The Guaranteed Network

Closer to you, Further into the future.

AX Series
Policy-based Routing Configuration Guide

Edition 1

Document No. NTS-11-R-041

ALAXALA Networks Corporation

Preface

This document informs system engineers of the technologies required to implement a layer-3 network system that determines routes based on the system policy by using the policy-based routing functionality of ALAXALA Network's AX series. This information helps system engineers understand overall operation, integrate the system, and ensure stable operation.

Related documents

- AX series product manuals (http://www.alaxala.com/en/techinfo/manual/index.html)

Notes on using this document

The information in this document is based on the basic operations verified under the environment specified by ALAXALA and does not guarantee operations regarding functionality, performance, and reliability under all environment requirements. Please understand that this document is intended to help with system configuration for our products.
Unless otherwise stated, the OS software version as of the creation of this document is as shown below.

AX3650S	Ver. 11.7
AX1200S	Ver. 2.3

The contents of this document are subject to change without prior notice due to product improvement.

Export restrictions

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

Trademarks

- The ALAXALA name and logo are trademarks and registered trademarks of ALAXALA Networks Corporation.
- Ethernet is a product name of Xerox Corporation.
- Other company and product names in this document are trademarks or registered trademarks of their respective owners.

Revision history

Edition	Rev.	Date	Description	Modified
First	--	February 29, 2012	First edition	--

Contents

1. Changing Routes Based on the Purpose or the Type of Communication

1.1 What is policy-based routing?

The communication route in the layer−3 network is typically determined based on the routing table that contains the routing information. However, you might wish to forward particular communications that match specific conditions to different routes than usual, to be handled by dedicated devices or to go through other lines according to the purpose or application type of the communication. You can satisfy such needs using policy-based routing.

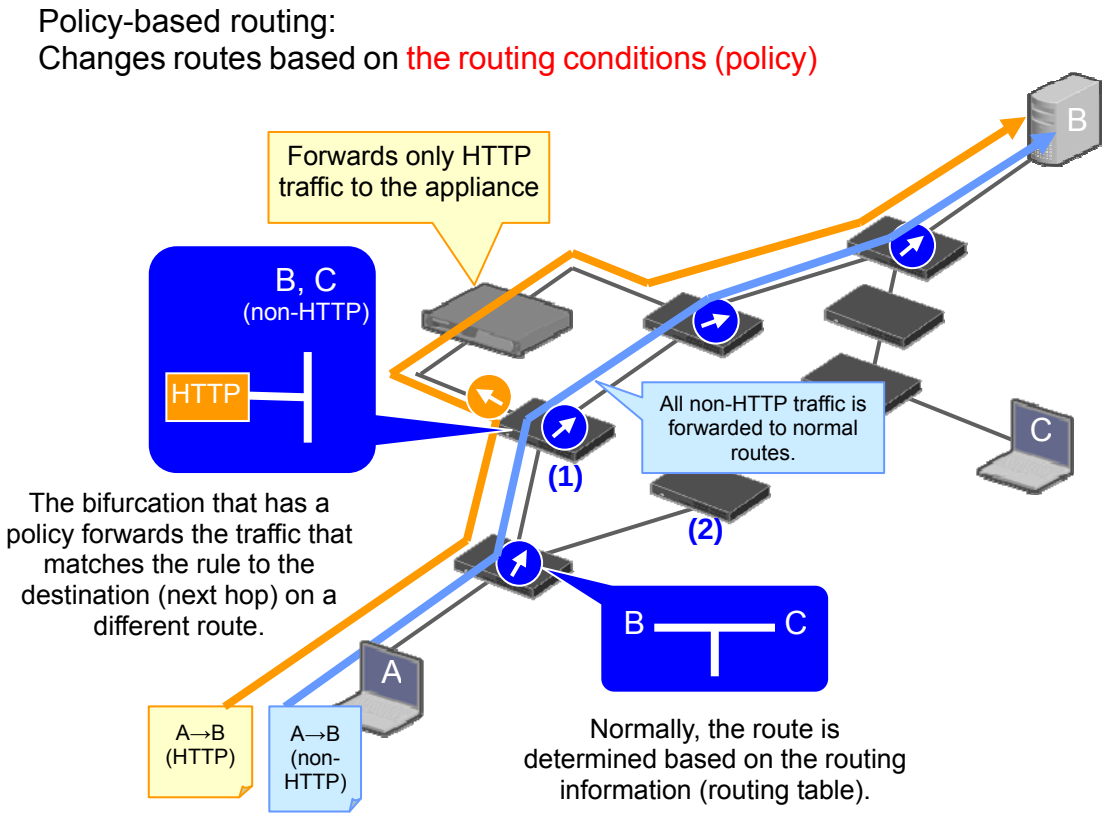


Figure 1.1-1: Overview of policy-based routing

Policy-based routing functions as a kind of access filter that is defined at the receiving VLAN interface. Therefore, route-changing conditions can be configured in the same way as in setting up the search conditions of an access filter.

An access filter only discards or passes the packet that matches the conditions, while policy-based routing forwards the communication traffic that matches the specified destination (next hop).

1.2 Applicable products and support functions

The table below lists the models that support policy-based routing and the overview of support functions.

1.2.1 Applicable models

Policy-based routing can be applied to the following products and software versions.

Table 1.2-1: Applicable products and supported functions

Applicable products and supported functions		Chassis-type switches	Box-type switches	
		AX6700S AX6600S AX6300S	AX3650S	AX3640S
Software version		Ver. 11.7 or later	Ver. 11.7 or later#1	
Policy-based routing	IPv4	○	○	○
	IPv6	○	--	--
	Tracking functionality	○ #2	○	○
VRF-enabled		○	○	--

#1: Advanced software only
#2: IPv4 only

1.2.2 Capacity limit

The following table provides the capacity limit for policy-based routing.

Table 1.2-2: Capacity limit for policy-based routing

Applicable products and capacity limit	Chassis-type switches	Box-type switches	
	AX6700S AX6600S AX6300S	AX3650S	AX3640S
Maximum number of access entries (that is, the number of policies that can be configured)	(Standard) 4000 (Extended) 32000	2048	512
Maximum number of next-hop entries (when configured directly in the access list)	256	-- #2	-- #2
Maximum number of policy-based routing lists that can be configured	256#1	256	256
Maximum number of routes that can be set in a single policy-based routing list	8#1	8	8
Maximum number of tracking settings	1024#1	1024	1024

#1: IPv4 only
#2: On box-type switches, the next hops can be defined only in the format of the policy-based routing list.

1.2.3 Features of policy-based routing in the AX series

The features of policy-based routing as supported in AX-series products are as follows.

(1) Multiple destinations (next hops) can be specified with a single condition, and redundant routes can also be set (IPv4 only).

Multiple next hops can be set for a single route changing condition (policy). Therefore, the routes that are to be changed based on the policy can also have redundancy.

Policy-based routing in AX-series products can handle a group of multiple next hops, called a *policy-based routing list*, as the destinations of route changing, and up to eight routes can be configured in a single group.
In cases where the traffic cannot be forwarded to any of the next hops defined in the policy-based routing list, the traffic can be chosen to be discarded or subject to the normal route of the routing table.

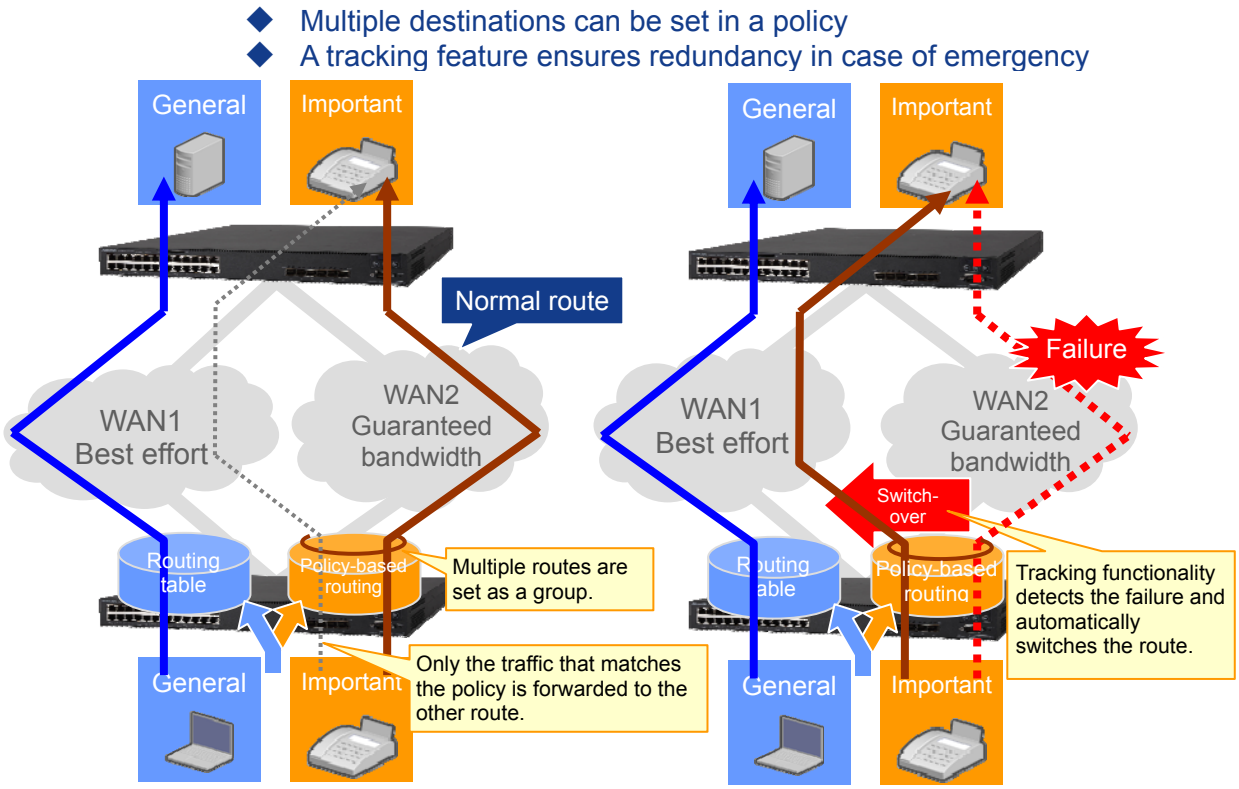


Figure 1.2-1: What can be done with the policy-based routing in the AX series

(2) Routes can be changed upon checking the online status of the target next hop and the future route (IPv4 only).

It is possible to check whether the device specified as the next hop or an even later hop can be used for communication. This allows you to ensure high availability even when integrating a system that uses policy-based routing.

This feature that we call *tracking functionality* checks reachability by regularly exchanging packets with the target (tracking target) using ICMP (ping). Even if the tracking target does not exist in the same subnet (when the target is connected via another device or through a WAN line), reachability can be checked.

By using this feature in conjunction with policy-based routing groups as described in the above (1), the next hops in the policy-based routing list can be dynamically switched according to the checked condition of the next hops or the forwarding route.

(3) Policy-based routing can be used within a virtual network or between virtual networks.

For products that support network partitions, policy-based routing can also be used in a virtual network environment.

You can use separate policy-based routing within a partition, and even between partitions you can apply policy-based routing on extranet communications.

◆ Policy-based routing can be also used with virtual networks

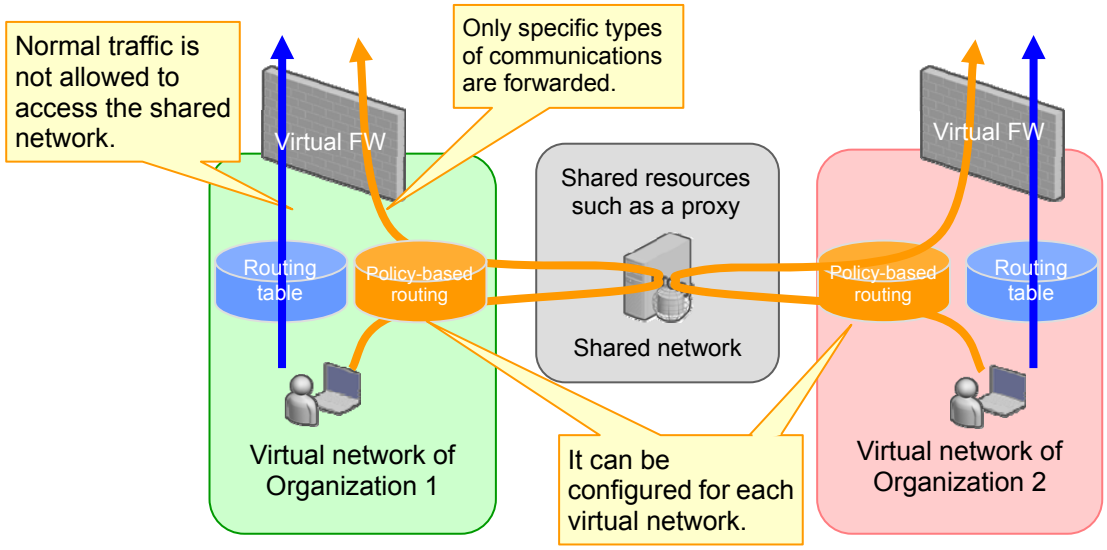


Figure 1.2-2: Securing shared networks with policy-based routing

2. Usage Examples of Policy-Based Routing

Below we introduce some system configuration examples using policy-based routing.

2.1 Route changing to avoid excessive network load on the appliance

These days, we can see many more types of devices dedicated to particular applications and services, such as appliance devices. If you can separate the traffic used for such applications or services from other communications and forward them to such devices, excessive network load can be avoided to ensure efficiency. Policy-based routing is suitable for this kind of network traffic control.

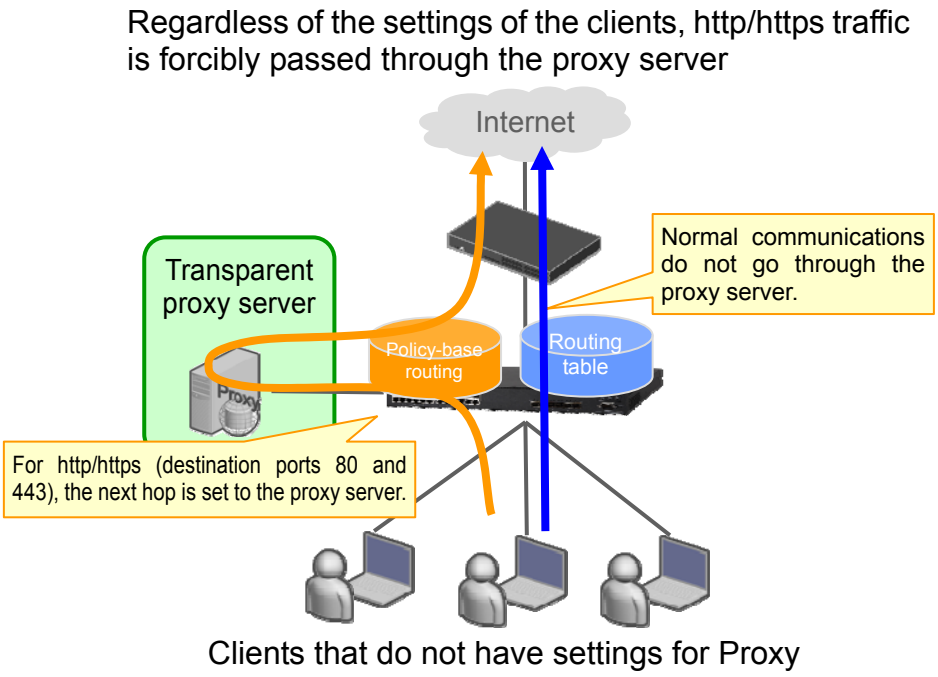


Figure 2.1-1: Example of forwarding only Web access to the proxy server

For example, when you want Web access to a network outside the company to be managed and controlled by a transparent proxy server, but when you do not want traffic other than Web access to place excessive load on the proxy server, you can configure the system to transfer only the Web-related traffic (http and https) to the proxy server using policy-based routing.

2.2 Efficient use of carrier-provided services (WAN lines)

For connections to the external network, various types of line services are provided for different purposes and demands, such as remote access between branch offices or from a mobile terminal to the office network, or an Internet connection from inside the company. Now that the content of communication is highly diversified, it is desirable to integrate a system that employs the most appropriate line type that suits the types and characteristics of traffic.

For example:

- For general Internet connections, low-cost broadband public lines are to be used.
- For critical communications that require higher privacy, leased lines are to be used.
- For communications that require real-time data delivery, lines with bandwidth guarantees are to be used.
- For emergencies only (not used in normal time), a line that enables minimum communications is to be ensured.
- Others

As can be seen from the above, policy-based routing is also recommended when you configure a system that uses different WAN lines for different types of communications with different characteristics.

- For important communications, such as IP telephone, routes with assured bandwidth are used to ensure quality.
- All lines are to be used efficiently, while a tracking feature ensures redundancy for emergency.

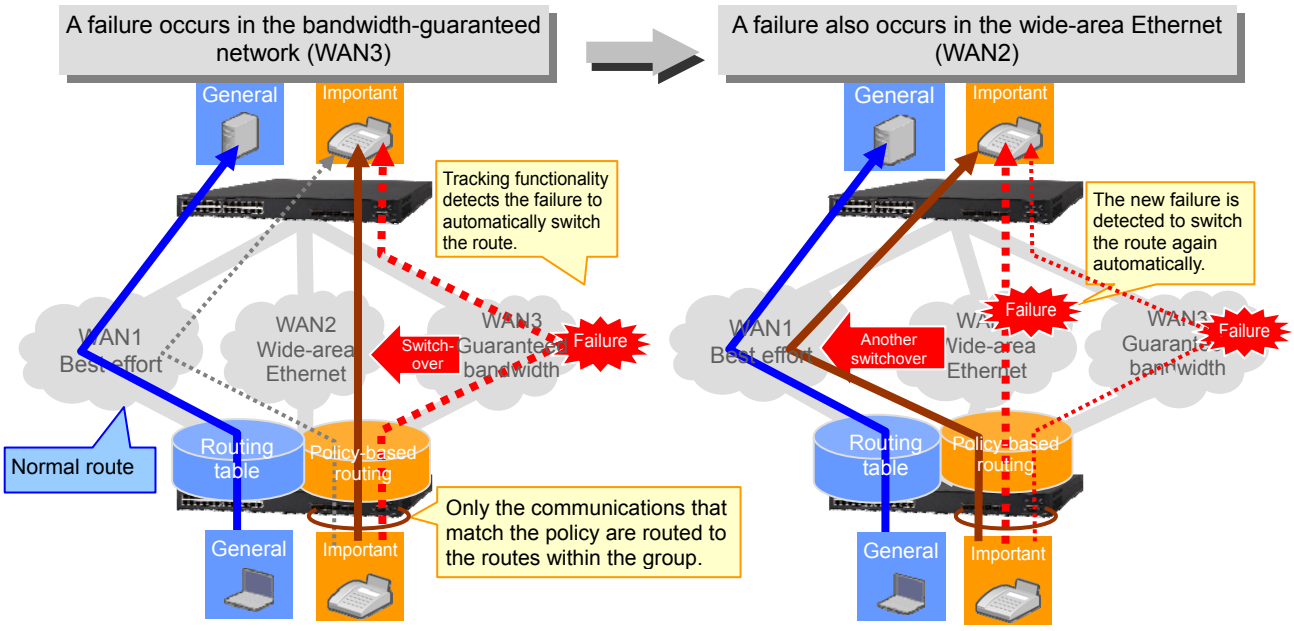


Figure 2.2-1: Example of forwarding only IP telephone traffic

Consider this specific example: One wants to build a system in which for general communications, a low-cost, broadband, but best-effort line will do, but for IP telephone traffic that requires real-time capability, a line with bandwidth guarantees is required, with a minimum bandwidth subscription (for IP telephone traffic).
As policy-based routing enables switching routes only for traffic that matches the condition, it can satisfy this demand and use different lines for specific communications.

In addition, policy-based routing group and a tracking feature would allow using alternative lines registered in the group to avoid communication failure even if the line with bandwidth guarantees cannot be used due to a failure.

3. Examples of System Integrations and Configurations

Below we explain how to configure your system to support policy-based routing.

3.1 System example that splits routes for particular services

You can use and define the route−changing conditions in the same way as in setting up the searching conditions of the access filter. Therefore, you can specify a port number for the traffic of a certain application as a condition for route changing.
This can be applied, for example, to a system that forwards only the communications for an application to a dedicated appliance device. Figure 3.1-1 below provides such an example.

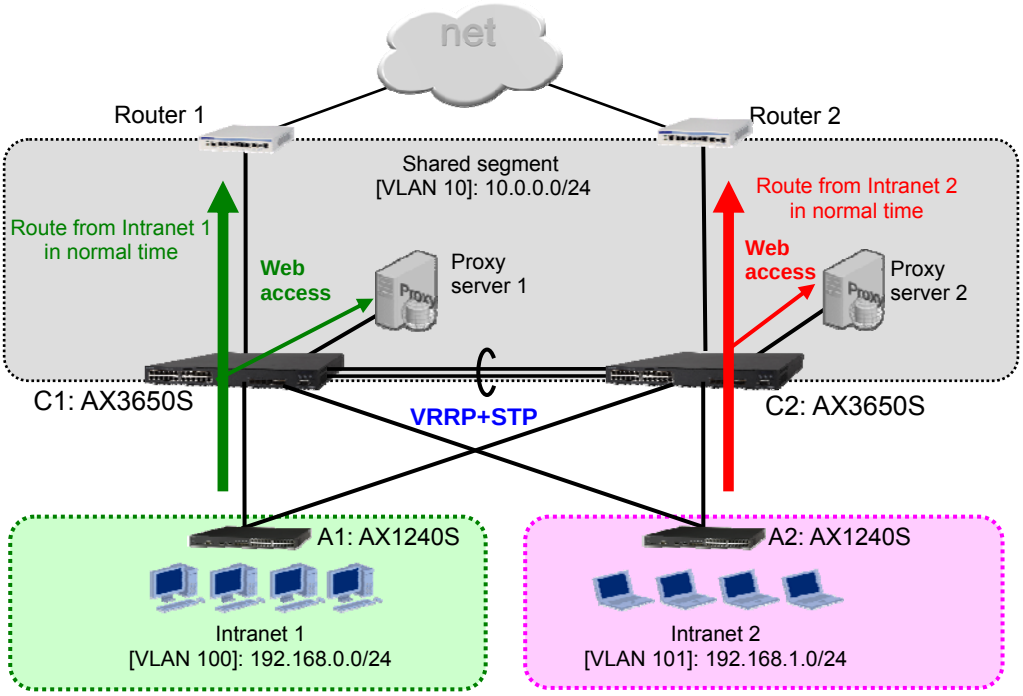


Figure 3.1−1: Example of a redundant system using proxy servers

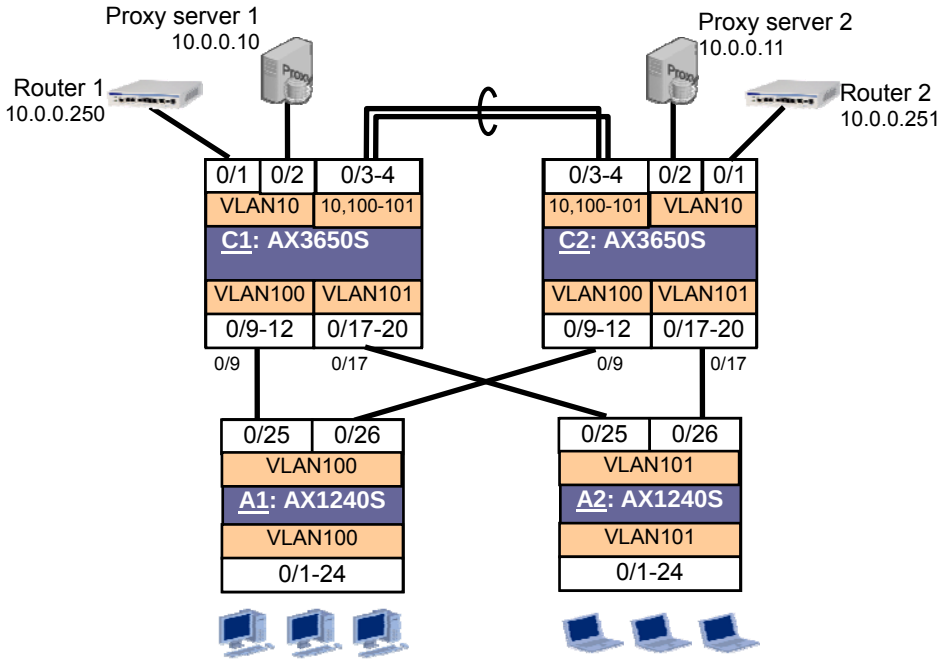
This is a typical configuration where the core switches are made redundant using VRRP and spanning trees, and two routers are used to ensure availability for connection to external networks. When it comes to Web access (http and https), however, the traffic is sent through the transparent proxy servers. For proxy servers as well, two servers are used to make a redundant configuration for ensuring availability.

In short, Table 3.1-1 below summarizes the devices and lines to be used for a redundant configuration and how to control them.

Table 3.1-1: Redundant segments and how to control them

Devices or lines to be made redundant	How to control the redundant configuration
Line between the core switches C1 and C2	Link aggregation
Line between the core switches C1 and C2, and the access switches	Spanning Tree Protocol (rapid-PVST+)
Default gateway for the accessing terminals (core switches C1 and C2)	VRRP
Routers 1 and 2 that connect to the external network	Static routing (Single path with dynamic monitoring functionality)
Proxy servers 1 and 2	Policy-based routing (with tracking functionality)

Figure 3.1-2 below provides the logical configuration of the system.



Purpose	VLAN ID	IP address
Intranet 1	100	192.168.0.0/24
Intranet 2	101	192.168.1.0/24
Shared segment for connecting to external networks	10	10.0.0.0/24

Figure 3.1-2: Logical configuration

The core switches have two segments divided by two VLANs, called Intranet 1 and Intranet 2, and in normal time, the load can be balanced for each segment on the upstream side of the core switches.

Specifically, the traffic of the terminals connected to Switch A1 goes through Core Switch C1 and Router 1, and Proxy Server 1 is used as the Web proxy. The traffic of the terminals connected to Switch A2 uses Core Switch C2 and Router 2, and Proxy Server 2 is used as the Web proxy.

When a failure occurs in any of the switches or lines, the traffic can be bypassed to the other route to ensure continuous communication.

3.1.1 Configuration key points

(1) When using policy-based routing in a box-type switch, set the flow detection mode to layer 3-6.

When you configure policy-based routing with a box-type switch, such as the AX3600S series, set the flow detection mode to layer 3-6. Policy-based routing cannot be used with any other flow detection mode.

(2) When configuring policy-based routing, set the following three elements consecutively.

Policy-based routing can be enabled by setting the following elements in combination:

- Policy-based routing list
  This contains the routes to be used.

- Access list
  This specifies the condition or policy for switching routes.

If you wish to use tracking functionality, you need to configure the following before setting up the above elements:

- Track object
  This is a setting used in policy-based routing for monitoring the status of the next hop and the future route.

When setting up policy-based routing, configure the elements in the following order, considering that they are referenced to each other:
(1)Track object -> (2) Policy-based routing list -> (3) Access list

(3) We recommend that you check the next hop by using tracking functionality (box-type switches such as AX3600S only).

In order to switch routes using policy-based routing in a box-type switch such as an AX3600S series switch, the ARP information and MAC address of the next hop need to be registered in the ARP table and the MAC address table respectively. Without such information, the target packets of policy-based routing will be discarded.
For this reason, in order to use policy-based routing with a box-type switch, perform either of the following procedures:

- Statically define the MAC address and ARP table for the next hop address.
- Use polling monitoring of tracking functionality in conjunction.

In the actual operation, it might be difficult to statically register the MAC address of the switch that has the next hop address, and when possible, we recommend that you enable the polling monitoring of tracking functionality to work with policy-based routing.

(4) Before changing the tracking functionality settings during the operation, make sure that you "disable" the functionality by specifying the default track status.

When you wish to change the settings of the tracking functionality after the operation has started (after route selection with policy-based routing enabled), we recommend that you set the default track status to stop (`disable`) the tracking behavior temporarily before making any modifications.

By doing so, you can modify the configuration of the track without affecting the configured route selections in the policy-based routing group.

When you finish with the necessary configurations, specify `no disable` to restart the tracking behavior.

(5) Default behaviors of the access list and the policy-based routing list

A route selecting condition (policy) of policy-based routing is handled as one of the filtering conditions of the access list. This is why packets that do not match any of the defined conditions are "denied" or discarded.

In general, communications traffic that does not match any route-changing conditions of policy-based routing should be forwarded to a route based on the routing information, so make sure that you set a condition that allows all the traffic (permit any any) at the end of the conditions.

In addition, if all the routes in the policy-based routing list, which is referenced when a matching occurs for route selection, are down, packets are discarded by default.

However, in such a case, where the destination of the route switching is not found, you can decide whether the traffic should be discarded as is or subject to the routing based on the routing information.

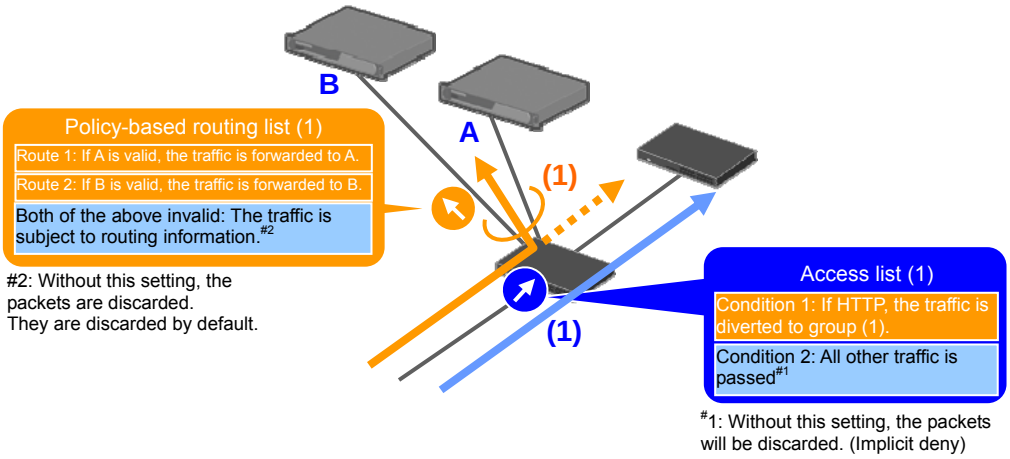


Figure 3.1-3: Default behaviors of the access list and the policy-based routing list

3.1.2 Configuration examples

Below we provide configuration setting examples.

(1) Configuration of Core Switch C1

Configuration of C1 (AX3650S)	
Configuration of the Spanning Tree Protocol	
`(config)# spanning-tree mode rapid-pvst`	Set the Spanning Tree Protocol mode to rapid-PVST+.
Configuration of the flow detection mode	
`(config)# flow detection mode layer3-6`	Set the flow detection mode to `layer3-6`. (Configuration key point (1))
Configuration of VLANs	
`(config)# vlan 2,10,100-101` `(config-vlan)# exit`	Configure the VLANs that are to be used.
Configuration of VLAN interfaces and VRRP	

`(config)# interface vlan 10`
`(config-if)# ip address 10.0.0.1 255.255.255.0`
`(config-if)# exit`
 	
`(config)# interface vlan 100`
`(config-if)# ip address 192.168.0.1`
`255.255.255.0`
`(config-if)# vrrp 1 ip 192.16.0.1`
`(config-if)# exit`
 	
`(config)# interface vlan 101`
`(config-if)# ip address 192.168.1.2`
`255.255.255.0`
`(config-if)# vrrp 2 ip 192.168.1.1`
`(config-if)# exit`
	Assign the IP address `10.0.0.1` to VLAN `10`.
	
	Assign the IP address `192.168.0.1` to VLAN `100`.
	Assign the virtual IP address `192.168.0.1` to VRRP `1`.
	
	Assign the IP address `192.168.1.2` to VLAN `101`.
	Assign the virtual IP address `172.16.1.1` to VRRP `2`.

Configuration of track objects (Configuration key point (2))	

`(config)# track-object 100`
`(config-track-object)# default-state up`
`(config-track-object)# disable`
`(config-track-object)# type icmp 10.0.0.10`
`(config-track-object)# exit`
 	
`(config)# track-object 101`
`(config-track-object)# default-state up`
`(config-track-object)# disable`
`(config-track-object)# type icmp 10.0.0.11`
`(config-track-object)# exit`
	Configure a track object with track ID `100`.
	Set the default track status of the track to `Up`.
	Set the behavior of the track during the configuration to `disable`. (Configuration key point (4))
	Specify `10.0.0.10` as the target track of the ICMP polling monitoring.
	
	Configure a track object with track ID `101`.
	Set the default track status of the track to `Up`.
	Set the behavior of the track during the configuration to `disable`. (Configuration key point (4))
	Specify `10.0.0.11` as the target track of the ICMP polling monitoring.

Configuration of the policy-based routing list (Configuration key point (2))	

`(config)# policy-list 10`
 	
`(config-pol)# policy-interface vlan 10`
`next-hop 10.0.0.10 track-object 100`
 	
`(config-pol)# policy-interface vlan 10`
`next-hop 10.0.0.11 track-object 101`
 	
`(config-pol)# default deny`
`(config-pol)# exit`
	Create a policy-based routing list with list #`10`.
	
	Specify `10.0.0.10` in VLAN `10` as the next hop of the first priority route and configure it to be monitored by track object `100`.
	(Configuration key point (3))
	
	Specify `10.0.0.11` in VLAN `10` as the next hop of the second priority route. This route is to be monitored by track object `101`. (Configuration key point (3))
	Set the default behavior to `deny`. (Configuration key point (5))
	These settings dictate that the Web traffic should be blocked when both of the routes are down (when both of the proxy servers are down).

Configuration of C1 (AX3650S)	
Configuration of the access list (Configuration key point (2))	
(config)# ip access-list extended PG_PROXY (config-ext-nacl)# permit tcp any any eq http action policy-list 10 (config-ext-nacl)# permit tcp any any eq https action policy-list 10 (config-ext-nacl)# permit ip any any (config-ext-nacl)# exit	Apply policy list #10 to http access (port number 80) and https access (port number 443) via tcp. Permit all other IP communications. (Configuration key point (5))
Configuration of static routes	
(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.250 noresolve poll (config)# ip route 0.0.0.0 0.0.0.0 10.0.0.251 200 noresolve poll	Set the default gateway to 10.0.0.250 and 10.0.0.251 while the dynamic monitoring functionality is applied. To configure 10.0.0.250 as a preferred single path, set the distance value 200 to the route on the side of 10.0.0.251.
Configuration of policy-based routing on the VLAN interfaces	
(config)# interface range vlan 100-101 (config-if-range)# ip access-group PG_PROXY in (config-if-range)# exit	Add the setting of policy-based routing PG_PROXY to VLAN 100 and VLAN 101.
Configuration of physical interfaces	
(config)# interface range gigabitethernet 0/1-2 (config-if-range)# switchport access vlan 10 (config-if-range)# exit (config)# interface range gigabitethernet 0/3-4 (config-if-range)# channel-group 1 mode on (config-if-range)# exit (config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk vlan 10,100-101 (config-if)# exit (config)# interface range gigabitethernet 0/9-12 (config-if-range)# switchport access vlan 100 (config-if-range)# exit (config)# interface range gigabitethernet 0/17-20 (config-if-range)# switchport access vlan 101 (config-if-range)# exit	Set ports 0/1–2 as access ports of VLAN 10. Add ports 0/3 and 0/4 to port channel 1 as a static link aggregation. Set port channel 1 as the trunk port of VLAN10, 100-101. Set ports 0/9–12 as access ports of VLAN 100. Set ports 0/17–20 as access ports of VLAN 101.
Start of tracking the track object (Configuration key point (4))	
(config)# track-object 100 (config-track-object)# no disable (config-track-object)# exit (config)# track-object 101 (config-track-object)# no disable (config-track-object)# exit	Start tracking the track ID 100. Start tracking the track ID 101.

(2) Configuration of Core Switch C2

Configuration of C2 (AX3650S)	
Configuration of the Spanning Tree Protocol	
`(config)# spanning-tree mode rapid-pvst`	Set the Spanning Tree Protocol mode to rapid-PVST+.
Configuration of the flow detection mode	
`(config)# flow detection mode layer3-6`	Set the flow detection mode to `layer3-6`. (Configuration key point (1))
Configuration of VLANs	
`(config)# vlan 2,10,100-101` `(config-vlan)# exit`	Configures the VLANs that are to be used.
Configuration of VLAN interfaces and VRRP	

`(config)# interface vlan 10`
`(config-if)# ip address 10.0.0.2 255.255.255.0`
`(config-if)# exit`
 	
`(config)# interface vlan 100`
`(config-if)# ip address 192.168.0.2`
`255.255.255.0`
`(config-if)# vrrp 1 ip 192.16.0.1`
`(config-if)# exit`
 	
`(config)# interface vlan 101`
`(config-if)# ip address 192.168.1.1`
`255.255.255.0`
`(config-if)# vrrp 2 ip 192.168.1.1`
`(config-if)# exit`
	Assign the IP address `10.0.0.2` to VLAN `10`.
	
	Assign the IP address `192.168.0.2` to VLAN `100`.
	Assign the virtual IP address `192.168.0.1` to VRRP `1`.
	
	Assign the IP address `192.168.1.1` to VLAN `101`.
	Assign the virtual IP address `172.16.1.1` to VRRP `2`.

Configuration of track objects for policy-based routing (Configuration key point (2))	

`(config)# track-object 100`
`(config-track-object)# default-state up`
`(config-track-object)# disable`
`(config-track-object)# type icmp 10.0.0.10`
`(config-track-object)# exit`
 	
`(config)# track-object 101`
`(config-track-object)# default-state up`
`(config-track-object)# disable`
`(config-track-object)# type icmp 10.0.0.11`
`(config-track-object)# exit`
	Configure a track object with track ID `100`.
	Set the default track status of the track to `Up`.
	Set the behavior of the track during the configuration to `disable`. (Configuration key point (4))
	Specify `10.0.0.10` as the target track of the ICMP polling monitoring.
	
	Configure a track object with track ID `101`.
	Set the default track status of the track to `Up`.
	Set the behavior of the track during the configuration to `disable`. (Configuration key point (4))
	Specify `10.0.0.11` as the target track of the ICMP polling monitoring.

Configuration of the policy-based routing list (Configuration key point (2))	

`(config)# policy-list 10`
 	
`(config-pol)# policy-interface vlan 10`
`next-hop 10.0.0.11 track-object 101`
`(config-pol)# policy-interface vlan 10`
`next-hop 10.0.0.10 track-object 100`
 	
`(config-pol)# default deny`
`(config-pol)# exit`
	Create a policy-based routing list with list #`10`.
	Specify `10.0.0.11` in VLAN `10` as the next hop of the first priority route and configure it to be monitored by track object `101`.
	(Configuration key point (3))
	Specify `10.0.0.10` in VLAN `10` as the next hop of the second priority route. This route is to be monitored by track object `100`. (Configuration key point (3))
	Set the default behavior to `deny`. (Configuration key point (5))
	These settings dictate that Web traffic should be blocked when both of the routes are down (when both of the proxy servers are down).

Configuration of C2 (AX3650S)	
Configuration of the access list (Configuration key point (2))	
(config)# ip access-list extended PG_PROXY (config-ext-nacl)# permit tcp any any eq http action policy-list 10 (config-ext-nacl)# permit tcp any any eq https action policy-list 10 (config-ext-nacl)# permit ip any any (config-ext-nacl)# exit	Apply policy list #10 to http access (port number 80) and https access (port number 443) via tcp. Permit all other IP communications. (Configuration key point (5))
Configuration of static routes	
(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.251 noresolve poll (config)# ip route 0.0.0.0 0.0.0.0 10.0.0.250 200 noresolve poll	Set the default gateway to 10.0.0.250 and 10.0.0.251 while the dynamic monitoring functionality is applied. To configure 10.0.0.251 as a preferred single path, set the distance value 200 to the route on the side of 10.0.0.250.
Configuration of policy-based routing on the VLAN interfaces	
(config)# interface range vlan 100-101 (config-if-range)# ip access-group PG_PROXY in (config-if-range)# exit	Add the setting of policy-based routing PG_PROXY to VLAN 100 and VLAN 101.
Configuration of physical interfaces	
(config)# interface range gigabitethernet 0/1-2 (config-if-range)# switchport access vlan 10 (config-if-range)# exit (config)# interface range gigabitethernet 0/3-4 (config-if-range)# channel-group 1 mode on (config-if-range)# exit (config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk vlan 10,100-101 (config-if)# exit (config)# interface range gigabitethernet 0/9-12 (config-if-range)# switchport access vlan 100 (config-if-range)# exit (config)# interface range gigabitethernet 0/17-20 (config-if-range)# switchport access vlan 101 (config-if-range)# exit	Set ports 0/1–2 as access ports of VLAN 10. Add ports 0/3 and 0/4 to port channel 1 as a static link aggregation. Set port channel 1 as the trunk port of VLAN 10, 100–101. Set ports 0/9–12 as access ports of VLAN 100. Set ports 0/17–20 as access ports of VLAN 101.
Start of tracking the track object (Configuration key point (4))	
(config)# track-object 100 (config-track-object)# no disable (config-track-object)# exit (config)# track-object 101 (config-track-object)# no disable (config-track-object)# exit	Start tracking the track ID 100. Start tracking the track ID 101.

(3) Configuration of Access Switch A1

Configuration of A1 (AX1240S)	
Configuration of the Spanning Tree Protocol	
(config)# spanning-tree mode rapid-pvst	Set the Spanning Tree Protocol mode to rapid-PVST+.
Configuration of the VLAN	
(config)# vlan 100 (config-vlan)# exit	Configure the VLAN that is to be used.
Configuration of physical interfaces	
(config)# interface range fastethernet 0/1-24 (config-if-range)# switchport access vlan 100	Set ports 0/1–24 as access ports of VLAN 100.

Configuration of A1 (AX1240S)	
(config-if-range)# exit (config)# interface range gigabitethernet 0/25-26 (config-if-range)# switchport access vlan 100 (config-if-range)# exit	Set ports 0/25–26 as access ports of VLAN100.

#1: The configuration of switch A2 will be same as that of A1, except that the VLAN that the switch handles is different (VLAN ID=101).

3.2 Usage example of policy-based routing in a virtual network

Policy-based routing in the AX series can also be used in an environment where network partitions are used, and you can even create a route between virtual networks by using policy-based routing.
Figure 3.2-1 below provides such an example.

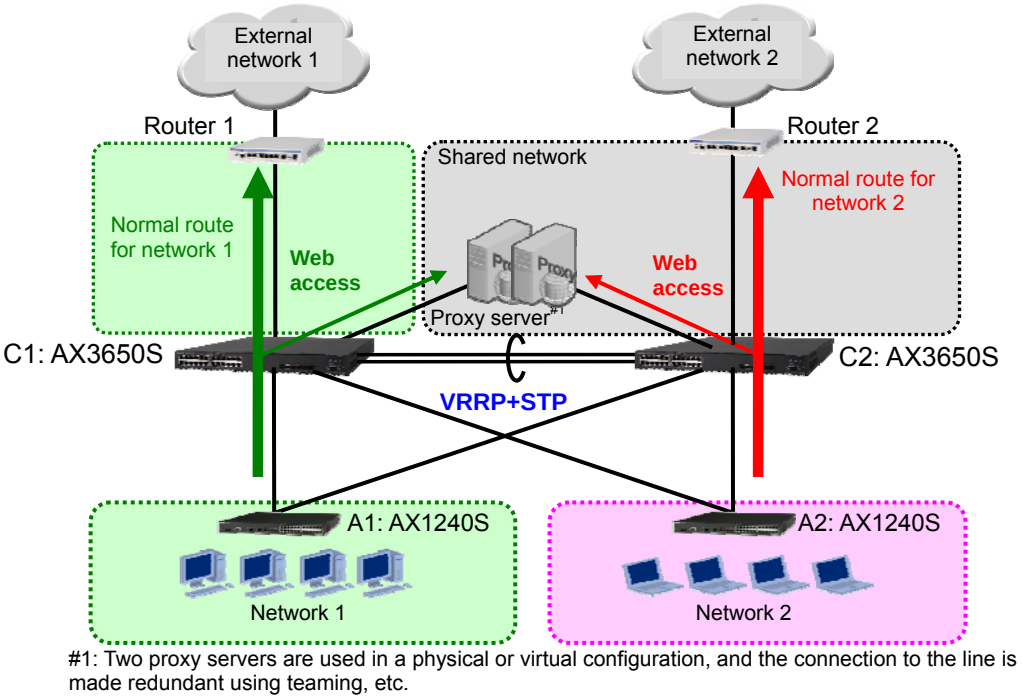


Figure 3.2-1: System example in which network partitions are used (physical configuration)

In terms of physical configurations, it is a typical system in which core switches and access switches are made redundant using VRRP and spanning trees. Also, for proxy servers, two servers are used to ensure redundancy. A single router is used for connecting to external networks 1 and 2.

Figure 3.2-2 and Figure 3.2-3 show the logical network image and logical configuration of this system.

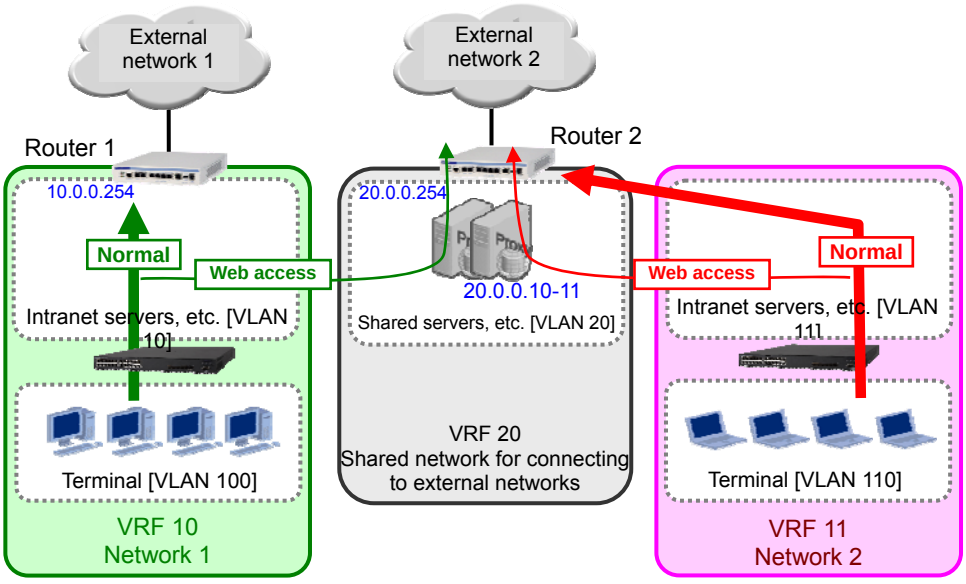
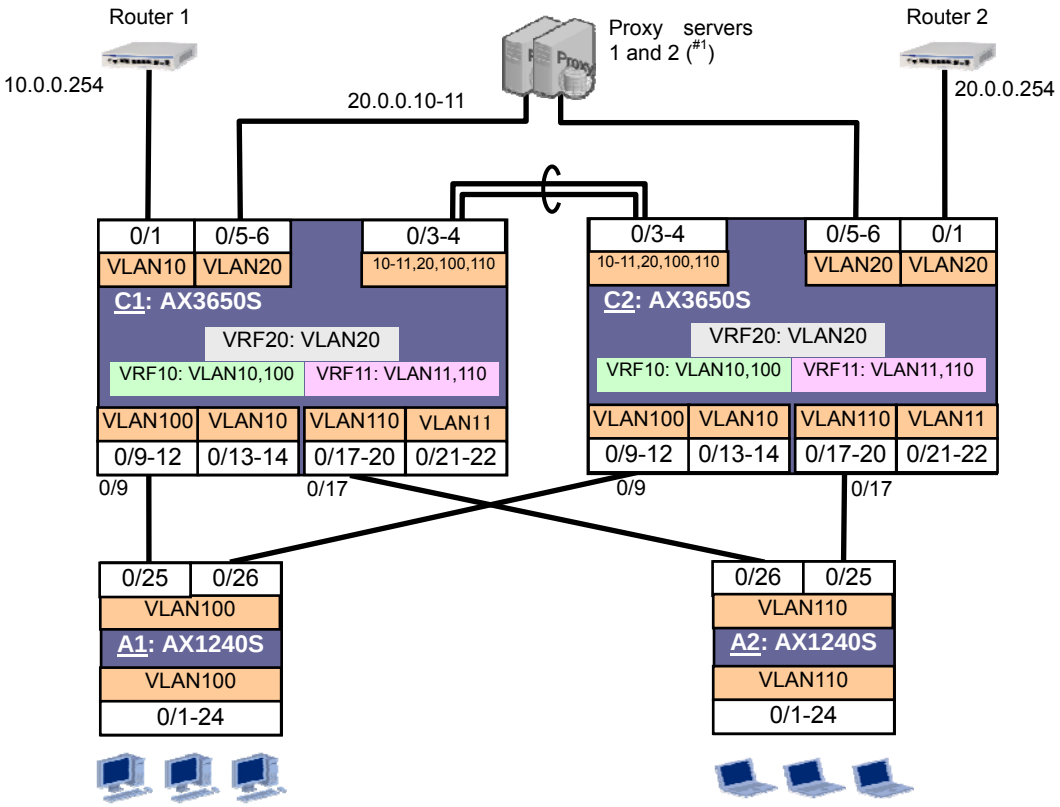


Figure 3.2-2: Configuration image of the logical network



#1: Two proxy servers are used in a physical or virtual configuration, and the connection to the line is made redundant using teaming; and a loop must not be made in VLAN 20.

Purpose	VRF	VLAN	IP address
For the server of network 1	10	10	10.0.0.0/24
For access to network 1		100	192.168.0.0/24
For the server of network 2	11	11	11.0.0.0/24
For access to network 2		110	172.16.0.0/24
Shared network for connecting to the external networks	20	20	20.0.0.0/24

Figure 3.2-3: Logical configuration of the system

The core switches accommodate all three networks by using network partitions: two standard office networks (networks 1 and 2) and the shared network used from those two networks.

For the communication to external networks, in principle, the traffic of network 1 uses router 1, which belongs to the local network. That of network 2 is relayed by router 2 in the shared network.
Note that Web access (http and https) traffic from both networks 1 and 2 go through the transparent proxy server in the shared network and use router 2 in the shared network for Web access.

3.2.1 Configuration key points

The configuration procedure of policy-based routing is the same as that described in *3.1.1 Configuration key points*, but below we explain the points when using policy-based routing in an environment where network partitions are used.

(1) Policy-based routing can be applied to routes between VRFs as is.

Routes can be established using policy-based routing even between networks that are logically divided using network partitions.
The only time network partition-related parameters such as the VRF number are necessary is when you configure a track object, and you do not have to specify the VRF number to create a policy-based routing list.

(2) Configure bidirectional traffic for the communication routes between virtual networks.

When configuring communications between VRFs in a network partition, establish routes bidirectionally (this is not restricted to policy-based routing).

For example, in the sample configuration, you need to set up the following four types of routes for the segment between VRFs:

(A) Routes that lead from core switches C1 and C2 to proxy servers 1 and 2
-> Routes are to be configured using policy-based routing.
(B) Route that leads from core switch C2 to router 2
-> A default route is to be configured using static routing between VRFs.
(C) Routes that exit proxy servers 1 and 2 and lead back to core switches C1 and C2
-> Static routes are to be configured by setting up a route map + proxy server.
(D) Route that exits router 2 and leads back to core switch C2
-> A default route is to be configured by setting up a route map + router.

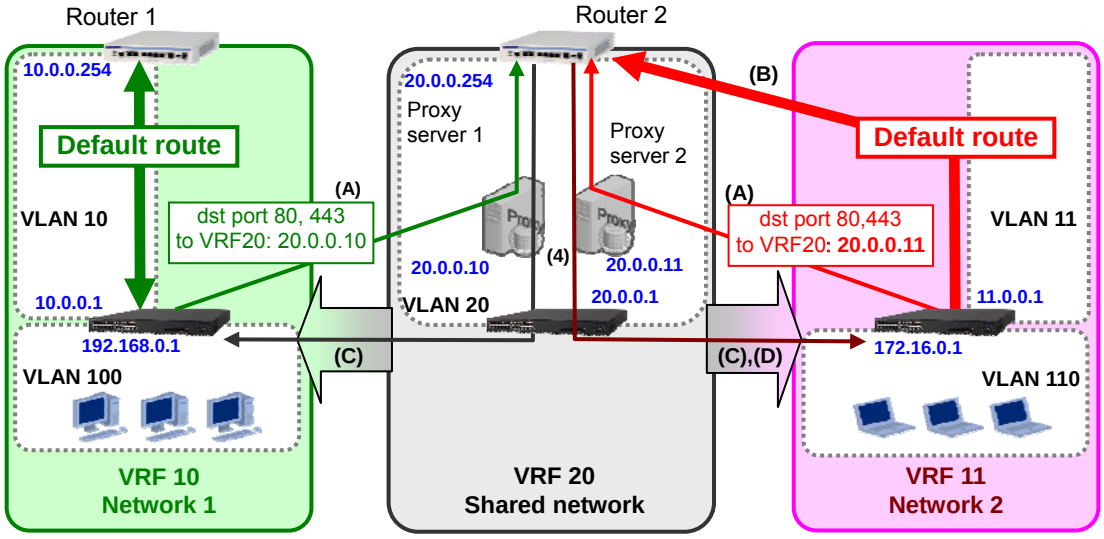


Figure 3.2-4: Image of the example policy-based routing configuration

3.2.2 Configuration examples

Below we provide configuration setting examples.

(1) Core Switch C1

Configuration of C1 (AX3650S)	
Configuration of the Spanning Tree Protocol	
`(config)# spanning-tree mode rapid-pvst`	Set the Spanning Tree Protocol mode to rapid-PVST+.
Configuration of the flow detection mode	
`(config)# flow detection mode layer3-6`	Set the flow detection mode to `layer3-6`. (Configuration key point 3.1.1(1))
Configuration of VRFs	

`(config)# vrf definition 10`
`(config-vrf)# exit`
 	
`(config-vrf)# vrf definition 11`
`(config-vrf)# exit`
 	
`(config-vrf)# vrf definition 20`
`(config-vrf)# import inter-vrf VRF20_IMPORT`
`(config-vrf)# exit`
	Define VRFs `10`, `11`, and `20` as the VRFs to be used in the network partition.
	Set a route-map ID to VRF `20`.

Configuration of VLANs	
`(config)# vlan 10-11,20,100,110` `(config-vlan)# exit`	Configure the VLANs `10`–`11`, `20`, `100`, and `110` that are to be used.
Configuration of VLAN interfaces and VRRP	

`(config)# interface vlan 10`
`(config-if)# vrf forwarding 10`
`(config-if)# ip address 10.0.0.1 255.255.255.0`
`(config-if)# vrrp 10 ip 10.0.0.1`
`(config-if)# exit`
 	
`(config)# interface vlan 11`
`(config-if)# vrf forwarding 11`
`(config-if)# ip address 11.0.0.2 255.255.255.0`
`(config-if)# vrrp 11 ip 11.0.0.1`
`(config-if)# exit`
 	
`(config)# interface vlan 20`
`(config-if)# vrf forwarding 20`
`(config-if)# ip address 20.0.0.1 255.255.255.0`
`(config-if)# exit`
 	
`(config)# interface vlan 100`
`(config-if)# vrf forwarding 10`
`(config-if)# ip address 192.168.0.1`
`255.255.255.0`
`(config-if)# vrrp 100 ip 192.168.0.1`
`(config-if)# exit`
 	
`(config)# interface vlan 110`
`(config-if)# vrf forwarding 11`
`(config-if)# ip address 172.16.0.2`
`255.255.255.0`
`(config-if)# vrrp 110 ip 172.16.0.1`
`(config-if)# exit`
	Set VLAN `10` as the IP address `10.0.0.1` that is to be used by VRF `10`. Assign the virtual IP address `10.0.0.1` to VRRP `10` so that this Switch becomes the VRRP master of this VLAN.
	
	Set VLAN `11` as the IP address `11.0.0.2` that is to be used by VRF `11`. Assign the virtual IP address `11.0.0.1` to VRRP `11`.
	
	Set VLAN `20` as the IP address `20.0.0.1` that is to be used by VRF `20`.
	
	Set VLAN `100` as the IP address `192.168.0.1` that is to be used by VRF `10`. Assign the virtual IP address `192.168.0.1` to VRRP `100` so that this Switch will become the VRRP master of this VLAN.
	
	Set VLAN `110` as the IP address `172.16.0.2` that is to be used by VRF `110`. Assign the virtual IP address `172.16.0.1` to VRRP `110`.

Configuration of track objects (Configuration key point 3.1.1 (2))	

`(config)# track-object 100`
`(config-track-object)# default-state up`
`(config-track-object)# disable`
`(config-track-object)# type icmp vrf 20`
`20.0.0.10`
`(config-track-object)# exit`
 	
`(config)# track-object 101`
`(config-track-object)# default-state up`
`(config-track-object)# disable`
`(config-track-object)# type icmp vrf 20`
`20.0.0.11`
`(config-track-object)# exit`
	Configure a track object with the track ID `100` to be used for monitoring the status of proxy server `1`. Set the default track status to `Up` and the track behavior to `disable` temporarily, and then specify `20.0.0.10` in VRF `20` as the target track of IPv4 ICMP polling monitoring. (Configuration key point 3.1.1 (4))
	
	Configure a track object with the track ID `101` to be used for monitoring the status of proxy server `2`. Set the default track status to `Up` and the track behavior to `disable` temporarily, and then specify `20.0.0.11` in VRF `20` as the target track of IPv4 ICMP polling monitoring. (Configuration key point 3.1.1 (4))

Configuration of C1 (AX3650S)	
Configuration of the policy-based routing list (Configuration key point 3.1.1 (2))	
(config)# policy-list 10 (config-pol)# policy-interface vlan 20 next-hop 20.0.0.10 track-object 100 (config-pol)# policy-interface vlan 20 next-hop 20.0.0.11 track-object 101 (config-pol)# default deny (config-pol)# exit (config)# policy-list 11 (config-pol)# policy-interface vlan 20 next-hop 20.0.0.11 track-object 101 (config-pol)# policy-interface vlan 20 next-hop 20.0.0.10 track-object 100 (config-pol)# default deny (config-pol)# exit	Create a policy-based routing list with list #10 for the routes leading to proxy server 1. First, if track object 100 is valid, define a route in which 20.0.0.10 (proxy server 1) in VLAN 20 is the next hop. Then, if track object 101 is valid, define a route in which 20.0.0.11 (proxy server 2) in VLAN 20 is the next hop. (Configuration key points 3.1.1(3) and (1)) Specify to discard the packets if these routes are not valid. (Configuration key point 3.1.1 (5)) Create a policy-based routing list with list #11 for the routes leading to proxy server 2. First, if track object 101 is valid, define a route in which 20.0.0.11 (proxy server 2) in VLAN 20 is the next hop. Then, if track object 100 is valid, define a route in which 20.0.0.10 (proxy server 1) in VLAN 20 is the next hop. (Configuration key points 3.1.1(3) and (1)) Specify to discard the packets if these routes are not valid. (Configuration key point 3.1.1 (5))
Configuration of access lists (Configuration key point 3.1.1 (2))	
(config)# ip access-list extended PBR_TO_PROXY1 (config-ext-nacl)# permit tcp any any eq http action policy-list 10 (config-ext-nacl)# permit tcp any any eq https action policy-list 10 (config-ext-nacl)# permit ip any any (config-ext-nacl)# exit (config)# ip access-list extended PBR_TO_PROXY2 (config-ext-nacl)# permit tcp any any eq http action policy-list 11 (config-ext-nacl)# permit tcp any any eq https action policy-list 11 (config-ext-nacl)# permit ip any any (config-ext-nacl)# exit	Create access list PBR_TO_PROXY1, which defines policy-based routing for the route leading to proxy server 1. Apply policy-based routing list #10 to http access (port number 80) and https access (port number 443) via tcp. Permit all other IP communications. (Configuration key point 3.1.1 (5)) Create access list PBR_TO_PROXY2, which defines policy-based routing for the route leading to proxy server 2. Apply policy-based routing list #11 to http access (port number 80) and https access (port number 443) via tcp. Permit all other IP communications. (Configuration key point 3.1.1 (5))
Configuration of the route filter (route-map)	
(config)# route-map VRF20_IMPORT permit 10 (config-route-map)# match vrf 10 11 (config-route-map)# exit	In the route filter to be applied to VRF 20, configure to permit communication to VRF 10 and VRF 11, excluding the default route. These settings enable communications from the shared network to the respective networks. (Configuration key point (2))
Configuration of static routes	
(config)# ip route vrf 10 0.0.0.0 0.0.0.0 10.0.0.254 noresolve (config)# ip route vrf 11 0.0.0.0 0.0.0.0 20.0.0.254 vrf 20 noresolve (config)# ip route vrf 20 0.0.0.0 0.0.0.0 20.0.0.254 noresolve	Set 10.0.0.254 (router 1) as the default gateway of VRF 10. Set 20.0.0.254 (router 2) in VRF 20 as the default gateway of VRF 11. Set 20.0.0.254 (router 2) as the default gateway of VRF 20.
Configuration of policy-based routing on the VLAN interfaces	
(config)# interface vlan 100 (config-if)# ip access-group PBR_TO_PROXY1 in (config-if)# exit (config)# interface vlan 110 (config-if)# ip access-group PBR_TO_PROXY2 in (config-if)# exit	Apply a policy-based routing setting PBR_TO_PROXY1 to VLAN 100. Apply a policy-based routing setting PBR_TO_PROXY2 to VLAN 110.
Configuration of physical interfaces	

Configuration of C1 (AX3650S)	
(config)# interface gigabitethernet 1/0/1 (config-if)# switchport access vlan 10 (config-if)# exit	Set port 0/1 as an access port of VLAN 10.
(config)# interface range gigabitethernet 1/0/5-6 (config-if-range)# switchport access vlan 20 (config-if-range)# exit	Set ports 0/5–6 as access ports of VLAN 20.
(config)# interface range gigabitethernet 1/0/3-4 (config-if-range)# channel-group 1 mode on (config-if-range)# exit	Add ports 0/3 and 0/4 to port channel 1 as a static link aggregation.
(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk vlan 10-11,20,100,110 (config-if)# exit	Set port channel 1 as the trunk port of VLANs 10–11, 20, 100, and 110.
(config)# interface range gigabitethernet 1/0/9-12 (config-if-range)# switchport access vlan 100 (config-if-range)# exit	Set ports 0/9–12 as access ports of VLAN 100.
(config)# interface range gigabitethernet 1/0/13-14 (config-if-range)# switchport access vlan 10 (config-if-range)# exit	Set ports 0/13–14 as access ports of VLAN 10.
(config)# interface range gigabitethernet 1/0/17-20 (config-if-range)# switchport access vlan 110 (config-if-range)# exit	Set ports 0/17–20 as access ports of VLAN 110.
(config)# interface range gigabitethernet 1/0/21-22 (config-if-range)# switchport access vlan 11 (config-if-range)# exit	Set ports 0/21–22 as access ports of VLAN 11.
Start of tracking the track objects (Configuration key point 3.1.1(4))	
(config)# track-object 100 (config-track-object)# no disable (config-track-object)# exit	Start tracking track ID 100.
(config)# track-object 101 (config-track-object)# no disable (config-track-object)# exit	Start tracking track ID 101.

(2) Core Switch C2

Configuration of C2 (AX3650S)	
Configuration of the Spanning Tree Protocol	
`(config)# spanning-tree mode rapid-pvst`	Set the Spanning Tree Protocol mode to rapid-PVST+.
Configuration of the flow detection mode	
`(config)# flow detection mode layer3-6`	Set the flow detection mode to `layer3-6`. (Configuration key point 3.1.1(1))
Configuration of VRFs	

`(config)# vrf definition 10`
`(config-vrf)# exit`
 	
`(config-vrf)# vrf definition 11`
`(config-vrf)# exit`
 	
`(config-vrf)# vrf definition 20`
`(config-vrf)# import inter-vrf VRF20_IMPORT`
`(config-vrf)# exit`
	Define VRFs `10`, `11`, and `20` as the VRFs to be used in the network partitions.
	Set a route-map ID to VRF `20`.

Configuration of VLANs	
`(config)# vlan 10-11,20,100,110` `(config-vlan)# exit`	Configure the VLANs `10`–`11`, `20`, `100` and `110` that are to be used.
Configuration of VLAN interfaces and VRRP	

`(config)# interface vlan 10`
`(config-if)# vrf forwarding 10`
`(config-if)# ip address 10.0.0.2 255.255.255.0`
`(config-if)# vrrp 10 ip 10.0.0.1`
`(config-if)# exit`
 	
`(config)# interface vlan 11`
`(config-if)# vrf forwarding 11`
`(config-if)# ip address 11.0.0.1 255.255.255.0`
`(config-if)# vrrp 11 ip 11.0.0.1`
`(config-if)# exit`
 	
`(config)# interface vlan 20`
`(config-if)# vrf forwarding 20`
`(config-if)# ip address 20.0.0.2 255.255.255.0`
`(config-if)# exit`
 	
`(config)# interface vlan 100`
`(config-if)# vrf forwarding 10`
`(config-if)# ip address 192.168.0.2 255.255.255.0`
`(config-if)# vrrp 100 ip 192.168.0.1`
`(config-if)# exit`
 	
`(config)# interface vlan 110`
`(config-if)# vrf forwarding 11`
`(config-if)# ip address 172.16.0.1 255.255.255.0`
`(config-if)# vrrp 110 ip 172.16.0.1`
`(config-if)# exit`
	Set VLAN `10` as the IP address `10.0.0.2` that is to be used by VRF `10`. Assign the virtual IP address `10.0.0.1` to VRRP `10`.
	
	Set VLAN `11` as the IP address `11.0.0.1` that is to be used by VRF `11`. Assign the virtual IP address `11.0.0.1` to VRRP `11` so that the Switch becomes the VRRP master of this VLAN.
	
	Set VLAN `20` as the IP address `20.0.0.1` that is to be used by VRF `20`.
	
	Set VLAN `100` as the IP address `192.168.0.2` that is to be used by VRF `10`. Assign the virtual IP address `192.168.0.1` to VRRP `100`.
	
	Set VLAN `110` as the IP address `172.16.0.1` that is to be used by VRF `10`. Assign the virtual IP address `172.16.0.1` to VRRP `110` so that the Switch becomes the VRRP master of this VLAN.

Configuration of track objects (Configuration key point 3.1.1(2))	

`(config)# track-object 100`
`(config-track-object)# default-state up`
`(config-track-object)# disable`
`(config-track-object)# type icmp vrf 20 20.0.0.10`
`(config-track-object)# exit`
 	
`(config)# track-object 101`
`(config-track-object)# default-state up`
`(config-track-object)# disable`
`(config-track-object)# type icmp vrf 20 20.0.0.11`
`(config-track-object)# exit`
	Configure a track object with the track ID `100` to be used for monitoring the status of proxy server `1`. Set the default track status to `Up` and the track behavior to `disable` temporarily, and then specify `20.0.0.10` in VRF `20` as the target track of IPv4 ICMP polling monitoring. (Configuration key point 3.1.1(4))
	
	Configure a track object with the track ID `101` to be used for monitoring the status of proxy server `2`. Set the default track status to `Up` and the track behavior to `disable` temporarily, and then specify `20.0.0.11` in VRF `20` as the target track of IPv4 ICMP polling monitoring. (Configuration key point 3.1.1(4))

Configuration of C2 (AX3650S)	
Configuration of the policy-based routing list (Configuration key point 3.1.1(2))	
(config)# policy-list 10 (config-pol)# policy-interface vlan 20 next-hop 20.0.0.10 track-object 100 (config-pol)# policy-interface vlan 20 next-hop 20.0.0.11 track-object 101 (config-pol)# default deny (config-pol)# exit (config)# policy-list 11 (config-pol)# policy-interface vlan 20 next-hop 20.0.0.11 track-object 101 (config-pol)# policy-interface vlan 20 next-hop 20.0.0.10 track-object 100 (config-pol)# default deny (config-pol)# exit	Create a policy-based routing list with list #10 for the routes leading to proxy server 1. First, if track object 100 is valid, define a route in which 20.0.0.10 (proxy server 1) in VLAN 20 is the next hop. Then, if track object 101 is valid, define a route in which 20.0.0.11 (proxy server 2) in VLAN 20 is the next hop. (Configuration key points 3.1.1(3) and (1)) Specify to discard the packets if these routes are not valid. (Configuration key point 3.1.1(5)) Create a policy-based routing list with list #11 for the routes leading to proxy server 2. First, if track object 101 is valid, define a route in which 20.0.0.11 (proxy server 2) in VLAN 20 is the next hop. Then, if track object 100 is valid, define a route in which 20.0.0.10 (proxy server 1) in VLAN 20 is the next hop. (Configuration key points 3.1.1(3) and (1)) Specify to discard the packets if these routes are not valid. (Configuration key point 3.1.1(5))
Configuration of access lists (Configuration key point 3.1.1(2))	
(config)# ip access-list extended PBR_TO_PROXY1 (config-ext-nacl)# permit tcp any any eq http action policy-list 10 (config-ext-nacl)# permit tcp any any eq https action policy-list 10 (config-ext-nacl)# permit ip any any (config-ext-nacl)# exit (config)# ip access-list extended PBR_TO_PROXY2 (config-ext-nacl)# permit tcp any any eq http action policy-list 11 (config-ext-nacl)# permit tcp any any eq https action policy-list 11 (config-ext-nacl)# permit ip any any (config-ext-nacl)# exit	Create access list PBR_TO_PROXY1, which defines policy-based routing for the route leading to proxy server 1. Apply policy-based routing list #10 to http access (port number 80) and https access (port number 443) via tcp. Permit all other IP communications. Create access list PBR_TO_PROXY2, which defines policy-based routing for the route leading to proxy server 2. Apply policy-based routing list #11 to http access (port number 80) and https access (port number 443) via tcp. Permit all other IP communications.
Configuration of the route filter (route-map)	
(config)# route-map VRF20_IMPORT permit 10 (config-route-map)# match vrf 10 11 (config-route-map)# exit	In the route filter to be applied to VRF 20, configure to permit communications to VRF 10 and VRF 11. These settings enable communications from the shared network to the respective networks. (Configuration key point (2))
Configuration of static routes	
(config)# ip route vrf 10 0.0.0.0 0.0.0.0 10.0.0.254 noresolve (config)# ip route vrf 11 0.0.0.0 0.0.0.0 20.0.0.254 vrf 20 noresolve (config)# ip route vrf 20 0.0.0.0 0.0.0.0 20.0.0.254 noresolve	Set 10.0.0.254 (router 1) as the default gateway of VRF 10. Set 20.0.0.254 (router 2) in VRF 20 as the default gateway of VRF 11. Set 20.0.0.254 (router 2) as the default gateway of VRF 20.
Configuration of policy-based routing on the VLAN interfaces	
(config)# interface vlan 100 (config-if)# ip access-group PBR_TO_PROXY1 in (config-if)# exit (config)# interface vlan 110 (config-if)# ip access-group PBR_TO_PROXY2 in (config-if)# exit	Apply a policy-based routing setting PBR_TO_PROXY1 to VLAN 100. Apply a policy-based routing setting PBR_TO_PROXY2 to VLAN 110.

Configuration of C2 (AX3650S)	
Configuration of physical interfaces	
(config)# interface gigabitethernet 1/0/1 (config-if)# switchport access vlan 20 (config-if)# exit	Set port 0/1 as an access port of VLAN 10.
(config)# interface range gigabitethernet 1/0/5-6 (config-if-range)# switchport access vlan 20 (config-if-range)# exit	Set ports 0/5–6 as access ports of VLAN 20.
(config)# interface range gigabitethernet 1/0/3-4 (config-if-range)# channel-group 1 mode on (config-if-range)# exit	Add ports 0/3 and 0/4 to port channel 1 as a static link aggregation.
(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk vlan 10-11,20,100,110 (config-if)# exit	Set port channel 1 as the trunk port of VLANs 10–11, 100 and 110.
(config)# interface range gigabitethernet 1/0/9-12 (config-if-range)# switchport access vlan 100 (config-if-range)# exit	Set ports 0/9–12 as access ports of VLAN 100.
(config)# interface range gigabitethernet 1/0/13-14 (config-if-range)# switchport access vlan 10 (config-if-range)# exit	Set ports 0/13–14 as access ports of VLAN 10.
(config)# interface range gigabitethernet 1/0/17-20 (config-if-range)# switchport access vlan 110 (config-if-range)# exit	Set ports 0/17–20 as access ports of VLAN 110.
(config)# interface range gigabitethernet 1/0/21-22 (config-if-range)# switchport access vlan 11 (config-if-range)# exit	Set ports 0/21–22 as access ports of VLAN 10.
Start of tracking the track objects (Configuration key point 3.1.1(4))	
(config)# track-object 100 (config-track-object)# no disable (config-track-object)# exit	Start tracking track ID 100.
(config)# track-object 101 (config-track-object)# no disable (config-track-object)# exit	Start tracking track ID 101.

(3) Access Switch A1

Configuration of A1 (AX1240S)	
Configuration of spanning tree	
(config)# spanning-tree mode rapid-pvst	Set the spanning tree mode to rapid-PVST+.
Configuration of the VLAN	
(config)# vlan 100 (config-vlan)# exit	Configure the VLAN that is to be used.
Configuration of physical interfaces	
(config)# interface range fastethernet 0/1-24 (config-if-range)# switchport access vlan 100 (config-if-range)# exit	Set ports 0/1–24 as access ports of VLAN 100.
(config)# interface range gigabitethernet 0/25-26 (config-if-range)# switchport access vlan 100 (config-if-range)# exit	Set ports 0/25–26 as access ports of VLAN 100.

#1: The configuration of switch A2 is same as that of A1, except that the VLAN handled by the switch is different (VLAN ID=110).

(4) Routers 1 and 2

Configuration of routes for routers 1 and 2

Configuration of static routes

In addition to the settings for connecting to the external networks, configure the following static routes:

- The route to `192.168.0.0/24` goes through gateway `20.0.0.1`.
- The route to `172.16.0.0/24` goes through gateway `20.0.0.1`.

(5) Proxy servers 1 and 2

Configuration of routes for proxy servers 1 and 2

Configuration of static routes

- Set default gateway to `20.0.0.254`.
- The route to `192.168.0.0/24` goes through gateway `20.0.0.1`.
- The route to `172.16.0.0/24` goes through gateway `20.0.0.1`.

4. Confirmation of Policy-Based Routing

Although policy-based routing is one of the ways to determine a route, the content is not directly reflected in the general routing information (routing table). To confirm how the policy-based routing is applied during the operation of a system that uses policy-based routing, use the following operation commands.
Below we explain methods used to check the routing information based on policy-routing and other conditions.

4.1 Checking whether policy-based routing settings exist, and checking the route changing conditions and the routes

(1) Checking whether policy-based routing settings exist

To check whether route control with policy-based routing is enabled, use the `show ip policy` command. This command shows VLAN interfaces, applied access lists, and the list numbers of policy routing group lists.

```
C1# show ip policy
Date 2012/02/20 16:49:04 JST
VLAN ID Access List Name/Number Sequence Policy List
    100 PG_PROXY                      10          10
    100 PG_PROXY                      20          10
    101 PG_PROXY                      10          10
    101 PG_PROXY                      20          10
C1#
```

VLAN No. / Name or number of the access list / Sequence number of the access list / List number of the policy-based routing list

Figure 4.1-1: Execution result of the show ip policy command (on Switch C1 in the configuration in section 3.1)

This example shows that policy-based routing is configured for VLAN 100 and VLAN 101 under the access list name `PG_PROXY`.

(2) Checking route changing conditions (policy)

Policy-based routing functions as a kind of access filter. Therefore, you can use the `show access-filter` command to check the route changing conditions (policy) applied in policy-based routing and the list numbers of the policy-based routing lists that are referenced by the route changing conditions.

```
C1# show access-filter interface vlan 100
Date 2012/02/20 16:49:18 JST
Using Interface:vlan 100 in
Extended IP access-list:PG_PROXY
     permit tcp(6) any any eq http(80) action policy-list 10
        matched packets        :          6
     permit tcp(6) any any eq https(443) action policy-list 10
        matched packets        :          0
     permit ip any any
        matched packets        :       1805
     implicitly denied packets:          0

C1#
```

Interface to which policy-based routing is applied / Type and name of access list / Access list conditions=route changing conditions / List number of policy-based routing list to be referenced / Statistical information / Access lists

Figure 4.1-2: Execution result of the show access-filter command (on Switch C1 in the configuration in section 3.1)

This example shows the detailed information of the access lists set in VLAN 100. It also shows that the route of policy-based routing list #10 is applied to http and https traffic.

(3) Checking the routes used in route changing

You can use the `show ip cache policy` command to check the routes defined in policy-based routing. The command allows you to check the details of the policy-based routing lists to confirm the defined routes and the currently selected routes.

```
C1# show ip cache policy
Date 2012/02/20 16:49:36 JST
Policy Base Routing Default Init Interval :  200
   Start Time : 2012/02/20 16:22:11
   End Time   : 2012/02/20 16:25:31
Policy Base Routing List :  10 <-- Policy-based routing list number
   Default : Deny
   Recover : On
   Priority    Sequence  VLAN ID  Status  Next Hop        Track Object ID
          1          10       10  Down    10.0.0.10                   100
 *>       2          20       10  Up      10.0.0.11                   101
C1#
                          Policy-based routing list
```

Figure 4.1-3: Execution result of the show ip cache policy command (on Switch C1 in the configuration in section 3.1)

This example shows that policy-based routing list #`10` is specified and that the list defines two next hops. It also shows that `10.0.0.11` that is in the `UP` state is currently selected as a valid next hop.

4.2 Checking the status of the destination and the next hop

(1) Checking the status of the destination by using the tracking functionality

When the tracking functionality of policy-based routing is used, you can use the `show track-object` command to check the current status of the tracking target. When the `show track-object` command is used alone, it shows summary information; if you specify the track ID, the command shows detailed information regarding the track ID.

```
C1# show track-object
Date 2012/02/20 16:49:58 JST
Track State          Type         Target
100   DOWN(Active)   ICMP         10.0.0.10
101   UP(Active)     ICMP         10.0.0.11
C1#
      Track ID and status  Type (ICMP only)  Tracking target
```

Figure 4.2-1: Execution result of the show track-object command (on Switch C1 in the configuration in section 3.1)

This example shows the summary tracking information. The content shows that `10.0.0.10` (track ID `100`) and 10.0.0.11 (track ID `101`) are configured as tracking targets and which are both being tracked (`Active`), but 10.0.0.10 is in a `DOWN` state (there is no ping reply and it is considered as `DOWN`), while 10.0.0.11 is in an `UP` state (there is a ping reply and it is considered "in operation").

(2) Checking the entry of the next hops in ARP/MAC address table

As explained in *Configuration key points* in Chapter 3 and *Considerations (1)* in Chapter 5, when using policy-based routing in a box-type switch such as the AX3600S series, if the ARP and MAC address information of the next hop devices is not registered in the switch, the forwarding to the next hop fails and the packets are discarded.

In case the status of the next hop is checked using the tracking functionality (because status monitoring with ICMP communications is regularly performed), you do not have to worry about the entry of the next hop in the ARP table and the MAC address table, but if you have defined the next hops in the ARP table and MAC address table directly (that is, static entry), we recommend confirming that the information is correctly registered in the respective tables.

```
C1# show ip arp
Date 2012/02/20 16:50:18 JST
Total: 4 entries                                          Next hop entry in the ARP table
 IP Address       Linklayer Address  Netif                Expire     Type
 10.0.0.11        0000.2000.0011     VLAN0010             3h59m31s   arpa
 10.0.0.251       0060.b946.dd2a     VLAN0010             3h54m22s   arpa
 192.168.0.15     0024.8142.c104     VLAN0100             3h54m29s   arpa
C1#
C1#
C1# show mac-address-table
Date 2012/02/20 16:50:31 JST
MAC address        VLAN    Type     Port-list
0000.2000.0011       10    Dynamic  0/3-4   Next hop entry in the MAC address table
0012.e242.6a2c       10    Dynamic  0/3-4
0060.b946.dd2a       10    Dynamic  0/3-4
0012.e242.6a2f      100    Dynamic  0/3-4
0024.8142.c104      100    Dynamic  0/3-4
0000.5e00.0102      101    Dynamic  0/3-4
0012.e242.6a2f      101    Dynamic  0/3-4
```

Figure 4.2-2: Execution results of the show ip arp and show mac-address-table commands (on Switch C1 in the configuration in section 3.1)

This example checks the entries of the next hop (switch with IP address `10.0.0.11`) in the ARP table and MAC address table.

5. Considerations

Below we provide you with some points to be aware of when you use policy-based routing.
For details about the following notes and other considerations, see the chapters on policy-based routing in the *Software Manual Configuration Guide Vol. 3* of the AX6000S family or the AX3640S and AX3650S series.

(1) Setting routes for a forwarding destination in a box-type switch

When using policy-based routing in a box-type product such as the AX3600S series, if the ARP and MAC address information of the next hop device is not registered in the switch, the target packets of policy-based routing will be discarded. Therefore, when using policy-based routing in a box-type switch, perform either of the following procedures:

- Specify the MAC address and ARP table of the next hop address statically.
- Specify the routes registered in the policy-based routing list to be monitored by polling monitoring of the tracking functionality.

(2) Packets that cannot be forwarded by policy-based routing

The following types of packets are detected by the access list that defines the policy-based routing list information and counted for statistics, but they cannot be forwarded by policy-based routing and therefore will be discarded:

- Frames discarded by layer 2 authentication
- Frames discarded by DHCP snooping
- Packets discarded by flow control

(3) Packets that are not subject to policy-based routing

The following types of packets cannot be detected by the access list that defines the policy-based routing list information and therefore they are not subject to policy-based routing:

- Frames discarded because the data transfer status of the VLAN port is `Blocking` (data forwarding is stopped)
- Frames discarded when the inter-port relay blocking functionality blocks the route between the receiving interface to which the access list that defines the policy-based routing list information is applied, and the transmission destination interface of policy-based routing
- Untagged frames that are received when the native VLAN is not configured to handle untagged frames on the trunk port
- Tagged frames not configured to be received by the trunk port for the VLAN
- Tagged frames received at the access port, protocol port, or MAC port
- Frames discarded by the MAC address learning functionality
- Packets discarded because of an error detected by the IP packet header validity check
- Packets discarded by hardware because their addresses cannot be resolved
- Packets discarded at the null interface
- Packets discarded because IPv4 and IPv6 forwarding is disabled by the `no ip routing` configuration command

(4) When ICMP redirected packets are configured subject to policy-based routing

In a box-type switch, if ICMP redirect packets are configured as targets of policy-based routing, their forwarding destinations will be the redirection targets, and therefore, a heavy load might be placed on the CPU.

Appendix: Configuration Files

This section lists the configuration examples that we explained in this guide.
The text files of all the configurations for the switches in the respective network configurations in Chapter 3 are attached to this file. (Adobe Acrobat 5.0 or later, or Adobe Reader 6.0 or later, is required to extract the attached files.)
For each configuration, see the attached file that corresponds to the same name listed below.

3.1 System example that separates routes for particular services

	Name of the switch and the target switch	Target file
L3 core switch	C1 (AX3650S-48T4XW)	3-1_PBR_C1.txt
	C2 (AX3650S-24T6XW)	3-1_PBR_C2.txt
L2 access switch	A1 (AX1240S-24T2C)	3-1_PBR_A1.txt
	A2 (AX1240S-24T2C)	3-1_PBR_A2.txt

3.2 Use example of policy-based routing in a virtual network

	Name of the switch and the target switch	Target file
L3 core switch	C1 (AX3650S-48T4XW)	3-2_PBR_C1.txt
	C2 (AX3650S-24T6XW)	3-2_PBR_C2.txt
L2 access switch	A1 (AX1240S-24T2C)	3-2_PBR_A1.txt
	A2 (AX1240S-24T2C)	3-2_PBR_A2.txt

Edition 1 issued on February 29, 2012
Document No. NTS-11-R-041

ALAXALA Networks Corporation
Network Technical Support

Shin-Kawasaki Mitsui Bldg West Tower 13F, 890 Kashimada, Saiwai-ku, Kawasaki-shi, Kanagawa 212-0058 Japan
http://www.alaxala.com/en/