of assigning IP addresses in dynamic VLAN mode and legacy mode.

(1) IP address distribution using the Switch's internal DHCP server function

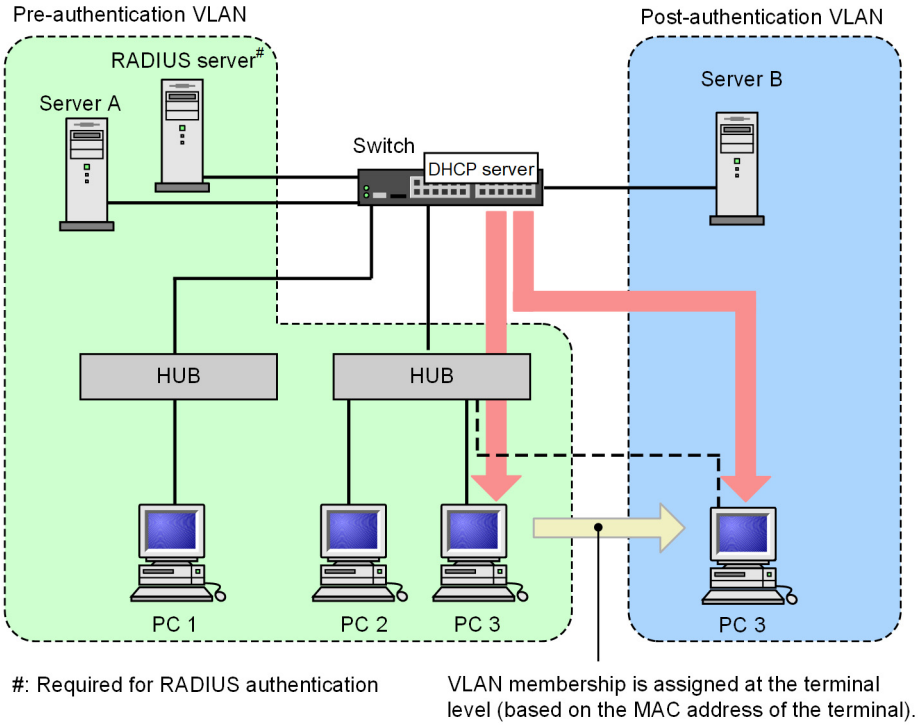
The figure below shows an example configuration in which the DHCP server built into the Switch assigns IP addresses.

The DHCP server function distributes the IP address associated with the pre-authentication VLAN to terminals seeking authentication. A terminal user can then use a Web browser to perform authentication.

Terminals that complete the authentication process gain membership to the post-authentication VLAN. After the lease for the IP address expires, the DHCP server distributes to the terminal an IP address associated with

the post-authentication VLAN, which enables access from the terminal.

Figure 8-8: Web authentication system (internal DHCP server)



Notes

- The DHCP server must be configured to distribute IP addresses associated with the pre-authentication and post-authentication VLANs.
- The DHCP server must be configured to distribute its default gateway address to attached terminals.

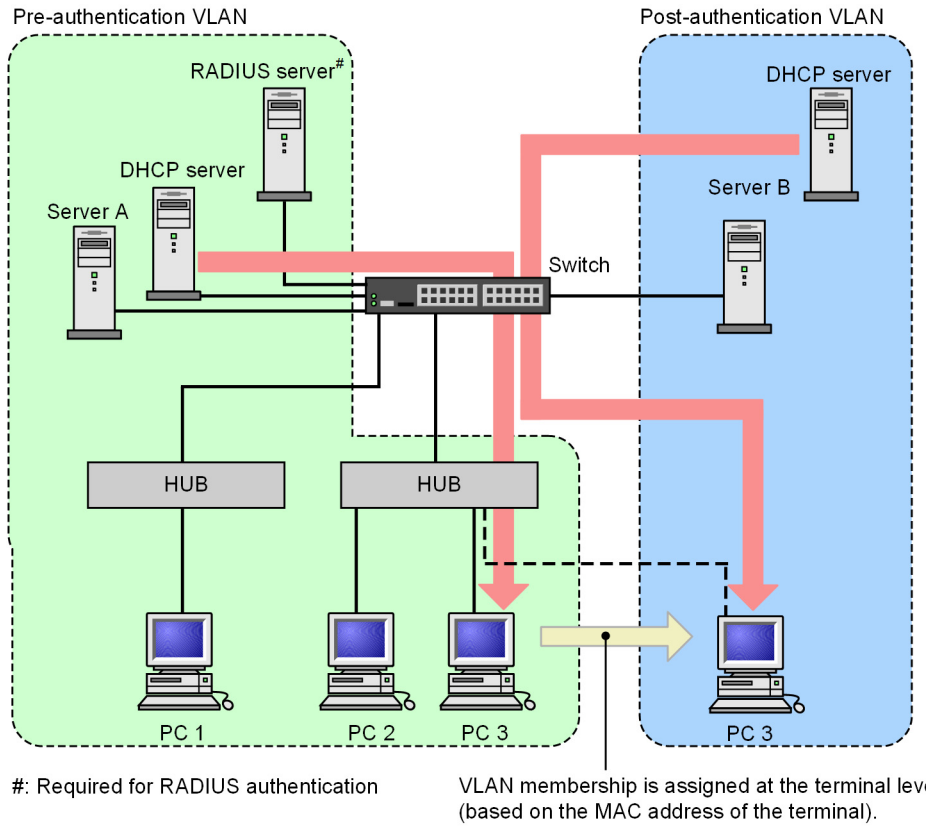
(2) Using an external DHCP server

The figure below shows an example of a configuration in which an external DHCP server distributes the IP addresses the terminal uses during and after authentication.

The external DHCP server distributes an IP address associated with the pre-authentication VLAN to a terminal seeking authentication. A user of the terminal can then perform authentication using a Web browser.

Terminals that complete the authentication process gain membership to the post-authentication VLAN. After the lease for the IP address expires, the DHCP server distributes the terminal an IP address associated with the post-authentication VLAN.

Figure 8-9: Web authentication system (external DHCP server)



Notes

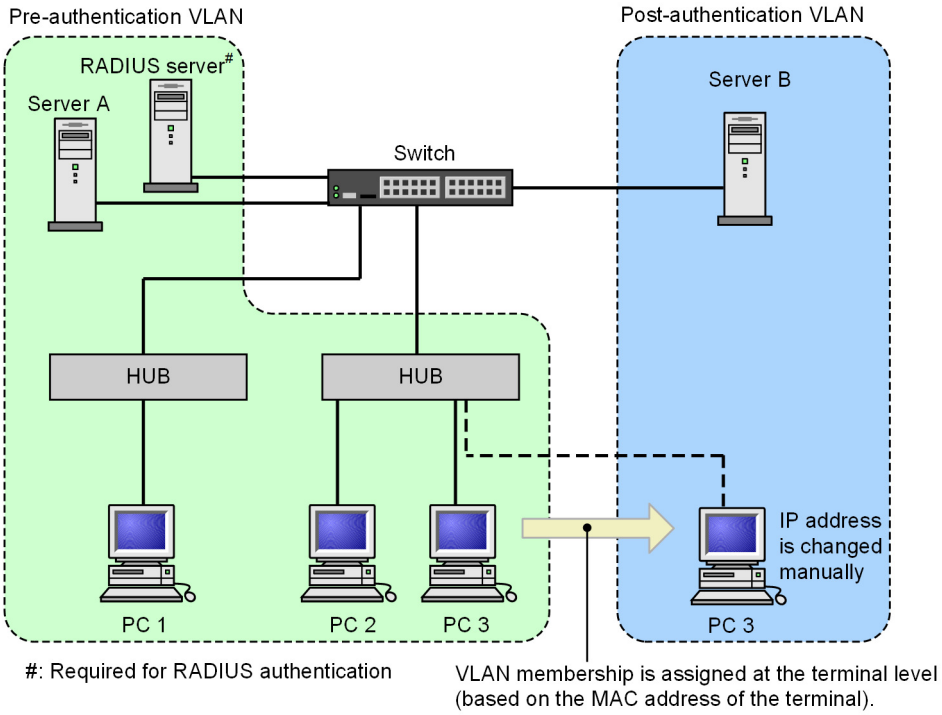
- The external DHCP server must be configured to distribute its default gateway address to attached terminals.

(3) Assigning IP addresses manually

The figure below shows an example configuration in which you change the IP address of authenticated terminals manually.

In this configuration, you give an authenticated terminal access to the post-authentication VLAN by manually assigning the terminal an IP address in the subnet for the post-authentication VLAN.

Figure 8-10: Web authentication system (manual IP address assignment)



Notes

- If you assign the wrong IP address to an authenticated terminal, the terminal will be unable to access the network even if authentication was successful.

8.3 Authentication function

8.3.1 Permitting communication by unauthenticated terminals

To allow network access by unauthenticated terminals, you must configure an authentication IPv4 access list. For details about the authentication IPv4 access list, see "5.3 Function common to all Layer 2 authentication modes".

8.3.2 Logging in to an authentication network

Terminals seeking to join an authentication network in fixed VLAN mode or dynamic VLAN mode can log in via URL redirection or by specifying a Web authentication IP address. Both methods require you to configure a Web authentication IP address.

The Web authentication IP address is an IPv4 address that terminals use to access the Switch during the Web authentication process. Because the address is not tied to a particular interface on the switch, it allows terminals on different IP subnets to use the same IP address to log in and out of the authentication network. Because packets directed to the Web authentication IP address are never forwarded outside the Switch, you can use the same address at any number of switches in the network. Therefore, the process for logging in and out of the authentication network is identical at every terminal.

Notes

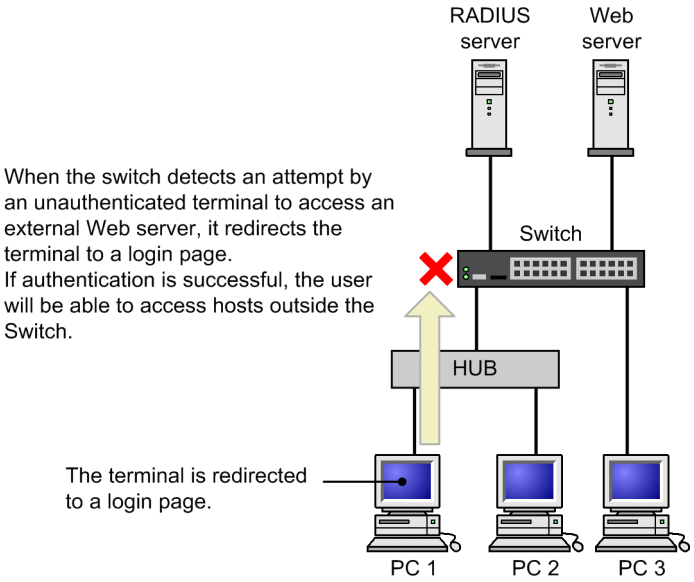
- Before terminals can use the Web authentication IP address, you must configure the "authentication arp-relay" configuration command. In an environment where this command is not configured, specify the IP address of the Switch interface when configuring the default gateway for the terminal.

(1) URL redirection function

You can configure the switch to forcibly display a login page in response to outgoing HTTP and HTTPS requests received from an unauthenticated terminal.

You can use an FQDN (fully qualified domain name) as the destination URL by specifying the name in the "web-authentication ip address" configuration command.

Figure 8-11: URL redirect function



Notes

- If the Web browser on the terminal is configured to use a proxy server, make sure that access to the Web authentication IP address bypasses the proxy server when you use the URL redirection in the following situations:

  •The "web-authentication redirect-mode" configuration command is set with the https parameter

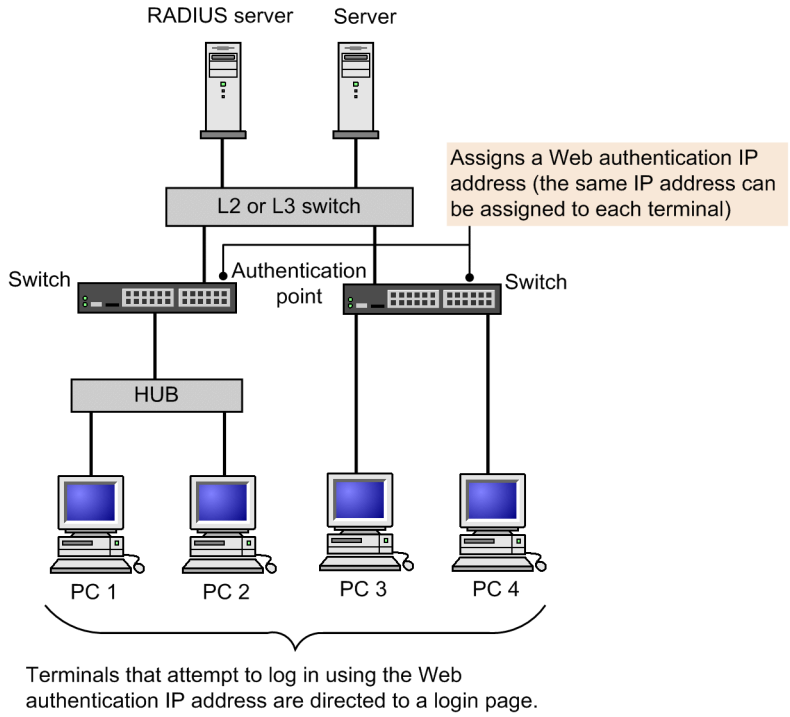
  •A user of an unauthenticated terminal accesses an external Web server using HTTPS

- When a user of an unauthenticated terminal uses the HTTPS protocol to access a URL and is redirected, if the domain name of the URL does not match the domain name of the certificate registered on the switch, a warning message about the mismatched certificate appears in the Web browser. If the user chooses to continue, a login page for Web authentication appears in the Web browser, and the user can continue the login process.

(2) Logging in by using the Web authentication IP address

Users can log in and log out by using the Web authentication IP address configured on the Switch.

Figure 8-12: Login operation using the Web authentication IP address



8.3.3 Forced authentication

For details about forced authentication in the context of Web authentication, see "5.3 Function common to all Layer 2 authentication modes".

8.3.4 Logging out of an authentication network

The following table describes the methods a terminal can use to log out of an authentication network.

Table 8-1: Logout methods by authentication mode

Logout method	Fixed VLAN mode	Dynamic VLAN mode	Legacy mode
Logout using the Web interface	Y	Y	Y
Logout when maximum connection time is exceeded	Y	Y	Y
Logout of authenticated terminals by the connection monitoring function	Y	—	—
Logout of authenticated terminals by MAC address table aging	—	Y	Y
Logout using an operation command	Y	Y	Y
Logout in response to special packets received from authenticated terminals	Y	—	—
Logout of terminals connected to link-down ports	Y	—	—
Logout resulting from changes to the VLAN configuration	Y	Y	Y

Logout method	Fixed VLAN mode	Dynamic VLAN mode	Legacy mode
Logout resulting from authentication method changes	Y	Y	Y
Logout resulting from authentication mode changes	Y	Y	Y
Logout due to suspension of Web authentication	Y	Y	Y
Logout due to deletion of a dynamically registered VLAN	—	Y	—

Legend: Y: Supported; —: Not applicable

In dynamic VLAN mode and legacy mode, after a terminal logs out in one of these ways, you must change the IP address of a terminal to an address associated with the pre-authentication VLAN. If you are using a DHCP server, you need to direct the terminal to request a new IP address after logging out.

- If you are using a DHCP server, you need to delete the IP address of the terminal before obtaining a new one from the DHCP server. (In Windows, for example, execute ipconfig /release and then ipconfig /renew from the command prompt.)
- If you assign IP addresses manually, change the IP address of the terminal to an address associated with the pre-authentication VLAN.

(1) Logout using the Web interface

When an authenticated terminal accesses the logout URL, a logout page appears on the terminal. When the user completes the logout operation in this page, their Web authentication status is cleared and a page appears indicating that the logout process is complete.

(2) Logout when maximum connection time is exceeded

When a terminal exceeds the maximum connection time specified by the "web-authentication max-timer" configuration command, its Web authentication status is forcibly cleared and the terminal is prohibited further communication outside the Switch. Clearing of the authentication status takes place within one minute of the maximum connection time being exceeded. The user is not presented with a logout page.

A user can continue to use a terminal after the maximum connection time has elapsed by repeating the login process. Only users who are confirmed to already be authenticated by a combination of user ID, password, and MAC address can extend their connection time, and only in increments of the maximum connection time.

If you use the "web-authentication max-timer" configuration command to shorten or extend the maximum connection time, the changes do not take effect until the next time the user logs in. Existing authentication sessions are unaffected.

(3) Logout of authenticated terminals by the connection monitoring function

The switch monitors the connection status of authenticated terminals by sending ARP packets at the interval specified by the "web-authentication logout polling interval" configuration command and monitoring for a response. If it receives no response 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 forcibly clears the Web authentication status of the terminal. The user is not presented with a logout page.

You can disable this function by using the "no web-authentication logout polling enable" configuration command.

Notes

In environments with a large number of authenticated users, if you use the default settings for the connection monitoring function, there might be a delay of about one minute between the switch recognizing that the terminal has timed out and the authentication status being cleared.

It might take even longer for authentication statuses to clear if the CPU is operating under a heavy load.

(4) Logout of authenticated terminals by MAC address table aging

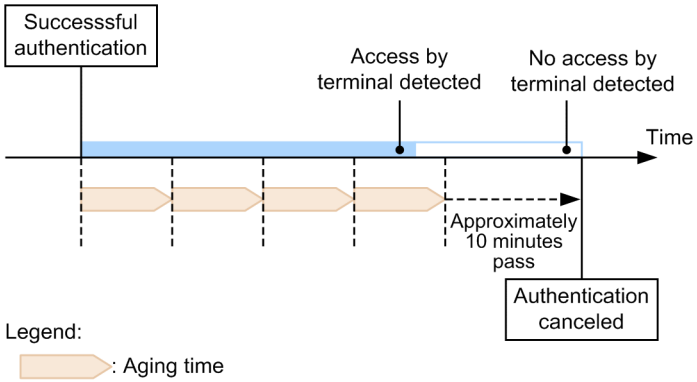
The switch monitors the MAC address table periodically for entries related to authenticated terminals, and checks for signs of recent access by those terminals. If the switch consistently finds that there has been no access by a particular terminal, it forcibly clears the Web authentication status of the terminal. The user is not presented with a logout page.

To prevent a situation in which a brief network interruption causes a terminal to lose its authentication status, authentication cancellation takes place when there has been no access from a terminal for a 10 minute period after its MAC address is scheduled to be aged out of the MAC address table.

The figure below shows the relationship between the aging time specified for the MAC address table, and the time when the terminal is logged out due to MAC address table aging.

Use the default value for the aging time, or specify a larger value than the default.

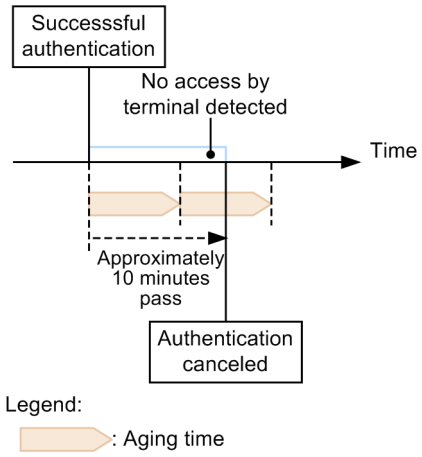
Figure 8-13: Logout of an authenticated terminal by MAC address table aging



If there is no access by a terminal in the 10 minute period after successful authentication, the terminal loses its authentication status immediately without regard to the aging time.

The following figure shows a situation in which a terminal is logged out due to inactivity after successful authentication.

Figure 8-14: Logout due to inactivity after successful authentication



You can disable this function by using the "no web-authentication auto-logout" configuration command. In this case, terminals are not forcibly logged out regardless of how long they remain inactive.

In legacy mode, if a terminal makes no attempt to access the VLAN to which it gains membership after authentication, the switch has no opportunity to learn its MAC address. 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. To avoid this situation, make sure that terminals access the VLAN in some way after authentication.

(5) Logout using an operation command

You can use the "clear web-authentication auth-state" operation command to forcibly log out individual users. When you use this command, the switch terminates every authentication session associated with the user ID you specify. The user is not presented with a logout page.

(6) Logout in response to special packets received from authenticated terminals

The switch clears the authentication status of terminals from which it receives a special packet. The user is not presented with a logout page. Special packets are defined as follows:

- A ping packet sent from an authenticated terminal to the Web authentication IP address
- A packet having a particular TOS value as specified by the "web-authentication logout ping tos-windows" configuration command
- A packet having a particular TTL value as specified by the "web-authentication logout ping ttl" configuration command

(7) Logout of terminals connected to link-down ports

When a port with authenticated terminals connected goes down, the switch clears the authentication status of terminals connected to that port. The user is not presented with a logout page.

(8) Logout 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 user is not presented with a logout page.

The following configuration changes trigger a logout:

- Deletion of a VLAN
- Suspension of a VLAN

(9) Logout resulting from authentication method changes

If you change the authentication method from RADIUS authentication to local authentication method or vice-versa, the switch clears the authentication status of all terminals. The user is not presented with a logout page.

(10) Logout resulting from authentication mode changes

If you use the "copy" command to change the switch configuration in a manner that results in changes to the authentication mode, the switch clears the authentication status of all terminals. The user is not presented with a logout page.

(11) Logout due to suspension of Web authentication

If a configuration command deletes the Web authentication configuration, which results in the suspension of Web authentication, the switch clears the authentication status of all terminals. The user is not presented with a logout page.

(12) Logout due to deletion of a dynamically registered VLAN

If the "switchport mac vlan" configuration command is set to an authentication port for which a VLAN is dynamically created, the VLAN ID dynamically created for the port is deleted, and terminals that belonged to the VLAN are unauthenticated.

8.3.5 Limited number of authentications

You can limit the number of authenticated users at the device level and at the port level. For details, see "5.3 Function common to all Layer 2 authentication modes".

8.3.6 Moving authenticated terminals between ports

For details about how the authentication status of a terminal is affected when you move it between ports, see "5.3 Function common to all Layer 2 authentication modes".

8.3.7 Accounting function

The Switch use the accounting function described below to record the results of authentication operations.

(1) Accounting logs

Web authentication accounting logs contain information about the use of Web authentication services on the Switch. You can display the log information by using the "show web-authentication logging" operation command. The following table describes the events recorded as accounting log information.

Table 8-2: Authentication results output as accounting log information

Event	Time	User ID	IP addresses	MAC addresses	VLAN ID	Port No.	Message
Login succeeded	F/D/L	F/D/L	F/D[#1]	F/D/L	F/D[#1]	F/D	Successful authentication Message
logout	F/D/L	F/D/L	F/D	F/D/L[#2]	F/D	F/D	Authentication status canceled Message
Login failed	F/D/L	F/D/L	F/D/L[#2]	F/D/L[#2]	F/D/L[#2]	F/D[#2]	Reason for failure Message

Event	Time	User ID	IP addresses	MAC addresses	VLAN ID	Port No.	Message
Forced logout	F/D/L	F/D/L	F/D#2	F/D/L#2	F/D/L#2	F/D#2	Authentication forcibly cleared Message

Legend

F/D/L: Output in fixed VLAN mode, dynamic VLAN mode, and legacy mode.

F/D: Output in fixed VLAN mode and dynamic VLAN mode.

#1: 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.

#2: Depending on the message, the IP address or other information might not be output.

The Switch can store a maximum of 2100 lines of Web authentication accounting log information. Upon reaching this limit, the switch starts overwriting the existing accounting information in order from the oldest.

(2) Providing information to the RADIUS server accounting function

You can enable the accounting feature for the RADIUS server by using the "aaa accounting web-authentication default start-stop group radius" configuration command. The accounting function records the following information: The information to be recorded is as follows.

- Login information. The following information is recorded in the event of a successful login:
  Server timestamp, user ID, MAC address
- Logout information. The following information is recorded upon logout:
  Server timestamp, user ID, MAC address, elapsed time between login and logout
- For a forced logout, the following information is recorded upon logout:
  Server timestamp, user ID, MAC address, elapsed time between login and logout

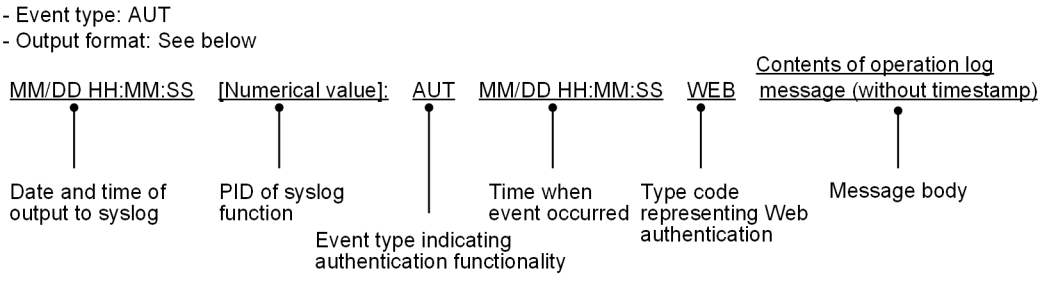
(3) Recording login information on a RADIUS server (using RADIUS server function)

If you are using RADIUS authentication method, the accounting feature of the RADIUS server records the success or failure of authentication attempts. Note that the information that is recorded differs depending on the RADIUS server implementation. For details, see the documentation for the RADIUS server deployed in your network.

(4) Writing action logs to a syslog server

You can output the action logs for Web authentication to a syslog server. These action logs include the Web authentication accounting logs. The following figure shows the format of log output to the syslog server.

Figure 8-15: Format of output to syslog server



You can start and stop output to syslog by using the "web-authentication logging enable" and "logging event-kind aut" configuration commands.

8.4 Authentication procedure

This section describes the steps involved in Web-based user authentication. The description below assumes that the user is using Internet Explorer 6.0 as their Web browser.

(1) Displaying the login page for Web authentication

Display the login screen on the web browser of the terminal and enter the user ID and password.

In an environment that uses URL redirection in fixed VLAN mode or dynamic VLAN mode, when you access any Web server via the Switch on the web browser of the terminal, the URL redirection feature intercepts HTTP or HTTPS requests and directs the user to a login page.

If you do not use the URL redirect function, access the login screen for Web authentication by specifying the following login URL on the web browser of the terminal. In the fixed VLAN mode and dynamic VLAN mode, specify a web authentication IP address in the web server portion of the login URL.

[Login URL in fixed VLAN mode or dynamic VLAN mode]

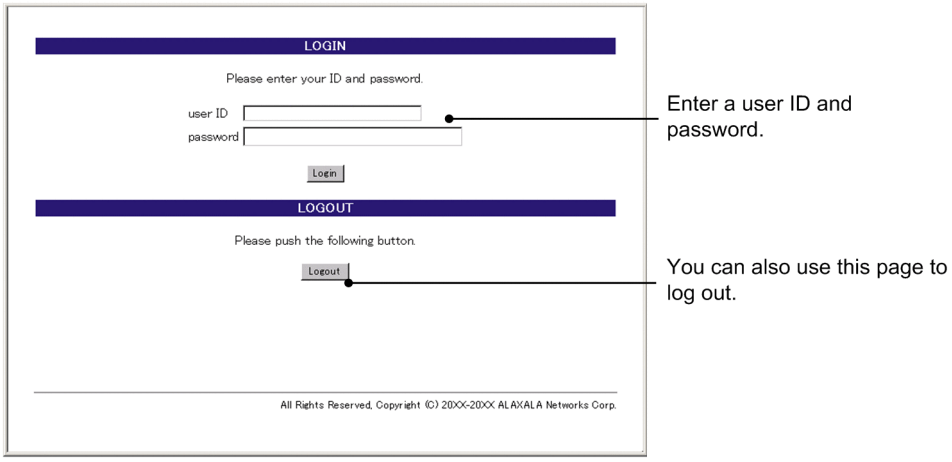
- When using HTTP: http://Web authentication IP address/login.html
- When using HTTPS: https://Web authentication IP address/login.html

The URL redirect function cannot be used in the legacy mode. Access the login screen for Web authentication by specifying the following login URL on the web browser of the terminal. In legacy mode, specify the IP address of the pre-authentication VLAN in the Web server part of the login URL.

[Login URL in legacy mode]

- When using HTTP: http://interface IP address of pre-authentication VLAN/login.html
- When using HTTPS: https://interface IP address of pre-authentication VLAN/login.html

Figure 8-16: Login page (browser display example)



(2) Authenticating the user ID and password entered in the login page

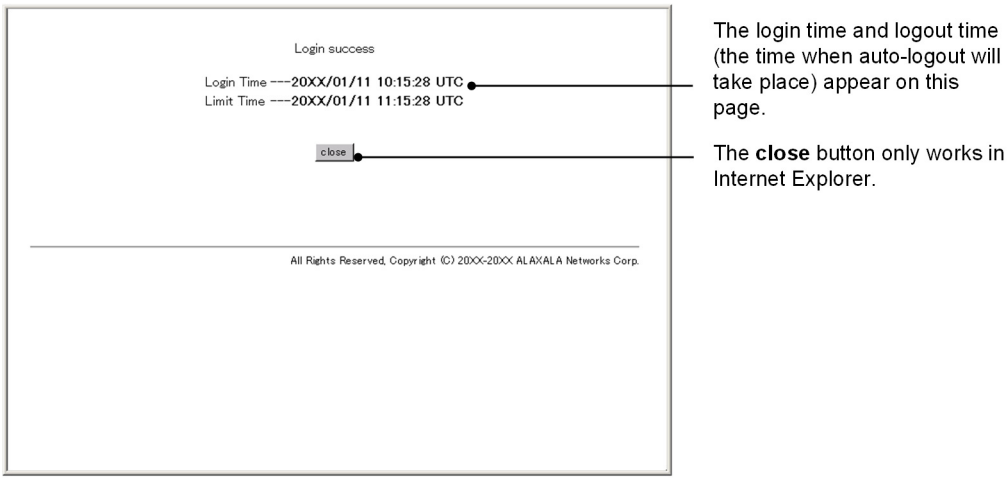
In local authentication method, the switch compares the entered user ID and password against user information stored in the internal Web authentication DB. In RADIUS authentication method, the switch validates the entered credentials by checking with the RADIUS server.

(3) Displaying a successful authentication result

If the user ID and password that the user entered match user information in the internal Web authentication DB or on the RADIUS server, the user is presented with a login success page and is able to access the network.

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.

Figure 8-17: Login success page (browser display example)

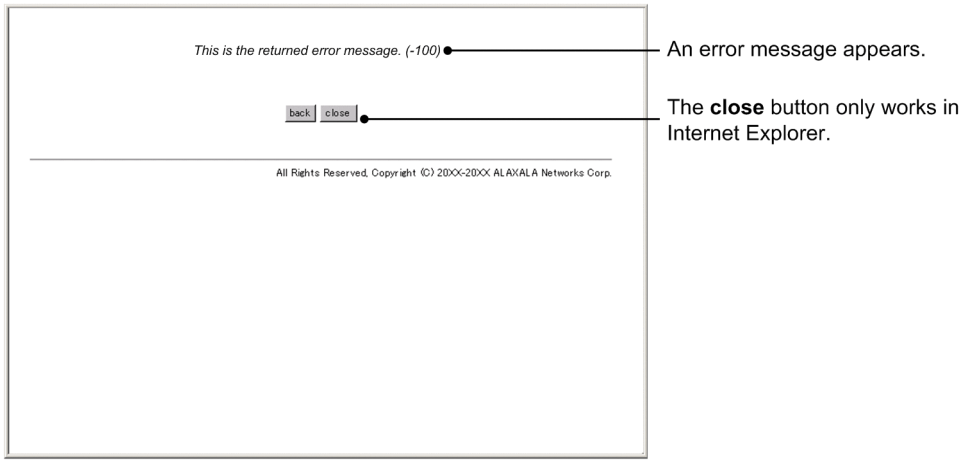


(4) Displaying a page when login fails

If authentication fails, an authentication error page appears in the Web browser.

For details about what causes each error displayed on this page, see "8.6 Authentication error messages".

Figure 8-18: Login failed page (browser display example)



(5) Displaying a Web authentication logout page

Access the authenticated terminal from a web browser specifying the logout URL to display the logout screen. When the [Logout] button is pressed on the logout screen, Web Authentication will cancel authentication of the terminal. and a page appears indicating that the logout process is complete.

In the logout URL in the fixed VLAN mode or dynamic VLAN mode, specify a web authentication IP address in the web server portion of URL.

[Logout URL in fixed VLAN mode or dynamic VLAN mode]

- When using HTTP: http://Web authentication IP address/logout.html
- When using HTTPS: https://Web authentication IP address/logout.html

You can also log out from the login screen. Press the [Logout] button on the login screen.

[Login URL in fixed VLAN mode or dynamic VLAN mode]

- When using HTTP: http://Web authentication IP address/login.html
- When using HTTPS: https://Web authentication IP address/login.html

In legacy mode, specify the IP address of the post-authentication VLAN in the Web server part of the logout URL.

[Logout URL in legacy mode]

- When using HTTP: http://interface IP address of post-authentication VLAN/login.html
- When using HTTPS: https://interface IP address of post-authentication VLAN/login.html

Figure 8-19: Logout page (browser display example)

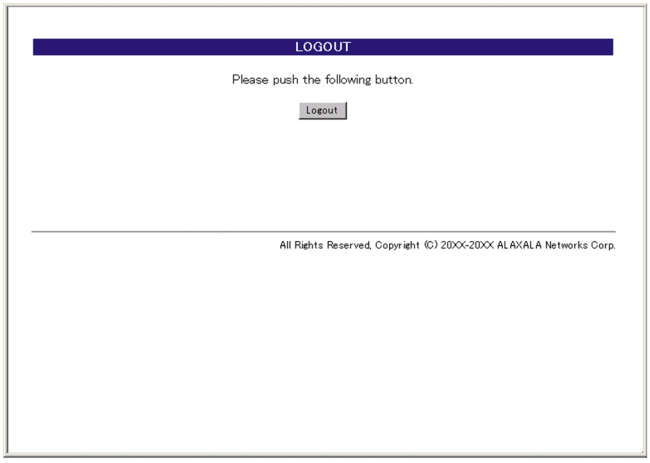
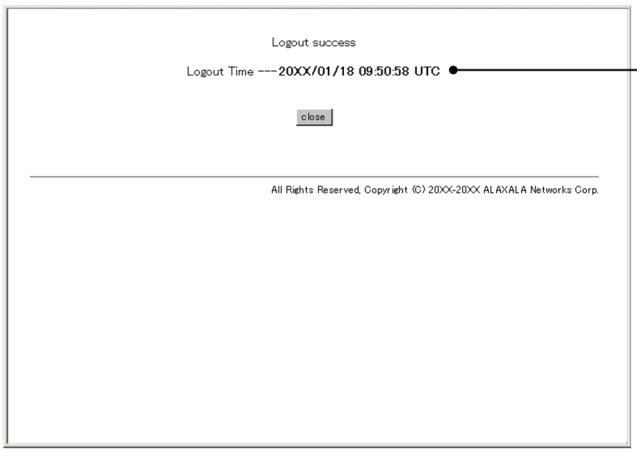


Figure 8-20: Logout completed page (browser display example)



The logout time (the time when the logout process was completed) appears.

8.5 Preparing an internal Web authentication DB and the RADIUS server

8.5.1 Preparing an internal Web authentication DB

You need to build an internal Web authentication DB before you can use Web authentication in local authentication method. You can then use commands to back up and restore the internal Web authentication DB that you built.

(1) Creating an internal Web authentication DB

You can use the "set web-authentication user" operation command to register information about a Web authentication user (such as a user ID, password, and VLAN ID) in the internal Web authentication DB. You can also use this command to change a password or delete an existing user ID.

Additions or changes to the database do not take effect until you execute the "commit web-authentication" operation command.

Note that additions or changes committed to the internal Web authentication DB by the operation command do not apply to authentication sessions that are already in progress. They will apply the next time the user logs in.

(2) Backing up the internal Web authentication DB

You can use the "store web-authentication" operation command to back up the internal Web authentication DB you created for use in local authentication.

(3) Restoring the internal Web authentication DB

You can use the "load web-authentication" operation command to restore the internal Web authentication DB from a backup file you created. Keep in mind that any recent additions or changes you made using the "set web-authentication user" operation command or similar will be lost and replaced with the contents of the backup file.

8.5.2 Preparing the RADIUS server

Before you can use Web authentication in RADIUS authentication method, you need to configure the RADIUS server as described below.

Also described below are the RADIUS attributes used by the Web authentication function in the Switch.

(1) RADIUS+ server setup

On the RADIUS server, set user information such as a user ID, password, and VLAN ID for each authentication user. For details about how to configure the RADIUS server, see the documentation for the RADIUS server deployed in your network.

Use the following procedure to configure the post-authentication VLAN to which a terminal is assigned after successful authentication in dynamic VLAN mode.

1. Specify 13 (Virtual LANs (VLAN)) for the Tunnel-Type attribute.
2. Specify 6 for the Tunnel-Medium-Type attribute.
3. Specify a VLAN ID for the Tunnel-Private-Group-ID attribute, in one of the following formats:
   - As a numerical value
     Example: If the VLAN ID is 2048, specify the character string 2048.
   - As the character string "VLAN" followed by a numerical value
     Example: If the VLAN ID is 2048, specify the character string VLAN2048.
   - As a VLAN name defined using the "name" configuration command

If you perform authentication in dynamic VLAN mode without setting Tunnel-Type, Tunnel-Medium-Type,

and Tunnel-Private-Group-ID, the native VLAN will be assigned as the post-authentication VLAN.

User IDs and passwords can be from 1 to 32 characters long, and can contain the following characters:

- User ID:ASCII character codes from 0x21 to 0x7E
- Password: ASCII character codes from 0x21 to 0x7E

As the authentication method, specify PAP.

(2) RADIUS attributes used by Web authentication

The following table describes the RADIUS attributes used for Web authentication.

Table 8-3: Attributes used for authentication (Part 1: Access-Request)

Attribute name	Type value	Description
User-Name	1	The user name.
User-Password	2	The user's password.
NAS-IP-Address	4	This attribute contains the loopback interface IP address, if one is specified. If no loop-back interface is specified, the IP address of the interface that communicates with the RADIUS server.
Service-Type	6	Specify Framed(2).
State	24	The State value in the last Access-Challenge message received from the RADIUS server in relation to the authentication session. Do not specify a value if the Access-Challenge message does not contain a State attribute.
Calling-Station-Id	31	The MAC address of the terminal to be authenticated (as a hyphen-punctuated lower-case ASCII string) Example: 00-12-e2-12-34-56
NAS-Identifier	32	A numerical string representing the VLAN ID to which authenticated terminals gain membership in fixed VLAN mode. Example (for VLAN ID 100): 100 In dynamic VLAN mode and legacy mode, use the device name as specified by the "hostname" configuration command.
NAS-Port-Type	61	Specify Virtual(5).
NAS-IPv6-Address	95	The IPv6 address of the loopback interface, if one is specified. If no loop-back interface is specified, the IPv6 address of the interface that communicates with the RADIUS server. When communicating via an IPv6 link-local address, this attribute specifies the IPv6 link-local address of the sending interface regardless of whether an IPv6 address is set for the loop-back interface.

Table 8-4: Attributes used in authentication (Part 2: Access-Accept)

Attribute name	Type value	Description
Service-Type	6	Returns Framed(2): This attribute is ignored in Web authentication.
Reply-Message	18	(Not used)
Tunnel-Type	64	Used in dynamic VLAN mode and legacy mode. The MAC-based authentication function checks whether the value is 13 (VLAN). This attribute is not used in fixed VLAN mode.
Tunnel-Medium-Type	65	Used in dynamic VLAN mode and legacy mode. The MAC-based authentication function checks whether the Tunnel-Medium-Type value is 6, as for IEEE 802.1X. This attribute is not used in fixed VLAN mode.
Tunnel-Private-Group-Id	81	Used in dynamic VLAN mode and legacy mode. The value of this attribute is a number representing a VLAN, or the character string VLANxx (where xx is the VLAN ID). An initial octet with a value in the range from 0x00 to 0x1f indicates a tag. In this case the VLAN ID is represented by the second octet onward. If the first octet has a value of 0x20 or higher, the entire value of the attribute represents the VLAN. In dynamic VLAN mode, if this attribute contains a VLAN name as specified by the "name" configuration command, the switch uses the VLAN ID associated with the VLAN name. This attribute is not used in fixed VLAN mode.

Table 8-5: Attributes used in RADIUS Accounting

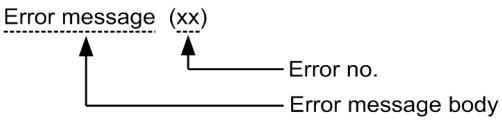
Attribute name	Type value	Description
User-Name	1	The user name.
NAS-IP-Address	4	The IP address of the NAS. This attribute contains the loopback interface IP address, if one is specified. If no loop-back interface is specified, this attribute contains the IP address of the interface that communicates with the server.
Service-Type	6	Specify Framed(2).
Calling-Station-Id	31	The MAC address of the terminal (as a hyphen-punctuated ASCII string). Example: 00-12-e2-12-34-56
NAS-Identifier	32	A numerical string representing the VLAN ID to which authenticated terminals gain membership in fixed VLAN mode. Example (for VLAN ID 100): 100 In dynamic VLAN mode and legacy mode, use the device name as specified by the "hostname" configuration command.
Acct-Status-Type	40	Contains the value Start(1) at login, and the value Stop(2) at logout.
Acct-Delay-Time	41	The length of time (in seconds) between the event occurring and transmission to the server.

Attribute name	Type value	Description
Acct-Session-Id	44	An ID for identifying the accounting information (This value is the same at login and logout.)
Acct-Authentic	45	The manner in which the user was authenticated (either RADIUS or Local).
Acct-Session-Time	46	The length of time (in seconds) between login and logout.
NAS-Port-Type	61	Specify Virtual(5).
NAS-IPv6-Address	95	The IPv6 address of the NAS. The IPv6 address of the loopback interface, if one is specified. If no loop-back interface is specified, this attribute contains the IPv6 address of the interface that communicates with the server. When communicating via an IPv6 link-local address, this attribute specifies the IPv6 link-local address of the sending interface regardless of whether an IPv6 address is set for the loop-back interface.

8.6 Authentication error messages

The figure below shows the format of the error messages displayed on the authentication error page.

Figure 8-21: Format of authentication error messages



The table below describes the cause of each authentication error you might encounter.

Table 8-6: 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 32 characters.
	13	No password was specified or the specified password contained too many characters.
	14	The specified user ID is not registered in the internal Web authentication DB.
	15	No password is registered in the internal Web authentication DB.
	16	The QUERY_STRING parameter of the GET method contains fewer than 21 characters or more than 256 characters.
	17	The CONTENT_LENGTH parameter of the POST method contains fewer than 21 characters or more than 340 characters.
	18	The login user ID contains illegal characters.
	20	The password contains illegal characters.
	22	An attempt to log in again from an authenticated terminal using local authentication method failed because the user entered the wrong password.
RADIUS: Authentication reject.	31	A response other than Accept was received from the RADIUS server. A rejection or challenge triggers this error.
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.
You cannot login by this machine.	33	The post-authentication VLAN specified by the RADIUS server does not appear in the Web authentication definition. Alternatively, no interface is assigned to the VLAN.
	34	An attempt to log in again from an authenticated terminal using RADIUS authentication method failed because a response other than Accept was received from the RADIUS server. This error is triggered when the response is a rejection or challenge.

Error message	Error no.	Cause
	35	In fixed VLAN mode, the authentication port to which the terminal is connected has gone down. Alternatively, the port is not configured for fixed VLAN mode.
	36	The VLAN containing a port configured for fixed VLAN mode has been suspended. Alternatively, no interface is assigned to the VLAN.
	41	A login request was received under a different user ID from a Web-authenticated terminal. Alternatively, in dynamic VLAN mode, a login request was received from an authenticated terminal in a different VLAN.
	42	The VLAN ID specified in the internal Web authentication DB does not match the VLAN specified in the Web authentication definition. Alternatively, no interface is assigned to the VLAN.
	44	The terminal has already been authenticated by IEEE 802.1X or MAC-based authentication, or the terminal's MAC address has been registered in a MAC VLAN by the "mac-address" configuration command.
	45	The terminal is connected to a link-down port. Alternatively, the port is not configured for fixed VLAN mode or dynamic VLAN mode.
	46	The VLAN containing the authentication port is suspended. Alternatively, no interface is assigned to the VLAN.
	47	The authentication failed because the number of users logged in by Web authentication exceeded the capacity limits.
	76	The port where the terminal is connected was down when the switch attempted to register the MAC address in the MAC address table. Alternatively, the port is not configured for fixed VLAN mode or dynamic VLAN mode.
	77	The associated VLAN was suspended when the switch attempted to register the MAC address of a terminal in the MAC address table. Alternatively, no interface is assigned to the VLAN.
Sorry, you cannot login just now. Please try again after a while.	37	There are more than 256 RADIUS authentication requests pending. The user can try again.
	43	The number of users logged in by Web authentication, MAC-based authentication, and IEEE 802.1X authentication has exceeded the capacity limits.
	48	The number of authenticated users at the authentication port has exceeded the maximum.
	51	The switch could not resolve the terminal's MAC address from its IP address.

Error message	Error no.	Cause
	52	The Web server failed to connect to the Web authentication daemon.
	53	An internal Web authentication error occurred (The Web server could not pass the login request to the Web authentication daemon.)
	54	An internal Web authentication error occurred (The Web server did not get a response from the Web authentication daemon.)
The system error occurred. Please contact the system administrator.	61	An internal Web authentication error occurred (The switch could not acquire the CONTENT_LENGTH parameter of the POST method.)
	62	An internal Web authentication error occurred (A parameter acquired by the POST or GET method contained two or more ampersands (&).)
	63	An internal Web authentication error occurred (The Web server could not acquire the IP address of the terminal.)
	64	The switch could not access the RADIUS and Accounting servers (causing authentication to fail).
A fatal error occurred. Please inform the system administrator.	65	An internal Web authentication error occurred (more than 256 RADIUS authentication requests occurred simultaneously).
	72	The switch could not register the MAC address of the authenticated terminal in the MAC VLAN.
	73	The switch could not remove from a MAC VLAN the MAC address of a terminal whose authentication status was cleared.
	74	An error occurred when the switch attempted to register a MAC address in the MAC address table.
	75	An error occurred when the switch attempted to delete a MAC address from the MAC address table.
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 to 2x: Log in again using the correct user ID and password.
- 3x: Review the RADIUS configuration.
- 4x: Review the Web authentication configuration and the internal Web authentication DB settings.
- 5x: Repeat the login process. If the same message appears again, use the "restart web-authentication" operation command to restart Web authentication.

- 6x to 7x: Use the "restart web-authentication" operation command to restart Web authentication.
- 8x: Repeat the logout process.

8.7 Replacing Web authentication pages

You can use an operation command to replace the pages that appear during the Web authentication process (for example, the login and logout pages) with your own HTML files. If a file corresponding to a page listed below is contained in the directory you specify in the operation command, the switch replaces the default page with the new file. You can also register image files in GIF and other formats. 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.

The pages you can replace are listed below.

Replaceable pages:

- Login page
- Logout page
- Login success page
- Login failed page
- Logout completed page
- Logout failed page
- Reply-Message page

You can use another operation command to delete the Web authentication pages you registered. In this case, the default pages are restored.

You can also replace the authentication error messages listed in "Table 8-6: 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.

For details about each file, see "9.3 Procedure for creating Web authentication pages".

If the registration process is interrupted in one of the following ways, a situation might arise in which the default pages appear instead of the registered pages, despite the results of the "show web-authentication html-files" operation command indicating that registration was successful.

- You intentionally interrupt the registration process by pressing [CTRL] + [C]
- You log in via a Telnet console, and the Telnet connection is dropped for some reason during the registration process

If the process of registering Web authentication pages is interrupted, try the registration process again.

8.8 Notes on using Web authentication

(1) Notes on use with other functions

For details about the interoperability with other functions, see "5.2 Interoperability of Layer 2 authentication with other functions".

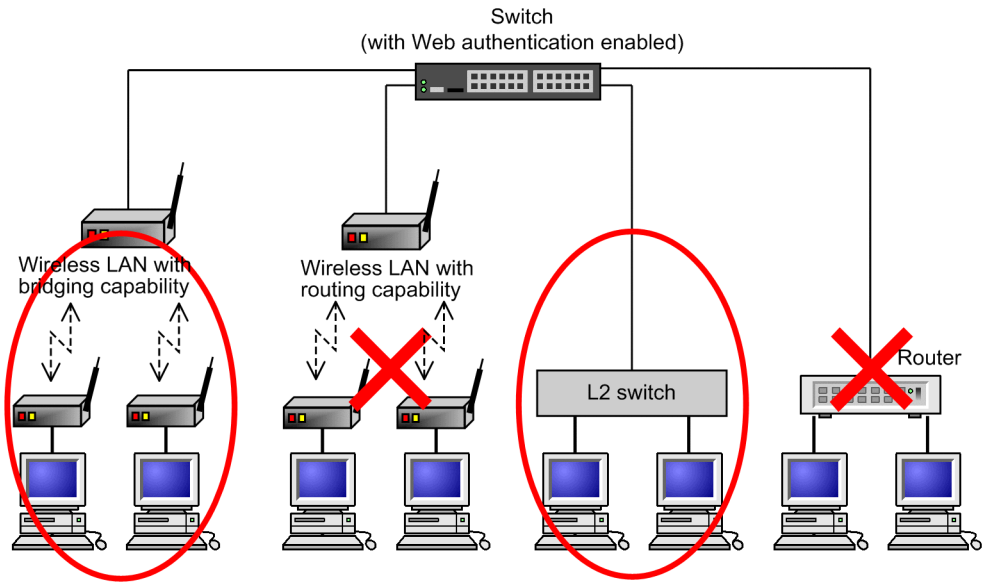
(2) Connecting devices between the terminal and the Switch

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.

Exercise caution when connecting a hub without inter-port isolation function 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 8-22: Connections between terminals and the switch

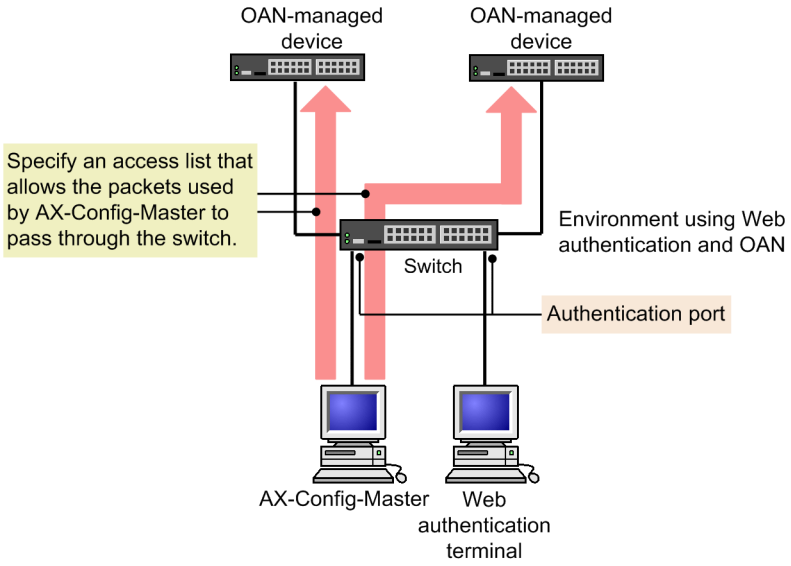


(3) Interoperability with OAN

Web authentication can coexist with OAN. However, the following conditions apply when using Web authentication and OAN together in fixed VLAN mode and dynamic VLAN mode:

- If you connect the AX-Config-Master tool to an authentication port of the Switch and wish to manage the switch without going through Web authentication, you must use the "web-authentication web-port" configuration command to specify the HTTPS ports used by OAN (ports 832, 9698).
- If the AX-Config-Master tool is connected to an authentication port of the Switch and you want the tool to manage devices outside the Switch without going through Web authentication, you must configure the access list to forward IP packets used by OAN as shown in the figure below.

Figure 8-23: Interoperability with OAN



(4) Behavior when the VLAN feature restarts

When you use the "restart vlan" operation command to restart the VLAN function, the switch does not clear the authentication status of Web-authenticated users. Instead, users are re-registered in the same order in which they performed authentication. Note that affected users will be unable to access the network until the registration process is complete, which can take some time depending on the number of users.

(5) Restarting the Web authentication program

If you restart the Web authentication daemon, the switch cancels the authentication status of all authenticated users. In this case, users need to perform re-authentication manually after the daemon restarts.

(6) Setting the lease time for IP addresses from the DHCP server

When using a DHCP server to distribute 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.

(7) Changes to the post-authentication VLAN after re-authentication in legacy mode

In legacy mode, if a user performs a successful login operation (re-authentication operation) from an authenticated terminal using the ID of an authenticated user, the user does not change VLAN ID even if the VLAN ID returned by the RADIUS server or set in the internal Web authentication DB has changed in the interim.

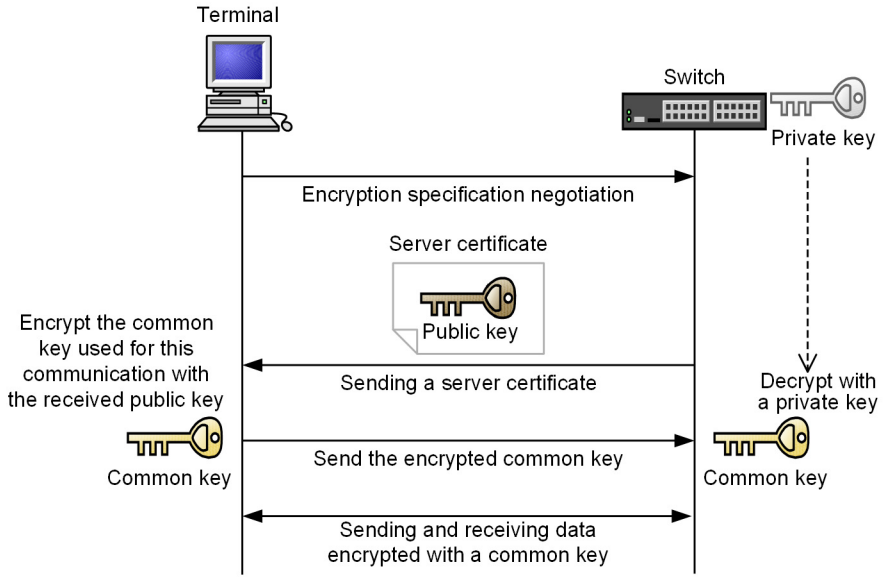
For local authentication and RADIUS authentication method, the same condition applies in that the user remains attached to the post-authentication VLAN assigned at the first successful authentication.

8.9 Operating SSL certificates

8.9.1 Login and logout via HTTPS

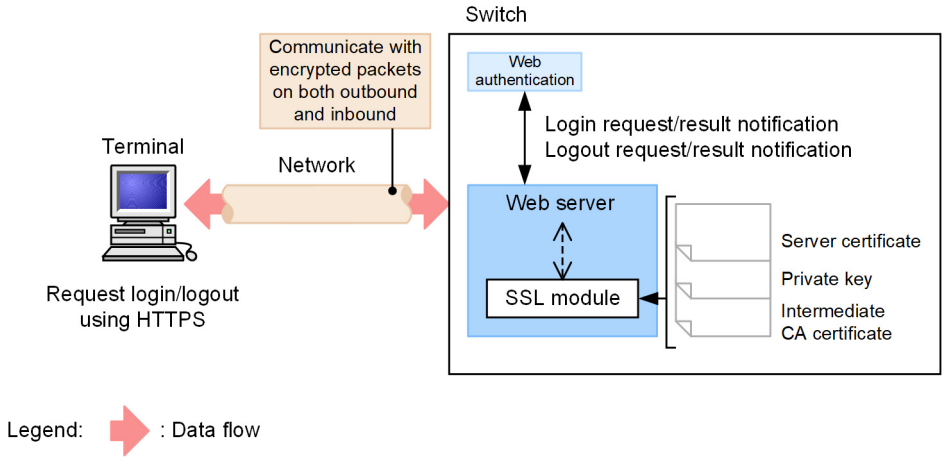
HTTPS can be used to protect the communication of Web authentication login and logout operations from others. Web authentication uses a one-way authentication method that treats the Switch as a server, and encrypts communication with a server certificate and key using the SSL module installed in the Switch. In addition, TLS is also included when it is written as SSL below. The following figure shows SSL behavior.

Figure 8-24: SSL behavior



Using HTTPS for login and logout operations encrypts the packets that pass over the network. The following figure shows Web authentication communication between the Switch and a terminal using HTTPS.

Figure 8-25: Web authentication communication between the Switch and a terminal using HTTPS



To use SSL, it is necessary to register a server certificate, private key, and intermediate CA certificate in the Switch. When shipped from the factory, a default server certificate and private key are registered, but in actual operation, be sure to create a server certificate, private key, and intermediate CA certificate according to your usage environment, and register them in the Switch (the intermediate CA certificate is not registered when shipped from the factory).

8.9.2 Supported specifications

The following table describes the specifications of SSL supported by the Switch.

Table 8-7: SSL supported specifications

Category	Description	Supported
SSL/TLS version	TLS 1.0	Y
	TLS 1.1	Y
	TLS 1.2	Y
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Y
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Y
	TLS_RSA_WITH_AES_256_GCM_SHA384	N
	TLS_RSA_WITH_AES_128_GCM_SHA256	N
	TLS_RSA_WITH_AES_256_CBC_SHA	Y
	TLS_RSA_WITH_AES_128_CBC_SHA	Y
	TLS_RSA_WITH_3DES_EDE_CBC_SHA	Y
	TLS_RSA_WITH_RC4_128_SHA	Y
Authentication method	RSA (1024 to 4096 bits)	Y
Message authentication code	SHA-256, SHA-384, SHA-512, and SHA-1	Y

Legend: Y: Supported; N: Not supported.

We recommend RSA 2048-bit for the authentication method and SHA-256 for the message authentication code.

8.9.3 Operation flow

Follow the steps below to use HTTPS (SSL communication).

1. Create a server certificate and key on your PC.
2. Transfer the server certificate and key to the Switch using the memory card or the "sftp" and "scp" operation commands.
3. Registering the server certificate and key to the Switch.
4. Restart Web authentication.

9 Settings and Operation for Web Authentication

This chapter explains the Web authentication feature, which controls VLAN access at the user level based on credentials supplied from a Web browser. This chapter describes the Web authentication operation.

9.1 Configuration

9.1.1 List of configuration commands

The following table describes the list of configuration commands for Web authentication.

Table 9-1: List of configuration commands

Command name	Description
aaa accounting web-authentication default start-stop group radius	Enables accounting for Web authentication sessions.
aaa authentication web-authentication default group radius	Specifies RADIUS as the default method for Web authentication.
web-authentication auto-logout	Configures forced logout based on MAC address aging.
web-authentication ip address	Specifies the Web authentication IP address for use in fixed VLAN mode and dynamic VLAN mode.
web-authentication jump-url	Specifies the URL to which terminals are directed after successful authentication.
web-authentication logging enable	Starts the output of authentication results and action logs to the syslog server.
web-authentication logout ping tos-windows	Specifies the TOS value of special pings sent by authenticated terminals.
web-authentication logout ping ttl	Specifies the TTL value of special pings sent by authenticated terminals.
web-authentication logout polling count	Specifies the number of times the switch resends the monitoring packet when there is no response.
web-authentication logout polling enable	Enables the connection monitoring function that monitors the behavior of authenticated terminals.
web-authentication logout polling interval	Specifies the interval between transmissions of monitoring (ARP) packets by the connection monitoring function.
web-authentication logout polling retry-interval	Specifies the interval between retransmissions of monitoring (ARP) packets when there is no response.
web-authentication max-timer	Specifies the maximum connection time for Web-authenticated users.
web-authentication max-user	Specifies the maximum number of Web-authenticated users permitted in dynamic VLAN mode and legacy mode.
web-authentication port	Designates a port as an authenticating port in fixed VLAN mode and dynamic VLAN mode.
web-authentication redirect enable	Enables URL redirection function.
web-authentication redirect-mode	Specifies the protocol (HTTP or HTTPS) used to display login pages on a terminal subject to URL redirection.
web-authentication ssl connection-timeout	Sets the timeout value for SSL session establishment.

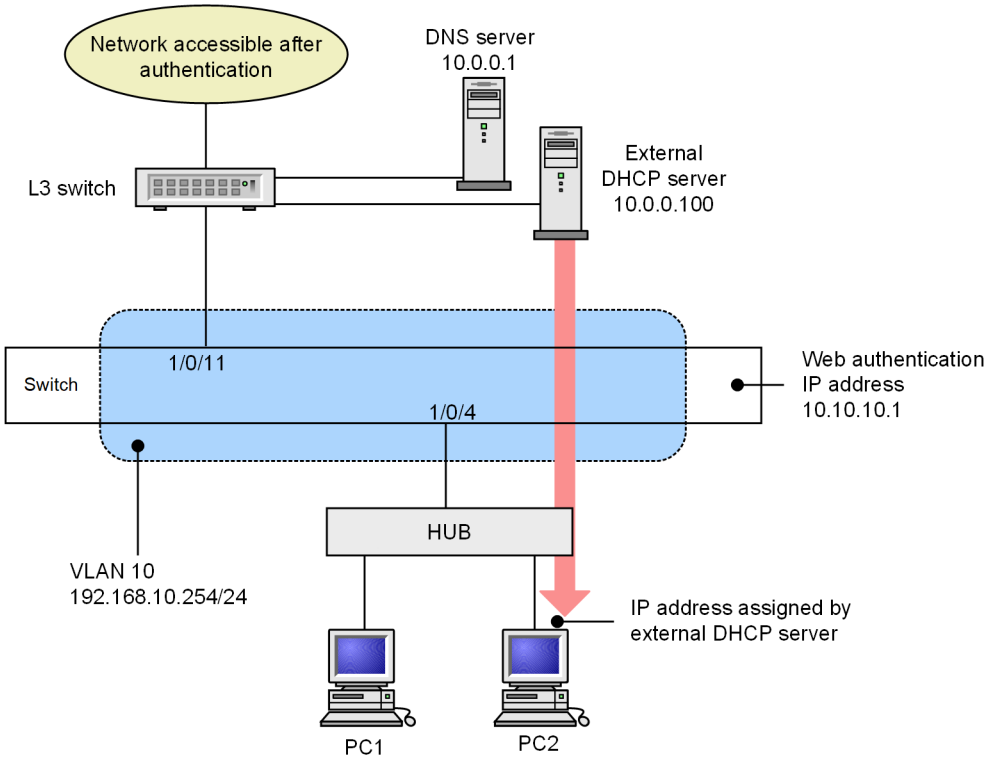
Command name	Description
web-authentication static-vlan max-user	Specifies the maximum number of authenticated users permitted in fixed VLAN mode.
web-authentication system-auth-control	Enables Web authentication.
web-authentication vlan	In legacy mode, specifies the VLAN IDs that can serve as post-authentication VLANs for Web authentication.
web-authentication web-port	Adds an access port capable of Web server access.

9.1.2 Configuration for fixed VLAN mode

(1) Basic configuration for local authentication method

The figure below describes the basic configuration required to use local authentication method.

Figure 9-1: Basic configuration for local authentication method in fixed VLAN mode



(a) Configuring an authentication port

Points to note

Configure the port to be used for Web authentication.

Command examples

1.
```
(config)# vlan 10
(config-vlan)# state active
(config-vlan)# exit
```
2.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode access
```

```
(config-if)# switchport access vlan 10
(config-if)# web-authentication port
(config-if)# exit
```

Assigns a VLAN ID and configures Web authentication at a port where terminals will be authenticated.

3.
```
(config)# interface gigabitethernet 1/0/11
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit
```

Specifies the port that connects to the L3 switch of the network accessed after authentication.

(b) 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 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
```

Assigns an IP address to VLAN ID 10 used in Web authentication.

(c) Setting the authentication IPv4 access list

Points to note

Configure an authentication IPv4 access list that allows traffic from unauthenticated terminals to reach destinations outside the Switch.

Command examples

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit udp any any eq bootps
(config-ext-nacl)# permit udp any any eq domain
(config-ext-nacl)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# authentication ip access-group 100
(config-if)# authentication arp-relay
(config-if)# exit
```

Configures an authentication IPv4 access list that allows unauthenticated terminals to send DHCP packets and access the DNS server. These commands also configure the Switch to forward ARP packets to external destinations.

(d) Configuring Web authentication

Points to note

Enable Web authentication by using configuration commands.

Command examples

1. `(config)# web-authentication ip address 10.10.10.1`

   Sets the Web authentication IP address (IPv4 address).

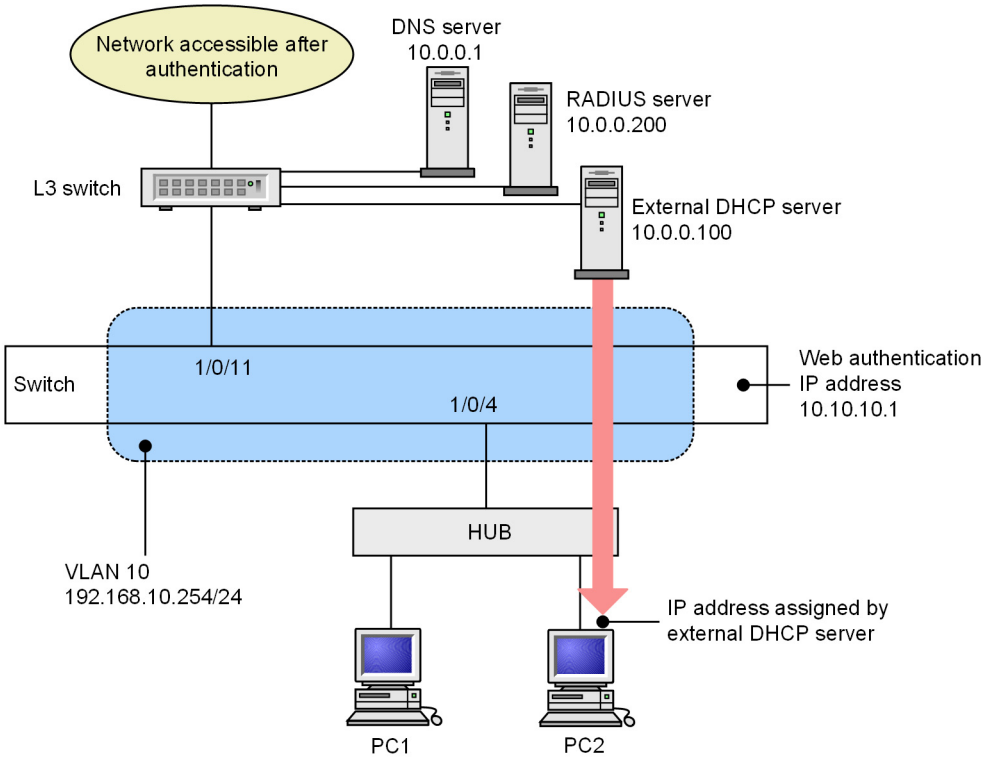
2. `(config)# web-authentication system-auth-control`

   Starts Web authentication.

(2) Basic configuration for RADIUS authentication method

The following figure shows the basic configuration required to use RADIUS authentication method.

Figure 9-2: Basic configuration for RADIUS authentication method in fixed VLAN mode



(a) Configuring an authentication port

Points to note

Configure the port to be used for Web authentication.

Command examples

1. `(config)# vlan 10`

   `(config-vlan)# state active`

   `(config-vlan)# exit`

2. `(config)# interface gigabitethernet 1/0/4`

   `(config-if)# switchport mode access`

   `(config-if)# switchport access vlan 10`

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

   `(config-if)# exit`

   Assigns a VLAN ID and configures Web authentication at a port where terminals will be authenticated.

3.
```
(config)# interface gigabitethernet 1/0/11
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit
```

Specifies the port that connects to the L3 switch of the network accessed after authentication.

(b) 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 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
```

Assigns an IP address to VLAN ID 10 used in Web authentication.

(c) Setting the authentication IPv4 access list

Points to note

Configure an authentication IPv4 access list that allows traffic from unauthenticated terminals to reach destinations outside the Switch.

Command examples

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit udp any any eq bootps
(config-ext-nacl)# permit udp any any eq domain
(config-ext-nacl)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# authentication ip access-group 100
(config-if)# authentication arp-relay
(config-if)# exit
```

Configures an authentication IPv4 access list that allows unauthenticated terminals to send DHCP packets and access the DNS server. These commands also configure the Switch to forward ARP packets to external destinations.

(d) Configuring Web authentication

Points to note

Enable Web authentication by using configuration commands.

Command examples

1.
```
(config)# web-authentication ip address 10.10.10.1
```

Sets the Web authentication IP address (IPv4 address).

2.
```
(config)# aaa authentication web-authentication default group radius
(config)# radius-server host 10.0.0.200 key "webauth"
```

Specifies the IP address and RADIUS key used to access the RADIUS server to perform user authentication.

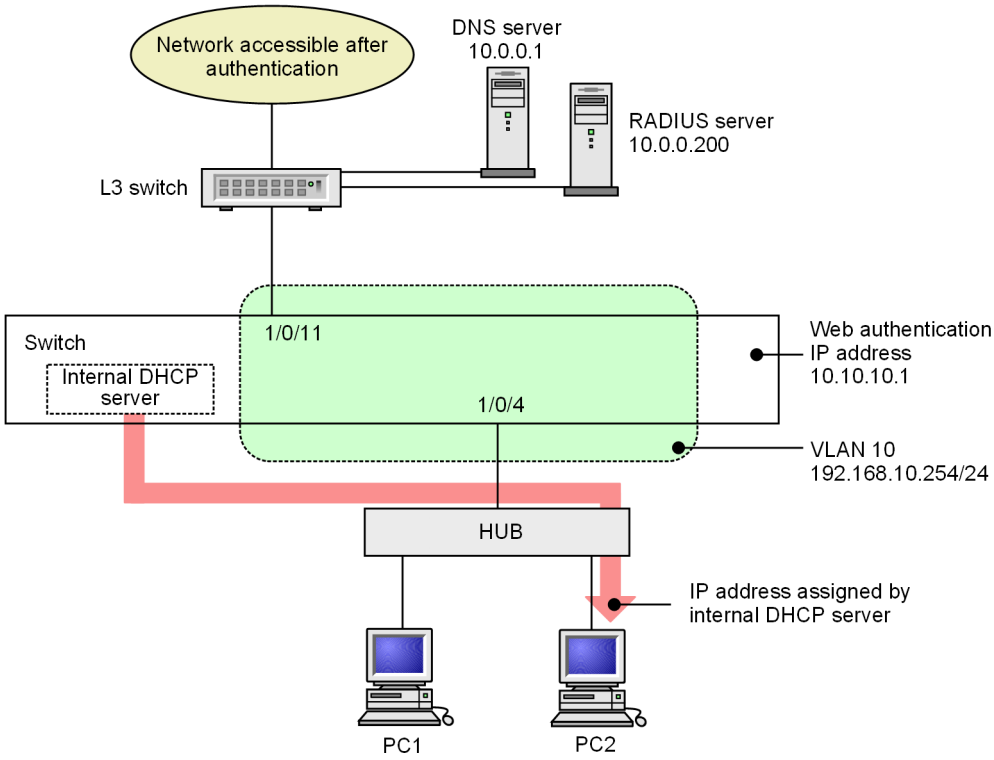
3. `(config)# web-authentication system-auth-control`

   Starts Web authentication.

(3) Configuration when using RADIUS authentication method and an internal DHCP server

The following figure shows the basic configuration required to use RADIUS authentication method with the DHCP server built in to the Switch.

Figure 9-3: Basic configuration for RADIUS authentication method using the internal DHCP server in fixed VLAN mode



(a) Configuring an authentication port

Points to note

Configure the port to be used for Web authentication.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# web-authentication port
(config-if)# exit
```

   Assigns a VLAN ID and configures Web authentication at a port where terminals will be authenticated.

2.
```
(config)# interface gigabitethernet 1/0/11
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit
```

Specifies the port that connects to the L3 switch of the network accessed after authentication.

(b) 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 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
```

Assigns an IP address to VLAN ID 10 used in Web authentication.

(c) Setting the authentication IPv4 access list

Points to note

Configure an authentication IPv4 access list that allows traffic from unauthenticated terminals to reach destinations outside the Switch.

Command examples

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit udp any any eq domain
(config-ext-nacl)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# authentication ip access-group 100
(config-if)# authentication arp-relay
(config-if)# exit
```

Configures an authentication IPv4 access list that allows unauthenticated terminals to send DHCP packets to the internal DHCP server and to access the DNS server. These commands also configure the Switch to forward ARP packets to external destinations.

(d) Configuring Web authentication

Points to note

Enable Web authentication by using configuration commands.

Command examples

1.
```
(config)# web-authentication ip address 10.10.10.1
```

Sets the Web authentication IP address (IPv4 address).

2.
```
(config)# aaa authentication web-authentication default group radius
(config)# radius-server host 10.0.0.200 key "webauth"
```

Specifies the IP address and RADIUS key used to access the RADIUS server to perform user authentication.

3.
```
(config)# web-authentication system-auth-control
```

Starts Web authentication.

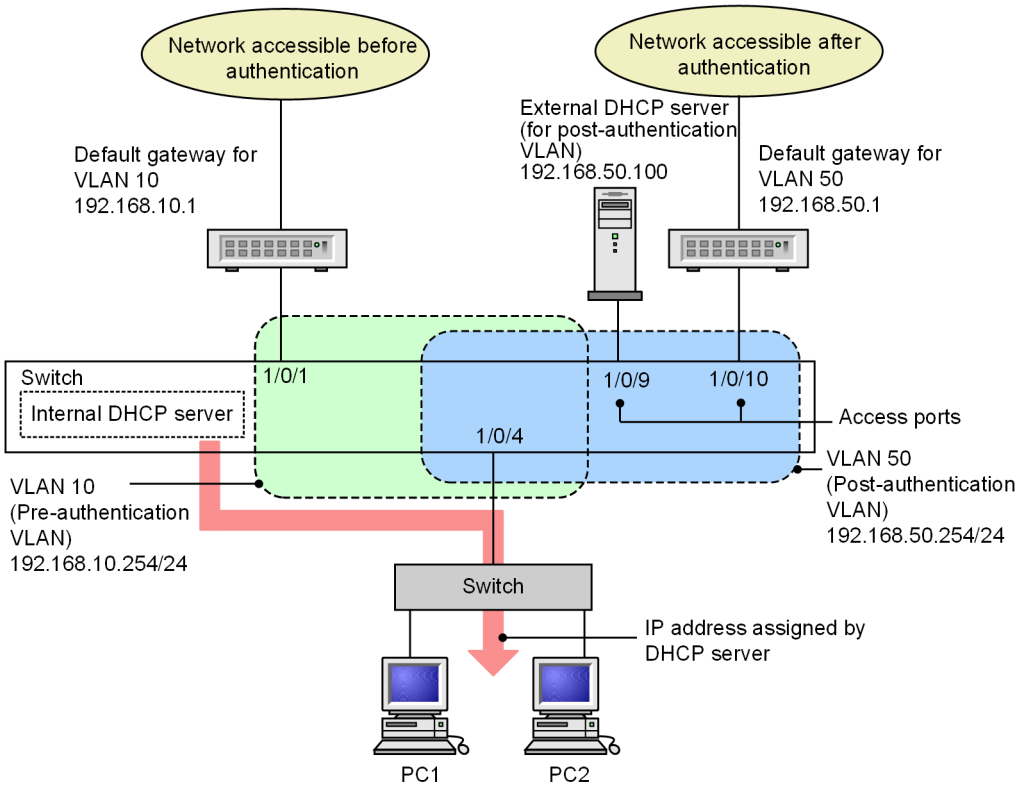
9.1.3 Configuration for dynamic VLAN mode

(1) Basic configuration for local authentication method

The figure below shows the basic configuration required to use local authentication method. Note that the terminal obtains its IP address from the internal DHCP server prior to authentication and from an external DHCP server after authentication.

This configuration includes putting a filter in place that prohibits communication between the pre-authentication VLAN and the post-authentication VLAN.

Figure 9-4: Basic configuration for local authentication method in dynamic VLAN mode



(a) Configuring an authentication port

Points to note

Configure the port to be used for Web authentication.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 10
(config-if)# web-authentication port
(config-if)# exit
```

Assigns a MAC VLAN and configures Web authentication at a port where terminals will be authenticated.

2.
```
(config)# interface range gigabitethernet 1/0/9-10
(config-if-range)# switchport mode access
```

```
(config-if-range)# switchport access vlan 50
(config-if-range)# exit
```

Specifies the access port of the network accessed after authentication.

(b) Assigning IP addresses to VLAN interfaces

Points to note

Assign IP addresses to the pre-authentication and post-authentication VLANs.

Command examples

1.
```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit
```

Assigns IP addresses to the pre-authentication VLAN and the post-authentication VLAN.

(c) Setting the authentication IPv4 access list

Points to note

Configure an authentication IPv4 access list that allows traffic from unauthenticated terminals to reach destinations outside the Switch.

Command examples

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit ip host 192.168.10.0 host 192.168.10.1
(config-ext-nacl)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# authentication ip access-group 100
(config-if)# authentication arp-relay
(config-if)# exit
```

Configures an authentication IPv4 access list that allows unauthenticated terminals to send DHCP packets to the internal DHCP server, and to access the default gateway of VLAN 10 (IP address 192.168.10.1). These commands also configure the Switch to forward ARP packets to external destinations.

(d) Prohibiting communication between VLANs

Points to note

Filter traffic between the pre-authentication and post-authentication VLANs.

Command examples

1.
```
(config)# ip access-list extended 110
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
```

```
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 10
(config-if)# ip access-group 110 in
(config-if)# exit
```

2.
```
(config)# ip access-list extended 150
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.50.100 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit udp host 192.168.50.100 any eq bootpc
(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 192.168.50.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 50
(config-if)# ip access-group 150 in
(config-if)# exit
```

Configures the switch to block communication between the pre-authentication VLAN and the post-authentication VLAN.

(e) Configuring Web authentication

Points to note

Enable Web authentication by using configuration commands.

Command examples

1.
```
(config)# web-authentication ip address 10.10.10.1
```

Sets the Web authentication IP address (IPv4 address).

2.
```
(config)# web-authentication system-auth-control
```

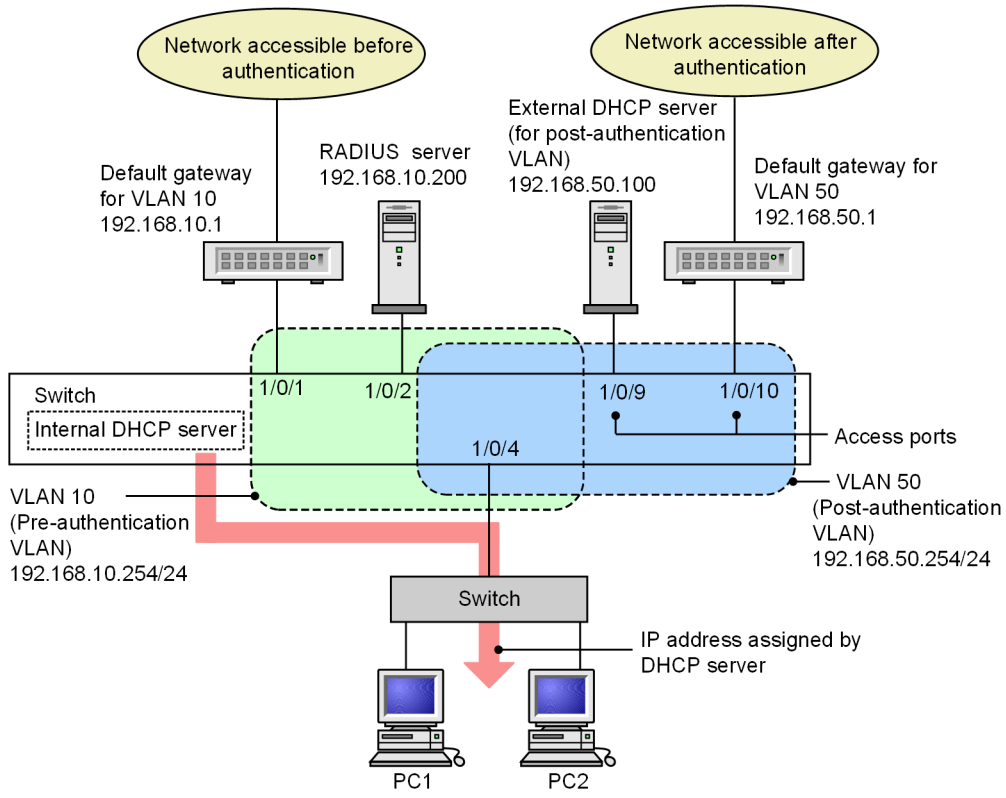
Starts Web authentication.

(2) Basic configuration for RADIUS authentication method

The figure below shows the basic configuration required to use RADIUS authentication method. Note that the terminal obtains its IP address from the internal DHCP server prior to authentication and from an external DHCP server after authentication.

This configuration includes putting a filter in place that prohibits communication between the pre-authentication VLAN and the post-authentication VLAN.

Figure 9-5: Basic configuration for RADIUS authentication method in dynamic VLAN mode



(a) Configuring an authentication port

Points to note

Configure the port to be used for Web authentication.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 10
(config-if)# web-authentication port
(config-if)# exit
```

Assigns a MAC VLAN and configures Web authentication at a port where terminals will be authenticated.

2.
```
(config)# interface range gigabitethernet 1/0/9-10
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 50
(config-if-range)# exit
```

Specifies the access port of the network accessed after authentication.

(b) Assigning IP addresses to VLAN interfaces

Points to note

Assign IP addresses to the pre-authentication and post-authentication VLANs.

Command examples

1.
```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit
```

   Assigns IP addresses to the pre-authentication VLAN and the post-authentication VLAN.

(c) Setting the authentication IPv4 access list

Points to note

Configure an authentication IPv4 access list that allows traffic from unauthenticated terminals to reach destinations outside the Switch.

Command examples

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit ip host 192.168.10.0 host 192.168.10.1
(config-ext-nacl)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# authentication ip access-group 100
(config-if)# authentication arp-relay
(config-if)# exit
```

   Configures an authentication IPv4 access list that allows unauthenticated terminals to send DHCP packets to the internal DHCP server and to access the default gateway of VLAN 10 (IP address 192.168.10.1). These commands also configure the Switch to forward ARP packets to external destinations.

(d) Prohibiting communication between VLANs

Points to note

Filter traffic between the pre-authentication and post-authentication VLANs.

Command examples

1.
```
(config)# ip access-list extended 110
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 10
```

```
(config-if)# ip access-group 110 in
(config-if)# exit
```

2.
```
(config)# ip access-list extended 150
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.50.100 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit udp host 192.168.50.100 any eq bootpc
(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 192.168.50.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 50
(config-if)# ip access-group 150 in
(config-if)# exit
```

   Configures the switch to block communication between the pre-authentication VLAN and the post-authentication VLAN.

(e) Configuring Web authentication

Points to note

Enable Web authentication by using configuration commands.

Command examples

1.
```
(config)# web-authentication ip address 10.10.10.1
```

   Sets the Web authentication IP address (IPv4 address).

2.
```
(config)# aaa authentication web-authentication default group radius
(config)# radius-server host 192.168.10.200 key "webauth"
```

   Specifies the IP address and RADIUS key used to access the RADIUS server to perform user authentication.

3.
```
(config)# web-authentication system-auth-control
```

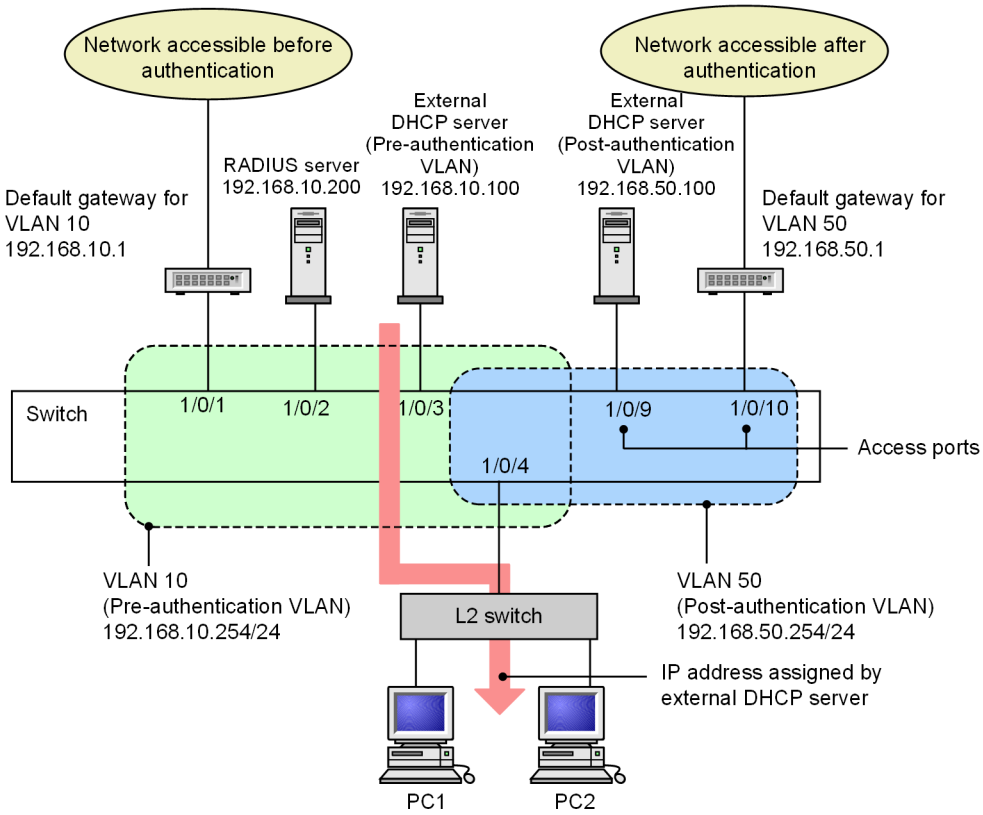
   Starts Web authentication.

(3) Configuration for RADIUS authentication method using an external DHCP server prior to authentication

The figure below describes the basic configuration required to use RADIUS authentication method in an environment where terminals obtain IP addresses from external DHCP servers before and after authentication.

This configuration includes putting a filter in place that prohibits communication between the pre-authentication VLAN and the post-authentication VLAN.

Figure 9-6: Configuration for RADIUS authentication method in dynamic VLAN mode using external DHCP servers



(a) Configuring an authentication port

Points to note

Configure the port to be used for Web authentication.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 10
(config-if)# web-authentication port
(config-if)# exit
```

Assigns a MAC VLAN and configures Web authentication at a port where terminals will be authenticated.

2.
```
(config)# interface range gigabitethernet 1/0/9-10
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 50
(config-if-range)# exit
```

Specifies the access port of the network accessed after authentication.

(b) Assigning IP addresses to VLAN interfaces

Points to note

Assign IP addresses to the pre-authentication and post-authentication VLANs.

Command examples

1.
```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit
```

Assigns IP addresses to the pre-authentication VLAN and the post-authentication VLAN.

(c) Setting the authentication IPv4 access list

Points to note

Configure an authentication IPv4 access list that allows traffic from unauthenticated terminals to reach destinations outside the Switch.

Command examples

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.100 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit ip host 192.168.10.0 host 192.168.10.1
(config-ext-nacl)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# authentication ip access-group 100
(config-if)# authentication arp-relay
(config-if)# exit
```

Configures an authentication IPv4 access list that allows unauthenticated terminals to send DHCP packets to the external DHCP server and to access the default gateway of VLAN 10 (IP address 192.168.10.1). These commands also configure the Switch to forward ARP packets to external destinations.

(d) Prohibiting communication between VLANs

Points to note

Filter traffic between the pre-authentication and post-authentication VLANs.

Command examples

1.
```
(config)# ip access-list extended 110
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit udp host 192.168.10.100 any eq bootpc
(config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 10
(config-if)# ip access-group 110 in
(config-if)# exit
```

2.
```
(config)# ip access-list extended 150
(config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.50.100 eq bootps
(config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit udp host 192.168.50.100 any eq bootpc
(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 192.168.50.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 50
(config-if)# ip access-group 150 in
(config-if)# exit
```

   Configures the switch to block communication between the pre-authentication VLAN and the post-authentication VLAN.

(e) Configuring Web authentication

Points to note

Enable Web authentication by using configuration commands.

Command examples

1.
```
(config)# web-authentication ip address 10.10.10.1
```

   Sets the Web authentication IP address (IPv4 address).

2.
```
(config)# aaa authentication web-authentication default group radius
(config)# radius-server host 192.168.10.200 key "webauth"
```

   Specifies the IP address and RADIUS key used to access the RADIUS server to perform user authentication.

3.
```
(config)# web-authentication system-auth-control
```

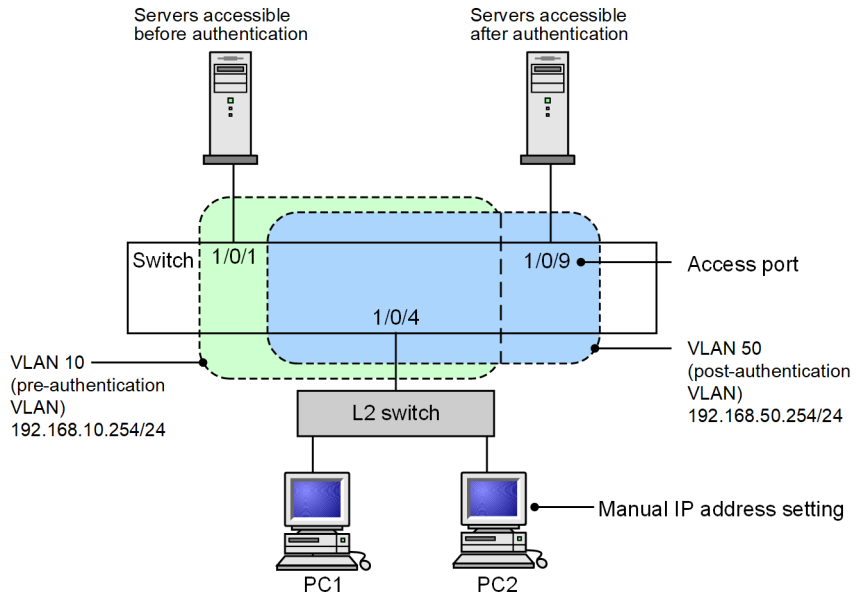
   Starts Web authentication.

9.1.4 Configuration for legacy mode

(1) Basic configuration for local authentication method

The figure below describes the basic configuration required to use local authentication method. In this case, you manually assign the pre-authentication and post-authentication IP addresses to the terminals (PC1 and PC2).

Figure 9-7: Example configuration for local authentication method



In this configuration, you configure Web authentication after you set up the pre-authentication and post-authentication VLANs and define the access lists. The access lists you define prohibit members of the pre-authentication VLAN from communicating with the post-authentication VLAN and permit communication from the post-authentication VLAN to the pre-authentication VLAN only by Web browser.

(a) Configuring an authentication port

Points to note

Configure the port to be used for Web authentication.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 50
(config-if)# switchport mac native vlan 10
(config-if)# exit
```

Specifies the pre-authentication VLAN and the post-authentication VLAN at a port where terminals will be authenticated.

2.
```
(config)# interface gigabitethernet 1/0/9
(config-if)# switchport mode access
(config-if)# switchport access vlan 50
(config-if)# exit
```

Specifies a post-authentication VLAN for the port which server users access after authentication is connected.

(b) Assigning IP addresses to VLAN interfaces

Points to note

Assign IP addresses to the pre-authentication and post-authentication VLANs.

Command examples

1.
```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit
```

   Assigns IP addresses to the pre-authentication VLAN and the post-authentication VLAN.

(c) Setting the access lists

Points to note

Configure the access lists for the post-authentication VLAN and the pre-authentication VLAN.

Command examples

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 10
(config-if)# ip access-group 100 in
(config-if)# exit
```

   Sets an access list that prohibits communication from the pre-authentication VLAN to the post-authentication VLAN.

2.
```
(config)# ip access-list extended 150
(config-ext-nacl)# permit tcp 192.168.50.0 0.0.0.255 host 192.168.10.254 eq http
(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 any
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 50
(config-if)# ip access-group 150 in
(config-if)# exit
```

   Sets an access list that permits access by Web browser from the post-authentication VLAN to the pre-authentication VLAN.

(d) Configuring Web authentication

Points to note

Enable Web authentication by using configuration commands.

Command examples

1.
```
(config)# web-authentication vlan 50
```

   Specifies the VLAN IDs of the post-authentication VLANs used for Web authentication.

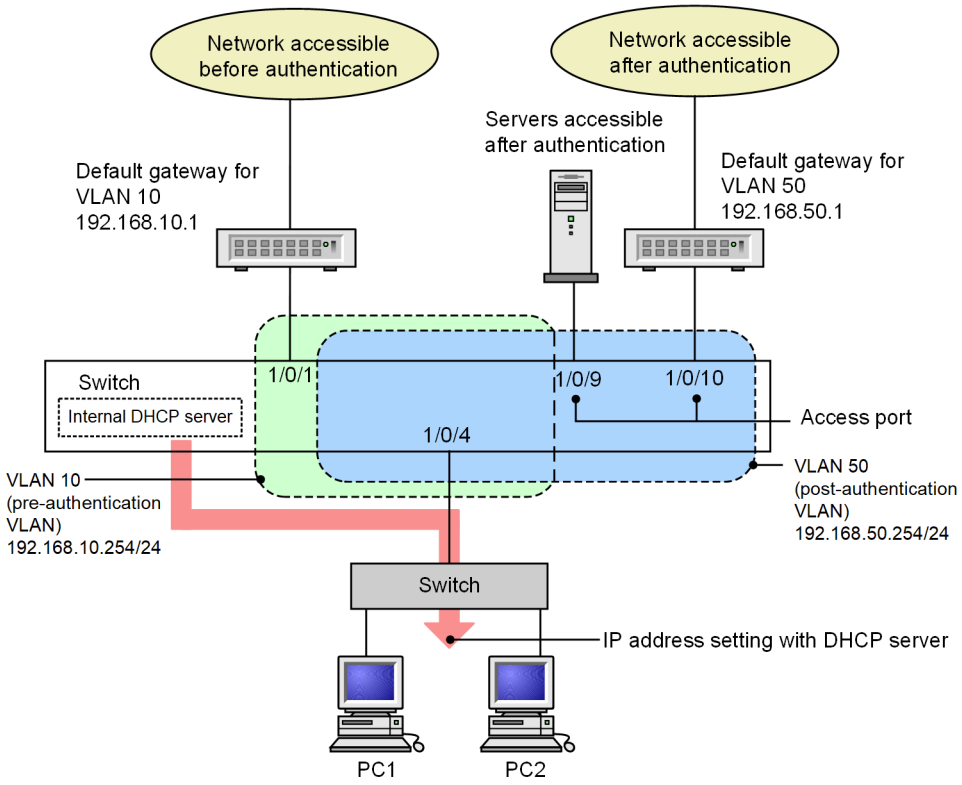
2.
```
(config)# web-authentication system-auth-control
```

Starts Web authentication.

(2) Configuration when using local authentication method and an internal DHCP server

The figure below describes an example configuration for Web authentication that uses local authentication method with the DHCP server built in to the switch. In this case, the DHCP server function built in to the Switch assigns IP addresses to the terminals (PC1 and PC2).

Figure 9-8: Example configuration for local authentication method using internal DHCP



In this configuration, you configure Web authentication after you have set up the pre-authentication and post-authentication VLANs, defined the access lists, and configured the DHCP server. The access lists you define prohibit members of the pre-authentication VLAN from communicating with the post-authentication VLAN and permit communication from the post-authentication VLAN to the pre-authentication VLAN only by Web browser.

(a) Configuring an authentication port

Points to note

Configure the port to be used for Web authentication.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 50
(config-if)# switchport mac native vlan 10
(config-if)# exit
```

Specifies the pre-authentication VLAN and the post-authentication VLAN at a port where terminals will be authenticated.

2.
```
(config)# interface range gigabitethernet 1/0/9-10
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 50
(config-if-range)# exit
```

Specifies a post-authentication VLAN for the port which server users access after authentication is connected.

(b) Assigning IP addresses to VLAN interfaces

Points to note

Assign IP addresses to the pre-authentication and post-authentication VLANs.

Command examples

1.
```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit
```

Assigns IP addresses to the pre-authentication VLAN and the post-authentication VLAN.

(c) Setting the access lists

Points to note

Configure the access lists for the post-authentication VLAN and the pre-authentication VLAN.

Command examples

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 10
(config-if)# ip access-group 100 in
(config-if)# exit
```

Sets an access list that prohibits communication from the pre-authentication VLAN to the post-authentication VLAN.

2.
```
(config)# ip access-list extended 150
(config-ext-nacl)# permit tcp 192.168.50.0 0.0.0.255 host 192.168.10.254 eq http
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.10.254
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.50.254
(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 any
```

```
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 50
(config-if)# ip access-group 150 in
(config-if)# exit
```

Sets an access list that permits the switch to only relay traffic generated by a Web browser from the post-authentication VLAN to the pre-authentication VLAN.

(d) DHCP+ server setup

Points to note

Configure the DHCP server to distribute IP addresses to terminals.

Command examples

1.
```
(config)# service dhcp vlan 10
(config)# ip dhcp excluded-address 192.168.10.1
(config)# ip dhcp excluded-address 192.168.10.254
(config)# ip dhcp pool POOL10
(dhcp-config)# network 192.168.10.0/24
(dhcp-config)# lease 0 0 1
(dhcp-config)# default-router 192.168.10.1
(dhcp-config)# exit
```

Performs DHCP server configuration for the pre-authentication VLAN. These commands configure the allocation of IP addresses to terminals seeking authentication and define 192.168.10.1 as the IP address of the default router.

2.
```
(config)# service dhcp vlan 50
(config)# ip dhcp excluded-address 192.168.50.1
(config)# ip dhcp excluded-address 192.168.50.254
(config)# ip dhcp pool POOL50
(dhcp-config)# network 192.168.50.0/24
(dhcp-config)# lease 0 0 1
(dhcp-config)# default-router 192.168.50.1
(dhcp-config)# exit
```

Performs DHCP server configuration for the post-authentication VLAN. These commands configure the allocation of IP addresses to authenticated terminals and define 192.168.50.1 as the IP address of the default router.

(e) Configuring Web authentication

Points to note

Enable Web authentication by using configuration commands.

Command examples

1.
```
(config)# web-authentication vlan 50
```

Specifies the VLAN IDs of the post-authentication VLANs used for Web authentication.

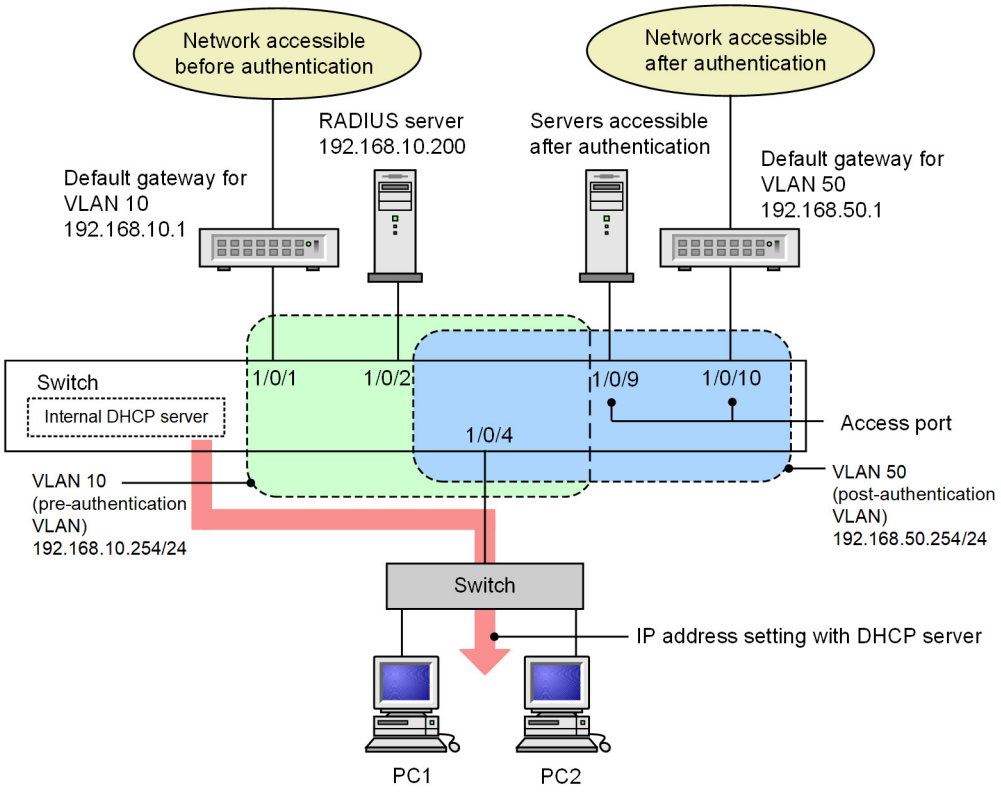
2. `(config)# web-authentication system-auth-control`

Starts Web authentication.

(3) Configuration when using RADIUS authentication method and an internal DHCP server

The figure below describes an example configuration for Web authentication that uses RADIUS authentication method with the DHCP server built in to the switch. In this case, the DHCP server function built in to the Switch assigns IP addresses to the terminals (PC1 and PC2).

Figure 9-9: Example configuration for RADIUS authentication method using internal DHCP



In this configuration, you configure Web authentication after you have set up the pre-authentication and post-authentication VLANs, defined the access lists, and configured the DHCP server. The access lists you define prohibit members of the pre-authentication VLAN from communicating with the post-authentication VLAN and permit communication from the post-authentication VLAN to the pre-authentication VLAN only by Web browser.

(a) Configuring an authentication port

Points to note

Configure the port to be used for Web authentication.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 50
(config-if)# switchport mac native vlan 10
(config-if)# exit
```

Specifies the pre-authentication VLAN and the post-authentication VLAN at a port where terminals will be authenticated.

2.
```
(config)# interface range gigabitethernet 1/0/9-10
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 50
(config-if-range)# exit
```

Specifies a post-authentication VLAN for the port which server users access after authentication is connected.

(b) Assigning IP addresses to VLAN interfaces

Points to note

Assign IP addresses to the pre-authentication and post-authentication VLANs.

Command examples

1.
```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit
```

Assigns IP addresses to the pre-authentication VLAN and the post-authentication VLAN.

(c) Setting the access lists

Points to note

Configure the access lists for the post-authentication VLAN and the pre-authentication VLAN.

Command examples

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 10
(config-if)# ip access-group 100 in
(config-if)# exit
```

Sets an access list that prohibits communication from the pre-authentication VLAN to the post-authentication VLAN.

2.
```
(config)# ip access-list extended 150
(config-ext-nacl)# permit tcp 192.168.50.0 0.0.0.255 host 192.168.10.254 eq http
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.10.254
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.50.254
```

```
(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 any
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 50
(config-if)# ip access-group 150 in
(config-if)# exit
```

Sets an access list that permits the switch to only relay traffic generated by a Web browser from the post-authentication VLAN to the pre-authentication VLAN.

(d) DHCP+ server setup

Points to note

Configure the DHCP server to distribute IP addresses to terminals.

Command examples

1.
```
(config)# service dhcp vlan 10
(config)# ip dhcp excluded-address 192.168.10.1
(config)# ip dhcp excluded-address 192.168.10.254
(config)# ip dhcp pool POOL10
(dhcp-config)# network 192.168.10.0/24
(dhcp-config)# lease 0 0 1
(dhcp-config)# default-router 192.168.10.1
(dhcp-config)# exit
```

Performs DHCP server configuration for the pre-authentication VLAN. These commands configure the allocation of IP addresses to terminals seeking authentication and define 192.168.10.1 as the IP address of the default router.

2.
```
(config)# service dhcp vlan 50
(config)# ip dhcp excluded-address 192.168.50.1
(config)# ip dhcp excluded-address 192.168.50.254
(config)# ip dhcp pool POOL50
(dhcp-config)# network 192.168.50.0/24
(dhcp-config)# lease 0 0 1
(dhcp-config)# default-router 192.168.50.1
(dhcp-config)# exit
```

Performs DHCP server configuration for the post-authentication VLAN. These commands configure the allocation of IP addresses to authenticated terminals and define 192.168.50.1 as the IP address of the default router.

(e) Configuring Web authentication

Points to note

Enable Web authentication by using configuration commands.

Command examples

1. `(config)# web-authentication vlan 50`

   Specifies the VLAN IDs of the post-authentication VLANs used for Web authentication.

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

   `(config)# radius-server host 192.168.10.200 key "webauth"`

   Specifies the IP address and RADIUS key used to access the RADIUS server to perform user authentication.

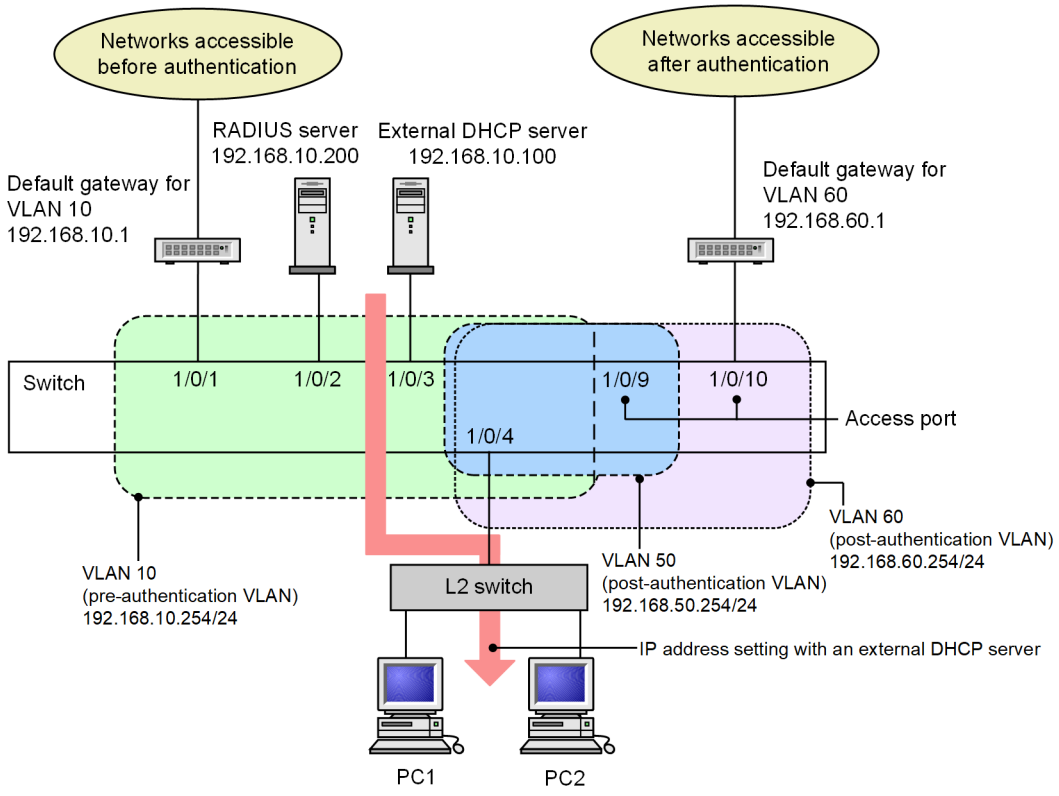
3. `(config)# web-authentication system-auth-control`

   Starts Web authentication.

(4) Configuration when using RADIUS authentication method, an external DHCP server, and multiple post-authentication VLANs

The figure below describes an example configuration for Web authentication that uses RADIUS authentication method and an external DHCP server in an environment where multiple post-authentication VLANs are configured. In this case, the external DHCP server assigns IP addresses to the terminals (PC1 and PC2).

Figure 9-10: Example configuration for RADIUS authentication method using an external DHCP server with multiple post-authentication VLANs



In this configuration, you configure Web authentication after you set up the pre-authentication and post-authentication VLANs and define the access lists. The access lists you define prohibit members of the pre-authentication VLAN from communicating with the post-authentication VLAN and permit communication from the post-authentication VLAN to the pre-authentication VLAN only by Web browser.

The access lists you define also prohibit communication between post-authentication VLANs.

(a) Configuring an authentication port

Points to note

Configure the port to be used for Web authentication.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 50,60
(config-if)# switchport mac native vlan 10
(config-if)# exit
```

Specifies the pre-authentication VLAN and the post-authentication VLAN at a port where terminals will be authenticated.

2.
```
(config)# interface gigabitethernet 1/0/9
(config-if)# switchport mode access
(config-if)# switchport access vlan 50
(config-if)# exit
```

Specifies a post-authentication VLAN for the port which server users access after authentication is connected.

3.
```
(config)# interface gigabitethernet 1/0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 60
(config-if)# exit
```

Specifies a post-authentication VLAN for the port which server users access after authentication is connected.

(b) Assigning IP addresses to VLAN interfaces

Points to note

Assign IP addresses to the pre-authentication and post-authentication VLANs.

Command examples

1.
```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 60
(config-if)# ip address 192.168.60.254 255.255.255.0
(config-if)# exit
```

Assigns IP addresses to the pre-authentication VLAN and the post-authentication VLAN.

(c) Setting the access lists

Points to note

Configure the access lists for the post-authentication VLAN and the pre-authentication VLAN.

Command examples

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 10
(config-if)# ip access-group 100 in
(config-if)# exit
```

   Sets an access list that prohibits communication from the pre-authentication VLAN to the post-authentication VLAN.

2.
```
(config)# ip access-list extended 150
(config-ext-nacl)# permit tcp 192.168.50.0 0.0.0.255 host 192.168.10.254 eq http
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.10.254
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.50.254
(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 any
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 50
(config-if)# ip access-group 150 in
(config-if)# exit
```

   Sets an access list that permits communication by Web browser from the post authentication VLAN (VLAN ID 50) to the pre-authentication VLAN, and prohibits all access to the other post-authentication VLAN (VLAN ID 60).

3.
```
(config)# ip access-list extended 160
(config-ext-nacl)# permit tcp 192.168.60.0 0.0.0.255 host 192.168.10.254 eq http
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.10.254
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.60.254
(config-ext-nacl)# permit ip 192.168.60.0 0.0.0.255 any
(config-ext-nacl)# deny ip any any
(config-ext-nacl)# exit
(config)# interface vlan 60
(config-if)# ip access-group 160 in
(config-if)# exit
```

Sets an access list that permits communication by Web browser from the post authentication VLAN (VLAN ID 60) to the pre-authentication VLAN, and prohibits all access to the other post-authentication VLAN (VLAN ID 50).

(d) Setting the DHCP relay agent

Points to note

Configure the DHCP relay agent for IP address distribution to terminals.

Command examples

1.
```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# ip helper-address 192.168.10.100
(config-if)# exit
```

Configures the DHCP relay agent for the pre-authentication VLAN.

2.
```
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# ip helper-address 192.168.10.100
(config-if)# exit
```

Configures the DHCP relay agent for the post-authentication VLAN (VLAN ID 50).

3.
```
(config)# interface vlan 60
(config-if)# ip address 192.168.60.254 255.255.255.0
(config-if)# ip helper-address 192.168.10.100
(config-if)# exit
```

Configures the DHCP relay agent for the post-authentication VLAN (VLAN ID 60).

(e) Configuring Web authentication

Points to note

Enable Web authentication by using configuration commands.

Command examples

1.
```
(config)# web-authentication vlan 50
(config)# web-authentication vlan 60
```

Specifies the VLAN IDs of the post-authentication VLANs used for Web authentication.

2.
```
(config)# aaa authentication web-authentication default group radius
(config)# radius-server host 192.168.10.200 key "webauth"
```

Specifies the IP address and RADIUS key used to access the RADIUS server to perform user authentication.

3.
```
(config)# web-authentication system-auth-control
```

Starts Web authentication.

9.1.5 Configuring Web authentication parameters

This section describes how to set the parameters for Web authentication.

(1) Setting the maximum authentication time

Points to note

Set the length of time after which authenticated terminals are forcibly logged out.

Command examples

1. `(config)# web-authentication max-timer 60`

   Configures the switch to forcibly log out terminals after 60 minutes.

(2) Setting the maximum number of authenticated users (fixed VLAN mode)

Points to note

Set the maximum number of Web-authenticated users allowed in fixed VLAN mode.

Command examples

1. `(config)# web-authentication static-vlan max-user 100`

   Specifies 100 as the maximum number of Web-authenticated users allowed in fixed VLAN mode.

(3) Setting the maximum number of authenticated users (dynamic VLAN mode and legacy mode)

Points to note

Set the maximum number of Web-authenticated users allowed in dynamic VLAN mode or legacy mode.

Command examples

1. `(config)# web-authentication max-user 5`

   Specifies a maximum of five Web-authenticated users.

(4) RADIUS+ server setup

Points to note

Configure the RADIUS server used to implement RADIUS authentication method.

Command examples

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

   Specifies that user authentication takes place using a RADIUS server.

Notes

If the total wait time for each RADIUS server as specified by the "radius-server" command is longer than 60 seconds, authentication might fail while the switch is still waiting for a response from the RADIUS servers. Because the parameters set by the "radius-server" command apply universally to login authentication, command authorization, and IEEE 802.1X authentication, take care when setting the wait time.

(5) Configuring accounting

Points to note

Enable the collection of accounting information for Web authentication.

Command examples

1. `(config)# aaa accounting web-authentication default start-stop group radius`

   Enables the collection of accounting information by the RADIUS server.

(6) Setting the Web authentication IP address (fixed VLAN mode and dynamic VLAN mode)

Points to note

Set the Web authentication IP address.

Command examples

1. `(config)# web-authentication ip address 10.10.10.1`

   Sets the Web authentication IP address (10.10.10.1).

Notes

- After setting the access ports, use the "restart web-authentication web-server" operation command to restart the Web server. Users in the process of authentication will need to log in again.
- In legacy mode (in an environment without the "web-authentication port" command configured), if you execute the "web-authentication port" command after you specify this command, you must then restart the Web server by using the "restart web-authentication web-server" operation command.

(7) Setting the Web authentication IP address and FQDN (fixed VLAN mode and dynamic VLAN mode)

Points to note

Specify the Web authentication IP address and associated FQDN.

Command examples

1. `(config)# web-authentication ip address 10.10.10.1 fqdn host.example.com`

   Specifies the Web authentication IP address (10.10.10.1) and FQDN (host.example.com).

Notes

- After setting the access ports, use the "restart web-authentication web-server" operation command to restart the Web server. Users in the process of authentication will need to log in again.
- In legacy mode (in an environment without the "web-authentication port" command configured), if you execute the "web-authentication port" command after you specify this command, you must then restart the Web server by using the "restart web-authentication web-server" operation command.

(8) Disabling URL redirection function (fixed VLAN mode and dynamic VLAN mode)

Points to note

Disable the URL redirection function for Web authentication.

Command examples

1. `(config)# no web-authentication redirect enable`

   Disables the URL redirection function for Web authentication.

Notes

After setting the access ports, use the "restart web-authentication web-server" operation command to restart the Web server. Users in the process of authentication will need to log in again.

(9) Setting the login protocol for login operations subject to URL redirection function (fixed VLAN mode and dynamic VLAN mode)

Points to note

Specify the protocol used for login operations that are subject to URL redirection function.

Command examples

1. `(config)# web-authentication redirect-mode https`

   Uses the HTTPS protocol for Web authentication via URL redirection function.

Notes

After setting the access ports, use the "restart web-authentication web-server" operation command to restart the Web server. Users in the process of authentication will need to log in again.

(10) Configuring output to the syslog server

Points to note

Configure the Switch to output authentication results and action logs to the syslog server.

Command examples

1. `(config)# web-authentication logging enable`

   `(config)# logging event-kind aut`

   Configures the Switch to output Web authentication results and action logs to the syslog server.

(11) Configuring the connection monitoring function (fixed VLAN mode)

Points to note

Configure the connection monitoring function that monitors the status of authenticated terminals.

Command examples

1. `(config)# web-authentication logout polling enable`

   Enables the connection monitoring function.

2. `(config)# web-authentication logout polling interval 300`

   Specifies a 300-second interval between transmissions of performance monitoring packets.

3. `(config)# web-authentication logout polling retry-interval 10`

   Specifies a resending interval of 10 seconds for performance monitoring packets.

4. `(config)# web-authentication logout polling count 5`

   Specifies a retry count of 5 for performance monitoring packets.

(12) Disabling the connection monitoring function (fixed VLAN mode)

Points to note

Disable the connection monitoring function that monitors the status of authenticated terminals.

Command examples

1. `(config)# no web-authentication logout polling enable`

   Disables the connection monitoring function.

(13) Assigning a Web server access port

Points to note

Set the service port numbers for the Web server used in Web authentication. You can use these parameters to provide access to the Web server via a port other than the default (80 for HTTP and 443 for HTTPS).

In an environment running OAN, use this procedure to set the service port numbers used by OAN (832 and 9698). You cannot use the OAN service ports to perform Web authentication login and logout operations.

Command examples

1. `(config)# web-authentication web-port http 8080`

   Specifies port 8080 as an alternate to port 80 for accessing the Web server via HTTP.

2. `(config)# web-authentication web-port https 8443`

   Specifies port 8443 as an alternate to port 443 for accessing the Web server via HTTPS.

Notes

After setting the access ports, use the "restart web-authentication web-server" operation command to restart the Web server. Users in the process of authentication will need to log in again.

(14) Setting the URL accessed after 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/"`

   Directs to http://www.example.com/ after successful authentication.

9.1.6 Configuring authentication-exempted ports and terminals

This section describes how to configure Web authentication-exempted ports and terminals.

(1) Configuring a port as an authentication-exempted port in fixed VLAN mode

Use the following procedure to configure a port to be permitted access in fixed VLAN mode without the need for authentication.

Points to note

Do not designate an authentication-exempted port as an authentication port.

Command examples

1.
```
(config)# vlan 10
(config-vlan)# state active
(config-vlan)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# web-authentication port
(config-if)# exit
(config)# interface gigabitethernet 1/0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit
```

   Specifies port 1/0/4, which is assigned to VLAN ID 10 in fixed VLAN mode, as an authentication port. This procedure then configures port 1/0/10 to be permitted access without the need for authentication.

(2) Configuring a terminal as an authentication-exempted terminal in fixed VLAN mode

Use the following procedure to specify the MAC address of a terminal to be permitted access in fixed VLAN mode without the need for authentication.

Points to note

Register the MAC address of an authentication-exempted terminal in the MAC address table.

Command examples

1.
```
(config)# vlan 10
(config-vlan)# exit
```

```
(config)# mac-address-table static 0012.e212.3456 vlan 10 interface gigabitethernet 1/0/10
```

Specifies the MAC address of a terminal to be permitted access to port 1/0/10 with VLAN ID 10, without the need for authentication.

(3) Configuring a port as an authentication-exempted port in dynamic VLAN mode

Uses the following procedure to configure a port to be permitted access in dynamic VLAN mode without the need for authentication.

Points to note

Designate an authentication-exempted port as an access port, but not as an authentication port.

Command examples

1.
```
(config)# vlan 50 mac-based
(config-vlan)# state active
(config-vlan)# exit
(config)# interface gigabitethernet 1/0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 50
(config-if)# exit
```

Permits access by unauthenticated terminals to MAC VLAN ID 50 from port 1/0/10.

(4) Configuring a terminal as an authentication-exempted terminal in dynamic VLAN mode

Use the following procedure to specify the MAC address of a terminal to be permitted access in dynamic VLAN mode without the need for authentication.

Points to note

Register the MAC address of an authentication-exempted terminal in a MAC VLAN and a MAC address table.

Command examples

1.
```
(config)# vlan 50 mac-based
(config-vlan)# mac-address 0012.e212.3456
(config-vlan)# exit
(config)# mac-address-table static 0012.e212.3456 vlan 50 interface gigabitethernet 1/0/10
```

Specifies the MAC address of a terminal to be permitted access to MAC VLAN 50 through port 1/0/10 without the need for authentication.

(5) Configuring a port as an authentication-exempted port in legacy mode

Use the commands below to configure a port to be permitted access in legacy mode without the need for authentication.

Points to note

Designate an authentication-exempted port as an access port.

Command examples

1.
```
(config)# vlan 50 mac-based
(config-vlan)# state active
(config-vlan)# exit
```

```
(config)# interface gigabitethernet 1/0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 50
(config-if)# exit
```

Permits access by unauthenticated terminals to MAC VLAN ID 50 from port 1/0/10.

(6) Configuring a terminal as an authentication-exempted terminal in legacy mode

Use the commands below to specify the MAC address of a terminal to be permitted access in legacy mode without the need for authentication.

Points to note

Register the MAC address of an authentication-exempted terminal in a MAC VLAN.

Command examples

1.
```
(config)# vlan 50 mac-based
(config-vlan)# mac-address 0012.e212.3456
(config-vlan)# exit
```

Specifies the MAC address of a terminal to be permitted access to MAC VLAN ID 50 without the need for authentication.

9.2 Operation

9.2.1 List of operation commands

The following table describes the list of operation commands used in Web authentication.

Table 9-2: List of operation commands

Command name	Description
set web-authentication user	Adds a user ID for a new Web-authenticated user.
set web-authentication passwd	Changes the password of a registered user.
set web-authentication vlan	Changes the VLAN ID assigned to a registered user.
remove web-authentication user	Deletes a registered user ID.
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	Shows 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 login	Shows accounting log information for authenticated accounts.
show web-authentication	Shows the configuration for Web authentication.
show web-authentication statistics	Shows statistics for Web authentication.
clear web-authentication statistics	Clears the statistics.
show web-authentication logging	Shows the action logs related to Web authentication.
clear web-authentication logging	Clears the action logs related to Web authentication.
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	Shows the file names and sizes of the Web authentication page files, as well as the date and time of their registration.
clear web-authentication dead-interval-timer	Directs the switch to return to accessing the first RADIUS server, having moved on to another RADIUS server as a result of the dead interval function.
set web-authentication ssl-crt	Registers the server certificate and private key for SSL communication.
clear web-authentication ssl-crt	Deletes the registered SSL certificate and private key.
show web-authentication ssl-crt	Displays the registered SSL certificate and private key.
restart web-authentication	Restarts the Web authentication software.
dump protocols web-authentication	Creates a dump file of information related to Web authentication.

9.2.2 Displaying the Web authentication configuration

You can use the "show web-authentication" command to display the Web authentication configuration.

(1) Configuration information displayed for RADIUS authentication in fixed VLAN mode

Figure 9-11: Web authentication configuration information (RADIUS authentication in fixed VLAN mode)

```
# show web-authentication
Date 20XX/10/17 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Static-VLAN
   Authentic-method : RADIUS        Accounting-state : disable
   Dead-interval    : 10
          Max-timer : 60                  Max-user  : 256
         VLAN Count : -                 Auto-logout : -
   Syslog-send      : enable
   Alive-detection  : enable
              timer : 60    interval-timer : 3     count : 3
   URL-redirect     : enable    Protocol : http
   Jump-URL         : http://www.example.com/
   Web-IP-address   : 10.10.10.1
   FQDN             : aaa.example.com
   Web-port         : http  : 80, 8080       https : 443, 8443
   ARP-relay Port   : 0/1-2
   Force-Authorized : disable
   Auth-max-user    : 1024

         Port          :    0/1
         VLAN ID       :    5,10,15
         Access-list-No:    100
         Max-user      :    64

         Port          :    0/2
         VLAN ID       :    15-16
         Access-list-No:    100
         Max-user      :    64
```

(2) Configuration information displayed for local authentication in dynamic VLAN mode

Figure 9-12: Web authentication configuration information (local authentication in dynamic VLAN mode)

```
# show web-authentication
Date 20XX/10/17 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Dynamic-VLAN
   Authentic-method : Local         Accounting-state : disable
   Dead-interval    : 10
          Max-timer : 60                   Max-user : 256
         VLAN Count : -                 Auto-logout : disable
   Syslog-send      : enable
   URL-redirect     : enable    Protocol : http
   Jump-URL         : http://www.example.com/
   Web-IP-address   : 192.168.1.1
   FQDN             : aaa.example.com
   Web-port         : http  : 80, 8080       https : 443, 8443
   ARP-relay Port   : 0/10,12
   Force-Authorized : enable
   Auth-max-user    : 1024

         Port          :    0/10
         VLAN ID       :    1000,1500
         Native VLAN   :    10
         Forceauth VLAN:    1000
         Access-list-No:    100
         Max-user      :    64

         Port          :    0/12
         VLAN ID       :    1000,1500
         Native VLAN   :    10
```

```
         Forceauth VLAN:    1000
         Access-list-No:    100
         Max-user      :    64
```

(3) Configuration information displayed for RADIUS authentication in dynamic VLAN mode

Figure 9-13: Web authentication configuration information (RADIUS authentication in dynamic VLAN mode)

```
# show web-authentication
Date 20XX/10/17 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Dynamic-VLAN
   Authentic-method : RADIUS        Accounting-state : enable
   Dead-interval    : 10
     Max-timer      : 60                  Max-user  : 256
     VLAN Count     : -                 Auto-logout : disable
   Syslog-send      : enable
   URL-redirect     : enable    Protocol : http
   Jump-URL         : http://www.example.com/
   Web-IP-address   : 192.168.1.1
   FQDN             : aaa.example.com
   Web-port         : http  : 80, 8080       https : 443, 8443
   ARP-relay Port   : 0/10,12
   Force-Authorized : enable
   Auth-max-user    : 1024

         Port          :    0/10
         VLAN ID       :    1000,1500
         Native VLAN   :    10
         Forceauth VLAN:    1000
         Access-list-No:    100
         Max-user      :    256

         Port          :    0/12
         VLAN ID       :    1000,1500
         Native VLAN   :    10
         Forceauth VLAN:    -
         Access-list-No:    100
         Max-user      :    256
```

(4) Configuration information displayed for local authentication in legacy mode with VLANs registered

Figure 9-14: Web authentication configuration information (local authentication)

```
# show web-authentication
Date 20XX/10/17 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Legacy
   Authentic-method : Local         Accounting-state : disable
          Max-timer : 60                  Max-user  : 256
         VLAN Count : 16                Auto-logout : disable
    Syslog-send     : enable
    Jump-URL        : http://www.example.com/
    Web-port        : http  : 80             https : 443

VLAN Information:
            VLAN ID :    5,10,15,20,25,30,35,40,1000-1007
```

(5) Configuration information displayed for RADIUS authentication in legacy mode with VLANs registered

Figure 9-15: Web authentication configuration information (RADIUS authentication)

```
# show web-authentication
Date 20XX/10/17 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Legacy
   Authentic-method : RADIUS        Accounting-state : disable
          Max-timer : 60                  Max-user  : 256
         VLAN Count : 16                Auto-logout : disable
   Syslog-send      : enable
   Jump-URL         : http://www.example.com/
   Web-port         : http  : 80             https : 443
```

```
VLAN Information:
      VLAN ID :    5,10,15,20,25,30,35,40,1000-1007
```

9.2.3 Displaying the status of Web authentication

You can use the "show web-authentication statistics" command to display the status of Web authentication and the status of communication with the RADIUS server.

Figure 9-16: Displaying Web authentication status information

```
# show web-authentication statistics
Date 20XX/10/17 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :         100
  Authentication Current Count :          10
  Authentication Error Total   :          30
  Force Authorized Count       :          10
RADIUS web-authentication Information:
[RADIUS frames]
           TxTotal   :        10  TxAccReq  :        10  TxError   :         0
           RxTotal   :        30  RxAccAccpt:        10  RxAccRejct:        10
                                  RxAccChllg:        10  RxInvalid :         0
Account web-authentication Information:
[Account frames]
           TxTotal   :        10  TxAccReq  :        10  TxError   :         0
           RxTotal   :        20  RxAccResp :        10  RxInvalid :         0
Port Information
  Port     User-count
   0/10       5/ 256
   0/12       5/1024
```

9.2.4 Displaying the status of Web authentication sessions

You can use the "show web-authentication login" command to display the authentication status of users logged in using Web authentication.

(1) Information displayed in fixed VLAN mode

Figure 9-17: Displaying the status of Web authentication sessions (fixed VLAN mode)

```
# show web-authentication login
Date 20XX/10/17 10:52:49 UTC
Total user counts:2
F Username
  VLAN    MAC address      Port  IP address
  Login time               Limit time
  USER00123456789
     3    0012.e200.9166   0/5   192.168.0.1
  20XX/10/17 09:58:04 UTC  00:10:20
* USER01
  4094    0012.e268.7527   0/6   192.168.1.10
  20XX/10/17 10:10:23 UTC  00:20:35
```

(2) Information displayed in dynamic VLAN mode

Figure 9-18: Displaying the status of Web authentication sessions (dynamic VLAN mode)

```
# show web-authentication login
Date 20XX/10/17 10:52:49 UTC
Total user counts:2
F Username
  VLAN    MAC address      Login time               Limit time
  USER00123456789
     3    0012.e200.9166   20XX/10/17 09:58:04 UTC  00:10:20
* USER01
  4094    0012.e268.7527   20XX/10/17 10:10:23 UTC  00:20:35
```

(3) Information displayed in legacy mode

Figure 9-19: Displaying status information for Web-authenticated users (legacy mode)

```
# show web-authentication login
Date 20XX/10/17 10:52:49 UTC
Total user counts:2
```

```
Username
VLAN    MAC address      Login time               Limit time
USER00123456789
   3    0012.e200.9166   20XX/10/17 09:58:04 UTC  00:10:20
USER01
4094    0012.e268.7527   20XX/10/17 10:10:23 UTC  00:20:35
```

9.2.5 Creating an internal Web authentication DB

After you set up the environment for the Web authentication system and complete the configuration process, the next step is to create the internal Web authentication DB. This section also describes how to alter the existing user information in the internal Web authentication DB.

(1) Registering users

Use the "set web-authentication user" command to register a user ID, password, and VLAN ID for each user of Web authentication. The following example registers user information for five users (USER01 to USER05):

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

The following describes how to change the password or VLAN ID of a registered user and how to delete a user from the database.

(a) Changing passwords

Command input

```
# set web-authentication passwd USER01 PAS0101 PPP4321
```

Changes the password of USER01 from PAS0101 to PPP4321.

```
# set web-authentication passwd USER02 PAS0200 BBB1234
```

Changes the password of USER02 from PAS0200 to BBB1234.

(b) Changing VLAN IDs

Command input

```
# set web-authentication vlan BBB1234 200
```

Changes the VLAN ID of user BBB1234 to 200.

(c) Deleting users

Command input

```
# remove web-authentication user PPP4321
```

Deletes user PPPP4321.

(3) Applying changes to the internal Web authentication DB

The example shows a command applying the changes you made using the "set web-authentication" and "remove web-authentication" commands to the internal Web authentication DB.

Command input

```
# commit web-authentication
```

9.2.6 Backing up the internal Web authentication DB

This section shows 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

Use the "store web-authentication" command to back up the contents of the internal Web authentication DB to a file (named backupfile in the example below).

Command input

```
# store web-authentication backupfile
Backup web-authentication user data.  Are you sure? (y/n): y
#
```

(2) Restoring the internal Web authentication DB

Use the "load web-authentication" command to re-create the internal Web authentication DB from the contents of the backup file (named backupfile in the example below).

Command input

```
# load web-authentication backupfile
Restore web-authentication user data.  Are you sure? (y/n): y
#
```

9.2.7 Registering Web authentication pages

To register pages for use in the Web authentication process:

1. Using a PC or other external device, create the HTML pages to be used as the Web authentication pages.
2. Log in to the Switch, and in the current directory, create a directory for storing the Web authentication pages you created.
3. Use a file transfer protocol or a memory card to place the Web authentication page files in the directory you created in step 2.
4. Execute the "set web-authentication html-files" command to register the Web authentication pages.

Figure 9-20: Registering Web authentication pages

```
# mkdir docs…1

# set web-authentication html-files docs
Would you wish to install new html-files ? (y/n):y
executing...
Install complete.
#
```

1.This process creates the directory docs, and places the files to be registered in that directory.

9.2.8 Deleting registered Web authentication pages

Use the "clear web-authentication html-files" command to delete the Web authentication pages you registered using the "set web-authentication html-files" command.

Figure 9-21: Deleting Web authentication pages

```
# clear web-authentication html-files
Would you wish to clear registered html-files and initialize? (y/n):y
Clear complete.
#
```

9.2.9 Displaying information about the Web authentication pages

To display information about the Web authentication pages you registered, use the "show web-authentication html-files" command.

Figure 9-22: Displaying information about Web authentication pages

```
# show web-authentication html-files
Date 20XX/04/15 10:00:10 UTC
TOTAL SIZE      :       62976
-------------------------------------------------
                        SIZE         DATE
login.html      :        2049      20XX/04/10 14:05
loginProcess.html        2002      20XX/04/10 14:05
loginOK.html    :        1046      20XX/04/10 14:05
loginNG.html    :         985      20XX/04/10 14:05
logout.html     :         843      20XX/04/10 14:05
logoutOK.html   :         856      20XX/04/10 14:05
logoutNG.html   :         892      20XX/04/10 14:05
webauth.msg     :         104      20XX/04/10 14:05
favicon.ico     :         199      20XX/04/10 14:05
the other files :       54000      20XX/04/10 14:05
#
```

9.2.10 Restoring access to the first RADIUS server after intervention by the dead interval function

If the first RADIUS server becomes unresponsive, the dead interval function causes the switch to start using the second or later RADIUS server. In this case, you can direct the switch to resume use of the first RADIUS server before the time specified by the "authentication radius-server dead-interval" configuration command has elapsed by executing the "clear web-authentication dead-interval-timer" command.

Figure 9-23: Restoring access to the first RADIUS server

```
# clear web-authentication dead-interval-timer
#
```

9.3 Procedure for creating Web authentication pages

The following are the pages you can replace by using the Web authentication page replacement function, 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 file in HTML format.

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, see "9.3.1 Login page (login.html)". For details about the logout page, see "9.3.2 Logout page: logout.html".

You can replace the authentication error messages listed in "Table 8-6: Authentication error messages and their causes". The file names that can be used are as follows: For details about how to create this file, see "9.3.3 Authentication error message file (file name: 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)

Notes

Make sure that the file names you assign to your replacement pages and authentication error messages match the file names given in this section.

9.3.1 Login page (login.html)

This page prompts a client to log in by entering a user ID and password.

(1) Condition for setting

You must include the code listed in the following table when creating an HTML file to serve as the login page.

Table 9-3: Code required in login page

Code	Meaning
<form name="Login" method="post" action="/cgi-bin/Log-in.cgi"></form>	Initiates a Web authentication login process. Do not modify this code.
<input type="text" name="uid" size="40" maxlength="32" autocomplete="OFF" />	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 six or more characters.

Code	Meaning
<input type="password" name="pwd" size="40" max-length="32" autocomplete="OFF" />	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 six or more characters.
<input type="submit" value="Login" />	Sends the login request to Web authentication. Do not modify this code. Place this code inside the <form></form> tags.

Notes

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 a login page (login.html).

Figure 9-24: Example of source code for 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>
<title> </title>
</head>
<body>
<!-- ===== Body ===== -->
<center>
<br />
<table width="100%">
<tr><td align="center" bgcolor="#2b1872">
<font color="#ffffff"><b>LOGIN</b></font>
</td></tr></table>
<br />
Please enter your ID and password.<br />
<br />

 <form name="Login" method="post" action="/cgi-bin/Login.cgi">
  <table><tr>                                   Runs the script that interacts with Web authentication
   <td>user ID</td>
   <td>

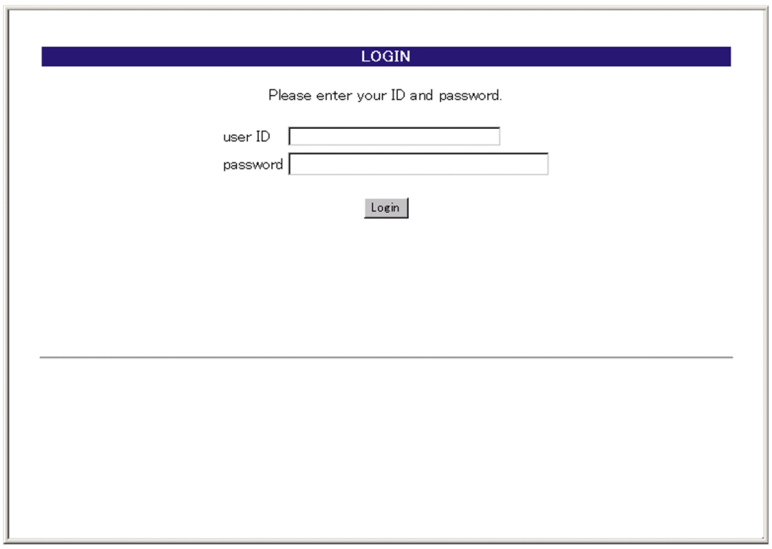
 <input type="text" name="uid" size="40" maxlength="32" autocomplete="OFF" />
                                                 Provides a field for user ID specification
  </td>
  </tr><tr>
   <td>password</td>
   <td>

 <input type="password" name="pwd" size="40" maxlength="32"
 autocomplete="OFF" />
                                                 Provides a field for password specification
  </td></tr>
  </table>
  <br />
 <input type="submit" value="Login" />
                                                 Submits a Web authentication login request
  </form>
  <br /><br /><br /><br /><br /><br />
  </center>
  <!-- ===== Footer ===== -->
  <hr>
  </body>
  </html>
```

(3) Login page display example

The following figure shows an example of how the login page appears to a user.

Figure 9-25: Login page (browser display example)



9.3.2 Logout page: logout.html

A client who has logged in using Web authentication uses this page to issue a logout request.

(1) Condition for setting

You must include the code listed in the following table when creating an HTML file to serve as the logout page.

Table 9-4: Code required in logout page

Code	Meaning
<form name="Logout" method="post" action="/cgi-bin/Logout.cgi"></form>	Initiates a Web authentication logout process. Do not modify this code.
<input type="submit" value="Logout" />	Sends the logout request to Web authentication. Do not modify this code. Place this code inside the <form></form> tags.

Notes

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 a logout page (logout.html).

Figure 9-26: Example of source code for 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>
<title> </title>
</head>
<body>
<!-- ===== Body ===== -->
<center>
<br />
<form name="Logout" method="post" action="/cgi-bin/Logout.cgi">
<table width="100%">
<tr><td align="center" bgcolor="#2b1872">
<font color="#ffffff"><b>LOGOUT</b></font>
</td></tr></table>
<br />
Please push the following button.<br />
<br />
<input type="submit" value="Logout" />
</form>
<br /><br /><br /><br /><br /><br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

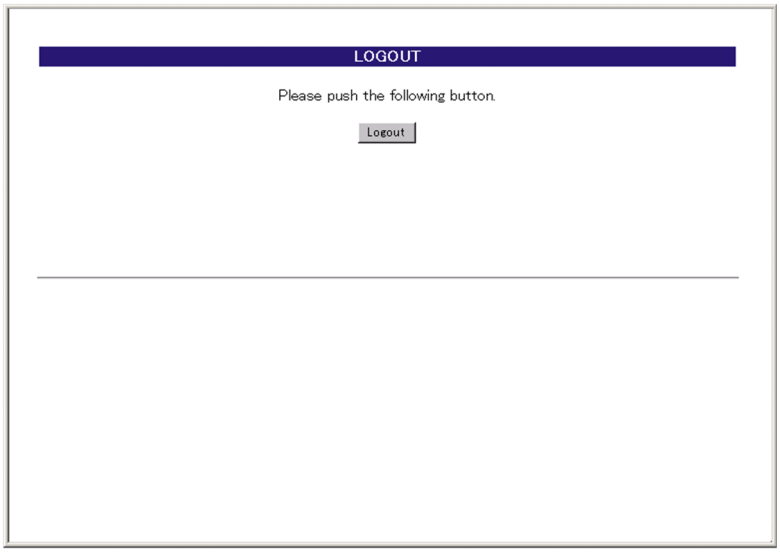
Runs the script that interacts with Web authentication

Submits a Web authentication logout request

(3) Logout page display example

The following figure shows an example of how the logout page appears to a user.

Figure 9-27: Logout page (browser display example)



9.3.3 Authentication error message file (file name: 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 nine lines of data, each corresponding to a specific message as described in the table below.

Table 9-5: 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."
4	The message output when login fails due to an error in the Switch configuration or a conflict with other function. 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) Condition 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 nine lines, subsequent lines are ignored.

(2) Key points regarding authentication 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).

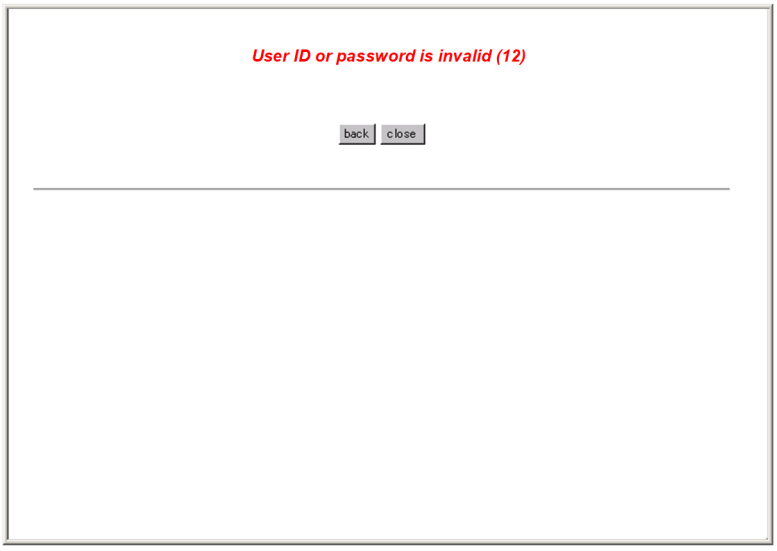
Figure 9-28: Example of source code for authentication error message file (webauth.msg)

```
The user name or password is incorrect.
The password is incorrect.
The authentication server could not be found.<BR>Contact the system administrator.
The system configuration contains an error.<BR>Contact the system administrator.
A minor system error occurred.<BR>Please try again later.
A major system error occurred.<BR>Contact the system administrator.
A critical system error occurred.<BR>Contact the system administrator.
The system is overloaded.<BR>Please try again later.
The client PC is not logged in.
```

(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 9-29: Login failed page (browser display example)



9.3.4 Tags specific to Web authentication

You can display information such as the login time and error messages by embedding tags specific to Web authentication in the HTML files that serve as the Web authentication pages.

The following table describes which Web authentication pages can display which tags.

Table 9-6: Special tags

Tag notation	Content displayed on screen	Login page	Logout page	Login success page	Login failed page	Logout completed page	Logout failed page	Reply-Message page
<!-- Login_Time -->	Login time#1	—	—	Y	—	—	—	—
<!-- Logout_Time -->	Logout time#2	—	—	Y	—	Y	—	—
<!-- After_Vlan -->	Post-authentication VLAN ID#3	—	—	Y	—	—	—	—
<!-- Error_Message -->	Error message#4	—	—	—	Y	—	Y	—
<!-- Redirect_URL -->	None	—	—	—#5	—	—	—	—
<!-- Session_Code -->	None	—	—	—	—	—	—	—#6
<!-- Reply_Message -->	Reply-Message to Access-Challenge received from RADIUS server	—	—	—	—	—	—	Y

Legend: Y: Appears on-screen; —:Appears as blank space on screen

#1: The time when login was successful

#2: This tag has different meanings depending on the page where it appears:

Login success page: The time when auto-logout will take place

Logout completed page: The time when the logout process was completed

#3: The VLAN ID of the VLAN that the user can access after authentication

#4: The error that caused the login or logout attempt to fail

#5: Does not display data on screen, but retains the URL to which the user is directed after successful authentication

#6: Does not display data on screen, but retains the user ID and State value

For examples of how to use these tags, see "9.3.5 Examples of other pages"

9.3.5 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 a login success page and how the page appears to the user.

Figure 9-30: Example of source code for 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>
</head>
<body oncontextmenu=\"return false;\">
<!-- ===== Body ===== -->
<center>
Login success
<br /><br />
<Table Border="0">
<Tr>
<Td Align="left">
Login Time
</Td>
<Td Align="left">
 ---
</Td>
<Td Align="left">
<b><!-- Login_Time --></b>          Tag for displaying login time
</Td>
</Tr>
<Tr>
<Td Align="left">
Logout Time
</Td>
<Td Align="left">
 ---
</Td>
<Td Align="left">
<b><!-- Logout_Time --></b>         Tag for displaying logout time
</Td>
</Tr>
</Table>                            Tag indicating destination of URL
<b><!-- Redirect_URL --></b>        redirection after successful authentication
<br /><br />

<form>
<input type="button" value="close" onClick="window.close()" />
</form>
<br /><br />
</center>
<br /><br />
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

Notes

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 authentication login is performed in the dynamic VLAN mode or the legacy mode when the loginOK.html file contains a reference to another file, the login success page might not appear correctly.

Figure 9-31: Login success page (browser display example)

(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 9-32: Example of source code for 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>        Tag for displaying logout time
<br /><br /><br />
<form>
<input type="button" value="close" onClick="window.close()" />
</form>
<br /><br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

Notes

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 9-33: Logout completed page (browser display example)

(3) Login/logout failed pages (loginNG.html/logoutNG.html)

The figures below show example of the source code for a login or logout failed page and how the page appears to the user.

Figure 9-34: Example of source code for login and logout failed pages (loginNG.html and logoutNG.html)

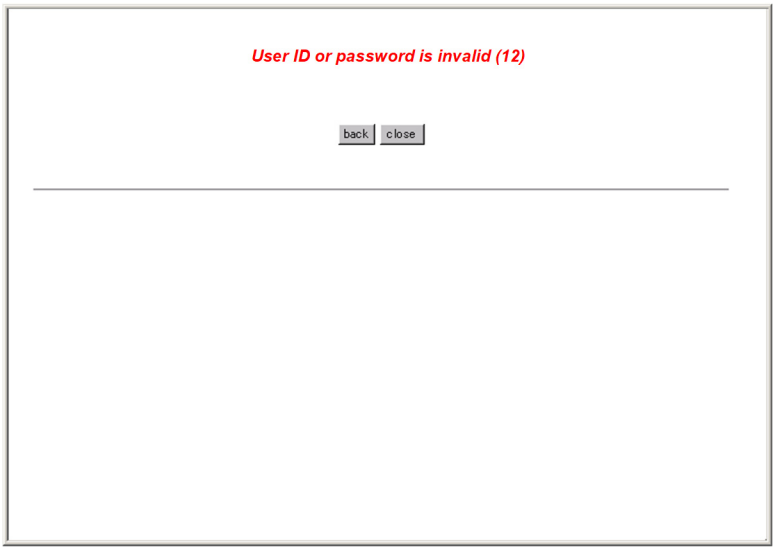
```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title> </title>
</head>
<body oncontextmenu=\"return false;\">
<!-- ===== Body ===== -->
<center>                                    Tag for displaying error messages
<br>
<i style="color:red"><b><!--Error_Message --></b></i>
<br /><br /><br /><br />
<form>
<input type="button" value="back" onClick="history.back()" />
<input type="button" value="close" onClick="window.close()" />
</form>
<br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

Notes

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 9-35: Login or logout failed page (browser display example)



9.4 Preparing the SSL certificate

9.4.1 Environment for creating the server certificate and key

To create a server certificate and key for SSL, you need an environment where openssl works. The operating systems on which openssl works are as follows:

- UNIX-based OS
- Windows-based OS (cygwin is required)

Run openssl to create a server certificate and key. Use openssl 1.0.2 or newer version. For building openssl, see the open source openssl documentation.

9.4.2 Creating the server certificate and key

The following table shows the information to be entered in openssl when creating a server certificate and key.

Table 9-7: Information to enter in openssl

Name	Description
pass phrase for server.key	Server password
Country Name	Country code
State or Province Name	Prefecture name
Locality Name	Municipal name
Organization Name	Organization name or company name
Organizational Unit Name	Department name
Common Name	IP address of FQDN or the Switch
Email Address	Admin email address
challenge password	—
optional company name	—

Legend: —: Input not required

A server certificate and key for SSL are created in an environment on which openssl works. The procedure is as follows. The following file names are used in the execution example.

- Private key file name: server.key
- File name of signature request form: server.pem
- File name of the server certificate to be created: server.crt
- File name of the private key to be created: serverinstall.key

Note that the openssl running environment prompt is "unix#".

(1) Prepare a random number seed file

Prepare a file (rand.dat) of several hundred bytes. Any content or code is acceptable.

(2) Create a key used for SSL communication

The figure below shows an example of creating a key (server.key) with a key length of 2048 bits.

Figure 9-36: Key creation

```
unix# openssl genrsa -out server.key -aes256 -rand rand.dat 2048
241 semi-random bytes loaded
Generating RSA private key, 2048 bit long modulus
.....................................................................+++
.............+++
e is 65537 (0x10001)
Enter pass phrase for server.key: *******                              …1
Verifying - Enter pass phrase for server.key: *******                  …2
```

1.Enter the password for the server.

2.Re-enter the password for the server.

(3) Create a signature request form

The figure below shows an example of creating a signature request form (server.pem) from a private key (server.key) using SHA256. Note that the information you enter in this figure is used to show the operation. Enter the information that is actually required for checking with the CA certificate issued by the CA office and the intermediate CA certificate.

Figure 9-37: Creating a signature request form

```
unix# openssl req -new -sha256 -key server.key -out server.pem
Enter pass phrase for server.key: *******                              …1
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP                                   …2
State or Province Name (full name) [Some-State]:KANAGAWA               …3

Locality Name (eg, city) []:KAWASAKI                                   …4
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AlaxalA     …5
Organizational Unit Name (eg, section) []:AX                           …6

Common Name (e.g. server FQDN or YOUR name) []:www.example.com         …7
Email Address []:admin@example.com                                     …8
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:                                               …9
An optional company name []:                                           …9
```

1.Enter the password for the server.

2.Enter the country code.

3.Enter the prefecture name.

4.Enter the region.

5.Enter the company name.

6.Enter any name.

7.Enter the IP address of FQDN or the Switch.

8.Enter the email address.

9.Do not enter anything.

(4) Creating a server certificate

The figure below shows an example of using the -days option to create a server certificate (server.crt) with an expiration date of 365 days.

Figure 9-38: Creating a server certificate

```
unix# openssl x509 -in server.pem -out server.crt -req -signkey server.key -days 365
Signature ok
subject=/C=JP/ST=KANAGAWA/L=KAWASAKI/O=AlaxalA/OU=AX/CN=www.example.com/emailAddress=admin@ex-
ample.com
Getting Private key
Enter pass phrase for server.key: *******                                    …1
```

1.Enter the password for the server.

(5) Generating a private key for installation on the Switch

The figure below shows an example of generating a private key (serverinstall.key) for installation on the Switch.

Figure 9-39: Generating a private key

```
unix# openssl rsa -in server.key -out serverinstall.key
Enter pass phrase for server.key: *******                                    …1
writing RSA key
```

1.Enter the password for the server.

9.4.3 Registering the server certificate and key

Register the server certificate and private key to the Switch using the "set web-authentication ssl-crt" operation command Also, if there is an intermediate CA certificate, register it at the same time as the server certificate and private key. The procedure is as follows.

(1) Transfer the server certificate and key to the Switch

Transfer the created server certificate and private key to the Switch using the memory card or such commands as the "sftp" operation commands and "scp" operation commands. If there is an intermediate CA certificate, transfer it to the Switch in the same way.

(2) Preparing an intermediate CA certificate

If you have an intermediate CA certificate, prepare a file for the intermediate CA certificate to be registered. Also, if there are multiple intermediate CA certificates (the two files root.crt and next.crt in the following execution example), merge the files to create a single file (ca.crt).

Figure 9-40: Preparing the intermediate CA certificate

```
# cp root.crt ca.crt
# cat next.crt >> ca.crt
#
```

(3) Registering the server certificate and key to the Switch

Login in administrator mode and place the server certificate (server.crt) and private key (serverinstall.key) in the current directory. If there is an intermediate CA certificate (ca.crt), place the intermediate CA certificate in the current directory.

With the file in place, execute the "set web-authentication ssl-crt" operation command to register it to the Switch.

Figure 9-41: Registering the server certificate and key

```
# set web-authentication ssl-crt
Set path to the key: serverinstall.key                                       …1
Set path to the certificate: server.crt                                      …2
Set path to the intermediate CA certificate: ca.crt                          …3
Would you wish to install SSL key and certificate? (y/n):y                   …4
Install complete.
Please restart web-authentication daemon or web-server daemon.
```

```
#
```

1.Specifies the file name of the private key.

2.Specifies the file name of the server certificate.

3.Specifies the file name of the intermediate CA certificate. If there is no intermediate CA certificate, press only the [Enter] key.

4.Enter y if what you entered is correct.

During registration, the content and validity of the server certificate, private key, and intermediate CA certificate are not checked. Therefore, if you do not register the correct combination of server certificate, private key, and intermediate CA certificate, you will not be able to log in or log out using HTTPS. In such a case, delete the registered certificate and private key, and then re-register the correct combination of server certificate, private key, and intermediate CA certificate.

(4) Checking registration

Execute the "show web-authentication ssl-crt" operation command to confirm that the server certificate, private key, and intermediate CA certificate are registered.

Figure 9-42: Checking the registration of the server certificate and key

```
# show web-authentication ssl-crt
Date 20XX/04/15 10:07:04 UTC
                              DATE
SSL key              :  20XX/03/30 14:05
SSL certificate      :  20XX/03/30 14:05
SSL intermediate cert:  20XX/03/30 14:05
```

(5) Restarting the web server

Execute the "restart web-authentication web-server" operation command to restart the web server.

Figure 9-43: Restarting the web server

```
# restart web-authentication web-server
```

(6) Checking the startup of web server

Use the "ps" command to confirm that the web server (httpd) is up and running.

Figure 9-44: Checking the startup of web server

```
# ps -auwx |grep httpd
root       471  0.0  0.1   212    672 ?? S    6:19PM  0:00.52 /usr/local/sbin/httpd -DS_WA -DSSL
-DWA_SSL
operator 11070  0.0  0.1   164   556 00 S+   6:20PM  0:00.01 sh -c ps -auwx | grep httpd
operator 11421  0.0  0.0    32    36 00 R+   6:20PM  0:00.00 grep httpd
```

9.4.4 Deleting the server certificate and key

Use the "clear web-authentication ssl-crt" operation command to delete the server certificate, private key, and intermediate CA certificate registered to the Switch. The procedure is as follows.

(1) Deleting the server certificate and key

Login in administrator mode and execute the "clear web-authentication ssl-crt" operation command to delete the registered server certificate, private key, and intermediate CA certificate.

Figure 9-45: Deleting the server certificate and key

```
# clear web-authentication ssl-crt
Would you wish to clear SSL key and certificate? (y/n):y              …1
Please restart web-authentication daemon or web-server daemon.
#
```

1.Enter y to delete the registered server certificate, private key, and intermediate CA certificate.

(2) Checking deletion

Execute the "show web-authentication ssl-crt" operation command to confirm that the server certificate, private key, and intermediate CA certificate are deleted.

Figure 9-46: Checking the deletion of the server certificate and key

```
# show web-authentication ssl-crt
Date 20XX/04/15 10:07:04 UTC
                              DATE
SSL key              :  default now
SSL certificate      :  default now
SSL intermediate cert:  -
```

(3) Restarting the web server

Execute the "restart web-authentication web-server" operation command to restart the web server.

Figure 9-47: Restarting the web server

```
# restart web-authentication web-server
```

(4) Checking the startup of web server

Use the "ps" command to confirm that the web server (httpd) is up and running.

```
# ps -auwx | grep httpd
root       471  0.0  0.1   212    672 ??  S     6:19PM  0:00.52 /usr/local/sbin/httpd -DS_WA -
DSSL -DWA_SSL
operator 11070  0.0  0.1   164    556 00  S+    6:20PM  0:00.01 sh -c ps -auwx | grep httpd
operator 11421  0.0  0.0    32     36 00  R+    6:20PM  0:00.00 grep httpd
```

10 Description of MAC-based Authentication

The MAC-based authentication function controls VLAN access based on the source MAC address of received frames. This chapter describes MAC-based authentication.

10.1 Overview

MAC-based authentication provides a method for authenticating terminals such as printers which, unlike PCs and similar devices, cannot participate in the login process as required by IEEE 802.1X and Web authentication.

The switch performs authentication based on the source MAC address of frames received at a port configured to perform MAC-based authentication, and admits frames originating from authorized terminals.

If DHCP snooping is enabled at the port, the ARP packets and DHCP packets sent from the terminal are subject to DHCP snooping before they become involved in the MAC-based authentication process. For this reason, MAC-based authentication applies only to packets that DHCP snooping allows through the port.

(1) Authentication mode

The Switch supports the following authentication modes:

- Fixed VLAN mode

  Terminals that undergo successful authentication have their MAC addresses entered in the MAC address table and are permitted access to the VLAN.

- Dynamic VLAN mode

  Terminals that undergo successful authentication have their MAC addresses registered in a MAC VLAN. Terminals are given access to different VLANs before and after authentication.

In the description of dynamic VLAN mode, the VLAN to which an unauthenticated terminal belongs is called Pre-authentication VLAN. The VLAN after authentication is called Post-authentication VLAN.

(2) Authentication method

Users of the Switch can choose to perform authentication locally or via a RADIUS server. Fixed VLAN mode and dynamic VLAN mode each support both variations.

- Local authentication method

  The Switch stores the MAC address in what is known as an internal MAC-based authentication DB. Authentication is successful when a MAC address in the received frame matches that in the database. This method is suited to small-scale networks that lack a RADIUS server.

- RADIUS authentication method

  Authentication is performed by using a RADIUS server deployed on the network. This method is suited to larger networks.

10.2 System configuration examples

This section describes sample configurations for networks using local and RADIUS authentication method in fixed VLAN mode and dynamic VLAN mode.

10.2.1 Fixed VLAN mode

In fixed VLAN mode, prior to authentication, a terminal does not appear in the MAC address table and is unable to access the VLAN associated with the interface to which it is attached. If authentication succeeds, the switch adds the terminal's MAC address to the MAC address table, thus permitting access to the VLAN.

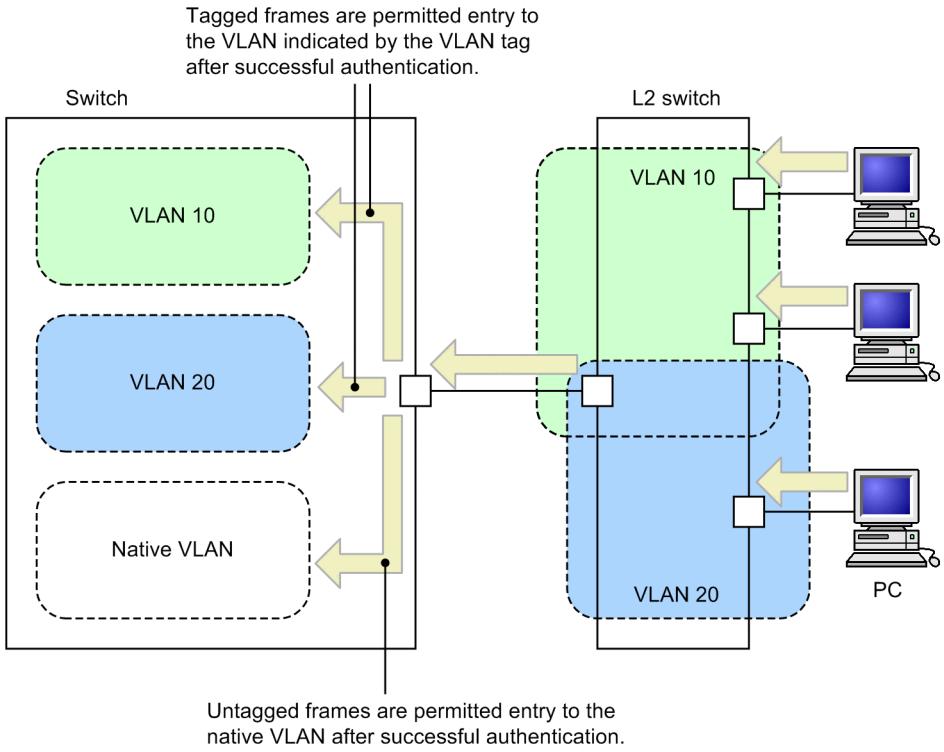
In the Switch, you can configure authentication at the following ports:

- Access port
- Trunk port

Tagged and untagged frames that enter a trunk port are handled as follows:

- Tagged frames are forwarded to the VLAN indicated by the VLAN tag after successful authentication
- Untagged frames are forwarded to the native VLAN after successful authentication

Figure 10-1: Handling of tagged and untagged frames

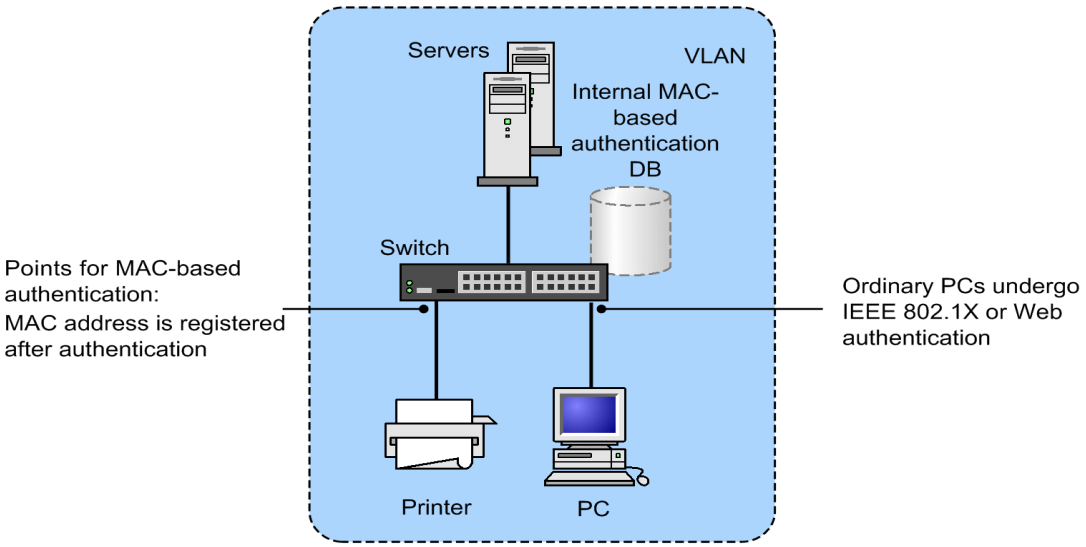


For a device to have access to the pre-authentication VLAN, you need to make sure that the authentication IPv4 access list contains the necessary filter conditions.

(1) Local authentication method

In the local authentication, the switch compares the source MAC address of frames received at a MAC-based authentication port against the MAC addresses registered in the internal MAC-based authentication DB. If the source MAC address matches an entry in the database, authentication is successful and the device is permitted to access the network.

Figure 10-2: Local authentication method in fixed VLAN mode



The local authentication method 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.

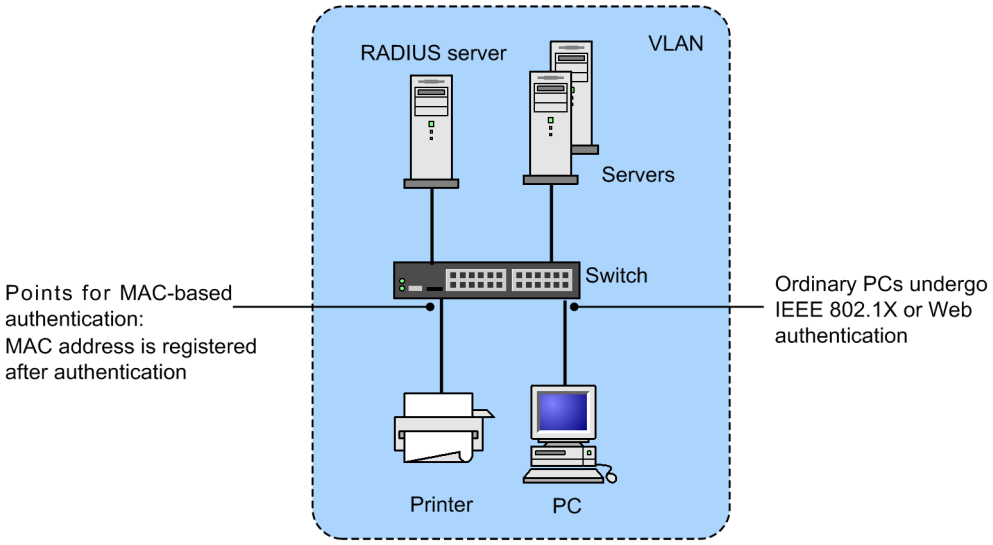
Table 10-1: Using VLAN IDs as a condition for local authentication method in fixed VLAN mode

Configuration command settings	Does the internal MAC-based authentication DB contain VLAN ID data?	
	Set	Not set
Set	Authentication is successful if the MAC address and VLAN ID both match.	Authentication is successful if the MAC address matches.
Not set	Authentication is successful if the MAC address matches.	Authentication is successful if the MAC address matches.

(2) RADIUS authentication method

In RADIUS authentication method, the switch submits the source MAC address of frames received at a MAC-based authentication port to the RADIUS server for authentication. If the source MAC address matches an entry on the server, authentication is successful and the device is permitted to access the network.

Figure 10-3: RADIUS authentication method in fixed VLAN mode



RADIUS authentication method 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 10-2: Using VLAN IDs as a condition for RADIUS authentication method in fixed VLAN mode

Configuration command settings	Operation
Set	Authentication is successful if the MAC address and VLAN ID both match.
Not set	Authentication is successful if the MAC address matches.

You can use the "mac-authentication password" configuration command to set the password that the Switch uses when submitting an authentication request to the RADIUS server. If you omit this command, the Switch uses the device's MAC address as the password.

10.2.2 Dynamic VLAN mode

When a terminal with membership to the pre-authentication VLAN undergoes successful authentication in dynamic VLAN mode, the terminal is registered in a MAC VLAN and a MAC address table based on a VLAN ID provided by the internal MAC-based authentication DB or the RADIUS server. As a result, the terminal gains access to the post-authentication VLAN. For this to work, the following configuration is required:

- The ports in the MAC VLAN must be configured as authentication ports

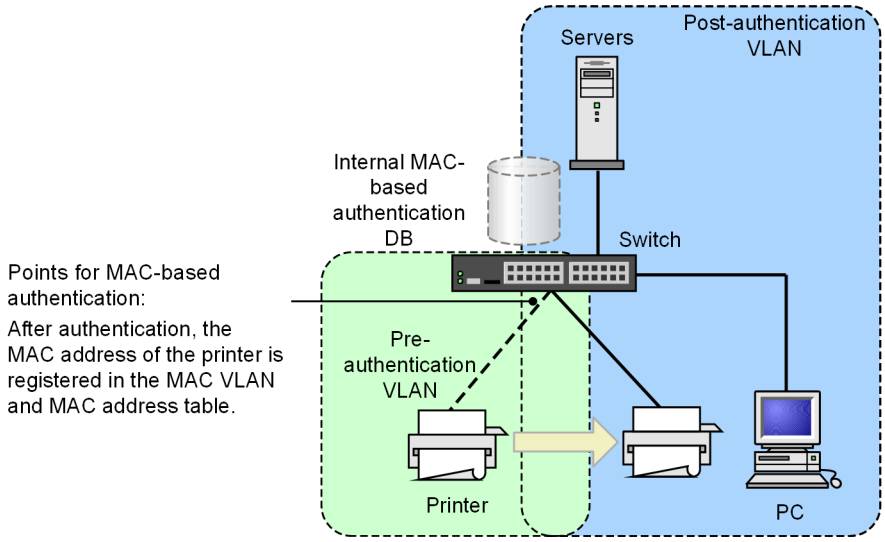
For a device to have access to the pre-authentication VLAN, you need to make sure that the authentication IPv4 access list contains the necessary filter conditions.

(1) Local authentication method

In the local authentication method, the switch compares the source MAC address of frames received at a MAC-based authentication port against the MAC addresses registered in the internal MAC-based authentication DB. If the source MAC address matches an entry in the database, the switch registers the MAC ad-

dress of the device in a MAC VLAN and MAC address table based on the VLAN ID that the database provides. The device is then able to access the post-authentication VLAN.

Figure 10-4: Configuring local authentication method for dynamic VLAN mode

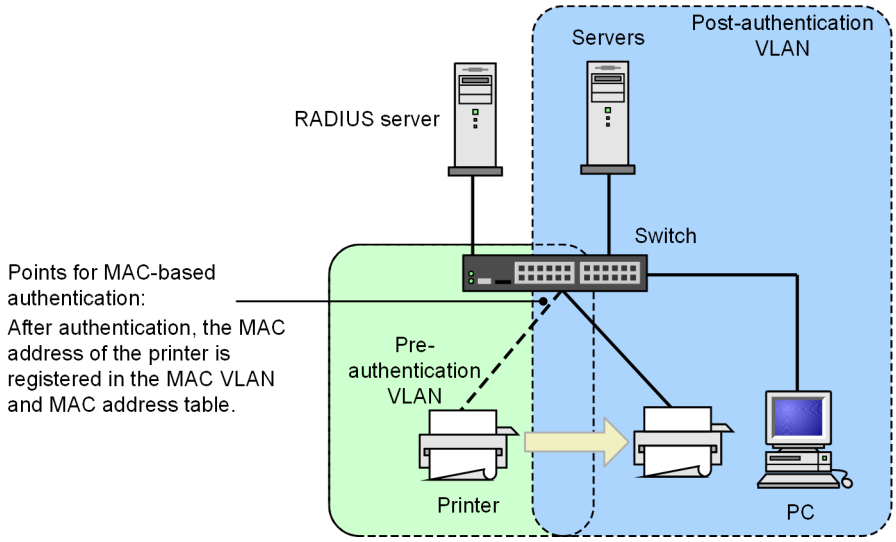


(2) RADIUS authentication method

In RADIUS authentication method, the switch submits the source MAC address of frames received at a MAC-based authentication port to the RADIUS server for authentication. If the source MAC address matches an entry on the server, the switch registers the MAC address of the device in a MAC VLAN and MAC address table based on the VLAN ID that the RADIUS server provides. The device is then able to access the post-authentication VLAN.

You can use the "mac-authentication password" configuration command to set the password that the Switch uses when submitting an authentication request to the RADIUS server. If you omit this command, the switch uses the device's MAC address as the password.

Figure 10-5: RADIUS authentication method in dynamic VLAN mode



10.2.3 Behavior with dot1q configured at a MAC port

For details about how a MAC port runs with dot1q configured, see "5.3 Function common to all Layer 2 authentication modes".

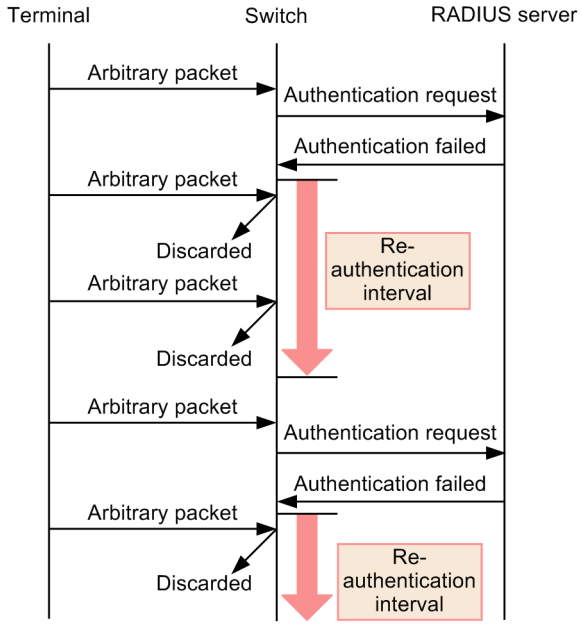
10.3 Authentication function

10.3.1 Behavior after authentication fails

If a terminal fails MAC-based authentication, the switch makes no more attempts to authenticate the terminal for a fixed time period (called the re-authentication interval). When this period has elapsed, the switch attempts MAC-based authentication for that terminal again.

You can set the re-authentication interval by using the "mac-authentication auth-interval-timer" configuration command. The authentication process typically resumes within a minute of the re-authentication period elapsing.

Figure 10-6: Running sequence after failed authentication



10.3.2 Forced authentication

For details about forced authentication behaviors in the context of MAC-based authentication, see "5.3 Function common to all Layer 2 authentication modes".

10.3.3 De-authentication method

The following table describes the events that lead to a terminal losing its authenticated status.

Table 10-3: De-authentication methods by authentication mode

De-authentication method	Fixed VLAN mode	Dynamic VLAN mode
De-authentication when the maximum connection time is exceeded	Y	Y
De-authentication using an operation command	Y	Y
De-authentication of terminals connected to link-down ports	Y	—

De-authentication method	Fixed VLAN mode	Dynamic VLAN mode
De-authentication of terminals by MAC address table aging	Y	Y
De-authentication resulting from changes to the VLAN configuration	Y	Y
De-authentication resulting from authentication method changes	Y	Y
De-authentication resulting from authentication mode changes	Y	Y
De-authentication due to suspension of MAC-based authentication	Y	Y
Logout due to deletion of a dynamically registered VLAN	—	Y

Legend: Y: Supported; —: Not applicable

(1) De-authentication when the maximum connection time is exceeded

When a terminal exceeds the maximum connection time specified by the "mac-authentication max-timer" configuration command, its MAC-based authentication status is forcibly cleared. This process takes place within a minute of the maximum connection time being exceeded.

If you use the "mac-authentication max-timer" configuration command to shorten or extend the maximum connection time, the changes do not take effect until the next time the terminal is authenticated. Existing authentication sessions are unaffected.

(2) De-authentication using an operation command

You can use the "clear mac-authentication auth-state" operation command to forcibly revoke the authentication status of individual MAC addresses. If the same MAC address is authenticated in more than one VLAN ID, the switch terminates every authentication session associated with the MAC address.

(3) De-authentication of terminals connected to link-down ports

When a port to which authenticated terminals are connected goes down, the switch clears the authentication status of terminals connected to that port.

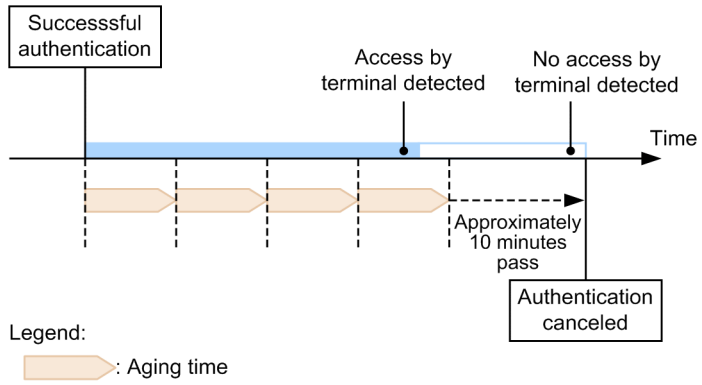
(4) De-authentication of terminals by MAC address table aging

The switch monitors the MAC address table periodically for entries related to authenticated terminals, and checks for signs of recent access by those terminals. If the switch consistently finds that there has been no access by a particular terminal, it forcibly clears the MAC-based authentication status of the terminal, and shifts its membership to the pre-authentication VLAN ID. To prevent a situation in which a brief network interruption causes a terminal to lose its authentication status, authentication cancellation takes place when there has been no access from a terminal for a 10 minute period after its MAC address is scheduled to be aged out of the MAC address table.

The figure below shows the relationship between the aging time specified for the MAC address table, and the time when the terminal is logged out due to MAC address table aging.

Use the default value for the aging time, or specify a larger value than the default.

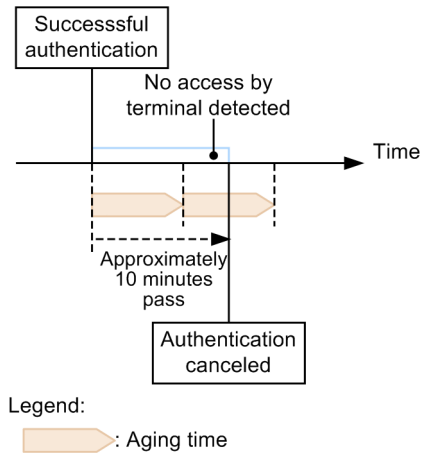
Figure 10-7: Logout of an authenticated terminal by MAC address table aging



If there is no access by a terminal in the 10 minute period after successful authentication, the terminal loses its authentication status immediately without regard to the aging time.

The following figure shows a situation in which a terminal is logged out due to inactivity after successful authentication.

Figure 10-8: Logout due to inactivity after successful authentication



You can disable this function by using the "no mac-authentication auto-logout" configuration command. In this case, terminals are not forcibly logged out, regardless of how long they stay inactive.

(5) De-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

(6) De-authentication resulting from authentication method changes

If you change the authentication method from RADIUS authentication to local authentication method or vice-versa, the switch clears the authentication status of all terminals.

(7) De-authentication resulting from authentication mode changes

If you use the "copy" command to change the switch configuration in a manner that results in changes to the authentication mode, the switch clears the authentication status of all terminals.

(8) De-authentication due to suspension of MAC-based authentication

If a configuration command deletes the MAC-based authentication configuration resulting in the suspension of MAC-based authentication, the switch clears the authentication status of all terminals.

(9) Logout due to deletion of a dynamically registered VLAN

If the "switchport mac vlan" configuration command is set to an authentication port for which a VLAN is dynamically created, the VLAN ID dynamically created for the port is deleted, and terminals that belonged to the VLAN are unauthenticated.

10.3.4 Limited number of authentications

You can limit the number of authenticated users at the device level and at the port level. For details, see "5.3 Function common to all Layer 2 authentication modes".

10.3.5 Moving authenticated terminals between ports

For details about how the authentication status of a terminal is affected when you move it between ports, see "5.3 Function common to all Layer 2 authentication modes".

10.3.6 Accounting function

The Switch use the accounting function described below to record the results of authentication operations.

(1) Accounting logs

MAC-based authentication accounting logs contain information about the use of MAC-based authentication services on the Switch. You can display the log information by using the "show mac-authentication logging" operation command.

The following table describes the events recorded as accounting log information.

Table 10-4: Authentication results output as accounting log information

Event	Time	MAC address	VLAN ID	Port number	Message
Successful authentication	Time when authentication succeeded	Y	Y	Y	Authentication success
Authentication status canceled	Time when authentication status was cleared	Y	Y#	Y#	Authentication cleared
Failed authentication	Time when authentication failed	Y	Y#	Y#	Reason for failed authentication

Legend: Y: Recorded

#: Might not be output depending on the message contents.

The Switch can store a maximum of 2100 lines of MAC-based authentication accounting log information. Upon reaching this limit, the switch starts overwriting the existing accounting information in order from the oldest.

(2) Providing information to the RADIUS server accounting function

You can enable the accounting function for the RADIUS server by using the "aaa accounting mac-authentication" configuration command. The accounting function records the following information:

- Authentication information. The following information is recorded when authentication is successful:

  Server timestamp, MAC address, VLAN ID

- De-authentication information. The following information is recorded when the authentication status of a terminal is cleared:

  Server timestamp, MAC address, VLAN ID, elapsed time between successful authentication and authentication cancellation

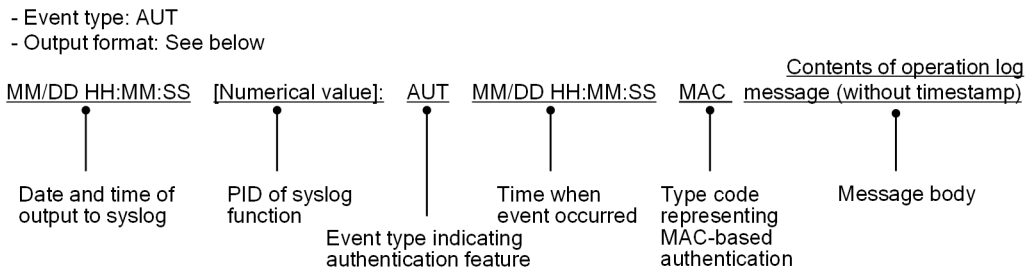
(3) Recording authentication information on a RADIUS server

If you are using RADIUS authentication method, the accounting function 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) Writing operation logs to a syslog server

You can output the action logs for MAC-based authentication to a syslog server. These action logs include the MAC-based authentication accounting logs. The following figure shows the format of log output to the syslog server.

Figure 10-9: Format of output to syslog server



You can start and stop output to syslog by using the mac-authentication logging enable and "logging event-kind aut" configuration commands.

10.4 Preparing an internal MAC-based authentication DB and the RADIUS server

10.4.1 Preparing an internal MAC-based authentication DB

You need to build an internal MAC-based authentication DB before you can use MAC-based authentication in local authentication method. You can then use commands to back up and restore the database that you built.

(1) Creating an internal MAC-based authentication DB

You can use the "set mac-authentication mac-address" operation command to register a MAC address and VLAN ID in the internal MAC-based authentication DB. If required, you can later use the "remove mac-authentication mac-address" operation command to delete a MAC address you registered.

Additions or changes to the database do not take effect until you execute the "commit mac-authentication" operation command.

Note that additions or changes committed to the internal MAC-based authentication DB by the "commit mac-authentication" operation command do not apply to authentication sessions that are already in progress. They will apply the next time the terminal is authenticated.

Notes

When using an internal MAC-based authentication DB in dynamic VLAN mode, keep the following in mind when you register information in the database:

- When you register a MAC address, you must also specify a VLAN ID. If you fail to do so, authentication attempts by that MAC address will end in an error.
- If the same MAC address is associated with more than one VLAN ID in the database, the VLAN ID with the smallest numerical value serves as the post-authentication VLAN for that MAC address.
- Do not specify 1 as the VLAN ID for a MAC address. VLAN ID 1 cannot be assigned to a MAC VLAN, and attempts to authenticate the MAC address will end in an error.

(2) Backing up the internal MAC-based authentication DB

You can use the "store mac-authentication" operation command to back up the internal MAC-based authentication DB you created for use in local authentication.

(3) Restoring the internal MAC-based authentication DB

You can use the "load mac-authentication" operation command to restore the internal MAC-based authentication DB from a backup file you created. Keep in mind that any recent additions or changes you made using the "set mac-authentication mac-address" operation command will be lost and replaced with the contents of the backup file.

10.4.2 Preparing the RADIUS server

Before you can use MAC-based authentication in RADIUS authentication method, you need to configure the MAC addresses and passwords on the RADIUS server.

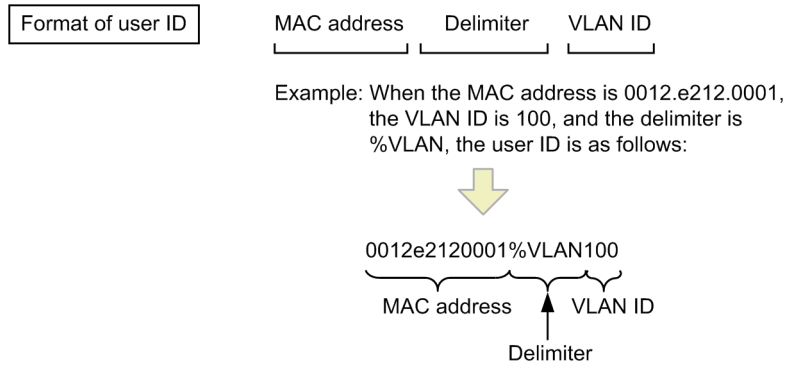
Also shown below are the RADIUS attributes used by the MAC-based authentication function in the Switch.

(1) Registering user IDs

MAC-based authentication requires you to register each MAC address as a user ID on the RADIUS server. Specify the MAC address as a string of 12 hexadecimal digits.

In fixed VLAN mode, if you want the RADIUS server to use both the MAC address and VLAN ID as credentials, register a user ID that combines the MAC address and VLAN ID in a character string with the following format.

Figure 10-10: Format of MAC address and VLAN ID registration



(2) Registering passwords

The password can be either of the following:

- The same MAC address specified as the user ID
- A common password used for all user IDs

(3) Configuring the post-authentication VLAN

Use the following procedure to configure the post-authentication VLAN to which a terminal is assigned after successful authentication in dynamic VLAN mode.

1. Specify 13 (Virtual LANs (VLAN)) for the Tunnel-Type attribute.
2. Specify 6 for the Tunnel-Medium-Type attribute.
3. Specify a VLAN ID for the Tunnel-Private-Group-ID attribute, in one of the following formats:
   - As a numerical value

     Example: If the VLAN ID is 2048, specify the character string 2048.
   - As the character string "VLAN" followed by a numerical value

     Example: If the VLAN ID is 2048, specify the character string VLAN2048.
   - As a VLAN name defined using the "name" configuration command

If you perform authentication in dynamic VLAN mode without setting Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID, the native VLAN will be assigned as the post-authentication VLAN.

(4) RADIUS server attributes used by MAC-based authentication

Make sure that you specify PAP as the authentication method used by the RADIUS server. The table below describes the RADIUS attributes used in the process of MAC-based authentication. For details about how to configure the RADIUS server, see the documentation for the RADIUS server deployed in your network.

Table 10-5: Attributes used in MAC-based authentication (part 1:Access-Request)

Attribute name	Type value	Description
User-Name	1	The MAC address, or a combination of a MAC address and VLAN ID in the format shown in "Figure 10-10: Format of MAC address and VLAN ID registration".
User-Password	2	The MAC address, or a common password specified by a configuration command.
NAS-IP-Address	4	This attribute contains the loopback interface IP address, if one is specified. If no loop-back interface is specified, the IP address of the interface that communicates with the RADIUS server.
Service-Type	6	Specify Framed(2).
Calling-Station-Id	31	The MAC address of the terminal to be authenticated (as a hyphen-punctuated lower-case ASCII string) Example: 00-12-e2-01-23-45
NAS-Identifier	32	A numerical string representing the VLAN ID to which authenticated terminals gain membership in fixed VLAN mode. Example (for VLAN ID 100): 100 In dynamic VLAN mode, use the device name as specified by the "hostname" configuration command.
NAS-Port-Type	61	Specify Virtual(5).
NAS-IPv6-Address	95	The IPv6 address of the loopback interface, if one is specified. If no loopback interface is specified, the IPv6 address of the interface that communicates with the RADIUS server. When communicating via an IPv6 link-local address, this attribute specifies the IPv6 link-local address of the sending interface regardless of whether an IPv6 address is set for the loopback interface.

Table 10-6: Attributes used in MAC-based authentication (part 2:Access-Accept)

Attribute name	Type value	Description
Service-Type	6	Returns Framed(2):This attribute is ignored in MAC-based authentication.
Reply-Message	18	(Not used)
Tunnel-Type	64	Used in dynamic VLAN mode. The MAC-based authentication function checks whether the value is 13 (VLAN). This attribute is not used in fixed VLAN mode.
Tunnel-Medium-Type	65	Used in dynamic VLAN mode. The MAC-based authentication function checks whether the Tunnel-Medium-Type value is 6, as for IEEE 802.1X. This attribute is not used in fixed VLAN mode.
Tunnel-Private-Group-Id	81	Used in dynamic VLAN mode. The value of this attribute is a number representing a VLAN, or the character string VLANxx (where xx is the VLAN ID).

Attribute name	Type value	Description
		An initial octet with a value in the range from 0x00 to 0x1f indicates a tag. In this case the VLAN ID is represented by the second octet onward. If the first octet has a value of 0x20 or higher, the entire value of the attribute represents the VLAN. If this attribute contains a VLAN name as specified by the "name" configuration command, the switch uses the VLAN ID associated with the VLAN name. This attribute is not used in fixed VLAN mode.

Table 10-7: Attributes used in RADIUS Accounting

Attribute name	Type value	Description
User-Name	1	The MAC address, or a combination of a MAC address and VLAN ID in the format shown in "Figure 10-10: Format of MAC address and VLAN ID registration".
NAS-IP-Address	4	The IP address of the NAS. This attribute contains the loopback interface IP address, if one is specified. If no loop-back interface is specified, this attribute contains the IP address of the interface that communicates with the server.
Service-Type	6	Specify Framed(2).
Calling-Station-Id	31	The MAC address of the terminal (as a hyphen-punctuated ASCII string). Example: 00-12-e2-01-23-45
NAS-Identifier	32	A numerical string representing the VLAN ID to which authenticated terminals gain membership in fixed VLAN mode. Example (for VLAN ID 100): 100 In dynamic VLAN mode, use the device name as specified by the "hostname" configuration command.
Acct-Status-Type	40	Contains the value Start(1) at successful authentication, and the value Stop(2) after authentication cancellation.
Acct-Delay-Time	41	The time (in seconds) between the event occurring and transmission to the server.
Acct-Session-Id	44	An ID for identifying the accounting information (This value is the same at authentication and authentication cancellation).
Acct-Authentic	45	The authentication method used (as either RADIUS or Local).
Acct-Session-Time	46	The time (in seconds) until authentication cancellation takes place.
NAS-Port-Type	61	Specify Virtual(5).
NAS-IPv6-Address	95	The IPv6 address of the NAS. The IPv6 address of the loopback interface, if one is specified. If no loop-back interface is specified, the IPv6 address of the interface that communicates with the server. When communicating via an IPv6 link-local address, this attribute specifies the IPv6 link-local address of the sending interface regardless of whether an IPv6 address is set for the loop-back interface.

10.5 Notes on using MAC-based authentication

(1) Notes on use with other functions

For details about the interoperability with other functions, see "5.2 Interoperability of Layer 2 authentication with other functions".

(2) Restarting the MAC-based authentication program

If you restart the MAC-based authentication program, the switch clears the authentication status of all authenticated terminals. In this case, terminals must undergo re-authentication after the program restarts.

11 Settings and Operation for MAC-based Authentication

The MAC-based authentication function controls VLAN access based on the source MAC address of received frames. This chapter describes the operation of the MAC-based authentication function,

11.1 Configuration

11.1.1 List of configuration commands

The following table describes the configuration commands for MAC-based authentication.

Table 11-1: List of configuration commands

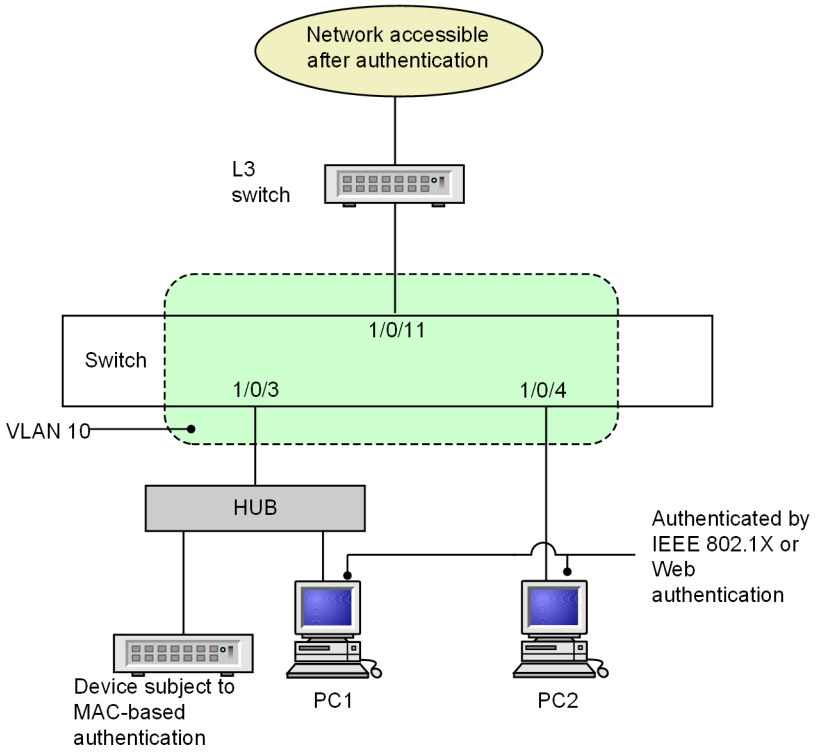
Command name	Description
aaa accounting mac-authentication default start-stop group radius	Enables RADIUS accounting for MAC-based authentication.
aaa authentication mac-authentication default group radius	Specifies RADIUS as the authentication method for MAC-based authentication.
mac-authentication auth-interval-timer	Specifies the time that the switch waits before processing another authentication request from a MAC address that failed authentication.
mac-authentication auto-logout	Disables the function that clears the authentication status of a terminal when there has been no access from its MAC address for a length of time.
mac-authentication dot1q-vlan force-authorized	Exempts tagged frames from authentication when switchport mac dot1q vlan is configured for the MAC port.
mac-authentication dynamic-vlan max-user	Specifies the maximum number of MAC addresses that can be authenticated in dynamic VLAN mode.
mac-authentication logging enable	This step configures the output of action logs on the syslog server.
mac-authentication max-timer	Specifies the maximum connection time for MAC-based authentication users.
mac-authentication password	Specifies the password used when submitting requests to the RADIUS server.
mac-authentication port	Configures a port to perform MAC-based authentication.
mac-authentication radius-server host	Specifies the IP address and other information about the RADIUS server used in the MAC-based authentication process.
mac-authentication static-vlan max-user	Specifies the maximum number of authenticated MAC addresses permitted in fixed VLAN mode.
mac-authentication system-auth-control	Starts the MAC-based authentication daemon.
mac-authentication vlan-check	Specifies that MAC-based authentication use the VLAN ID in addition to the MAC address as credentials.

11.1.2 Configuration for fixed VLAN mode

(1) Basic configuration for local authentication method

The following figure shows the basic configuration required to use local authentication method in fixed VLAN mode.

Figure 11-1: Basic configuration for local authentication method in fixed VLAN mode



(a) Configuring an authentication port

Points to note

Configure the port to be used for MAC-based authentication.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/3
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# mac-authentication port
(config-if)# exit
```

Configures MAC-based authentication at a port where a terminal will be authenticated.

(b) Configuring MAC-based authentication

Points to note

Enable MAC-based authentication by using configuration commands.

Command examples

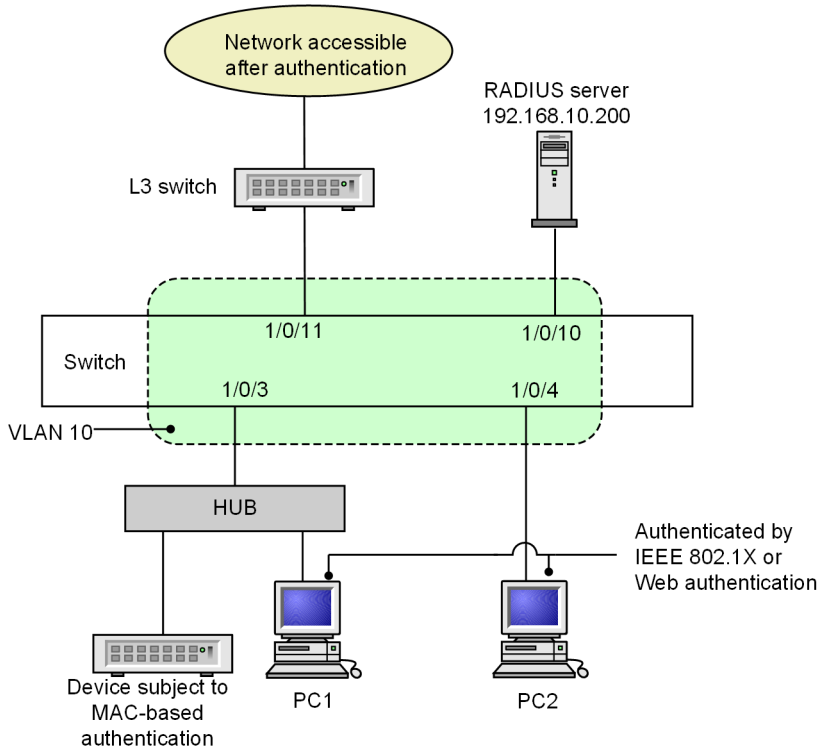
1.
```
(config)# mac-authentication system-auth-control
```

Starts MAC-based authentication.

(2) Basic configuration for RADIUS authentication method

The following figure shows the basic configuration required to use RADIUS authentication method in fixed VLAN mode.

Figure 11-2: Basic configuration for RADIUS authentication method in fixed VLAN mode



(a) Configuring an authentication port

Points to note

Configure the port to be used for MAC-based authentication.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/3
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# mac-authentication port
(config-if)# exit
```

Configures MAC-based authentication at a port where a terminal will be authenticated.

(b) Configuring MAC-based authentication

Points to note

Enable MAC-based authentication by using configuration commands.

Command examples

1.
```
(config)# aaa authentication mac-authentication default group radius
(config)# mac-authentication radius-server host 192.168.10.200 key "macauth"
```

Specifies the IP address and RADIUS key used to access the RADIUS server to perform authentication.

2.
```
(config)# mac-authentication system-auth-control
```

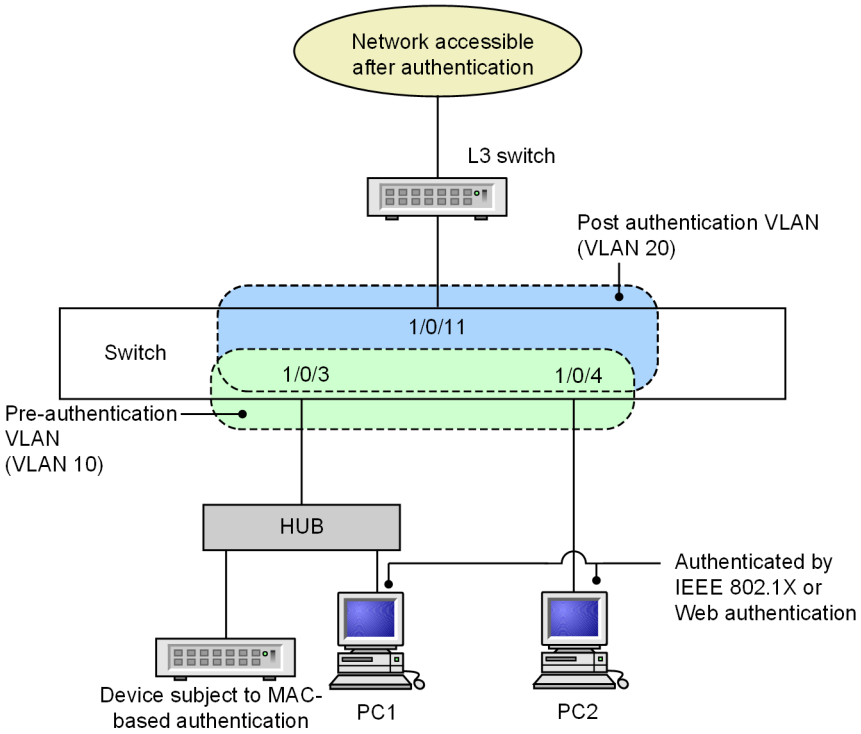
Starts MAC-based authentication.

11.1.3 Configuration for dynamic VLAN mode

(1) Basic configuration for local authentication method

The following figure shows the basic configuration required to use local authentication method in dynamic VLAN mode.

Figure 11-3: Basic configuration for local authentication method in dynamic VLAN mode



(a) Configuring an authentication port

Points to note

Configure the port to be used for MAC-based authentication.

Command examples

1.
```
(config)# interface range gigabitethernet 1/0/3-4
(config-if-range)# switchport mode mac-vlan
(config-if-range)# switchport mac native vlan 10
(config-if-range)# mac-authentication port
(config-if-range)# exit
```

Configures MAC-based authentication at a port where a terminal will be authenticated.

(b) Configuring MAC-based authentication

Points to note

Enable MAC-based authentication by using configuration commands.

Command examples

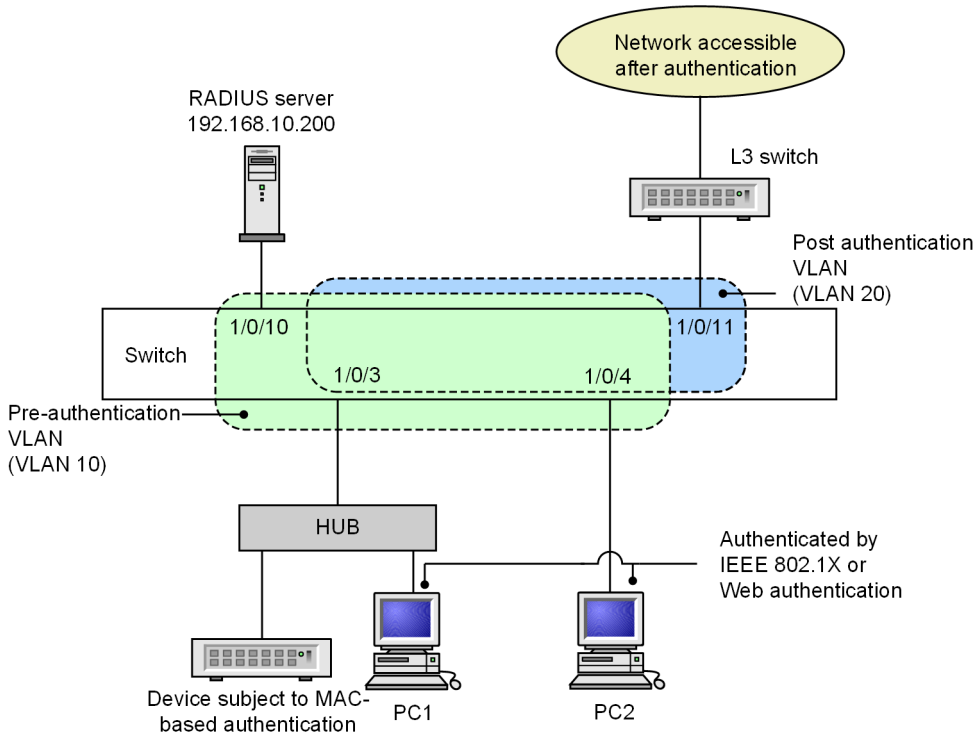
1.
```
(config)# mac-authentication system-auth-control
```

Starts MAC-based authentication.

(2) Basic configuration for RADIUS authentication method

The following figure shows the basic configuration required to use RADIUS authentication method in dynamic VLAN mode.

Figure 11-4: Basic configuration for RADIUS authentication method in dynamic VLAN mode



(a) Configuring an authentication port

Points to note

Configure the port to be used for MAC-based authentication.

Command examples

1.
```
(config)# interface range gigabitethernet 1/0/3-4
(config-if-range)# switchport mode mac-vlan
(config-if-range)# switchport mac native vlan 10
(config-if-range)# mac-authentication port
(config-if-range)# exit
```

Configures MAC-based authentication at a port where a terminal will be authenticated.

(b) Configuring MAC-based authentication

Points to note

Enable MAC-based authentication by using configuration commands.

Command examples

1.
```
(config)# aaa authentication mac-authentication default group radius
(config)# mac-authentication radius-server host 192.168.10.200 key "macauth"
```

Specifies the IP address and RADIUS key used to access the RADIUS server to perform authentication.

2. `(config)# mac-authentication system-auth-control`

   Starts MAC-based authentication.

11.1.4 Configuring MAC-based authentication parameters

This section describes how to set the parameters for MAC-based authentication.

(1) Setting the maximum authentication time

Points to note

Set the time after which the switch forcibly de-authenticates authenticated terminals.

Command examples

1. `(config)# mac-authentication max-timer 60`

   Configures the switch to forcibly de-authenticate terminals after 60 minutes.

(2) Setting the maximum number of authentications in fixed VLAN mode

Points to note

Set the maximum number of MAC addresses that can be authenticated in fixed VLAN mode.

Command examples

1. `(config)# mac-authentication static-vlan max-user 20`

   Specifies 20 as the maximum number of authenticated MAC addresses for MAC-based authentication in fixed VLAN mode.

(3) RADIUS+ server setup

Points to note

Configure the RADIUS server used to implement RADIUS authentication method.

Command examples

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

   Specifies that authentication takes place using a RADIUS server.

(4) Configuring accounting

Points to note

Enable the collection of accounting information for MAC-based authentication.

Command examples

1. `(config)# aaa accounting mac-authentication default start-stop group radius`

   Enables the collection of accounting information by the RADIUS server.

(5) Configuring output to the syslog server

Points to note

Configure the Switch to output authentication results and operation logs to the syslog server.

Command examples

1. `(config)# mac-authentication logging enable`

   `(config)# logging event-kind aut`

   Configures the Switch to output Mac-based authentication results and action logs to the syslog server.

(6) Checking the VLAN ID during authentication

Points to note

Direct the switch to use the MAC address and VLAN ID as the MAC-based authentication credentials, not just the MAC address.

Command examples

1. `(config)# mac-authentication vlan-check key "@@VLAN"`

   Configures MAC-based authentication to also check the VLAN ID.

   If you are using the RADIUS authentication method, the switch submits the MAC address and VLAN ID to the RADIUS server as one character string connected by the characters @@VLAN.

(7) Setting the password for RADIUS

Points to note

Specify the password used for all MAC-based authentication requests sent to the RADIUS server.

Command examples

1. `(config)# mac-authentication password pakapaka`

   Specifies pakapaka as the password sent to the RADIUS server.

(8) Setting the re-authentication interval for when authentication fails

Points to note

Specify how long the switch waits before processing another authentication request for a MAC address that failed authentication.

Command examples

1. `(config)# mac-authentication auth-interval-timer 10`

   Configures the switch to perform re-authentication 10 minutes after authentication fails.

(9) Setting the authentication IPv4 access list

Points to note

Configure the Switch to forward certain packets originating from unauthenticated terminals to destinations that are outside the Switch.

Command examples

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255 eq bootps
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.10.100 eq bootps
(config-ext-nacl)# exit
(config)# interface gigabitethernet 1/0/3
(config-if)# authentication ip access-group 100
(config-if)# exit
```

   Configures an IPv4 access list that permits unauthenticated terminals to send DHCP packets to 192.168.10.100.

(10) Setting the maximum number of authentications in dynamic VLAN mode

Points to note

Set the maximum number of MAC addresses that can be authenticated in dynamic VLAN mode.

Command examples

1. `(config)# mac-authentication dynamic-vlan max-user 20`

   Specifies 20 as the maximum number of authenticated MAC addresses for MAC-based authentication in dynamic VLAN mode.

(11) Disabling authentication cancellation of inactive terminals

Points to note

Disable the function that de-authenticates terminals with authenticated MAC addresses when there has been no access from the terminal for a period of time.

Command examples

1. `(config)# no mac-authentication auto-logout`

   Configures the switch to not clear the authentication status of terminals associated with authenticated MAC addresses when there has been no access from the terminal.

11.1.5 Configuring authentication-exempted ports and terminals

This section describes how to MAC-based authentication-exempted ports and terminals.

(1) Configuring a port as an authentication-exempted port in fixed VLAN mode

Use the following procedure to configure a port to be permitted access in fixed VLAN mode without the need for authentication.

Points to note

Do not designate an authentication-exempted port as an authentication port.

Command examples

1.
```
(config)# vlan 10
(config-vlan)# state active
(config-vlan)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# mac-authentication port
(config-if)# exit
(config)# interface gigabitethernet 1/0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit
```

   Specifies port 1/0/4, which is assigned to VLAN ID 10 in fixed VLAN mode, as an authentication port. This procedure then configures port 1/0/10 to be permitted access without the need for authentication.

(2) Configuring a terminal as an authentication-exempted terminal in fixed VLAN mode

Use the following procedure to specify the MAC address of a terminal to be permitted access in fixed VLAN mode without the need for authentication.

Points to note

Register the MAC address of an authentication-exempted terminal in the MAC address table.

Command examples

1.
```
(config)# vlan 10
(config-vlan)# state active
(config-vlan)# exit
(config)# mac-address-table static 0012.e212.3456 vlan 10 interface gigabitethernet 1/0/10
```

Specifies the MAC address of a terminal to be permitted access to port 1/0/10 with VLAN ID 10, without the need for authentication.

(3) Configuring a port as an authentication-exempted port in dynamic VLAN mode

Uses the following procedure to configure a port to be permitted access in dynamic VLAN mode without the need for authentication.

Points to note

Do not designate an authentication-exempted port as an authentication port.

Command examples

1.
```
(config)# vlan 10
(config-vlan)# state active
(config-vlan)# exit
(config)# interface gigabitethernet 1/0/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 20
(config-if)# switchport mac native vlan 10
(config-if)# mac-authentication port
(config-if)# exit
(config)# interface gigabitethernet 1/0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 20
(config-if)# exit
```

Specifies port 1/0/4, which is assigned to MAC VLAN ID 20 in dynamic VLAN mode, as an authentication port. This procedure then configures port 1/0/10 to be permitted access without the need for authentication.

(4) Configuring a terminal as an authentication-exempted terminal in dynamic VLAN mode

Use the following procedure to specify the MAC address of a terminal to be permitted access in dynamic VLAN mode without the need for authentication.

Points to note

Register the MAC address of an authentication-exempted terminal in a MAC VLAN and a MAC address table.

Command examples

1.
```
(config)# vlan 20 mac-based
(config-vlan)# mac-address 0012.e212.3456
(config-vlan)# exit
(config)# mac-address-table static 0012.e212.3456 vlan 20 interface gigabitethernet 1/0/10
```

   Specifies the MAC address of a terminal to be permitted access to MAC VLAN ID 20 through port 1/0/10 without the need for authentication.

(5) Configuring a MAC port with dot1q configured as an authentication-exempted port

Points to note

Configure the switch to exempt tagged frames received at a MAC port with dot1q configured from authentication.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/20
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 20
(config-if)# switchport mac native vlan 10
(config-if)# switchport mac dot1q vlan 100
(config-if)# mac-authentication port
(config-if)# mac-authentication dot1q-vlan force-authorized
(config-if)# exit
```

   Configures settings so that the tagged frames received at MAC-based authentication port 1/0/20 and destined for VLAN ID 100 are exempted from authentication.

11.2 Operation

11.2.1 List of operation commands

The following table describes the operation commands for MAC-based authentication.

Table 11-2: List of operation commands

Command name	Description
show mac-authentication login	Shows the MAC addresses currently authenticated by MAC-based authentication.
show mac-authentication logging	Shows the action log information for MAC-based authentication.
show mac-authentication	Shows the configuration for MAC-based authentication.
show mac-authentication statistics	Shows statistics.
clear mac-authentication auth-state mac-address	Forcibly clears the authentication status of authenticated terminals.
clear mac-authentication logging	Clears the action log information for MAC-based authentication.
clear mac-authentication statistics	Clears the statistics.
set mac-authentication mac-address	Registers a MAC address in the internal MAC-based authentication DB.
remove mac-authentication	Deletes a MAC address from the internal MAC-based authentication DB.
commit mac-authentication	Commits the internal MAC-based authentication DB to flash memory.
show mac-authentication mac-address	Shows the contents of the internal MAC-based authentication DB.
store mac-authentication	Backs up the internal MAC-based authentication DB.
load mac-authentication	Restores the internal MAC-based authentication DB from a backup file.
clear mac-authentication dead-interval-timer	Directs the switch to return to accessing the first RADIUS server, having moved on to another RADIUS server as a result of the dead interval function.
restart mac-authentication	Restarts the MAC-based authentication program.
dump protocols mac-authentication	Creates a dump file of information related to MAC-based authentication.

11.2.2 Displaying the MAC-based authentication configuration

You can use the "show mac-authentication" command to display the MAC-based authentication configuration.

Figure 11-5: MAC-based authentication configuration information

```
# show mac-authentication
Date 20XX/10/17 10:52:49 UTC
mac-authentication Information:
   Authentic-method : RADIUS        Accounting-state   : disable
   Dead-interval    : 10
   Syslog-send      : enable
   Force-Authorized : enable
   Auth-max-user    : 1024
```

```
   Authentic-mode   : Static-VLAN
        Max-timer   : 60                  Max-terminal : 1024
        Port Count  : 2                    Auto-logout : enable
   VLAN-check       : enable
         Vid-key    : %VLAN

   Authentic-mode   : Dynamic-VLAN
         Max-timer  : 60            Max-terminal : 256
         Port Count : 2              Auto-logout : enable

Port Information:
       Port               :    0/1
         Static-VLAN      :
            VLAN ID       :    5,10,15
            Auth type     :    force-authorized
         Dynamic-VLAN     :
            VLAN ID       :    1200,1500
            Native VLAN   :    10
            Forceauth VLAN:    1500
         Access-list-No   :    100
         Max-user         :    64

       Port               :    0/2
         Dynamic-VLAN     :
            VLAN ID       :    1300-1310
            Native VLAN   :    20
            Forceauth VLAN:    1300
         Access-list-No   :    100
         Max-user         :    64

       Port               :    0/10
         Static-VLAN      :
            VLAN ID       :    300,305
         Access-list-No   :    100
         Max-user         :    64
```

11.2.3 Displaying MAC-based authentication statistics

You can use the "show mac-authentication statistics" command to display the status of MAC-based authentication, and the status of communication with the RADIUS server.

Figure 11-6: Displaying MAC-based authentication statistics

```
# show mac-authentication statistics
Date 20XX/10/17 11:10:49 UTC
mac-authentication Information:
  Authentication Request Total :         100
  Authentication Current Count :          10
  Authentication Error Total   :          30
  Force Authorized Count       :          10
Unauthorized Information:
  Unauthorized Client Count    :           5
RADIUS mac-authentication Information:
[RADIUS frames]
             TxTotal   :       130  TxAccReq  :       130  TxError   :         0
             RxTotal   :       130  RxAccAccpt:       100  RxAccRejct:        30
                                    RxAccChllg:         0  RxInvalid :         0
Account mac-authentication Information:
[Account frames]
             TxTotal   :       100  TxAccReq  :       100  TxError   :         0
             RxTotal   :       100  RxAccResp :       100  RxInvalid :         0
Port Information:
  Port     User-count
   0/10      10/ 256
   0/12      10/1024
```

11.2.4 Displaying the status of MAC-based authentication sessions

You can use the "show mac-authentication login" command to display the status of MAC-based authentication sessions.

Figure 11-7: Displaying status information for MAC-based authentication

```
# show mac-authentication login
Date 20XX/10/17 10:52:49 UTC
Total client counts:2
F MAC address         Port    VLAN    Login time               Limit time  Mode
* 0012.e200.0001      0/1     3       20XX/10/15 09:58:04 UTC  00:10:20    Static
* 0012.e200.0002      0/10    4094    20XX/10/15 10:10:23 UTC  00:20:35    Dynamic
```

11.2.5 Creating an internal MAC-based authentication DB

After you set up the environment for the MAC-based authentication system and complete the configuration process, the next step is to create the internal MAC-based authentication DB. This section also describes how to make changes to the database contents.

(1) Registering MAC addresses

Use the "set mac-authentication mac-address" command to register a MAC address and VLAN ID for each MAC address that is subject to MAC-based authentication. The following example registers information for five MAC addresses:

Command input

```
# set mac-authentication mac-address 0012.e200.1234 100
# set mac-authentication mac-address 0012.e200.5678 100
# set mac-authentication mac-address 0012.e200.9abc 100
# set mac-authentication mac-address 0012.e200.def0 100
# set mac-authentication mac-address 0012.e200.0001 100
```

(2) Deleting MAC address information

The command below deletes a MAC address registered in the database.

Command input

```
# remove mac-authentication mac-address 0012.e200.1234
Removes the MAC address 0012.e200.1234 from the database.
```

(3) Applying changes to the internal MAC-based authentication DB

The "commit mac-authentication" command applies the changes you made using the "set mac-authentication mac-address" and "remove mac-authentication mac-address" commands to the internal MAC-based authentication DB.

Command input

```
# commit mac-authentication
```

11.2.6 Backing up the internal MAC-based authentication DB

This section describes how to back up the internal MAC-based authentication DB and restore the database from the backup file.

(1) Backing up the internal MAC-based authentication DB

Use the "store mac-authentication" command to back up the contents of the internal MAC-based authentication DB to a file (named backupfile in the example below).

Command input

```
# store mac-authentication backupfile
Backup mac-authentication MAC address data.  Are you sure? (y/n): y
#
```

(2) Restoring the internal MAC-based authentication DB

Use the "load mac-authentication" command to re-create the internal MAC-based authentication DB from the contents of the backup file (named backupfile in the example below).

Command input

```
# load mac-authentication backupfile
Restore mac-authentication MAC address data.  Are you sure? (y/n): y
#
```

11.2.7 Restoring access to the first RADIUS server after intervention by the dead interval function

If the first RADIUS server becomes unresponsive, the dead interval function causes the switch to start using the second or later RADIUS server. In this case, you can direct the switch to resume use of the first RADIUS server before the time specified by the "authentication radius-server dead-interval" configuration command has elapsed, by executing the "clear mac-authentication dead-interval-timer" command.

Figure 11-8: Restoring access to the first RADIUS server

```
# clear mac-authentication dead-interval-timer
#
```

12 DHCP Snooping

DHCP snooping monitors the DHCP packets that pass through the Switch to restrict access from untrusted terminals. DHCP snooping is used on IPv4 networks.

This chapter provides an overview of DHCP snooping and describes its use.

12.1 Description

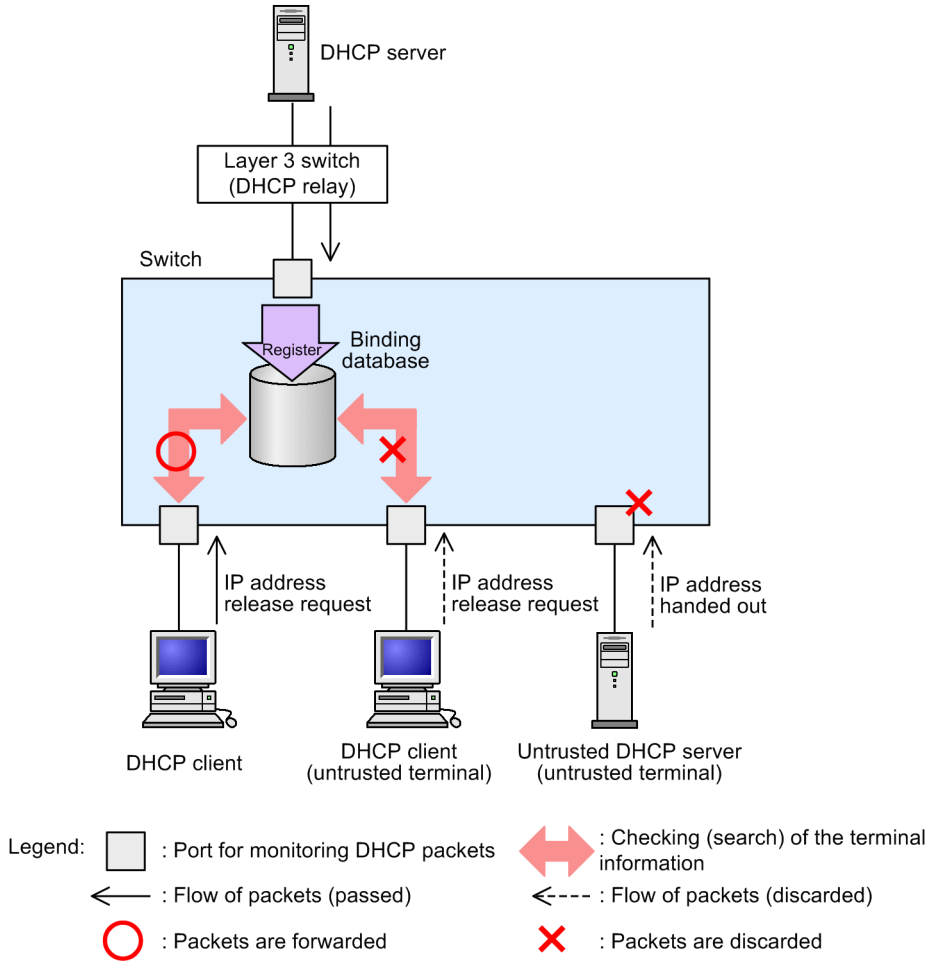
12.1.1 Overview

DHCP snooping monitors the DHCP packets that pass through the Switch to restrict access from untrusted terminals.

DHCP snooping also supports terminal filters, which limit the IPv4 packets from untrusted terminals, and dynamic ARP inspection, which discards invalid ARP packets.

To enable DHCP snooping, place the Switch between the DHCP server and DHCP clients as shown in the following figure.

Figure 12-1: Overview of DHCP snooping



Terminal information is registered in a binding database.

The following table describes the function provided by DHCP snooping.

Table 12-1: Function provided by DHCP snooping

Item	Description
Monitoring DHCP packets	• Monitors the DHCP clients that received IP addresses distributed by a DHCP server and manages terminal information in a binding database.
Registration of terminals with a fixed IP address	• Statically registers terminal information in a binding database.
Saving a binding database	• Saves a binding database and restores it when the Switch restarts.
Inspecting DHCP packets	• Untrusted DHCP servers from distributing IP addresses • Prevents untrusted DHCP clients from releasing IP addresses • Prevents MAC address spoofing • Prevents Option 82 spoofing
Limiting the rate of DHCP packet reception	• Discards DHCP packets that exceed the predetermined reception rate.
Terminal filter	• Prohibits the forwarding of IPv4 packets from untrusted terminals.
Inspecting ARP packets	• Prohibits the forwarding of ARP packets from untrusted terminals. • Prevents MAC address and IP address spoofing.
Limiting the rate of ARP packet reception	• Discards ARP packets that exceed the predetermined reception rate.

12.1.2 Monitoring DHCP packets

(1) Port type

DHCP snooping categorizes ports as follows when it monitors DHCP packets:

- trusted port

  A port is trusted when a trusted terminal is connected to it, such as DHCP servers and department servers.

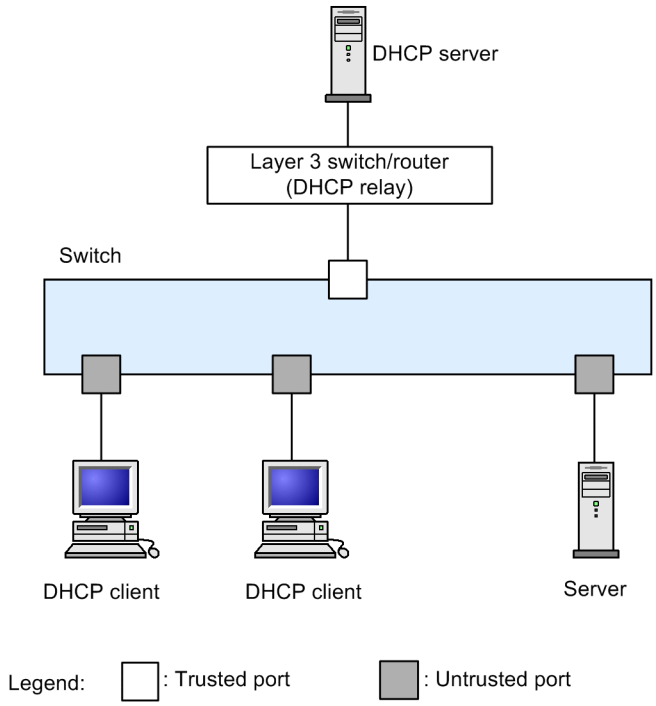
- untrusted port

  A port is untrusted when an untrusted terminal is connected to it, such as DHCP clients.

  Do not connect DHCP servers to untrusted ports.

The following figure shows the two port categories used when dynamic ARP inspection is enabled and an example of devices connected to such ports.

Figure 12-2: Port categories



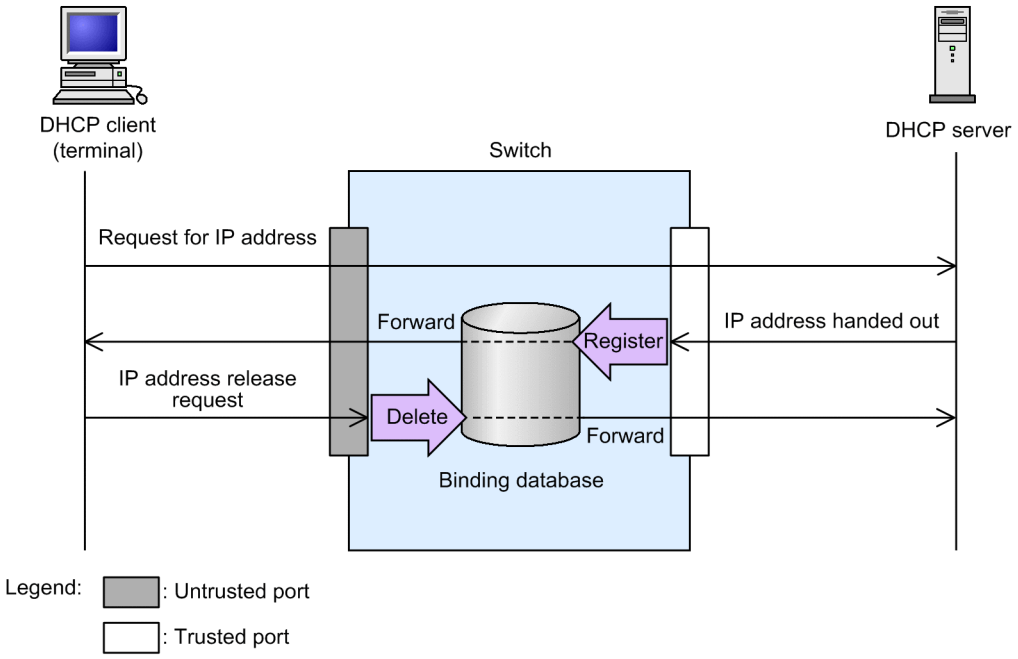
When you use the "ip dhcp snooping" configuration command to enable DHCP snooping, all the ports become untrusted by default. Set the port to which a DHCP server is connected as a trusted port. To do so, use the "ip dhcp snooping trust" configuration command.

Note that DHCP snooping monitors the VLANs that have been set by using the "ip dhcp snooping vlan" configuration command.

(2) Learning terminal information

The following figure provides an overview of how the Switch learns terminal information.

Figure 12-3: Overview of learning terminal information



The switch monitors the packets received on the trusted port from the DHCP server. When the DHCP server distributes an IP address, the switch registers the terminal information in the binding database. The terminal information of the terminal connected to the untrusted port is registered to the binding database.

The switch also monitors the request for release of packets received on the untrusted port from the DHCP client. When the DHCP client issues an IP address, the switch deletes the terminal information from the binding database.

Two methods are available for registering information in a binding database:

- Dynamic registration

  The switch registers terminal information when an IP address is distributed from a DHCP server.

  Usually, the Switch use dynamic registration to register terminal information.

- Static registration

  You can use the "ip source binding" configuration command to register terminal information.

  You usually use static registration to connect a server (such as a department server) with a fixed IP address to an untrusted port. You can permit communication by statically registering terminal information in the binding database.

The following table describes the types of terminal information that are registered in a binding database.

Table 12-2: Terminal information registered in a binding database

Item	Dynamic registration	Static registration
Terminal MAC address.	MAC address of a DHCP client	MAC address of a terminal with a fixed IP address
Terminal IP address.	IP address distributed by the DHCP server	IP address of a terminal with a fixed IP address

Item	Dynamic registration	Static registration
	The addresses in the following ranges are available: • 1.0.0.0 to 126.255.255.255 • 128.0.0.0 to 223.255.255.255	
VLAN containing the terminal	ID of the VLAN containing the port or channel group to which the terminal is connected	
Number of the port to which the terminal is connected	Number of the port or channel group to which the terminal is connected	
Aging time	Length of time until an entry is deleted due to aging. The lease time of the IP address distributed by the DHCP server is used for this item.	Aging is not applicable.

(3) Saving a binding database

Use configuration commands to save a binding database and to restore it when the Switch is restarted.

(a) Running conditions for saving a binding database

To save a binding database, use the "ip dhcp snooping database url" configuration command.

The saving of the binding database starts when the save delay time in the configuration information expires.

(b) Saving the database when the save delay time expires

The save delay time refers to the period of time between the point at which saving of the binding database is specified (called a save event) and the point at which saving of the binding database actually starts at the save location. The save delay timer starts when one of the following save events occurs and the saving of the binding database to the specified save location starts when the timer expires:

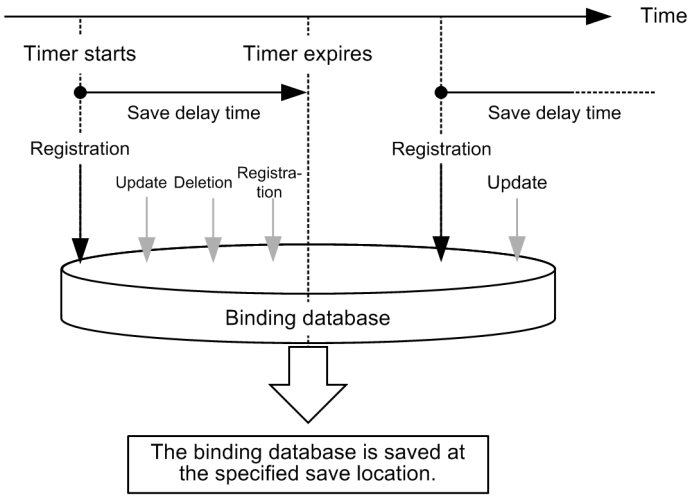
- When terminal information is dynamically registered, updated, or deleted in a binding database
- When the "ip dhcp snooping database url" configuration command is specified (includes a change of save location)
- When the "clear ip dhcp snooping binding" operation command is executed

To set the save delay time, use the "ip dhcp snooping database write-delay" configuration command.

When the save delay timer starts due to a save event, the timer does not stop until it expires. Even if terminal information is registered, updated, or deleted in the binding database before the timer expires, the timer will not be restarted.

The following figure shows the relationship between save events and the save delay time. In this figure, the save event is the registration of terminal information in the binding database.

Figure 12-4: Save events and save delay time



(c) Save location for the binding database

As the save location for the binding database, you can select either internal flash memory or an external memory card. To set the save location, use the "ip dhcp snooping database url" configuration command.

The items that are saved are all the entries in the binding database that exist at the time of the current write operation. The saved items will be overwritten by the next write operation.

(d) Restoring a saved binding database

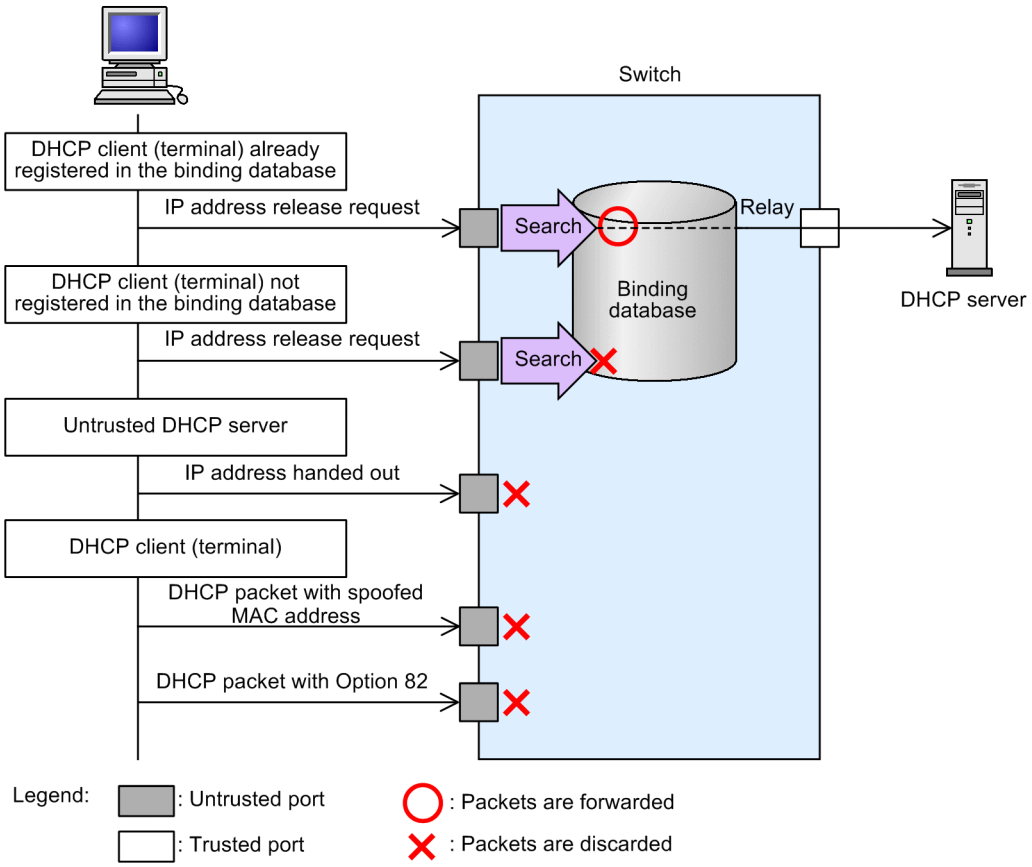
The saved binding database is restored when the Switch is started. The database will be restored only if both of the following conditions are met when the switch is started:

- The save location has been set by using the "ip dhcp snooping database url" configuration command.
- If the save location is an external memory card, the applicable card has been inserted.

(4) Inspecting DHCP packets

The following figure provides an overview of DHCP packet inspection.

Figure 12-5: Overview of DHCP packet inspection



The switch monitors the DHCP packets from terminals that are connected to untrusted ports to prevent the following:

- Untrusted DHCP servers from distributing IP addresses

  When the Switch receives a DHCP packet on an untrusted port from an untrusted DHCP server, the switch discards the DHCP packet, which prevents untrusted DHCP servers from distributing IP addresses.

- Prevents untrusted DHCP clients from releasing IP addresses

  When the Switch receives an IP address release request on an untrusted port from a terminal that is not registered in the binding database, the Switch discards the DHCP packet, which prevents the release of IP addresses from terminals that are given IP addresses by illegitimate DHCP servers.

  Similarly, when the Switch receives a duplicated IP address report, lease time update, or request for optional information, the Switch discards the DHCP packet which prevents untrusted DHCP clients from illegally releasing IP addresses, acquiring IP addresses, or acquiring optional information.

- Prevents MAC address spoofing

  When the Source MAC Address in a DHCP packet received on an untrusted port does not match the client hardware address (chaddr) in the DHCP packet, the Switch discards the DHCP packet, which prevents MAC address spoofing.

- Prevents Option 82 spoofing

  When data is added in the Option 82 field in a DHCP packet received on an untrusted port, the Switch discards the DHCP packet which prevents Option 82 spoofing.

12.1.3 Limiting the rate of DHCP packet reception

When DHCP snooping is enabled, the Switch discards the DHCP packets that exceed the predetermined reception rate during monitoring of received DHCP packets.

To set the reception rate, use the "ip dhcp snooping limit rate" configuration command. The reception rate has no limit if a limit has not been set with this command.

When a limit is applied to the DHCP packet reception rate, the limit is applied to all DHCP packets received by the Switch.

DHCP packets exceeding the rate are discarded, and the incident is logged in the operation log. However, SNMP notifications are not sent. To check the information in the operation log, execute the show "ip dhcp snooping logging" operation command.

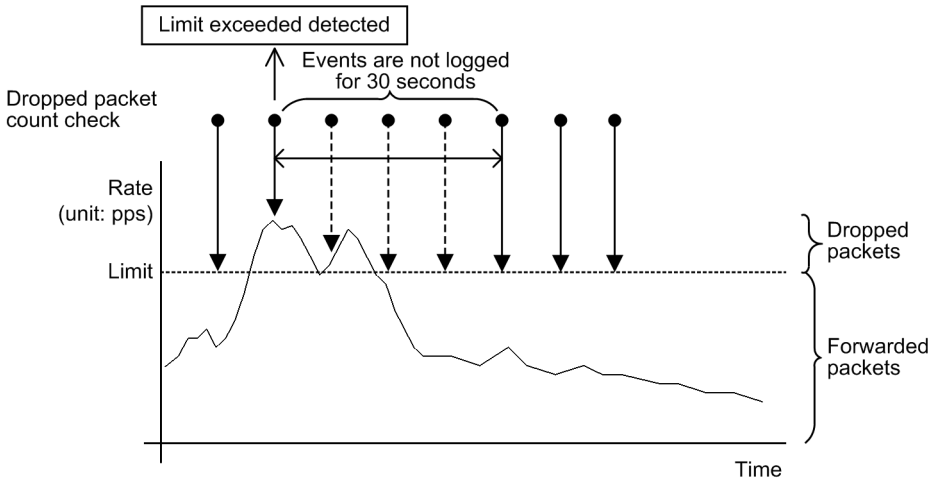
(1) Events logged in the operation log

The operation log records Limit Exceeded events. A Limit Exceeded event occurs when the configured reception rate is exceeded.

For 30 seconds after a Limit Exceeded event is logged, no events will be logged, even if packets are discarded, because the rate has been exceeded.

The following figure shows the point at which a Limit Exceeded event for the DHCP packet reception rate is logged in the operation log.

Figure 12-6: Point at which a Limit Exceeded event for the DHCP packet reception rate is logged in the operation log



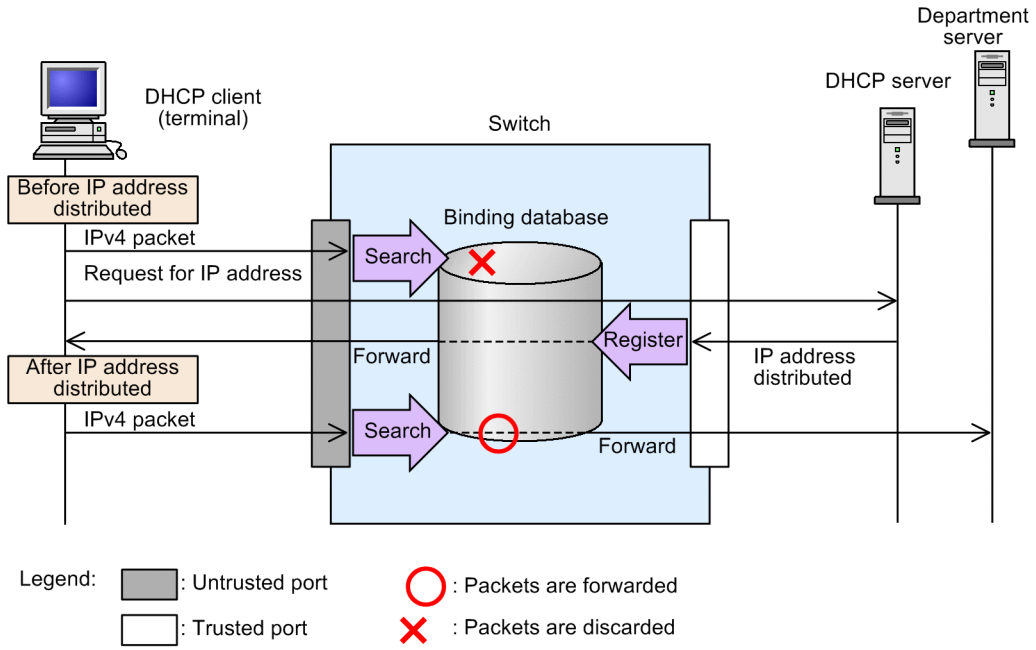
12.1.4 Terminal filter

(1) Overview

A terminal filter monitors the IPv4 packets that pass through the Switch and limits access from untrusted terminals.

The following figure provides an overview of how a terminal filter works.

Figure 12-7: Overview of terminal filtering



You can set a terminal filter for each port by using the "ip verify source" configuration command.

To use terminal filters, the applicable mode (custom with layer3-dhcp-1, layer3-suppress-dhcp-1, or dhcp-filter) must have already been set for the receiving-side flow detection mode.

(2) Inspecting IPv4 packets

If the switch receives an IPv4 packet on an untrusted port, the switch checks whether the source of the packet is in the binding database. If the packet comes from an unregistered terminal, the switch discards the IPv4 packet.

The following table describes the items checked by a terminal filter.

Table 12-3: Items checked by terminal filtering

Filtering to be performed	IPv4 packet			
	Receiving interface		Ethernet header	IP headers
	Port	VLAN ID	Source MAC address	Source IP address
Check source MAC addresses only	Y	Y	Y	—
Check source IP addresses only	Y	Y	—	Y
Check source MAC addresses and source IP addresses	Y	Y	Y	Y

Legend: Y: Checked, —: Not checked

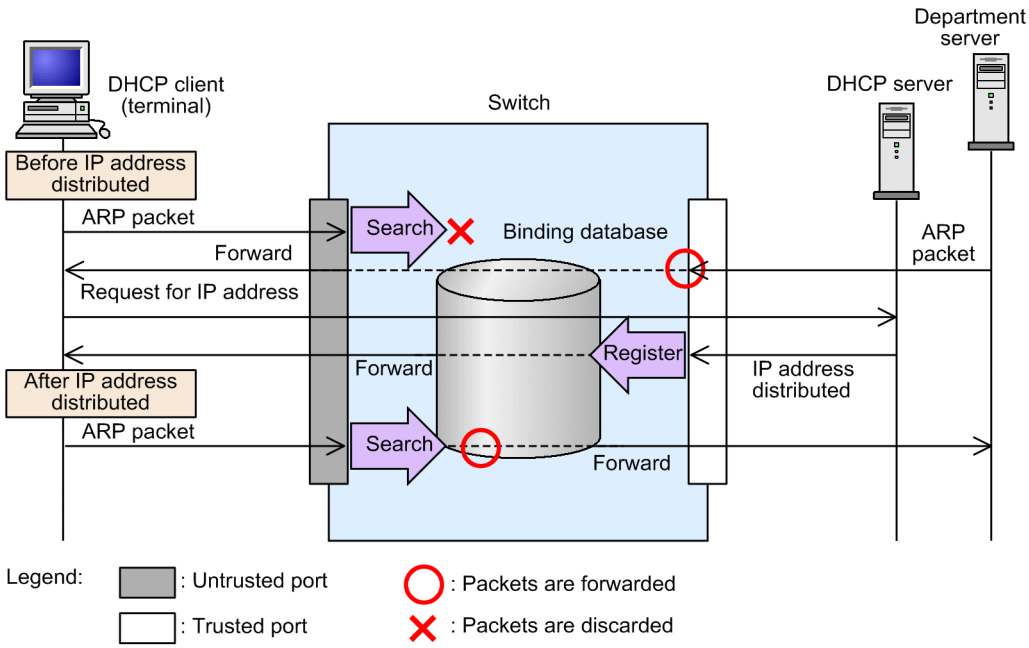
12.1.5 Dynamic ARP inspection

(1) Overview

Dynamic ARP inspection monitors the ARP packets that pass through the Switch to restrict access of ARP packets from untrusted terminals.

The following figure provides an overview of how dynamic ARP inspection works.

Figure 12-8: Overview of dynamic ARP inspection



(2) Port type

Like DHCP snooping, dynamic ARP inspection categorizes ports as follows when it monitors ARP packets:

- trusted port

  A port is trusted when a trusted terminal is connected to it, such as DHCP servers and department servers.

  Dynamic ARP inspection does not monitor ARP packets that are received on trusted ports.

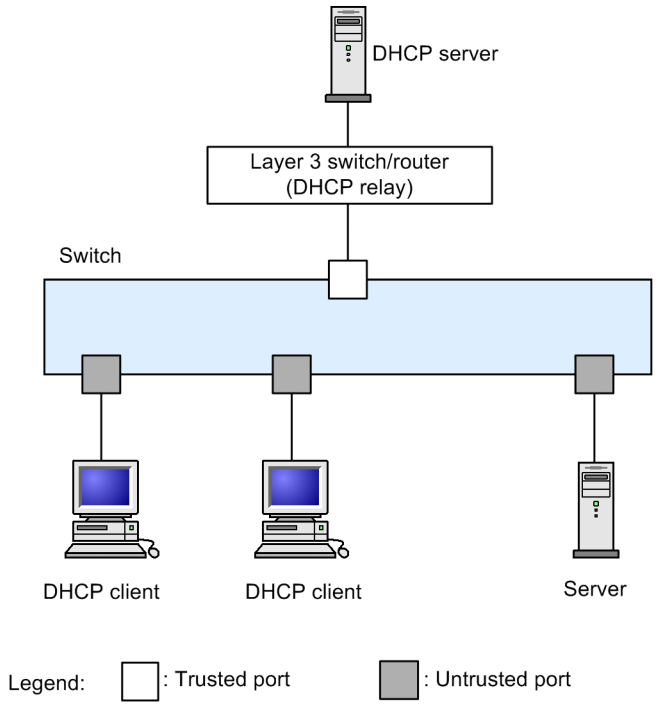
- untrusted port

  A port is untrusted when an untrusted terminal is connected to it, such as DHCP clients.

  Do not connect DHCP servers to untrusted ports.

The following figure shows the two port categories used when dynamic ARP inspection is enabled and an example of devices connected to such ports.

Figure 12-9: Port categories



When you use the "ip dhcp snooping" configuration command to enable DHCP snooping, all the ports become untrusted by default. Set the port to which a DHCP server is connected as a trusted port. You can set ports as trusted by using the "ip arp inspection trust" configuration command.

Note that dynamic ARP inspection monitors the VLANs that are specified by using the "ip arp inspection vlan" configuration command.

For normal operations, we recommend that you specify the same ports in both the "ip dhcp snooping trust" and "ip arp inspection trust" configuration commands.

(3) Basic inspection of ARP packets

When the switch receives an ARP packet on an untrusted port, the switch checks whether the source of the packet is in the binding database. If the packet comes from an unregistered terminal, the switch discards the packet.

The following table describes the basic inspection items.

Table 12-4: Basic inspection Items

ARP type	Receiving interface		ARP packet					
			Ethernet header		ARP headers			
	Port	VLAN ID	Destination MAC address	Source MAC address	Source MAC address	Source IP address	Destination MAC address	Destination IP address
Request	Y	Y	—	—	Y	Y	—	—
Reply	Y	Y	—	—	Y	Y	—	—

Legend: Y: Checked, —: Not checked

(4) Optional inspection of ARP packets

Optionally, the switch can check the integrity of data in the ARP packets received on untrusted ports.

To set optional inspection, use the "ip arp inspection validate" configuration command.

(a) Source MAC address inspection (src-mac option)

When the src-mac option is specified, the switch checks whether the source MAC address in the Layer 2 header matches the source MAC address in the ARP header.

This inspection is performed on both ARP Requests and ARP Replies.

The following table describes the items that are checked in the source MAC address inspection.

Table 12-5: Items checked by source MAC address inspection

ARP type	Receiving interface		ARP packet					
			Ethernet header		ARP headers			
	Port	VLAN ID	Destination MAC address	Source MAC address	Source MAC address	Source IP address	Destination MAC address	Destination IP address
Request	—	—	—	Y	Y	—	—	—
Reply	—	—	—	Y	Y	—	—	—

Legend: Y: Checked, —: Not checked

(b) Destination MAC address inspection (dst-mac option)

When the dst-mac option is specified, the switch checks whether the Destination MAC address in the Layer 2 header matches the Target MAC Address in the ARP header.

This inspection is performed on ARP Replies only.

The following table describes the items that are checked in the destination MAC address inspection.

Table 12-6: Items checked by destination MAC address inspection

ARP type	Receiving interface		ARP packet					
			Ethernet header		ARP headers			
	Port	VLAN ID	Destination MAC address	Source MAC address	Source MAC address	Source IP address	Destination MAC address	Destination IP address
Request	—	—	—	—	—	—	—	—
Reply	—	—	Y	—	—	—	Y	—

Legend: Y: Checked, —: Not checked

(c) IP address inspection (ip option)

When the ip option is specified, the switch checks whether the Target IP Address in the ARP header is within either of the following ranges:

- 1.0.0.0 to 126.255.255.255
- 128.0.0.0 to 223.255.255.255

This inspection is performed on ARP Replies only.

The following table describes the items that are checked in the IP address inspection.

Table 12-7: Items checked by IP address inspection

ARP type	Receiving interface		ARP packet					
			Ethernet header		ARP headers			
	Port	VLAN ID	Destination MAC address	Source MAC address	Source MAC address	Source IP address	Destination MAC address	Destination IP address
Request	—	—	—	—	—	—	—	—
Reply	—	—	—	—	—	—	—	Y

Legend: Y: Checked, —: Not checked

12.1.6 Limiting the rate of ARP packet reception

The Switch discards ARP packets that exceed a predetermined reception rate during monitoring of received ARP packets when dynamic ARP inspection is enabled.

To set the reception rate, use the "ip arp inspection limit rate" configuration command. The reception rate has no limit if a limit has not been set with this command.

When a limit is applied to the ARP packet reception rate, the limit is applied to all ARP packets received by the Switch.

The ARP packets exceeding the rate are discarded, and the incident is logged in the operation log. However, SNMP notifications are not sent. To check the information in the operation log, execute the "show ip dhcp snooping logging" operation command.

(1) Events logged in the operation log

The events logged in the operation log are the same as those logged when a limit is applied to the DHCP packet reception rate.

For details about the events logged in the operation log, see "(1) Events logged in the operation log in 12.1.3 Limiting the rate of DHCP packet reception".

12.1.7 Notes on using DHCP snooping

(1) When used with the Layer 2 switch function

See "Configuration Guide Vol. 1, 22.3 Compatibility between the Layer 2 switch function and other functions".

(2) When used with Layer 2 authentication

(a) When used with Web-based authentication

For details, see "5.2.1 Using Layer 2 authentication with other functions".

(b) Notes on configuring the authentication IPv4 access list

When you enable DHCP snooping and use the authentication IPv4 access list, if you specify the protocol name bootps or bootpc as a filtering condition in the authentication IPv4 access list, the packets of both bootps and bootpc are passed regardless of other filter conditions.

(c) When used with port mirroring

If DHCP snooping is enabled, DHCP packets sent by the Switch are not mirrored. If dynamic ARP inspection is also enabled in addition to DHCP snooping, ARP packets sent by the Switch are not mirrored, either.

(3) When used with policy-based routing

If packets with a protocol name of bootps or bootpc are subject to policy-based routing, all of those packets that pass through the Switch are forwarded based on the routing information of the routing protocol instead of the routing information of policy-based routing.

(4) Notes on saving and restoring a binding database

- If the "ip dhcp snooping database url" configuration command has not been specified (initial status), the binding database will not be saved. Therefore, stopping or restarting the switch will erase the registered binding database, disabling communication from DHCP clients. If this occurs, release and update the IP addresses on the DHCP clients. In Windows, for example, in the Command Prompt window, execute ipconfig /release and then execute ipconfig /renew.

  This re-registers terminal information in the binding database and enables communication by DHCP clients.
- When you restore a binding database, entries that have exceeded the lease time of the DHCP server will not be restored. If you change the time settings of the switch before you stop or restart the switch, the binding database might not be correctly restored when the switch starts.
- When you use the "ip source binding" configuration command to statically register entries, the entries will be restored based on the startup configuration.
- If you have saved the binding database on an external memory card, do not remove the memory card until a prompt appears on the screen after the switch starts.

(5) Notes on limiting the rate of DHCP packet reception

- When both the DHCP packet reception rate and the ARP packet reception rate have limits, the switch monitors packets for the total value of both limits.

(6) Notes on dynamic ARP inspection

- Dynamic ARP inspection can be enabled only after the following configuration commands have been executed and a binding database has been generated:
  - ip dhcp snooping
  - ip dhcp snooping vlan
- Dynamic ARP inspection also checks the entries that are statically registered in a binding database by using ip source binding.
- Dynamic ARP inspection cannot be used when the receiving-side flow detection mode is set to IP unset VLAN suppression mode.

(7) Notes on limiting the rate of ARP packet reception

- When both the ARP packet reception rate and the DHCP packet reception rate have limits, the switch monitors packets for the total value of both limits.

12.2 Configuration

12.2.1 List of configuration commands

The following table describes the configuration commands for DHCP snooping.

Table 12-8: List of configuration commands

Command name	Description
ip arp inspection limit rate	Specifies a limit on the rate of ARP packet reception on the Switch.
ip arp inspection trust	Specifies a port to which a trusted terminal is connected (when dynamic ARP inspection is enabled).
ip arp inspection validate	Specifies dynamic ARP inspection options.
ip arp inspection vlan	Specifies a VLAN that will use dynamic ARP inspection.
ip dhcp snooping	Enables DHCP snooping.
ip dhcp snooping database url	Specifies where a binding database is to be saved.
ip dhcp snooping database write-delay	Specifies the save delay time to be applied when a binding database is saved.
ip dhcp snooping information option allow-untrusted	Disable the Option 82 spoofing check for DHCP packets.
ip dhcp snooping limit rate	Specifies a limit on the rate of DHCP packet reception on the Switch.
ip dhcp snooping logging enable	This step configures the output of operation logs on the syslog server.
ip dhcp snooping loglevel	Specifies the level of messages to be logged in an action log.
ip dhcp snooping trust	Specifies a port to which a trusted terminal is connected when DHCP snooping is enabled.
ip dhcp snooping verify mac-address	Disables the MAC address spoofing check for DHCP packets.
ip dhcp snooping vlan	Specifies a target VLAN for DHCP snooping.
ip source binding	Registers a terminal with a fixed IP address in the binding database.
ip verify source	Specifies the port that uses terminal filters.

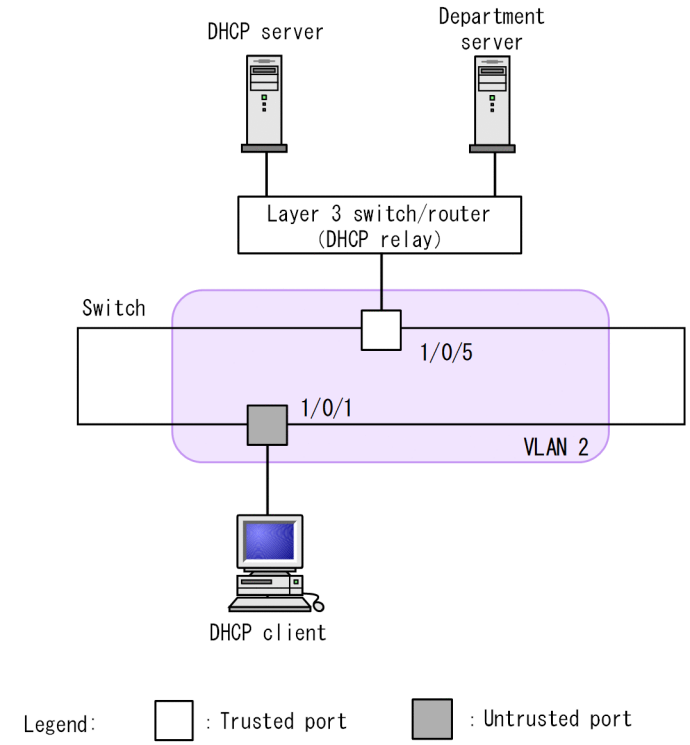
12.2.2 Basic configuration

This subsection describes the basic configuration for using DHCP snooping.

Before you use DHCP snooping, you need to use the "flow detection mode" configuration command to set the applicable receiving-side flow detection mode.

The following figure shows an example of a basic configuration for DHCP snooping.

Figure 12-10: Basic configuration for DHCP snooping



(1) Enabling DHCP snooping

Points to note

Enable DHCP snooping on the entire switch and specifies the VLAN where DHCP snooping needs to be enabled.

Command examples

1. `(config)# ip dhcp snooping`

   Enables DHCP snooping on the entire switch.

2. `(config)# vlan 2`

   `(config-vlan)# exit`

   `(config)# ip dhcp snooping vlan 2`

   Enables DHCP snooping on VLAN ID 2. DHCP snooping is enabled only on the VLANs that are specified by using this command.

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

   `(config-if)# switchport mode access`

   `(config-if)# switchport access vlan 2`

   `(config-if)# exit`

   Sets port 1/0/1 as an access port, and sets VLAN ID 2 as the VLAN containing port 1/0/1.

(2) Setting a trusted port for DHCP snooping

Points to note

Set the port to which a DHCP server is connected (port to which the Layer 3 switch/router is connected in "Figure 12-10: Basic configuration for DHCP snooping") as a trusted port.

Command examples

1. (config)# interface gigabitethernet 1/0/5
   (config-if)# ip dhcp snooping trust
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# exit
   Sets port 1/0/5 as a trusted port. Other ports are untrusted. The sequence also sets port 1/0/5 as an access port and sets VLAN ID 2 as the VLAN containing port 1/0/5.

(3) Setting where the binding database is to be saved

(a) Saving the binding database in internal flash memory

Points to note

Set internal flash memory as the location for saving the binding database.

Command examples

1. (config)# ip dhcp snooping database url flash
   Sets internal flash memory as the save location.

(b) Saving a binding database on an external memory card

Points to note

Set an external memory card as the location for saving a binding database. If you set an external memory card, you can specify the name of the file for saving the database.

Command examples

1. (config)# ip dhcp snooping database url mc dhcpsn-db
   Sets an external memory card as the save location and sets dhcpsn-db as the name of the file for saving the binding database.

Notes

Before you set an external memory card as the save location, make sure a card is already inserted in the memory card slot on the Switch. In addition, use memory cards manufactured by ALAXALA.

(4) Setting a save delay time to be applied before the binding database is saved

Points to note

Set a save delay time to be applied before a binding database is saved.

Command examples

1. (config)# ip dhcp snooping database write-delay 3600
   Sets 3600 seconds as the length of time to wait after one of the following save events occurs before saving actually starts:

- When terminal information is dynamically registered, updated, or deleted in the binding database
- When the "ip dhcp snooping database url" configuration command is specified (includes a change of save location)
- When the "clear ip dhcp snooping binding" operation command is executed

Notes

The length of time set by this command becomes operationally effective from the next save event.

12.2.3 Limiting the rate of DHCP packet reception

The following describes how to limit the rate of DHCP packet reception.

Points to note

Set the rate at which the Switch receives DHCP packets from terminals.

Command examples

1. `(config)# ip dhcp snooping limit rate 50`
   Set 50 packets per second as the reception rate for the Switch.

12.2.4 Terminal filter

The following describes how to configure a terminal filter.

Points to note

Configure a terminal filter on a port to which a DHCP client is connected.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# ip verify source port-security
(config-if)# exit
```
   Configures a terminal filter on port 1/0/1 and sets the source IP addresses and source MAC addresses as the filter conditions.

Notes

If you specify the "ip verify source" configuration command for trusted ports, terminal filters are not enabled. Also note that when DHCP snooping is enabled, terminal filters are enabled for VLANs that are not specified by using the "ip dhcp snooping vlan" configuration command.

12.2.5 Dynamic ARP inspection

The following describes how to configure dynamic ARP inspection.

(1) Basic configuration

Points to note

Set the VLAN for which basic dynamic ARP inspection is to be enabled.

Command examples

1. `(config)# ip arp inspection vlan 2`

Sets VLAN ID 2 as a VLAN subject to dynamic ARP inspection. Dynamic ARP inspection will be performed only for VLANs set by using this command.

Notes

- Specify the VLAN ID that was set by using the "ip dhcp snooping vlan" configuration command.
- When you specify this command, the entries registered in the binding database by using the "ip source binding" configuration command also become subject to dynamic ARP inspection.
- If you specify this command for a port belonging to the VLAN set by using the "ip arp inspection vlan" configuration command, dynamic ARP inspection will not be used to check the port.

(2) Setting a trusted port

Points to note

Set the port to which the DHCP server is connected as a trusted port.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/5
(config-if)# ip arp inspection trust
(config-if)# exit
```
Sets port 1/0/5 as a trusted port. Other ports are untrusted.

Notes

If the ports that are set by using this command belong to a VLAN subject to dynamic ARP inspection, dynamic ARP inspection will not be performed for those ports.

(3) Setting dynamic ARP inspection options

Points to note

Enable the source MAC address inspection (src-mac option) as an optional check of dynamic ARP inspection of the Switch.

Command examples

1.
```
(config)# ip arp inspection validate src-mac
```
Enables the source MAC address inspection (src-mac option) as an optional check.

12.2.6 Limiting the rate of ARP packet reception

The following describes how to limit the rate of ARP packet reception.

Points to note

Set the rate at which the Switch receives ARP packets.

Command examples

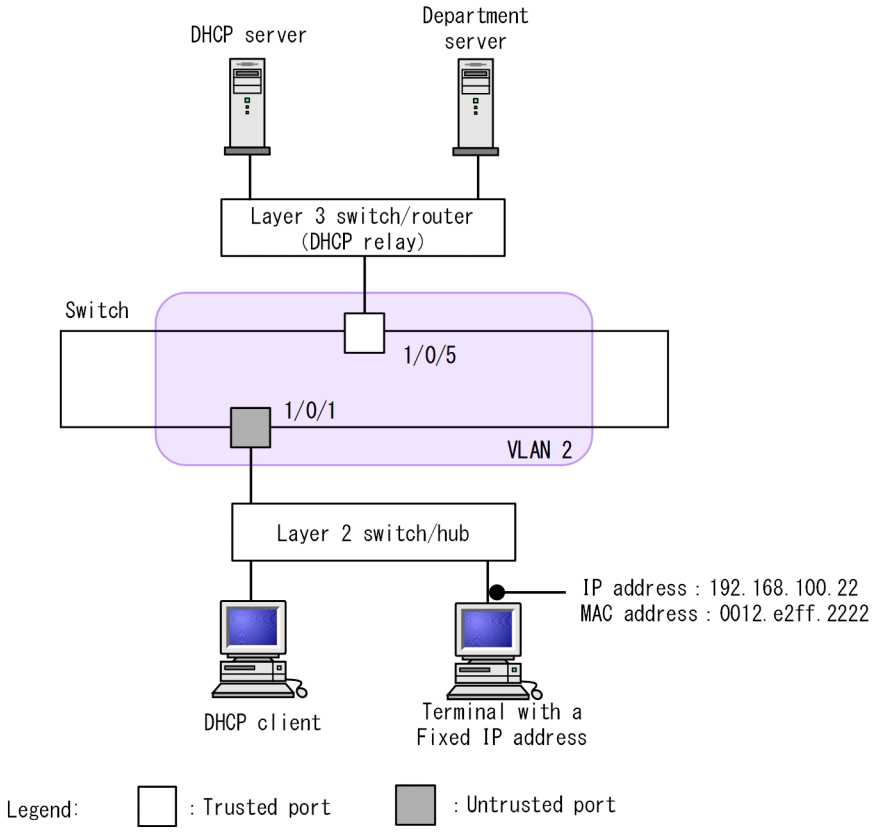
1.
```
(config)# ip arp inspection limit rate 100
```
Set 100 packets per second as the reception rate for the Switch.

12.2.7 Connecting a terminal with a fixed IP address

The following describes how to connect a terminal with a fixed IP address to the Switch.

The figure below shows an example configuration when a terminal with a fixed IP address is connected to the Switch.

Figure 12-11: Example configuration when a terminal with a fixed IP address is connected



You can configure DHCP snooping as described in "12.2.2 Basic configuration". In the example here, the terminal with a fixed IP address is connected to an untrusted port, and must therefore be statically registered in the binding database.

Points to note

Statically register the terminal information of the terminal with a fixed IP address in the binding database.

Command examples

1. `(config)# ip source binding 0012.e2ff.2222 vlan 2 192.168.100.22 interface gigabitethernet 1/0/1`

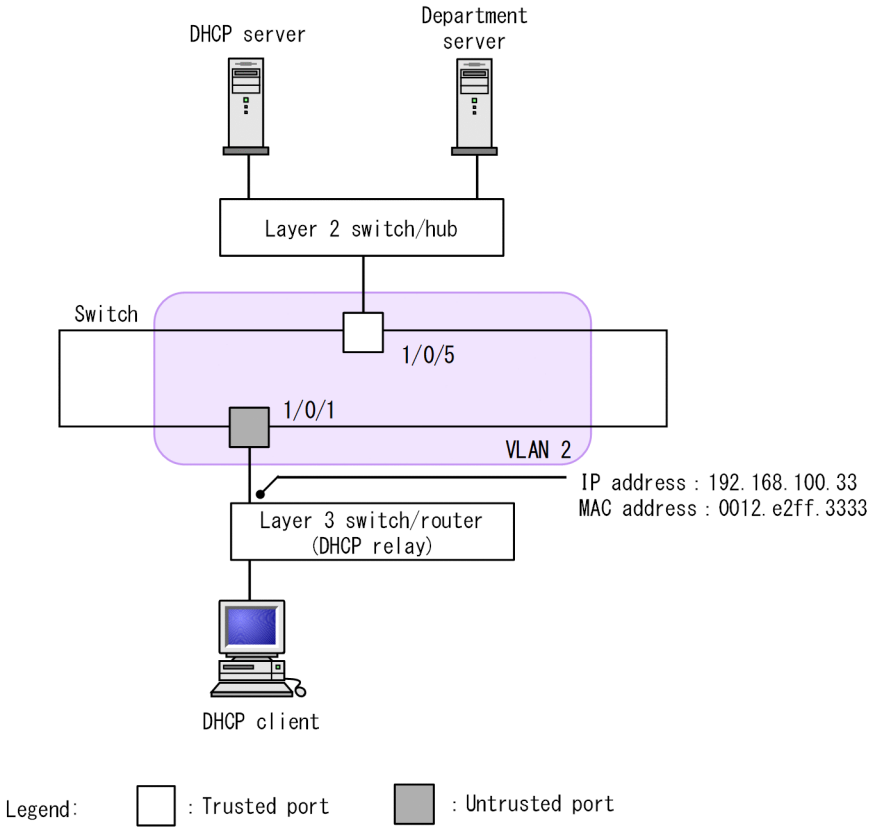
   Enters the MAC address of the terminal, the VLAN (VLAN ID) containing the terminal, the IP address of the terminal, and the number of the port to which the terminal is connected in the binding database.

12.2.8 Connecting a DHCP relay under the Switch

When you connect a DHCP relay under the Switch, configure the switch so that it can forward the packets.

The following figure shows an example configuration when a DHCP relay is connected under the Switch.

Figure 12-12: Example configuration when a DHCP relay is connected under the Switch



Configure DHCP snooping on the Switch as described in "12.2.2 Basic configuration", "12.2.4 Terminal filter", and "12.2.5 Dynamic ARP inspection".

In the example here, the DHCP packets and IPv4 packets from the DHCP client cannot be relayed. In addition, the ARP packets from the Layer 3 switch/router cannot be relayed.

To relay the packets, you need to permit the forwarding of DHCP packets, IPv4 packets, and ARP packets on the Switch.

(1) Permitting the forwarding of DHCP packets

Points to note

Because the source MAC addresses in the packets sent from the DHCP client are rewritten by the Layer 3 switch/router (DHCP relay), disables the MAC address spoofing check for DHCP packets.

Command examples

1. `(config)# no ip dhcp snooping verify mac-address`

   Disable the MAC address spoofing check for the DHCP packets received on the untrusted port.

Notes

If this command is not specified, the Switch performs the MAC address spoofing check, in which case the DHCP relay cannot be connected to the untrusted port.

(2) Permitting the forwarding of IPv4 packets

Points to note

Because the source MAC addresses in the packets sent from the DHCP client are rewritten by the Layer 3 switch/router (DHCP relay), configures a terminal filter on the untrusted port and sets only source IP addresses as the filter conditions.

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(config-if)# ip verify source
(config-if)# exit
```
Configures a terminal filter on port 1/0/1, and sets only source IP addresses as the filter conditions.

(3) Permitting the forwarding of ARP packets

The configuration for permitting the forwarding of ARP packets is the same as the configuration when a terminal with a fixed IP address is connected.

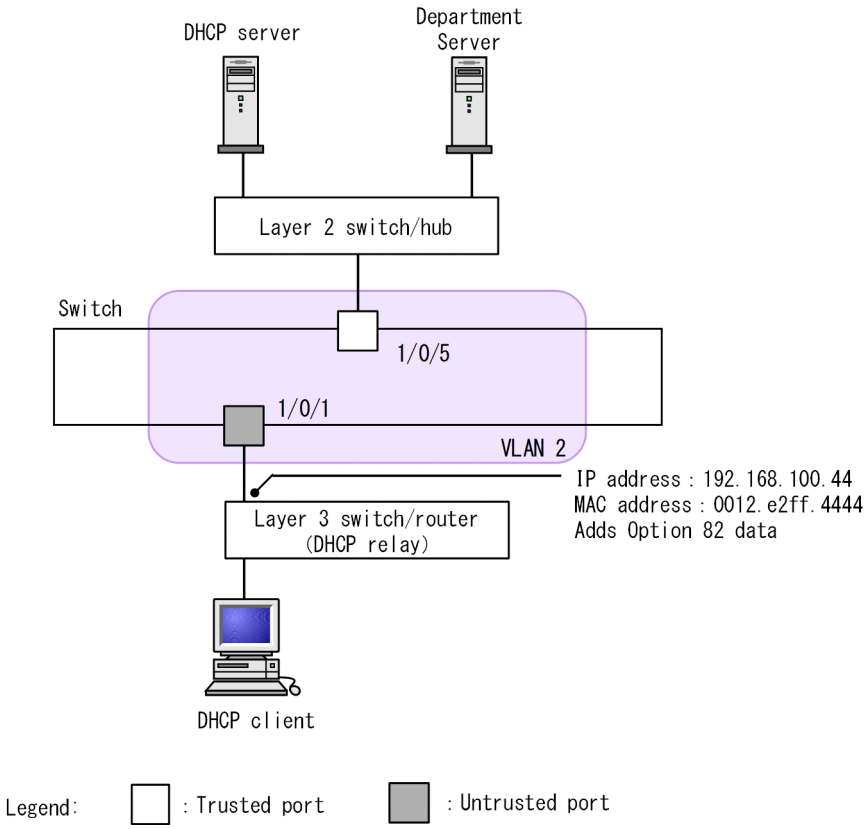
For details about the configuration, see "12.2.7 Connecting a terminal with a fixed IP address".

12.2.9 Connecting a DHCP relay that adds Option 82 data under the Switch

When you connect a DHCP relay under the Switch and the DHCP relay adds its data in the Option 82 field of the DHCP packets received from the DHCP client, configure the Switch so it can forward the packets.

The following figure shows an example configuration when a DHCP relay that adds Option 82 data is connected under the Switch.

Figure 12-13: Example configuration when a DHCP relay that adds Option 82 data is connected under the Switch



Configure DHCP snooping on the Switch as described in "12.2.2 Basic configuration", "12.2.4 Terminal filter", and "12.2.5 Dynamic ARP inspection".

In the example here, the DHCP packets and IPv4 packets from the DHCP client cannot be relayed. In addition, the ARP packets from the Layer 3 switch/router cannot be relayed.

To relay the packets, you need to permit the forwarding of DHCP packets, IPv4 packets, and ARP packets on the Switch. When the DHCP relay adds Option 82 data, you also need to permit the forwarding of DHCP packets with Option 82 data.

(1) Permitting the forwarding of DHCP packets

The configuration for permitting the forwarding of IPv4 packets is the same as the configuration when a DHCP relay is connected under the Switch.

For details about the configuration, see "(1) Permitting the forwarding of DHCP packets in 12.2.8 Connecting a DHCP relay under the Switch".

(2) Permitting the forwarding of IPv4 packets

The configuration for permitting the forwarding of IPv4 packets is the same as the configuration when a DHCP relay is connected under the Switch.

For details about the configuration, see "(2) Permitting the forwarding of IPv4 packets in 12.2.8 Connecting a DHCP relay under the Switch".

(3) Permitting the forwarding of ARP packets

The configuration for permitting the forwarding of ARP packets is the same as the configuration when a terminal with a fixed IP address is connected.

For details about the configuration, see "12.2.7 Connecting a terminal with a fixed IP address".

(4) Permitting the forwarding of DHCP packets with Option 82 data

Points to note

Disable the Option 82 spoofing check for DHCP packets.

Command examples

1. `(config)# ip dhcp snooping information option allow-untrusted`
   Disables the Option 82 spoofing check for the DHCP packets received on the untrusted port.

12.2.10 Output to the syslog server

Points to note

Configure output of operation logs to the syslog server.

Command examples

1. `(config)# ip dhcp snooping logging enable`
   Configure output of operation logs to the syslog server.
2. `(config)# logging event-kind dsn`
   Sets DHCP snooping as the message type of the log information to be sent to the syslog server.

12.3 Operation

12.3.1 List of operation commands

The following table describes the operation commands for DHCP snooping.

Table 12-9: List of operation commands

Command name	Description
show ip dhcp snooping binding	Shows the information in a binding database.
clear ip dhcp snooping binding	Clears the information in a binding database.
show ip dhcp snooping statistics	Shows statistics.
clear ip dhcp snooping statistics	Clears the statistics.
show ip arp inspection statistics	Shows statistics for dynamic ARP inspection.
clear ip arp inspection statistics	Clears dynamic ARP inspection statistics.
show ip dhcp snooping logging	Shows the log messages logged by DHCP snooping.
clear ip dhcp snooping logging	Clears the log messages logged by DHCP snooping.
restart dhcp snooping	Restarts DHCP snooping.
dump protocols dhcp snooping	Outputs the logs and internal information logged by DHCP snooping to a file.

12.3.2 Checking a DHCP snooping binding database

Use the "show ip dhcp snooping binding" command to display the information in a binding database. The information includes the MAC addresses and IP addresses of terminals and the aging time of the binding database.

The following figure shows the result of executing the "show ip dhcp snooping binding" command.

Figure 12-14: Results of executing show ip dhcp snooping binding

```
> show ip dhcp snooping binding
Date 20XX/04/20 12:00:00 UTC
Agent URL: flash
Last succeeded time: 20XX/04/20 11:50:00 UTC
Total Bindings Used/Max    :       5/   3070
Total Source guard Used/Max:       2/   3070

Bindings: 5
MAC Address     IP Address       Expire(min)  Type      VLAN  Port
0012.e287.0001  192.168.0.201    -            static*   1     0/1
0012.e287.0002  192.168.0.204    1439         dynamic   2     0/4
0012.e287.0003  192.168.0.203    -            static    3     0/3
0012.e287.0004  192.168.0.202    3666         dynamic   4     ChGr:2
0012.e2be.b0fb  192.168.100.11   59           dynamic*  12    0/11
>
```

12.3.3 Checking DHCP snooping statistics

Use the "show ip dhcp snooping statistics" command to display the DHCP snooping statistics. The statistics include the total number of DHCP packets received on untrusted ports, the number of DHCP packets received by each interface, and the number of DHCP packets filtered out.

The following figure shows the result of executing the "show ip dhcp snooping statistics" command.

Figure 12-15: Results of executing show ip dhcp snooping statistics

```
> show ip dhcp snooping statistics
Date 20XX/04/20 12:00:00 UTC
Database Exceeded: 0
Total DHCP Packets: 8995
Port         Recv       Filter
0/1           170          170
0/3          1789           10
           :
0/25            0            0
ChGr:1       3646         2457
>
```

12.3.4 Checking dynamic ARP inspection

(1) Checking the dynamic ARP inspection statistics

Use the "show ip arp inspection statistics" command to display the dynamic ARP inspection statistics. The statistics include the number of relayed ARP packets, the number of discarded ARP packets, and details about the discarded ARP packets.

The following figure shows the result of executing the "show ip arp inspection statistics" command.

Figure 12-16: Results of executing show ip arp inspection statistics

```
> show ip arp inspection statistics
Date 20XX/04/20 12:00:00 UTC
Port       Forwarded     Dropped  ( DB mismatch     Invalid  )
0/1                0          15  (           15           0  )
0/2              584         883  (          883           0  )
0/3                0           0  (            0           0  )
                                :
ChGr:2           170          53  (           53           0  )
>
```

12.3.5 Checking the DHCP snooping log messages

Use the "show ip dhcp snooping logging" command to display the messages logged by DHCP snooping. The log messages include those pertaining to updating of the binding database, updating of terminal filters, detection of invalid DHCP servers, discarding of invalid DHCP packets, and discarding of ARP packets.

The following figure shows the result of executing the "show ip dhcp snooping logging" command:

Figure 12-17: Results of executing show ip dhcp snooping logging

```
> show ip dhcp snooping logging
Date 20XX/04/20 12:00:00 UTC
Apr 20 11:00:00 ID=2201 NOTICE DHCP server packets were received at an untrust port(0/2/1/
0012.e2ff.fe01/192.168.100.254).
>
```

13 Description of GSRP

GSRP provides redundancy for the Switch on Layers 2 and 3. This chapter provides an overview of GSRP.

13.1 Overview of GSRP

13.1.1 Overview

Gigabit Switch Redundancy Protocol (GSRP) provides redundancy for the Switch by securing a communication path via another switch in the same network even if the primary switch has failed.

In Layer 2, you can use Spanning Tree Protocols to provide redundancy on the network. In Layer 3, you can use VRRP to provide redundancy for the default gateway. However, GSRP can by itself provide redundancy for both Layers 2 and 3.

- Layer 2

  Because the paired switches exchange control frames to check each other's status, the switchover from one switch to another is faster than using a Spanning Tree Protocol. GSRP is also suitable for large-scale configurations in which core switches are used in multiple stages on a network.

- Layer 3

  GSRP provides redundancy for the default gateway by allowing the paired switches to have the same IP addresses and same MAC address. By using GSRP for the default gateway for PCs, you can have redundant communication paths from PCs to the upstream network. If the default gateway device fails, the backup device takes over for the original device by using the same IP addresses and MAC address allowing the PCs to continue sending traffic through the default gateway.

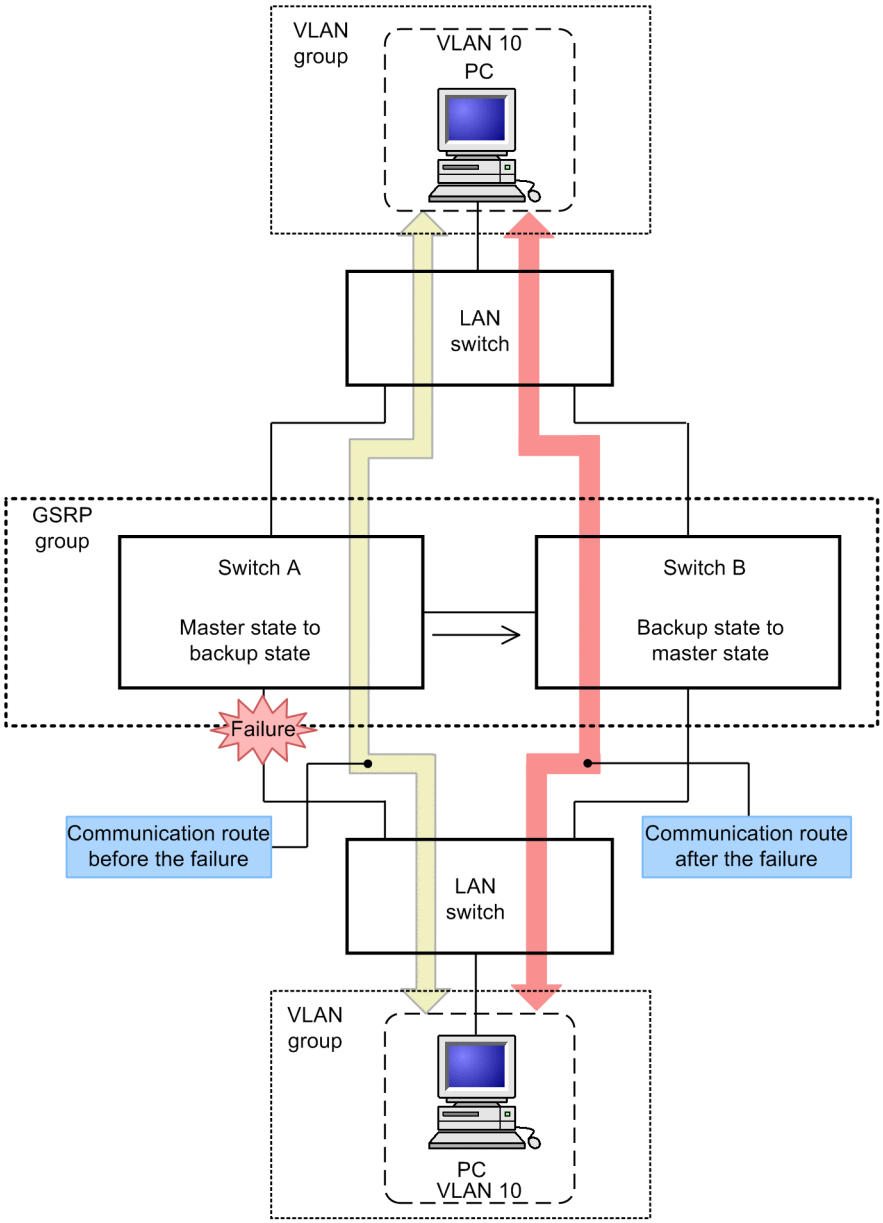
The following table compares the protocols for providing redundancy simultaneously for both Layers 2 and 3.

Table 13-1: Comparing the protocols for providing redundancy simultaneously for both Layers 2 and 3

Protocol for redundancy	Description
GSRP	• Management is easy because one protocol provides redundancy for both Layers 2 and 3. • GSRP is specific to the Switch. GSRP switches cannot be connected to switches manufactured by other companies.
Spanning Tree Protocols and VRRP	• Both a Spanning Tree Protocol and VRRP must be configured to provide redundancy simultaneously for both Layers 2 and 3. • Because these protocols are standards, you can create 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 13-1: Overview of GSRP



The Switches with GSRP are paired to create a group. In normal behavior, one switch serves as the master switch and the other serves as the backup switch. The master Switch (Switch A) forwards frames, and the backup Switch (Switch B) blocks frames. If a link or a switch fails, the master/backup relationship between Switches A and B is reversed, allowing communication to continue.

13.1.2 Features

(1) Avoiding the simultaneous master status

When GSRP is enabled, the paired Switches send and receive control frames on the direct link between them to check each other's status. When a link failure is detected, if control frames are successfully sent and received, the switches automatically switch over. The master Switch makes sure that the neighbor Switch is operating in the backup status, and then the backup Switch takes over as the master Switch. This precaution prevents the two Switches from being in the master status at the same time.

If the master Switch fails, control frames cannot be successfully sent and received, and neither Switch is able

to check the status of the neighbor Switch. Accordingly, the Switches need to be manually switched over. The reason is that the failed master Switch might still be operating in the master status. If the backup Switch automatically enters the master status, the two Switches would be in the simultaneous master status. Manual switchover is necessary to avoid this problem. The assumption is that the user takes action for the failure and determines that it is safe to allow the backup switch to enter the master status before manually changing the backup switch to the master status. Besides manual switchover, GSRP also supports automatic switchover. When a Switch detects a failure on the direct link with the neighbor Switch, the switch assumes that a failure has occurred on the neighbor Switch and automatically takes over.

(2) Limiting the range for sending control frames

To avoid sending control frames to unnecessary locations, GSRP limits the range for sending and receiving control frames only to the specified VLANs.

13.1.3 Supported specifications

The following table describes the function and settings supported by GSRP and their specifications.

Table 13-2: Function and settings supported by GSRP and their specifications

Item		Description
Applicable layer	Layer 2	Y
	Layer 3	Y (IPv4, IPv6)
Maximum number of GSRP groups to which each switch can belong		1
Maximum number of Switches making up a GSRP group		2
Maximum number of VLAN groups per GSRP group		64
Maximum number of VLANs per VLAN group		1024
Interval at which GSRP Advertise frames are sent		Can be set in 0.5-second intervals in the range from 0.5 to 60.
Time GSRP Advertise frames are retained		Can be set in 1-second intervals in the range from 1 to 120.
Load balancing function		Y
Backup locking function		Y
Port resetting		Y
To prevent repeated switchover, you can choose not to count link ports that are up as active ports until the links are stable.		Y
GSRP VLAN group-only control function		Y
Ports that are not under GSRP control		Y

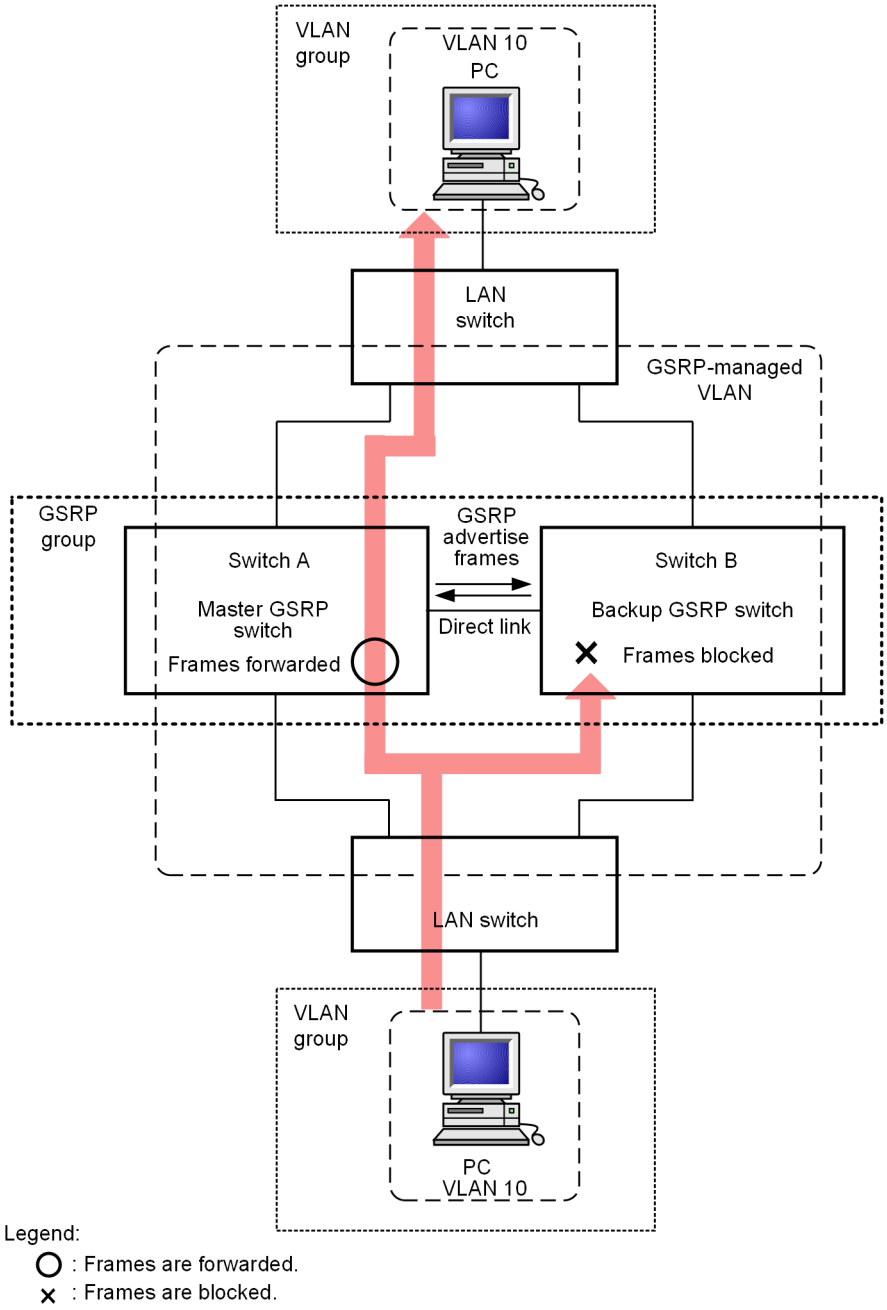
Legend: Y: Supported

13.2 GSRP principles

13.2.1 Network configuration

The following figure shows the basic network configuration when GSRP is used.

Figure 13-2: Network configuration for GSRP



A switch configured with GSRP is called a GSRP switch. A pair of GSRP switches forms a GSRP group. In normal operation, one switch is the master switch and the other is the backup switch. The basic GSRP configuration consists of two GSRP switches and neighboring switches.

The two GSRP switches must be directly connected. This link is called a direct link.

On the direct link, control frames, called GSRP Advertise frames, are exchanged between the GSRP switches so the switches can check each other's status. Other data frames are blocked by default. If you want to send and receive data frames on the direct link, configure the GSRP VLAN group-only control function and use a VLAN that does not belong to any VLAN group or set the direct-link ports as ports not under GSRP control. When you use Layer 3 redundancy switching function, the direct link might be used to relay ordinary data between the GSRP switches. In that case, use the GSRP VLAN group-only control function or configure the direct-link ports as ports not under GSRP control. For details, see "13.4 Layer 3 redundancy switching function" and "13.5.3 Switchover due to a failure in the upstream network when Layer 3 redundancy switching function is used".

The GSRP switches send and receive GSRP Advertise frames to check each other's status and to control the switchover between the master and backup statuses. The switchover between the master and backup statuses is performed for logical groups consisting of VLANs. These logical groups are called a VLAN groups.

The master GSRP switch forwards the frames from the specified VLAN groups, and the backup GSRP switch blocks the frames from the same VLAN groups.

13.2.2 GSRP-managed VLANs

In a network deploying GSRP, dedicated VLANs must be configured to limit the range for sending GSRP control frames. These VLANs are called GSRP-managed VLANs. The GSRP switches send and receive control frames for GSRP-managed VLANs only.

Before a GSRP switch becomes the master switch, it sends a control frame called a GSRP Flush request frame to the neighboring switches to request the clearing of MAC address table entries. Therefore, in addition to the direct-link ports, all the VLAN ports that participate in VLAN groups must be assigned to GSRP-managed VLANs. Furthermore, the neighboring switches require the same VLAN settings as the GSRP-managed VLANs so that they can receive GSRP control frames. However, GSRP-managed VLAN settings are not required for the ports on the GSRP switches if the neighboring switches that are connected to them do not support the clearing of MAC address tables triggered by the reception of GSRP Flush request frames, or for the ports on those neighboring switches.

13.2.3 GSRP switchover control

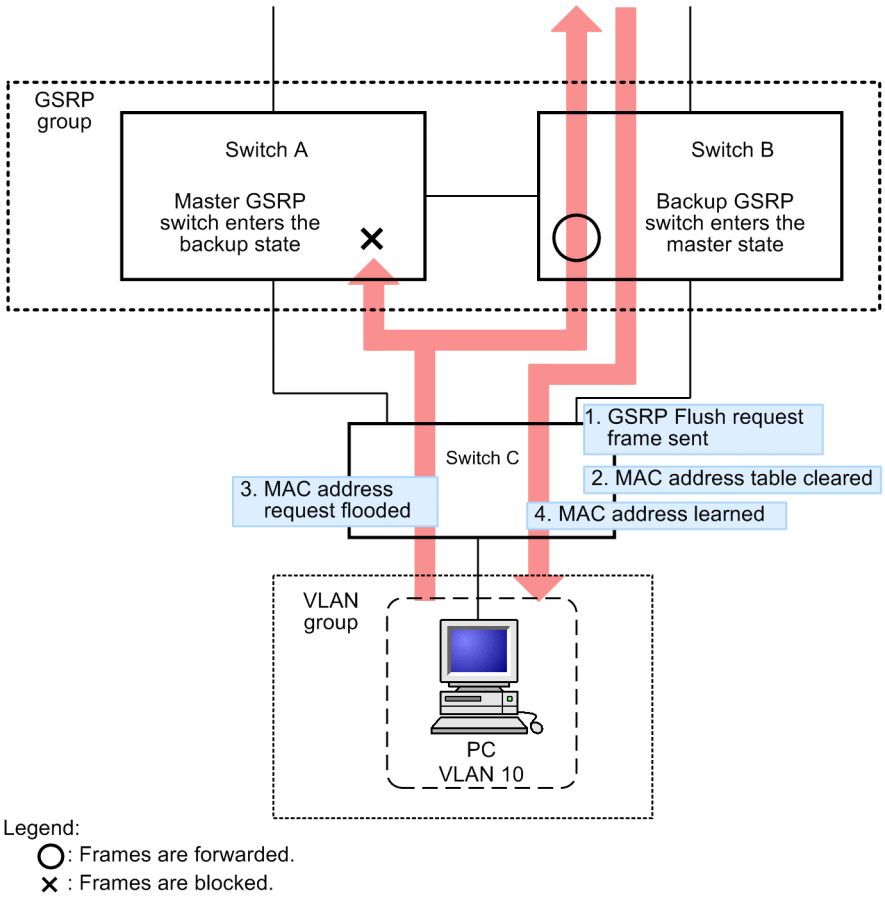
When the backup GSRP switch takes over as the master switch, the backup switch assumes the forwarding and blocking responsibility for frames. However, that is not enough to immediately resume end-to-end communication, because the MAC address entries in the MAC address tables in the neighboring switches are still registered for the previous master GSRP switch. To immediately resume communication, the MAC address table entries on the neighboring switches need to be cleared when the GSRP switches change.

GSRP supports the following methods for clearing the MAC address table entries in the neighboring 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 neighboring 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. The Switch is GSRP-aware unless specified otherwise in the configuration. GSRP-aware switches flood GSRP Flush request frames. A switch that does not support GSRP Flush request frames is GSRP unaware. If a neighboring switch is GSRP-unaware, you need to use the function described in "(2) Port resetting". The following figure provides an overview of clearing MAC address table entries by using GSRP Flush request frames.

Figure 13-3: Overview of clearing MAC address table entries by using GSRP Flush request frames



1. Switch B takes over from Switch A. Switch B sends a GSRP Flush request frame to Switch C.
2. Switch C receives the GSRP Flush request frame, and clears the internal MAC address table.
3. As a result, Switch C 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.
4. The frames sent from the PC are forwarded to the destination via the master Switch (Switch B). When a frame returns to the PC as a response, Switch C learns the MAC address of the PC.

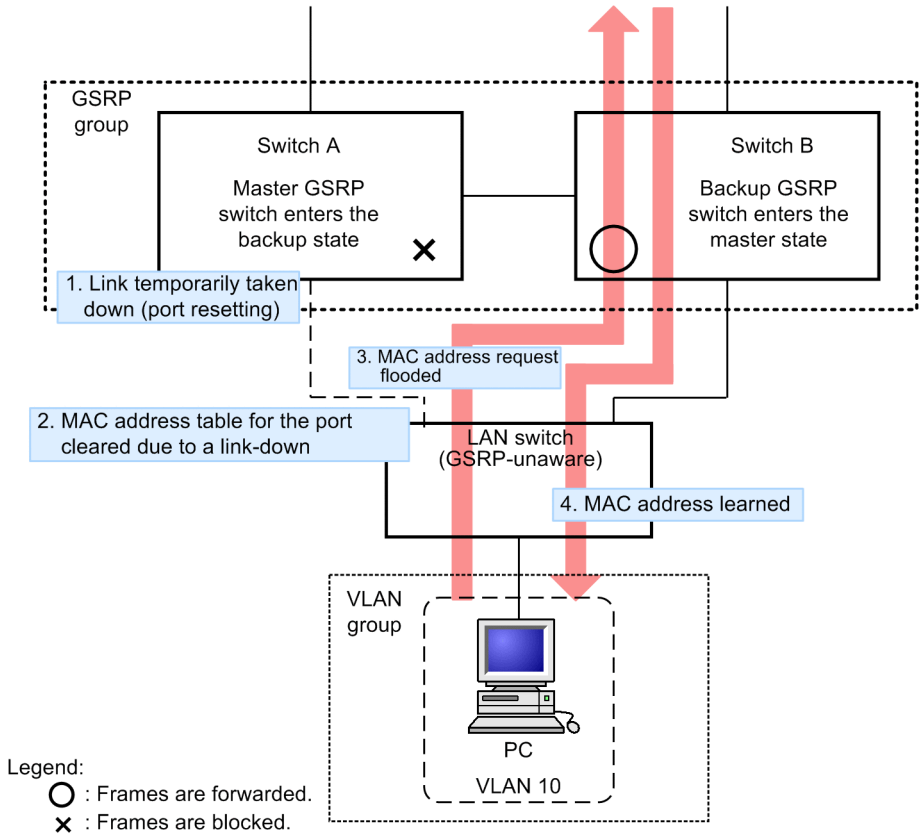
   Thereafter, Switch C forwards the frames from the PC only to Switch B.

(2) Port resetting

Port resetting temporarily disconnects the link between a GSRP switch and a neighboring switch. Use this function for neighboring switches that are GSRP-unaware. This function is useful because, when the switches detect a link disconnection on the port, switches clear the MAC address entries learned via a port from their MAC address tables.

The following figure provides an overview of clearing MAC address table entries by using port resetting.

Figure 13-4: Overview of clearing MAC address table entries by using port resetting



1. Switch B takes over from Switch A. Switch A uses port resetting to disconnect the link with the GSRP-unaware LAN switch.
2. The GSRP-unaware LAN switch clears the MAC address table for the port link that went down.
3. As a result, the GSRP-unaware LAN 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 (Switch B).
4. When a frame returns to the PC as a response, the GSRP-unaware LAN switch learns the MAC address of the PC.
   Thereafter, the GSRP-unaware LAN switch forwards the frames from the PC only to Switch B.

13.2.4 Selecting the master and backup switches

(1) Selection conditions

GSRP switches periodically send and receive GSRP Advertise frames. The master and backup GSRP switches are determined for each VLAN group based on the selection conditions information for each VLAN group contained in the GSRP Advertise frames. The following table describes the conditions supported by GSRP for selecting the master and backup switches.

Table 13-3: Conditions supported by GSRP for selecting the master and backup switches

Item	Description
Number of active ports	The number of enabled physical ports among the physical ports assigned to all the VLANs (except for the VLANs specified by using the "state suspend" configuration command) participating in the VLAN groups on a switch. The switch with more active ports becomes the master. If link aggregation is configured, a channel group is counted as a port.
Priority	Priority level set for a VLAN group in the configuration. The switch that has higher priority becomes the master.
Device MAC address	MAC address of a switch. The switch that has the larger MAC address value becomes the master.

(2) Priority of conditions

You can specify the priority of the conditions explained in "(1) Selection conditions" by using a configuration command. The available priority sets are the following:

- Number of active ports -> priority -> switch MAC address (default)
- Priority -> number of active ports -> switch MAC address

13.3 Overview of GSRP switch behaviors

13.3.1 GSRP switch statuses

GSRP switches have five behavior states. The following table describes the states.

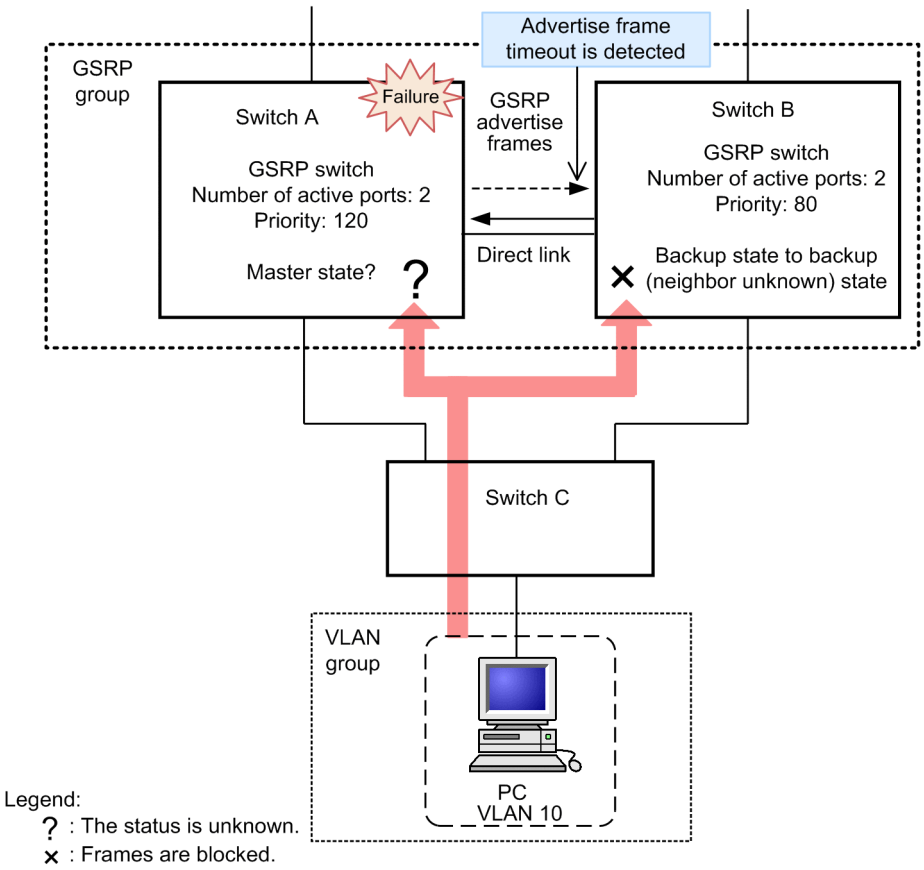
Table 13-4: GSRP switch statuses

Status	Description
Backup	The switch is operating in the backup status. The backup GSRP switch blocks frames on each port on a VLAN in a VLAN group. Because the backup GSRP switch only relays GSRP control frames, it does not learn MAC addresses. Every GSRP switch starts in the backup status when it is initially started.
Backup (wait for master)	A transient state for a switch that is waiting to enter the master status from the backup status until it has confirmed that the neighbor GSRP switch is definitely in the backup status or backup (locked) status. When a switch is in the backup (wait for master) status, as in the backup status, it only relays GSRP control frames.
Backup (neighbor unknown)	A switch in the backup status or backup (wait for master) status enters this state when it detects a timeout for receiving GSRP Advertise frames from the neighbor GSRP switch. Because the neighbor GSRP switch might be operating in the master status, the backup switch remains in this backup status unless it receives a GSRP Advertise frame again or the user uses the "set gsrp master" operation command to place the backup switch in the master status. As in the backup status, the switch in the backup (neighbor unknown) status only relays GSRP control frames.
Backup (locked)	The backup switch is forcibly set in the backup status by a configuration command. The backup switch remains in this state unless the configuration is deleted. The switch remains in the backup (locked) status until the switch configuration is deleted. In the backup (locked) status, as in the backup status, the switch only relays GSRP control frames.
Master	The switch is operating in the master status. The master GSRP switch forwards frames on each port on a VLAN in a VLAN group. The master GSRP switch relays all frames, including GSRP control frames, and learns MAC addresses.

13.3.2 Behavior when a switch fails

The following figure shows an example of how a GSRP switch runs when it fails.

Figure 13-5: Behavior when a switch fails



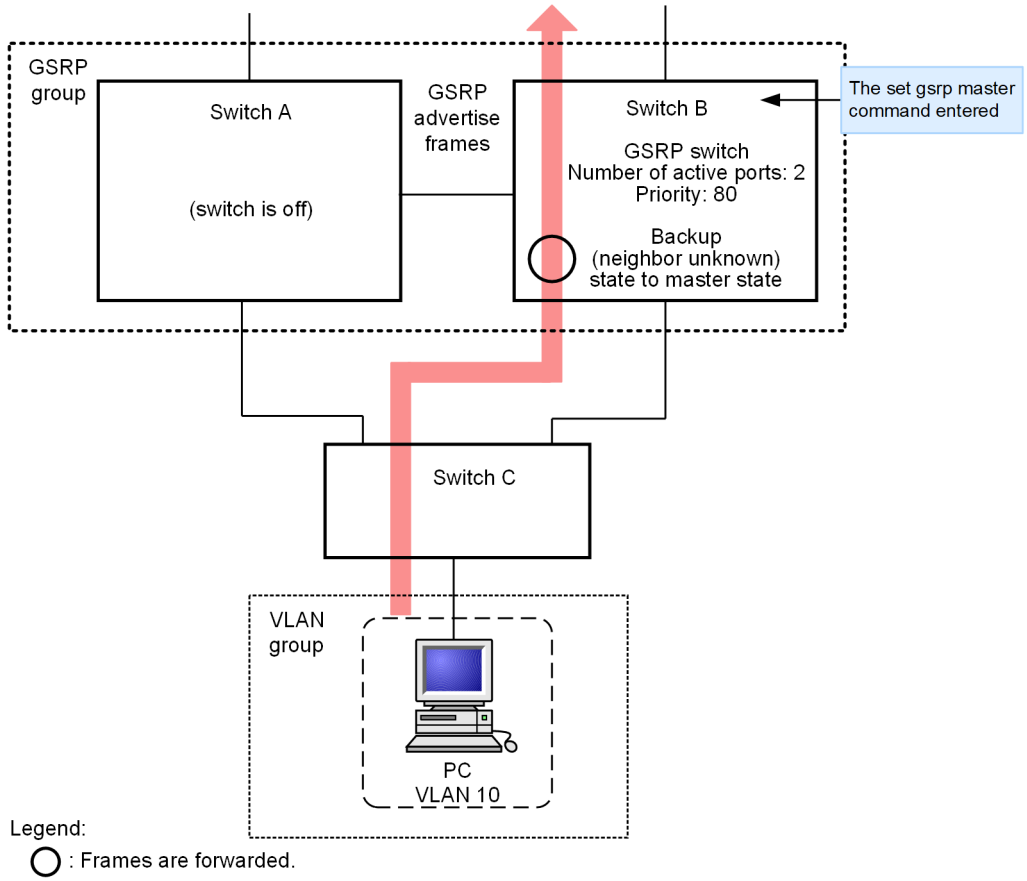
When the master Switch (Switch A) is unable to successfully send GSRP Advertise frames due to a failure on the switch, switch B detects a timeout for receiving GSRP Advertise frames from switch A. At this point, Switch B enters the backup (neighbor unknown) status. In this state, as in the backup status, Switch B does not relay frames. When a switch is in the backup (neighbor unknown) status, it outputs a message prompting the user to check its state.

GSRP supports two methods for changing the state of Switch B from backup (neighbor unknown) to master: manual switchover and automatic switchover.

(1) Manual switchover (operation command used)

GSRP supports the "set gsrp master" operation command to manually change the switch status to the master status. Before the user executes this command to change the state of Switch B to the master status, the user must check whether the ports on Switch A are blocked or whether Switch A is deactivated. The following figure shows what happens after the "set gsrp master" operation command is entered.

Figure 13-6: Behavior after the set gsrp master operation command is entered



(2) Automatic switchover (direct link failure detected)

For automatic switchover, GSRP supports a direct link failure detection function. GSRP also supports function for switchover to the master status by independently started GSRP switches. This is not handled by the direct link failure detection function.

- Direct link failure detection function

  To enable the direct link failure detection function, specify the direct-down parameter in the "no-neighbor-to-master" configuration command.

  This function can be used after a switch has been started and has received a GSRP Advertise frame from the neighbor switch. When a switch discovers that the direct-link port is down after it enters the backup (neighbor unknown) status, the backup switch assumes that the neighbor switch has failed and automatically switches to the master status.

  Automatic switchover following direct link failure detection function is not performed if a switch has already been started[#1] but has not received a GSRP Advertise frame from the neighbor switch yet because the status of the neighbor switch is unknown. If you want to make the switch the master in this case, manually set the switch as the master. If you want to perform automatic switchover after a switch has been started but before it has received a GSRP Advertise frame from the neighbor switch, use the function for switchover to the master status by an independently started GSRP switch.

- Function for switchover to the master status by an independently started GSRP switch

  To enable switchover to the master status by an independently started GSRP switch, specify the direct-down forced-shift-time parameter in the "no-neighbor-to-master" configuration command.

  This function works only when the neighbor GSRP switch has not started due to a failure and the direct link has not been up since switch startup[#2].

When all the conditions#3 for starting switchover to the master status for an independently started GSRP switch are satisfied, the applicable switch enters the automatic master wait state and automatically enters the master status after the automatic master wait time specified in the forced-shift-time parameter has elapsed.

When a switch is in the automatic master wait state, you can use the "clear gsrp forced-shift" operation command to cancel the state to prevent the switch from automatically entering the master status.

This function places the switch in the master status without knowing the state of the neighbor switch. Make sure you wait a sufficient period of time before having the switch enter the master status in order to make certain that either the ports on the neighbor switch are blocked or the neighbor switch is not running.

#1

A switch is assumed to have been started when any of the following behaviors is performed:

- Execution of the "restart vlan" operation command
- Executing the "restart gsrp" operation command
- Specifying direct-down for no-neighbor-to-master in the "gsrp" configuration command.
- Configuring a direct-link port by using direct-link in the "grsp" configuration command.
- Applying the setting to the running configuration by using the "copy" operation command

#2

The switchover to the master status by an independently started GSRP switch is performed in the same way as when a switch has been started by any of the following behaviors:

- Execution of the "restart vlan" operation command
- Executing the "restart gsrp" operation command
- Applying the setting to the running configuration by using the "copy" operation command

#3

The conditions for starting the switchover to the master status by an independently started GSRP switch as follows:

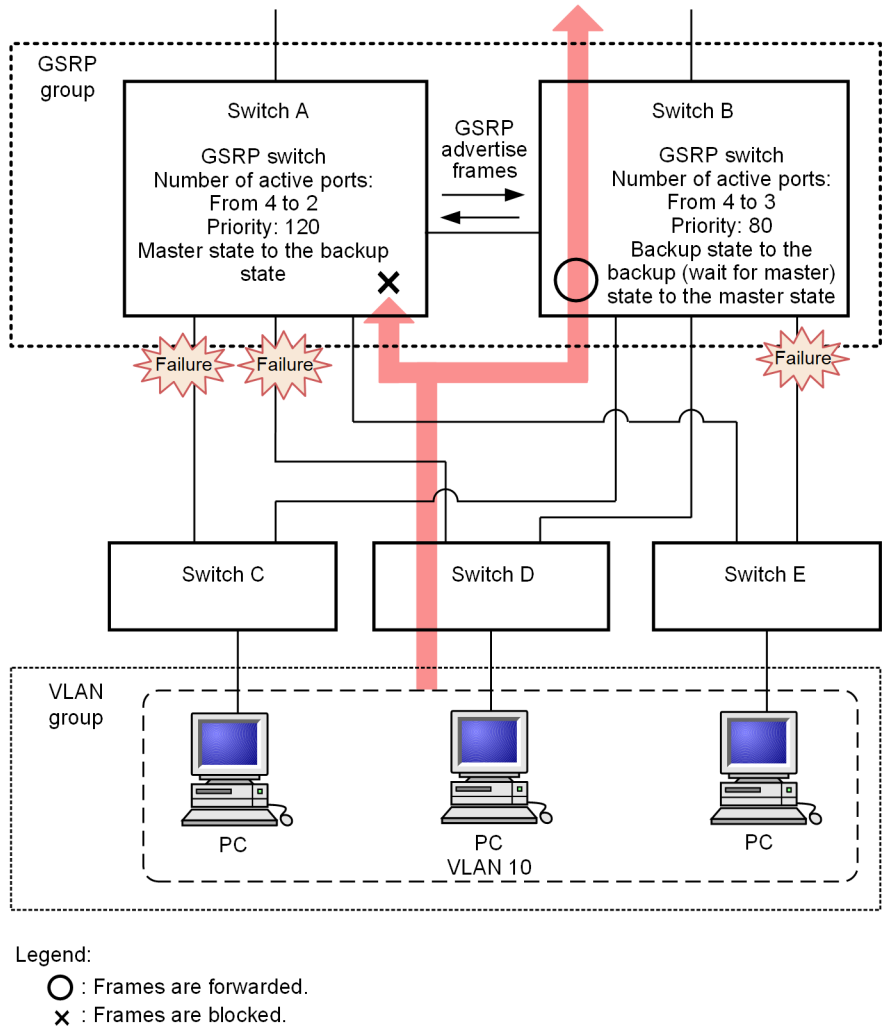
- The timeout period for receiving GSRP Advertise frames expires.
- Any of the member ports in the VLAN groups configured for a Switch is enabled.

13.3.3 Behavior example when a link fails

(1) Prevention of repeated switchover when links are unstable

The following figure shows an operation example when a link fails.

Figure 13-7: Behavior example when a link fails



In this figure, Switch A is the master switch and Switch B is the backup switch. Failures have occurred on the link between Switches A and C, on the link between Switches A and D, and on the link between Switches B and E. For Switches A and B, the number of active ports is the top-priority condition in the master/backup selection conditions. Because Switch B has more active ports than Switch A, Switch B becomes the master Switch. Before Switch B enters the master status, it enters the backup (wait for master) status. In the backup (wait for master) status, Switch B waits for a GSRP Advertise frame from Switch A. When Switch B receives a GSRP Advertise frame, it makes sure that Switch A is in the backup status and then enters the master status. Note that the example in this figure shows that Switch E cannot establish communication because the link between Switch E and Switch B (master switch) has failed.

(2) To prevent repeated switchover, you can choose not to count link ports that are up as active ports until the links are stable.

GSRP uses the number of active ports as the top-priority condition for selecting the master and backup switches. If links become unstable (for example, links frequently come up and go down), the number of active ports also changes frequently, resulting in repeated switchover between the master and backup switches.

For this purpose, GSRP provides the "port-up-delay" configuration command that you can use to specify a delay time during which link ports that are up are not counted as active ports. This specification prevents unnecessary switchovers when links are unstable.

In the "port-up-delay" command, you can specify a value in one-second units in the range from 1 to 43200 seconds (12 hours). If you specify infinity, the delay time is unlimited. If you are sure the links are stable,

you can use the "clear gsrp port-up-delay" operation command to start counting the number of active ports without waiting for the delay time you specified in the "port-up-delay" command to expire.

13.3.4 Backup locking function

By using the backup locking function, you can forcibly change the status of a GSRP switch to the backup status. To change a switch to the backup (locked) status, use the "backup-lock" configuration command. The switch remains in the backup (locked) status until the switch configuration is deleted. In the backup (locked) status, as in the backup status, the switch only relays GSRP control frames.

13.3.5 GSRP VLAN group-only control function

Using the "gsrp limit-control" configuration command, you can limit the VLANs under GSRP control only to those that belong to VLAN groups. Because VLANs that do not belong to VLAN groups are not under GSRP control, you can always use them for communication.

When GSRP-managed VLANs do not belong to VLAN groups, the VLANs are not under GSRP control. As the result, the VLANs are in a loop configuration. To prevent this, make sure that GSRP-managed VLANs belong to VLAN groups when using this function. Here, we recommend that you configure and operate VLAN groups to which only GSRP-managed VLANs belong to prevent this function from affecting other VLAN groups.

13.3.6 Ports that are not under GSRP control

Use the "gsrp exception-port" configuration command to exempt the specified ports from GSRP control. Ports not under GSRP control can be used for communication any time regardless of the master and backup status.

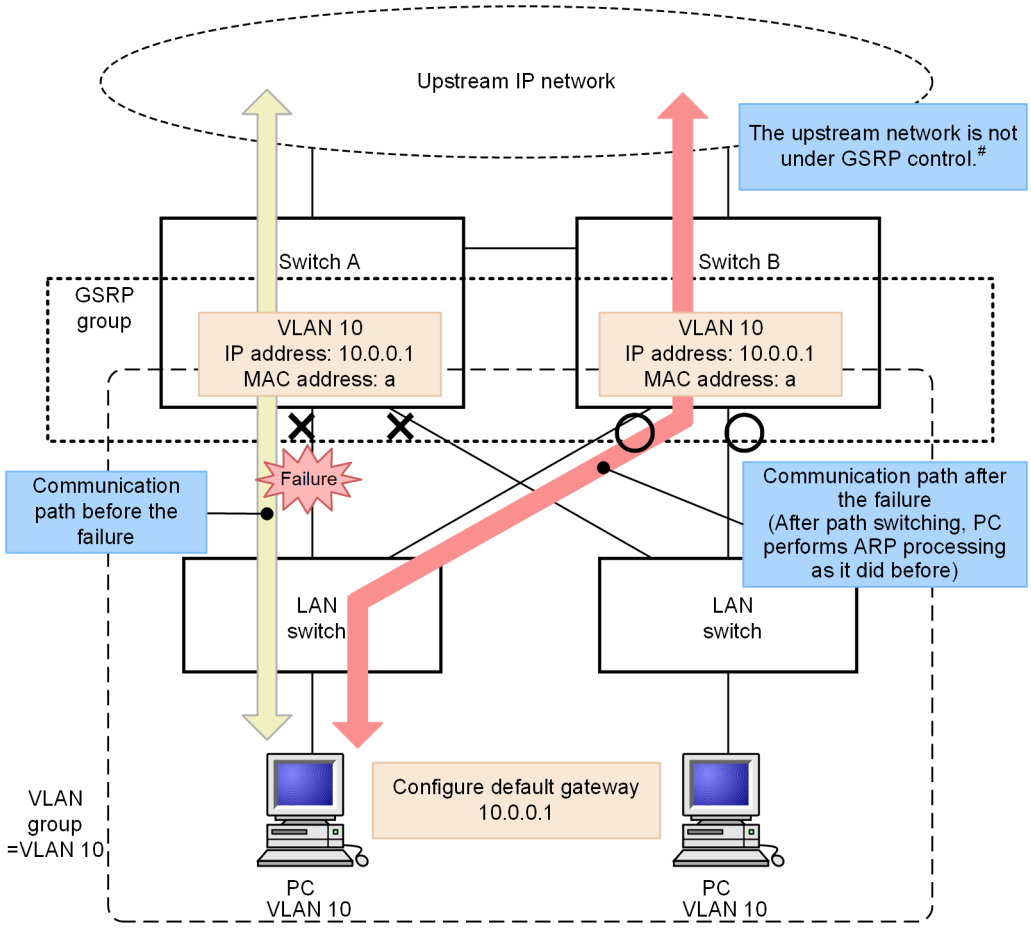
13.4 Layer 3 redundancy switching function

13.4.1 Overview

Layer 3 redundancy switching allows two switches to be switched over using the same IP addresses and same MAC address. This way, PCs can continuously send and receive traffic via the default gateway without stopping.

The following figure provides an overview of GSRP Layer 3 redundancy switching function. In this example, the network containing the PCs is called the downstream network. The network that receives the IP packets forwarded from the downstream network is called the upstream network. GSRP master/backup switchover affects the downstream network.

Figure 13-8: Overview of GSRP Layer 3 redundancy switching function



(1) IP addresses of the default gateway

When you use GSRP to provide redundancy for the default gateway, assign the same IP address to the same VLAN on each paired GSRP switch. On the master GSRP switch, VLANs are enabled. The master GSRP switch forwards IP packets as the default gateway. On the backup GSRP switch, VLANs are disabled. The backup GSRP switch does not forward IP packets.

(2) MAC addresses of the default gateway

When you use GSRP to provide redundancy for the default gateway, a GSRP-specific virtual MAC address is used as the MAC address of the default gateway. A different virtual MAC address is assigned to each VLAN group ID.

The master switch periodically sends a GSRP control frame (a frame for virtual MAC address learning) containing its virtual MAC address as the source MAC address to the lower-level LAN switches so that they can learn the virtual MAC address of the master switch.

The figure and table below describe the format and components of the virtual MAC addresses used by GSRP.

When the VLAN group ID is not greater than 8, a virtual MAC address is generated by using the method described below.

Figure 13-9: Format of a virtual MAC address for GSRP Layer 3 redundancy switching function (when the VLAN group ID is 8 or less)

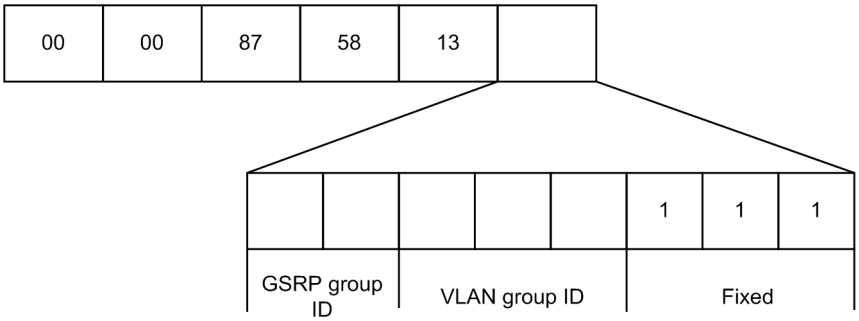


Table 13-5: How to generate a virtual MAC address for the GSRP Layer 3 redundancy switching function (VLAN group ID is 8 or less)

Item	Code
GSRP group ID	Set a value in the range from 0 to 3 for GSRP group IDs 1 to 4. For Layer 3 redundancy switching function, the GSRP group ID must be 1, 2, 3, or 4.
VLAN group ID	Set a value in the range from 0 to 7 for VLAN group IDs 1 to 8.
Fixed (3 bits)	The three least significant bits are fixed at 7.

When the VLAN group ID is 9 or greater, virtual MAC addresses in the range from 0000.8758.1311 to 0000.8758.1350 are sequentially assigned to VLAN group IDs 9 to 64.

(3) Sending VLAN ports and sending interval of frames for virtual MAC address learning

Frames for virtual MAC address learning are sent to each VLAN port belonging to the master VLAN group, at the specified interval. The number of frames (sending rate) that can be sent per second is determined so that the frames can be sent to the target VLAN port at the specified interval. The sending rate is calculated by the following equation, and changes automatically in a range that is less than or equal to 100 pps. If the sending rate exceeds the maximum value (100 pps), no frames are sent.

[Equation for calculating the sending rate for frames for virtual MAC address learning]

Sending rate (pps) = number of VLAN ports that are to be sent/sending interval (seconds)

Example: If there are 200 VLAN ports to be sent and if the sending interval is set to 5 seconds, the sending rate will be 40 pps.

When the sending rate is calculated to be more than 100 pps, take caution because this means a VLAN port that does not send frames for virtual MAC address learning exists.

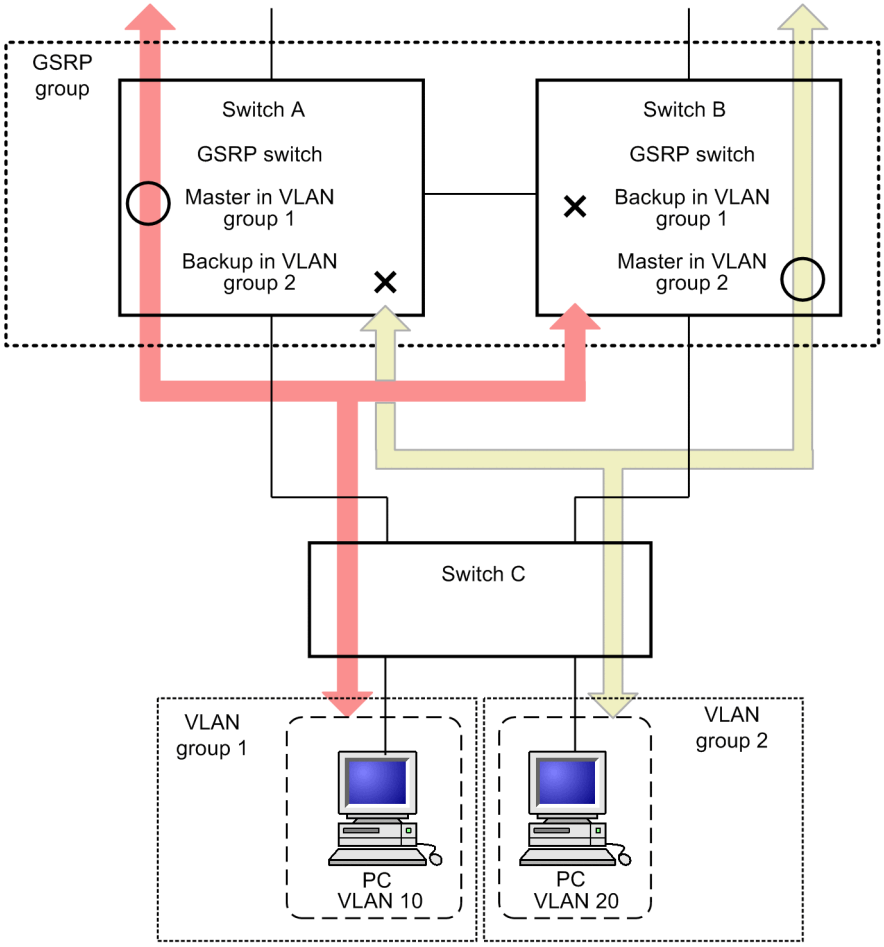
13.5 Network design for GSRP

13.5.1 Load balancing at the VLAN group level

GSRP manages the master and backup statuses of the switches for each VLAN group. A maximum of 64 VLAN groups can be configured on each GSRP switch. Permitting multiple VLAN groups and performing load balancing at the VLAN group level allows the GSRP switches to distribute the traffic load. The figure below provides an overview of load balancing.

In the example in the figure, Switch A is the master in VLAN group 1 and the backup in VLAN group 2. Switch B is the backup in VLAN group 1 and the master in VLAN group 2.

Figure 13-10: Load balancing configuration

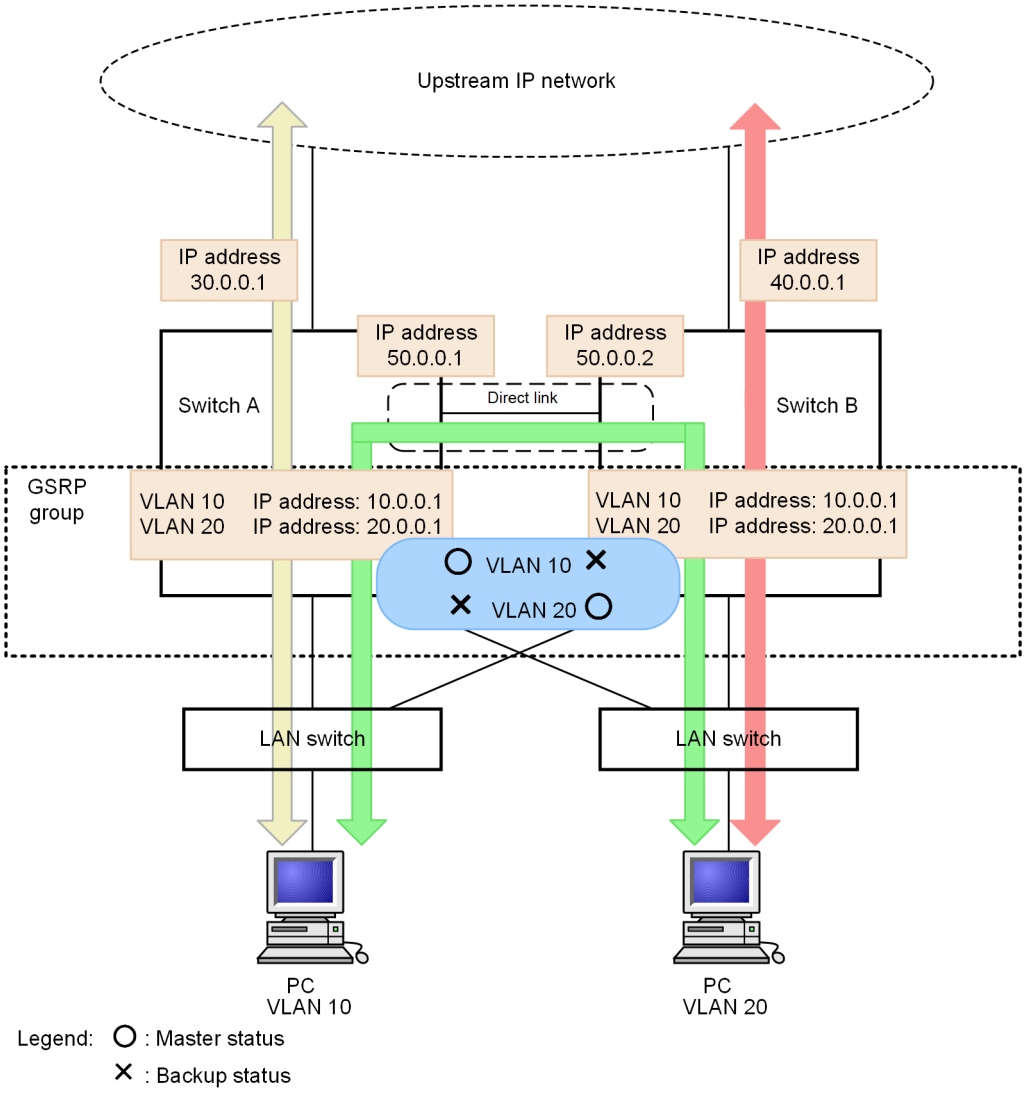


Legend:
○: Frames are forwarded.
×: Frames are blocked.

When you use Layer 3 redundancy switching function to balance the load, you need to provide a communication path between the GSRP switches to enable communication between the VLANs of the different master switches. This communication is performed via the VLAN configured on the direct link described in "13.5.3 Switchover due to a failure in the upstream network when Layer 3 redundancy switching function is used ". The figure below provides an overview of load balancing when Layer 3 redundancy switching function is used.

In this figure, Switch A is the master in VLAN 10 and Switch B is the master in VLAN 20. Traffic to the upstream IP network is forwarded by the master switch for each VLAN. The communication between VLAN 10 and VLAN 20 takes place via the VLAN on the direct link.

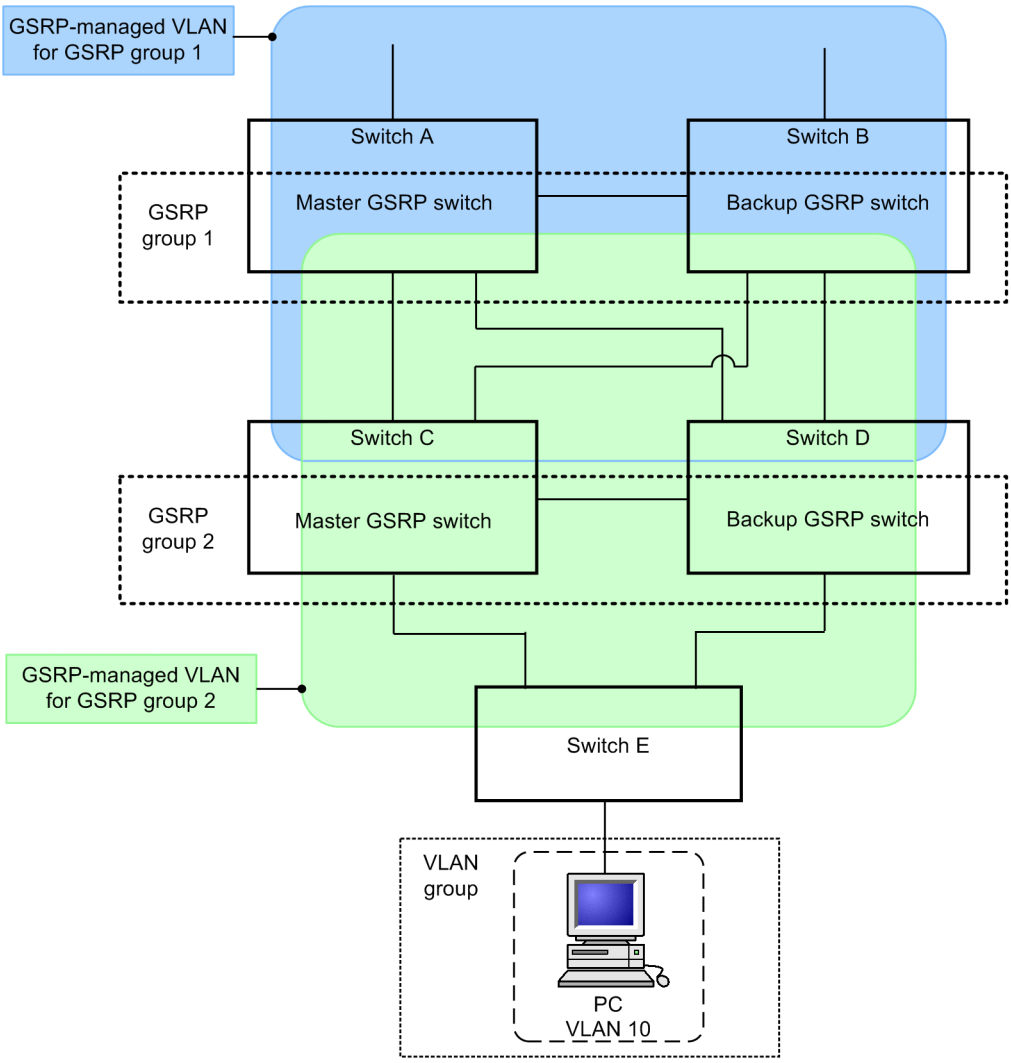
Figure 13-11: Load balancing when Layer 3 redundancy switching function is used



13.5.2 Multi-stage configuration of GSRP groups

GSRP permits multi-stage configuration of multiple GSRP groups on the same Layer 2 network, which assures redundancy on a large-scale network. When you allocate GSRP groups in a multi-stage configuration, configure a GSRP-managed VLAN for each GSRP group to limit the range for sending GSRP control frames. The following figure provides an overview of the multi-stage configuration of GSRP groups.

Figure 13-12: Multi-stage configuration of GSRP groups



In this figure, Switches A and B make up GSRP group 1, and Switches C and D make up GSRP group 2. Each GSRP group operates independently. If the master and the backup are switched in a GSRP group, the other GSRP group is not affected. Configure a GSRP-managed VLAN to include neighboring switches with the GSRP switches at the core.

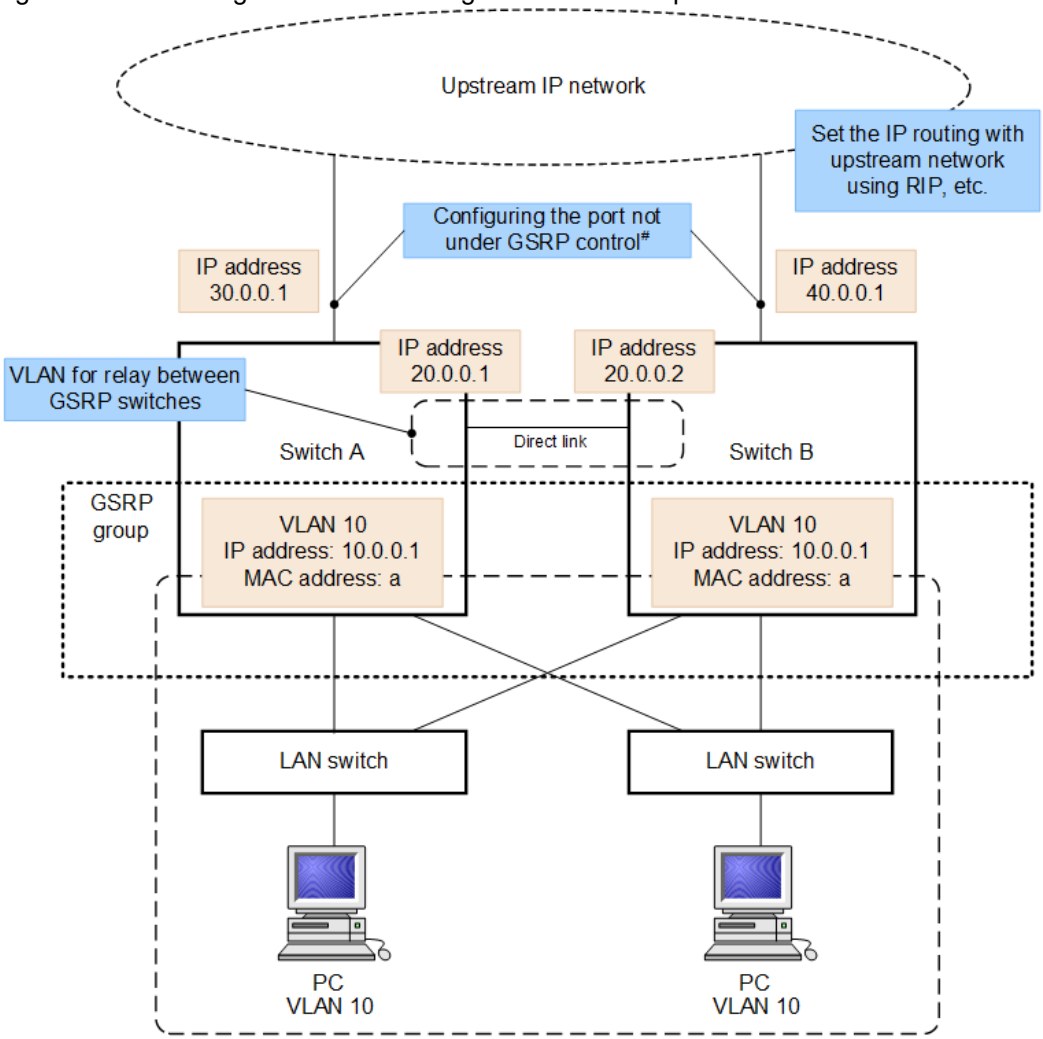
13.5.3 Switchover due to a failure in the upstream network when Layer 3 redundancy switching function is used

For the upstream network, configure IP routing and do not use GRSP to control the network. When you use Layer 3 redundancy switching function, IP routing detects failures in the upstream network and performs path switching as necessary.

Two GSRP switches must be connected to the upstream network. To assure continued communication with the upstream network, secure a communication path between the GSRP switches. By doing so, traffic can pass through the active backup switch even if the master GSRP switch fails due to a failure such a port failure.

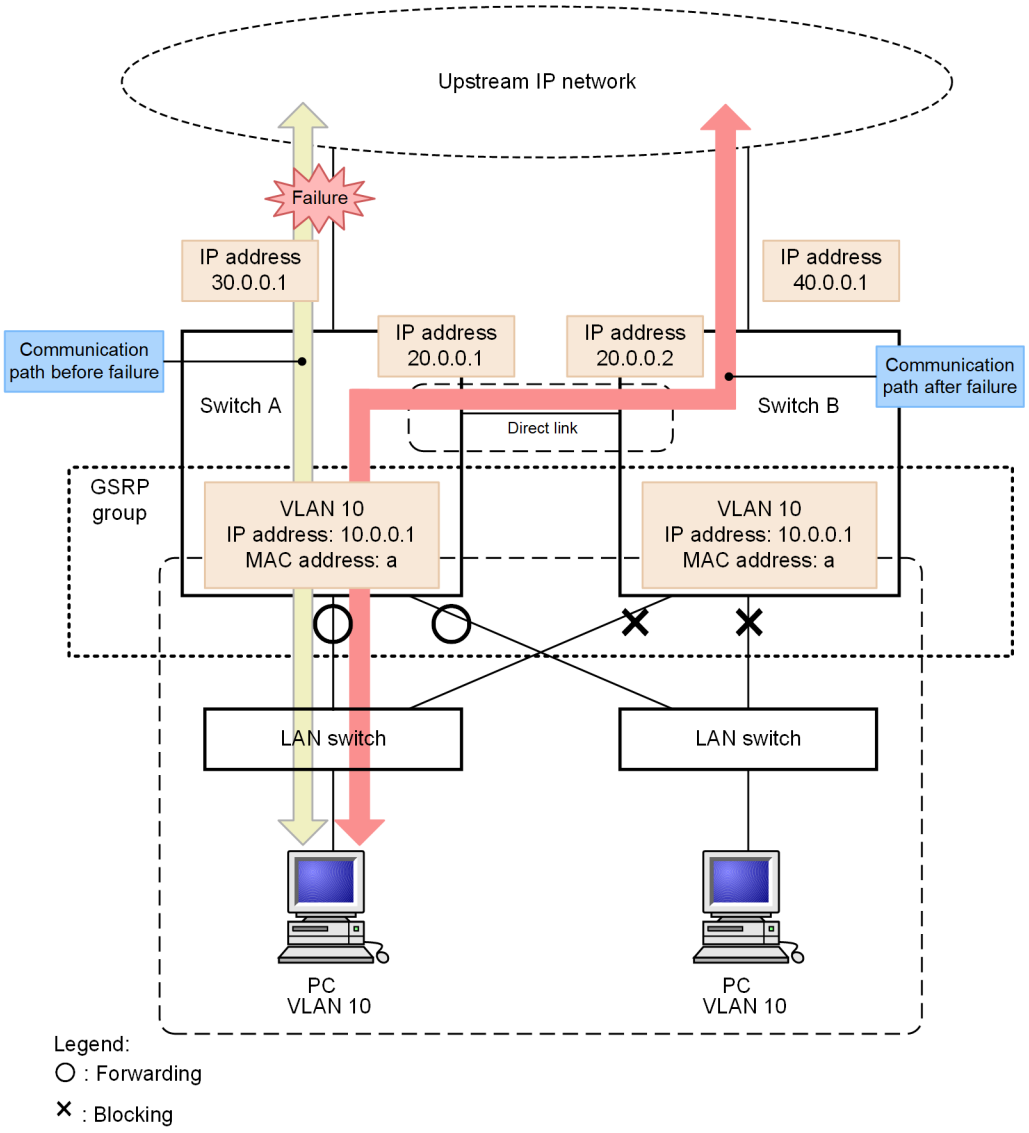
The following figures provide an overview of the configuration necessary to handle failures occurring on the upstream network and an example communication path to be used in case of a failure.

Figure 13-13: Configuration for handling failures on the upstream network



The following methods can be used to exclude the GSRP control.
- Configure the port not under GSRP control for the target port
- Apply the GSRP VLAN group-only control function and use a VLAN that does not belong to a VLAN group

Figure 13-14: Communication path to be used in case of failures on the upstream network



(1) Configuring ports to which the upstream network is connected

Use the following methods to allow both the master and backup GSRP switches to communicate with the upstream network through the ports or VLANs on the GSRP switches.

- Configure the ports on the GSRP switches to which the upstream network is connected as ports not under GSRP ("gsrp exception-port" configuration command).
- Use the GSRP VLAN group-only control function ("gsrp limit-control" configuration command) to configure the VLANs on the GSRP switches to which the upstream network is connected as VLANs not belonging to any VLAN group and therefore not under GSRP control.

Assign IP addresses to the ports and VLANs, and configure IP routing to connect to the upstream network.

Configure IP routing so that both GSRP switches are able to communicate with the upstream network. In addition, configure dynamic monitoring function of dynamic routing or static routing to detect failures in the upstream network.

Normally, both GSRP switches directly communicate with the upstream network. If a link between one switch and the upstream network fails, the failed switch uses the direct link with the other switch to continue communication with the upstream network. This becomes possible by configuring IP routing to assign a lower priority to the route to the upstream network via the neighbor GSRP switch. For static routing, configure

dynamic monitoring function to periodically check for the arrival of packets and to detect failures.

(2) Configuring a communication path between GSRP switches

Because the upstream network is connected to both GSRP switches, the backup GSRP switch might receive packets from the upstream network. To relay these packets to the master GSRP switch, configure a Layer 3 communication path between the GSRP switches.

The GSRP switches are thus connected by a direct link and exchange GSRP Advertise frames over the GSRP-managed VLAN. You can also configure a VLAN other than a GSRP-managed VLAN and IP routing on this direct link to relay packets between the GSRP switches. However, if you do so, configure IP routing to assign a lower priority to this communication path when it is used to directly forward traffic from downstream to the upstream network.

13.6 Notes on using GSRP

(1) Use with other function

(a) When used with the Layer 2 switch function

See "Configuration Guide Vol. 1, 22.3 Compatibility between the Layer 2 switch function and other functions".

(b) When used with Layer 2 authentication

For details, see "5.2.1 Using Layer 2 authentication with other functions".

(c) Coexistence with high reliability based on redundant configurations

The following table describes the high reliability based on redundant configurations that cannot be used, or only partially used, with GSRP.

Table 13-6: Function that cannot be used, or only partially used, with GSRP

Function	Restrictions
VRRP	Cannot be used
Uplink redundancy	

(2) When using port resetting

When you install a transmitter between a port configured with port resetting on a GSRP switch and a neighboring switch, the neighboring switch might not be able to directly detect a link-down port on the GSRP switch.

When you use port resetting, design the network so that neighboring switches can directly detect link-down ports on GSRP switches.

Also, if the port resetting operates while some of the physical ports belonging to the channel group are inactive, the relevant physical port becomes active.

(3) When using port resetting in a load-balancing configuration

When multiple VLAN groups share a physical port and port resetting is configured for that port, communication might be disconnected when the master switch enters the backup status in a VLAN group. This problem occurs because the port link goes down even though the switch is still operating as the master in another VLAN group. If you want to avoid this kind of temporarily disconnected communication, design the network so that multiple VLAN groups do not share a physical port.

The port that temporarily goes down because of port resetting is treated as an active port during the selection of the master and backup switches. This kind of port does not affect the selection of the master and backup switches in the VLAN group that is running in the master status.

(4) VLANs to be controlled by GSRP

When you use GSRP, GSRP controls all VLANs. Therefore, the VLAN ports that do not belong to any VLAN group are blocked. If you want to control only the VLANs that belong to VLAN groups, use the GSRP VLAN group-only control function.

(5) GSRP VLAN group-only control function

When you perform either of the following behaviors while the GSRP VLAN group-only control function is configured, all VLANs temporarily go down. In this case, the VLAN ports are blocked.

- Use the "gsrp" configuration command to specify a GSRP group ID.
- Executing the "restart gsrp" operation command

(6) Direct link failure detection function

If a transmitter that is installed on a direct link between Switches fails, the backup Switch might assume that a failure has occurred on the master Switch even when the master is running normally. In such cases, the backup Switch might automatically become the master, with the result that two Switches simultaneously act as the master. The same problem might occur when either of two direct links is disconnected. To prevent the problem, before you specify direct-down in the "no-neighbor-to-master" configuration command, create three or more direct links so that at least two direct links are available to send and receive GSRP Advertise frames. You can create the redundant direct links by using link aggregation or multiple normal ports. The effect is the same.

When Layer 3 redundancy switching function requires a VLAN on direct links to continue communication with the upstream network, use link aggregation to assign the redundant direct links.

(7) Creating a network when using GSRP

A network using GSRP is basically a loop configuration. To prevent frames from looping, take the following steps when you create a GSRP network:

- When you configure Switches as GSRP Switches, disable the ports on the Switches beforehand by specifying shutdown. After configuring the GSRP switches, wait until the status transition of the GSRP switches is complete and then start operation.
- Start one of the two Switches that make up a GSRP group, configure the Switch, and make sure that its state changes to the backup status. Next, start the other Switch and configure it.
- When the GSRP VLAN group-only control function has been configured, the VLANs that do not belong to any VLAN group are up. If you want to place a VLAN in a VLAN group, disable the VLAN beforehand, wait until the status of the VLAN group is determined, and then enable the VLAN. If you want to delete a VLAN from a VLAN group, disable the VLAN beforehand to prevent looping.

(8) Changing the ports assigned to VLANs while using GSRP

GSRP uses the number of active ports as a condition for selecting the master and backup switches. The number of active ports refers to the number of ports assigned to the VLANs that belong to a VLAN group. The number of active ports changes when you add a port to a VLAN or change the network configuration. In these cases, the same change is normally applied to both the master and backup switches. However, if the number of active ports for the backup switch temporarily exceeds that of the master switch while the change is applied, the master and backup switches are switched over.

To prevent the switchover, take the following steps when you change the ports assigned to VLANs:

- Lock the current master by setting priority level as the highest-priority condition for selecting the master and backup switches ("selection-pattern" configuration command). You can lock the current master because the GSRP switch with higher priority is the master. Next, change the ports that are to be assigned to the VLANs.
- If you need to perform a major change that requires changes to the cabling or a restart of switches, use backup locking function to force one GSRP switch into the backup status. Next, make the other GSRP switch the master for all VLAN groups, and then change the ports assigned to the VLANs.

(9) When a GSRP-unaware switch relays GSRP control frames

When all the neighboring switches of a GSRP switch are GSRP-unaware, GSRP control frames are flooded. As a result, the GSRP control frames might be forwarded to locations in the topology that does not require such frames. To prevent the unnecessary forwarding of control frames, also correctly configure GSRP-managed VLANs on GSRP-unaware switches.

(10) Forwarding GSRP Flush request frames

GSRP-aware switches flood GSRP Flush request frames. Because GSRP switches do not flood GSRP Flush request frames, you cannot have GSRP switches forward GSRP Flush request frames in a multi-stage configuration of GSRP groups.

(11) Remotely managing Switches when using GSRP

If you want to use telnet or SNMP to remotely manage the Switches that use GSRP, configure the following:

- Ports that are not under GSRP control
- Use the GSRP VLAN group-only control function to configure the VLAN interfaces of VLANs that do not belong to any VLAN group.

(12) Ports not controlled by GSRP

The ports that are specified as ports not under GSRP control can always be used to send and receive traffic regardless of whether the switch is the master or the backup. Therefore, the IP interface of the VLANs that contain such ports is up. Use caution in a network configuration that expects the IP interface to go down, such as when Layer 3 redundancy switching function is used.

(13) Interoperability

GSRP is a special feature deployed only on Switches. GSRP cannot communicate with the Extreme Standby Router Protocol (ESRP) employed on LAN switches manufactured by Extreme Networks or the Virtual Switch Redundant Protocol (VSRP) employed on LAN switches manufactured by Brocade Communications Systems.

(14) If CPU load is excessive

If the CPU is overloaded, the GSRP Advertise frames sent and received by the Switches might be dropped or their processing might be delayed, causing output of timeout messages and status transitions. If CPU overload is frequent, specify a longer sending interval and retention time for GSRP Advertise frames.

(15) Learning virtual MAC addresses

When you use Layer 3 redundancy switching function, the MAC address of the default gateway for which GSRP is providing redundancy is a virtual MAC address. Conversely, the source MAC addresses in forwarded IP packets or frames that are voluntarily sent by the Switch are not virtual MAC addresses. Instead, a source MAC address is the MAC address of a switch or a VLAN.

GSRP periodically sends frames for virtual MAC address learning to the devices that use a GSRP switch as the default gateway to allow them to learn the virtual MAC address of the default gateway. Frames for virtual MAC address learning are non-IP unicast frames with virtual MAC addresses as the source MAC addresses.

Design the network so that all the devices receive GSRP control frames when they use a GSRP switch as the default gateway. If GSRP control frames are filtered out by a firewall, the devices will not be able to learn virtual MAC addresses, resulting in flooded GRSP control frames that might affect network operation.

14 Settings and Operation for GSRP

This chapter provides examples of GSRP function configuration.

14.1 Configuration

14.1.1 List of configuration commands

The following table describes the list of configuration commands for GSRP.

Table 14-1: List of configuration commands

Command name	Description
advertise-holdtime	Sets the retention time for GSRP Advertise frames.
advertise-interval	Sets the sending interval for GSRP Advertise frames.
backup-lock	Enables backup locking.
flush-request-count	Sets the number of times that GSRP Flush request frames are sent.
gsrp	Enables GSRP.
gsrp-vlan	Configures a GSRP-managed VLAN.
gsrp direct-link	Configures a direct link.
gsrp exception-port	Configures a port not under GSRP control.
gsrp limit-control	Enables GSRP VLAN group-only control function.
gsrp no-flush-port	Configures a port that does not send GSRP Flush request frames.
gsrp reset-flush-port	Configures a port on which port resetting is used.
layer3-redundancy	Enables Layer 3 redundancy switching function.
no-neighbor-to-master	Sets the switchover method to be used when a switch is in the backup (neighbor unknown) status.
port-up-delay	Enables the prevention of repeated switchover when links are unstable.
reset-flush-time	Sets the length of the link-down time when port resetting is used.
selection-pattern	Sets the priority for selecting the master and backup switches.
virtual-mac-learning-interval	Sets the sending interval for frames for virtual MAC address learning.
vlan-group disable	Disables a VLAN group. The VLANs belonging to a disabled VLAN group stop sending and receiving traffic.
vlan-group priority	Configures the priority of a VLAN group.
vlan-group vlan	Assigns VLANs to a VLAN group.

14.1.2 Configuring basic GSRP settings

(1) Configuring a GSRP group

Points to note

To use GSRP, set a GSRP group ID for the Switch. If a GSRP group ID is set, the Switch will start GSRP. Specify the same GSRP group ID for the neighbor GSRP switch.

When you use Layer 3 redundancy switching function, specify 1, 2, 3, or 4 as the GSRP group ID. If you specify a different number, Layer 3 redundancy switching function cannot be used.

Before you configure GSRP, you need to disable the Spanning Tree Protocol.

Command examples

1. `(config)# spanning-tree disable`

   Disables a Spanning Tree Protocol.

2. `(config)# gsrp 1`

   Sets 1 as the GSRP group ID. When a GSRP group ID has been set, the Switch begins running as a GSRP switch.

Notes

If you set a GSRP group ID when the GSRP VLAN group-only control function has not been configured, all VLANs are controlled by GSRP. The VLAN ports that do not belong to any VLAN group are blocked.

(2) Configuring a GSRP-managed VLAN

Points to note

Specify a VLAN to be used as the GSRP-managed VLAN. If you do not specify a VLAN, VLAN 1 is used as the GSRP-managed VLAN.

The GSRP-managed VLAN is used to send and receive GSRP control frames. Assign the direct links between GSRP switches and the ports to which GSRP-aware switches are connected (if used) to this VLAN. Configure the same VLAN on the GSRP-aware switches by assigning the ports used to connect to GSRP switches.

Command examples

1. `(config)# gsrp 1`

   Switches to GSRP configuration mode.

2. `(config-gsrp)# gsrp-vlan 5`

   Sets VLAN 5 as the GSRP-managed VLAN.

(3) Configuring direct links

Points to note

Configure the ports used for a direct link between GSRP switches. The direct link is configured on Ethernet interfaces or port channel interfaces.

When you use direct link failure detection function, we recommend that you use redundant direct links to decrease the possibility of direct link failures other than those caused by failures on the partner switch. As redundant direct links, you can assign an aggregated link or multiple normal links. The effect is the same. When Layer 3 redundancy switching function requires a VLAN on direct links to continue communication with the upstream network, use link aggregation to assign the redundant direct links.

Command examples

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

   Switches ports 1/0/1 and 1/0/2 to Ethernet interface configuration mode. To create redundant direct links, multiple ports are specified.

2. `(config-if-range)# channel-group 10 mode on`
   `(config-if-range)# exit`
   Adds ports 1/0/1 and 1/0/2 to channel group 10 in static mode.
3. `(config)# interface port-channel 10`
   `(config-if)# gsrp 1 direct-link`
   Sets channel group 10 as the direct links for GSRP group ID 1.

(4) Configuring a VLAN group

Points to note

Configure a VLAN group for GSRP and the VLANs that participate in the VLAN group. The VLANs in the VLAN group with the master switch can process traffic. You can specify multiple VLAN groups. Each VLAN group has a master and a backup switch. Configure the same VLAN group and participating VLANs for both of the GSRP switches.

To add a VLAN to a VLAN group, use the "vlan-group vlan add" command. To delete a VLAN from a VLAN group, use the "vlan-group vlan remove" command. If you use the "vlan-group vlan" command to specify VLANs for a VLAN group, and then use the same command again to specify other VLANs, the previously specified VLANs will be replaced by the new VLANs.

If you want to stop communication by a VLAN group, use the "vlan-group disable" command to disable the VLAN group.

Command examples

1. `(config)# gsrp 1`
   Switches to GSRP configuration mode.
2. `(config-gsrp)# vlan-group 1 vlan 10,20`
   Creates VLAN group 1, and assigns VLANs 10 and 20 to it.
3. `(config-gsrp)# vlan-group 1 vlan add 30`
   Adds VLAN 30 to VLAN group 1.
4. `(config-gsrp)# vlan-group 1 vlan remove 20`
   Deletes VLAN 20 from VLAN group 1.
5. `(config-gsrp)# vlan-group 1 vlan 100,200`
   Assigns VLANs 100 and 200 to VLAN group 1. The previously specified VLANs are replaced by VLANs 100 and 200.

Notes

The behavior of a VLAN that does not belong to any VLAN group depends on whether the GSRP VLAN group-only control function has been configured.

If the function has not been configured, GSRP controls all VLANs. Therefore, the VLAN ports that do not belong to any VLAN group are blocked.

If the function has been configured, GSRP controls only the VLANs that belong to VLAN groups. Therefore, the VLAN ports that do not belong to any VLAN group can forward frames.

14.1.3 Configuring the selection of the master and backup switches

(1) Configuring the priority of the conditions for selecting the master and backup switches

Points to note

Configure the priority of the conditions for selecting the master and backup GSRP switches (number of active ports, priority, and device MAC address). Select either of the following sets of priority: Number of active ports -> priority -> switch MAC address and priority -> number of active ports -> device MAC address.

We recommend that you use number of active ports as the top-priority condition in normal operations. If the number of VLAN ports changes or links need to be taken down when you change the network configuration, you might want to use priority as the top-priority condition. By using priority as the top-priority condition, you can change the network configuration without switching over the master and backup switches.

Command examples

1. `(config)# gsrp 1`

   Switches to GSRP configuration mode.

2. `(config-gsrp)# selection-pattern priority-ports-mac`

   Sets priority -> number of active ports -> device MAC address as the order of priority of conditions.

(2) Configuring the priority of a VLAN group

Points to note

Assign a priority to each VLAN group. The larger the value, the higher the priority. The priority is used to determine the master switch when both devices have the same number of active ports.

You can perform load balancing at the VLAN group level by creating multiple VLAN groups and assigning a different priority to each VLAN group.

Command examples

1. `(config)# gsrp 1`

   Switches to GSRP configuration mode.

2. `(config-gsrp)# vlan-group 1 priority 80`

   Sets 80 as the priority of VLAN group 1.

(3) Enabling backup locking

Points to note

Backup locking forcibly places all the VLAN groups of one GSRP switch in the backup status. You might want to use backup locking when you perform a large-scale configuration change that requires the changing of cables or restarting of a GSRP switch. By using backup locking, you can make one GSRP switch as the master for all VLAN groups while you perform a configuration change involving the other GSRP switch.

Command examples

1. `(config)# gsrp 1`

   Switches to GSRP configuration mode.

2. `(config-gsrp)# backup-lock`

   Enables backup locking. All VLAN groups of the target GSRP switch enter the backup status, and the neighbor GSRP switch becomes the master.

14.1.4 Configuring Layer 3 redundancy switching function

Points to note

Enable Layer 3 redundancy switching function on both GSRP Switches. Layer 3 redundancy switching function can be used only when the GSRP group ID is 1, 2, 3, or 4. When Layer 3 redundancy switching function is used, the device under the downstream network learns the virtual MAC address for GSRP by receiving the frame for virtual MAC address learning. These device become flooded when aging occurs on the learned MAC address. Also, when a device is added to the downstream network, this device becomes flooded until the device receives a frame for virtual MAC address learning. Set the sending interval for frames for virtual MAC address learning by taking into account the amount of time flooding will occur.

When you use Layer 3 redundancy switching function, assign the same IP addresses to VLANs on both GSRP switches. For information on how to set the IP address, see "Configuration Guide Vol. 1, 24.9 VLAN interface". In addition, when you use Layer 3 redundancy switching function, you must configure a special path to continue communication with the upstream network even if a GSRP switch fails. For details, see "13.5.3 Switchover due to a failure in the upstream network when Layer 3 redundancy switching function is used".

Command examples

1. `(config)# gsrp 1`
   Switches to GSRP configuration mode.
2. `(config-gsrp)# layer3-redundancy`
   Enables Layer 3 redundancy switching function.
3. `(config-gsrp)# virtual-mac-learning-interval 100`
   Sets the sending interval for frames for virtual MAC address learning to 100 seconds.

14.1.5 Configuring the GSRP VLAN group-only control function

Points to note

Enables GSRP VLAN group-only control function. When this function is enabled, GSRP controls only the VLANs that belong to VLAN groups. The VLAN ports that do not belong to any VLAN group are always able to forward frames.

You can use the GSRP VLAN group-only control function for the following purposes:

- To make it easier for Layer 3 redundancy switching function to provide a connection to the upstream network
- To use VLANs that do not belong to any GSRP VLAN group as VLANs that are not under GSRP control
- To remotely manage the Switches

Command examples

1. `(config)# gsrp limit-control`
   Enables GSRP VLAN group-only control function.

14.1.6 Configuring ports not under GSRP control

Points to note

Set a port or link aggregation port as a port not under GSRP control. When you set Ethernet interfaces or port channel interfaces as such ports, those interfaces are always able to forward frames regardless of the status of GSRP switches.

You can use ports that are not under GSRP control for the following purposes:

- To make it easier for Layer 3 redundancy switching function to provide a connection to the upstream network
- To remotely manage the Switches

Command examples

1. `(config)# interface gigabitethernet 1/0/1`
   Switches to the Ethernet interface configuration mode for port 1/0/1.
2. `(config-if)# gsrp exception-port`
   Sets port 1/0/1 as a port not under GSRP control.

14.1.7 Configuring GSRP parameters

(1) Enabling the function preventing repeated switchover for unstable links

GSRP uses the number of active ports as the condition for selecting the master and backup switches. If ports become unstable (for example, ports are frequently enabled and disabled), the number of active ports changes frequently, leading to repeated switchovers between the master and backup switches. If ports are unstable, use this command to specify a delay time to prevent unnecessary switchovers.

Points to note

Specify a time for delaying the inclusion of ports that have come up in the number of active ports.

If you specify infinity, the delay time is unlimited and the ports that come up are not automatically included in the number of active ports. If you do not specify a delay time, ports that come up are immediately included in the number of active ports (delay time is 0 seconds).

Command examples

1. `(config)# gsrp 1`
   Switches to GSRP configuration mode.
2. `(config-gsrp)# port-up-delay 10`
   Sets 10 seconds as the time for delaying the inclusion of ports that come up in the number of active ports.
3. `(config-gsrp)# port-up-delay infinity`
   Changes the delay time. infinity is specified as the time for delaying the inclusion of ports that come up in the number of active ports. After this specification, to include enabled ports in the number of active ports, you need to use the "clear gsrp port-up-delay" command.

(2) Specifying the sending interval and retention time of GSRP Advertise frames

Points to note

Set the sending interval and retention time of GSRP Advertise frames. For advertise-holdtime, specify a value greater than advertise-interval. If you specify a value equal to or less than advertise-interval for advertise-holdtime, the Switch detects a timeout for receiving GSRP Advertise frames.

Command examples

1. `(config)# gsrp 1`
   Switches to GSRP configuration mode.

2. `(config-gsrp)# advertise-interval 5`
   Sets 5 seconds as the sending interval of GSRP Advertise frames.
3. `(config-gsrp)# advertise-holdtime 20`

   Sets 20 seconds as the retention time of GSRP Advertise frames. In this case, if a switch does not receive GSRP Advertise frames more than three times, a timeout occurs.

Notes

If CPU load is excessive, the GSRP Advertise frames exchanged between Switches might be dropped or their processing might be delayed. In such cases, a timeout message might be output or the master and backup Switches might be switched over. If excessive CPU load is frequent, specify a longer sending interval and retention time for GSRP Advertise frames.

(3) Configuring ports that do not send GSRP Flush request frames

Points to note

Configure a port or link aggregation port so that it will not send GSRP Flush request frames. You can configure Ethernet interfaces or port channel interfaces this way.

GSRP Flush request frames are sent to all the ports assigned to GSRP-managed VLANs except for direct-link ports and ports on which port resetting is configured. Use this function if you do not want to use port resetting for GSRP-unaware switches that are connected to GSRP switches. However, if you do so, note that communication will not be restored until the MAC address tables on GSRP-unaware switches are cleared due to aging when the master and backup switches are switched over. For normal operation, we recommend that you use port resetting for GSRP-unaware switches connected to GSRP switches.

Command examples

1. `(config)# interface gigabitethernet 1/0/1`
   Switches to the Ethernet interface configuration mode for port 1/0/1.
2. `(config-if)# gsrp 1 no-flush-port`
   Configures port 1/0/1 so that it will not send GSRP Flush request frames.

(4) Specifying the number of times GSRP Flush request frames are sent

Points to note

Specify the number of times GSRP Flush request frames are sent to neighboring switches to request the clearing of MAC address tables.

By default, GSRP Flush request frames are sent three times. If you increase this number, you can decrease the number of lost frames.

Command examples

1. `(config)# gsrp 1`
   Switches to GSRP configuration mode.
2. `(config-gsrp)# flush-request-count 5`
   Sets 5 as the number of times GSRP Flush request frames are sent.

14.1.8 Configuring port resetting

Use the port resetting function for GSRP-unaware switches that are connected to a GSRP switch. When the master GSRP switch enters the backup status, it temporarily disables the links on the ports on which resetting is configured.

(1) Configuring a port on which port resetting is to be used

Points to note

Configure port resetting. You can configure Ethernet interfaces or port channel interfaces this way.

Command examples

1. `(config)# interface gigabitethernet 1/0/1`
   Switches to the Ethernet interface configuration mode for port 1/0/1.
2. `(config-if)# gsrp 1 reset-flush-port`
   Configures port resetting on port 1/0/1.

(2) Setting the port-down time

Points to note

Set the port-down time to be applied when port resetting is used. By default, the port-down time is 3 seconds. Set the port-down time if you use port resetting if the link-down detection time of a partner switch is long. If a local GSRP switch is paired with a Switch that can configure the link-down detection time, such as a Switch with a link-down detection timer ("link debounce" configuration command), specify a port-down time that is longer than link-down detection time.

Command examples

1. `(config)# gsrp 1`
   Switches to GSRP configuration mode.
2. `(config-gsrp)# reset-flush-time 5`
   Sets 5 seconds as the port down time.

14.1.9 Configuring direct link failure detection

Points to note

To allow a GSRP switch in the backup (neighbor unknown) status to take over the master that failed due to a direct-link failure, you can choose whether to perform manual switchover (by entering a command that change the switch status to the master status) or automatic switchover (direct link failure detection function).

If you use direct link failure detection function to perform automatic switchover, we recommend that you configure redundant direct links to decrease the possibility of direct link failures other than those caused by failures on the partner switch. As redundant direct links, you can assign an aggregated link or multiple normal links. The effect is the same. When Layer 3 redundancy switching function requires a VLAN on direct links to continue communication with the upstream network, use link aggregation to assign the redundant direct links.

Command examples

1. `(config)# gsrp 1`
   Switches to GSRP configuration mode.

2. `(config-gsrp)# no-neighbor-to-master direct-down`
   Configure direct link failure detection function to automatically change the backup switch status to the master status when a direct-link failure occurs.

14.2 Operation

14.2.1 List of operation commands

The following table describes the list of operation commands for GSRP.

Table 14-2: List of operation commands

Command name	Description
show gsrp	Shows GSRP information.
show gsrp aware	Shows GSRP aware information.
clear gsrp	Clears the GSRP statistics.
set gsrp master	Changes backup (neighbor unknown) status to master status.
clear gsrp port-up-delay	Includes ports that are assigned to the VLANs in VLAN groups and that have come up in the number of active ports without waiting for the delay time specified in the "port-up-delay" configuration command to expire.
clear gsrp forced-shift	Cancels the wait period for automatically switching to the master status when the function for switchover to the master status by an independently started GSRP switch is enabled.
restart gsrp	Restarts the GSRP program.
dump protocols gsrp	Dumps detailed event trace information and control table information collected by the GSRP program to a file.

14.2.2 Checking the GSRP status

When you configure GSRP on the Switch, you can check the GSRP status at the following points.

(1) Check after configuration

Use the "show gsrp" command to check the GSRP configuration. You can check whether the GSRP configuration set with configuration commands is correct. You can also check whether the priority of the master and backup selection conditions (Selection Pattern), the Layer 3 redundancy switching settings, the VLAN group IDs, and the VLANs that belong to VLAN groups are the same on both Switches in a GSRP group. If Layer 3 redundancy switching function is configured, you can check whether the IP addresses assigned to the VLANs belonging to VLAN groups are the same on both GSRP switches. For confirmation of IP address, see "Configuration Guide Vol. 1, 24.11.2 Checking the VLAN status" and "Configuration Guide Vol. 3, 2.2.2 Checking the up/down status for an IPv4 interface" or "Configuration Guide Vol. 3, 19.2.2 Checking the up/down status of an IPv6 interface". Note that, in the backup status, the interfaces are down for the VLANs that belong to VLAN groups.

The following figures show example results of executing the "show gsrp detail" command and the "show gsrp vlan-group" command.

Figure 14-1: Results of executing the show gsrp detail command

```
> show gsrp detail
Date 20XX/11/07 22:24:36 UTC

GSRP ID: 1
 Local MAC Address       : 0012.e205.0000
 Neighbor MAC Address    : 0012.e205.0011
 Total VLAN Group Counts : 2
 GSRP VLAN ID            : 105
 Direct Port             : 0/10-11
 Limit Control           : Off
```

```
 GSRP Exception Port     : 0/1-5
 No Neighbor To Master   : manual
 Backup Lock             : disable
 Port Up Delay           : 0
 Last Flush Receive Time : -
 Forced Shift Time       : -
 Layer 3 Redundancy      : On
 Virtual MAC Learning    : Interval 120  (Output rate 30pps)
 VLAN Port Counts        : Configuration    15,  Capacity 3600
 Virtual Link ID         : 100(VLAN ID : 20)

                           Local               Neighbor
 Advertise Hold Time     : 5                   5
 Advertise Hold Timer    : 4                   -
 Advertise Interval      : 1                   1
 Selection Pattern       : ports-priority-mac  ports-priority-mac

 VLAN Group ID      Local State         Neighbor State
 1                  Backup              Master
 8                  Master              Backup
>
```

Figure 14-2: Results of executing the show gsrp vlan-group command

```
> show gsrp 1 vlan-group 1
Date 20XX/11/07 22:25:13 UTC

GSRP ID: 1
 Local MAC Address       : 0012.e205.0000
 Neighbor MAC Address    : 0012.e205.0011
 Total VLAN Group Counts : 1
 Layer 3 Redundancy      : On
 Virtual MAC Learning    : Interval 120  (Output rate 30pps)
 VLAN Port Counts        : Configuration    15,  Capacity 3600

 VLAN Group ID : 1
  VLAN ID                : 110,200-210
  Member Port            : 0/6-8
  Last Transition        : 20XX/11/07 22:20:11  (Master to Backup)
  Transition by reason   : Priority was lower than neighbor's
  Master to Backup Counts : 4
  Backup to Master Counts : 4
  Virtual MAC Address    : 0000.8758.1307

                           Local               Neighbor
  State                  : Backup              Master
  Acknowledged State     : Backup              -
  Advertise Hold Timer   : 3                   -
  Priority               : 100                 101
  Active Ports           : 3                   3
  Up Ports               : 3                   -
>
```

(2) During operation

A pair of Switches forms a GSRP group. You can check whether either switch is the master for a VLAN group. You can also check whether each VLAN group has only one master. By using the "show gsrp" command, you can check with which VLAN group each of the paired Switches is associated.

Figure 14-3: Results of executing the show gsrp command

```
> show gsrp
Date 20XX/11/07 22:28:38 UTC

GSRP ID: 10
 Local MAC Address       : 0012.e205.0000
 Neighbor MAC Address    : 0012.e205.0011
 Total VLAN Group Counts : 2
 Layer 3 Redundancy      : On
 Virtual MAC Learning    : Interval 120  (Output rate 30pps)
 VLAN Port Counts        : Configuration    15,  Capacity 3600

 VLAN Group ID      Local State         Neighbor State
 1                  Backup              Master
 8                  Master              Backup
>
```

14.2.3 Using a command to change the status of a switch

You can use the "set gsrp master" command to change a switch in the backup (neighbor unknown) status to the master status.

This command is effective only for backup (neighbor unknown) status. Execute this command after making sure the applicable VLAN group of the partner switch is in backup status.

Figure 14-4: Results of executing the set gsrp master command

```
> set gsrp master 1 vlan-group 1
Transit to Master. Are you sure? (y/n):y
>
```

14.2.4 Immediately including enabled ports in the number of active ports without waiting for the delay time to expire

When using the function for preventing repeated switchovers for unstable links ("port-up-delay" configuration command), use the "clear gsrp port-up-delay" command to immediately include ports that have come up in the number of active ports without waiting for the delay time to expire.

Figure 14-5: Results of executing the clear gsrp port-up-delay command

```
> clear gsrp port-up-delay port 0/1
>
```

15 VRRP

The Virtual Router Redundancy Protocol (VRRP) is hot standby function for securing communication paths for terminals via another router on the same Ethernet LAN if the original router fails. This chapter describes VRRP.

15.1 Description

The Virtual Router Redundancy Protocol (VRRP) is hot standby function for securing communication paths for terminals via another router on the same Ethernet LAN if the original router fails.

By using VRRP, you can create a virtual router that is a representation of multiple routers working as a group on the same Ethernet LAN. When a terminal specifies this virtual router as its default gateway, if the original router fails, the terminal can continue communication without any awareness that it is actually using another router.

A virtual router has a virtual router identifier (VRID) selected from a range from 1 to 255. The physical routers that participate in a virtual router on the same Ethernet LAN use the same virtual router identifier. Among such physical routers, one router operates as the master virtual router and routes packets. The other router or routers, called backup virtual routers, wait in hot standby status and do not route packets.

15.1.1 MAC address and IP address of the virtual router

A virtual router has a virtual MAC address. When a physical router running VRRP (VRRP router) operates as the master of a virtual router, it uses the virtual MAC address instead of its own physical MAC address. A virtual MAC address is automatically generated from the virtual router identifier.

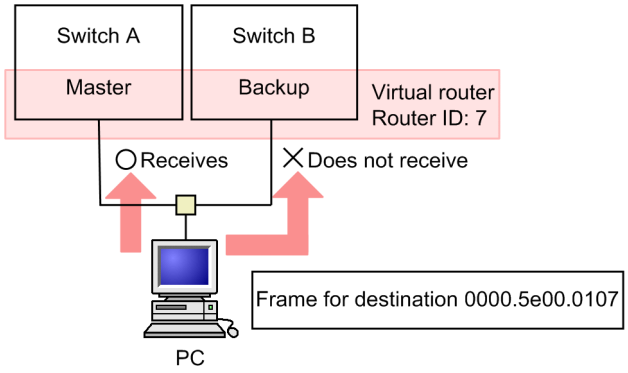
The following table describes the supported VRRP specifications and corresponding virtual MAC addresses.

Table 15-1: VRRP standards and virtual MAC addresses

Standards		Virtual MAC address
IPv4	RFC 3768	0000.5e00.01 {Virtual router ID}
IPv6	draft-ietf-vrrp-ipv6-spec-02	0000.5e00.01 {Virtual router ID}
	draft-ietf-vrrp-ipv6-spec-07	0000.5e00.02 {Virtual router ID}

When the master virtual router receives an Ethernet frame for the virtual MAC address, it forwards the packet. Backup virtual routers do not receive frames for the virtual MAC address. VRRP selects the virtual router that receives Ethernet frames for the virtual MAC address based on the status of the virtual routers. When the master virtual router receives a frame for the virtual MAC address, it forwards the IP packet based on its routing table. Because terminals send frames to the virtual MAC address, they can continue communication even if the master and backup routers are switched over. The following figure shows how a frame for the virtual MAC address is received.

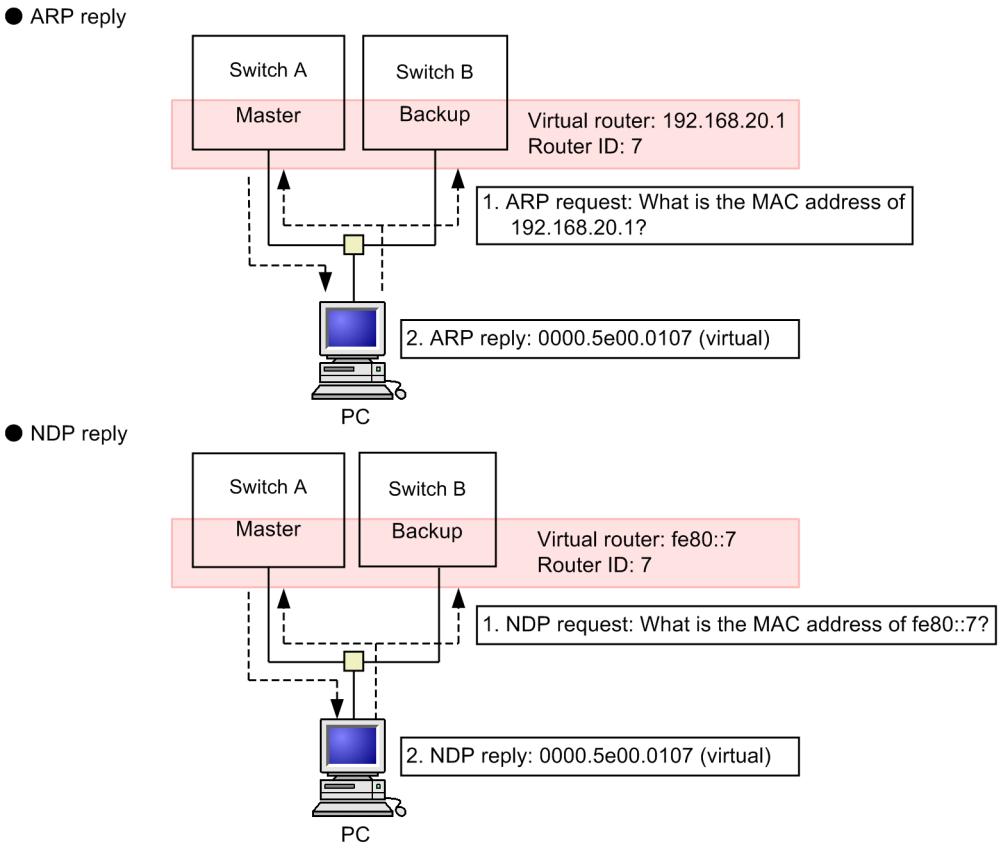
Figure 15-1: Receiving a frame for the virtual MAC address



A virtual router also has a virtual IP address. When the master virtual router receives an ARP request packet or an NDP request packet sent to the virtual IP address, it always uses the virtual MAC address to send an ARP reply or NDP reply. The following figure shows an example of an ARP reply and NDP reply with a

virtual MAC address.

Figure 15-2: ARP reply and NDP reply with a virtual MAC address

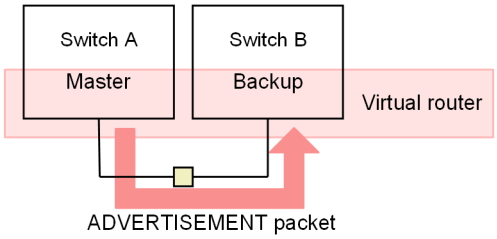


A host (such as a PC) that uses a virtual router as its default router receives the virtual MAC address when it receives an ARP reply from the virtual router. When the host obtains the virtual MAC address, it records the virtual IP address-virtual MAC address combination in its ARP cache. Thereafter, the host always specifies the virtual MAC address as the destination when it sends frames to the virtual router. This way, the host can continue communication even if the VRRP master and backup routers are switched over.

15.1.2 Mechanism of failure detection in VRRP

The master virtual router periodically (every second by default) sends ADVERTISEMENT packets from the IP interface on which the virtual router is configured to report its operating status to the backup virtual routers. When the backup virtual routers receive an ADVERTISEMENT packet from the master virtual router, they know the master virtual router is running normally. The following figure shows an example of sending an ADVERTISEMENT packet.

Figure 15-3: Sending an ADVERTISEMENT packet



If the master virtual router fails, it cannot send ADVERTISEMENT packets. A failure can occur, for exam-

ple, if the entire Switch has failed, a failure prevents the IP interface on which the virtual router is configured from sending packets, or cables are disconnected.

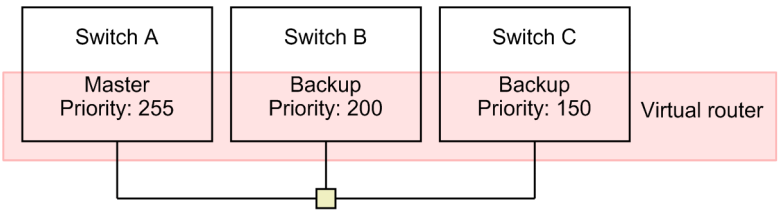
If backup virtual routers do not receive an ADVERTISEMENT packet from the master virtual router for a specified period, they determine that the master virtual router has failed, and one of them enters the master status.

15.1.3 Selecting the master

(1) Priority

VRRP uses priority to select the master virtual router from a group of virtual routers. Assign a priority to each virtual router in the range from 1 to 255. The default value is 100. Larger values indicate higher priority. When the real IP address assigned to a virtual router's interface is the same as the virtual router's virtual IP address, the virtual router is the IP address owner and automatically has the highest priority (255). The following figure shows how the master virtual router is selected.

Figure 15-4: Selecting the master



In this figure, switch A is the master virtual router because it has the highest priority. If switch A goes down, switch B becomes the master virtual router because it has the next highest priority. Switch C becomes the master virtual router only if both switches A and B go down.

To be able to select the master router unambiguously, assign different priorities to the virtual routers that have the same virtual router identifier on the same Ethernet LAN. If multiple virtual routers have the same priority, you will not know which router becomes the master. This could result in unintended behavior.

(2) Performing and suppressing automatic switch-back

In VRRP operation, if a backup virtual router discovers that the master virtual router has a lower priority that itself, the backup virtual router automatically becomes the master. If the master virtual router detects a backup virtual router with a higher priority than itself, the master virtual router automatically becomes a backup.

Consider the configuration in "Figure 15-4: Selecting the master". Suppose switches A and B have both gone down and switch C is the master virtual router. When switch B is restored, switch B becomes the master virtual router because it has a higher priority than switch C, and switch C becomes a backup virtual router again.

You can suppress this automatic preemption by using either of the following methods.

- Using PREEMPT mode

  If you prefer to suppress automatic switch-back, use the "no vrrp preempt" configuration command to turn off PREEMPT mode. When you turn off PREEMPT mode, a backup virtual router with a higher priority than the master virtual router does not become the master.

- Using a suppression timer

If you want to delay the start of automatic switch-back for a particular period, use the "vrrp preempt delay" configuration command to configure the suppression timer. The timer value delays the start of automatic switch-back processing after a cause for invoking automatic switch-back is detected. For automatic switch-back to be completed, the specified length of time and several additional seconds are required.

Whether you use PREEMPT mode or the suppression timer, automatic switch-back cannot be used if the applicable VRRP router is the IP address owner (priority: 255).

If a backup virtual router detects that the master virtual router is inoperable due to a failure and the backup router knows it has the highest priority among the remaining routers, it becomes the master even if automatic switch-back is suppressed.

- Manual switch-back

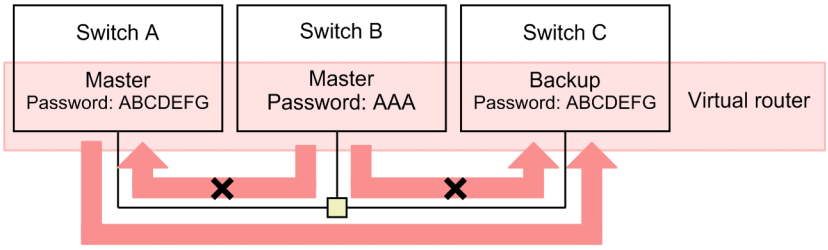
  When automatic switch-back is suppressed, you can use the "swap vrrp" operation command to start switch-back processing for virtual routers.

  When you specify this command for a router remaining in the backup status due to automatic switch-back suppression, the router becomes the master if it has a higher priority than the master virtual router at the time the command is executed.

15.1.4 Authenticating ADVERTISEMENT packets

ADVERTISEMENT packets are sent to the multicast address (224.0.0.18 for IPv4 and ff02::12 for IPv6) in the link-local scope. Virtual routers only receive packets with 255 as the TTL or hop limit in IP headers as a means of preventing remote attacks from beyond the routers. Also note that the Switch supports VRRP ADVERTISEMENT packet authentication that uses text passwords. When you assign a password consisting of eight or fewer characters to each virtual router, the virtual routers discard ADVERTISEMENT packets if the passwords do not match. The following figure shows the result when the passwords do not match.

Figure 15-5: When passwords do not match



In this example, the password of switch B differs from that of switch A or C. Therefore, when switch A or C receives an ADVERTISEMENT packet from switch B, they discard it. In the case here, switch C receives and processes only the ADVERTISEMENT packets from switch A. This function prevents the behavior of an illegally installed virtual router because it will fail ADVERTISEMENT packet authentication.

15.1.5 Accept mode

The virtual router, unless it is the IP address owner, does not reply to the packets sent to the virtual IP address even if it is the master. In general, however, such a virtual router will check the status of network devices by pinging them.

The switch supports an accept mode. In accept mode, the master virtual router can reply to the packets sent to the virtual IP address. Even if the master virtual router is not the IP address owner, you can use the "vrrp accept" configuration command to specify accept mode and allow the master virtual router to receive ICMP Echo Request packets and send ICMP Echo Reply packets. This command allows you to check the status of VRRP routers externally.

15.1.6 Tracking function

This Switch has a function to monitor network faults and dynamically operate priority of virtual router (tracking function) in the format of fault monitoring interfaces and VRRP polling.

If a failure occurs on an interface on which a virtual router is configured, a backup router takes over as the master router. However, if a failure occurs on an interface on which no virtual router is configured, such as an IP interface, a port channel interface, or an Ethernet interface that is the destination of packet routing, no backup router takes over as the master even if communication is disabled.

As a unique additional function, the Switch provides functionality for monitoring the VLAN interfaces, port channel interfaces, and Ethernet interfaces on it and for lowering the priorities of virtual routers if the interfaces go down. This tracking function is called fault monitoring interfaces. Note that an IP address must be assigned to a VLAN interface if you want to monitor it for failures.

The fault monitoring interfaces cannot detect failures that occur beyond the routers because they can only monitor the failures that are manifested as interface-down failures. The Switch has another special function that can be used as tracking functionality. VRRP polling monitors the specified VLAN interfaces, checks the reachability of the specified destinations by pinging them, and lowers the priorities of virtual routers if no reply is returned. This tracking function is called VRRP polling.

You can use the fault monitoring interfaces to monitor the failures that occur between the Switch and neighboring devices. You can use VRRP polling to monitor the failures that occur between the Switch and devices located beyond the routers.

Two methods are provided for changing the priorities of virtual routers.

One method is priority switching. Priority switching allows you to change the priority of a virtual router to the value specified in the "vrrp track priority" configuration command when the tracking function detects a failure on it.

The other is priority decrement. Priority decrement subtracts the value specified in the "vrrp track decrement" configuration command for the fault monitoring interfaces from the priority value of a virtual router when the tracking function detects a failure.

For priority switching, you can specify one fault monitoring interface or one instance of VRRP polling. For priority decrement, you can specify multiple fault monitoring interfaces and multiple instances of VRRP polling.

When the priority of a virtual router becomes 0 as a result of executing tracking function, the IP interface on which the virtual router is configured goes down.

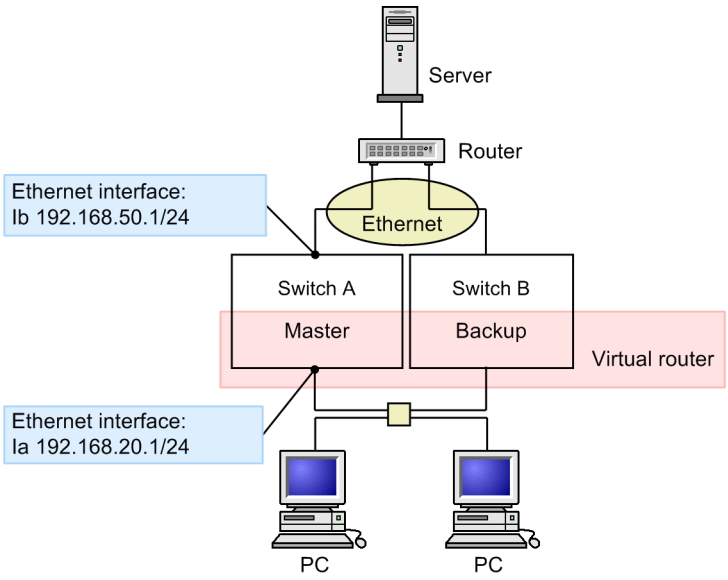
Table 15-2: Combinations of method for changing the priority and monitoring method

Method for changing priority	Fault monitoring interfaces	VRRP polling
Priority switching	Only one instance of polling can be specified.	Only one instance of polling can be specified.
Priority decrement	Multiple instances of polling can be specified.	Multiple instances of polling can be specified.

(1) Fault monitoring interfaces

The following figure shows fault monitoring interfaces for a virtual router.

Figure 15-6: Fault monitoring interfaces



In this example, VLAN interfaces are specified as fault monitoring interfaces. VLAN interface Ia and VLAN interface Ib are assigned to Switch A. The virtual router is configured on VLAN interface Ia. In normal VRRP behavior, if VLAN interface Ib goes down due to a VLAN failure, the behavior of the virtual router is not affected. However, on the Switch, you can change the running status of a virtual router by specifying fault monitoring interfaces and a priority switching value or priority decrement value to be applied if a fault monitoring interface goes down.

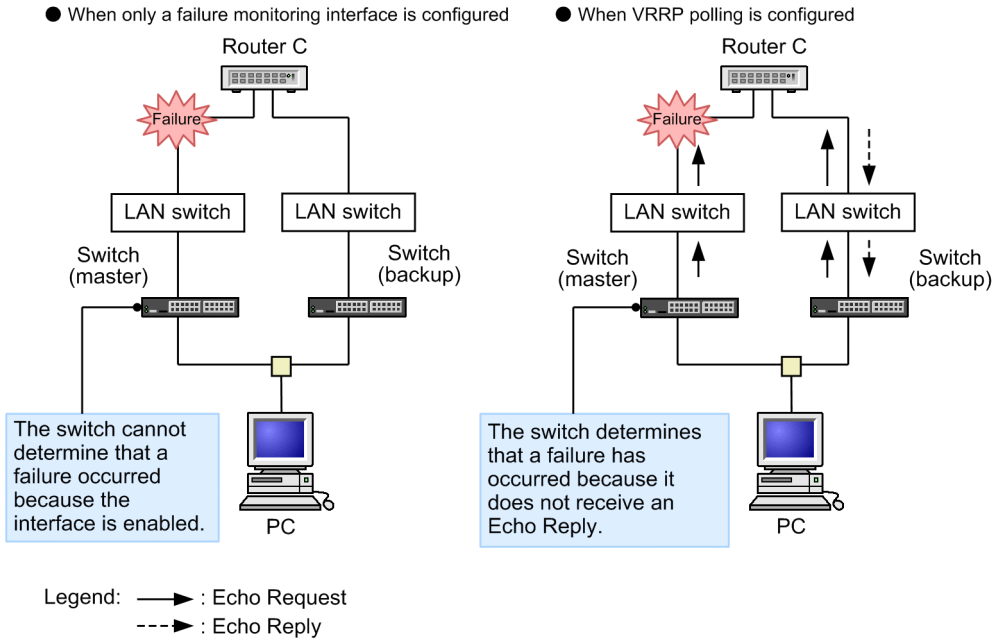
Specify VLAN interface Ib as the fault monitoring interface for the virtual router on Switch A. Specify 0 as the priority to be applied if the fault monitoring interface goes down. If VLAN interface Ib goes down, Switch B automatically takes over for Switch A and becomes the master.

Similarly, you can change the running status of a virtual router by assigning a port channel interface or Ethernet interface as a fault monitoring interface.

(2) VRRP polling

The following figure shows the difference between when VRRP polling is configured and when VRRP polling is not configured.

Figure 15-7: Difference between when VRRP polling is configured and when VRRP polling is not configured



If a failure occurs on the device that is the destination of VRRP polling or if no reply is returned due to a network failure, VRRP polling lowers the priority based on the predefined switching priority or priority decrement.

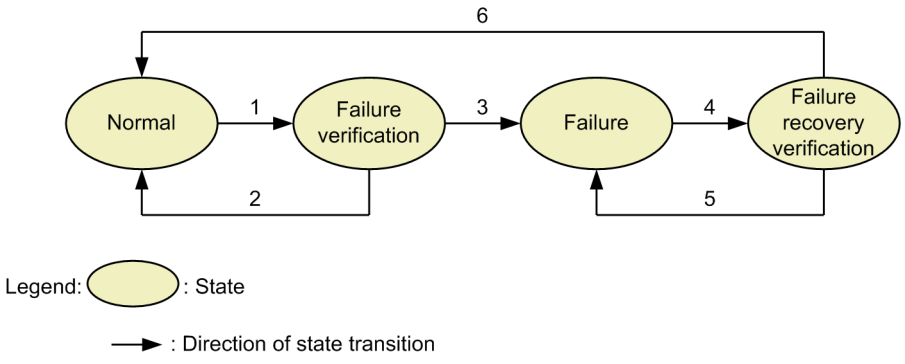
The following table describes the VRRP status and the corresponding priority and intervals of polling attempts.

Table 15-3: VRRP status and the corresponding priority and intervals of polling attempts

Status	Priority	Polling attempt interval
Normal	Priority set by the vrrp priority configuration command	track check-status-interval
Failure detection inspection		track failure-detection-interval
Failure	Based on the switching priority set by the vrrp track priority configuration command or the priority decrement set by the vrrp track decrement configuration command, lowers the priority	track check-status-interval
Failure recovery inspection		track recovery-detection-interval

The following figure shows the status transitions of VRRP polling and transition conditions.

Figure 15-8: Status transitions of VRRP polling and transition conditions



1. No reply was made, and a timeout occurred.
2. Received responses that satisfy the polling success condition[#2] within the number of polling retries[#1]
3. Determined that it is not possible to receive responses that satisfy the polling success condition[#2] within the number of polling retries[#1]
4. Received a response
5. Determined that it is not possible to receive responses that satisfy the polling success condition[#3] within the number of polling retries[#1]
6. Received responses that satisfy the polling success condition[#3] within the number of polling retries[#1]

#1: Set by using the "track check-trial-times" configuration command.

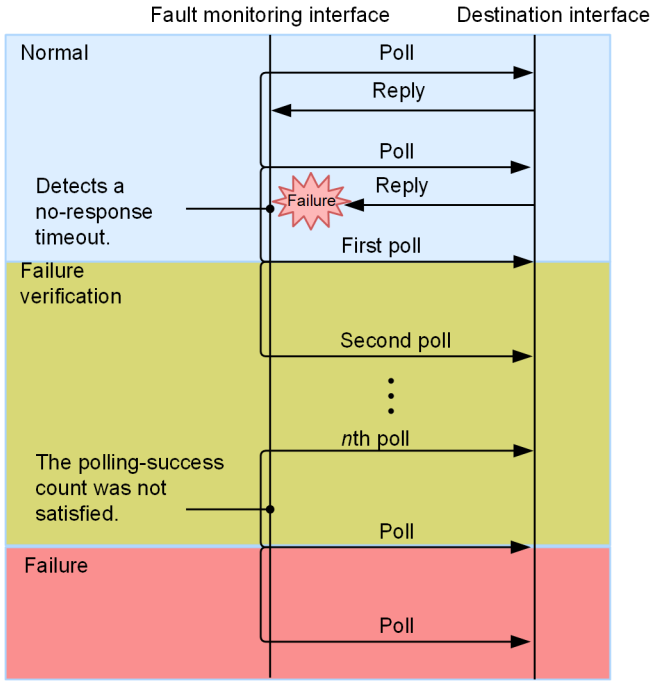
#2: Set by using the "track failure-detection-times" configuration command.

#3: Set by using the "track recovery-detection-interval" configuration command.

● Failure detection inspection behavior

The following figure shows the failure detection inspection sequence.

Figure 15-9: Failure detection inspection sequence



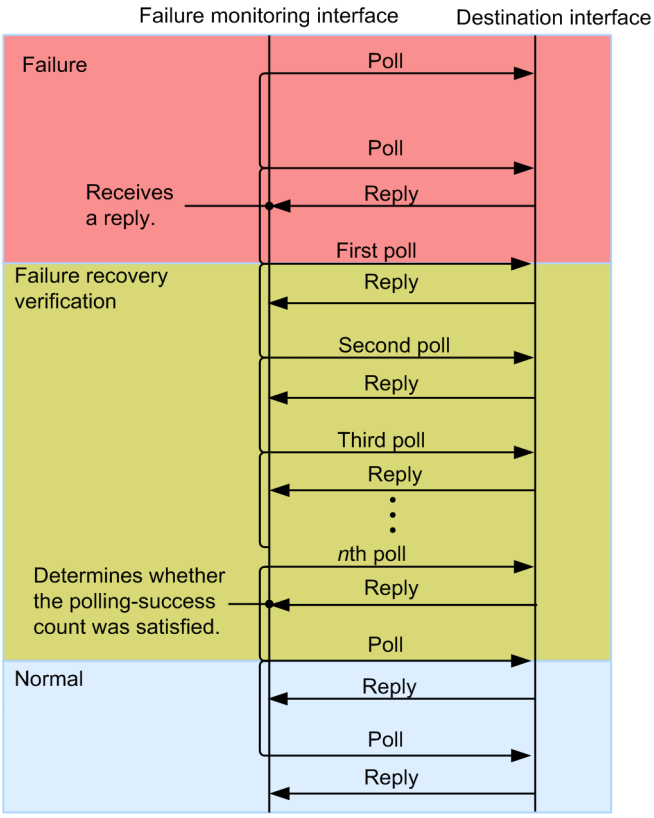
In failure detection inspection, polling is performed at the special intervals. When the Switch determines that it is not possible to satisfy the polling success condition within the number of polling retries (in this figure when the nth response timed out), the Switch determines a failure has occurred and lowers the priority.

In the factory default configuration, the number of polling retries is set to 4. The Switch determines that polling will not succeed within the number of polling retries when two responses time out (four seconds after the failure detection behavior started) and lowers the priority.

● Failure recovery inspection behavior

The following figure shows the failure recovery inspection sequence.

Figure 15-10: Failure recovery inspection sequence



Failure recovery verification performs polling at special intervals. When the Switch satisfies the polling success condition within the number of polling retries (in this figure when the nth response is received), the Switch determines that it has recovered from a failure and returns the priority of the Switch to normal.

In the factory default configuration, the number of polling retries is set to 4. The Switch determines that polling is successful when the Switch receives three responses (six seconds after the failure recovery inspection started) and returns its priority to normal.

If an interface goes down, VRRP polling assumes that a failure has occurred and waits until the interface is enabled. When the interface is enabled, VRRP polling restarts the polling and performs failure recovery verification. When VRRP polling determines that operation is normal, switch-back is performed.

When the IP address of the VRRP polling destination is on the network beyond the routers, the routing tables of the routers are used to determine the IP address. Therefore, "Figure 15-11: When the sending and receiving interfaces do not match", the interface that receives a reply for VRRP polling might not be the interface that sent the VRRP polling request. In this case, specify the receiving interface check ("track check-reply-interface" configuration command) to check the sending interface and receiving interface. Packets are dropped when the sending interface and receiving interface do not match. If the sending and receiving interfaces do not match on a network that is not managed by a Switch, operation is not guaranteed, as shown in "Figure 15-12: When the sending and receiving interfaces do not match on a network not managed by the Switch".

Figure 15-11: When the sending and receiving interfaces do not match

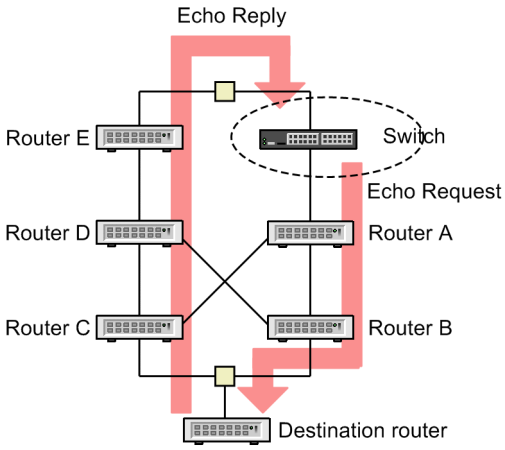
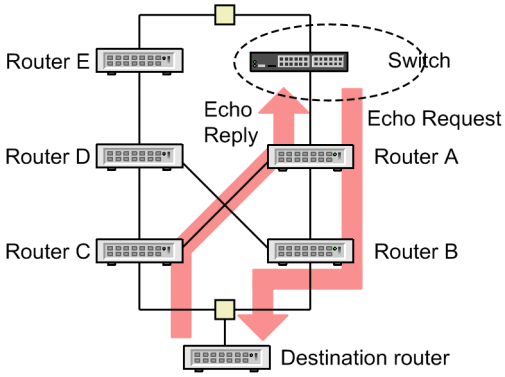


Figure 15-12: When the sending and receiving interfaces do not match on a network not managed by the Switch



15.1.7 Supported VRRP specifications

The Switch supports multiple VRRP specifications. Therefore, you can configure virtual routers as desired according to the specification used in an existing system. To select a VRRP specification for the virtual routers, specify a VRRP behavior mode.

The following table describes the supported VRRP specifications and the commands for specifying the VRRP behavior mode.

Table 15-4: VRRP specifications and the commands for specifying the VRRP behavior mode

Standards		Command for specifying the VRRP behavior mode
IPv4	RFC 3768	The mode is set by IPv4 virtual routers by default.
IPv6	draft-ietf-vrrp-ipv6-spec-02	The mode is set by IPv6 virtual routers by default.
	draft-ietf-vrrp-ipv6-spec-07	vrrp ietf-ipv6-spec-07-mode

The format of an ADVERTISEMENT packet and the meaning of the fields differ according to the specification. If a device that participates in a virtual router uses a different specification, the device might regard an ADVERTISEMENT packet sent from another device as an invalid packet and discard it. In this case, multiple devices might become the master router. To prevent this problem, configure the same VRRP behavior mode on all the devices that participate in a virtual router.

(1) Overview of the default behavior for IPv4 virtual routers

IPv4 virtual routers use VRRP packets of VRRP protocol version 2 (specified in RFC 3768) to send and receive advertisements. The IPv4 virtual routers can authenticate ADVERTISEMENT packets.

Determine the failure detection time based on the sending interval of ADVERTISEMENT packets configured for the Switch. The sending interval of ADVERTISEMENT packets is set in one-second units.

(2) Overview of the default behavior for IPv6 virtual routers

IPv6 virtual routers use VRRP packets of VRRP protocol version 3 (specified in draft-ietf-vrrp-ipv6-spec-02) to send and receive advertisements. The IPv6 virtual routers can authenticate ADVERTISEMENT packets.

Determine the failure detection time based on the sending interval of ADVERTISEMENT packets configured for the Switch. The sending interval of ADVERTISEMENT packets is set in one-second units.

(3) Overview of the behavior for IPv6 virtual routers in vrrp ietf-ipv6-spec-07-mode

Another VRRP behavior mode supported by IPv6 virtual routers is vrrp-ietf-ipv6-spec-07-mode.

The IPv6 virtual routers in this mode use VRRP packets of VRRP protocol version 3 (specified in draft-ietf-vrrp-ipv6-spec-07) to send and receive advertisements.

Determine the failure detection time based on the sending interval of ADVERTISEMENT packets configured for the Switch. The sending interval of ADVERTISEMENT packets is set in one-second units.

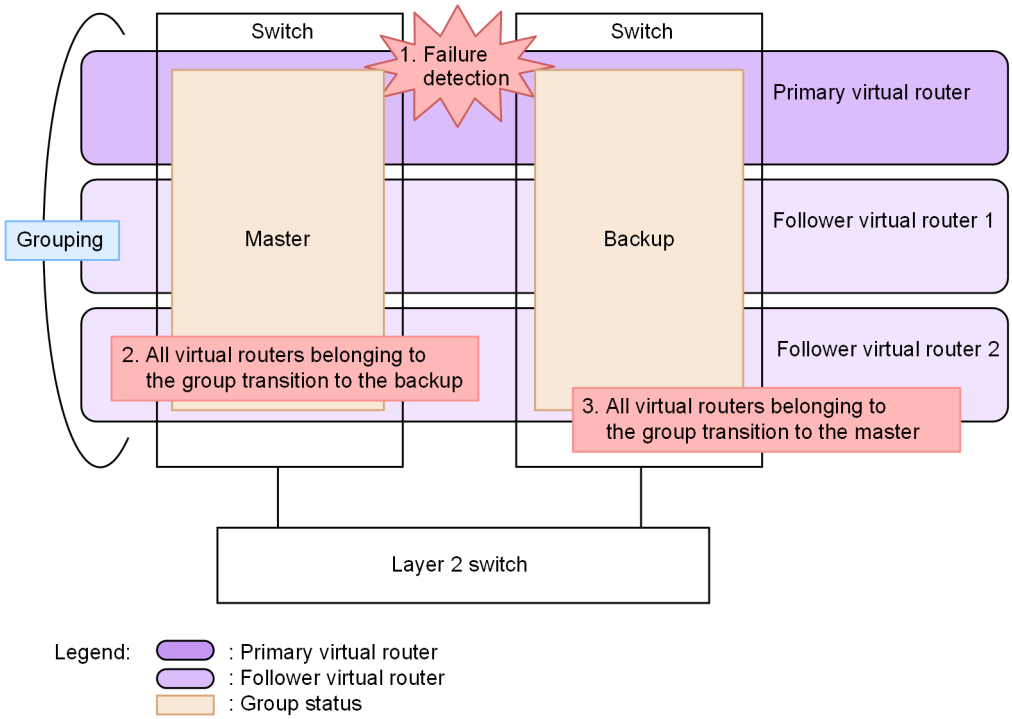
In this mode, the IPv6 virtual routers cannot authenticate ADVERTISEMENT packets.

15.1.8 Group switching function

(1) Overview

The Switch can group IPv4 virtual routers as a unique additional function. You can switch between the master and backup for each group. A group consists of a primary virtual router and a follower virtual router. A maximum of 1023 virtual routers can be used when grouped. The following figure provides an overview of the configuration and switching of group switching function.

Figure 15-13: Grouping of virtual routers



1. Failures are detected by the respective monitoring function of the master device and backup device
2. On the master device, all virtual routers in the group that detected the failure transition to backup
3. On the backup device, all virtual routers in the group that detected the failure transition to the master

Role of virtual routers	Interface on which the virtual router is configured	Virtual router ID	Virtual router name	Primary virtual router name to follow
Primary virtual router	VLAN 100	70	VRRPNAME	—
Follower virtual router 1	VLAN 200	70	—	VRRPNAME
Follower virtual router 2	VLAN 300	70	—	VRRPNAME

Legend: —: Not applicable

(2) Primary virtual router

The virtual router that sends and receives ADVERTISEMENT packets and runs tracking coordination and switches between the master and backup is called the primary virtual router. The status of the primary virtual router determines the state of all virtual routers belonging to the group.

(3) Follower virtual router

A virtual router that determines its status according to the status of the primary virtual router is called, follower virtual router. The follower virtual router follows the status of the primary virtual router without performing failure detection or status transitions through the sending or receiving of ADVERTISEMENT packets or the tracking coordination. If the primary virtual router is not running, it will be in the initial status. Also, it cannot follow the status of follower virtual routers including itself. Since the follower virtual router follows the status of the primary virtual router, it cannot become the address owner.

The following table shows the function of the follower virtual router that differs from that of the primary virtual router.

Table 15-5: Function of follower virtual router

Function different from the primary virtual router	Operation
Master/backup switched	It follows the status of the primary virtual router without performing failure detection or status transitions through the sending or receiving of ADVERTISEMENT packets or the tracking coordination.
Configuration settings	The following configuration commands used to select the master method are invalid. • vrrp authentication • vrrp preempt • vrrp preempt delay • vrrp timers non-preempt-swap • vrrp priority • vrrp track
Operation log	Operation logs associated with status transitions are not output. If the primary virtual router that constitutes the group is not set, a log will be output to inform you that the follower virtual router is invalid. It also outputs a recovery message when the primary virtual router is set.
Get MIB information	This command is not supported. Only the primary virtual router can be obtained.
Sending SNMP notification	This command is not supported. Sends only the primary virtual router.

(4) MAC learning frame

The virtual router in the master status must allow downstream LAN switches to learn its virtual MAC address.

- Primary virtual router

  The primary virtual router sends ADVERTISEMENT packets. The downstream LAN switch learns the virtual MAC address by receiving it.

- Follower virtual router

  The follower virtual router does not send ADVERTISEMENT packets. Instead, it periodically sends MAC learning frames with the source MAC address as the virtual MAC address. The downstream LAN switch learns the virtual MAC address by receiving this MAC learning frame.

(5) Notes

1. The configuration of the virtual router must be the same among the devices that make up a virtual router. For example, if a virtual router is the primary virtual router on one device and the follower virtual router on the other device, it will not work correctly.
2. Set the primary virtual router so that it can detect all failures of the follower virtual routers belonging to the group. The follower virtual router that cannot detect failures using the tracking function of the follower virtual router become unable to make status transitions and communicate when a failure occurs.

   For example, if the ADVERTISEMENT packet communication route differs between the primary virtual router and the follower virtual router, or if the VLAN that needs to be monitored differs, the primary virtual router must monitor all of them.
3. MAC learning frames are sent in a cycle of 2 minutes per follower virtual router. If the MAC address table aging time is set to 2 minutes or less, the downstream LAN switch repeats aging and MAC address learning. It is recommended to set the aging time to 4 minutes or more.

15.1.9 Notes on using VRRP

(1) Use with other function

(a) When used with the Layer 2 switch function

See "Configuration Guide Vol. 1, 22.3 Compatibility between the Layer 2 switch function and other functions".

(b) When used with Layer 2 authentication

For details, see "5.2.1 Using Layer 2 authentication with other functions".

(c) Coexistence with high reliability based on redundant configurations

The following table describes the high reliability based on redundant configurations that cannot be used, or only partially used, with VRRP.

Table 15-6: Function that cannot be used, or only partially used, with VRRP

Function	Restrictions
GSRP	Cannot be used

(2) Sending interval of ADVERTISEMENT packets

In the cases listed below, the VRRP ADVERTISEMENT packets to be sent and received by the Switch might be dropped or their processing might be delayed, resulting in status transitions. If status transitions occur frequently, specify a longer sending interval for the VRRP ADVERTISEMENT packets.

- When the CPU load on the Switch is excessive
- When too many virtual routers are configured on the Switch
- When network load is excessive
- When a virtual router consists of three or more Switches

(3) Using VRRP polling to monitor multipath routes

VRRP polling cannot be used to monitor multipath routes.

(4) Linkage between IPv6 VRRP and RA

When router advertisement (RA) is enabled on an interface on which IPv6 VRRP is configured, RA runs as follows in conjunction with VRRP:

- RA distributes information only when it resides on the IPv6 VRRP master router.
- The source MAC address in the MAC header in an RA packet is the virtual MAC address of the virtual router.
- The source IPv6 address in the IPv6 header in an RA packet is the virtual IPv6 address of the virtual router.

In this way, a terminal can use the IPv6 automatic configuration function to specify a virtual router as its default gateway.

However, the behavior of a network with RA might be adversely affected by the behavior of a terminal in the following cases:

- When multiple virtual routers are configured on a single interface, RA operates only with the master router with the smallest VRID. If you intend to use VRRP for load balancing, manually specify the default router on each terminal.
- When you specify a global address instead of a link-local address as the virtual IPv6 address, you need to specify a link-local address that is specific to an interface as the source IPv6 address of RA, not the virtual IPv6 address. This is because RA requires a link-local address as the source IPv6 address. In this case, VRRP and RA will not work together. If you want to use VRRP in conjunction with RA, do not specify a global address as the virtual IPv6 address.

(5) Configuring the follower virtual router

Keep the following in mind when a follower virtual router is configured.

- If you use the same virtual router ID, group them and make them belong to the same group.
- When the same virtual router ID is used by the Switch and another device, layer 2 forwarding cannot be performed on the Switch for the frame whose destination is the related virtual MAC address. Use a different virtual router ID for the Switch and another device.

15.2 Configuration

IP addresses must be assigned to VLANs when you configure VRRP on them. If no IP address is assigned to the VLANs, the virtual router will not work even if a configuration command for VRRP is entered.

To run a virtual router, you need to configure the Switch and other switches or routers that participate in the virtual router in the same way. You also need to configure the routing.

15.2.1 List of configuration commands

The following table describes the list of configuration commands for VRRP.

Table 15-7: List of configuration commands

Command name	Description
vrrp accept	Enables accept mode.
vrrp authentication	Sets a password for authenticating ADVERTISEMENT packets.
vrrp follow	Specify the primary virtual router and set the virtual router as the follower virtual router.
vrrp ietf-ipv6-spec-07-mode	Sets an IPv6 virtual router to run in the mode specified in draft-ietf-vrrp-ipv6-spec-07.
vrrp ip vrrp ipv6	Sets a virtual IP address for the virtual router
vrrp name	Sets a name for the virtual router.
vrrp preempt	Enables automatic switch-back.
vrrp preempt delay	Sets a period of time for suppressing automatic switch-back.
vrrp priority	Sets the priority to a virtual router.
vrrp timers advertise	Sets the sending interval of ADVERTISEMENT packets to be sent by a virtual router.
vrrp timers non-preempt-swap	Sets the switch-back suppression time to be applied when switch-back processing is performed while automatic switch-back is suppressed.

Table 15-8: List of configuration commands (VRRP tracking function)

Command name	Description
track check-reply-interface	Sets whether to check if the sending and receiving interfaces for VRRP polling match.
track check-status-interval	Sets the normal VRRP polling interval.
track check-trial-times	Sets the normal count for VRRP polling.
track failure-detection-interval	Sets the VRRP polling interval to be applied during failure verification.
track failure-detection-times	Sets the count for VRRP polling to be performed during failure verification.
track interface	Sets an interface to be monitored for failures and the method for monitoring failures.
track ip route	Sets the destination for VRRP polling for a track.

Command name	Description
track recovery-detection-interval	Sets the VRRP polling interval to be applied during failure recovery verification.
track recovery-detection-times	Sets the count for VRRP polling to be performed during failure recovery verification.
vrrp track	Sets a track for a virtual router.

15.2.2 Sequence of configuring VRRP

When you use IPv6, you need to use the "swrt_table_resource" command to change beforehand the mode to one for using IPv6 resources.

(1) Set up the IP interfaces in advance.

Assign IP addresses to VLANs. The IP addresses of VLANs must belong to the same family of IP addresses as the IP address to be assigned to the virtual router.

After you assign an IPv6 address to a VLAN for the first time, you need to execute the "ipv6 enable" command to enable the assigned IPv6 address.

(2) Sets a virtual IP address for the virtual router

When the IP address assigned to an IP interface is the same as the IP address configured for a virtual router, the virtual router containing the IP interface is the IP address owner. The priority of this virtual router is fixed at 255.

When you configure an IPv6 address for a virtual router, you can only specify a link-local unicast address according to VRRP specifications. However, with the Switch, you can also specify a global address (including a site-local address).

(3) Sets the priority to a virtual router.

Assign different priorities to the virtual routers with the same virtual router identifier other than the virtual router of the IP address owner.

(4) Set the sending interval for ADVERTISEMENT packets

If the network load is high and backup routers often lose advertisement packets, specify a longer sending interval for ADVERTISEMENT packets on the master and backup virtual routers.

(5) Configure the fault monitoring interfaces and VRRP polling

Configure the fault monitoring interfaces and VRRP polling on virtual routers as necessary so that virtual routers will not be switched over due to failures other than failures on the interfaces on which a virtual router is configured.

15.2.3 Configuring a virtual IPv4 address for a virtual router

Points to note

Configure the virtual IPv4 address for a virtual router. This behavior causes the virtual router to start running. A virtual router can have only one virtual IP address.

If the virtual IP address configured for a virtual router is the same as the IP address assigned to a VLAN on which the virtual router is configured, the virtual router containing the VLAN is the IP address owner. The priority of this virtual router is fixed at 255.

The identifier of a virtual router with a virtual IP address must be unique in the IP subnetwork.

Command examples

1. `(config)# interface vlan 10`

   `(config-if)# ip address 192.168.10.10 255.255.255.0`

   For example, to configure a virtual router on VLAN 10, enter VLAN configuration mode for VLAN 10. Next, assign an IP address to VLAN interface, if one has not already been assigned.

2. `(config-if)# vrrp 1 ip 192.168.10.1`

   Configures a virtual IP address (192.168.10.1) for virtual router ID 1.

Notes

- If the behavior terminal displays the log message "The VRRP virtual MAC address entry can't be registered at hardware tables." after you configure the IP address for a virtual router, the virtual router will not run normally. In response, delete the virtual router configuration and change the virtual router identifier. Alternatively, change the VLAN ID of the VLAN on which the virtual router is configured, and then configure an IP address for the virtual router again.
- When you configure an IP address for a virtual router, the virtual router starts behavior. Depending on the priority settings of other virtual routers, another virtual router might become the master later.
- If you plan to configure 64 or more virtual routers on the device, see "Table 15-9: Guidelines for the sending interval of ADVERTISEMENT packets" and adjust the sending interval of ADVERTISEMENT packets.

15.2.4 Configuring a virtual IPv6 address for a virtual router

Points to note

Configure the virtual IPv6 address for a virtual router. This behavior causes the virtual router to start running. A virtual router can have only one virtual IPv6 address.

If the virtual IP address configured for a virtual router is the same as the IP address assigned to a VLAN on which the virtual router is configured, the virtual router containing the VLAN is the IP address owner. The priority of this virtual router is fixed at 255.

The identifier of a virtual router with a virtual IP address must be unique in the IP subnetwork.

Command examples

1. `(config)# interface vlan 50`

   `(config-if)# ipv6 enable`

   `(config-if)# ipv6 address 2001:100::1/64`

   For example, to configure a virtual router on VLAN 50, enter VLAN configuration mode for VLAN 50. Next, assign an IPv6 address to VLAN 50 if one has not been assigned already.

2. `(config-if)# vrrp 3 ipv6 fe80::10`

   Configures a virtual IPv6 address (fe80::10) for virtual router VRID 3.

Notes

- See the notes in "15.2.3 Configuring a virtual IPv4 address for a virtual router".

15.2.5 Configuring priorities

Assign a priority to a virtual router in the range from 1 to 254. The default priority is 100 if the virtual router is not the IP address owner. The priority of the IP address owner is fixed at 255 and cannot be changed.

Of the devices that make up a virtual router, the device with the highest priority becomes the master. If the master virtual router fails, the backup virtual router with the next highest priority assumes the master role.

Points to note

To make sure that only one virtual router becomes the master, assign different priorities to the virtual routers that have the same virtual router identifier.

Command examples

1. `(config-if)# vrrp 1 priority 150`
   Sets 150 as the priority of a virtual router VRID 1.

15.2.6 Configuring the sending interval of ADVERTISEMENT packets

If the master and backup routers are switched over frequently because the network load is high and many advertisement packets are lost, you might be able to alleviate the problem by specifying a longer sending interval for ADVERTISEMENT packets. However, note that a backup virtual router becomes the master if it does not receive an ADVERTISEMENT packet three consecutive times. If you specify a longer sending interval for ADVERTISEMENT packets, it might take longer for a backup virtual router to take over as the master if the master fails.

The master and backup routers might also be switched over frequently when many virtual routers are configured on the Switch. In this case, adjust the sending interval of ADVERTISEMENT packets according to the following table.

Table 15-9: Guidelines for the sending interval of ADVERTISEMENT packets

Number of virtual routers configured on the Switch	Sending interval of ADVERTISEMENT packets
1 to 64	1 second or longer
65 to 128	2 second or longer
129 to 192	3 second or longer
193 to 255	4 second or longer

Points to note

Specify the same sending interval of ADVERTISEMENT packets on both the master and backup virtual routers.

Command examples

1. `(config-if)# vrrp 1 timers advertise 3`
   Sets the sending interval of ADVERTISEMENT packets to 3 seconds for virtual router VRID 1.

15.2.7 Configuring the suppression of automatic switch-back

Automatic switch-back runs by default. If a backup virtual router takes over a failed master virtual router and then the previous master is restored, the previous master (now a backup) automatically takes over as the current master because it has a higher priority than the current master. If you suppress this automatic switch-back, the backup virtual router with a higher priority than the master virtual router will not automatically take over the master virtual router.

Points to note

Suppress automatic switch-back on the master virtual router that is not the IP address owner

Command examples

1. `(config-if)# no vrrp 1 preempt`

   Suppresses automatic switch-back on virtual router VRID 1.

15.2.8 Configuring the automatic switch-back suppression time

Set the length of time before the processing for a switchover of a backup virtual router with a higher priority to the master automatically starts after recovery from a fault, following the occurrence of a fault on the master virtual router and a switchover to a backup. The default automatic switch-back suppression time is 0 seconds, which means automatic switch-back is not suppressed.

Points to note

Specify the automatic switch-back suppression time for the master virtual router that is not the IP address owner.

Command examples

1. `(config-if)# vrrp 1 preempt delay 60`

   Specifies 60 seconds as the automatic switch-back suppression time for a virtual router with VRID 1.

15.2.9 Configuring fault monitoring interfaces and VRRP polling

The Switch uses numbered tracks to manage the configured fault monitoring interfaces and VRRP polling. To create a track, use the "track" configuration command to specify a track number. When a track is configured for a virtual router, the virtual router monitors the fault monitoring interface specified for the numbered track based on the configuration settings. To configure a track for a virtual router, use the "vrrp track" configuration command.

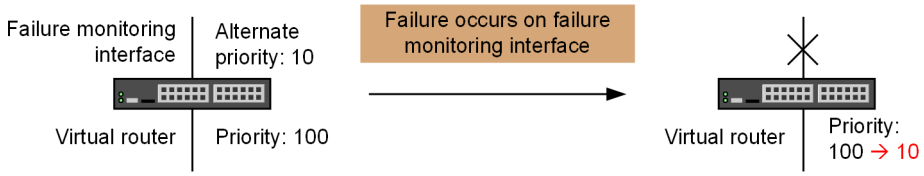
You can configure either a priority switching track or a priority decrement track for one virtual router.

If you want to configure multiple tracks for one virtual router, only priority decrement can be used as the priority change method.

The priority switching method changes the priority of a virtual router to the specified priority if a failure is detected. If you do not specify a priority or if you specify a priority higher than the priority of a virtual router, the default value (0) is used. When you select the priority switching method, you can configure only one track for one virtual router.

As an example, suppose you select the priority switching method, specify 100 as the priority of the virtual router, and specify 10 as the alternate priority to be used if a fault monitoring interface fails as shown in "Figure 15-14: Priority switching". If a failure occurs on the fault monitoring interface, the priority of the virtual router changes to 10, which is the specified alternate priority.

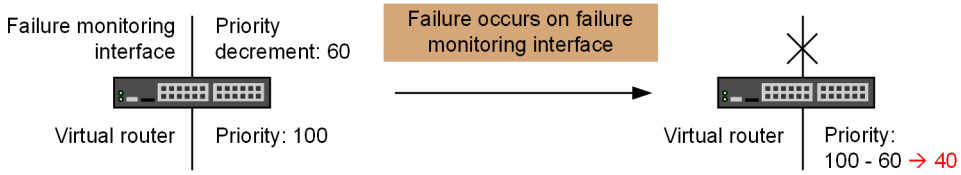
Figure 15-14: Priority switching



The priority decrement method reduces the priority of a failed virtual router by the value specified as the priority decrement. If you do not specify a priority, the default value (255) is used. When you select the priority decrement method, you can configure a maximum of 16 tracks for a virtual router.

As an example, suppose you select the priority decrement method, specify 100 as the priority of the virtual router, and specify 60 as the priority decrement to be used if a fault monitoring interface fails as shown in "Figure 15-15: Priority decrement". If a failure occurs on the fault monitoring interface, the priority of the virtual router is decreased by 60 (priority decrement) from the original value of 100. The priority of the virtual router is now 40.

Figure 15-15: Priority decrement



(1) Configuring tracks for the fault monitoring interfaces

Points to note

Specify line-protocol in the "track interface" configuration command to monitor the status of the specified VLAN interface, port channel interface, and Ethernet interface.

Set the tracks for the VLAN interface, port channel interface, and Ethernet interface to be monitored.

Use the "vrrp track" configuration command to configure tracks for a virtual router. The tracks contain the object for which failures will be monitored.

An IP address must be assigned to the VLAN interface that will be monitored for failures.

Command examples

1.
```
(config)# track 20 interface vlan 30 line-protocol
(config)# track 30 interface gigabitethernet 1/0/8 line-protocol
(config)# track 40 interface port-channel 10 line-protocol
```

   - Sets track 20 as the fault monitoring interface for monitoring the status of VLAN 30.
   - Sets track 30 as the fault monitoring interface for monitoring the status of Gigabit Ethernet interface 1/0/8.
   - Sets track 40 as the fault monitoring interface for monitoring the status of channel group 10.

2.
```
(config-if)# vrrp 1 track 20 decrement 60
(config-if)# vrrp 1 track 30 decrement 10
(config-if)# vrrp 1 track 40 decrement 40
```

Enter VLAN configuration mode for the VLAN on which the virtual router has been configured beforehand. In this case, tracks 20, 30, and 40 are configured for virtual router VRID 1.

- If a failure occurs on the fault monitoring interface set for track 20, the priority of the virtual router 1 is decreased by 60.
- If a failure occurs on the fault monitoring interface set for track 30, the priority of the virtual router 1 is decreased by 10.
- If a failure occurs on the fault monitoring interface set for track 40, the priority of the virtual router 1 is decreased by 40.

(2) Configuring tracks for VRRP polling

Points to note

Specify ip routing in the "track interface" configuration command to monitor the specified VLANs and to check reachability of the destinations specified in the "track ip route" configuration command by pinging them.

Set tracks for the VLAN interfaces for which VRRP is to be used.

Use the "vrrp track" configuration command to configure tracks for a virtual router. The tracks contain the configuration settings for VRRP polling.

When you use VRRP polling to monitor failures, you need to assign an IP address to the VLAN interface used for VRRP polling and specify the route to the destination specified in the "track ip route" command.

When you configure the same track for multiple virtual routers, each virtual router sends VRRP polling packets.

Command examples

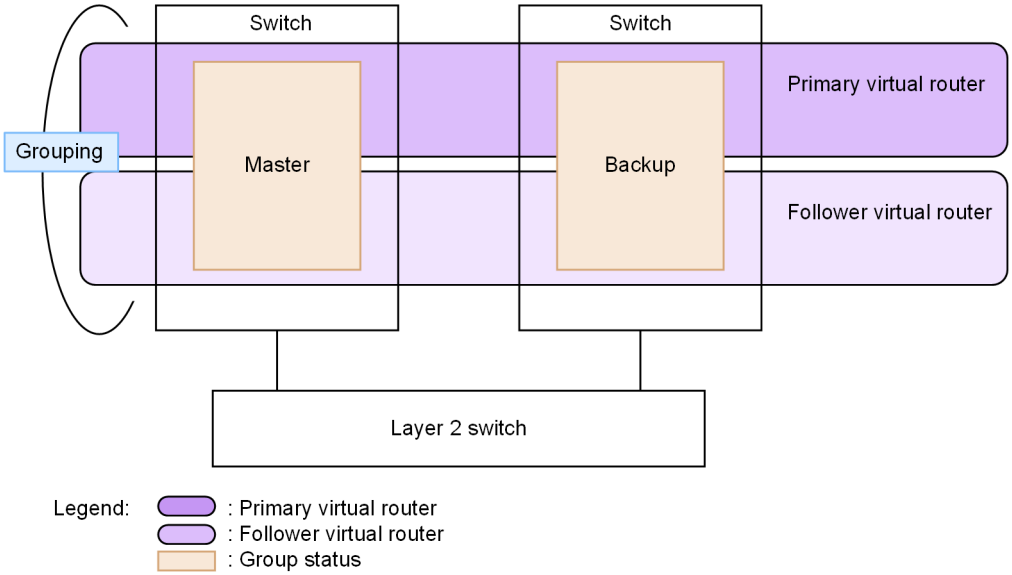
1.
```
(config)# track 50 interface vlan 34 ip routing
(config)# track 51 interface vlan 35 ip routing
(config)# track 52 interface vlan 36 ip routing
```
   - Sets track 50 as the sending interface for VRRP polling for monitoring the status of VLAN 34.
   - Sets track 51 as the sending interface for VRRP polling for monitoring the status of VLAN 35.
   - Sets track 52 as the sending interface for VRRP polling for monitoring the status of VLAN 36.
2.
```
(config)# track 50 ip route 192.168.20.1 reachability
(config)# track 51 ip route 192.168.21.1 reachability
(config)# track 52 ip route 192.168.22.1 reachability
```
   - For track 50, 192.168.20.1 is set as the VRRP polling destination.
   - For track 51, 192.168.21.1 is set as the VRRP polling destination.
   - For track 52, 192.168.22.1 is set as the VRRP polling destination.
3.
```
(config-if)# vrrp 3 track 50 priority 10
(config-if)# vrrp 4 track 51 decrement 20
(config-if)# vrrp 4 track 52 decrement 50
```

- Enter VLAN configuration mode for the VLAN on which the virtual router has been configured beforehand.
- The first command configures track 50 for virtual router VRID 3, sets priority switching as the priority change method, and sets 10 as the alternate priority. If a failure is detected by the VRRP polling defined for track 50, the priority of the virtual router 3 is changed to 10.
- The second and third commands configure tracks 51 and 52 for virtual router VRID 4 and set the priority change method to priority decrement. The third command sets 20 as the priority decrement value for track 51. The third command sets 50 as the priority decrement value for track 52. If a failure is detected by the VRRP polling defined for track 51, the priority of the virtual router 4 is decreased by 20. If a failure is detected by the VRRP polling defined for track 52, the priority of the virtual router 4 is decreased by 50. If failures occur on both fault monitoring interfaces defined for tracks 51 and 52, the priority of the virtual router 4 is decreased by 70.

15.2.10 Grouping of virtual routers

A maximum of 1023 virtual routers can be used by grouping multiple virtual routers. The following shows an example of setting the following group configuration.

Figure 15-16: Example of group configuration settings for a virtual router



Role of virtual routers	Interface on which the virtual router is configured	Virtual router ID	Virtual router name	Primary virtual router name to follow
Primary virtual router	VLAN 10	1	VRRPNAME	—
Follower virtual router	VLAN 20	1	—	VRRPNAME

Legend: —: Not applicable

(1) Setting the primary virtual router

Points to note

The status of the primary virtual router determines the state of all virtual routers belonging to the group. After the configuration, make sure that the primary virtual router is running properly.

Command examples

1. `(config)# interface vlan 10`

   `(config-if)# ip address 192.168.10.1 255.255.255.0`

   Switches to the VLAN interface configuration mode for VLAN 10. Next, assign an IP address to VLAN interface, if one has not already been assigned.

2. `(config-if)# vrrp 1 ip 192.168.10.100`

   Configures the virtual IP address 192.168.10.100 for the virtual router with VLAN 10 and virtual router ID 1.

3. `(config-if)# vrrp 1 name VRRPNAME`

   Configures the virtual router name VRRPNAME to the virtual router with VLAN 10 and virtual router ID 1.

(2) Configuring the follower virtual router

Points to note

Specify the primary virtual router name from the virtual router. A virtual router that specifies a primary virtual router becomes a follower virtual router and follows the status of the specified primary virtual router.

We recommend that you set the same virtual router ID as the primary virtual router for the follower virtual router.

Command examples

1. `(config)# interface vlan 20`

   `(config-if)# ip address 192.168.20.1 255.255.255.0`

   Switches to the VLAN interface configuration mode for VLAN 20. Next, assign an IP address to VLAN interface, if one has not already been assigned.

2. `(config-if)# vrrp 1 follow VRRPNAME`

   Specifies VRRPNAME as the primary virtual router name followed by the follower virtual router with VLAN 20 and virtual router ID 1.

3. `(config-if)# vrrp 1 ip 192.168.20.100`

   Configures the virtual IP address 192.168.20.100 for the virtual router with VLAN 20 and virtual router ID 1.

Notes

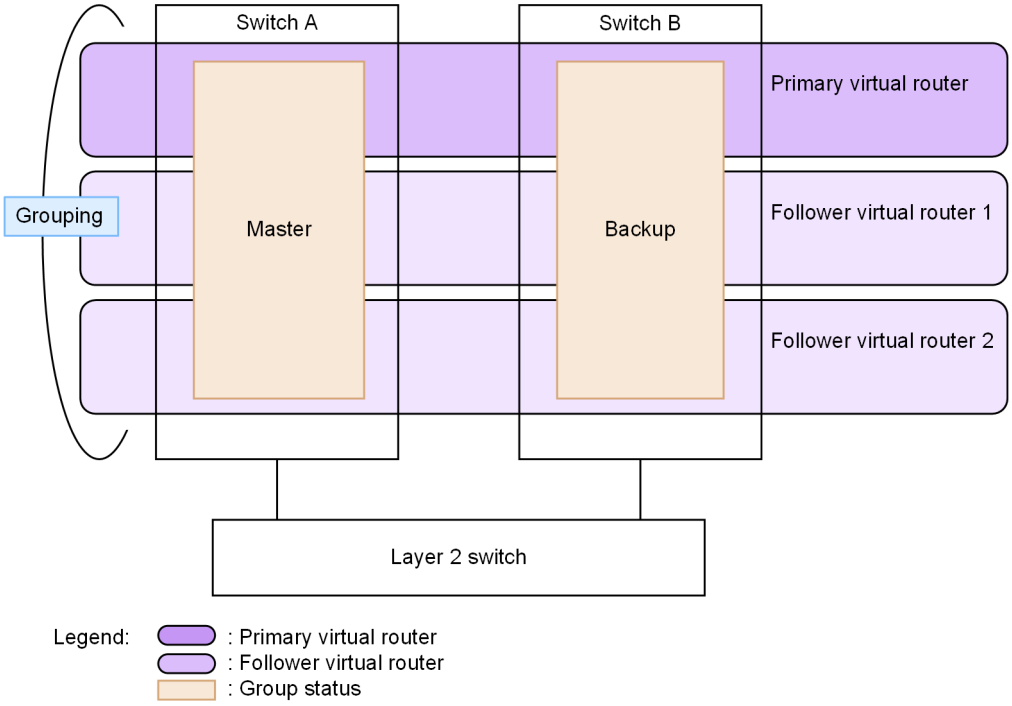
- To set a follower virtual router, start with the "vrrp follow" command.
- If the specified primary virtual router does not exist, the follower virtual router will be in the initial status.

15.2.11 Changing the group configuration

The procedure for changing the primary virtual router to another virtual router is shown below. If you do not follow this procedure, the virtual routers on both devices might be in the master status.

The following shows the group configuration of the virtual router before and after the change. Note the Switch A is the master device and the Switch B is the backup device.

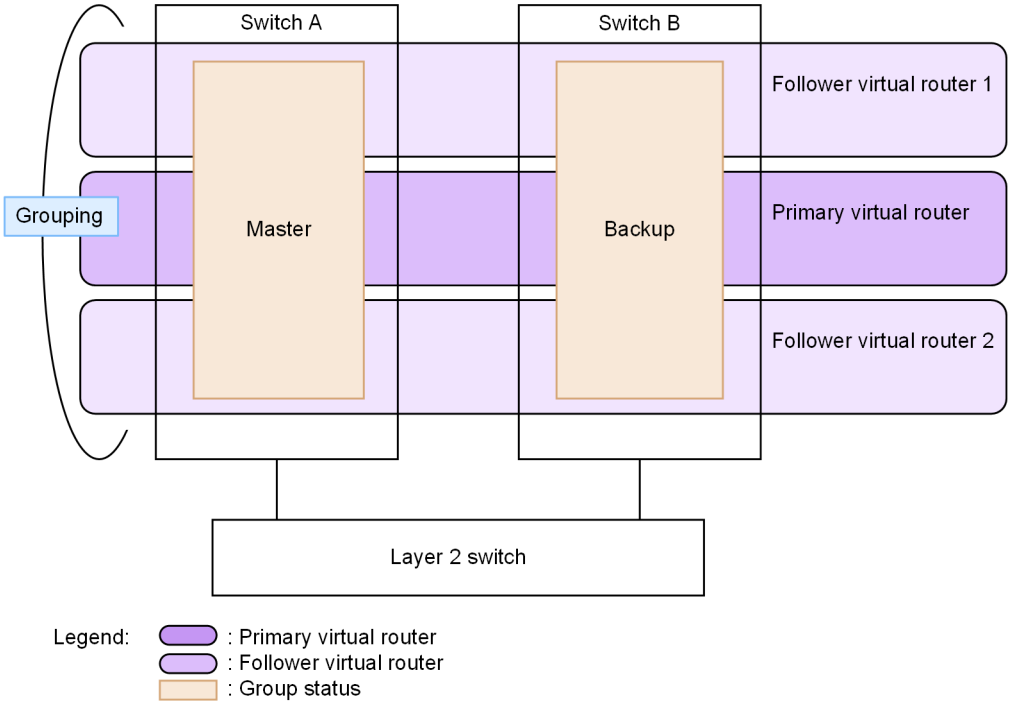
Figure 15-17: Example of group configuration settings for a virtual router (before change)



Role of virtual routers	Interface on which the virtual router is configured	Virtual router ID	Virtual router name	Primary virtual router name to follow
Primary virtual router	VLAN 10	1	VRRPNAME	—
Follower virtual router 1	VLAN 20	1	—	VRRPNAME
Follower virtual router 2	VLAN 30	1	—	VRRPNAME

Legend: —: Not applicable

Figure 15-18: Example of group configuration settings for a virtual router (after change)



Role of virtual routers	Interface on which the virtual router is configured	Virtual router ID	Virtual router name	Primary virtual router name to follow
Follower virtual router 1	VLAN 10	1	VRRPNAME	NEW_VRRPNAME
Primary virtual router	VLAN 20	1	NEW_VRRPNAME	—
Follower virtual router 2	VLAN 30	1	—	NEW_VRRPNAME

Legend: —: Not applicable

(1) Change from the follower virtual router to primary virtual router

Points to note

Change the follower virtual router to the primary virtual router. It is necessary to change the settings of the master device (Switch A) first.

If the change is made from the backup device (Switch B), the virtual router of the backup device (Switch B) does not receive the ADVERTISEMENT packet, so it transitions to the master status. Also, since the master device (Switch A) remains in the master status according to the primary virtual router in the master status, the virtual routers of both devices will be in the master status.

Command examples

1. `(config)# interface vlan 20`

   Switches to the VLAN interface configuration mode for VLAN 20.

2. `(config-if)# no vrrp 1 follow`

   Makes the follower virtual router with VLAN 20 and virtual router ID 1 as the primary virtual router.

   Change the Switch A, then Switch B.

3. `(config-if)# vrrp 1 name NEW_VRRPNAME`

   Configures the virtual router name NEW_VRRPNAME to the primary virtual router with VLAN 20 and virtual router ID 1.

(2) Changing the configuration of the follower virtual router

Points to note

Change the primary virtual router that the follower virtual router is following.

Since the follower virtual router follows the status of the primary virtual router without sending or receiving ADVERTISEMENT packets, settings can be changed from either device. If you specify a primary virtual router that is not running, the follower virtual router will be in the initial status.

Command examples

1. `(config)# interface vlan 30`

   Switches to the VLAN interface configuration mode for VLAN 30.

2. `(config-if)# vrrp 1 follow NEW_VRRPNAME`

   Changes the primary virtual router followed by the follower virtual router with VLAN 30 and virtual router ID 1 to NEW_VRRPNAME.

(3) Changing from the primary virtual router to follower virtual router

Points to note

Change the primary virtual router to follower virtual router. You need to change the settings from the backup device side.

If the change is made from the master device (Switch A), the virtual router of the backup device (Switch B) does not receive the ADVERTISEMENT packet, so it transitions to the master status. Also, since the master device (Switch A) remains in the master status according to the primary virtual router in the master status, the virtual routers of both devices will be in the master status.

Command examples

1. `(config)# interface vlan 10`

   Switches to the VLAN interface configuration mode for VLAN 10.

2. `(config-if)# vrrp 1 follow NEW_VRRPNAME`

   Makes the virtual router with VLAN 10 and virtual router ID 1 as the follower virtual router.

   Change the Switch B, then Switch A.

15.3 Operation

15.3.1 List of operation commands

The following table describes the list of operation commands for VRRP.

Table 15-10: List of operation commands

Command name	Description
show vrrpstatus	Shows the running status of a virtual router.
clear vrrpstatus	Initializes the statistics regarding a virtual router.
swap vrrp	Starts switch-back processing when automatic switch-back is suppressed.
show track	Shows the configuration for failure monitoring saved to a track.

15.3.2 Checking the configuration of a virtual router

Use the "show vrrpstatus" operation command to check the configuration of a virtual router.

(1) Checking details

When you specify the detail parameter, you can obtain the detailed configuration of a virtual router.

Figure 15-19: Results of executing the "show vrrpstatus" command

```
> show vrrpstatus detail interface vlan 10 vrid 1
Date 20XX/12/10 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
   Virtual Router IP Address : 170.10.10.2
   Virtual MAC Address : 0000.5e00.0101
   Virtual Router Name  : VRRPNAME1 (primary)
   Virtual Router Follow : -
   Number of Follow virtual routers : 4
   Current State : MASTER
   Admin State : enable
   Priority : 80 /100
   IP Address Count : 1
   Master Router's IP Address : 170.10.10.2
   Primary IP Address : 170.10.10.1
   Authentication Type : SIMPLE TEXT PASSWORD
   Authentication Key : ABCDEFG
   Advertisement Interval : 1 sec
   Preempt Mode : ON
   Preempt Delay : 60
   Non Preempt swap timer : 30
   Accept Mode : ON
   Virtual Router Up Time : Mon Dec  6 16:55:00 20XX
   track 10 VLAN0022 VRF 3 Status : (IF UP) Down Priority : 50
     Target Address : 192.168.0.20
     Vrrp Polling Status : reachable
   track 20 VLAN0023  Status : (IF UP) Down Priority : 40
   track 30 gigabitethernet 0/10 Status : (IF DOWN) Down Priority : 20
   track 40 port-channel 2 Status : (IF UP) Down Priority : 20
>
```

(2) Checking the group information

When you specify the group parameter, you can check the group information of the virtual router settings. If you know the virtual router name, you can check the virtual router information by specifying the name parameter.

Figure 15-20: Results of executing the show vrrpstatus group command (for the primary virtual router)

```
> show vrrpstatus group name VRRPNAME1
Date 20XX/12/15 12:00:00 UTC
VLAN0010: VRID 1 VRF 2
    Virtual Router Name                : VRRPNAME1 (primary)
    Virtual Router Follow              : -
    Number of Follow virtual routers   : 4
    Followed by virtual routers        :
        VLAN0020: VRID 1 VRF 2
        VLAN0030: VRID 1 VRF 2
        VLAN0040: VRID 1 VRF 2
        VLAN0050: VRID 1 VRF 2
```

Figure 15-21: Results of executing the show vrrpstatus group command (for the follower virtual router)

```
> show vrrpstatus group interface vlan 20 vrid 1
Date 20XX/12/15 12:00:00 UTC
VLAN0020: VRID 1 VRF 2
    Virtual Router Name              : VRRPNAME2 (follow)
    Virtual Router Follow            : VRRPNAME1 (VLAN0010: VRID 1 VRF 2 )
    Number of Follow virtual routers : 0
    Followed by virtual routers      : -
```

15.3.3 Checking the settings in tracks

Use the "show track" operation command to check the track configurations.

Figure 15-22: Results of executing the show track command

```
> show track detail
Date 20XX/10/15 12:00:00 UTC
track : 20  interface : VLAN0030  Mode : (polling)
   Target Address : 192.168.20.1
   Assigned to :
     VLAN0010: VRID 1
track : 30  interface : VLAN0031  Mode : (interface)
   Assigned to :
     VLAN0010: VRID 1
track : 40  interface : VLAN0032  Mode : (polling)
   Target Address : 192.168.40.1
   Assigned to :
     VLAN0010: VRID 1
track : 50  interface : VLAN0034  Mode : (polling)
   Target Address : 192.168.20.1
>
```

15.3.4 Executing switch-back

When automatic switch-back is suppressed on a backup router that has a higher priority than the master, execute the "swap vrrp" command to start switch-back processing. Note that you cannot switch a virtual router with a low priority to the master status by executing the "swap vrrp" command.

16 Uplink Redundancy

Uplink redundancy provides redundancy for ports used for uplink; that is, one of the paired ports is used for communication, and the other stands by in case a failure occurs. For uplink ports, you can specify physical ports or link aggregation ports.

This chapter describes uplink redundancy and its use.

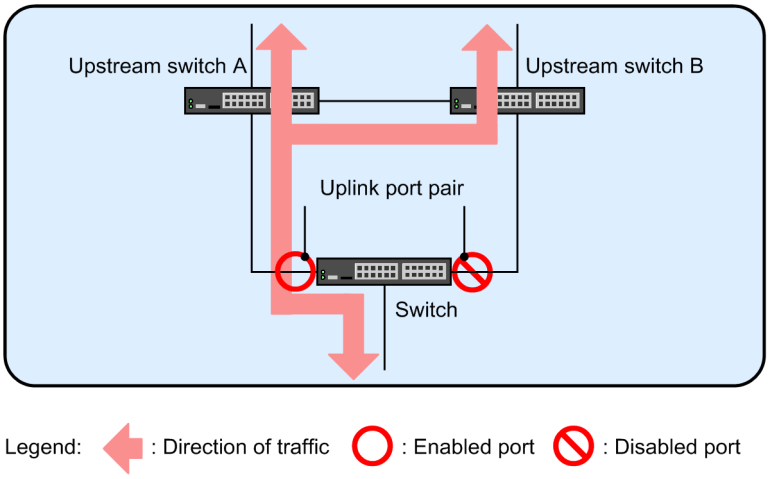
16.1 Description

16.1.1 Overview

Uplink redundancy enables duplexed uplink ports on the Switch. If a link failure occurs during communication, the standby 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 complex protocols such as Spanning Tree Protocols. The two ports for redundancy are called uplink ports.

The following figure shows the basic configuration of uplink redundancy.

Figure 16-1: Basic configuration 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.

16.1.2 Supported specifications

The following table describes the specifications supported for uplink redundancy.

Table 16-1: Specifications supported for uplink redundancy

Item		Support or specified value	
		Standalone	Stack
Applicable interfaces	Physical ports	Y	Y#1
	Link aggregation	Y	Y#1#2
Number of uplink ports		50	50
Number of interfaces that can be configured for one uplink port pair		2	2
Automatic active port switchback to the primary port		Y	Y
Suppression of automatic active port switchback to the primary port		Y	Y
Command for changing the active port		Y	Y
Send/receive function for flush control frames when the active port is changed		Y	Y
MAC address update function when the active port is changed		Y	Y

Item	Support or specified value	
	Standalone	Stack
Port resetting when the active port is changed	Y	Y
Active port locking function at Switch startup	Y	Y#3
Private MIB and private SNMP notification	Y	Y

Legend Y: Supported

#1

The primary port and secondary port cannot be set on the same member switch.

#2

The link aggregation across multiple member switches cannot be set for the primary port or secondary port.

#3

This function is canceled when the master switch is switched.

16.1.3 Overview of uplink redundancy behavior

Uplink redundancy provides redundancy by using a pair of ports or bundles of ports (link aggregation ports). This pair of ports is called an uplink port pair. An uplink port pair 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.

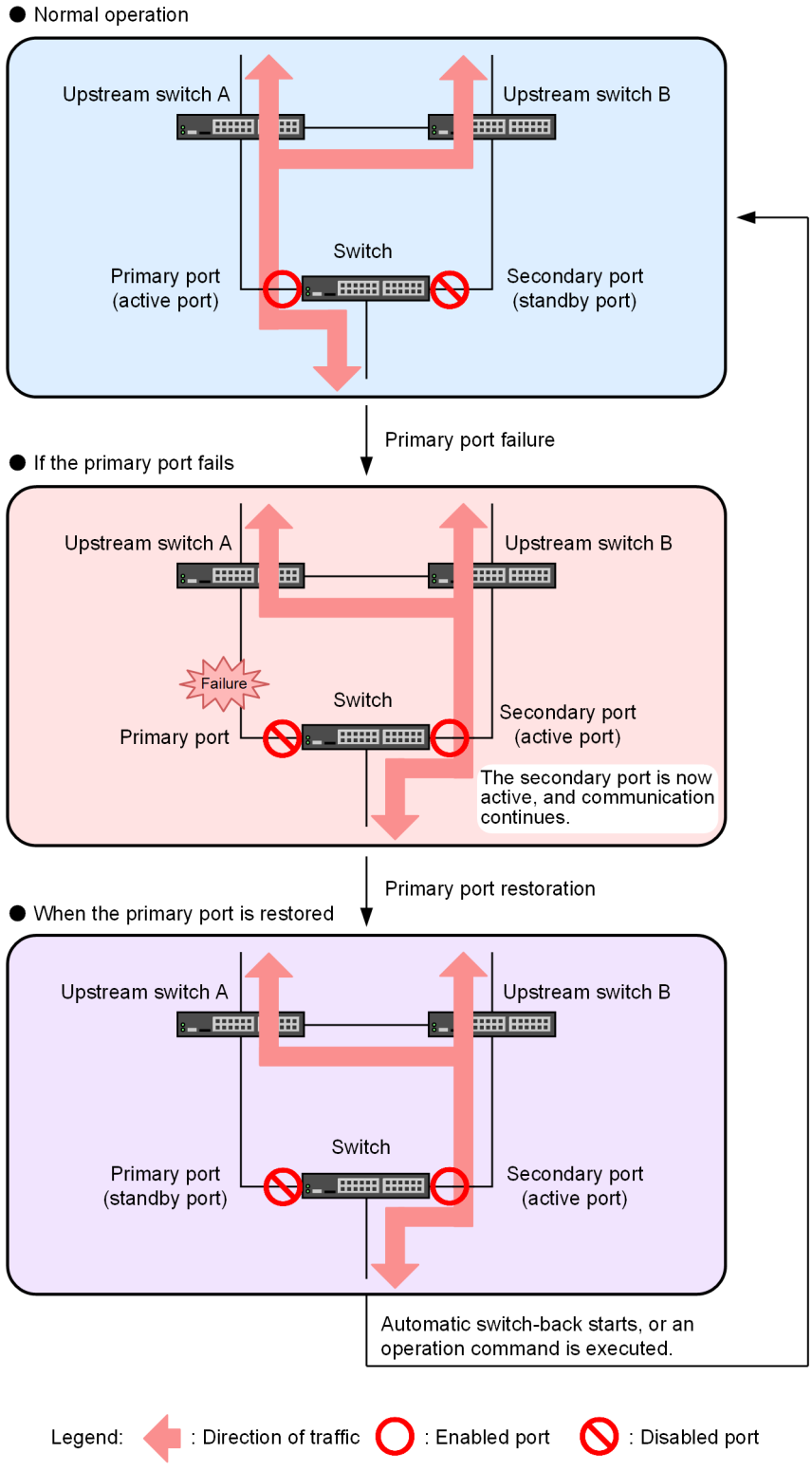
The primary port and the secondary port do not need to have the same bandwidth or consist of the same number of ports. For example, you can specify a 10 Gigabit Ethernet port as the primary port and a link aggregation group consisting of five 1 Gigabit Ethernet ports as the secondary port.

In the uplink port pair, 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 pair must belong to the same VLAN and have the same settings. In addition, the ports used for an uplink port pair cannot be used as another uplink port pair.

The following figure provides an overview of uplink redundancy behavior.

Figure 16-2: Behavior overview of uplink redundancy



Normal operation

Communication with upstream switches is possible via the primary port on the Switch. 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 to the secondary port and uses it to continue communication with upstream switches. This action is called a switchover. At this time, the secondary port, which is now the active port, sends a special control frame called a flush control frame or an MAC address update frame to the upstream switches. When the upstream switches receive either frame, they update their MAC address tables and immediately resume communication.

When the primary port is restored

When the primary port link is enabled and the port is standing by, you can use automatic switchback function or execute the appropriate operation command on the device to switch the active port to the primary port. This action is called switchback.

As in a switchover, the active port sends a flush control frame or an MAC address update frame or temporarily brings down the old active port using the port reset function to immediately resume communication.

16.1.4 Switchover and switchback

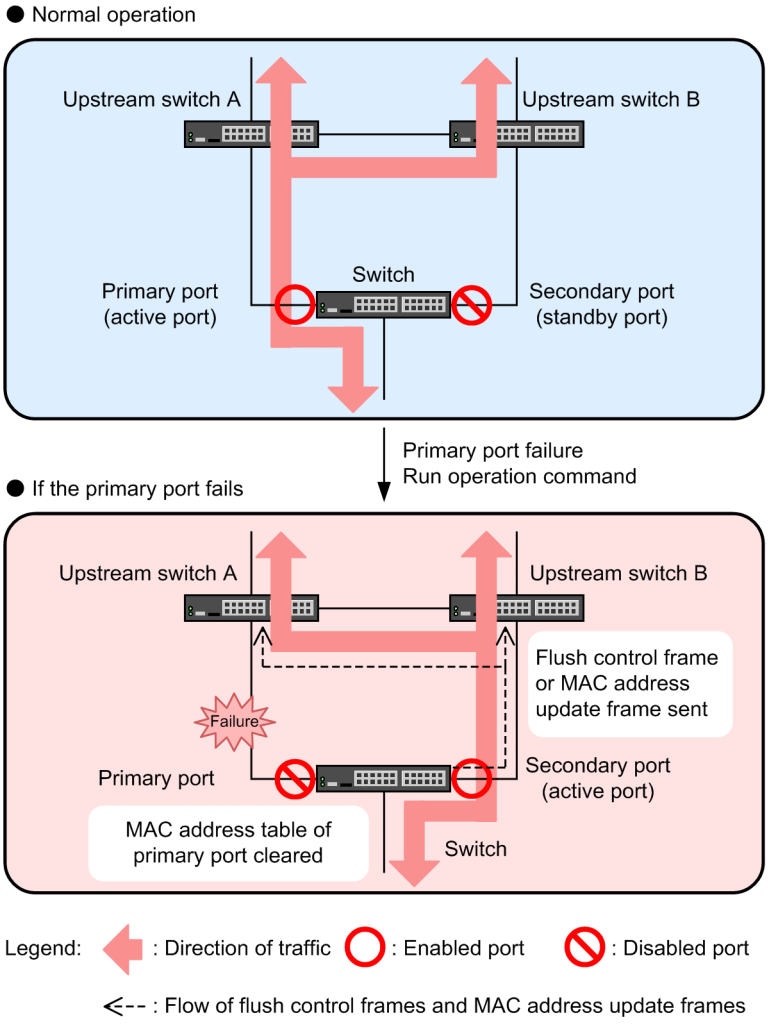
Switchover and switchback change the port that performs communication. Switchover or switchback is triggered by one of the following events when the partner port of the active port is the standby port:

- When a failure occurs on the active port
- When the automatic switchback function wait time has expired
- When a user enters an operation command to change the active port

When switchover or switchback occurs, all the MAC addresses learned on the previous active port are cleared, and the new active port starts communication. When the uplink port pair is configured to send flush control frames or MAC address update frames, the new active port sends either type of frame when switchover or switchback occurs. If the port resetting is set, temporarily bring down the old active port.

The following figure illustrates switchover.

Figure 16-3: Switching behavior (when the flush control frame or MAC address update frame sending is set)



16.1.5 Automatic switchback function

If the primary port fails, the secondary port replaces the primary port as the active port. Automatic switch-back function automatically restores the primary port as the active port when it is restored after a failure. You can specify from 0 (immediate) to 300 seconds for the switchback wait time.

If you have used an operation command to change the active port, automatic switchback usually does not work. However, in either of the following conditions, automatic switchback occurs:

- An operation command has been used to change the active port, after which the applicable configuration command for specifying automatic switch-back or changing the automatic switch-back settings was used.
- An operation command has been used to change the active port after failure of the primary port or restoration of the primary port.

16.1.6 Auxiliary communication recovery function

Uplink redundancy supports three types of function to help restore communication at switchover or switchback. Note that you can use only one of these for an uplink port pair.

- Send/receive function for flush control frames

  The Switch sends a flush control frame to upstream switches, where it is flooded, to clear their MAC address tables and restore communication. Upstream switches need to support the clearing of MAC address tables triggered by flush control frames.

- MAC address update function

  The Switch sends an MAC address update frame to upstream switches to have them relearn the MAC addresses of terminals and restore communication. Upstream switches do not require the receiving function for this. However, the number of MAC addresses an upstream switch can relearn is limited. Note that it might take about 10 seconds for communication to be restored.

- Port resetting

  By temporarily bringing down the old active port, the upstream switch that detects the link-down clears the MAC address entries learned on the corresponding port from the MAC address table and restores communication by flooding. The upstream switch does not require a dedicated function, but the primary port and secondary port must be connected to the same upstream switch.

The send/receive function for flush control frames is used for the devices connected to upstream switches that support flush control frames. The MAC address update function and port resetting are used for the devices connected to upstream switches that cannot receive flush control frames.

16.1.7 Send/receive function for flush control frames

(1) Sending behavior

When the active port is changed due to a failure on the communication link or when an operation command is executed to change the active port, the Switch can send a flush control frame to request an upstream switch to clear its MAC address table. You can configure the sending of flush control frames for each uplink port pair, and you can specify the destination VLANs.

If there is any switch or router on the network whose MAC address table you do not wish to clear, configure a special VLAN for sending and receiving flush control frames. Then, set the configuration to send flush control frames only to the specified VLAN to limit the devices and routers that clear their MAC address table when flush control frames are sent.

The Switch sends flush control frames from the new active port immediately after the port is enabled.

When you use a trunk port to send flush control frames, you need to specify the destination VLAN. For access ports, MAC ports, and protocol ports, the Switch sends untagged flush control frames regardless of whether the destination VLAN is specified.

(2) Receiving behavior

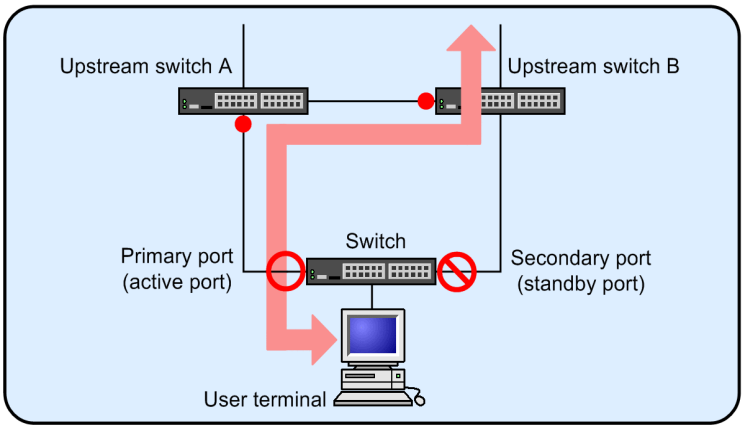
When the Switch receives a flush control frame, it clears its MAC address table.

You do not need to specify any configuration command to receive flush control frames. However, when the Switch is configured to send flush control frames to a specific VLAN, that VLAN must be enabled to receive flush control frames.

The following figure shows the difference in switchover behavior according to the use of flush control frames.

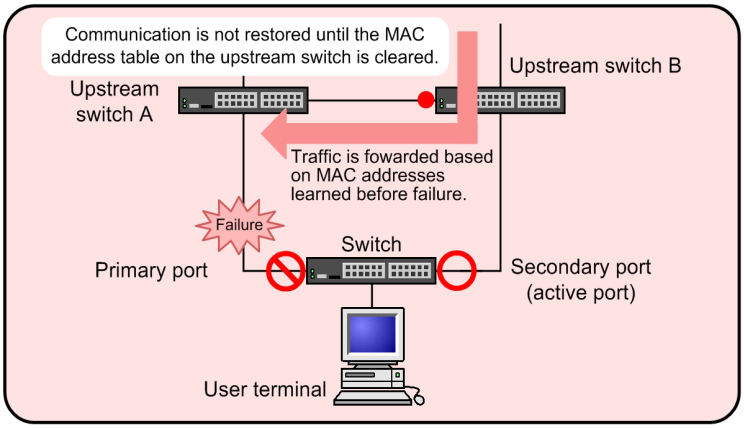
Figure 16-4: Difference in switchover behavior according to flush control frame use

● Normal operation (data passes through upstream switches A and B)

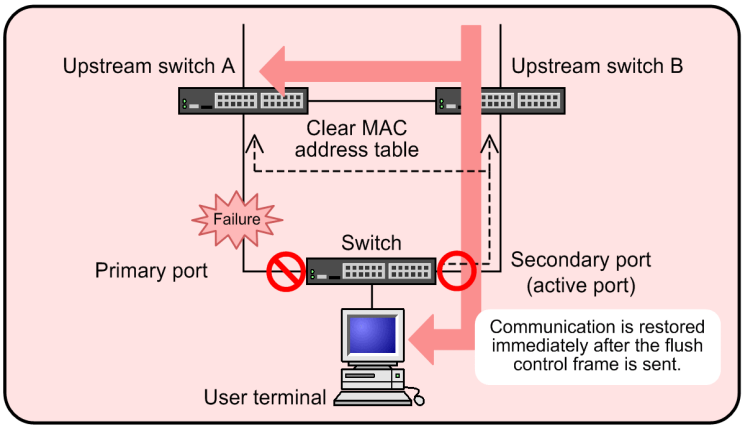


● If the primary port fails

When flush control frames are not sent



When flush control frames are sent



Legend: : Direction of traffic : Enabled port : Disabled port

<-- : Flow of flush control frames ● : Port where user terminal MAC address is learned

Normal operation

The primary port on the Switch performs communication. Upstream switches learn the MAC address of the user terminal via the current communication path.

If the primary port fails (when flush control frames are not sent)

If the Switch is not configured to send flush control frames, although the secondary port is now active, upstream switch B retains the MAC address of the user terminal on the previous port. Therefore, communication is not restored until the MAC address learned by upstream switch B is erased or the user terminal sends traffic to upstream switch B.

If the primary port fails (when flush control frames are sent)

If the Switch is configured to send flush control frames, it sends a flush control frame to request that upstream switch B clear its MAC address table as soon as the secondary port becomes active. Therefore, communication can be restored immediately.

16.1.8 MAC address update function

(1) Sending operation

When the active port is changed due to a failure on the communication link or when an operation command is executed to change the active port, the Switch can send an MAC address update frame to have an upstream switch relearn the MAC address of a terminal. The MAC address update frame has the following features:

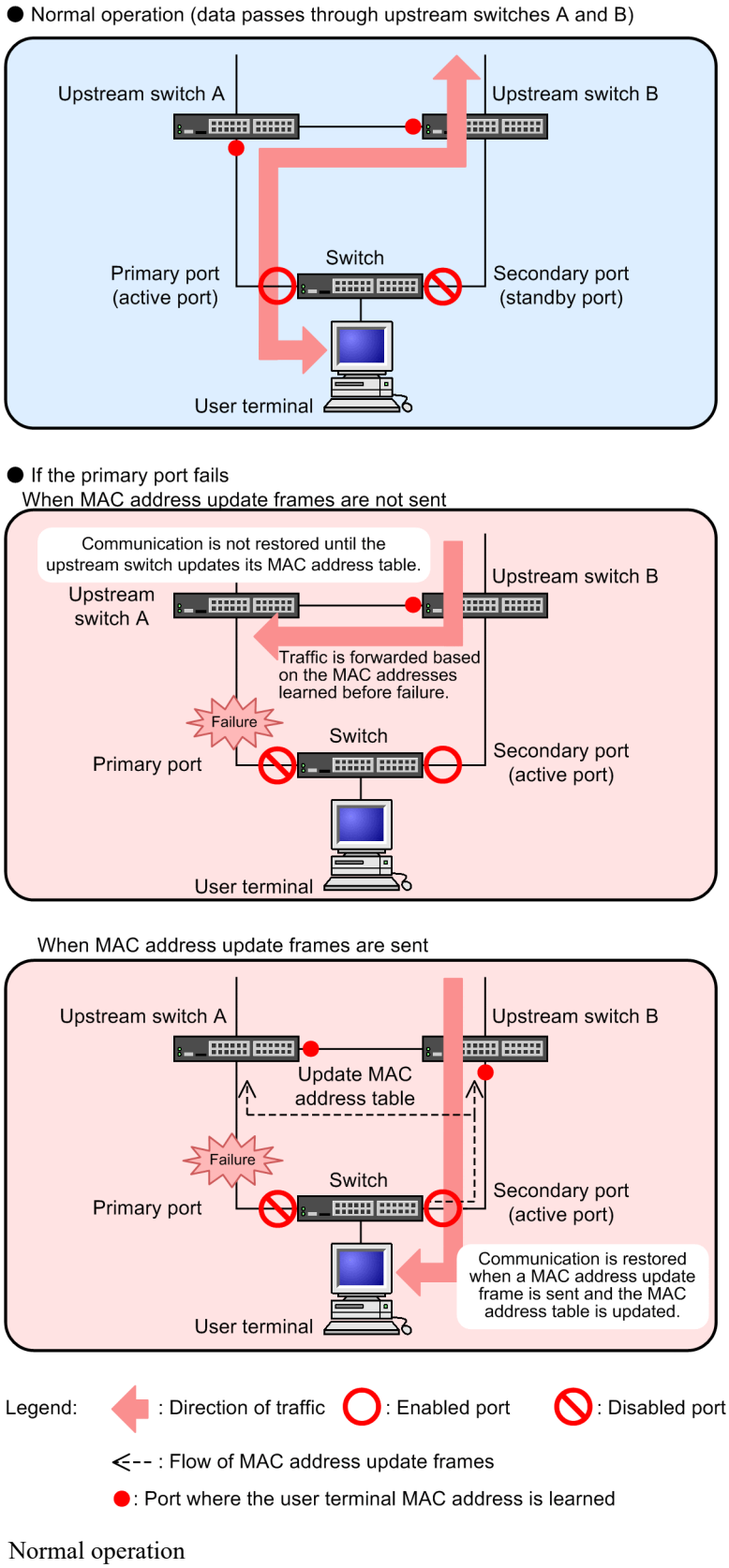
- The MAC address update frame is a multicast frame.
- You specify the MAC address to be learned by upstream switches as the source MAC address.
- Upstream switches do not need a special receiving functionality.

You can configure the MAC address update function for each uplink port pair. You can also specify VLANs to which MAC address update frames are not to be sent.

When you use this function, the maximum number of recommended entries in a MAC address table is 16384. If you exceed the recommended value, it might take more time before communication is restored, or the response of operation commands for uplink redundancy might be slow.

The following figure shows the difference in switchover behavior according to the use of MAC address update frames.

Figure 16-5: Difference in the switchover behavior according to MAC address update frame use



Normal operation

The primary port on the Switch performs communication. Upstream switches learn the MAC address of the user terminal via the current communication path.

If the primary port fails (when MAC address update frames are not sent)

If the Switch is not configured to send MAC address update frames, although the secondary port is now active, upstream switch B retains the MAC address of the user terminal on the previous port. Therefore, communication is not restored until the MAC address learned by upstream switch B is erased or the user terminal sends traffic to upstream switch B.

If the primary port fails (when MAC address update frames are sent)

If the device is configured to send MAC address update frames, it sends an MAC address update frame to request that upstream switch B update MAC address learning port of the user terminal as soon as the secondary port becomes active. Therefore, communication can be restored immediately.

The following table describes the specifications of the MAC address update function.

Table 16-2: Specifications of the MAC address update function

Item	Description
Unit for ports that send MAC address update frames	Per uplink port
Sending port	Enabled active port
Number of times frames are sent#	1 to 3 (times)
MAC address entries to be sent	Entries must concurrently satisfy the following conditions: • They must be entries that are learned on the VLANs containing the applicable uplink port pair. These entries do not include entries learned on the VLANs not subject to the sending MAC address update frames as specified in the applicable configuration. • They must be entries that are learned on ports other than the applicable uplink port pair.
Types of MAC address entries to be sent	• Dynamic entries • Static entries • Entries authenticated by IEEE 802.1X • Entries authenticated by Web-based authentication • Entries authenticated by MAC-based authentication • Device MAC address • MAC addresses of VLAN interfaces • Virtual MAC address
Maximum number of MAC address entries to be sent	3000 entries. If the number of entries to be sent exceeds 3000, only 3000 entries are sent and an operation log message indicating that the capacity limit has been exceeded is output.
Sending rate	300 pps at maximum

#

Set in the configuration

(2) Receiving operation

As with other receive frames, when the Switch relays MAC address update frames, it learns the source MAC addresses contained in the frames and registers them in its MAC address table. For details, see "Configuration Guide Vol. 1, 23 MAC Address Learning".

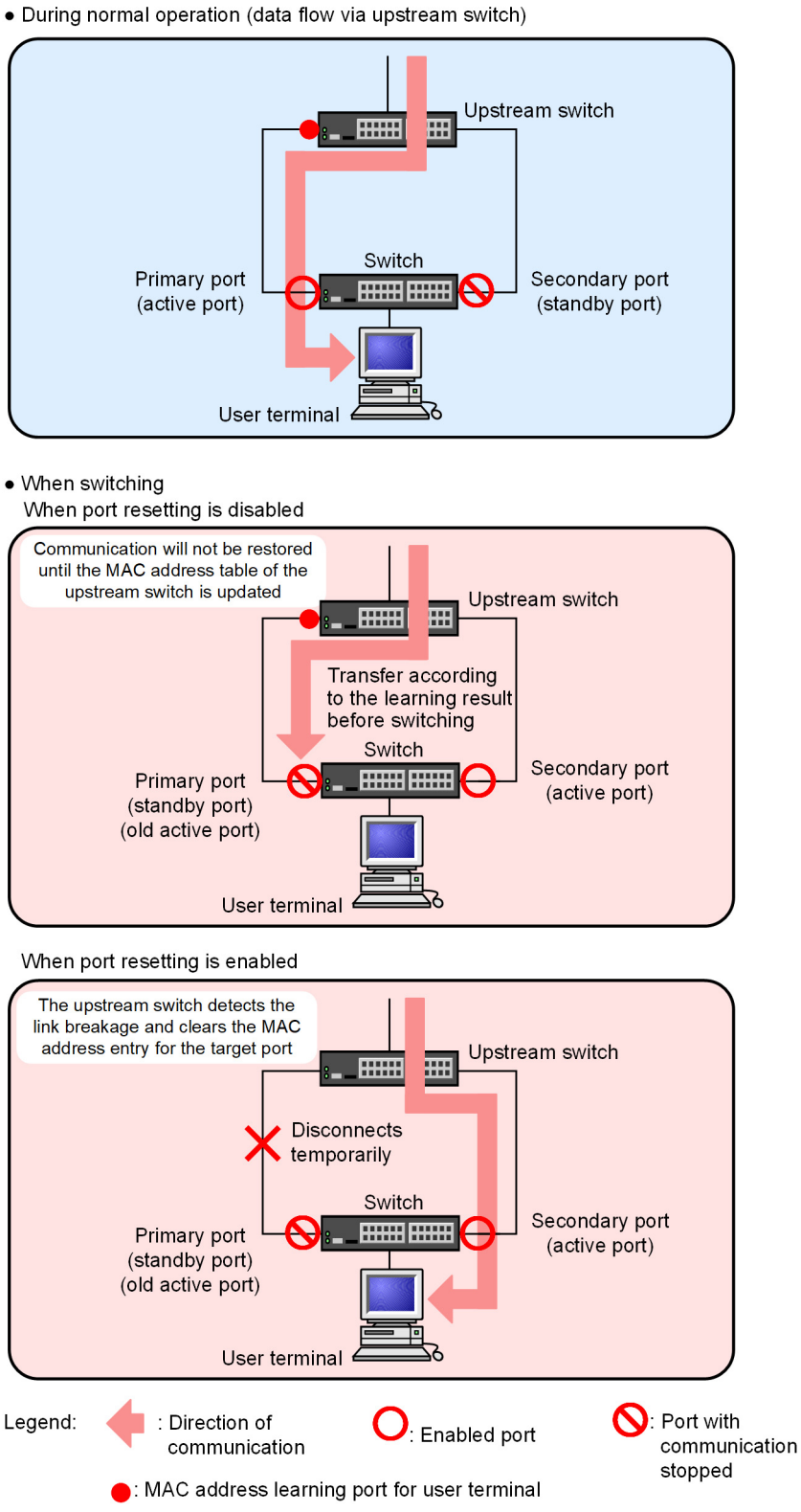
16.1.9 Port resetting

(1) Behavior overview

When the active port is changed by an operation command or automatic switchback, the old active port is temporarily brought down in order to quickly restore communication. The upstream switch to which the old active port is connected detects the link-down and clears the MAC address entry learned on the corresponding port from the MAC address table.

The following figure shows the difference in switching behavior depending on whether the port resetting is enabled or disabled.

Figure 16-6: Difference in switching behavior depending on whether the port resetting is enabled or disabled



Normal operation

The primary port on the Switch performs communication. Upstream switches learn the MAC address of the user terminal via the current communication path.

During port resetting (port resetting is disabled)

If the port resetting is disabled, although the secondary port is now active, the upstream switch retains the MAC address of the user terminal on the previous port. Therefore, communication is not restored until the MAC address learned on the corresponding port is erased or the user terminal sends traffic to the upstream switch.

During port resetting (port resetting is enabled)

When the port resetting is enabled, the active port is switched to the secondary port, and at the same time, the primary port (the old active port) is temporarily brought down. The upstream switch to which the old active port is connected detects the link-down and deletes the MAC address learned on the corresponding port, so the communication can be restored quickly.

16.1.10 Active port locking function at device startup

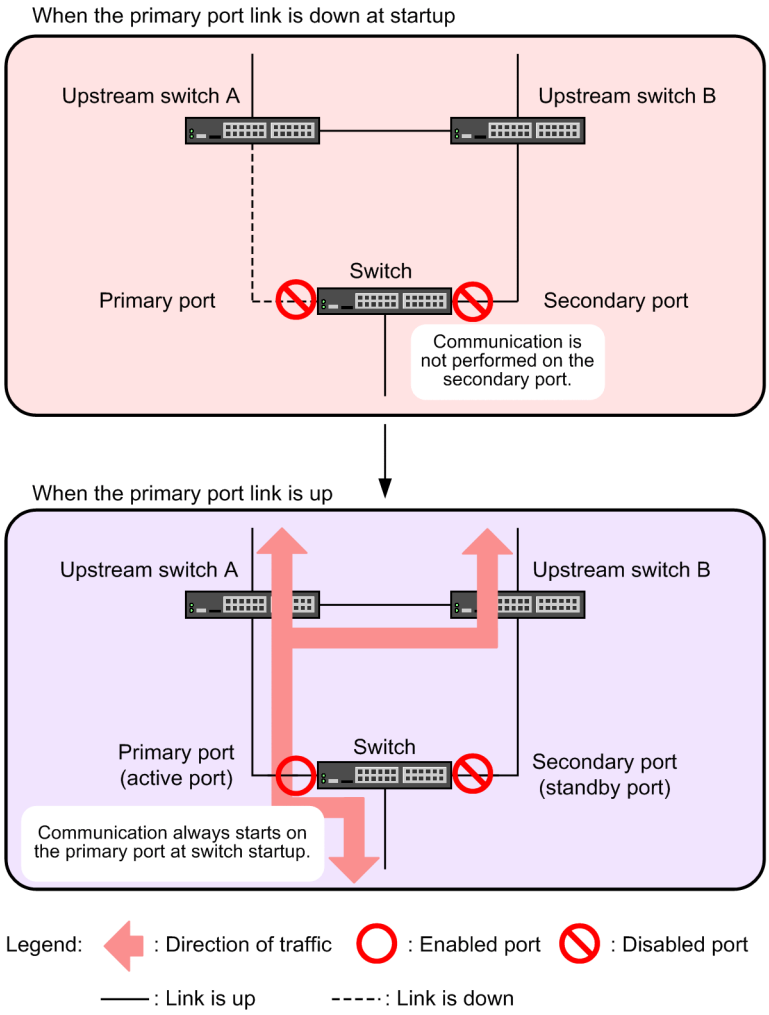
Use the active port locking function at device startup if you want to always start communication on the primary port when the device starts. When this function is enabled on a device, communication via the uplink port does not start even if the secondary port is enabled at startup. Instead, communication starts only when the primary port is enabled.

The active port locking function is canceled when one of the following conditions is met, and the active port is determined. After the active port is determined, the behavior proceeds as usual, and the active port is switched when a failure occurs on the active port or when an operation command is executed.

- When a link-up occurs on the primary port
- When a secondary port is changed to an active port due to an operation command
- When the master switch is switched during the stack configuration

The following figure shows behavior when the active port locking function at device startup is enabled.

Figure 16-7: Behavior when the active port locking function at device startup is enabled



16.1.11 Notes on using uplink redundancy

(1) Use with other function

(a) When used with the Layer 2 switch function

See "Configuration Guide Vol. 1, 22.3 Compatibility between the Layer 2 switch function and other functions".

(b) When used with Layer 2 authentication

For details, see "5.2.1 Using Layer 2 authentication with other functions".

(c) Coexistence with high reliability based on redundant configurations

The following table describes the high reliability based on redundant configurations that cannot be used, or only partially used, with uplink redundancy.

Table 16-3: Functions that cannot be used, or only partially used, with uplink redundancy

Function	Restrictions
GSRP	Cannot be used

(2) Using the send/receive function for flush control frames

Check whether the upstream switches support the reception of flush control frames sent by uplink redundancy.

If the upstream switches do not support the flush control frame function, the MAC address tables on the switches will not be cleared even if flush control frames are sent from the Switch. As a result, it might take some time before communication is restored.

(3) Sending flush control frames on trunk ports

If you want to send flush control frames on a trunk port, make sure you specify the destination VLAN. If you do not specify the destination VLAN, untagged flush control frames are sent only when a native VLAN exists. If no native VLAN is configured, flush control frames are not sent.

(4) Specifying configuration commands that disable VLANs

When you specify one of the configuration commands below related to uplink redundancy for the first time on the Switch, all VLANs temporarily go down. Therefore, before you create a network that uses uplink redundancy, we recommend that you set the following configuration commands beforehand.

- switchport backup flush-request
- switchport backup interface
- switchport backup mac-address-table update exclude-vlan
- switchport backup mac-address-table update transmit

(5) When using port resetting

When you install a transmitter between an uplink port and partner switch, the partner switch might not be able to directly detect a link-down. When you use port resetting, design the network so that the partner switch can directly detect a link-down.

Also, if the port resetting runs while some of the physical ports belonging to the channel group are inactive, the corresponding physical port on the old active port becomes active.

(6) When using port resetting in a stack configuration

In a stack configuration, if the master switch is switched while the port is down by the port resetting, the corresponding port may remain down. In this case, execute the operation command on the corresponding port.

(7) In a stack configuration

In a stack configuration, the link aggregation across multiple member switches cannot be set for the primary port and secondary port. The primary port and secondary port cannot be set on the interface of the same member switch.

(8) When using MAC address update function in a stack configuration

When using this function, set the learned MAC address aging time to 300 seconds or longer. Note that this function may not run correctly if the master switch is switched within 300 seconds after the initialization of the backup switch is completed.

16.2 Configuration

16.2.1 List of configuration commands

The following table describes the list of configuration commands for uplink redundancy.

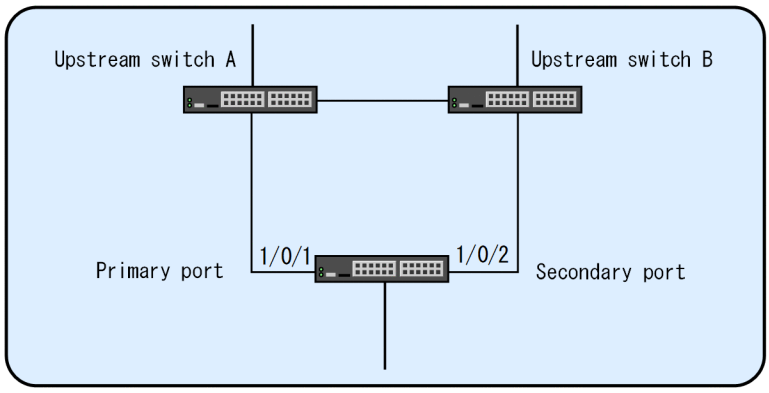
Table 16-4: List of configuration commands

Command name	Description
switchport backup flush-request transmit	Enables the sending of flush control frames to upstream switches at switchover or switchback to request that the upstream switches clear their MAC address tables.
switchport backup interface	Allows you to specify a primary port and secondary port for uplink redundancy and define them as an uplink port pair. You can also specify the automatic switchback wait time to enable automatic switchback.
switchport backup mac-address-table update exclude-vlan	Specifies a VLAN as one to which MAC address update frames are not to be sent.
switchport backup mac-address-table update transmit	Enables the sending of MAC address update frames to upstream switches at switchover or switchback to request that the upstream switches update their MAC address tables.
switchport backup reset-flush-port	Enables the port resetting during switching and switchback.
switchport backup reset-flush-time	Sets the port-down time due to the port resetting.
switchport-backup startup-active-port-selection	Enables the active port locking function at device startup.

16.2.2 Configuring uplink redundancy

The figure below describes an example uplink redundancy configuration. This subsection describes how to configure uplink redundancy based on this example.

Figure 16-8: Example of an uplink redundancy configuration



On the Switch, this configuration configures port 1/0/1 as the primary port and port 1/0/2 as the secondary port. It also specifies 60 seconds as the automatic switchback wait time and enables the sending of flush control frames.

(1) Configuring uplink redundancy

Points to note

Configure port 1/0/1 as the primary port and port 1/0/2 as the secondary port. Specify 60 seconds as the automatic switchback wait time. You need to disable Spanning Tree Protocols before you configure uplink redundancy. Configure the sending of flush control frames on the primary port.

Command examples

1. `(config)# spanning-tree disable`

   Disables a Spanning Tree Protocol.
2. `(config)# interface gigabitethernet 1/0/1`

   `(config-if)# switchport backup interface gigabitethernet 1/0/2 preemption-delay 60`

   Enters configuration command mode for port 1/0/1.

   Sets port 1/0/2 as the secondary port in the configuration command mode for port 1/0/1, which is the primary port. Sets the wait time for automatic switchback to 60 seconds.
3. `(config-if)# switchport backup flush-request transmit`

   `(config-if)# exit`

   Enables the sending of flush control frames.

Notes

- Before you configure uplink redundancy, the network is in a loop configuration. Shut down the primary port or the secondary port to prevent loops, and then set up the configuration.
- If you want to specify the ports in a link aggregation group as the primary port, use a port channel interface. You cannot use an Ethernet interface in a link aggregation group as the primary port.

16.2.3 Configuring port resetting

When the active port is switched, the uplink port for which the port resetting is set temporarily brings down the old active port.

Points to note

If you set port 1/0/1 as the primary port and port 1/0/2 as the secondary port, set the port resetting to port 1/0/1, which is the primary port.

Sets 5 seconds as the port-down time. The default is 3 seconds, but set this longer than the link-down detection time of the partner switch (e.g., when the Switch's "link debounce" configuration command or equivalent is set).

Command examples

1. `(config)# interface gigabitethernet 1/0/1`

   `(config-if)# switchport backup reset-flush-port`

   `(config-if)# switchport backup reset-flush-time 5`

   `(config-if)# exit`

Transitions to the configuration command mode of the primary port 1/0/1, and sets the port resetting. Sets 5 seconds as the port-down time.

16.3 Operation

16.3.1 List of operation commands

The following table describes the list of operation commands for uplink redundancy.

Table 16-5: List of operation commands

Command name	Description
show switchport-backup	Shows information about uplink redundancy.
show switchport-backup statistics	Shows statistics pertaining to uplink redundancy.
clear switchport-backup statistics	Deletes statistics pertaining to uplink redundancy.
set switchport-backup active	Specifies a new active port.
restart uplink-redundant	Restarts the uplink redundancy program.
dump protocols uplink-redundant	Outputs dump data regarding uplink redundancy to a file.

16.3.2 Displaying the status of uplink redundancy

You can display the destination VLANs for flush control frames and the status of the primary and secondary ports.

Figure 16-9: Results of executing show switchport-backup

```
> show switchport-backup
Date 20XX/09/04 16:48:07 UTC
startup active port selection: primary only
Switchport Backup pairs                          Preemption   Flush
 Primary     Status     Secondary   Status     Delay  Rest   VLAN  Update  Reset
 Port 1/0/1  Forwarding Port 2/0/18 Blocking       -     -   4093       -      -
 Port 1/0/10 Down       ChGr 4      Forwarding     -     -      -       1      -
*Port 1/0/11 Down       Port 2/0/15 Blocking       -     -     10       -      -
*Port 1/0/12 Down       Port 2/0/16 Down           -     -      -       -     3s
>
```

- Status column
  Forwarding indicates the active port, and Blocking indicates the standby port.

16.3.3 Manually changing the active port

To change the active port, use the "set switchport-backup active" command.

This command is effective only when the specified port is the standby port.

Figure 16-10: Results of executing set switchport-backup active

```
> set switchport-backup active port 1/0/1
Are you sure to change the forwarding port to specified port? (y/n): y
>
```

17 L2 Loop Detection

L2 loop detection is a function that detects a loop failure in a Layer 2 network and corrects the loop failure by deactivating the port causing the loop.

This chapter describes L2 loop detection and its use.

17.1 Description

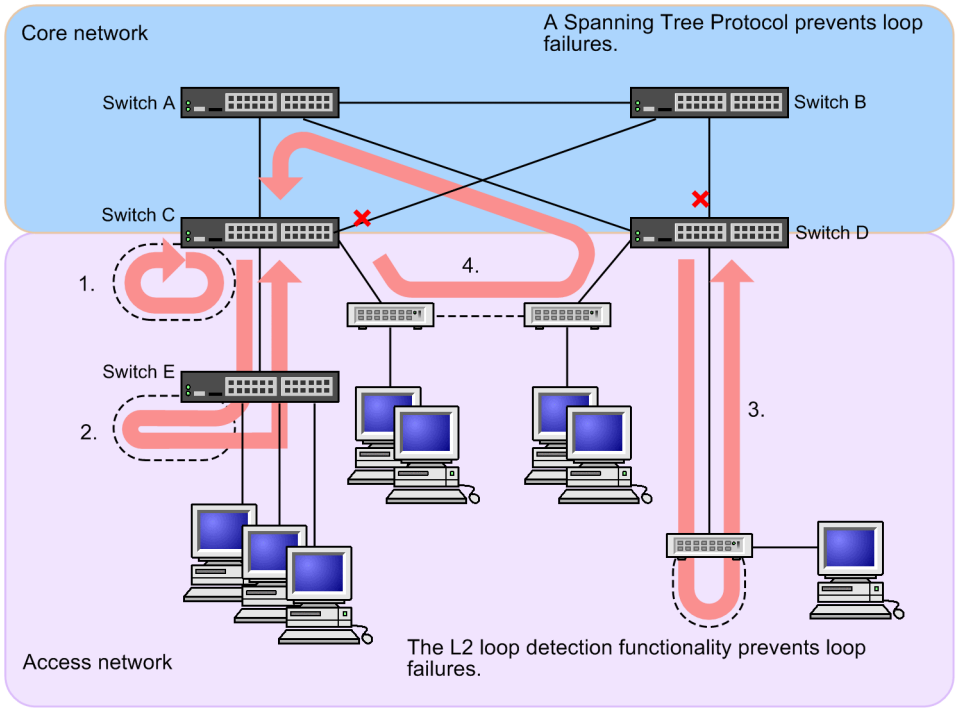
17.1.1 Overview

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 device. Spanning Tree Protocols and the Ring Protocol are provided to avoid such states. Generally, the L2 loop detection function corrects loop failures in a non-redundant access network, but not in the core network in which these protocols are used.

When a loop failure is detected on a local device, the L2 loop detection function deactivates 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.

The following figure shows the basic pattern of a loop failure.

Figure 17-1: Basic patterns of loop failures



Example loop failure patterns

1. A line is connected incorrectly to the Switch C and a loop failure occurs.
2. A line is connected incorrectly to the Switch E, which is lower than the Switch C, and a loop failure occurs.
3. A line is connected incorrectly to a device, which is lower than the Switch D, and a loop failure occurs.
4. A line is connected to a lower-level switch incorrectly, and a loop failure that spreads to the core network occurs.

As described above, the L2 loop detection function can detect loop failures in various locations, including those with incorrect connections to the local switch or to other devices.

17.1.2 Running specifications

In L2 loop detection, an L2 control frame for detecting an L2 loop (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 is received on a port on which the L2 loop detection function is enabled, a loop failure is detected, and the port on which the frame is received or the port originating the frame is deactivated.

After the cause of the loop failure has been corrected, an operation command can be used to activate the deactivated port. If the automatic-restoration function has been configured, the deactivated port can be activated automatically.

(1) Types of ports used by the L2 loop detection function

The following table describes the types of ports used by the L2 loop detection function.

Table 17-1: Port types

Type	Function
Detecting and blocking port	• This port sends an L2 loop detection frame to detect a loop. • If a loop failure is detected, an operation log is displayed and the problem port is deactivated by this port.
Detecting and sending port	• This port sends an L2 loop detection frame to detect a loop. • If a loop failure is detected, an operation log is displayed. The problem port is not deactivated.
Detecting port (when configuration has not been performed)	• This port does not send an L2 loop detection frame to detect a loop. • If a loop failure is detected, an operation log is displayed. The problem port is not deactivated.
Ports exempted from detection	• Any port for which the function is not used. The L2 loop detection frame for detecting a loop is not sent and a loop failure is not detected.
Uplink port	• This port does not send an L2 loop detection frame to detect a loop. • If a loop failure is detected, a behavior determined by the port type of the source port is performed. For example, if the source port is a detecting and blocking port, an operation log is displayed, and the source port is deactivated.

(2) Ports that send the L2 loop detection frame

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 specified interval. The maximum number of frames that can be sent with the function is predetermined, and any frames exceeding the maximum 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. For this reason, specify a maximum number of frames according to the capacity limits. For details, see "Configuration Guide Vol. 1, 3.9.1 L2 loop detection".

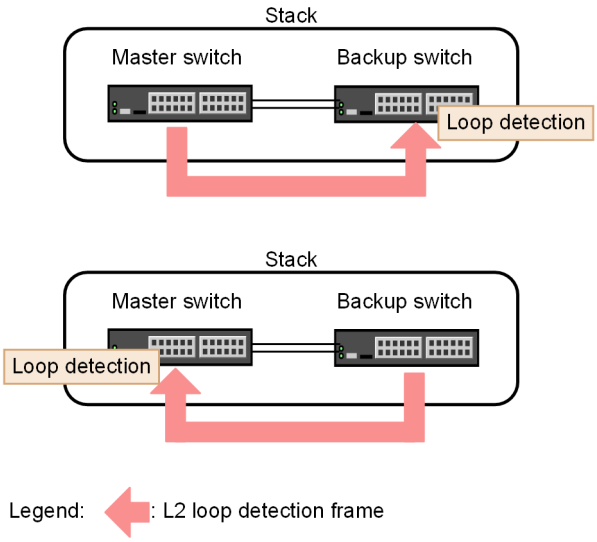
(3) How loop failures are detected and conditions for deactivating ports

When an L2 loop detection frame is received, if the frame is an L2 loop detection frame sent from the device and VLAN is set to the receiving port, it is considered a loop failure even between different VLANs. If a loop failure is determined by receiving an L2 loop detection frame, the number of received frames is counted for each port. When the number reaches the number of received L2 loop detection frames specified during configuration (the initial value is 1), the relevant port is deactivated.

(4) L2 loop detection behavior in a stack configuration

Even if L2 loop detection frames sent between member switches within the same stack are received, the L2 loop detection function works. The following figure shows loop detection in response to L2 loop detection frames in a stack configuration.

Figure 17-2: Loop detection in response to L2 loop detection frames in a stack configuration



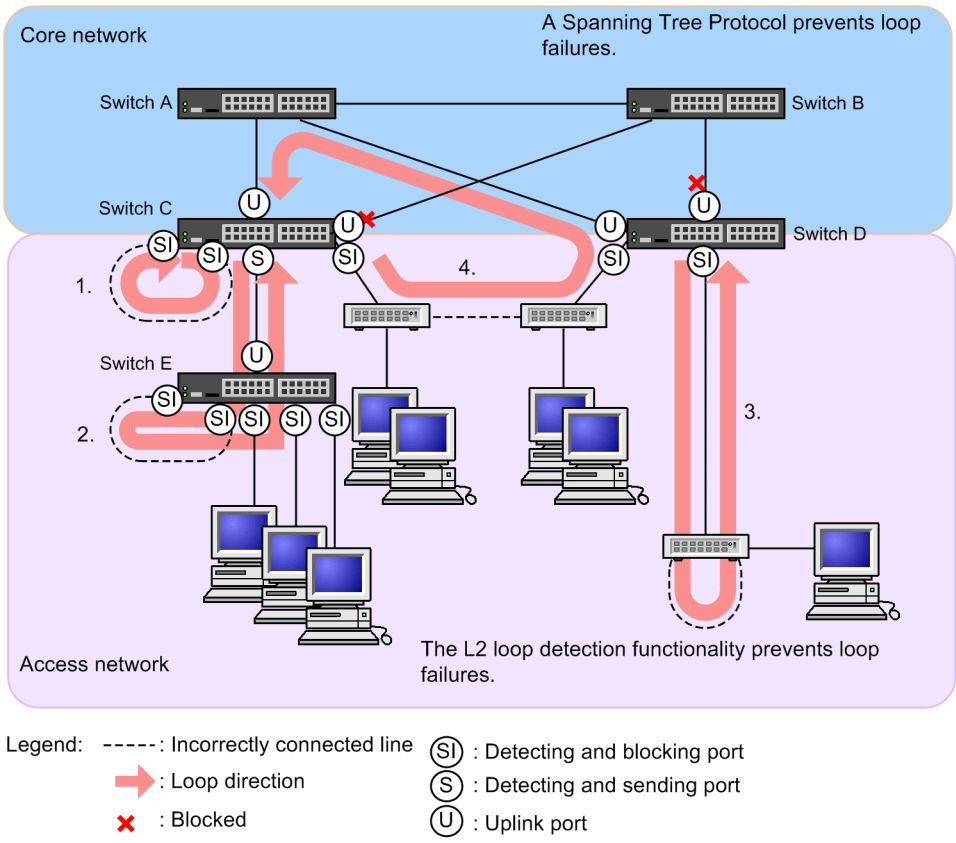
(5) Operational message indications

Even if an operation message for loop failure detection is displayed on some port and an L2 loop detection frame is received on the same port immediately after that, the operation message will not be displayed for 1 minute after the previous display. After 1 minute has passed since the previous display, when an L2 loop detection frame is received after that, the operation message for loop failure detection is displayed.

17.1.3 Application example

The following figure shows a network configuration to which the L2 loop detection function is used.

Figure 17-3: Network configuration in which the L2 loop detection function is used



(1) Using detecting and blocking ports

This port type is generally specified for L2 loop detection. As shown by Switches C, D, and E in the figure, specifying lower-level ports as detection-frame-sending-and-port-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 L2 loop detection is used on a device at the lowest possible level. When a Switch is connected to multiple layers (see Switches C and E in the figure), if a port on the Switch C side is deactivated due to an incorrect connection (2 in the figure), none of the terminals unrelated to the loop failure occurring on Switch E can connect to a higher-level network. This is the reason that using the L2 loop detection function in a lower-level Switch (Switch E in the figure) is recommended.

For such cases, specify a port on the Switch C side as the detecting and sending port. This setting allows Switch E to detect loop failures during normal operation, but if the Switch is unable to detect loop failures because L2 loop detection is configured incorrectly, Switch C can detect loop failures instead of being de-activated.

(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 4 in the figure is found, this setting allows connection to the core network to be reserved because the Switch C source port has been deactivated.

17.1.4 Notes on using the L2 loop detection function

(1) Behavior 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 devices 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.

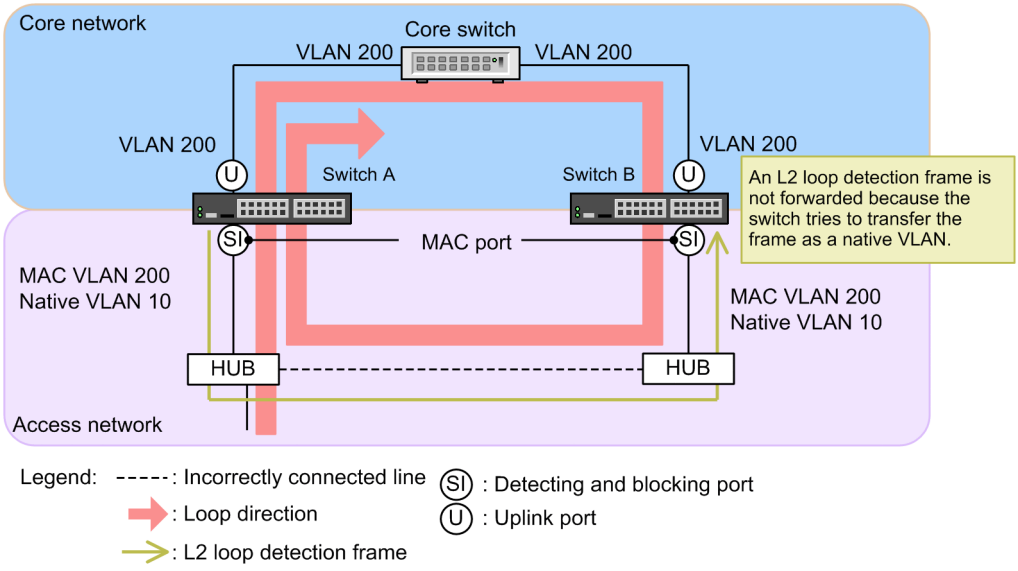
In such cases, if a port on the core network side specified as an uplink port is specified as the detecting and sending port, loop failures can be detected. The following are specific configuration examples.

(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.

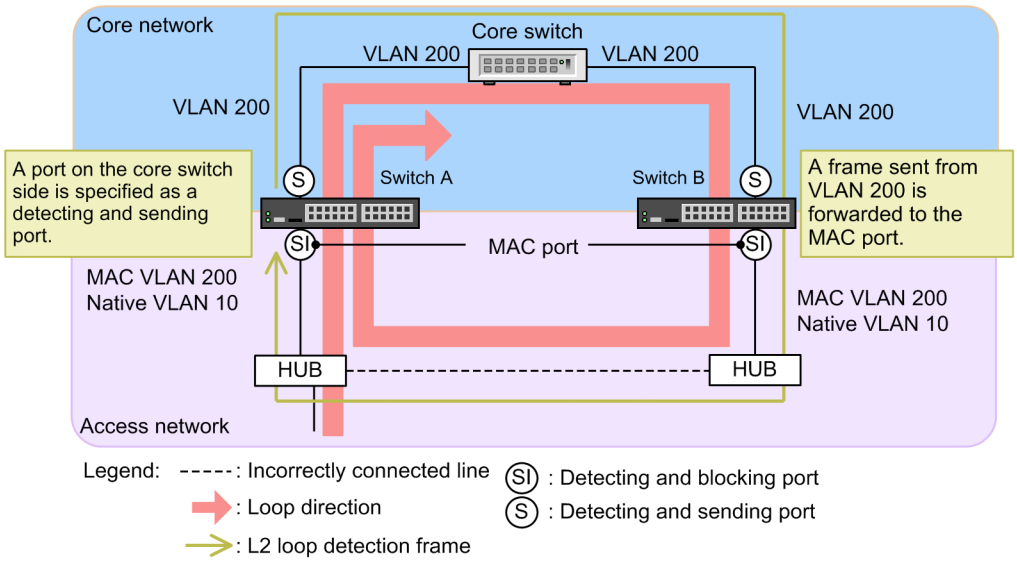
Figure 17-4: Configuration in which loop detection is restricted



(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 17-5: Configuration in which loops can be detected



(2) Behavior of the Switch when tag translation is used

A loop failure is detected in the following cases.

- When the tag-translated L2 loop detection frame sent from the tag translation port of the device returns within the network and is received by the device
- When an L2 loop detection frame that has been tag-translated by another device is received by the device

If you intentionally configure a network that loops back to the device, set the target port as a port exempted from detection to avoid a loop failure.

(3) Running environment for L2 loop detection

When the L2 loop detection function is used, if AX6700S and AX6300S series devices (before version 10.7), which do not support the functionality, are installed on the same network and either 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) Function that activates a deactivated port automatically (automatic-restoration function)

Note the following if you use the automatic-restoration function in static link aggregation:

- To change the line speed (which changes the network configuration), specify mixed-speed mode for the applicable channel group. If a loop is detected while changing the line speed when the mixed-speed mode is not specified, the automatic-restoration function might not run properly in the applicable channel group.
- If you use the auto-negotiation function 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 function might not run in the applicable channel group.

If the automatic-restoration function does not run, correct the cause of the loop, and then use the "activate" operation command to activate the port.

(5) Automatic-restoration function in a stack configuration

In a stack configuration where the automatic-restoration function is set and which automatically changes the port status from inactive to active, if a loop failure is detected and thus the master switch is changed when the port is inactive, the port for a new master switch remains inactive. In this case, use the "activate" operation command to activate the port.

(6) Using a Ring Protocol or Spanning Tree with stack configuration

In a stack configuration, if the Ring Protocol or Spanning Tree is enabled, do not target ports in the blocking status for L2 loop detection.

17.2 Configuration

17.2.1 List of configuration commands

The following table describes the list of configuration commands for L2 loop detection.

Table 17-2: List of configuration commands

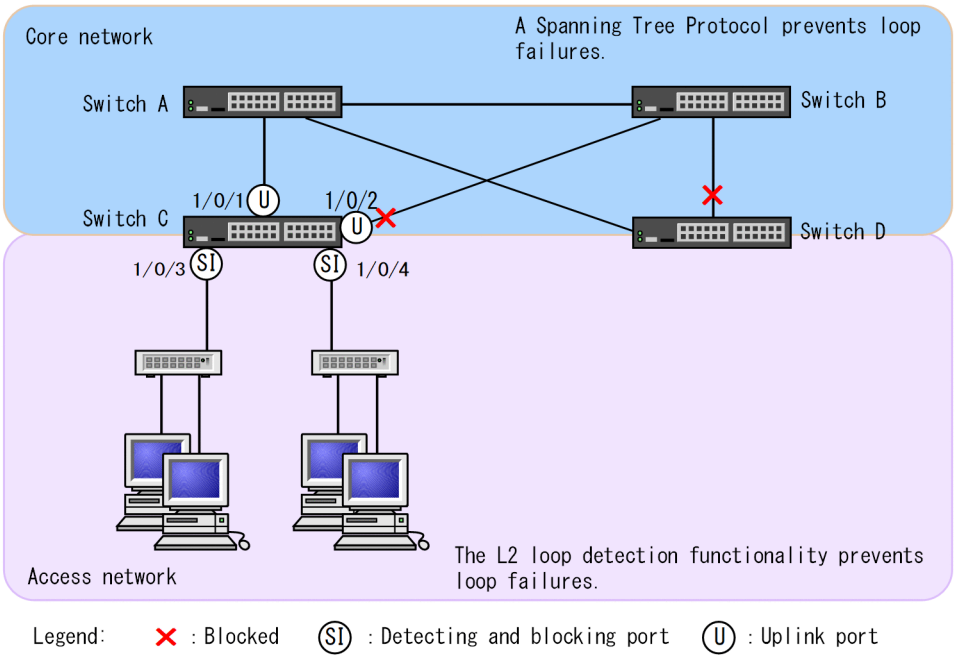
Command name	Description
loop-detection	Sets the port type for the L2 loop detection function.
loop-detection auto-restore-time	Sets the time (in seconds) until a deactivated port is activated automatically.
loop-detection enable	Enables the L2 loop detection function.
loop-detection hold-time	Specifies the time (in seconds) that the number of received L2 loop detection frames is held before a port is changed to the inactive status.
loop-detection interval-time	Sets the interval for sending L2 loop detection frames.
loop-detection threshold	Sets the number of received L2 loop detection frames before a port is deactivated.

17.2.2 Configuring the L2 loop detection function

The following describes how to configure L2 loop detection. Switch C is used in the figure below as an example.

Specify ports 1/0/1 and 1/0/2 as uplink ports because they are connected to the core network. Set ports 1/0/3 and 1/0/4 as detecting and blocking ports because they are connected to lower-level switches.

Figure 17-6: Example of configuring L2 loop detection



(1) Configuring L2 loop detection

Points to note

In the configuration file for L2 loop detection, enable L2 loop detection for the entire device and specify the ports on which to actually detect L2 loop failures.

Command examples

1. `(config)# loop-detection enable`

   Enables the L2 loop detection function on the Switch.

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

   `(config-if-range)# loop-detection uplink-port`

   `(config-if-range)# exit`

   Sets ports 1/0/1 and 1/0/2 as uplink ports. With this specification, if an L2 loop detection frame is received on ports 1/0/1 and 1/0/2, behaviors based on the port type of the source port are performed for the source port.

3. `(config)# interface range gigabitethernet 1/0/3-4`

   `(config-if-range)# loop-detection send-inact-port`

   `(config-if-range)# exit`

   Sets ports 1/0/3 and 1/0/4 as detecting and blocking ports. With this specification, the ports 1/0/3 and 1/0/4 send L2 loop detection frames. In addition, if a loop failure is detected on either of these ports, the port is deactivated.

(2) Setting interval for sending L2 loop detection frames

Points to note

Frames exceeding the maximum rate for sending L2 loop detection frames will not be 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 rate for sending L2 loop detection frames is exceeded, specify a longer interval so that no frames will exceed the maximum sending 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

Normally, a port is deactivated if a loop failure is detected, in which case you do not need to change the initial value (one occurrence). However, to avoid deactivating a port 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`

   Deactivates a port when 100 L2 loop detection frames have been received.

2. `(config)# loop-detection hold-time 60`

   Holds the number of received L2 loop detection frames for 60 seconds. The period starts from the time the last frame was received.

(4) Setting the automatic-restoration time

Points to note

The example below shows how to activate a deactivated port automatically.

Command examples

1. `(config)# loop-detection auto-restore-time 300`
   Sets deactivated ports to automatically activate in 300 seconds.

17.3 Operation

17.3.1 List of operation commands

The following table describes the list of operation commands for the L2 loop detection function.

Table 17-3: List of operation commands

Command name	Description
show loop-detection	Shows L2 loop detection information.
show loop-detection statistics	Shows L2 loop detection statistics.
show loop-detection logging	Shows L2 loop detection log data.
clear loop-detection statistics	Clears L2 loop detection statistics.
clear loop-detection logging	Clears L2 loop detection log data.
restart loop-detection	Restarts the L2 loop detection program.
dump protocols loop-detection	Outputs L2 loop detection dump information to a file.

17.3.2 Checking the L2 loop status

You can use the "show loop-detection" 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.

You can also check for ports that have been deactivated due to a loop failure in the status section of the port information section.

Figure 17-7: L2 loop detection information

```
> show loop-detection
Date 20XX/04/21 12:10:10 UTC
Interval Time           :10
Output Rate             :30pps
Threshold               :1
Hold Time               :infinity
Auto Restore Time       :-
VLAN Port Counts
    Configuration       :103         Capacity      :300
Port Information
  Port    Status     Type         DetectCnt RestoringTimer  SourcePort  Vlan
  1/0/1   Up         send-inact           0              -  -
  1/0/2   Down       send-inact           0              -  -
  1/0/3   Up         send                 0              -  -
  1/0/4   Up         exception            0              -  -
  1/0/5   Down(loop) send-inact           1              -  CH:32(U)     100
  CH:1    Up         trap                 0              -  -
  CH:32   Up         uplink               -              -  1/0/5        100
>
```

18 Storm Control

Storm control function limits the number of flooding frames that are forwarded. This chapter describes storm control and its use.

18.1 Description

18.1.1 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 the function 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.

In the Switch, the allowable reception rate for each Ethernet interface can be specified, so that the frames subject to flooding that exceed that reception rate are discarded. You can specify three separate allowable reception rates, one each for broadcast frames, multicast frames, and unicast frames.

Furthermore, as actions when a storm is detected, you can block the port, send a private SNMP notification, or output an operation message.

Storm control function does not have any operation commands.

18.1.2 Notes on using storm control function

(1) Execution of action by storm detection and frame discard trigger

The action performed during the storm detection runs when the number of frames received per second exceeds the specified reception rate. On the other hand, in order to reduce the impact of burst reception in a short period of time, frames are discarded in a shorter period when the allowable reception rate is exceeded. Therefore, if short-time burst reception of less than one second occurs, no action may be taken even if the allowable reception rate is exceeded and frames are discarded.

(2) Execution of action by storm detection

Actions that are executed when a storm is detected may be executed at a reception rate lower than the specified reception rate, such as when the CPU load is high. Set the receiving rate to a rate with a margin.

(3) Storm detection and recovery

The Switch determines that a storm has occurred when the number of frames received in one second exceeds the reception rate specified in the configuration section. After a storm occurs, if the number of frames received per second drops below the reception rate and remains there for 30 seconds, the switch is considered to have recovered from the storm.

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 a port is 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.

(4) Handling unicast frames

For the Switch, unicast storm detection and the frames to be discarded are not the same. A unicast storm detection is performed for all unicast frames received on the port for which the allowable reception rate is set. On the other hand, frames are discarded and counted only for unicast frames that are flooded because the destination MAC address is not registered in the MAC address table when this number of frames exceeds the reception rate.

(5) Storm detection when using filters

If a filter discard and a storm detection occur simultaneously, more frames may be discarded, including frames that should have been relayed.

(6) Storm detection when using bandwidth monitoring

If a bandwidth monitoring violation and a storm detection occur simultaneously, more frames may be discarded, including frames that should have been relayed.

18.2 Configuration

18.2.1 List of configuration commands

The following table describes the list of configuration commands for storm control.

Table 18-1: List of configuration commands

Command name	Description
storm-control	Sets the allowable reception rate for storm control. In addition, behaviors that can be performed when a storm is detected can be specified.

18.2.2 Configuring storm control

- Suppressing broadcast frames

  To prevent broadcast storms, specify the allowable reception rate 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 reception rate 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 IPv4 multicast packets, IPv6 multicast packets, and control packets such as the OSPF packet.

- 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 reception rate with enough margin so that a storm is not detected from normal-behavior frames.

- Behaviors when a storm is detected

  Specify the Switch behaviors to be performed when a storm is detected. You can select any combination of blocking a port, sending a private SNMP notification, and outputting an operation message for each port.

  - Blocking a port

    When a storm is detected on a port, deactivate the port. To activate the port again after recovery from the storm, use the "activate" command.

  - Sending a private SNMP notification

    When a storm has been detected, after recovery is detected, a private SNMP notification is sent.

  - Operation message output

    When a storm has been detected, after recovery is detected, an operation message is output as a notification. Note that a message must be output if a port is blocked.

Points to note

The mirroring of sent or received frames can be defined for Ethernet interfaces.

If a storm occurs on a port, the port is blocked.

Command examples

1. `(config)# interface gigabitethernet 1/0/10`

   `(config-if)# storm-control broadcast level pps 50`

   Sets the allowable reception rate for broadcast frames to 50 pps.
2. `(config-if)# storm-control multicast level pps 500`

   Sets the allowable reception rate for multicast frames to 500 pps.
3. `(config-if)# storm-control unicast level pps 1000`

   Sets the allowable reception rate for unicast frames to 1000 pps.
4. `(config-if)# storm-control action inactivate`

   Deactivates a port when a storm is detected on the port.

19 Port Mirroring

Port mirroring is a function that sends a copy of sent or received frames to the specified physical port. This chapter describes port mirroring and its use.

19.1 Description

19.1.1 Overview of port mirroring

Port mirroring is a function that sends a copy of frames sent or received on the specified physical port to the specified physical port. Copying a frame is called mirroring, and the copied frame is called a mirroring frame. By using an analyzer to receive the forwarded mirroring frame, you can monitor or analyze traffic.

The following figures show the flow of received frames and sent frames when mirroring is used.

Figure 19-1: Mirroring of received frames

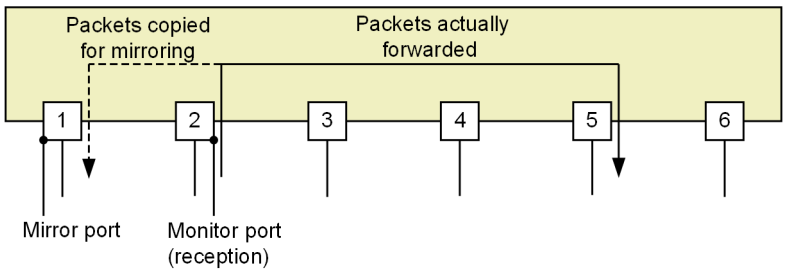
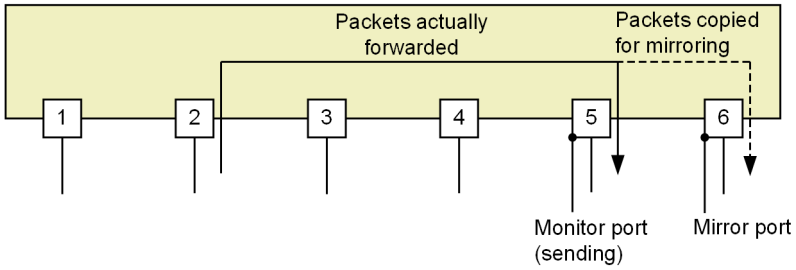


Figure 19-2: Mirroring of sent frames



As shown in these figures, the physical port that monitors traffic is called the monitor port, and the physical port to which mirroring frames are sent is called the mirror port.

19.1.2 Running specifications of port mirroring

(1) Basic behavior

Port mirroring on the Switch sets the port that monitors traffic as a monitor port. The destination port for mirroring frames is set as the mirror port. A mirror port is a port dedicated to mirroring.

Note that when a mirroring frame is sent, the TTL value (IPv4) or the hop limit value (IPv6) is not decremented. Frames received on the mirror port are discarded.

(2) Monitored session

The combination of a monitor port and a mirror port is called a monitored session. In a monitored session, you can specify the frame to be monitored, monitor port, and mirror port. Select one of the three types of frames to be monitored: receive frame, send frame, or send or receive frame.

For the Switch, a maximum of four monitored sessions can be defined. You can set up to three monitored sessions for mirroring sent or received or sent frames, and up to four monitored sessions for mirroring received frames.

For each monitor session, monitor and mirror ports can be configured "multipoint-to-point". That is, copies of frames sent or received by multiple monitor ports can be sent to one mirror port.

You can also use mirroring for the monitor port and mirror port even if the speed and line type are different. If you specify multiple monitor ports in one monitor session, you can specify monitor ports with different speeds and line types at the same time. However, because mirroring frames are sent at a speed equal to or less than the line bandwidth of the mirror port, mirroring frames may be discarded if the volume of mirroring frames exceeds the bandwidth of the mirror port.

(3) Monitor port

You can specify an Ethernet interface other than the following ports for the monitor port. Even if it is specified as a monitor port, there are no restrictions on port or interface function.

- Ports set as mirror ports
- Port designated as monitor port for other monitored sessions
- Management port

(4) Mirror ports

Set the port to which you want to send mirroring frames as the mirror port. A mirror port is a port dedicated to mirroring. Each function on the mirror port is described below.

- VLANs and Layer 3 communication function are unavailable. Therefore, Spanning Tree Protocols, the Ring Protocol, and IGMP snooping/MLD snooping, which are based on VLANs, and SNMP and DHCP, which are based on Layer 3 communication function, are also unavailable.
- When the function to send control frames to the mirror port is set, control frames for the set function are sent to the mirror port in addition to the mirroring frames.
- If a filter is set on the sending side of a mirror port, mirroring frames are also filtered. Therefore, by setting discard for the filter, only the necessary frames can be sent from the mirroring frames when mirroring is performed for each port.
- The QoS send control also works with mirror ports. As a result, mirroring frames may be discarded and not sent from the mirror port. For details, see "4 Send Control".
- Mirroring frames are also sent when a mirror port is set for a port that is used as an uplink redundancy port and is in standby port status.
- A mirroring frame is also sent when a mirror port using the 802.1Q tagging function is set for a port in the standby link status due to the link-not-down mode of link aggregation.

(5) Mirroring of received frames

If you specify a send or receive frame or receive frame as a frame to be monitored, you can mirror the receive frame. At this time, all frames received by the monitor port are subject to mirroring.

Therefore, frames discarded at the monitor port due to the receive filter set for the monitor port, QoS bandwidth monitoring, or storm control are not relayed, but are subject to mirroring. However, frames discarded as error frames on the Ethernet interface when received are not mirrored.

(6) Mirroring of sent frames

If you specify a send or receive frame or send frame as a frame to be monitored, you can mirror the send frame. Frames to be monitored and behavior for each condition are as follows.

- The Switch mirrors only the frames that are forwarded by hardware. The switches do not mirror any frames sent by software (such as frames addressed to the device and packets with an IP option). However, the switch can mirror frames sent by the software only if the port of the backup switch is set as the monitor port when a stack is configured. At this time, some control frames are mirrored as tagged frames with a VLAN ID of 4095.
- When untagged frames are mirrored, tagged frames with the VLAN ID of the VLAN sent by the monitor port are mirrored.
- When the tag translation is used on the monitor port, mirroring is performed as a tagged frame with the VLAN ID of the VLAN sent by the monitor port, not the VLAN tag specified by the tag translation.
- The TPID of the mirroring frame will be the TPID of the mirror port.
- Frames discarded by QoS send control on the monitor port are not mirrored.
- When discard is set in the sender filter, the mirroring of frames to be discarded is as follows.
  - When set to the Ethernet interface, frames discarded by the filter on the monitor port are also subject to mirroring and are sent from the mirror port.
  - If the VLAN interface to which the monitor port belongs is set, frames discarded by the filter on the monitor port are also subject to mirroring. However, if the VLAN ID of the mirroring frame matches that filter, it will be discarded by the filter after mirroring, so it will not be sent from the mirror port.
- For mirroring of VXLAN frames, see "Configuration Guide Vol. 1, 22.3 Compatibility between the Layer 2 switch function and other functions".

19.1.3 802.1Q Tagging function

The 802.1Q tagging function is the functionality that attaches VLAN tags to mirroring frames. By using this function, mirroring frames can be forwarded to a traffic monitoring device such as an analyzer in a remote location through Layer 2 forwarding based on the attached VLAN tag. However, because the MAC address of the frame received on the monitor port is used as the MAC address of the mirroring frame, the device that relays the mirroring frame receives a frame with a MAC address that differs from the actual network configuration. Therefore, suppress MAC address learning in the VLAN used for relay (VLAN tag attached to the mirroring frame).

When this function is used even if it is set as a mirror port, function other than protocol VLAN and MAC VLAN can be used.

The following table shows the VLAN tag fields attached to frames by the 802.1Q tagging function.

Table 19-1: VLAN tag field attached to frames by the 802.1Q tagging function

field	Description	Support
TPID	An EtherType value indicating that the IEEE 802.1Q VLAN tag continues	Follows the TPID of the port used as the mirror port.
User Priority	IEEE 802.1D priority	The Switch supports only default (3).
CF (Canonical Format)	Whether the MAC address in the MAC header follows a standard format	The Switch supports only standard (0) formats.
VLAN ID	VLAN ID	VLAN IDs from 2 to 4094 can be used.

19.1.4 Notes applying when port mirroring is used

(1) Notes on use with other functions

- When the following functions are used together, the target packets will be sent by software, so they are not mirrored.
  - All DHCP packets sent by the Switch when DHCP snooping originating from the device is enabled
  - All ARP packets sent by the Switch when dynamic ARP inspection is enabled
- Keep the following in mind when using the policy-based mirroring.
  - Monitored session numbers used in policy-based mirroring cannot be used.
  - Sent frames cannot be mirrored.
  - A port used as a mirror port in policy-based mirroring cannot be set as a mirror port.

(2) Notes when mirroring sent frames

- The order of frames sent from the mirror port may differ from the order of frames sent from the monitor port.
- For frames flooding to multiple monitor ports with multiple monitor ports set to one monitored session, only one frame is mirrored.
- When IP multicast relay frames are sent from the monitor port, the frames sent from the mirror port are tagged with the VLAN ID of the VLAN that received the frame. As for Ethernet frame header information other than VLAN tags, the port mirroring function also uses the received frame.
- Some frames are mirrored even if communication is not possible on the monitor port due to the following conditions.
  - Blocking, Discarding, Listening, or Learning status caused by the Spanning Tree Protocols
  - Blocking status caused by GSRP
  - Blocking status caused by the Ring Protocol
  - Standby port for uplink redundancy
  - Not authorized by IEEE 802.1X

  Frames to be mirrored are as follows:

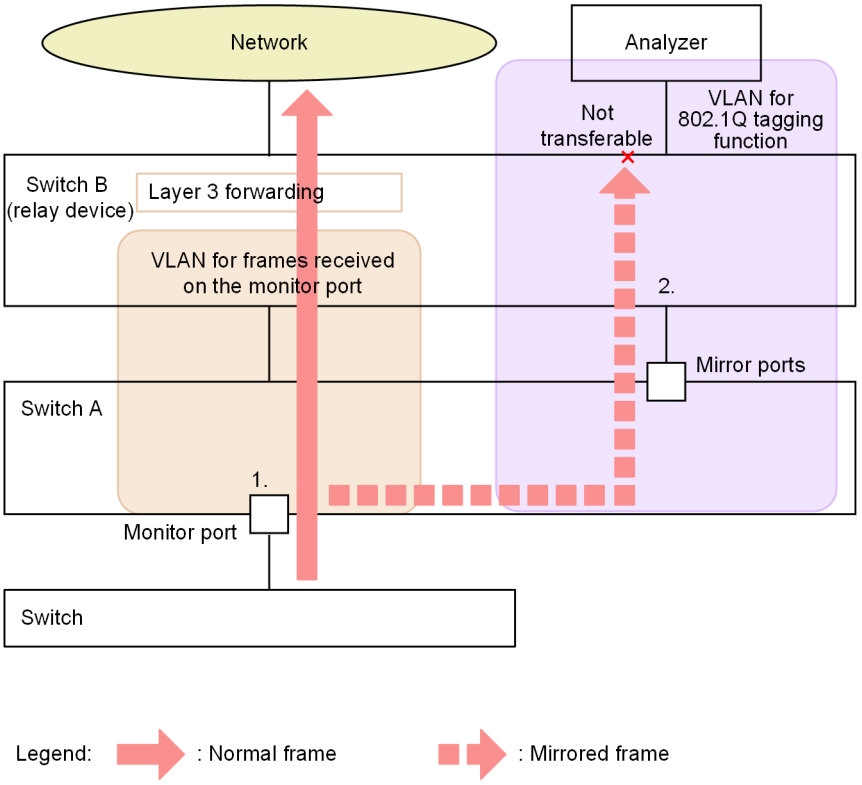
  - Flooded frames
  - Frames that match entries in the MAC address table while the MAC address table is being cleared to prevent the status of the monitor port from being sent
- When flooding frames received on a VXLAN Access port while this port is specified as a monitor port, the target frames are mirrored.

  At this time, if the target VXLAN Access port is using the VNI mapping method for subinterface mapping and an untagged frame to be flooded is received, the mirroring frame will be a tagged frame with a VLAN ID of 4095. [SL-L3A]
- If you are using the IP multicast routing function and the IGMP/MLD snooping function at the same time on the Switch, a port with IP multicast enabled is specified as the monitor port, and an IP multicast packet corresponding to a registered negative cache or forwarded entry is received on the corresponding monitor port, the corresponding IP multicast packet is mirrored.

(3) Notes applying when port mirroring 802.1Q tagging function is used

- Because VLAN tags are attached, frames that are 4 bytes larger than usual need to be handled. In particular, when mirroring tagged frames and sent frames, frames that are 8 bytes larger than usual need to be handled since the mirroring frame has two levels of VLAN tags.
- Connect a trunk port to the port to be set as a mirror port.
- Mirroring frames are sent regardless of the communication status of the link aggregation and Layer 2 switch function set for the same port as the mirror port.
- When a unicast frame received on a monitor port is addressed to a relay device, it is received by the relay device that has the MAC address of the mirroring frame as its own address, so layer 2 forwarding based on the attached VLAN tag is not possible. To perform Layer 2 forwarding on the relay device, set the MAC address for each VLAN for the VLAN that will forward the monitored frame.

Figure 19-3: Mirroring of frames addressed to the relay device



1. Unicast frames addressed to the Switch B is received at the monitor port of the Switch A
   The MAC address of the VLAN of the frame received on the monitor port and that of the VLAN of the 802.1Q tagging function will be the same.
2. The mirroring frame is received by the Switch B as its own address
   Frames addressed to the device cannot be forwarded to the analyzer because Layer 2 forwarding is not performed.

19.2 Configuration

19.2.1 List of configuration commands

The following table describes the list of configuration commands for port mirroring.

Table 19-2: List of configuration commands

Command name	Description
monitor session	Configures port mirroring.

19.2.2 Configuring port mirroring

When port mirroring is configured, a combination of monitor ports and a mirror port is defined as a monitored session.

Monitored sessions are identified by using session numbers 1 to 4. A session number is specified when a new session is created or an existing session is deleted. If an existing session number is specified when a new session is created, the existing session definition corresponding to the specified session number is overwritten by the new definition.

Ports used for normal data communication are specified as monitor ports. A port to which an analyzer is connected for monitoring or analyzing the traffic, or the port for Layer 2 forwarding of mirroring frames using 802.1Q tagging function 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 2 source interface gigabitethernet 1/0/1 rx destination interface gigabitethernet 1/0/5`

   Sets monitored session in which an analyzer is connected to port 1/0/5, and sets the mirroring of frames received by the Gbit Ethernet interface 1/0/1. Use session number 2.

(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. When sent frames are mirrored, session numbers 1 to 3 can be used.

Command examples

1. `(config)# monitor session 1 source interface gigabitethernet 1/0/2 tx destination interface gigabitethernet 1/0/6`

Sets monitored session in which an analyzer is connected to port 1/0/6, and sets the mirroring of frames sent by the Gbit Ethernet interface 1/0/2. Use session number 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. When sent or receive frames are mirrored, session numbers 1 to 3 can be used.

Command examples

1. `(config)# monitor session 1 source interface gigabitethernet 1/0/3 both destination interface gigabitethernet 1/0/11`

   Sets monitored session in which an analyzer is connected to port 1/0/11, and sets the mirroring of frames sent and received by the Gbit Ethernet interface 1/0/3. Use session number 1.

(4) Mirroring of multiple monitor ports

Points to note

You can set multiple monitor ports in the form of a list. You can also add or remove ports from an already-set list.

Command examples

1. `(config)# monitor session 1 source interface gigabitethernet 1/0/1-23, tengigabitethernet 1/0/25 both destination interface gigabitethernet 1/0/24`

   Sets monitored session in which an analyzer is connected to port 1/0/24 and sets the mirroring of frames sent and received by the Gbit Ethernet interfaces 1/0/1 to 1/0/23 and the 10 Gbit Ethernet interface 1/0/25. Use session number 1.

(5) Mirroring using 802.1Q tagging function

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.

When mirroring tagged frames and sent frames, frames that are 8 bytes larger than usual need to be handled since the mirroring frame has two levels of VLAN tags. Therefore, it is necessary to change the MTU length with the "mtu" command.

Command examples

1. `(config)# monitor session 1 source interface gigabitethernet 1/0/1 both destination interface gigabitethernet 1/0/2 encapsulation dot1q 10`

   Mirror frames sent and received on the Gigabit Ethernet interface 1/0/1, set mirroring frames to be sent from ports 1/0/2 with a VLAN Tag of VLAN 10. Use session number 1.

20 Policy-based Mirroring

Policy-based mirroring is a function that copies specific flows from received frames and sends them to specified interfaces. This chapter describes policy-based mirroring and its use.

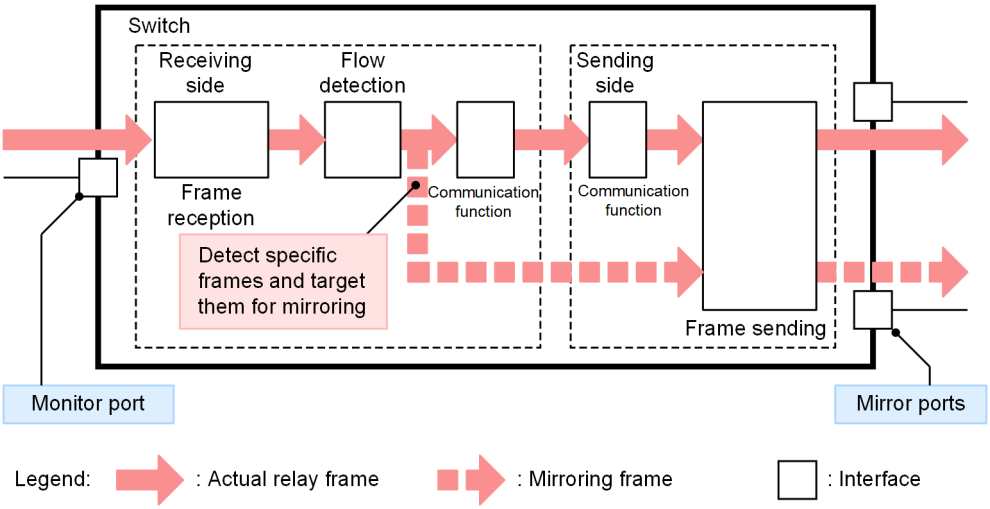
20.1 Description

20.1.1 Overview

Policy-based mirroring is a function that copies specific flows from received frames and sends them to specified interfaces. Copying a frame is called mirroring, and the copied frame is called a mirroring frame. By using an analyzer to receive the forwarded mirroring frame for each flow, you can monitor or analyze traffic.

The following figure shows how mirroring works for received frames.

Figure 20-1: Mirroring of received frames



As shown in the figure, the interface that monitors traffic is called the monitor port, and the interface to which mirroring frames are sent is called the mirror port.

The policy-based mirroring of the Switch can identify frames in detail by flow detection. In addition, mirroring can be performed simultaneously on multiple mirror ports.

20.1.2 Running specifications of policy-based mirroring

(1) Basic specifications

A port to which an analyzer is connected for monitoring or analyzing the traffic is specified as a mirror port. A mirror port is a port dedicated to mirroring.

The combination of a monitor port and a mirror port is called a monitored session. For the Switch, multiple monitored sessions can be defined. Also, frames received by the monitor port can be sent to different mirror ports.

The monitor port and mirror port can be used in the following combinations.

- 1 monitor port to 1 mirror port
- Multiple monitor ports to multiple mirror ports

Different speed ports can be set for the monitor port and mirror port. Since mirrored frames are sent within the line bandwidth of the mirror port, frames that exceed the line bandwidth are discarded.

(2) Monitor port

The monitor port for policy-based mirroring is set using an access list that identifies the target flows. When setting a monitor port, set the flow detection mode on the receiving side to the mode that supports policy-based mirroring.

By applying the access list where the destination interface list of policy-based mirroring is configured as "behavior" to the interface, the corresponding interface is used as a monitor port. The following table shows the configuration command parameters that are specified when applying an access list to an interface.

Table 20-1: Parameters to be specified when applying the access list

Mirroring direction	Parameter
Receiving-side	in-mirror

For target interfaces, flow detection conditions, and notes, see "1 Filters".

(3) Mirror ports

The mirror port for policy-based mirroring is set in the destination interface list.

Multiple mirror ports can be set for the destination interface list. If multiple mirror ports are set, mirroring is performed simultaneously on all set mirror ports. Only physical interfaces can be set as mirror ports.

Each function on the mirror port is described below.

- VLANs and Layer 3 communication function are unavailable. Therefore, Spanning Tree Protocols, the Ring Protocol, and IGMP snooping/MLD snooping, which are based on VLANs, and SNMP and DHCP, which are based on Layer 3 communication function, are also unavailable.
- When the function to send control frames to the mirror port is set, control frames for the set function are sent to the mirror port in addition to the mirroring frames.
- If a filter is set on the sending side of a mirror port, mirroring frames are also filtered. Therefore, if the filter is set to discard, the mirroring frames are discarded on the mirror port.
- Mirroring frames are also sent when a mirror port is set for a port that is used as an uplink redundancy port and is in standby port status.
- A mirroring frame is also sent when a mirror port is set for a port in the standby link status due to the link-not-down mode of link aggregation.

(4) Mirroring of received frames

- Among the frames received on the monitor port, mirroring targets frames for which flows are detected by an access list that specifies policy-based mirroring. However, frames discarded as error frames on the Ethernet interface when received are not mirrored.
- Frames discarded at the monitor port due to the receive filter set for the monitor port, QoS bandwidth monitoring, or storm control are not relayed, but are subject to mirroring.

20.1.3 Notes applying when policy-based mirroring is used

(1) When used with port mirroring

- The monitor session number used in port mirroring cannot be set for policy-based mirroring.
- Policy-based mirroring cannot be used when mirroring of sent frames is used for the port mirroring.

(2) Notes applying when policy-based mirroring is used

If a filter is set on the sending side on a VLAN interface, the filter is also enabled when the VLAN ID of a mirrored frame matches. Therefore, if the filter is set to discard, the mirroring frames are discarded.

20.2 Configuration

20.2.1 List of configuration commands

The following table describes the list of configuration commands for policy-based mirroring.

Table 20-2: List of configuration commands

Command name	Description
destination session	Specifies a mirror port for policy-based mirroring.
destination-interface-list	Sets the destination interface list for policy-based mirroring.
flow detection mode#1	Specifies the receiving-side flow detection mode.
ip access-group#2	Applies an IPv4 packet filter that detects frames subject to policy-based mirroring to the interface.
ip access-list extended#2	Sets an access list that detects frames subject to policy-based mirroring with an IPv4 packet filter.
ipv6 access-list#2	Sets an access list that detects frames subject to policy-based mirroring with an IPv6 filter.
ipv6 traffic-filter#2	Applies an IPv6 filter that detects frames subject to policy-based mirroring to the interface.
mac access-group#2	Applies a MAC filter that detects frames subject to policy-based mirroring to the interface.
mac access-list extended#2	Sets an access list that detects frames subject to policy-based mirroring with a MAC filter.
permit#2	In the access list, specifies the flow detection conditions under which the target packets are detected and the destination interface list to which the target frames are mirrored.

#1

See "Configuration Command Reference Vol. 1, 24 Flow Detection Modes/Flow Performance".

#2

See "Configuration Command Reference Vol. 1, 25 Access Lists".

20.2.2 Configuring policy-based mirroring

Use an access list to specify the target frames for policy-based mirroring and the destination interface list to which the target frames are to be mirrored. Set the destination interface in the destination interface list.

When policy-based mirroring is used, set the flow detection mode on the receiving side to the mode that supports policy-based mirroring.

(1) Configuring 1 monitor port to 1 mirror port

An example of behavior with 1 monitor port to 1 mirror port is shown below. In this example, the analyzer is connected to Ethernet interface 1/0/10.

Points to note

Set the destination interface list for the mirror port. For the monitor port, set the access list with the destination interface list specified as "behavior" as policy-based mirroring.

Command examples

1. ```
   (config)# destination-interface-list MIRROR-LIST-A mode mirror
   (config-dest-mirror)# destination session 1 interface gigabitethernet 1/0/10
   (config-dest-mirror)# exit
   ```

   Set Ethernet interface 1/0/10 as a mirror port in the destination interface list (MIRROR-LIST-A).

2. ```
   (config)# mac access-list extended MIRROR-A
   (config-ext-macl)# permit any any vlan 100 action policy-mirror-list MIRROR-LIST-A
   (config-ext-macl)# exit
   ```

   Create a MAC access list (MIRROR-A) and set the destination interface list (MIRROR-LIST-A) for VLAN 100 packets.

3. ```
   (config)# interface gigabitethernet 1/0/1
   (config-if)# mac access-group MIRROR-A in-mirror
   (config-if)# exit
   ```

   Apply the MAC access list (MIRROR-A) to the receiving side of Ethernet interface 1/0/1 as policy-based mirroring.

(2) Configuring multiple monitor ports to multiple mirror ports

An example of behavior with multiple monitor ports to multiple mirror ports is shown below. In this example, the analyzer is connected to Ethernet interface 1/0/10 and 1/0/11.

Points to note

Set multiple mirror ports for the destination interface list. Set the access list with the destination interface list specified as "behavior" as policy-based mirroring for multiple monitor ports.

Command examples

1. ```
   (config)# destination-interface-list MIRROR-LIST-B mode mirror
   (config-dest-mirror)# destination session 1 interface gigabitethernet 1/0/10
   (config-dest-mirror)# destination session 2 interface gigabitethernet 1/0/11
   (config-dest-mirror)# exit
   ```

   Set Ethernet interface 1/0/10 and 1/0/11 as a mirror port in the destination interface list (MIRROR-LIST-B).

2. ```
   (config)# ip access-list extended MIRROR-B
   (config-ext-nacl)# permit udp any any action policy-mirror-list MIRROR-LIST-B
   (config-ext-nacl)# exit
   ```

   Create an IPv4 access list (IPv4-MIRROR-B) and set the destination interface list (MIRROR-LIST-B) for IPv4 packets.

3. ```
   (config)# interface gigabitethernet 1/0/1
   (config-if)# ip access-group MIRROR-B in-mirror
   ```

```
(config-if)# exit
(config)# interface gigabitethernet 1/0/2
(config-if)# ip access-group MIRROR-B in-mirror
(config-if)# exit
(config)# interface gigabitethernet 1/0/3
(config-if)# ip access-group MIRROR-B in-mirror
(config-if)# exit
```

Apply IPv4 access list (IPv4-MIRROR-B) to the receiving side of Ethernet interfaces 1/0/1, 1/0/2, and 1/0/3 as policy-based mirroring.

20.3 Operation

20.3.1 List of operation commands

The following table describes the list of operation commands for policy-based mirroring.

Table 20-3: List of operation commands

Command name	Description
show access-filter#	Displays the settings and statistics of an access list where the destination interface list of the policy-based mirroring is specified as "behavior".
clear access-filter#	Clears the statistics of an access list where the destination interface list of the policy-based mirroring is specified as "behavior".

#

See "Operation Command Reference Vol. 1, 29 Filters".

20.3.2 Checking policy-based mirroring

You can use the "show access-filter" command to check the access list where the destination interface list of the policy-based mirroring is specified as "behavior".

Figure 20-2: Results of executing the show access-filter command

```
> show access-filter
Date 20XX/06/09 13:58:27 UTC
Using Port:1/0/1 in-mirror
Extended IP access-list:ipv4-MIRROR-A
      permit tcp(6) 25.11.2.0 0.0.0.255 any range 100 200 action policy-mirror-list dst-list-ipv4
         matched packets       :     94286
      permit tcp(6) any any
         matched packets       :     52207
>
```

Make sure that "Extended IP access-list" and the access list name (ipv4-MIRROR-A) appear in the filter for the specified interface. Also confirm that "action policy-mirror-list" and the destination interface list name (dst-list-ipv4) are displayed in the access list and that "matched packets" are being counted.

21 sFlow Statistics (Flow Statistics) Function

This chapter describes the sFlow statistics function, which analyzes the traffic characteristics of packets forwarded by the Switch, and its use.

21.1 Description

21.1.1 sFlow statistics overview

sFlow statistics is a function that uses a relay device (such as a router or a switch) to monitor traffic across networks to analyze end-to-end traffic (flow) characteristics or the traffic characteristics of the neighboring networks. sFlow is a publicly available flow statistics protocol (RFC 3176) that supports statistics on Layer 2 to Layer 7. A device that receives and displays sFlow statistics (referred to hereafter as sFlow packets) is called an sFlow collector (referred to hereafter as collector). A device that sends sFlow packets to collectors is called an sFlow agent (referred to hereafter as agent). The following figure shows an example of a network configuration that uses sFlow statistics.

Figure 21-1: Example of a network configuration using sFlow statistics

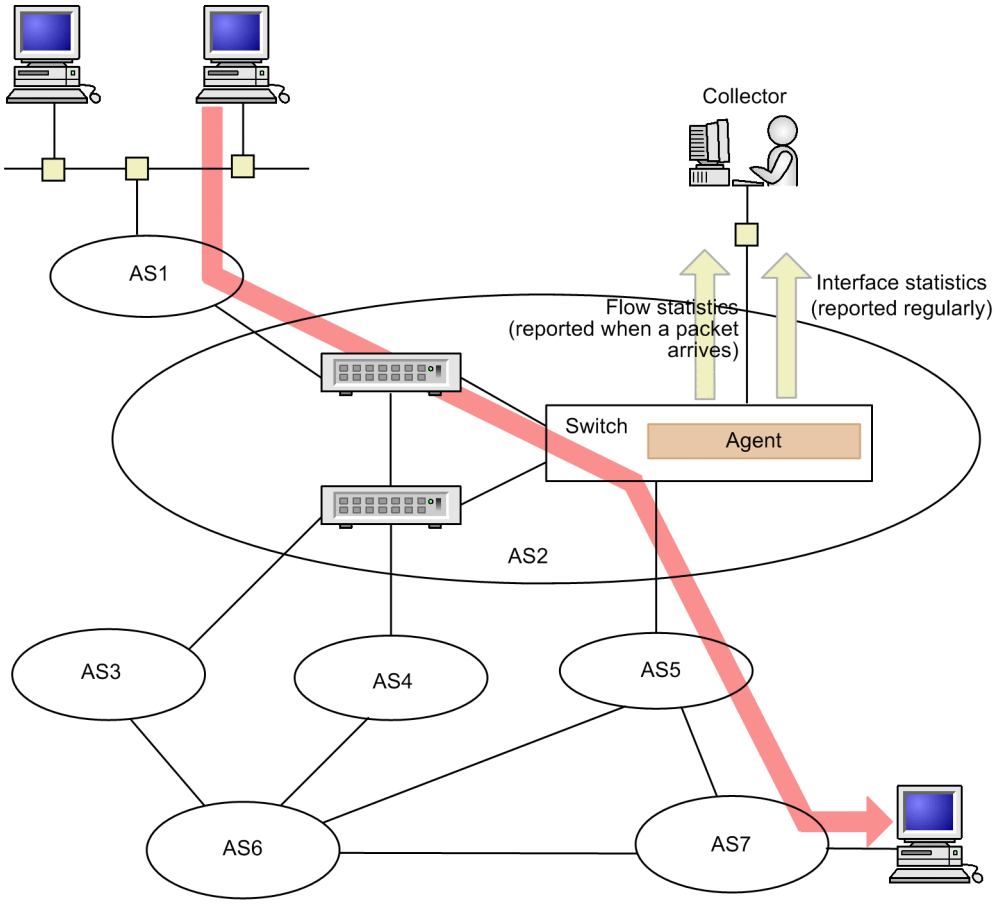
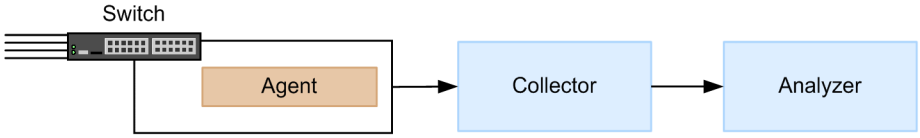


Figure 21-2: System configuration



Information monitored by an agent on the Switch is collected by a collector, and the statistical results are displayed graphically by an analyzer. Accordingly, use of the sFlow statistics function requires a collector and an analyzer.

Table 21-1: Components required for system configuration

Parameters	Role
Agent (Switch)	Collects statistics and sends them to a collector.
Collector#	Aggregates, edits, and displays statistics sent from an agent. The collector also sends edited data to an analyzer.
Analyzer	Graphically displays data sent from a collector.

#: The collector can sometimes be combined with the analyzer.

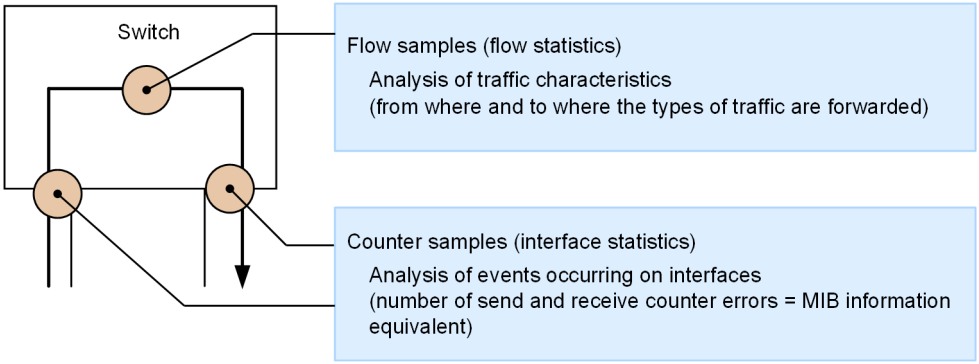
21.1.2 sFlow statistic agent function

An agent on the Switch consists of the following two types of function:

- Flow statistics (called "flow sample" in sFlow statistics. This name will be used hereafter.) Creation function
- Interface statistics (called "counter sample" in sFlow statistics. This name will be used hereafter.) Creation function

The flow sample creation function samples sent and received packets (frames) at a user-specified rate, processes the packet information, and then sends it to a collector in flow sample format. The counter sample creation function sends interface statistics to a collector in counter sample format. The following figure shows collection points and collected data for the function.

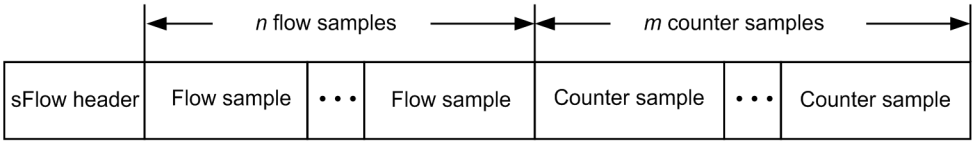
Figure 21-3: Flow sample and counter sample



21.1.3 sFlow packet format

This section describes sFlow packets (flow sample and counter sample) that the Switch sends to a collector. The format used to send the packets to a collector is defined in RFC 3176. The following figure shows the sFlow packet format.

Figure 21-4: sFlow packet format



Note that the Switch does not include the flow sample and counter sample in one sFlow packet at the same time.

(1) sFlow header

The following table describes information set in the sFlow header.

Table 21-2: sFlow header format

Configuration items	Description	Supported
Version number	sFlow packet version (Versions 2 and 4 are supported.)	Y
Address type	IP type of the agent (where 1 is IPv4, and 2 is IPv6)	Y
Agent IP address	Agent IP address	Y
Sequence number	Number incremented each time an sFlow packet is generated#	Y
Generation time	Time in milliseconds since the device started	Y
Number of samples	Number of sampled (flow and counter) packets contained in the signal.# (n+m is set in the example in "Figure 21-4: sFlow packet format")	Y

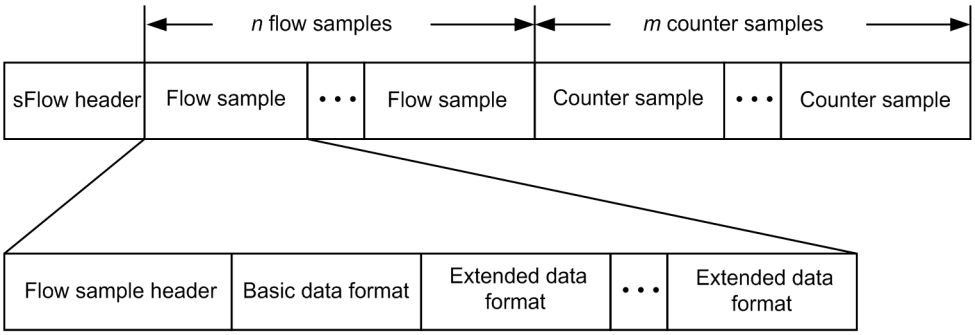
Legend: Y: Supported

#: Reset when the master switch is switched during the stack configuration.

(2) Flow sample

Flow sample is the format used to retrieve packets from among the received packets that are to be forwarded to another device or sent to the Switch at a specified sampling interval for transmission to a collector. However, the Switch does not support flow sample of packets addressed to the Switch. Because the flow sample functionality collects information about the monitored packets and information that is not contained in a packet (such as the receiving interface, sending interface, and the AS number), detailed network monitoring becomes possible. The following figure shows the flow sample format.

Figure 21-5: Flow sample format



(a) Flow sample header

The following table describes the information set in the flow sample header.

Table 21-3: Flow sample header format

Configuration items	Description	Supported
sequence_number	Number incremented each time a flow sample is generated#1	Y
source_id	The SNMP Interface Index, which indicates the source on a device from which the flow sample was created (receiving interface)	Y
sampling_rate	Sampling rate of flow samples	Y
sample_pool	Total number of packets arriving at an interface	Y
drops	Total number of discarded flow samples Fixed at 0 for the Switch	Y
input	The SNMP Interface Index of a receiving interface. If the interface is unknown, 0 is set.	Y
output	The SNMP Interface Index# of a sending interface#2 If the sending interface is unknown, 0 is set.	N

Legend: Y: Supported, N: Not supported.

#1: Reset when the master switch is switched during the stack configuration.

#2: Fixed at 0 because the Switch does not support the setting item output

(b) Basic data format

There are three basic data format types (header, IPv4, and IPv6), but only one can be set. By default, the header type is set as the basic data type. If you want to use the IPv4 type or the IPv6 type, use a configuration command to change the setting. The following tables describe the formats.

Table 21-4: Header type format

Configuration items	Description	Supported
packet_information_type	Basic data format type (header type is 1)	Y
header_protocol	Header protocol number (ETHERNET is 1)	Y
frame_length	Length of the original packet	Y
header_length	Length of a packet as sampled (default length is 128)	Y
header<>	Contents of the sampled packet	Y

Legend: Y: Supported

#: This format is used if a packet cannot be analyzed as an IP packet.

Table 21-5: IPv4 type format

Configuration items	Description	Supported#
packet_information_type	Basic data format type (IPv4 type is 2)	Y
length	Length of the IPv4 packet	Y
protocol	IP protocol type (if where 6 is TCP and 17 is UDP, for example)	Y
src_ip	Source IP address	Y

Configuration items	Description	Supported#
dst_ip	Destination IP address	Y
src_port	Source port number	Y
dst_port	Destination port number	Y
tcp_flags	TCP flag	Y
TOS	IP TOS (type of service)	Y

Legend: Y: Supported

#: If a VLAN-tagged frame with multiple tiers is the target, information is not collected in sFlow packets.

Table 21-6: IPv6 type format

Configuration items	Description	Supported#1
packet_information_type	Basic data format type (IPv6 type is 3)	Y
length	Length of the IPv6 packet excluding the lower layers	Y
protocol	IP protocol type (if where 6 is TCP and 17 is UDP, for example)	Y
src_ip	Source IP address	Y
dst_ip	Destination IP address	Y
src_port	Source port number	Y
dst_port	Destination port number	Y
tcp_flags	TCP flag	Y
priority	Priority #2	Y

Legend: Y: Supported

#1: If a VLAN-tagged frame with multiple tiers is the target, information is not collected in sFlow packets.

#2: The Switch collects traffic classes.

(c) Extended data format

There are five types of extended data formats: switch type, router type, gateway type, user type, and URL type. By default, the extended data format is configured to collect all the extended data formats and send them to a collector. This format can be changed by using the configuration file. The following tables describe the formats.

Table 21-7: List of extended data formats

Extended data type	Description	Supported
Switch type	Collects switch information (such as VLAN information).	Y
Router type	Collects router information (such as NextHop).	Y#1#2
Gateway type	Collects gateway information (such as AS the number).	Y#1#2
User type	Collects user information (such as TACACS or RADIUS information).	Y#2

Extended data type	Description	Supported
URL type	Collects URL information.	Y#2

Legend: Y: Supported
#1: Information is not collected in sFlow packets during L2 forwarding.
#2: If a VLAN-tagged frame with multiple tiers is the target, information is not collected in sFlow packets.

Table 21-8: Switch type format

Configuration items	Description	Supported
extended_information_type	Extended data format type (switch type is 1)	Y
src_vlan	802.1Q VLAN ID of a received packet	Y
src_priority	802.1p priority of a received packet	Y
dst_vlan	802.1Q VLAN ID of a sent packet	N#
dst_priority	802.1p priority of a sent packet	N#

Legend: Y: Supported, N: Not supported.
#: Fixed at 0 because the item is not supported

Table 21-9: Router type format

Configuration items	Description	Supported
extended_information_type	Extended data format type (router type is 2)	Y
nexthop_address_type	IP address type of the next forward destination	Y#
nexthop	IP address of the next forward destination router	Y#
src_mask	Prefix mask bit of the source switch address	Y
dst_mask	Prefix mask bit of the destination switch address	Y

Legend: Y: Supported
#: Fixed at 0 if the path to the destination address is one of multipaths routes.

Table 21-10: Gateway type format

Configuration items	Description	Supported
extended_information_type	Extended data format type (gateway type is 3)	Y
as	AS number of the Switch	Y
src_as	AS number of the source switch	Y#1
src_peer_as	Neighboring AS number to the source switch	Y#1#2
dst_as_path_len	Number of AS information items (fixed to 1)	Y
dst_as_type	Type of the AS path (2 is AS_SEQUENCE)	Y
dst_as_len	Number of ASs (fixed to 2)	Y

Configuration items	Description	Supported
dst_peer_as	Neighboring AS number to the destination	Y#1
dst_as	AS number of the destination	Y#1
communities<>	Community for the route#3	N
localpref	Local preference about this route#3	N

Legend: Y: Supported, N: Not supported.

#1: If the path to the sending and receiving destination is a direct route, the AS number is recorded as 0.

#2: The neighboring AS number if the sending destination was retrieved from the Switch. This number might be different from the neighboring AS number to which the information was actually forwarded.

#3: Fixed at 0 because the item is not supported

Table 21-11: User type format

Configuration items	Description	Supported
extended_information_type	Extended data format type (user type is 4)	Y
src_user_len	Length of the user name of the source	Y
src_user<>	User name of the source	Y
dst_user_len	Length of the user name of the destination#	N
dst_user<>	User name of the destination#	N

Legend: Y: Supported, N: Not supported.

#: Fixed at 0 because the item is not supported

Table 21-12: URL type format

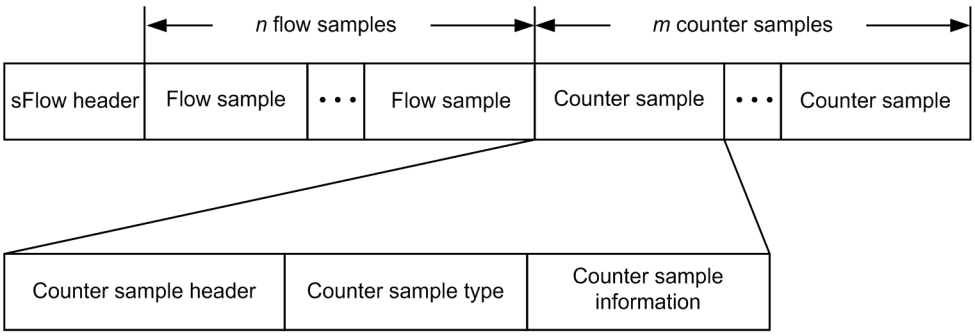
Configuration items	Description	Supported
extended_information_type	Extended data format type (URL type is 5)	Y
url_direction	URL information source (The source address is 1, and the destination address is 2.) Fixed at 2 for the Switch	Y
url_len	URL length	Y
url<>	Contents of the URL	Y

Legend: Y: Supported

(3) Counter sample

A counter sample sends interface statistics (number of arrived packets and number of errors). Also, the format to be sent to a collector is determined according to the interface type. The following figure shows the counter sample format.

Figure 21-6: Counter sample format



(a) Counter sample header

The following table describes the information set in the counter sample header.

Table 21-13: Counter sample header format

Configuration items	Description	Supported
sequence_number	Number incremented each time a counter sample is generated#	Y
source_id	The SNMP Interface Index, which indicates the source (specific port) on a device for the counter sample	Y
sampling_interval	Sending interval at which counter samples are sent to a collector	Y

Legend: Y: Supported

#: Reset when the master switch is switched during the stack configuration.

(b) Counter sample type

The counter sample types reflect interface types and are collected according to this classification. The following table describes the items set for counter sample type.

Table 21-14: List of counter sample types

Configuration items	Description	Supported
GENERIC	General statistics (counters_type is set to 1)	N#1
ETHERNET	Ethernet statistics (counters_type is set to 2)	Y
TOKENRING	Token ring statistics (counters_type is set to 3)	N#1
FDDI	FDDI statistics (counters_type is set to 4)	N#1
100BaseVG	VG statistics (counters_type is set to 5)	N#1
WAN	WAN statistics (counters_type is set to 6)	N#1
VLAN	VLAN statistics (counters_type is set to 7)	N#2

Legend: Y: Supported, N: Not supported.

#1: This interface type is not supported by the Switch.

#2: The Switch does not support VLAN statistics.

(c) Counter sample information

Counter sample information to be collected varies according to the counter sample type. Except for VLAN statistics, information is sent according to the statistics (RFC) used by MIBs. The following table describes items set as counter sample information.

Table 21-15: Counter sample information

Configuration items	Description	Supported
GENERIC	General statistics (see RFC 2233)	N
ETHERNET	Ethernet statistics (see RFC 2358)	Y#
TOKENRING	Token ring statistics (see RFC 1748)	N
FDDI	FDDI statistics (see RFC 1512)	N
100BaseVG	VG statistics (see RFC 2020)	N
WAN	WAN statistics (see RFC 2233)	N
VLAN	VLAN statistics (see RFC 3176)	N

Legend: Y: Supported, N: Not supported.
#: Among the Ethernet statistics, ifDirection and dot3StatsSymbolErrors cannot be collected.

21.1.4 Behavior of sFlow statistics on a Switch

(1) Target ports for sFlow statistics collection

The Switch targets all Ethernet interfaces except the management port and stack port (in stack configuration) for sFlow statistics sampling. You can also select either receiving (ingress) or sending (egress) as the sampling attribute per device.

(2) Target packets for flow sample

The Switch targets packets relayed by hardware for flow sample.

Neither receiving nor sending of the following packets is treated as the target of flow sample.

- Software-forwarded packets
- Packets originating from the device
- Packets addressed to the device

Depending on the sampling attribute, the following packets are not treated as sampling targets.

Packets that are not treated as sampling targets in the receiving specification

- Packets discarded by the Ethernet interface

Packets that are not treated as sampling targets in sending specification

- Packets sent from the mirror port of port mirroring and policy-based mirroring

(3) Flow sample behavior for discarded packets

The flow sample of the Switch may send sFlow packets to the collector as if they were relayed even if the packets are discarded by the Switch. Check the conditions under which packets are discarded by other functions before starting operation. The following table shows the flow sample behavior of packets discarded by other functions.

Table 21-16: Flow sample of packets discarded by other functions

Discard function	Receiving specification	Sending specification	
		Switches with the same receiving and sending ports	Switches with different receiving and sending ports in a stack configuration
Filter (receiving side)	Collect	Do not collect	Do not collect
QoS (Bandwidth monitoring)	Collect	Do not collect	Do not collect
Filter (sending side)	Collect	Collect	Collect
QoS (drop control)	Collect	Collect	Collect
Policy-based routing	Collect	Do not collect	Do not collect
Storm control	Do not collect	Do not collect	Do not collect
Inter-port forwarding block	Collect	Do not collect	Do not collect
Layer 2 function#1	Collect	Do not collect	Do not collect
Layer 3 function#2	Collect	Do not collect	Do not collect

#1

Frames discarded by Layer 2 include: At this time, if an untagged packet is received on a trunk port without a native VLAN, the reception VLAN ID in the switch type information will be 4095.

- Discarded by the MAC address learning function
- Discarded without being able to relay by VLAN
- Discarded due to blocking by Layer 2 protocol
- Discarded by the Layer 2 authentication
- Discarded by IGMP snooping, MLD snooping, and DHCP snooping
- Discarded when Layer 2 protocol is invalid

#2

The discarded packets by Layer 3 include the following.

- Error packets discarded by IP layer
- Packets discarded by routing protocol

(4) Notes on flow sample contents based on the sampling position

In principle, the flow sample of the Switch collects the contents of an sFlow packet when it enters a Switch regardless of whether sampling is performed with receiving or sending specified. (The contents are not reflected in sFlow packets even after conversion on the Switch.)

The same applies when packets discarded by the Switch are subject to flow sample. However, when sampling a packet that is relayed (sent from a switch port different from the receiving port) over multiple member

switches in a stack configuration with sending specified, the contents of the packet at the time it is sent from the Switch may be collected by other combined function or due to the relay conditions. The following table shows the contents of flow sampling by relay pattern.

Table 21-17: Flow sampling contents by relay pattern

Sampling attribute	Standalone configuration	Stack configuration	
		Packets relayed within the same switch	Packets relayed across multiple member switches
Receiving specification	Contents when received	Contents when received	Contents when received
Sending specification	Contents when received	Contents when received	Contents when received or sent

(5) Notes on flow sample contents when used in combination with other functions

Flow sample flow sample collected by the Switch differs depending on the function used in combination with the sampling target port and the relay conditions of the sampling packets. The following table shows the contents of flow sample collection when used in combination with other functions and according to relay conditions.

Table 21-18: Contents of flow sample collection when used in combination with other functions and according to relay conditions

Combined function and relay conditions	Receiving specification	Sending specification	
		Switches with the same receiving and sending ports	Switches with different receiving and sending ports in a stack configuration
VLAN tunneling (Tunneling port reception)	Information before adding the tag for tunneling		Information after adding the tag for tunneling[#1]
VLAN tunneling (Tunneling port sending)	Information before deleting the tag for tunneling[#2]		
VLAN tag translation (Tag translation port receiving)	Tag information before translation		Tag information after translation[#3]
QoS marking (DSCP rewrite)	DSCP value before rewriting[#4]		DSCP value after rewriting[#4]
QoS marking (User priority rewriting)	User priority before rewriting[#5]		User priority after rewriting[#5]
Layer 3 unicast forwarding	Information when receiving		Information when sending[#6]
Policy-based routing	Information when receiving[#7]		Information when sending[#6]

#1

When collecting switch type information, the tags for tunneling are collected as source VLAN information. Also, if the VLAN tag becomes two or more rows as a result of adding a tag for tunneling, IPv4 type, IPv6 type, user type, and URL type information will not be collected.

#2

IPv4 type, IPv6 type, user type, and URL type information will not be collected if the VLAN tag has two or more rows.

#3

When collecting switch type information, the tags after the tag translation are collected as source VLAN information.

#4

Header type frame information, IPv4 type TOS information, IPv6 type priority information.

#5

Header-type frame information, VLAN information for switch type received packets.

#6

Header type and switch type information are collected at the time of sending. Information on router type and gateway type is not collected.

#7

The following information is the routing information of the forwarding destination according to the routing protocol, instead of the routing information of the forwarding destination based on the policy-based routing.

- nexthop and dst_mask of router type formats
- dst_peer_as and dst_as of gateway type formats

(6) Target packets for counter sample collection

Counter sample on the Switch counts all sent/received packets of the target port regardless of whether sending or receiving is specified.

21.1.5 Notes on using sFlow statistics

(1) In a stack configuration

In a stack configuration, set the "sflow source" configuration command. Or, set an IP address on the loopback interface of the global network.

21.2 Configuration

21.2.1 List of configuration commands

The following table describes the configuration commands for sFlow statistics.

Table 21-19: List of configuration commands

Command name	Description
sflow destination	Specifies the IP address of the collector, which is the destination for sFlow packets.
sflow extended-information-type	Sets whether to send flow samples in an extended data format.
sflow forward egress	Causes the send traffic of the specified port to be monitored by the sFlow statistics.
sflow forward ingress	Causes the received traffic of the specified port to be monitored by the sFlow statistics.
sflow max-header-size	Sets the maximum size from the beginning of the sample packet to be copied if the header type is used for the basic data format (see the "sflow packet-information-type" command).
sflow max-packet-size	Sets the sFlow packet size.
sflow packet-information-type	Sets the basic data format of the flow sample.
sflow polling-interval	Specifies the interval for sending counter samples to the collector.
sflow sample	Sets the sampling interval applying to the entire switch.
sflow source	Specifies the IP address to be configured as the sFlow packet source (agent).
sflow url-port-add	Sets the port number used for HTTP packets to a port number other than 80 when URL information is used in the extended data format.
sflow version	Sets the version of the sFlow packet to be sent.

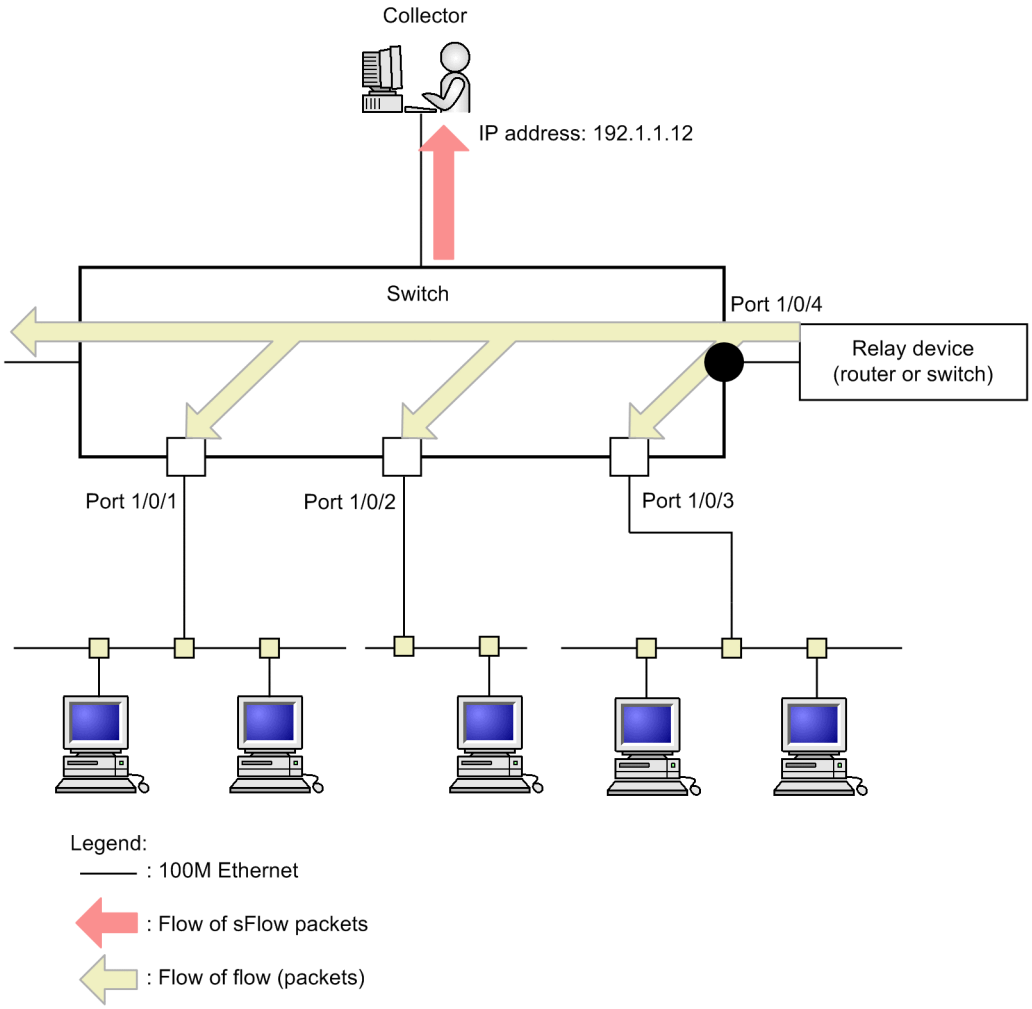
21.2.2 Configuring basic settings for the sFlow statistics function

(1) Configuration for monitoring received packets

Points to note

Two separate configurations are required: one configuration is enabled for the entire device, and the other configuration is used to specify a port that is actually used. This subsection describes the configuration for monitoring incoming packets on port 1/0/4.

Figure 21-7: Example configuration for monitoring received packets on port 1/0/4



Command examples

1. `(config)# sflow destination 192.1.1.12`
   Sets the IP address 192.1.1.12 for the collector.
2. `(config)# sflow sample 512`
   Monitors the traffic every 512 packets.
3. `(config)# interface gigabitethernet 1/0/4`
   Switches to the Ethernet interface configuration mode for port 1/0/4.
4. `(config-if)# sflow forward ingress`
   Enables the sFlow statistics function for packets received on port 1/0/4.

Notes

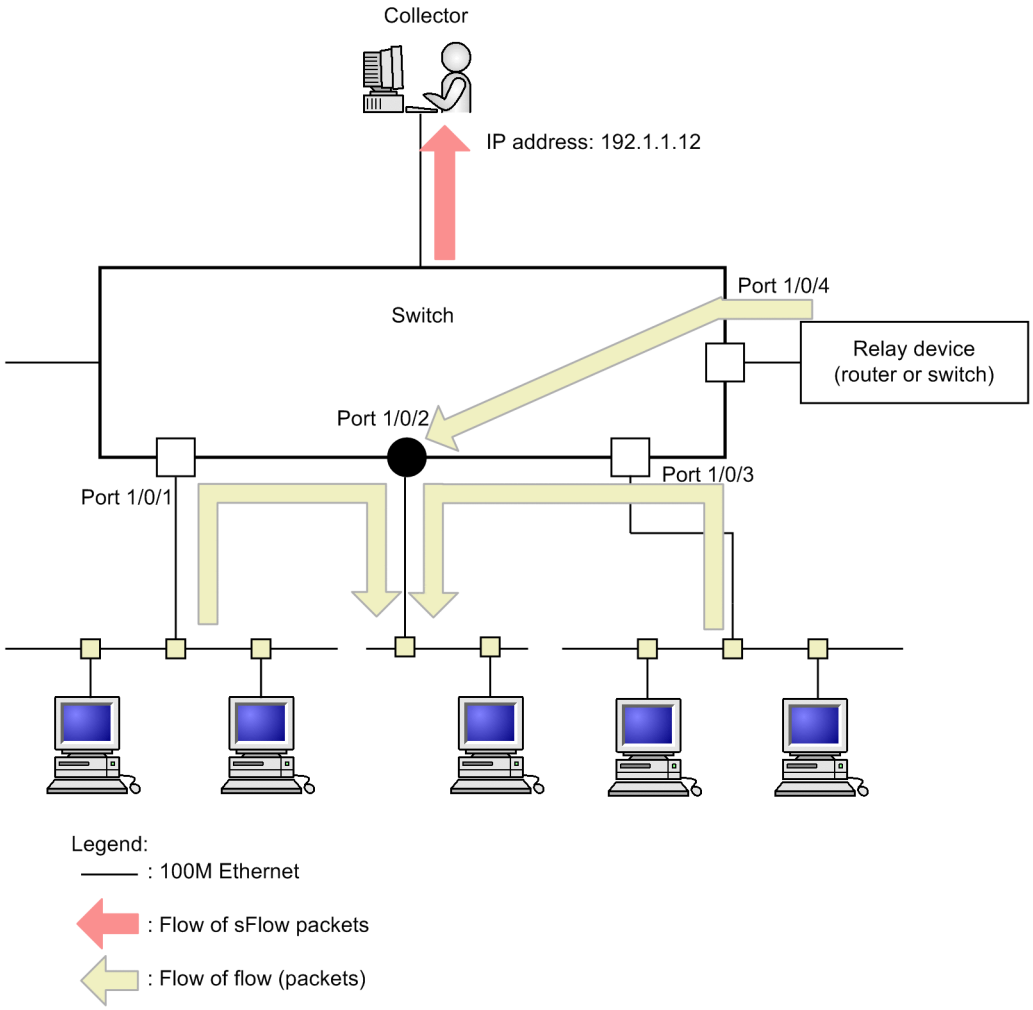
The sampling interval that can be specified by the "sflow sample" command must be determined after taking into consideration the line speed of the interface. For details, see the sflow sample section of the Configuration Command Reference Vol. 1.

(2) Configuration for monitoring sent packets

Points to note

Enabling the sFlow statistics function for received packets or sent packets is determined by the command specified when performing configuration in the interface configuration mode ("sflow forward ingress" or "sflow forward egress" command). This subsection describes the configuration for monitoring outgoing packets on port 1/0/2.

Figure 21-8: Example configuration for monitoring sent packet on port 1/0/2



Command examples

1. `(config)# sflow destination 192.1.1.12`
   Sets the IP address 192.1.1.12 for the collector.
2. `(config)# sflow sample 512`
   Monitors the traffic every 512 packets.
3. `(config)# interface gigabitethernet 1/0/2`
   Switches to the Ethernet interface configuration mode for port 1/0/2.
4. `(config-if)# sflow forward egress`
   Enables the sFlow statistics function for sent packets on port 1/0/2.

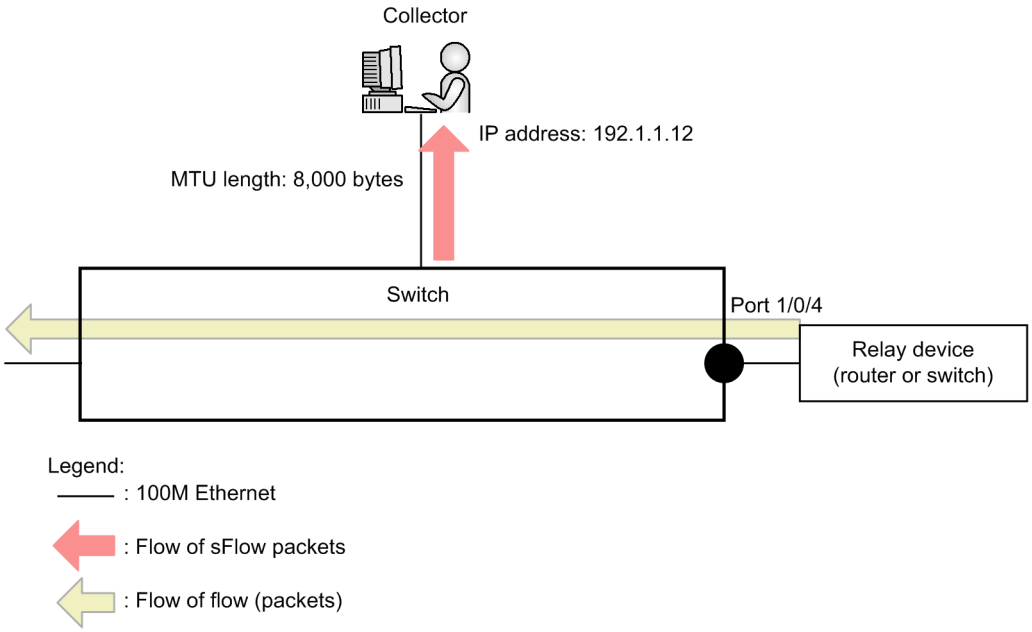
21.2.3 Configuring sFlow statistics parameter

(1) Adjusting the MTU length and the sFlow packet size

Points to note

By default, sFlow packets with a maximum of 1400 bytes are sent to a collector. If the MTU value of the line to the collector is large, adjust the packet size to the same size as the MTU value so that packets can be sent efficiently to the collector. This subsection describes the setting when a line with an MTU length of 8000 bytes is connected to a collector.

Figure 21-9: Example when the MTU value of the line to the collector is set to 8000 bytes



Command examples

1. `(config)# sflow destination 192.1.1.12`
   Sets the IP address 192.1.1.12 for the collector.
2. `(config)# sflow sample 512`
   Monitors the traffic every 512 packets.
3. `(config)# sflow max-packet-size 8000`
   Sets the maximum sFlow packet size to 8000 bytes.
4. `(config)# interface gigabitethernet 1/0/4`
   Switches to the Ethernet interface configuration mode for port 1/0/4.
5. `(config-if)# sflow forward ingress`
   Enables the sFlow statistics function for packets received on port 1/0/4.

(2) Narrowing down the information to be collected

Points to note

All information about sFlow packets is collected by the default configuration. If you want to decrease CPU usage, you can change the configuration settings so that unnecessary information will not be collected. This subsection describes the configuration when only IP address information is needed.

Command examples

1. `(config)# sflow destination 192.1.1.12`
   Sets the IP address 192.1.1.12 for the collector.
2. `(config)# sflow sample 512`
   Monitors the traffic every 512 packets.
3. `(config)# sflow packet-information-type ip`
   Sets the IP format as the basic data format for flow samples.
4. `(config)# sflow extended-information-type router`
   Sets "router" as the extended data format for flow samples (only router information can be retrieved).
5. `(config)# interface gigabitethernet 1/0/4`
   Switches to the Ethernet interface configuration mode for port 1/0/4.
6. `(config-if)# sflow forward ingress`
   Enables the sFlow statistics function for packets received on port 1/0/4.

(3) Fixing the agent IP address of sFlow packets

Points to note

A normal collector determines if a switch is the same device based on the agent IP address contained in an sFlow packet. Therefore, if the agent IP address is not set by using the "sflow source" or "interface loopback" command, the collector might display the status as if packets had been sent from multiple devices. To see long-term information, fix the agent IP address. This subsection describes configuration for sending packets to a collector by using the IP address assigned to loopback as the agent IP address.

Command examples

1. `(config)# interface loopback 0`
   Switches to the loopback interface configuration mode.
2. `(config-if)# ip address 176.1.1.11`
   Configures the loopback interface as 176.1.1.11 for IPv4.
3. `(config-if)# ipv6 address 3ffe:100::1`
   `(config-if)# exit`
   Configures the loopback interface as 3ffe:100::1 for IPv6.
4. `(config)# sflow destination 192.1.1.12`
   Sets the IP address 192.1.1.12 for the collector.
5. `(config)# sflow sample 512`
   Monitors the traffic every 512 packets.
6. `(config)# interface gigabitethernet 1/0/4`
   Switches to the Ethernet interface configuration mode for port 1/0/4.
7. `(config-if)# sflow forward ingress`
   Enables the sFlow statistics function for packets received on port 1/0/4.

Notes

When the loopback IP address is used, configuration using the "sflow source" command is not needed. If the IP address is specified by using the "sflow source" command, then the specified IP address takes priority.

(4) Collecting URL information in a local network environment

Points to note

When URL information (HTTP packets) is collected by using the sFlow statistics function on the Switch, the default destination port number is set to 80. However, in a local network, the port number might be different. The following describes configuration when port 8080 is used for HTTP packets in a local network environment.

Command examples

1. `(config)# sflow destination 192.1.1.12`
   Sets the IP address 192.1.1.12 for the collector.
2. `(config)# sflow sample 512`
   Monitors the traffic every 512 packets.
3. `(config)# sflow url-port-add 8080`
   When URL information is used in the extended data format, configure an additional destination port number 8080 for packets that are determined to be HTTP packets.
4. `(config)# interface gigabitethernet 1/0/4`
   Switches to the Ethernet interface configuration mode for port 1/0/4.
5. `(config-if)# sflow forward ingress`
   Enables the sFlow statistics function for packets received on port 1/0/4.

Notes

Even after this parameter has been configured, destination port number 80 is valid for HTTP packets.

21.3 Operation

21.3.1 List of operation commands

The following table describes the operation commands used for the sFlow statistics function.

Table 21-20: List of operation commands

Command name	Description
show sflow	Shows the configuration conditions and running status of the sFlow statistics function.
clear sflow statistics	Clears statistics managed by sFlow statistics.
restart sflow	Restarts the flow statistics program.
dump sflow	Outputs a file containing debug information collected by the flow statistics program.

21.3.2 Checking communication with collectors

When you configure the sFlow statistics function to send packets to a collector on the Switch, verify the following.

(1) Connection with the collector

Execute the "ping" command with the IP address of the collector specified to make sure that the IP communication from the Switch to the collector is possible. If the communication is not possible, see the "Troubleshooting Guide".

(2) sFlow packet communication

On the collector side, make sure that sFlow packets are received.

For the action to be taken if packets are not being received, see the "Troubleshooting Guide".

21.3.3 Checking the sFlow statistics during operation

When you use the sFlow statistics function on the Switch, you must check the following during operation.

(1) Number of discarded sFlow packets

Execute the "show sflow" command to display the sFlow statistics, and then use the sFlow statistics function to check the Dropped sFlow samples section (number of discarded packets) or the Overflow Time of sFlow Queue section (time that packets were discarded). If either value has increased, adjust the sampling interval so that they do not increase.

Figure 21-10: Results of executing the show sflow command

```
> show sflow
Date 20XX/12/13 14:10:32 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  16:00:05
sFlow agent data :
  sFlow service version : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate    : 1 per 2048 packets
  Configured sFlow ingress ports :  1/0/2-4
  Configured sFlow egress ports  :  ----
  Received sFlow samples : 37269  Dropped sFlow samples         :    2093
  Exported sFlow samples : 37269  Couldn't export sFlow samples :       0
  Overflow time of sFlow queue: 12 seconds                                  …1
sFlow collector data :
  Collector IP address: 192.168.4.199  UDP:6343  Source IP address: 130.130.130.1
```

```
  Send FlowSample UDP packets   : 12077  Send failed packets:     0
  Send CounterSample UDP packets:   621  Send failed packets:     0
  Collector IP address: 192.168.4.203  UDP:65535  Source IP address: 130.130.130.1
  Send FlowSample UDP packets   : 12077  Send failed packets:     0
  Send CounterSample UDP packets:   621  Send failed packets:     0
```

1. If the time for discarding packets increases, review the sampling interval settings.

(2) CPU usage rate

Execute the "show cpu" command to display the CPU usage rate and verify the load. If the CPU usage rate is high, use the "sflow sample" configuration command to reset the sampling interval.

Figure 21-11: Results of executing the show cpu command

```
>show cpu minutes
Date 20XX/12/13 14:15:37 UTC
*** minute ***
date    time              cpu average
Dec 13  14:42:00-14:42:59     6
Dec 13  14:43:00-14:43:59    20
                  :
                  :
Dec 13  15:41:00-15:41:59    10             …1
```

1. If the CPU usage ratio becomes high, review the sampling interval settings.

21.3.4 Adjusting the sampling interval for sFlow statistics

When the sFlow statistics function is used on the Switch, the sampling interval can be adjusted as explained below.

(1) Adjusting the line speed

When the rate of traffic (pps) of all ports on which the sFlow statistics function is enabled is checked by using the "show interfaces" command and received packets are to be collected as statistics, add the value of "Input rate". If sent packets are to be collected, add the value of "Output rate" as well. The value calculated by dividing the total value by 100 gives a sampling interval. Set the sampling interval using this value, and then use the "show sflow" command to make sure that the number of packets to be discarded does not increase.

The following example shows a sampling interval that can be used as a guideline for retrieving receive packets on ports 1/0/4 and 1/0/5.

Figure 21-12: Results of executing the show interfaces command

```
> show interfaces gigabitethernet 1/0/4
Date 20XX/12/24 17:18:54 UTC
NIF0:
Port4: active up  100BASE-TX full(auto)    0012.e220.ec30
        Time-since-last-status-change:1:47:47
        Bandwidth:10000kbps  Average out:0Mbps  Average in:5Mbps
        Peak out:5Mbps at 15:44:36  Peak in:5Mbps at 15:44:18
        Output rate:       0.0bps         0.0pps
        Input  rate:    4063.5kbps       10.3kpps
        Flow control send   :off
        Flow control receive:off
        TPID:8100
                              :

> show interfaces gigabitethernet 1/0/5
Date 20XX/12/24 17:19:34 UTC
NIF0:
Port5: active up  100BASE-TX full(auto)    0012.e220.ec31
        Time-since-last-status-change:1:47:47
        Bandwidth:10000kbps  Average out:5Mbps  Average in:5Mbps
        Peak out:5Mbps at 15:44:36  Peak in:5Mbps at 15:44:18
        Output rate:    4893.5kbps       16.8kpps
        Input  rate:    4893.5kbps       16.8kpps
        Flow control send   :off
        Flow control receive:off
```

```
        TPID:8100
                                :
```

Sampling interval to be used as a guideline

= Total PPS value of the ports on which the sFlow statistics function is enabled / 100

= (10.3 kpps + 16.8 kpps)/100

= 271#

#: When the sampling interval is set to 271, the behavior is actually performed with the sampling interval set to 512. For details about the sampling interval, see the description of the "sflow sample" configuration command.

(2) Making adjustments from the detailed information

Sets the value for Sampling rate to collector (recommended sampling interval in which no packets are discarded) displayed by executing the "show sflow detail" command as the sampling interval. Next, execute the "clear sflow statistics" command to check the behavior for a while. If, after this time, the Sampling rate to collector value is still larger than the setting, use the same procedure to adjust the sampling interval again.

Figure 21-13: Results of executing the show sflow detail command

```
> show sflow detail
Date 20XX/12/21 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  8:00:05
                              :
   Collector IP address: 192.168.4.203  UDP:65535  Source IP address: 130.130.130.1
   Send FlowSample UDP packets     : 12077  Send failed packets:     0
   Send CounterSample UDP packets:     621  Send failed packets:     0
Detail data :
   Max packet size: 1400 bytes
   Packet information type: header
   Max header size: 128 bytes
   Extended information type: switch,router,gateway,user,url
   Url port number: 80,8080
   Sampling mode: random-number
   Sampling rate to collector: 1 per 2163 packets
   Target ports for CounterSample: 1/0/2-4
```

22 IEEE 802.3ah/UDLD

The IEEE 802.3ah/UDLD function detects unidirectional link failures to prevent related network failures.

This chapter describes the IEEE 802.3ah/UDLD function and its use.

22.1 Description

22.1.1 Overview

UDLD (Uni-Directinal Link Detection) function detects unidirectional link failures.

When a unidirectional link failure occurs, one device is able to send data but cannot receive data, while the other device is able to receive data but cannot send data. Furthermore, a malfunction occurs in an upper layer protocol, and various other failures occur throughout the network. Some of the known failures are loops in Spanning Tree Protocols 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 reachability at a remote device to monitor the bidirectional link status. The Switch uses the IEEE 802.3ah/OAM function to monitor the bidirectional link status. If the status cannot be checked in this case, UDLD function is used to detect unidirectional link failures. The UDLD function of this Switch determines that the Switch is in a loop configuration when it not only detects unidirectional link failures, but also when the Switch receives a control frame sent by itself and deactivates the port that received the frame.

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 function, all ports run in passive mode.

Unidirectional link failures are detected by executing the "efmoam active udld" configuration command to configure the ports of both devices connected by an Ethernet cable. If a unidirectional link failure is detected on one of the ports configured with the "efmoam active udld" command, the port is deactivated and a link-down is detected on the port of the partner device. As a result, operations on the two ports of the connected devices are stopped.

22.1.2 Supported specifications

IEEE 802.3ah/UDLD functionality supports IEEE 802.3ah/OAM function as described in the following table.

Table 22-1: 802.3ah OAMPDUs supported by IEEE 802.3ah/UDLD function

Name	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
Loopback Control	Controls the loopback status of a remote device.	N
Organization Specific	Used for function expansion	N

Legend Y: Supported; N: Not supported

22.1.3 Notes on using IEEE 802.3ah/UDLD

(1) When a device that does not support IEEE 802.3ah/OAM function is connected between devices configured with IEEE 802.3ah/UDLD function

Because a standard switch does not forward control frames used by IEEE 802.3ah/OAM function, information cannot be transmitted between devices, and a unidirectional link failure is detected on a port configured with the "efmoam active udld" configuration command. Accordingly, IEEE 802.3ah/UDLD function cannot be used.

(2) When a media converter or other relay device is connected between devices configured with IEEE 802.3ah/UDLD function

If a media converter that does not automatically disconnect the link when the other link is disconnected is installed between devices, recognition of the link status varies between the devices. Accordingly, a unidirectional link failure is detected even if the remote device is not running on a port configured with the "efmoam active udld" command. When you attempt recovery from a failure, you must synchronize both devices, 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 function of another manufacturer's switch

The IEEE 802.3ah/UDLD function of the Switch and the UDLD functionality of other manufacturers' switches cannot be connected because UDLD functionality specifications differ by manufacturer.

22.2 Configuration

22.2.1 List of configuration commands

The following table describes the list of configuration commands for IEEE 802.3ah/UDLD.

Table 22-2: List of configuration commands

Command name	Description
efmoam active	Activates IEEE 802.3ah/OAM function on a physical port.
efmoam disable	Disables IEEE 802.3ah/OAM function.
efmoam udld-detection-count	Specifies the counter value for determining a unidirectional link failure.

22.2.2 Configuring IEEE 802.3ah/UDLD

(1) Configuring IEEE 802.3ah/UDLD function

Points to note

To use IEEE 802.3ah/UDLD functionality, you must first enable IEEE 802.3ah/OAM function for the entire device. As the factory default setting, IEEE 802.3ah/OAM function 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 function.

In this subsection, IEEE 802.3ah/UDLD function is used for gigabitethernet 1/0/1.

Command examples

1. `(config)# interface gigabitethernet 1/0/1`

   Switches to the Ethernet interface configuration mode for port 1/0/1.

2. `(config-if)# efmoam active udld`

   Sets active mode for the IEEE 802.3ah/OAM function port 1/0/1 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 unidirectional 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.

22.3 Operation

22.3.1 List of operation commands

The following table describes the list of operation commands for IEEE 802.3ah/UDLD.

Table 22-3: List of operation commands

Command name	Description
show efmoam	Shows the IEEE 802.3ah/OAM configuration information and port setting information.
show efmoam statistics	Shows statistics regarding IEEE 802.3ah/OAM.
clear efmoam statistics	Clears statistics regarding IEEE 802.3ah/OAM.
restart efmoam	Restarts the IEEE 802.3ah/OAM program.
dump protocols efmoam	Outputs detailed event trace information and control table information obtained by the IEEE 802.3ah/OAM program to a file.

22.3.2 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 detail" command displays information about the ports in passive mode that recognize the remote device in addition to the active-mode ports. The "show efmoam statistics" command displays the status of failures detected by the IEEE 802.3ah/UDLD function in addition to IEEE 802.3ah/OAM protocol statistics.

Figure 22-1: Results of executing the show efmoam command

```
> show efmoam
Date 20XX/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port     Link status     UDLD status    Dest MAC
1/0/1    Up              detection    * 0012.e298.dc20
1/0/2    Down            active         unknown
1/0/4    Down(uni-link)  detection      unknown
>
```

Figure 22-2: Results of executing the show efmoam detail command

```
> show efmoam detail
Date 20XX/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port     Link status     UDLD status    Dest MAC
1/0/1    Up              detection    * 0012.e298.dc20
1/0/2    Down            active         unknown
1/0/3    Up              passive        0012.e298.7478
1/0/4    Down(uni-link)  detection      unknown
>
```

Figure 22-3: Results of executing the show efmoam statistics command

```
> show efmoam statistics
Date 20XX/10/02 23:59:59 UTC
Port 1/0/1 [detection]
  OAMPDUs   :Tx       =       295  Rx       =       295
             Invalid  =         0  Unrecogn.=         0
  TLVs      :Invalid  =         0  Unrecogn.=         0
  Info TLV  :Tx_Local =       190  Tx_Remote=       105  Rx_Remote=       187
```

```
            Timeout  =         3  Invalid  =         0  Unstable =         0
  Inactivate:TLV     =         0  Timeout  =         0
Port 1/0/2 [active]
  OAMPDUs   :Tx      =       100  Rx       =       100
             Invalid  =         0  Unrecogn.=         0
  TLVs      :Invalid  =         0  Unrecogn.=         0
  Info TLV  :Tx_Local =       100  Tx_Remote=       100  Rx_Remote=       100
             Timeout  =         0  Invalid  =         0  Unstable =         0
  Inactivate:TLV     =         0  Timeout  =         0
Port 1/0/3 [passive]
  OAMPDUs   :Tx      =       100  Rx       =       100
             Invalid  =         0  Unrecogn.=         0
  TLVs      :Invalid  =         0  Unrecogn.=         0
  Info TLV  :Tx_Local =         0  Tx_Remote=       100  Rx_Remote=       100
             Timeout  =         0  Invalid  =         0  Unstable =         0
  Inactivate:TLV     =         0  Timeout  =         0
>
```

23 CFM

CFM (Connectivity Fault Management) verifies the connectivity between bridges at the Layer 2 level and confirms routes; in other words, it is function for managing and maintaining wide-area Ethernet networks.

This chapter describes CFM and its operations.

23.1 Description

23.1.1 Overview

In addition to enterprise LANs, Ethernet is also starting to be used for wide area networks. As a result, maintenance and management function on par with SONET and ATM is required for Ethernet.

The CFM function uses the following types of function to maintain and manage Layer 2 networks:

1. Continuity Check

   This function always monitors whether information is delivered correctly to the destination (accessibility and continuity) between management points.

2. Loopback

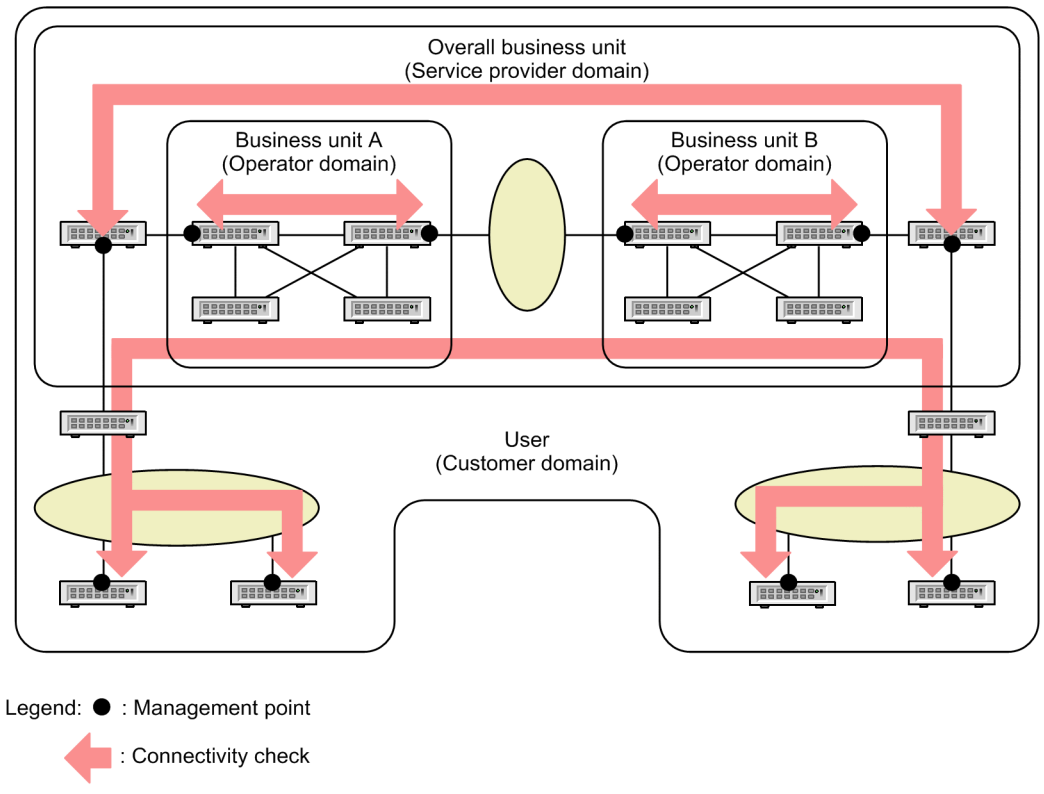
   After a failure is detected, the loopback function identifies the area affected by the failure on the route (loopback test).

3. Linktrace

   After a failure is detected, the linktrace function verifies the route to a management point (route searching within a Layer 2 network).

The following figure shows a configuration example of CFM.

Figure 23-1: Example of a CFM configuration



(1) CFM function

CFM is defined by IEEE 802.1ag and has the function described in the table below. The Switch supports all of this function.

Table 23-1: CFM function

Name	Description
Continuity Check (CC)	Continuously monitors accessibility between management points.
Loopback	Loopback test. Executes ping-equivalent function in Layer 2.
Linktrace	Route search. Executes traceroute-equivalent function in Layer 2.

(2) CFM configuration

The table below describes the elements configuring CFM. The scope of CFM behavior is maintenance and management defined by domains, MAs, MEPs, and MIPs.

Table 23-2: Elements configuring CFM

Name	Description
Domains (Maintenance Domain)	For management purposes, a group on the network to which CFM is applied
MA (Maintenance Association)	A group of VLANs used to subdivide a domain for management purposes
MEP (Maintenance association End Point)	A management end point. Set a MEP on the port at the domain boundary for each MA. In addition, the port is used to execute the CFM function.
MIP (Maintenance domain Intermediate Point)	A management intermediate point. This management point is located inside a domain.
MP (Maintenance Point)	A management point and the generic name used for a MEP or a MIP

23.1.2 CFM configuration elements

(1) Domains

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.

A higher domain level means that CFM PDUs from lower-level domains are discarded. Because a lower level domain forwards the CFM PDUs of higher-level domains without processing them, the CFM PDUs of lower-level domains are not forwarded to a higher-level domain. Accordingly, each domain can be maintained and managed independently.

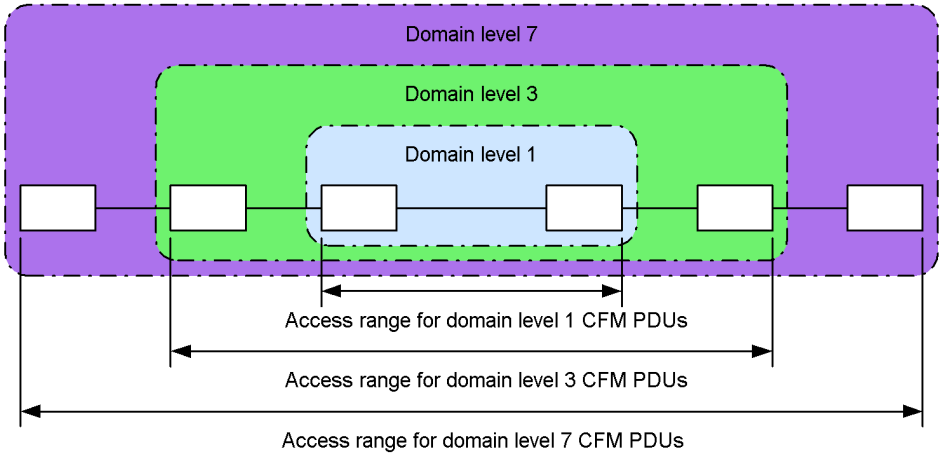
Standards stipulate that domain levels are to be used according to class. The following table describes the domain levels assigned to each class.

Table 23-3: Domain levels assigned to the classes

Domain level	Category
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 23-2: Example configuration of hierarchical domains



(2) MA

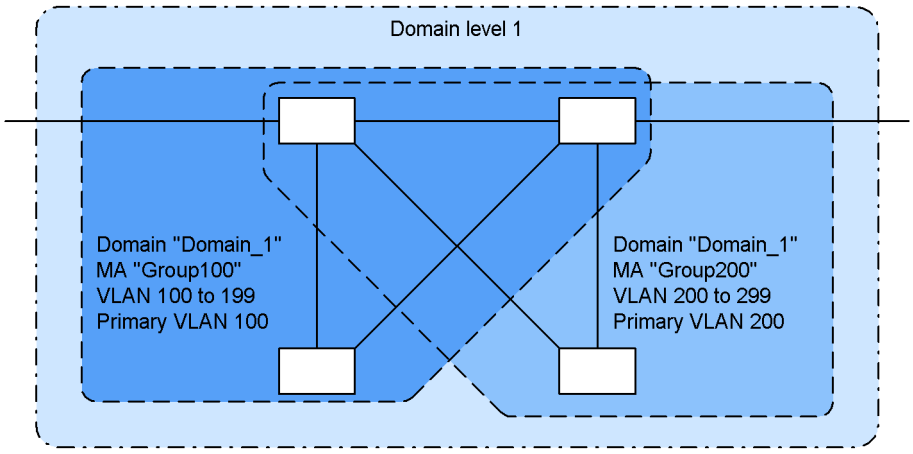
An MA is used to manage a domain by subdividing it into VLAN groups. A domain must have at least one MA.

Because CFM function can be used in an MA, setting MAs can divide the management range up even further.

MAs are identified by a domain name and an MA name. Accordingly, for the devices 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 23-3: Example of MA management scope



Also, the VLAN for sending and receiving CFM PDU (Primary VLAN) must be matched within the same MA.

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 the VLAN used 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 function is executed at a MEP. When CFM PDUs are sent and received between MEPs (that is, at domain boundaries), the CFM function is able to check the connectivity of the applicable network.

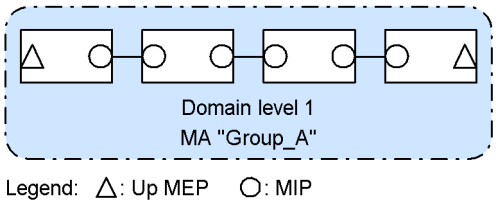
There are two types of MEPs:

- 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 23-4: Configuration example of up MEPs

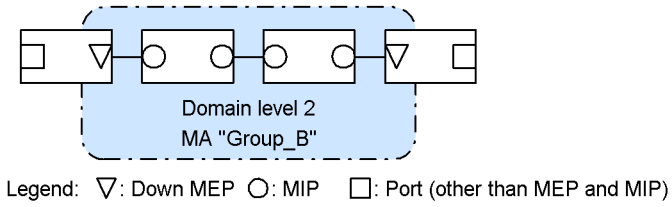


- Down MEP

  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 23-5: 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 23-6: Sending CFM PDFs from the down MEP or the up MEP

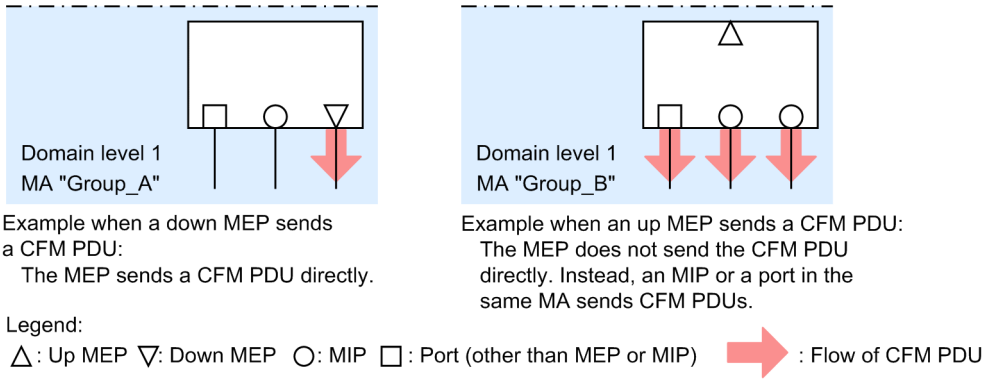
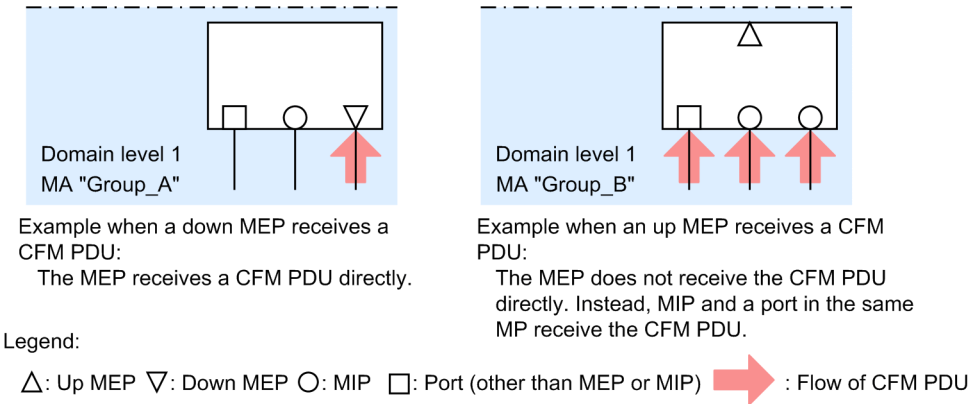
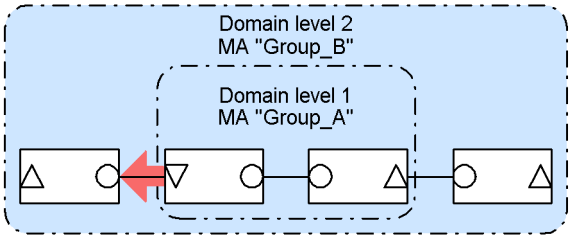


Figure 23-7: Receiving CFM PDF at the down MEP or up MEP



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 23-8: Example of an incorrectly set down MEP



If a down MEP is set outside MA "Group_A" by mistake, the CFM functionality does not operate correctly because the CFM PDU is sent outside MA "Group_A" (outside domain level 1).

Legend:
△: Up MEP ▽: Down MEP ○: MIP : Flow of CFM PDU

(4) MIP

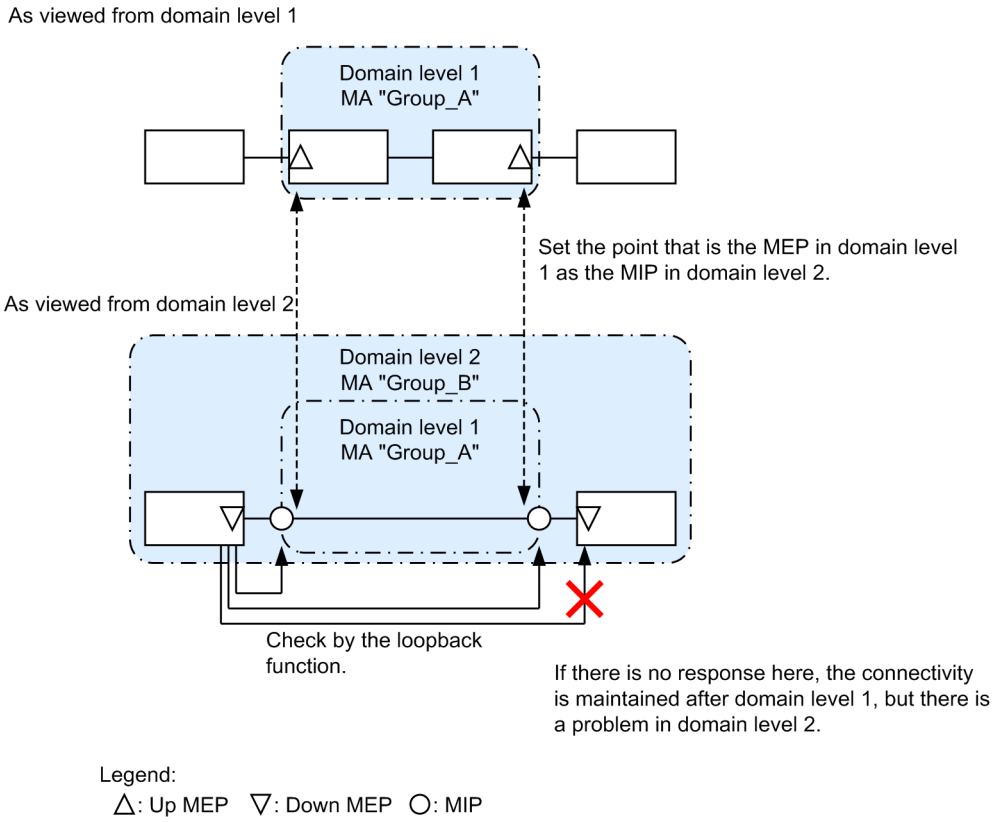
An MIP is a management point set inside a domain, and is specified for each domain (and is shared by all MAs inside a domain). For a hierarchical configuration, set a MIP at the point where a higher-level domain and a lower-level domain overlap. In addition, because MIPs respond to the loopback function and the link-trace function, 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 23-9: Example of a hierarchical structure configured by 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.

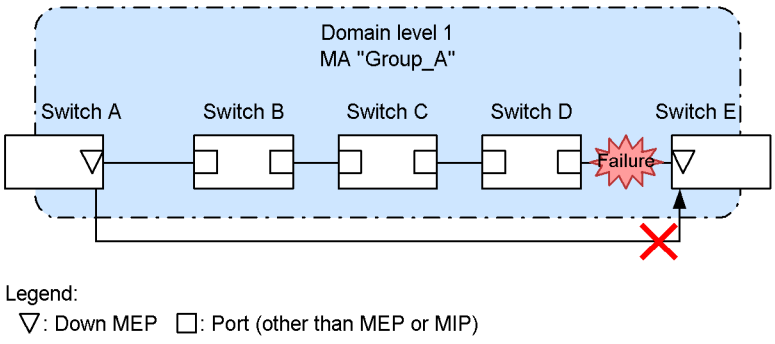
If a failure occurs, you can narrow down the scope of the investigation because you are able to isolate the cause of the failure to domain level 1 or domain level 2.

(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.

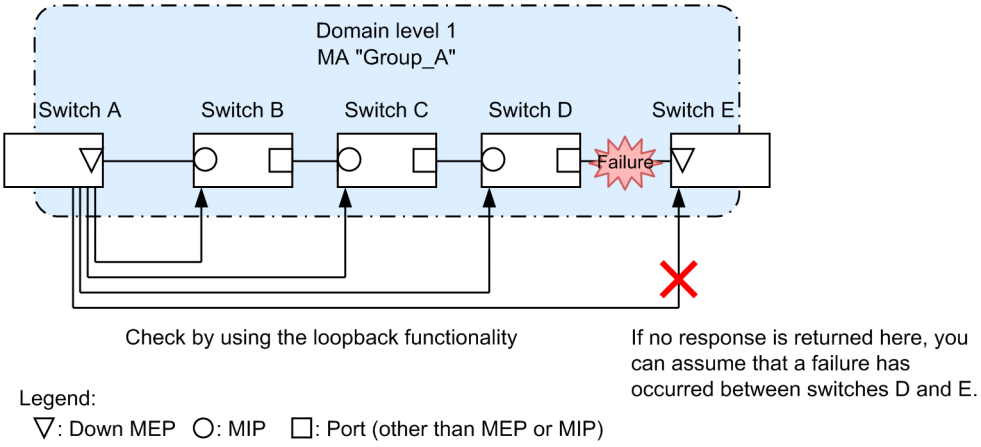
The figure below shows an example configuration where no MIPs are set in a domain. In this example, if a network failure occurs, you can confirm that the MEP of switch A cannot communicate with the MEP of switch E, but you cannot identify the point at which the failure occurred.

Figure 23-10: 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 device to respond to the loopback or linktrace function.

Figure 23-11: Example configuration where MIPs are set in a domain



23.1.3 Designing domains

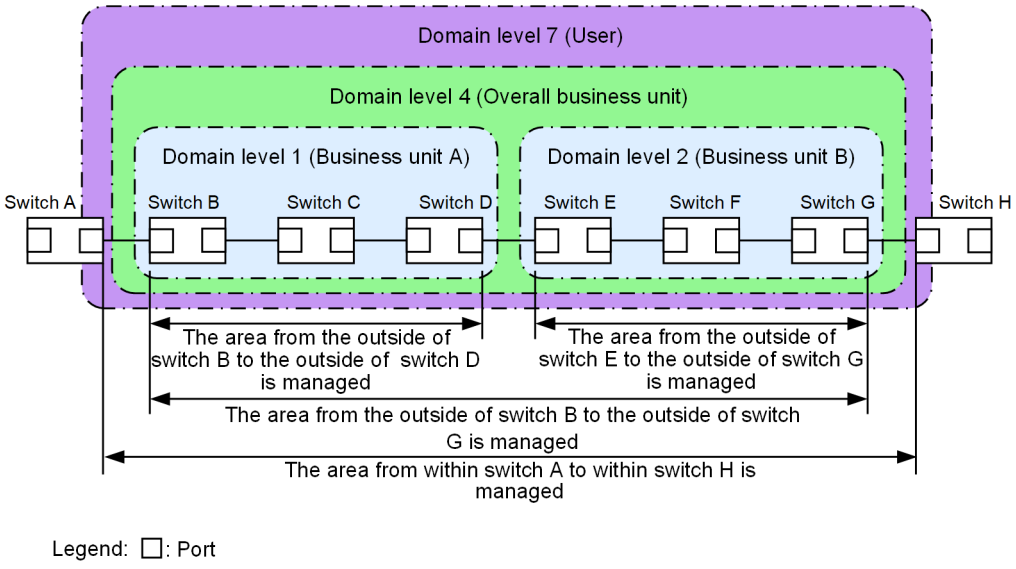
To use the CFM function, design the domains first. Then design the domain configurations and their hierarchies, and finally design the details of each domain.

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 23-12: 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 category. 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.

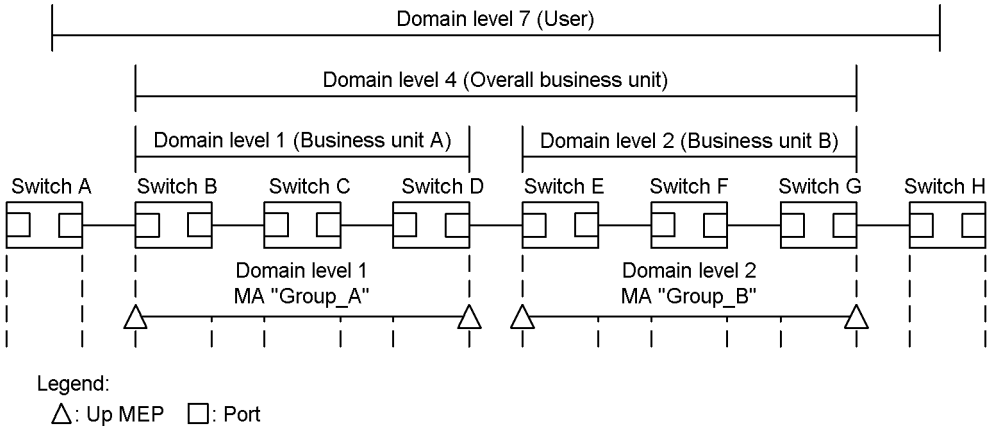
- Configuring domain levels 1 and 2

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 23-13: Configuring domain levels 1 and 2



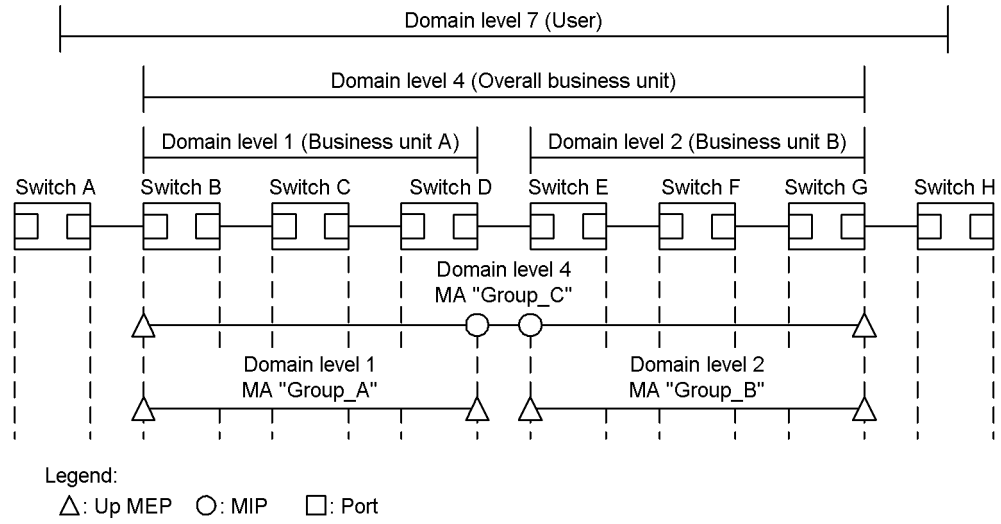
- Configuring domain level 4

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 function to determine if the problem has occurred in the domain you manage or in a lower-level domain.

Figure 23-14: Configuring domain level 4



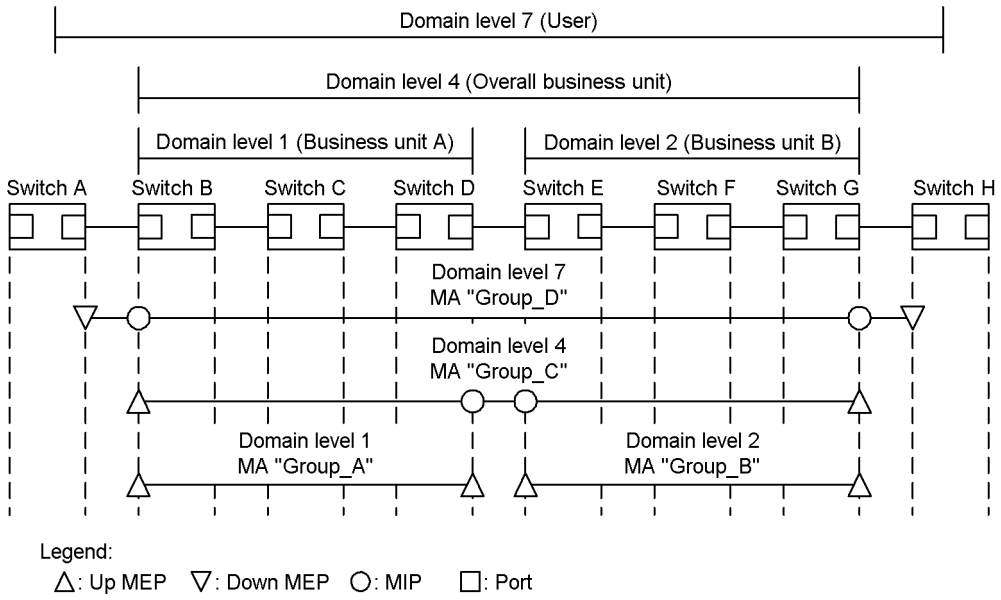
- Configuring domain level 7

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 G, 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 23-15: 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 function and the linktrace function.

The following figure shows configuration examples before and after MIPs are set.

Figure 23-16: Example configuration before MIPs are set

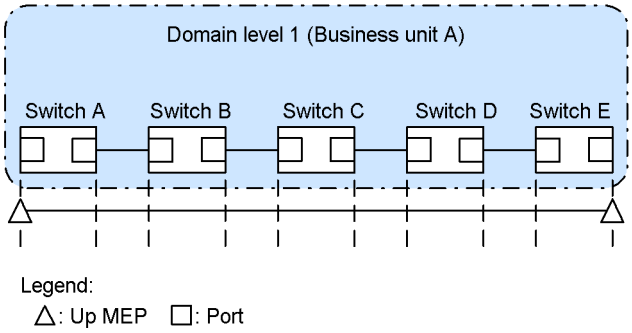
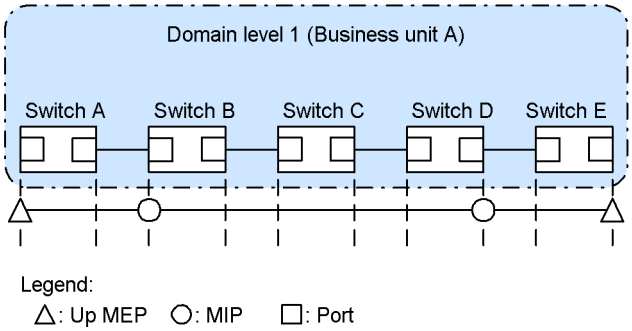


Figure 23-17: Example configuration after MIPs are set



Inside the domain, specify, as MIPs, the ports to be configured as the destination of the loopback function and the linktrace function. 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, routing information of the linktrace function is returned as a response.

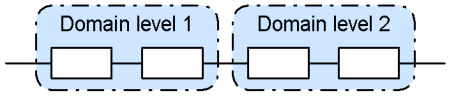
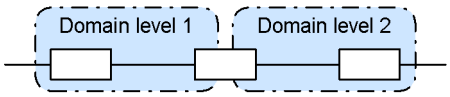
You cannot specify switch C as the destination for loopback and linktrace because no MIPs are configured on switch C. In addition, because switch C does not respond to the linktrace function, information about switch C is not contained in routing information.

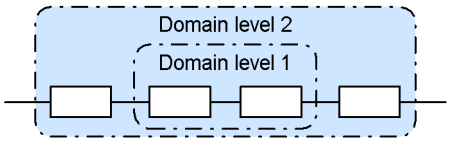
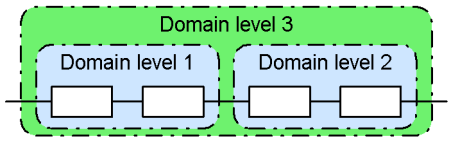
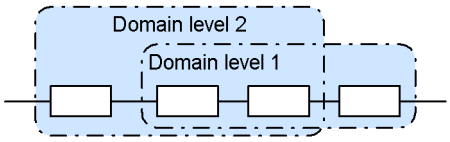
(3) Domain configuration examples

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 are states whether they are possible or not.

Table 23-4: Example of possible and impossible domain configurations

Configuration status	Configuration example	Whether configurable
Neighboring domains		Supported
Touching domains		Supported

Configuration status	Configuration example	Whether configurable
Nested domains		Supported
Combination of neighboring domains and nested domains		Supported
Overlapping domains		Not supported

23.1.4 Continuity Check

Continuity Check (CC) is function that constantly monitors connectivity between MEPs. All MEP in MA CCM (Continuity Check Message. A type of CFM PDU) are sent and received to learn the MEP in the MA. What the MEPs learn is used for the loopback function and the linktrace function.

If a device on which the CC function 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 function. There are five such Failure levels. The Switch is initially configured to detect level 2 and higher failures.

Table 23-5: Failures detected by the CC function

Failure level	Problem	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 device has entered a state in which it is unable to communicate.	
1	A CCM reporting failure detection was received. Remote Defect Indication	Not detected

When the failure recovery monitoring time after the failure recovery trigger point has elapsed, it is determined that recovery from the failure has succeeded.

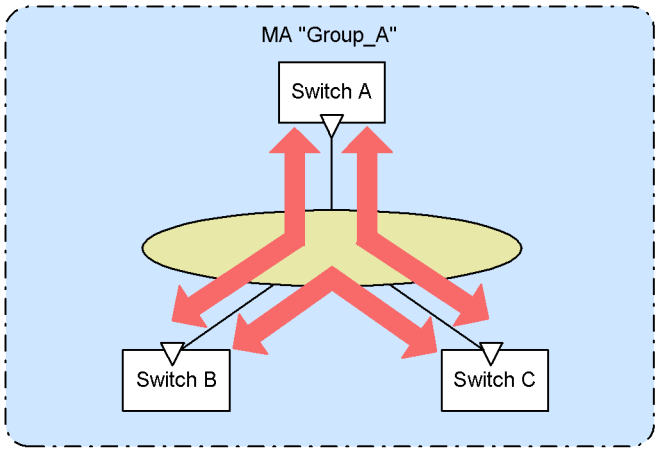
Table 23-6: Failure recovery trigger point and failure recovery monitoring time

Failure level	Failure recovery trigger point	Failure recovery monitoring time
5	A domain and an MA no longer receive different CCMs.	Sending interval of the received CCMs x 3.5
4	A CCM with an incorrect MEP ID or an incorrect sending interval is no longer received.	Sending interval of the received CCMs x 3.5
3	A CCM is received again.	Immediately after reception of the CCM
2	A CCM indicating that the port on the applicable device can now communicate.	Immediately after reception of the CCM
1	A CCM indicating no failure is detected is received.	Immediately after reception of the CCM

CC function behavior will be described using switch B in the following figures as an example.

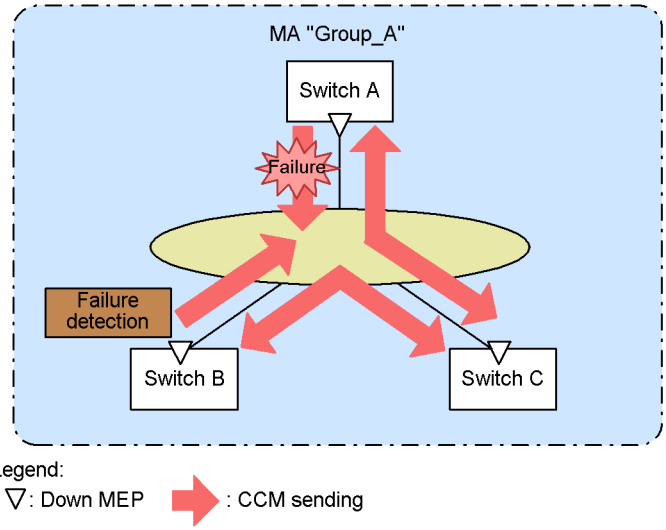
Each MEP multicasts a CCM regularly inside the MA. Because CCMs are received from each MEP regularly, connectivity is always monitored.

Figure 23-18: Continuous monitoring of connectivity using CC



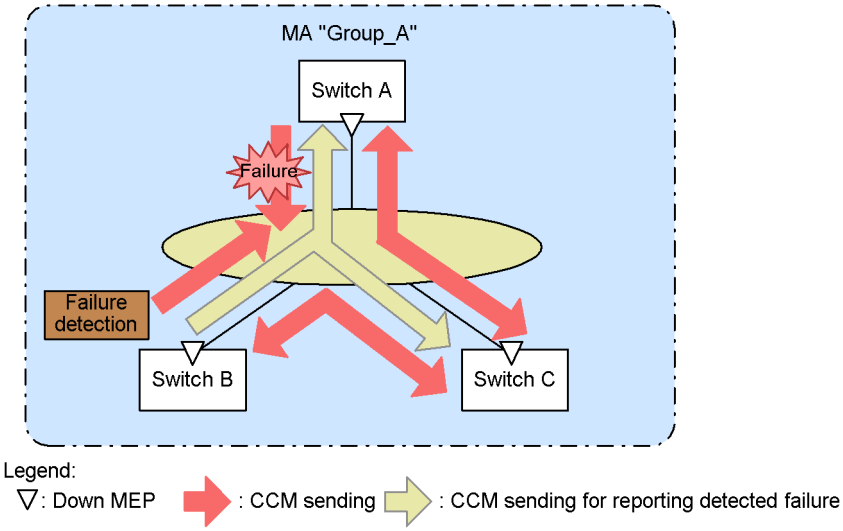
If a CCM from switch A cannot be delivered to switch B because of a switch failure or a network failure, switch B determines that the state is a network failure between switches A and B.

Figure 23-19: Detecting a failure with CC



When switch B detects a failure, switch B notifies all MEPs in the MA that a failure has been detected.

Figure 23-20: Notifying all MEPs of the failure



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 devices can determine the route inside the MA on which the failure occurred.

23.1.5 Loopback

The loopback function 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 function verifies the connectivity between MEPs. The loopback function 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 function. If, for example, multiple MIPs are configured on a device, connectivity can be verified for each MIP.

The following figure shows an example of executing the loopback for MIPs and MEPs.

Figure 23-21: Execution of loopback to MIPs

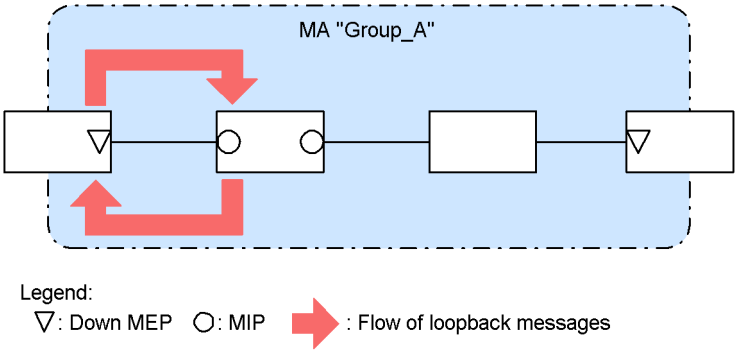
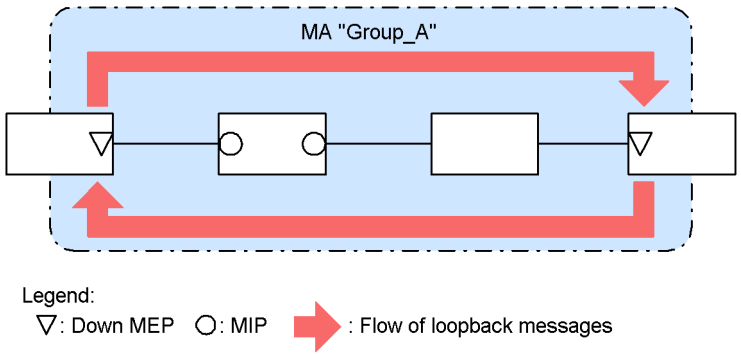


Figure 23-22: Execution of loopback to MEPs



Because the loopback function uses what the CC function learns, the CC function 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.

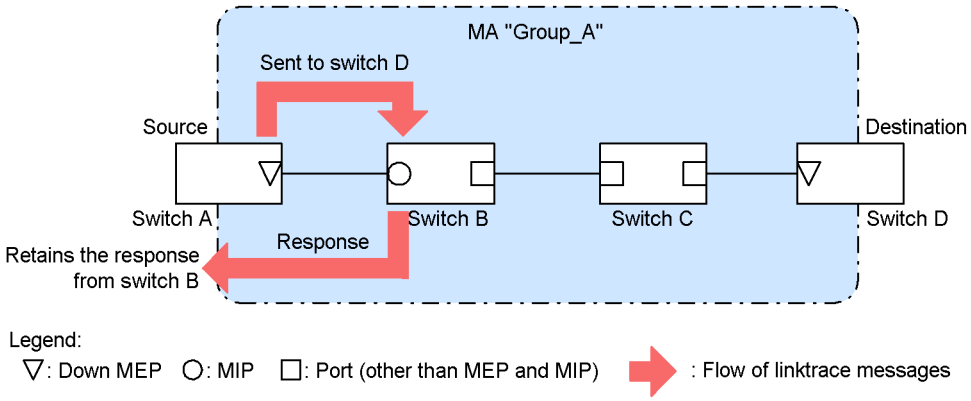
23.1.6 Linktrace

The linktrace function can be used at the Layer 2 level, and is equivalent to traceroute. The linktrace function collects information about devices that pass traffic between MEPs or between a MEP and a MIP of the same MA, and outputs routing information.

The linktrace function 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.

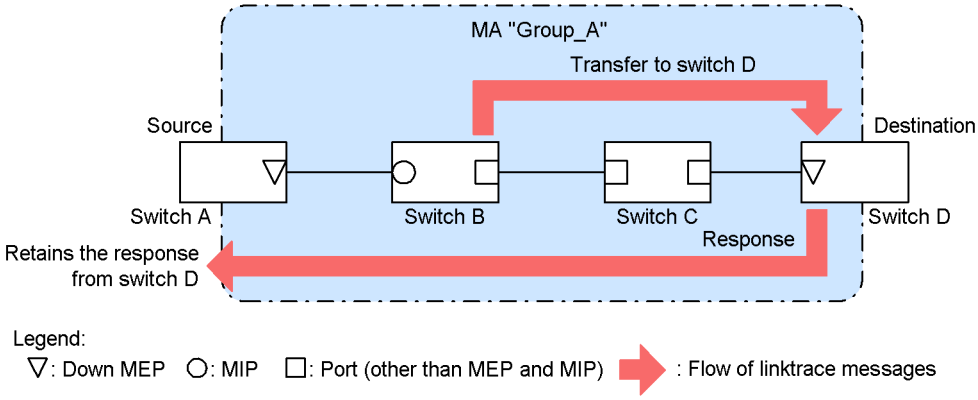
Figure 23-23: Sending a linktrace message to a destination



A linktrace message is forwarded to the destination via MIPs. An MIP sends back information about the port of the local device used to receive the MIP and the ports used to forward the MIP. The device from which the message was sent (the source switch) keeps the information sent by the MIPs as routing information.

The following figure shows an example of forwarding a linktrace message to the destination.

Figure 23-24: Forwarding a linktrace message to a 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 routing information that can be used to check the route to the destination.

The linktrace function provides information for each device. For example, whether one or multiple MIPs are configured on a device, the linktrace function provides information about the port used to receive the message and the port used to forward the message.

Because the linktrace function uses what the CC function learns, the CC function 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.

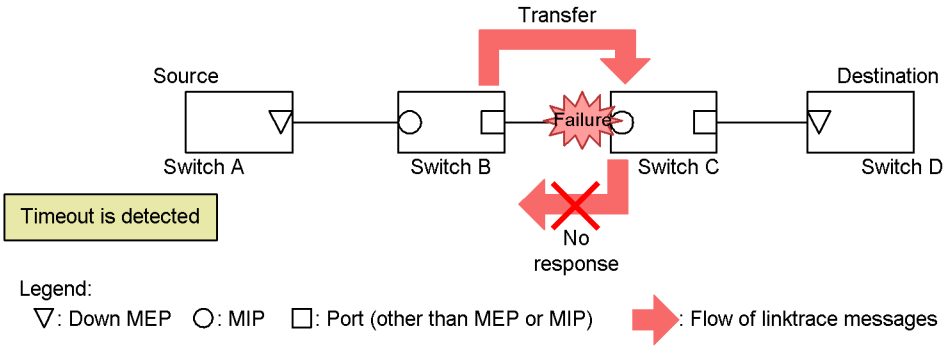
(a) Using the linktrace function to isolate failures

You can use the execution results of the linktrace function to isolate the device 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 function.

Figure 23-25: Example timeout detection by the linktrace function

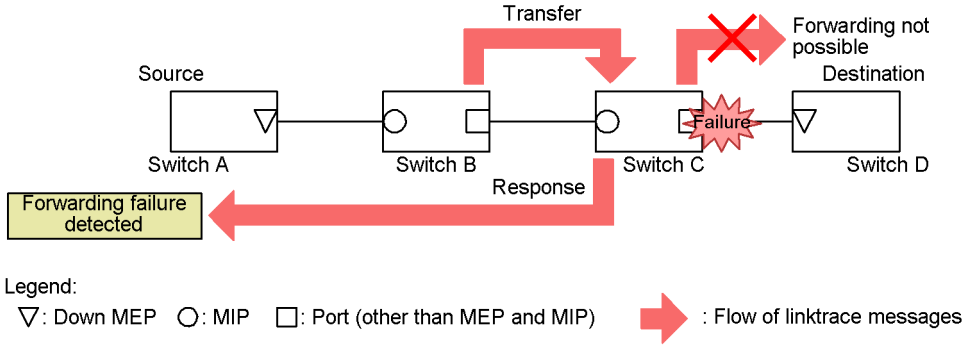


In this example, when switch A detects a timeout by using the linktrace function, a receiving port on the network might not be able to communicate. A linktrace message is forwarded from switch B to switch C, but because switch C cannot communicate and cannot return a response, a timeout occurs.

- When a forwarding failure is detected

The following figure shows an example of a communication failure detected by the linktrace function.

Figure 23-26: Example of detection of a communication failure by the linktrace function



If switch A detects a forwarding failure by using the linktrace function, a sending port on the network might not be able to communicate. The reason is that a linktrace message cannot be forwarded to switches C and D (destination), and therefore the linktrace function returns a message indicating that a sending port cannot communicate with switch A.

(b) Linktrace response

Linktrace messages are multicast frames.

When forwarding linktrace messages between devices on which CFM is used, see the MIP CCM database and the MAC address table to determine the port used to forward linktrace messages.

Devices 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 devices that are not on the route to the destination.

23.1.7 Specifications for common behaviors

(1) Behavior for a blocked port

The following tables describe the behavior of each type of CFM function for a blocked port.

Table 23-7: When an up MEP is blocked

function	Operation
CC	• Sends and receives a CCM and sets Blocked as the status of the port from which the CCM was sent.
Loopback	• The "l2ping" operation command cannot be executed. • Responds to loopback messages sent to the local switch.
Linktrace	• The "l2traceroute" operation command cannot be executed. • Responds to linktrace messages. Sets Blocked for the status of the egress port from which a response linktrace message is expected.

Table 23-8: When a down MEP is blocked

function	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.

function	Operation
Linktrace	• The "l2traceroute" operation command cannot be executed. • Does not respond to linktrace messages.

Table 23-9: When a MIP is blocked

function	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.
Linktrace	• Does not respond to a linktrace message received from the line side • Responds to a linktrace message received from the forwarding side. Sets Blocked for the status of the egress port from which a response linktrace message is expected. • Does not transmit linktrace messages

Table 23-10: When ports other than MEP and MIP ports are blocked

function	Operation
CC	• Does not transmit CCMs.
Loopback	• Does not transmit loopback messages.
Linktrace	• Does not transmit linktrace messages

(2) Settings for a VLAN tunneling configuration

When using the CFM function in a VLAN tunneling network, divide the domain for the VLAN tunneling network into an inside part and an outside part so that you can manage the resulting networks separately. Note, however, that some parts of the CFM function have restrictions on use depending on the locations where the domain is configured. The following table describes the restrictions on function according to where the domains are configured.

Table 23-11: Restrictions on using the CFM function according to where the domains are configured

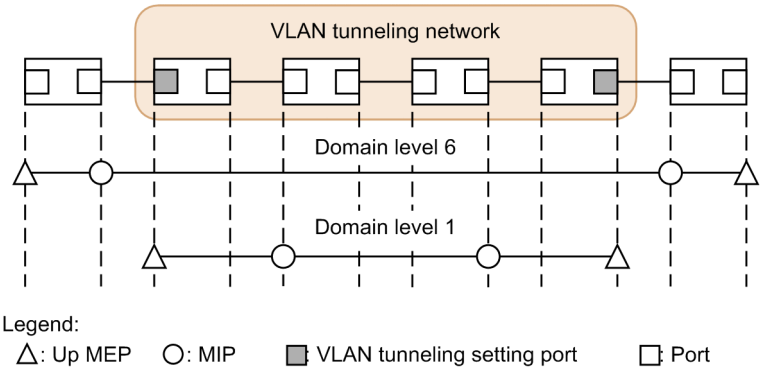
Where a domain is configured	Function		
	CC	Loopback	Linktrace
Inside the VLAN tunneling network and outside the VLAN tunneling network	Can be used	Can be used	• Can be used inside the VLAN tunneling network • Cannot be used outside the VLAN tunneling network via the VLAN tunnel
Inside the VLAN tunneling network only	Can be used	Can be used	Can be used
Outside the VLAN tunneling network only	Can be used	Can be used	Can be used

(a) When using CFM for the inside and outside parts of the VLAN tunneling network

The following figure shows an example of using the CFM function inside and outside the VLAN tunneling

network.

Figure 23-27: Example of using CFM inside and outside the VLAN tunneling network



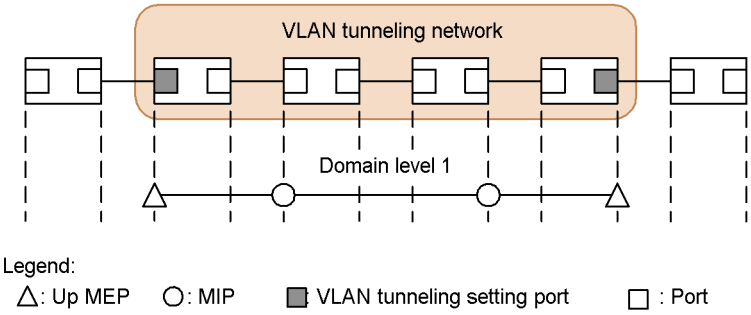
In domain level 1 inside the VLAN tunneling network, you can configure MPs anywhere on the VLAN tunneling network. At domain level 6 outside the VLAN tunneling network, you can configure MPs only on devices outside the VLAN tunneling network. You cannot configure MPs for domain level 6 inside the VLAN tunneling network. Management inside the VLAN tunneling network is performed at domain level 1.

In addition, in domain level 6 outside the VLAN tunneling network, you cannot use the linktrace function through a VLAN tunnel.

(b) When CFM is used only inside the VLAN tunneling network

The following figure shows an example of using the CFM function only inside the VLAN tunneling network.

Figure 23-28: Example of using the CFM function only inside the VLAN tunneling network

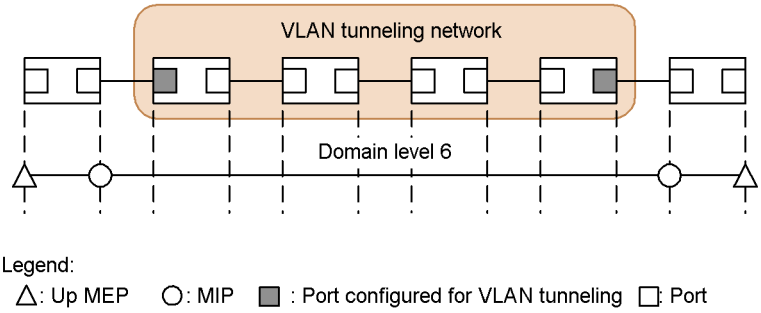


In domain level 1 inside the VLAN tunneling network, you can configure MPs anywhere on the VLAN tunneling network. You can use the CFM function in the domain.

(c) When using the CFM function only outside the VLAN tunneling network

The following figure shows an example of using the CFM function only outside the VLAN tunneling network.

Figure 23-29: Example of using the CFM function only outside the VLAN tunneling network



At domain level 6 outside the VLAN tunneling network, you can configure MPs only on devices outside the VLAN tunneling network. You cannot configure MPs for domain level 6 inside the VLAN tunneling network. You can use the CFM function in the domain.

23.1.8 Databases used for CFM

The following table describes the databases used by the CFM function.

Table 23-12: Databases used for CFM

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 function uses this database when it monitors pervasive connectivity. 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 function. The database holds the following information: • The MEPs and the destinations where the linktrace function was executed • TTL • Information about devices that sent back responses • Information about ports on which linktrace messages were received • Information about ports from which linktrace messages were forwarded	show cfm l2traceroute-db

(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 function and the linktrace function, 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 function 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, see the MAC address table to determine the port used to forward the message.

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 function is running.

(3) Linktrace database

The linktrace database holds the execution results of the linktrace function.

You can use the "show cfm l2traceroute-db" operation command to see the results of executing the linktrace function in the past.

(a) Number of routes that can be held

A switch can retain responses for a maximum of 1024 devices.

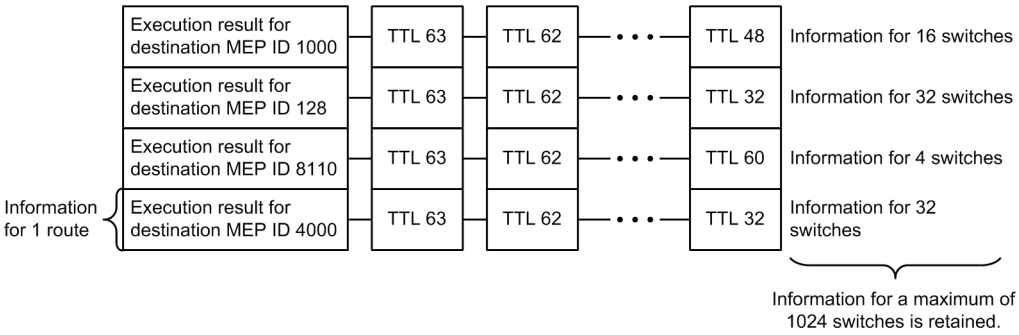
The number of routes that can be retained is determined by the number of devices per route. If you want to retain responses for 256 switches per route, you can have four routes. If you want to retain responses for 16 devices per route, you can have 64 routes.

If the number of responses exceeds for the number of responses allowed for 1024 devices, information about an old route is deleted, and information about the new route is saved.

When the linktrace function is executed at a destination that is registered in the linktrace database, the routing information from the linktrace database to the applicable destination is deleted first, and then the new linktrace response is saved.

The following figures show entries in the linktrace database.

Figure 23-30: Linktrace database



An entry in this database is created when a MEP receives a response while the linktrace function is running.

23.1.9 Notes on using CFM

(1) Devices on which the CFM function is not used

When you use the CFM function, you do not need to use it on all the devices in a domain. However, CFM PDUs must be transparent on the switches on which the function is not used.

Except for the Switch, you need to configure the devices on which the CFM function is not used so that the frames described in the following table are transparent.

Table 23-13: Frames to be transmitted

Frame type	Destination MAC address
Multicast	0180.c200.0030 to 0180.c200.003f

If the CFM function is not used, the Switch makes all CFM PDUs transparent.

(2) Use with other function

(a) When used with the Layer 2 switch function

See "Configuration Guide Vol. 1, 22.3 Compatibility between the Layer 2 switch function and other functions".

(b) When used with Layer 2 authentication

For details, see "5.2.1 Using Layer 2 authentication with other functions".

(3) Burst reception of CFM PDUs

When there are 96 or more remote MEPs to be monitored continuously by the CC function, 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 devices so that there is no timing overlap.

(4) MEP settings in MAs in which the same primary VLAN is configured in the same domain

In MAs in which the same primary VLAN is set within the same domain (including the same MA), you cannot set two or more MEPs on the same port. If you do so, the CFM function does not run correctly on the applicable MEPs.

(5) Collecting routing information by using the linktrace function

The linktrace function determines the destination port for forwarding linktrace messages by referencing the MIP CCM database or the MAC address table. However, correct routing information cannot be collected because the destination port cannot be determined until the CC function sends or receives a CCM when link-up is detected (including a second link-up after a link-down) or after a change of the route when a Spanning Tree Protocol is used.

(6) When the CFM function does not run at an up MEP and at a MIP

The CFM function does not work on the ports for up MEPs and MIPs for which link-up has not yet occurred after any of the events below has occurred. The function is able to run if link-up occurred once.

- Device startup (including restarting of the device)
- Application of the configuration file to a running configuration
- Execution of the "restart vlan" operation command
- Execution of the "restart cfm" operation command

(7) When a MIP on a blocked port does not respond to the loopback function and linktrace function

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 function and the linktrace function.

- Executing the Spanning Tree Protocol (PVST+, single) to use the loop guard function
- When the Spanning Tree Protocol (MSTP) is used, configuring the access VLAN or the native VLAN as the primary VLAN
- Using LLDP
- Using OADP

(8) Behavior of the CC function in a redundant configuration

When the CC function is used in a Layer 2 network configured redundantly (such as when the Spanning Tree Protocol or Ring Protocol is used), if a communication path is switched, a CCM sent from the MEP of the local switch may be received and an ErrorCCM may be detected. This failure is corrected after the communication path becomes stable.

23.2 Configuration

23.2.1 List of configuration commands

The following table describes the list of configuration commands for CFM.

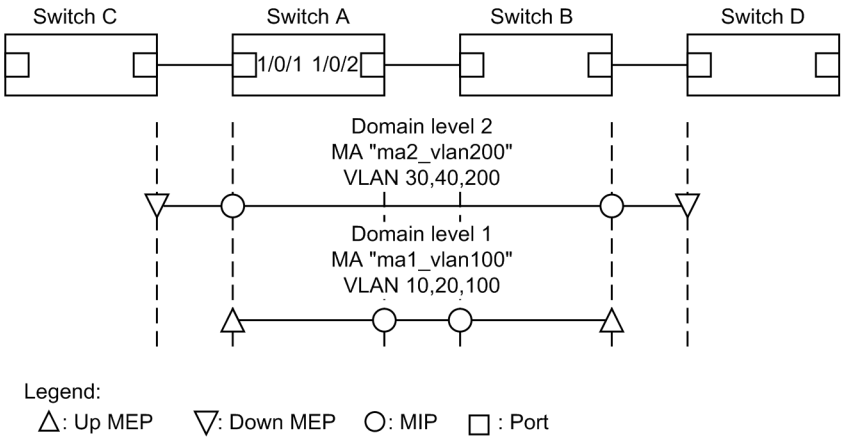
Table 23-14: List of configuration commands

Command name	Description
domain name	Sets the name used for the applicable domain.
ethernet cfm cc alarm-priority	Sets the failure level detected by the CC function.
ethernet cfm cc alarm-reset-time	Sets the period of time until the CC function recognizes that the failure is a redetected failure.
ethernet cfm cc alarm-start-time	Sets the time from the point at which CC detects a failure until it sends an SNMP notification.
ethernet cfm cc enable	Sets in a domain an MA in which the CC function is used.
ethernet cfm cc interval	Sets the CCM sending interval.
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 function.
ethernet cfm mip	Sets a MIP used by the CFM function.
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.

23.2.2 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 23-31: Configuration example for 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 sends 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.
Because you can use the MEPs and MIPs you specified, you need to enable the CFM function of the device.

Command examples

1. ```
   (config)# interface gigabitethernet 1/0/1
   (config-if)# ethernet cfm mep level 1 ma 1 mep-id 101
   (config-if)# ethernet cfm mip level 2
   (config-if)# exit
   (config)# interface gigabitethernet 1/0/2
   (config-if)# ethernet cfm mip level 1
   (config-if)# exit
   ```

   Sets MEPs belonging to domain level 1 and MA1 for port 1/0/1. Also, configures a MIP in domain level 2, Set MIPs for domain level 1 to port 1/0/2.

2. `(config)# ethernet cfm enable`

   Initiates operation of the CFM function on the Switch.

(3) Stopping the CFM function on a port

Points to note

This setting is required if you want to temporarily stop the CFM function on a port.

Command examples

1. `(config)# interface gigabitethernet 1/0/1`
   `(config-if)# no ethernet cfm enable`
   `(config-if)# exit`

   Stops CFM on port 1/0/1.

(4) Configuring CC

Points to note

The CC function starts behavior as soon as the "ethernet cfm cc enable" command is set.

Command examples

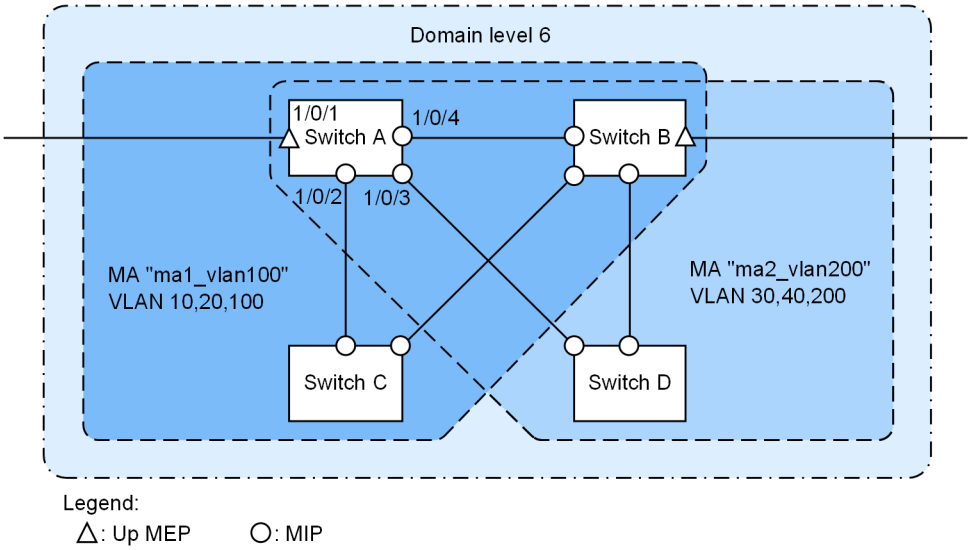
1. `(config)# ethernet cfm cc level 1 ma 1 interval 10s`
   `(config)# ethernet cfm cc level 1 ma 1 enable`

   Initiates behavior of the CC function in MA1 of domain level 1 with the CCM sending interval set to 10 seconds.

23.2.3 Configuring the CFM function (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 23-32: 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 "23.2.2 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 "23.2.2 Configuring CFM (multiple domains)".

Command examples

1.
```
(config)# interface gigabitethernet 1/0/1
(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 gigabitethernet 1/0/2-4
(config-if-range)# ethernet cfm mip level 6
(config-if-range)# exit
```

Sets MEPs belonging to domain level 6 and MA1 for port 1/0/1. Also, sets a MEP belonging to MA2, Sets MIPs of domain level 6 to port 1/0/2 to 1/0/4.

2.
```
(config)# ethernet cfm enable
```

Initiates operation of the CFM function on the Switch.

23.3 Operation

23.3.1 List of operation commands

The following table describes the list of operation commands for CFM.

Table 23-15: List of operation commands

Command name	Description
l2ping	Executes the CFM loopback function and verifies the connectivity between the specified MPs.
l2traceroute	Executes the CFM linktrace function and verifies the routing between the specified MPs.
show cfm	Shows information about a CFM domain.
show cfm remote-mep	Shows information about a CFM remote MEP.
show cfm fault	Shows CFM failure information.
show cfm l2traceroute-db	Shows routing information obtained by using the "l2traceroute" command.
show cfm statistics	Shows CFM statistics.
clear cfm remote-mep	Clears remote MEP information about a CFM MEP.
clear cfm fault	Clears CFM failure information.
clear cfm l2traceroute-db	Clears routing information obtained by using the "l2traceroute" command.
clear cfm statistics	Clears the CFM statistics.
restart cfm	Restarts the CFM program.
dump protocols cfm	Outputs CFM dump information to a file.

23.3.2 Checking connection between MPs

Use the "l2ping" command to check the connectivity between the specified MPs and to display the result. 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 5, and the time to wait for a response is set to 5 seconds. When a verification result is returned or the time to wait for a response has elapsed, another verification attempt is started.

Figure 23-33: Results of executing the l2ping command

```
>l2ping remote-mep 1010 domain-level 7 ma 1000 mep 1020 count 3 timeout 1
L2ping to MP:1010(0012.e220.00a3) on Level:7  MA:1000  MEP:1020  VLAN:20
Time:20XX/03/14 19:10:24
1: L2ping Reply from 0012.e220.00a3  64bytes  Time=  751 ms
2: L2ping Reply from 0012.e220.00a3  64bytes  Time=  752 ms
3: L2ping Reply from 0012.e220.00a3  64bytes  Time=  744 ms

--- L2ping Statistics ---
Tx L2ping Request :    3  Rx L2ping Reply :    3  Lost Frame  :   0%
Round-trip Min/Avg/Max : 744/749/752 ms

>
```

23.3.3 Checking the route between MPs

Use the "l2traceroute" command to obtain routing information about the route between the specified MPs and to display the result. 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 5 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 23-34: Results of executing the l2traceroute command

```
>l2traceroute remote-mep 2010 domain-level 7 ma 1000 mep 2020 timeout 10 ttl 64
Date 20XX/03/15 14:05:30 UTC
L2traceroute to MP:0012.e220.00a3 on Level:7  MA:1000  MEP:1020  VLAN:1000
Time:20XX/03/15 14:05:30
63  0012.e220.00c0  Forwarded
62  0012.e210.000d  Forwarded
61  0012.e242.00a3  NotForwarded  Hit
```

23.3.4 Checking the status of MPs on a route

You can use the "show cfm l2traceroute-db detail" 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 23-35: Results of executing the show cfm l2traceroute-db detail command

```
> show cfm l2traceroute-db remote-mac 0012.e220.1040 detail
Date 20XX/03/16 10:21:42 UTC
L2traceroute to MP:2010(0012.e220.1040) on Level:7  MA:2000  MEP:2020  VLAN:20
Time:20XX/03/16 10:21:42
63   0012.e220.10a9  Forwarded
  Last Egress : 0012.f110.2400  Next Egress : 0012.e220.10a0
  Relay Action: MacAdrTbl
  Chassis ID    Type: MAC       Info: 0012.e228.10a0
  Ingress Port  MP Address: 0012.e220.10a9  Action: OK
  Egress Port   MP Address: 0012.e220.10aa  Action: OK
62   0012.e228.aa3b  NotForwarded
  Last Egress : 0012.e220.10a0  Next Egress : 0012.e228.aa30
  Relay Action: MacAdrTbl
  Chassis ID    Type: MAC       Info: 0012.e228.aa30
  Ingress Port  MP Address: 0012.e228.aa2c  Action: -
  Egress Port   MP Address: 0012.e228.aa3b  Action: Down
>
```

23.3.5 Checking the CFM status

Use the "show cfm" command to display the CFM settings and the status of failure detection. If the CC function has detected a failure in the Status section, you can check the type of the failure that has the highest failure level of the failures detected.

Figure 23-36: Results of executing the show cfm command

```
>show cfm
Date 20XX/03/15 18:32:10 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:3  Start Time:2500ms  Reset Time:10000ms
    MEP Information
      ID:8012  UpMEP    CH12(Up)    Enable   MAC:0012.e200.00b2  Status:Timeout
  MA 400   Name(str) : Tokyo_to_Nagoya
    Primary VLAN:400   VLAN:30-40,400
    CC:Enable   Interval:1min
    Alarm Priority:3  Start Time:2500ms  Reset Time:10000ms
    MEP Information
```

```
      ID:8014  DownMEP  0/21(Up)    Disable  MAC:0012.e220.0040  Status:-
  MIP Information
      0/12(Up)    Enable   MAC:0012.e200.0012
      0/22(Down)  Disable  MAC:-
Domain Level 4 Name(str): ProviderDomain_4
  MIP Information
      CH12(Up)    Enable   MAC:0012.e220.00b2
>
```

23.3.6 Checking detailed information of failures

Use the "show cfm fault detail" command to display the status of failure detection and the CCM information. This information is an aid for detecting failures for each failure type. The remote MEP that sent the CCM can be checked in the RMEP, MAC, and VLAN sections.

Figure 23-37: Results of executing the show cfm fault detail command

```
>show cfm fault detail
Date 20XX/03/21 12:23:41 UTC
MD:7  MA:1000  MEP:1000  Fault
  OtherCCM : -  RMEP:1020 MAC:0012.e220.1e22 VLAN:1000 Time:20XX/03/20 11:22:17
  ErrorCCM : -
  Timeout  : -
  PortState: -
  RDI      : On RMEP:1011 MAC:0012.e220.11a2 VLAN:1000 Time:20XX/03/21 11:42:10
>
```

The remote MEP information displayed by the "show cfm fault detail" command is an aid in failure detection. In actuality, failures might occur at multiple remote MEPs.

You can use the "show cfm remote-mep" command to find the remote MEP where a failure is occurring from the ID and Status sections of the displayed remote MEP information.

Figure 23-38: Results of executing the show cfm remote-mep command

```
>show cfm remote-mep
Date 20XX/03/21 12:25:30 UTC
Total RMEP Counts:      5
Domain Level 7 Name(str): ProviderDomain_7
  MA 1000  Name(str) : Tokyo_to_Osaka
    MEP ID:1000  0/20(Up)    Enable   Status:RDI
      RMEP Information  Counts:  3
      ID:1011  Status:-           MAC:0012.e200.005a  Time:20XX/03/21 12:25:29
      ID:1020  Status:RDI         MAC:0012.e220.1e22  Time:20XX/03/21 12:25:29
      ID:1030  Status:RDI         MAC:0012.e220.1e09  Time:20XX/03/21 12:25:29
  MA 2000  Name(str) : Tokyo_to_Nagoya
    MEP ID:8012  CH1 (Up)    Enable   Status:-
      RMEP Information  Counts:  2
      ID:8003  Status:-           MAC:0012.e20a.1241  Time:20XX/03/21 12:25:28
      ID:8004  Status:-           MAC:0012.e20d.12a1  Time:20XX/03/21 12:25:29
>
```

24 LLDP

The Link Layer Discovery Protocol (LLDP) is function that collects information about the devices that are neighbors of the Switch. This chapter describes LLDP and its use.

24.1 Description

24.1.1 Overview

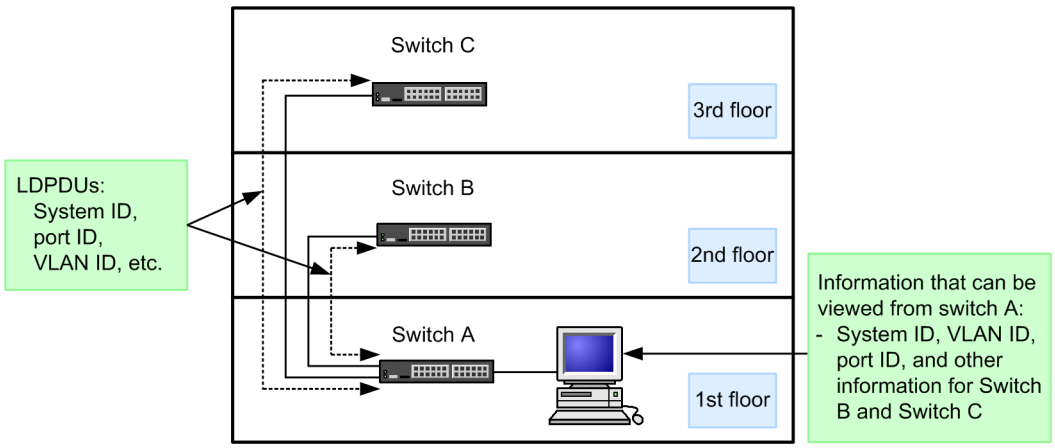
LLDP (Link Layer Discovery Protocol) is a protocol to collect information about neighboring devices. The purpose of the function provided by the protocol is to make the examination of information about connected devices easier during operation and maintenance.

(1) Example of using LLDP

LLDP allows a local device to send its own device and port information to the ports of neighboring devices connected to the local device. By managing the received information, the operator at the local device can check the status of connections to 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 24-1: Example of using the LLDP



24.1.2 Supported specifications

(1) LLDP standard that can be connected

The Switch supports the following two standards.

- IEEE Std 802.1AB-2009

  The Switch can receive only LLDPDUs with a destination MAC address of "01:80:C2:00:00:0E".

- IEEE 802.1AB Draft 6

By default, it runs with IEEE Std 802.1AB-2009 and sends IEEE 802.1AB Draft 6 LLDPDUs from ports that receive only IEEE 802.1AB Draft 6 LLDPDUs. Note that IEEE Std 802.1AB-2005 can also be connected. The following table shows the relationship between received LLDPDUs and sent LLDPDUs for each standard.

Table 24-1: Relationship between received LLDPDUs and sent LLDPDUs for each standard

Received LLDPDU standard		Sent LLDPDU standard
IEEE Std 802.1AB-2009 IEEE Std 802.1AB-2005	IEEE 802.1AB Draft 6	
Not received	Not received	IEEE Std 802.1AB-2009#
	Received	IEEE 802.1AB Draft 6
Received	Not received	IEEE Std 802.1AB-2009#
	Received	IEEE Std 802.1AB-2009#

#: Only the System Capabilities TLV is sent according to the IEEE Std 802.1AB-2005 standard.

(2) Support for TLV

The table below describes how TLV is supported on the Switch.

Table 24-2: Support for TLV

TLV name	IEEE 802.1AB Draft 6		IEEE Std 802.1AB-2009 IEEE Std 802.1AB-2005		Description
	Sending	Receiving	Sending#1	Receiving	
Chassis ID	Y	Y	Y	Y	Sends the MAC address of the Switch.
Port ID	Y	Y	Y	Y	Sends the MAC address of the port.
Time To Live	Y	Y	Y	Y	The retention time of information sent by the Switch can be changed in the configuration.
Port Description	Y	Y	Y	Y	Sends the same value as ifDescr in the interface group MIB.
System Name	Y	Y	Y	Y	Sends the same value as sysName in the system group MIB.
System Description	Y	Y	Y	Y	Sends the same value as sysDescr in the system group MIB.
System Capabilities	N	N	Y	Y	Send information on available and enabled functions.
Management Address	N	N	Y	Y	Sends the management address.
Organizationally-defined TLV extensions • VLAN information • VLAN Address information	Y	Y	N	N	Sends the configured VLAN ID and the IP address associated with the VLAN.

TLV name		IEEE 802.1AB Draft 6		IEEE Std 802.1AB-2009 IEEE Std 802.1AB-2005		Description
		Sending	Receiving	Sending#1	Receiving	
IEEE 802.1 Organizationally Specific TLVs	Port VLAN ID	N	N	Y	Y	Sends VLAN ID information for the configured port VLAN.
	Port And Protocol VLAN ID	N	N	Y	Y	Sends VLAN ID information for the configured protocol VLAN.
	VLAN Name	N	N	P#2	Y	Sends the VLAN ID of the configured port VLAN and the name of the VLAN.

Legend: Y: Supported, P: Partially supported, N: Not supported

#1

Sends LLDPDUs according to the IEEE Std 802.1AB-2009 standard. However, System Capabilities are sent according to the IEEE Std 802.1AB-2005 standard.

#2

The information of VLAN Name Length is sent as 0, and the VLAN name is not sent.

The following subsections describe the above information in detail.

(a) 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 24-3: List of Chassis ID subtypes (IEEE Std 802.1AB-2009)

subtype	Type	Value
1	Chassis component	The same value as entPhysicalAlias of the Entity MIB
2	Interface alias	The same value as ifAlias of the Interface MIB
3	Port component	The same value as portEntPhysicalAlias of the Entity MIB or the same value as backplaneEntPhysicalAlias of the Entity MIB
4	MAC address	The same value as macAddress of the LLDP MIB
5	Network address	The same value as networkAddress of the LLDP MIB
6	Interface name	The same value as ifName of the interface MIB
7	Locally assigned	The same value as local of the LLDP MIB

Table 24-4: List of Chassis ID subtypes (IEEE 802.1AB Draft 6)

subtype	Type	Value
1	Chassis component	The same value as entPhysicalAlias of the Entity MIB

subtype	Type	Value
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
7	Locally assigned	The same value as local of the LLDP MIB

The following are the sending and reception conditions for Chassis ID:

- Sending: The type of subtype to be sent is MAC address only. The value that will be sent is the device MAC address. Also, when configuring a stack, the device MAC address of the stack is used.
- Reception: Port ID with any subtype can be received.
- Maximum length of value that can be received: 255 octets

(b) Port ID (Port ID)

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 24-5: List of Port ID subtypes (IEEE Std 802.1AB-2009)

subtype	Type	Value
1	Interface alias	The same value as ifAlias of the Interface MIB
2	Port component	The same value as portEntPhysicalAlias of the Entity MIB or the same value as backplaneEntPhysicalAlias of the Entity MIB
3	MAC address	The same value as macAddr of the LLDP MIB
4	Network address	The same value as networkAddress of the LLDP MIB
5	Interface name	The same value as ifName of the interface MIB
6	Agent circuit ID	Circuit ID for RFC 3046
7	Locally assigned	The same value as local of the LLDP MIB

Table 24-6: List of Port ID subtypes (IEEE 802.1AB Draft 6)

subtype	Type	Value
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

subtype	Type	Value
6	Locally assigned	The same value as local of the LLDP MIB

The following are the sending and reception conditions for Port ID:

- Sending: The type of subtype to be sent is MAC address only. The value that will be sent is the MAC address of the port.
- Reception: Port ID with any subtype can be received.
- Maximum length of value that can be received: 255 octets

(c) Time-to-Live (Retention time for information)

Time-to-Live indicates how long the destination device will retain the distributed information.

Although you can change the retention time in configuration mode, we recommend that you do not change the initial value.

(d) Port description (port type)

Port Description is information that indicates the type of the port. This information does not have a subtype.

The following are the sending and reception conditions for System Description:

- Value to be sent: The same value as ifDescr of the Interface MIB
- Maximum length of value that can be received: 255 octets

(e) System name (device name)

System Name is information that indicates the name of the device. This information does not have a subtype.

The following are the sending and reception conditions for System Description:

- Value to be sent: The same value as sysName of the System MIB
- Maximum length of value that can be received: 255 octets

(f) System description (device type)

System Description is information that indicates the type of the device. This information does not have a subtype.

The following are the sending and reception conditions for System Description:

- Value to be sent: The same value as sysDescr of the System MIB
  If a stack is configured, sysDescr information of the master switch is used.
- Maximum length of value that can be received: 255 octets

(g) System Capabilities (device function)

Information that identifies available functions and enabled functions. This information may or may not have a subtype depending on the standard.

IEEE Std 802.1AB-2009

A subtype is defined and the chassis ID subtype is used for the subtype.

IEEE Std 802.1AB-2005
There is no subtype.

The value to be sent and reception conditions for System Capabilities are as follows.

- Sending
  Sends according to the IEEE Std 802.1AB-2005 standard. The following table shows the value to be sent of the System Capabilities TLV.

Table 24-7: Value to be sent of System Capabilities TLV

Data name	Description	Value
system capabilities	Function identifier (function possessed by the device)	MAC Bridge (1) Yes Router (1) Yes
enabled capabilities	Among function identifiers, function that is enabled	MAC Bridge (1) Enabled Router (1) Enabled

- Receiving
  Reception is possible according to IEEE Std 802.1AB-2009 and IEEE Std 802.1AB-2005 standards. The IEEE Std 802.1AB-2009 standard allows reception of all subtypes.

(h) Management Address

Information that identifies the IP address and MAC address of a Switch. This information has a subtype, and the value to be sent changes according to the subtype.

The following are the value to be sent and reception conditions for Management Address:

- Sending
  The following table shows the value to be sent of the Management Address TLV.

Table 24-8: Value to be sent of Management Address TLV

Data name	Description	Value set
management address subtype	Management address types	1: IP (IPv4 address) or 2: IP6 (IPv6 address)
management address	Management address	Use the address set by the configuration command lldp management-address
interface numbering subtype	Interface number subtype	1: Unknown
OID string length	OID information length	0

- Receiving
  Allows reception of all subtypes. If there are multiple Management Address TLVs on the LLDPDU, only the last information is retained.
- Maximum length of value that can be received
  167 octets

(i) Organizationally-defined TLV extensions

The organizationally defined TLV extensions supported by the Switch are as follows.

- VLAN ID

  VLAN ID indicates the VLAN tag used by the port. If the tag translation function is used, VLAN ID indicates the VLAN ID after translation. Note that VLAN ID is information that is effective on only trunk ports.

- VLAN Address

  VLAN Address indicates the smallest VLAN ID of the port's VLANs that have IP addresses as well as the IP address of that VLAN.

(j) IEEE 802.1 Organizationally Specific TLVs

The Switch supports the following information.

- Port VLAN ID

  This is the port VLAN information for the target port.

  For access ports, the VLAN ID of the target port VLAN is sent. For ports other than access ports, the VLAN ID of the native VLAN is sent when the native VLAN is enabled. Maximum length of value that can be received is 6 octets.

- Port And Protocol VLAN ID

  This is the protocol VLAN information for the target port.

  For protocol ports, the VLAN ID of the target protocol VLAN is sent. The VLAN ID information to be sent is the latest. If the protocol VLAN is not set, the protocol VLAN information is not sent. Maximum length of value that can be received is 7 octets.

- VLAN Name

  This is the port VLAN information for the target port.

  For access ports, the VLAN ID of the target port VLAN is sent. For trunk ports, the VLAN ID of the VLAN Tag is sent. When the native VLAN is enabled, the VLAN ID of the native VLAN is also sent. For ports other than access ports and trunk ports, the VLAN ID of each port is sent. When the native VLAN is enabled, the VLAN ID of the native VLAN is also sent.

  The VLAN ID information to be sent is the latest. Also, when Tag translation is used, VLAN ID after translation is sent, and when the VLAN tunneling function is used, VLAN ID of VLAN Tag attached by the VLAN tunneling function is sent. Maximum length of value that can be received is 39 octets.

24.1.3 Notes on using LLDP

(1) When used with the Layer 2 switch function

See "Configuration Guide Vol. 1, 22.3 Compatibility between the Layer 2 switch function and other functions".

(2) Connecting a device that does not support LLDP between neighboring devices that support LLDP

If using a configuration described below, it is difficult to know the exact status of the connection between neighboring devices for the following reasons:

- If a switch is connected between neighboring devices, the information distributed over LLDP from one neighboring device is forwarded by the switch to the other neighboring device. In this case, the device that receives the distributed information is unable to determine whether the received information is information about the other device or information about the device.

- If a router is connected between neighboring devices, the information distributed over LLDP from one device does not arrive at the other device, because the router discards the distributed information.

(3) Maximum number of neighboring devices

The distributed information about any neighboring devices exceeding the capacity limit is discarded. Note that the discarding of information is suppressed for a period of time to provide time within which the retention of saved information might time out. Note, however, that the maximum suppression time is the retention time for the neighboring device information to be discarded.

(4) Using with the VRF function [SL-L3A]

When the VRF function is enabled for VLANs, the IP addresses set to the VLANs are not distributed.

(5) In a stack configuration

In a stack configuration, when a switchover of the master switch occurs, information on neighboring devices is cleared. After that, it re-learns by receiving LLDPDU from a neighboring device.

24.2 Configuration

24.2.1 List of configuration commands

The following table describes the list of configuration commands for LLDP.

Table 24-9: List of configuration commands

Command name	Description
lldp enable	Enables operation of LLDP for a port.
lldp hold-count	Specifies how long the LLDP frames sent from the Switch to neighboring devices will be retained on the neighboring devices.
lldp interval-time	Specifies the interval at which the Switch sends LLDP frames.
lldp management-address	Sets the management address of the Management Address TLV to be sent.
lldp run	Enables LLDP for the entire device.

24.2.2 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.

The example below enables LLDP for gigabitethernet 1/0/1.

Command examples

1. `(config)# lldp run`
   Enables LLDP for the entire device.
2. `(config)# interface gigabitethernet 1/0/1`
   Switches to the Ethernet interface configuration mode for port 1/0/1.
3. `(config-if)# lldp enable`
   Starts behavior of LLDP function at port 1/0/1.

(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 retention time during which the destination-neighboring device will retain the information it received from the Switch. The sending interval time multiplied by the number of sending intervals specified here creates the retention time. In this example, the retention time is 180 seconds (60 seconds x 3).

(3) Configuring the management address to be sent

Points to note

When you set the management address, the set IP address is notified to neighboring devices. The IP address that can be set is not limited to the IP address set on the interface.

Command examples

1. `(config)# lldp management-address ip 192.168.1.20`

   Sets the management address of the Management Address TLV to be sent to 192.168.1.20.

24.3 Operation

24.3.1 List of operation commands

The following table describes the list of operation commands for LLDP.

Table 24-10: List of operation commands

Command name	Description
show lldp	Shows the configuration and neighboring device information for LLDP.
show lldp statistics	Shows LLDP statistics.
clear lldp	Clears the neighboring device information for LLDP.
clear lldp statistics	Clears the LLDP statistics.
restart lldp	Restarts the LLDP program.
dump protocols lldp	Dumps detailed event trace information and control table information collected by the LLDP program to a file.

24.3.2 Displaying LLDP information

LLDP information can be displayed by using the "show lldp" operation command. The "show lldp" command displays the LLDP settings and the number of neighboring devices for each port. The "show lldp detail" command displays detailed information about neighboring devices.

Figure 24-2: Result of executing the show lldp command

```
> show lldp
Date 20XX/11/09 19:16:20 UTC
Status: Enabled Chassis ID: Type=MAC      Info=0012.e268.2c21
Interval Time: 30   Hold Count: 4  TTL:120
Port Counts=3
1/0/1 (CH:10)  Link:Up    Neighbor Counts:  2
1/0/2          Link:Down  Neighbor Counts:  0
2/0/3          Link:Up    Neighbor Counts:  0
>
```

25 OADP

The Octpower Auto Discovery Protocol (OADP) is a function used for the collection of information about the devices that are neighbors of the Switch. This chapter describes OADP and its use.

25.1 Description

25.1.1 Overview

(1) Overview of the OADP function

The Octpower Auto Discovery Protocol (OADP) is a function that runs at the Layer 2 level of the Switch. OADP is used to collect information about neighboring devices by the exchange of OADP PDUs (Protocol Data Units) among devices.

The information can then be used to show the status of connections to neighboring devices. With this function, you can easily understand the status of connections to neighboring devices from the device and port information that is displayed. You can also use this function to check the status of a connection between devices without logging in to the neighboring devices or viewing a network configuration diagram. Furthermore, you can verify the correctness of a device connection by comparing the connection status information displayed by using this function against a network configuration diagram.

The devices that the Switch can recognize as neighboring devices are devices implementing OADP (including Switches) and devices implementing CDP.

(2) Overview of the CDP reception function

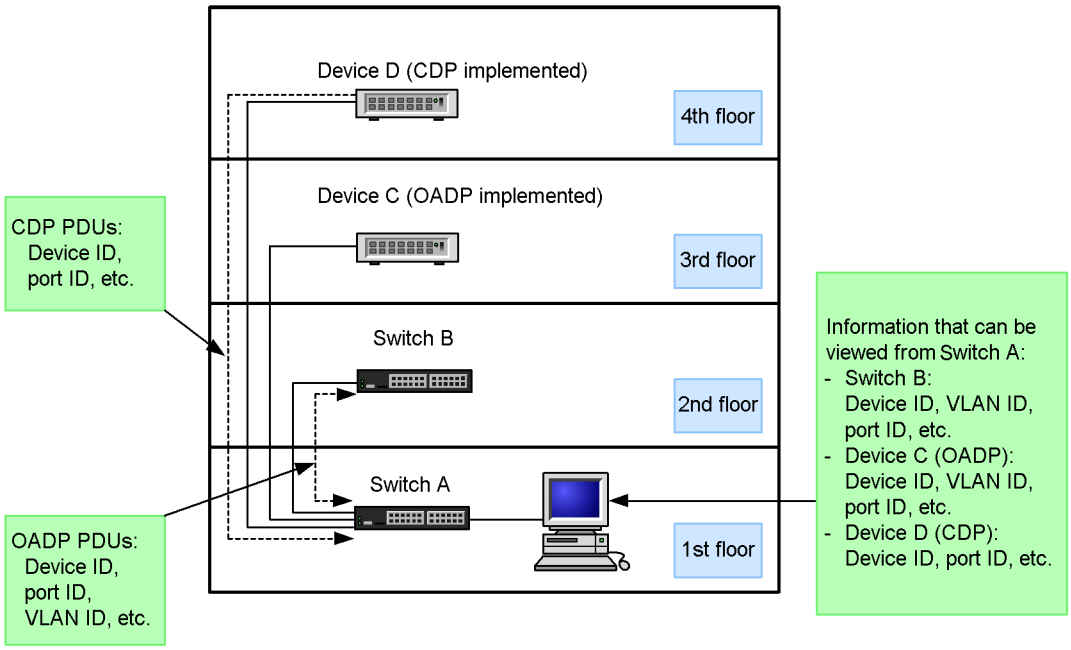
Because OADP can interpret the Cisco Discovery Protocol (CDP), the status of connections to neighboring devices that send CDP PDUs can also be checked from the Switch. Note, however, that the Switch does not send CDP PDUs. CDP runs at the Layer 2 level on Cisco Systems' devices to detect neighboring devices.

(3) Example of using OADP

OADP allows a local device to send its own device and port information to the ports of neighboring devices connected to the local device. The device and port information includes the device ID, port ID, IP address, and VLAN ID. By managing the received information, the operator at the local device can check the status of connections to neighboring devices.

The figure below shows an example of using OADP. 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 same building.

Figure 25-1: Example of using the OADP



25.1.2 Supported specifications

(1) Specifications supported by OADP

The following table describes the specifications supported by OADP.

Table 25-1: Functions and settings supported by OADP and their specifications

Item		Description
Applicable layer	Layer 2	Y
	Layer 3	N
Sending and receiving OADP PDUs		On a physical port basis or link aggregation basis
Reset function		Y
OADP PDU sending interval		Can be set in seconds in the range from 5 to 254.
OADP PDU retention time		Can be set in seconds in the range from 10 to 255.
CDP reception function		Y

Legend Y: Supported; N: Not supported

(2) Information used for OADP

The following table describes the information contained in OADP PDUs.

Table 25-2: Information supported by OADP

No.	Name	Description
1	Device ID	Identifier that uniquely identifies the device

No.	Name	Description
2	Address	Address associated with the interface from which OADP PDUs are sent, and the address of the loopback interface
3	Port ID	Identifier of the port from which OADP PDUs are sent
4	Capabilities	Device function
5	Version	Software version
6	Platform	Platform
7	Duplex	Duplex information for the port from which OADP PDUs are sent
8	ifIndex	ifIndex of the port from which OADP PDUs are sent
9	ifSpeed	ifSpeed of the port from which OADP PDUs are sent
10	VLAN ID	VLAN ID of the port from which OADP PDUs are sent
11	ifHighSpeed	ifHighSpeed of the port from which OADP PDUs are sent

The following table describes the information that might be received in CDP PDUs. Items 1 to 7 are the same as the items in OADP PDUs.

Table 25-3: Information supported by CDP

No.	Name	Description
1	Device ID	Identifier that uniquely identifies the device
2	Address	Address associated with the port from which CDP PDUs are sent
3	Port ID	Identifier of the port from which CDP PDUs are sent
4	Capabilities	Device function
5	Version	Software version
6	Platform	Platform
7	Duplex	Duplex information for the port from which CDP PDUs are sent

25.1.3 Notes on using OADP

(1) Connecting a device that does not support OADP between neighboring devices that support OADP

If using a configuration described below, it is difficult to know the exact status of the connection between neighboring devices for the following reasons:

- If a switch is connected between neighboring devices, the information distributed by OADP from one neighboring device is forwarded by the switch to the other neighboring device. In this case, the device that receives the information is unable to determine whether the received information is information about the other device or information about the device.
- If a router is connected between neighboring devices, the information distributed over OADP from one device does not arrive at the other device, because the router discards the distributed information.

(2) Maximum number of neighboring devices

The device can handle information for a maximum of 100 neighboring devices. The distributed information about any devices exceeding the maximum is discarded. Note that the discarding of information is suppressed for a period of time to provide time within which the retention of saved information might time out. Note, however, that the maximum suppression time is the retention time for the neighboring device information to be discarded.

(3) VLAN of a port that uses OADP

OADP sends and receives OADP PDUs over the VLAN set for the port. If the VLAN is disabled by using the "state suspend" command, OADP does not run over the VLAN.

(4) Connecting a device implementing CDP

When you connect the device to a device implementing CDP by using a trunk port, make sure that the native VLAN of the port is not disabled by using the "state suspend" command. If the native VLAN is disabled, the Switch discards CDP PDUs.

(5) Replacing an L2 switch with a Switch between devices implementing CDP

When you replace with a Switch an L2 switch through which CDP PDUs pass between devices implementing CDP, do not use the "oadp cdp-listener" command to enable the CDP reception function of the Switch. If you enable the functionality, CDP PDUs do not pass through the Switch because they are received by the Switch. As a result, the devices implementing CDP no longer recognize each other. If you want CDP PDUs to pass through the new Switch (that is, you want the devices recognize each other) after replacement, do not enable the CDP reception function.

(6) Using with the VRF function [SL-L3A]

IP addresses are not distributed when sending device information to VLANs for which the VRF function is enabled.

25.2 Configuration

25.2.1 List of configuration commands

The following table describes the list of configuration commands for OADP.

Table 25-4: List of configuration commands

Command name	Description
oadp cdp-listener	Enables the CDP reception function.
oadp enable	Enables OADP for a port or link aggregation.
oadp hold-time	Specifies how long the OADP frames sent from the Switch to neighboring devices will be retained on the neighboring devices.
oadp ignore-vlan	Specifies that any OADP frames received from the VLAN specified by the VLAN ID are to be ignored.
oadp interval-time	Specifies the interval at which the Switch sends OADP frames.
oadp run	Enables OADP for the entire device.

25.2.2 Configuring OADP

(1) Configuring OADP

Points to note

Configuration of OADP requires enabling of OADP for the entire device, and then enabling of OADP for the port for which it will be used.

If the port for which OADP will be used is a member of a link aggregation, enable the function for the relevant port channel interface.

The example below enables OADP for gigabitethernet 1/0/1.

Command examples

1. `(config)# oadp run`
   Enables OADP for the entire device.
2. `(config)# interface gigabitethernet 1/0/1`
   Switches to the Ethernet interface configuration mode for port 1/0/1.
3. `(config-if)# oadp enable`
   Initiates behavior of OADP on port 1/0/1.

Notes

The OADP runs only on active VLANs for the port. It does not run on suspended VLANs.

(2) Setting the sending interval and retention time of OADP frames

Points to note

How often neighboring device information is updated can be adjusted by changing the sending interval for sending OADP frames. If the sending interval is decreased, the information is updated more often, but the load on the local and neighboring devices might increase. If the sending interval is increased, the load might decrease, but the information is updated less often. Normally, you do not change this setting.

Command examples

1. `(config)# oadp interval-time 60`
   Sets 60 seconds as the interval for sending OADP frames.
2. `(config)# oadp hold-time 180`
   Sets 180 seconds as the time during which the information sent from the Switch will be retained on the neighboring devices.

(3) Configuring the CDP reception function

Points to note

If the CDP reception function is enabled, it runs on all ports on which OADP is running.

In this example, the CDP reception function operates on gigabitethernet 1/0/1.

Command examples

1. `(config)# interface gigabitethernet 1/0/1`
   Switches to the Ethernet interface configuration mode for port 1/0/1.
2. `(config-if)# oadp enable`
   Enables OADP for port 1/0/1.
3. `(config-if)# exit`
   Changes the mode from Ethernet interface configuration mode to global configuration mode.
4. `(config)# oadp cdp-listener`
   Enables the CDP reception function. The CDP reception function starts on the ports on which OADP is running.

(4) Setting VLANs that ignore OADP frames

Points to note

For a trunk port to which multiple VLANs belong, OADP sends and receives multiple OADP frames through the port by using VLAN tags. If the number of VLANs that belong to the port increases, the amount of neighboring device information also increases, adding to the load on the devices. The device load can be reduced by setting some of the VLANs to ignore received OADP frames.

Command examples

1. `(config)# oadp ignore-vlan 10-20`
   Sets VLANs 10 to 20 to ignore received OADP frames.

25.3 Operation

25.3.1 List of operation commands

The following table describes the list of operation commands for OADP.

Table 25-5: List of operation commands

Command name	Description
show oadp	Shows the configuration and neighboring device information for OADP and CDP.
show oadp statistics	Shows OADP and CDP statistics.
clear oadp	Clears the neighboring device information for OADP and CDP.
clear oadp statistics	Clears OADP/CDP statistics.
restart oadp	Restarts the OADP program.
dump protocols oadp	Dumps detailed event trace information and control table information collected by the OADP program to a file.

25.3.2 Displaying OADP information

OADP information can be displayed by using the "show oadp" operation command. The "show oadp" command displays the OADP settings and basic information for each port. The "show oadp detail" command displays detailed information about neighboring devices.

Figure 25-2: Result of executing the show oadp command

```
> show oadp
Date 20XX/11/09 19:50:20 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20
              CH 10

Total Neighbor Counts=2
Local VID Holdtime Remote    VID Device ID     Capability Platform
0/1   0         35 0/8       0    OADP-2       RS         AX3640S-24TW
0/16  0         9  0/1       0    OADP-3       S          AX2430S-48T

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
>
```

Figure 25-3: Results of executing the show oadp detail command

```
> show oadp detail
Date 20XX/11/09 19:55:52 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20

Total Neighbor Counts=2
------------------------------------------------------------------------------
Port: 0/1   VLAN ID: 0
Holdtime      : 6(sec)
Port ID       : 0/8   VLAN ID(TLV): 0
Device ID     : OADP-2
Capabilities  : Router, Switch
Platform      : AX3640S-24TW
```

```
Entry address(es):
    IP address    : 192.16.170.87
    IPv6 address  : fe80::200:4cff:fe71:5d1c
IfSpeed       : 1G   Duplex     : FULL
Version       : ALAXALA AX3640S AX-3640-24TW-A [AX3640S-24TW] Switching software Ver. 11.6 [OS-
L3A]
------------------------------------------------------------------------------
Port: 0/16   VLAN ID: 0
Holdtime      : 10(sec)
Port ID       : 0/1   VLAN ID(TLV): 0
Device ID     : OADP-3
Capabilities  : Switch
Platform      : AX2430S-48T
Entry address(es):
    IP address    : 192.16.170.100
IfSpeed       : 1G   Duplex     : FULL
Version       : ALAXALA AX2430S AX-2430S-48T [AX2430S-48T] Switching software Ver. 11.6 [OS-L2]
------------------------------------------------------------------------------
>
```

26 PTP

PTP is a function that synchronizes time with high precision (up to several hundred nanoseconds). This chapter describes PTP and its operations.

26.1 Description

26.1.1 Overview

PTP (Precision Time Protocol) is a protocol for time synchronization. It is specialized for use in Ethernet and aims to synchronize with higher accuracy (up to several hundred nanoseconds) than NTP (up to several milliseconds).

In PTP, the time during which packets are relayed between the master device and slave device (hereafter referred to as Transmission delay time) is measured, and the time is synchronized using the time information sent from the master device and the transmission delay time. The following table shows the role of each device in PTP.

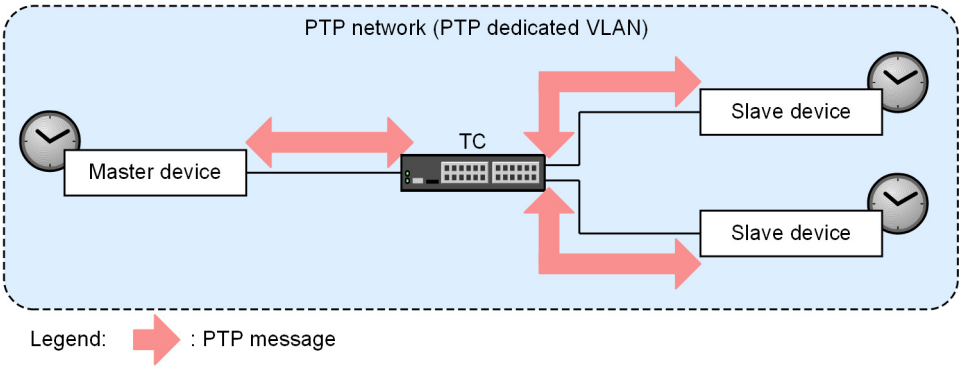
Table 26-1: Role of each device in PTP

Type of PTP device	Description
Master device	A device that distributes the reference time
Slave device	A device that synchronizes with the reference time received from the master device
Transparent Clock (TC)	A device that relays PTP messages for calculating transmission delay time
Management Node (MN)	Remote controller

The Switch runs as a TC. The master device, slave device and MN are not supported.

The PTP device synchronizes the time through the PTP-dedicated VLAN. The figure below shows an example of using PTP.

Figure 26-1: Example of using PTP



(1) Transmission delay measurement method

There are E2E (end-to-end) and P2P (peer-to-peer) methods for measuring PTP transmission delay time. The following table shows the features of E2E and P2P.

Table 26-2: Features of E2E and P2P

Item	E2E	P2P
Transmission delay time measurement unit	Measure transmission delay time between the master device and slave device	Measure the transmission delay time between the master device/ slave device/TC and neighboring devices on each device

Item	E2E	P2P
Possibility of connecting to devices that do not support PTP	Can be connected	Cannot be connected
Degradation of synchronization accuracy due to the number of hops	Large deterioration	Small deterioration
Processing load on the master device due to the number of slave devices	Large impact	Small impact

(2) Send time notification method

In PTP, the time when the PTP message was sent (send time) is used to measure the transmission delay time. There are two types of send time notification methods: One-step clock and Two-step clock.

Table 26-3: Send time notification method

Send time notification method	Overview
One-step clock	This is a method of notifying the send time by one message.
Two-step clock	This is a method of notifying the send time by two messages.

26.1.2 Supported function

The following table describes the function of PTP supported by the Switch.

Table 26-4: Supported function

Item		Support
Interface type	Ethernet interface	Y
	Port channel interface	N
	Management port	N
VLAN type	Port VLAN	Y
	Protocol VLAN	N
	MAC VLAN	N
Frame format for transferring PTP messages	IEEE 802.3-MAC	N
	UDP/IPv4	Y
	UDP/IPv6	N
Type of destination address	Multicast	Y
	unicast	N
Supported PTP version		PTP Version 2

Item			Support
PTP device type	Master device		N
	Slave device		N
	TC	E2E-TC	Y
		P2P-TC	N
	MN		N
Send time notification method	E2E	One-step clock	Y
		Two-step clock	N
Management function			N

Legend Y: Supported; N: Not supported

(1) PTP message

The following table shows the messages used in PTP E2E and the intended use.

Table 26-5: PTP messages and intended use

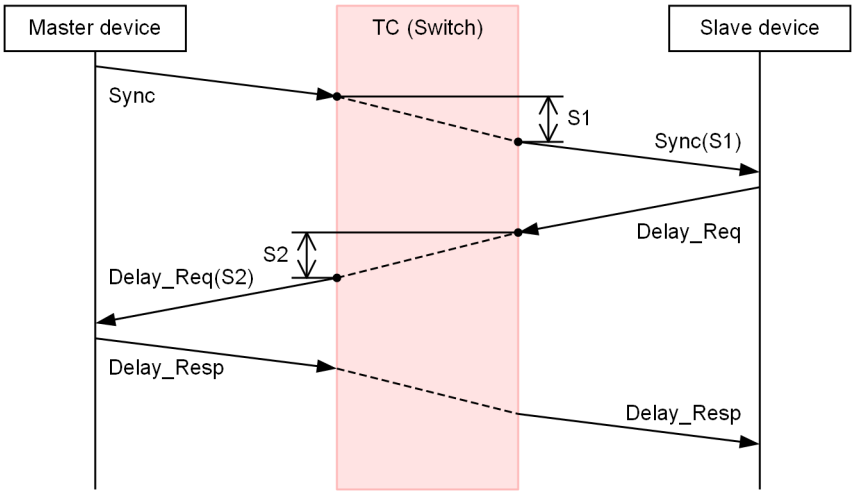
Message type		Intended use
Master determination	Announce	Message used for determining the PTP master Periodic transmissions are performed at the interval (Announce Interval) set by the master and slave devices.
Time synchronization	Sync	Time synchronization message from the master device to slave device Periodic transmissions are performed at the interval (Sync Interval) set by the master device.
	Follow_Up	Time synchronization message from the master device to slave device
Average transmission delay time measurement	Delay_Req	A message that measures the average transmission delay time between the master device and slave device
	Delay_Resp	A message that measures the average transmission delay time between the master device and slave device
Obtain and set each PTP device information	Management	Messages for obtaining and setting information for each PTP device#

#: The Switch supports only the NOT_SUPPORTED response.

26.1.3 Behavior of E2E-TC

When relaying Sync messages and Delay_Req messages, the Switch adds the relay delay time within the Switch to each message before sending. The relay delay time is not added to other PTP messages. The following figure shows an overview of the Switch behavior with E2E-TC.

Figure 26-2: Overview of the Switch behavior with E2E-TC



(Legend) S1: Sync message relay delay time in TC (Switch)
S2: Delay_Req message relay delay time in TC (Switch)

26.1.4 Notes on using PTP

(1) Use with other function

(a) When used with the Layer 2 switch function

See "Configuration Guide Vol. 1, 22.3 Compatibility between the Layer 2 switch function and other functions".

(b) When used with Layer 2 authentication

For details, see "5.2.1 Using Layer 2 authentication with other functions".

(c) When used with other function

The following table describes other function that cannot be used, or only partially used, with PTP.

Table 26-6: Possibility of coexistence of PTP and other function

Function	Restrictions
Filter (Inbound)	Can only be partially used#
DHCP snooping	Cannot be used
VRRP	
Uplink redundancy	
L2 loop detection	
Policy-based mirroring	
sFlow statistics	
IEEE 802.3ah/UDLD	

Function	Restrictions
CFM	
LLDP	
OADP	
DHCP/BOOTP relay agent	
DHCP server	
RIP	
OSPF	
BGP4	
IPv6 DHCP Relays	
IPv6 DHCP server	
RIPng	
OSPFv3	
BGP4+	
BFD	
VRF	

PTP messages addressed to the device cannot be discarded.

(2) Receiving PTP messages other than UDP/IPv4

The Switch does not respond when receiving unsupported IEEE 802.3-MAC and UDP/IPv6 PTP messages.

(3) Receiving PTP messages with VLAN tags

The Switch supports PTP messages without VLAN tags and PTP messages with one-step VLAN tags. PTP messages with two-step or more VLAN tags are not supported.

(4) Notes on using IPv4 multicast

When using PTP and IPv4 multicast on the same port, connect a PTP-supported device after setting PTP. If a PTP-supported device is connected before PTP is enabled, PTP messages may not be relayed temporarily after PTP is enabled.

(5) Notes on using the Layer 2 forwarding block function

PTP messages are not blocked even if the Layer 2 forwarding block function is used.

(6) Notes on using IGMP snooping

PTP messages are flooded regardless of the IGMP snooping entry.

(7) Notes applying when port mirroring is used

When mirroring sent frames using a PTP-enabled port as a monitor port, the relay delay time included in the mirrored PTP message will be a different value from the relay delay time included in the PTP message to be mirrored.

26.2 Configuration

26.2.1 List of configuration commands

The following table describes the list of configuration commands for PTP.

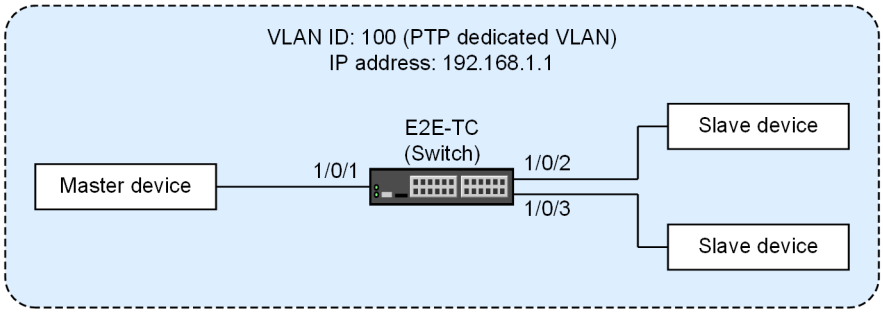
Table 26-7: List of configuration commands

Command name	Description
ptp description	Sets supplementary information.
ptp enable	Enables PTP for the target port.
ptp run	Enables PTP on the Switch and specify the communication function.
ptp source-interface	Specifies the source VLAN and IP address when sending PTP messages.

26.2.2 Configuring E2E-TC

The following figure shows a configuration example of E2E-TC.

Figure 26-3: configuration example of E2E-TC



Points to note

For the VLAN ID and IPv4 address specified for the PTP interface, set the VLAN ID and IPv4 address set for the VLAN interface. Also, set the PTP message priority (CoS) of the Switch to 7 (highest priority) to minimize fluctuations in the relay delay time of PTP messages.

Note that PTP must be enabled on all ports that send and receive PTP messages.

Command examples

1. `(config)# interface vlan 100`

   Creates VLAN ID 100 as port VLANs. Switches to VLAN configuration mode.

2. `(config-if)# ip address 192.168.1.1 255.255.255.0`

   `(config-if)# exit`

   Sets the IPv4 address 192.168.1.1 and the subnet mask 255.255.255.0 for VLAN 100.

3. `(config)# ptp source-interface vlan 100 ip-address 192.168.1.1`

   Sets VLAN 100 and IPv4 address 192.168.1.1 for the PTP interface.

4. `(config)# ip qos-flow-list PTP_PRIORITY`
   `(config-ip-qos)# qos udp any host 224.0.1.129 range 319 320 action cos 7`
   `(config-ip-qos)# exit`
   Creates an IPv4 QoS flow list (PTP_PRIORITY) and sets the PTP message frame priority to 7.
5. `(config)# interface range tengigabitethernet 1/0/1-3`
   Switches to the interface mode for ports 1/0/1 to 1/0/3.
6. `(config-if-range)# switchport mode access`
   `(config-if-range)# switchport access vlan 100`
   Sets ports 1/0/1 to 1/0/3 as access ports. Then, sets VLAN 100.
7. `(config-if-range)# ptp enable`
   Enables PTP for ports 1/0/1 to 1/0/3.
8. `(config-if-range)# ip qos-flow-group PTP_PRIORITY in`
   `(config-if-range)# exit`
   Enables the IPv4 QoS flow list (PTP_PRIORITY) on the receiving side for ports 1/0/1 to 1/0/3.
9. `(config)# ptp run e2e-tc`
   Sets the Switch to E2E-TC.
10. `(config)# save`
    `(config)# exit`
    Saves the settings and moves from configuration command mode to administrator mode.

26.3 Operation

26.3.1 List of operation commands

The following table describes the operation commands for PTP.

Table 26-8: List of operation commands

Command name	Description
show ptp	Displays the PTP information and the status of ports.
restart ptp	Restarts the PTP program.
dump protocols ptp	Dumps detailed event trace information and control table information collected by the PTP program to a file.

26.3.2 Checking the status of the PTP

(1) Checking the configuration settings and operation statuses

Use the "show ptp" command to check the PTP settings and operating status. You can check whether the PTP configuration set with configuration commands is correct.

Figure 26-4: Results of executing the show ptp command

```
> show ptp
Date 20XX/09/01 12:00:00 UTC
Clock types: E2E-TC
PTP profile information
  Profile name: AlaxalA PTP profile for AX3660S
  Profile version: 1.0
  Profile identifier: 0012.e200.0100
Clock description
  Manufacturer identity: 00-12-E2
  Product description: AlaxalA xxxxxxxxxxxxxxx
  Revision data: 1.0;1.0;1.0
  User description: E2E-TC NODE 101
  Profile identity: 0012.e200.0100
Transport mechanism protocol: IPv4
Source interface: VLAN 1000 (100.100.100.1)
Primary domain: 0
Port counts: 4
  Port      Port Identity
  1/0/1     0012.e2ff.fe00.0100:100
  1/0/2     0012.e2ff.fe00.0100:101
  1/0/10    0012.e2ff.fe00.0100:109
  1/0/20    0012.e2ff.fe00.0100:119
>
```

Appendix

A. Compliance standards

A.1 Diff-serv

Table A-1: Compliance standards and recommendations for Diff-serv

Name (month and year issued)	Title
RFC 2474 (December 1998)	Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers
RFC 2475 (December 1998)	An Architecture for Differentiated Services
RFC 2597 (June 1999)	Assured Forwarding PHB Group
RFC 3246 (March 2002)	An Expedited Forwarding PHB (Per-Hop Behavior)
RFC 3260 (April 2002)	New Terminology and Clarifications for Diffserv

A.2 IEEE 802.1X

Table A-2: Compliance standards and recommendations for IEEE 802.1X

Name (month and year issued)	Title
IEEE 802.1X (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 3162 (August 2001)	RADIUS and IPv6
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.3 Web authentication

Table A-3: Compliance 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
RFC 3162 (August 2001)	RADIUS and IPv6

A.4 MAC-based authentication

Table A-4: Compliance 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
RFC 3162 (August 2001)	RADIUS and IPv6

A.5 DHCP snooping

Table A-5: Compliance standards and recommendations for DHCP snooping

Name (month and year issued)	Title
RFC 2131 (March 1997)	Dynamic Host Configuration Protocol

A.6 VRRP

Table A-6: Compliance standards and recommendations for VRRP

Name (month and year issued)	Title
RFC 3768 (April 2004)	Virtual Router Redundancy Protocol
draft-ietf-vrrp-ipv6-spec-02 (March 2002)	Virtual Router Redundancy Protocol for IPv6
draft-ietf-vrrp-ipv6-spec-07 (October 2004)	Virtual Router Redundancy Protocol for IPv6

A.7 sFlow

Table A-7: Compliance standards and recommendations for sFlow

Name (month and year issued)	Title
RFC 3176 (September 2001)	InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks

A.8 IEEE 802.3ah/UDLD

Table A-8: Compliance standards and recommendations for IEEE 802.3ah/UDLD

Name (month and year issued)	Title
IEEE 802.3ah (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.9 CFM

Table A-9: Compliance standards and recommendations for CFM

Name (month and year issued)	Title
IEEE 802.1ag-2007 (December 2007)	Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management

A.10 LLDP

Table A-10: Compliance standards and recommendations for LLDP

Name (month and year issued)	Title
IEEE 802.1AB/D6.0 (October 2003)	Draft Standard for Local and Metropolitan Networks: Station and Media Access Control - Connectivity Discovery
IEEE Std 802.1AB-2009 (September 2009)	IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity Discovery

A.11 PTP

Table A-11: Compliance standards and recommendations for PTP

Name (month and year issued)	Title
IEEE Std 1588-2008 (July 2008)	IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems