



AX Series Network Partition: Solution Guide [Basic]

for
the
Guaranteed
Network

Second Edition

Introduction

This *AX Series Network Partition: Solution Guide [Basic]* document informs system engineers of the technologies required to implement a system based on a network partition, a simple network virtualization, by using the ALAXALA Network's AX series (AX6700S, AX6600S, and AX6300S). The guide is designed to ensure that users have a correct understanding of the outline of each function, of how to implement the system, and of how to achieve stable system operation.

Related documents

-*AX Series Network Partition: Solution Guide [For Authentication]*

-*AX Series Network Partition: Solution Guide [Advanced]*

-*AX Series Product Manual* (<http://www.alaxala.com/en/techinfo/manual/index.html>)

Instructions for using this document

The content of this document is based on basic operations that were confirmed in a specific environment. Therefore, the functionality, performance, and reliability described here cannot be guaranteed for all environments. Think of this as a guide for implementing your system with our products.

Unless otherwise indicated, this document refers to the following OS versions.

AX6700S, AX6600S, AX6300S

Ver.11.3 (with OP-NPAR license)

AX3600S, AX2400S

Ver.11.2.A

The content of this document is subject to change without prior notice.

Caution concerning export

If you export this guide, you must check and comply with all applicable laws, rules and restrictions of Japan and any other countries, such as Japan's Foreign Exchange and Foreign Trade Law and U.S. export control laws and regulations.

Trademarks

- ALAXALA and its logo are trademarks and registered trademarks of ALAXALA Networks Corporation.
- Ethernet is a product name of Xerox Corporation of the United States.
- All other company names and product names are trademarks or registered trademarks of their respective companies.

Revision History

Edition	Rev.	Date	Description	Modified
First	-	2009.1.22	First Edition	-
Second	-	2010.2.19	Added: AX6600S, AX6700S, AX6300S (for Ver11.3) in the list of VRF-enabled devices	Introduction
			Chapter 1: Introduction to Network Partition	
			Added: Use of network partitions in a GSRP configuration	1.3
			Chapter 2: Required Conditions and Support Status	
			Added: Items on the AX6600S in the requirement table	2.1
			Added: Ver11.3-compliant VRF operation modes into the number of configurable VRF instances	2.1
			Updated: VRF support conditions corresponding to Ver11.3	2.2
			Chapter 3: Examples of Implementing Systems with Network Partitions	
			Added: Example of a network partition configuration based on GSRP	3.3
			Added: Syslog host settings supporting VRF	3.1, 3.2

Contents

1. INTRODUCTION TO NETWORK PARTITION	5
1.1 VIRTUALIZATION OF NETWORKS	5
1.2 VRF AND PARTITIONS	6
1.3 COMBINED L2 NETWORKS	7
1.4 INTER-PARTITION COMMUNICATION AND SHARED NETWORKS	10
2. REQUIRED CONDITIONS AND SUPPORT STATUS	11
2.1 REQUIRED CONDITIONS	11
2.2 VRF SUPPORT STATUS	13
3. EXAMPLES OF IMPLEMENTING SYSTEMS WITH NETWORK PARTITION	15
3.1 NETWORK PARTITIONS IN AN FT NETWORK	15
3.1.1 Important points in the configuration	17
3.1.2 Example configuration	18
3.2 NETWORK PARTITIONS IN A RING NETWORK	21
3.2.1 Important points in the configuration	23
3.2.2 Example configuration	24
3.3 NETWORK PARTITION USING GSRP	27
3.3.1 Important points in the configuration	29
3.3.2 Example configuration	30
3.4 CONFIGURATION METHOD FOR SHARED NETWORKS	33
3.4.1 Important points in the configuration	34
3.4.2 Example configuration	35
4. NETWORK PARTITION OPERATIONS	36
4.1 SYSTEM LOG	36
4.2 OPERATIONAL COMMANDS	36
5. CAUTIONS	39
APPENDIX: CONFIGURATION FILES	40

1. Introduction to Network Partition

1.1 Virtualization of networks

System virtualization is a technology for separating or integrating system resources regardless of their physical configuration. Virtualization has advantages in cost and operation due to its small physical resource requirements compared to the assumed system size.

There are several network virtualization technologies already available, including MPLS-VPN. Unfortunately, these existing technologies are generally designed for large-scale systems or require expensive and high-performance devices, and thus are difficult to introduce into enterprise systems from both budgetary and technological standpoints. Currently, opportunities for adopting these technologies are limited.

ALAXALA Networks provides a new solution to these problems: network partitions.

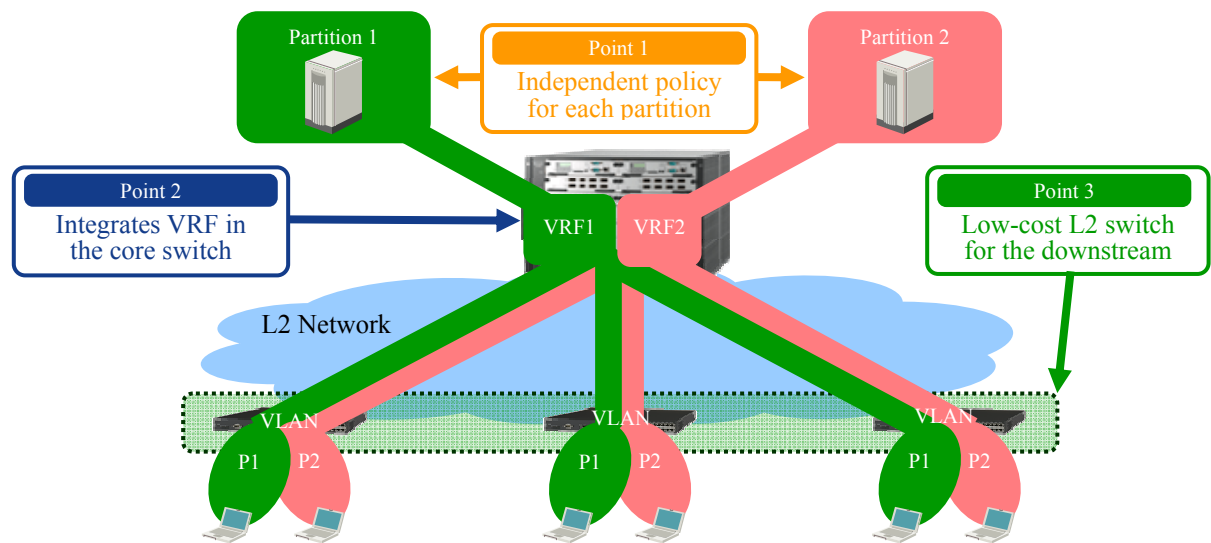


Figure 1.1-1 Network partition: A simple network virtualization

Network partition uses a combination of VRF (Virtual/VPN Routing and Forwarding) technology that logically separates Layer 3 functionality and VLAN technology that establishes Layer 2 logical networks. This combination allows the creation of multiple logical networks with a simple physical configuration.

Actual operation of network partitions requires you to know about the configuration of VRF (which is not as complicated as MPLS-VPN) and the traditional concepts and configurations of VLANs. Required devices include any one of the AX6700S, AX6600S, or AX6300S series switches with an option license for VRF (OP-NPAR) as the core, and L2 switches, such as a AX2400S series or the AX1200S series one, as the distribution or access edges. Network partition provides a solution for establishing a virtualized enterprise network system with advantages in cost and technology.

1.2 VRF and partitions

One of the core technologies of network partition is Virtual/VPN Routing and Forwarding (VRF), which handles multiple logically separated Layer 3 networks in a single device.

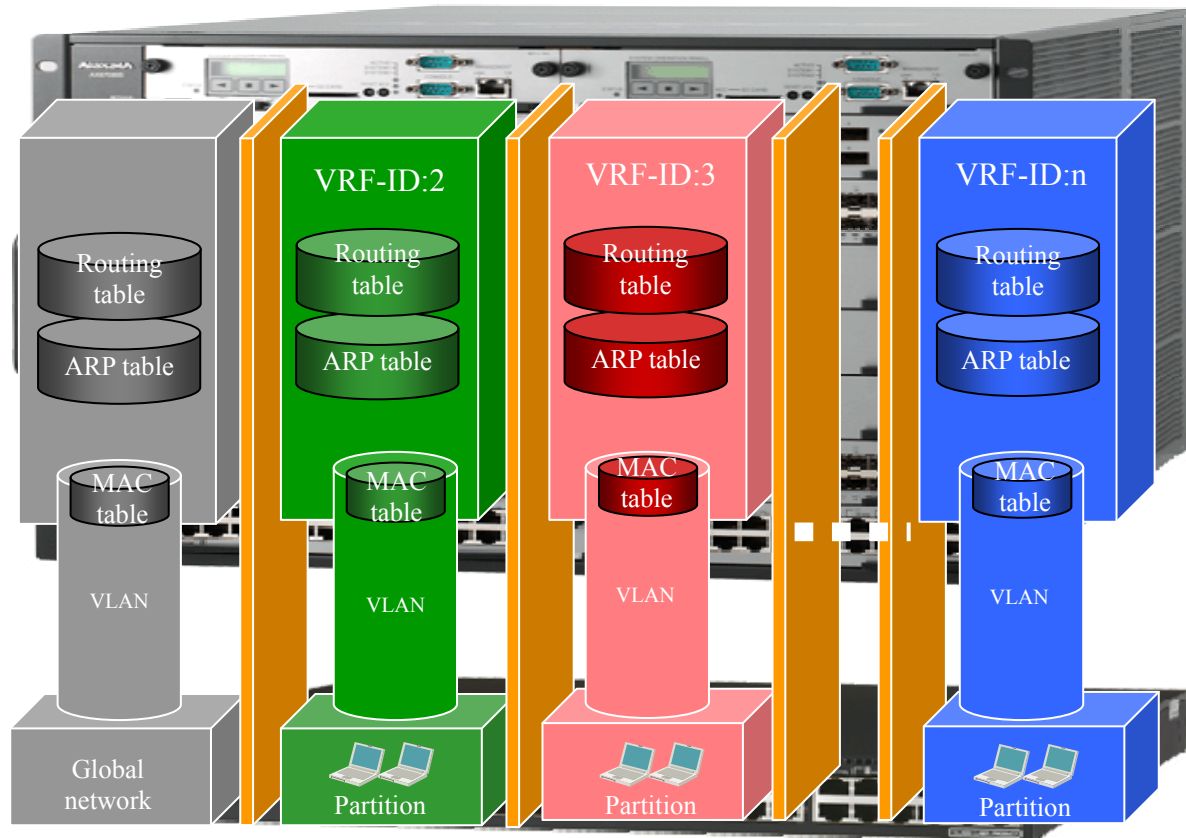


Figure 1.2-1 VRF and partitions

In VRF, the fundamental information of the Layer 3 network (routing tables and ARP tables) is controlled and managed in each separate network. The integration of the logical Layer 3 network separated by VRF and the logical Layer 2 network separated by VLANs is called the *partition* for each separated network unit.

Each partition of a device with VRF functionality is identified with an individually assigned, unique ID called a *VRF-ID*. There is, however, a network containing a partition without a VRF-ID that is used for overall system management. This is called a *global network*. A global network has broader support than common VRF for system management functionality, including telnet, FTP and syslog.

1.3 Combined L2 networks

In Network Partition, high availability is required to handle multiple networks. To achieve this, various routing protocols (static, RIP OSPF, and BGP) are independently available for each partition in the Layer 3 networks.

Further, Network Partition combined with link aggregation and ring protocols is available in Layer 2 networks (GSRP is also available starting with software ver.11.2.). This allows you to implement a system that takes advantage of the various types of L2 networks, such as high-availability, fault-tolerant networks (FT networks), as well as ring networks, which feature reliability and configuration flexibility.

The figure below is an example of a system utilizing the benefits described above.

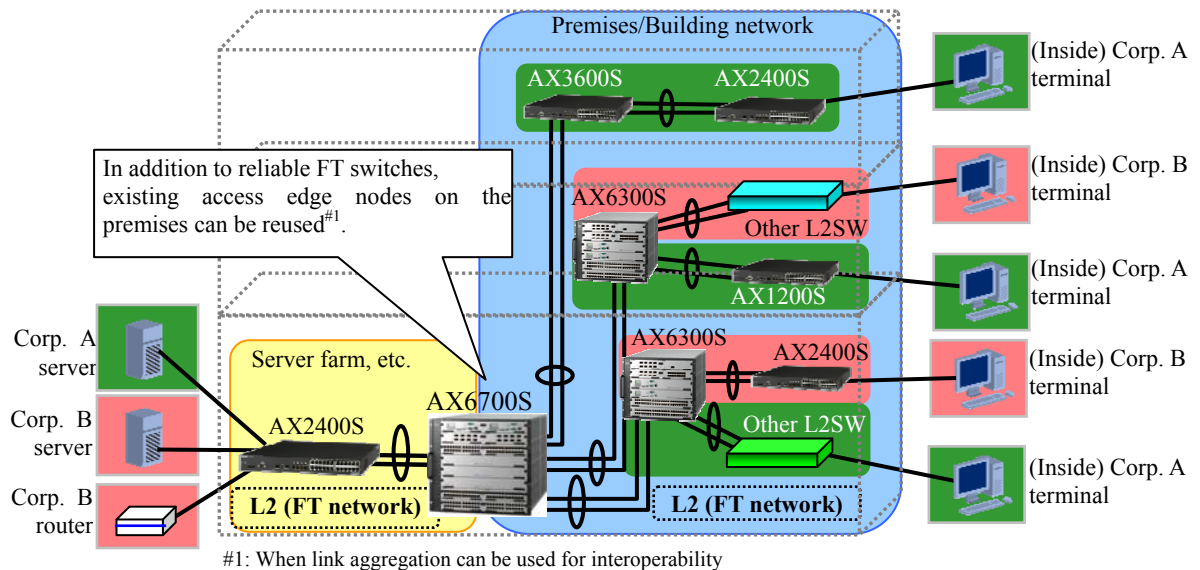


Figure 1.3-1 Example of a configuration for a building network with FT networks and network partition

Network partition combined with FT networks enables you to effectively implement a network system that has both the high availability of FT networks and the high security achieved by separation into partitions. In addition, because FT networks are mainly composed of core devices whose internal modules are duplicated and line connections with surrounding switches are achieved through link aggregation, L2 switches of other vendors, together with those of ALAXALA, can be used as the access edge devices, providing cost advantages when proposing replacements.

As an example, Figure 1.3-1 illustrates a building occupied by more than one company (Corp. A and Corp. B). In addition to sufficient reliability for the entire network system, each company requires an independent network for security reasons, with a minimum level of additional equipment and cost increase. Network partition with an FT network is the optimal solution to meet these requirements.

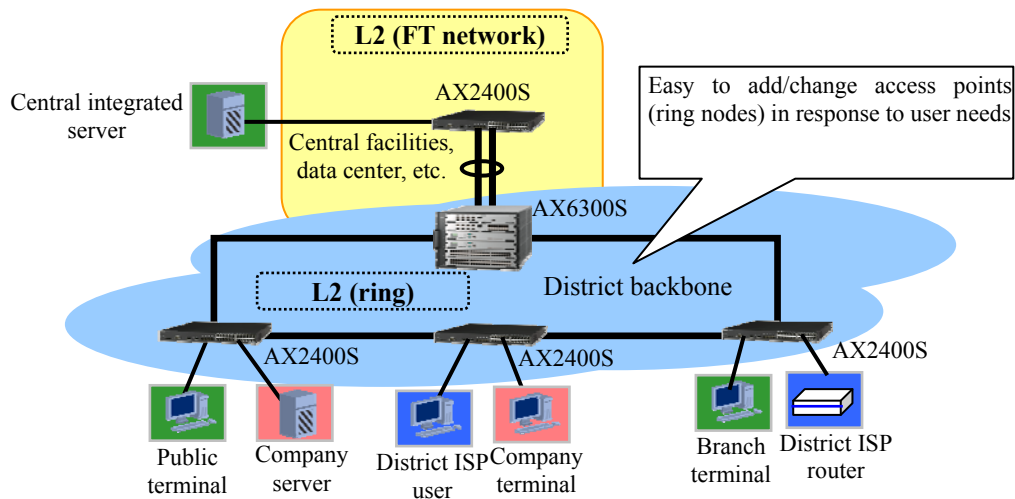


Figure 1.3-2 Example of a self-management VPN utilizing a ring network and network partition

Network Partition combined with a ring network using a ring protocol allows you to integrate the high reliability and availability of the ring protocol with the easy configuration of partitions. Thus, you are able to accommodate changes in network scale with minimum investment.

As shown in Figure 1.3-2, in a self-management VPN system where a municipality-owned public VPN is used to provide communication service, a district backbone network requires high reliability to prevent system overflow and achieve system recovery with a minimum downtime period, and requires flexibility to achieve quick change of system configuration in response to increase/decrease in users without influencing the performance of the system. Network partition with a ring network meets these needs. This solution also has the advantage of reducing additional costs.

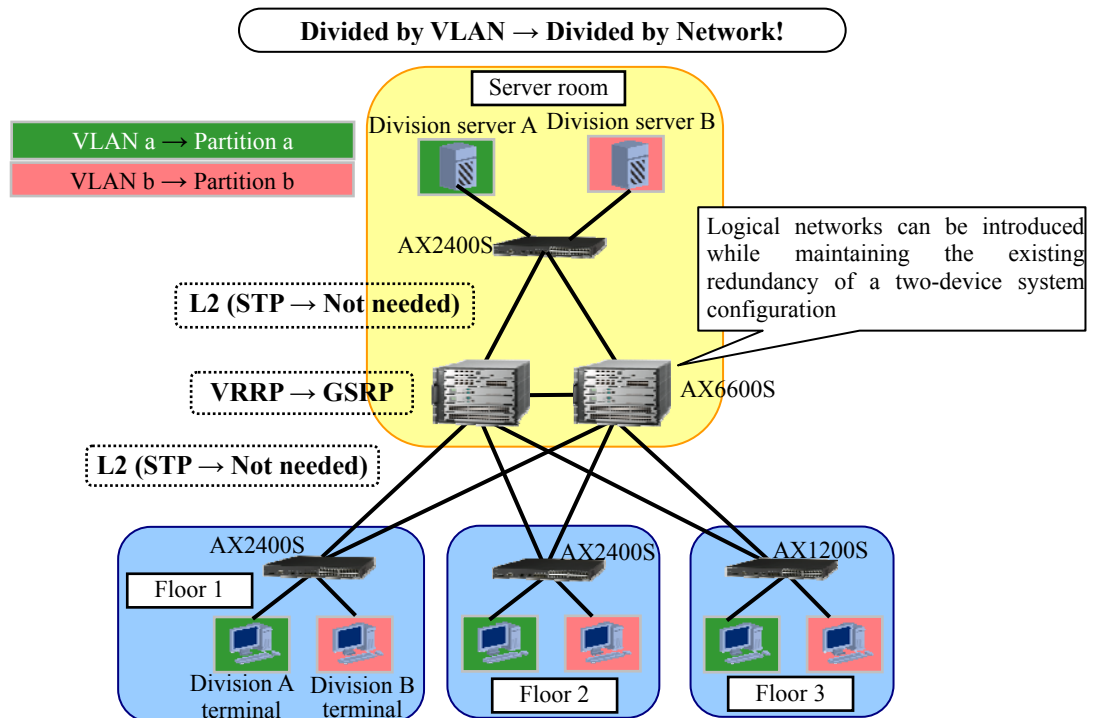


Figure 1.3-3 Example of the replacement of GSRP with network partition

Starting with software ver.11.2, the parallel use of VRF and GSRP is supported. Network partition is now applicable to a redundant system composed of two core switches.

Assume, for example, an average redundant system composed of two core switches forming a VRRP network, and access edge switches forming an STP network (see Figure 1.3-3). For such a system, GSRP is recommended as a method of introducing Network Partition into an existing redundant system without changing its topology. For example, it is possible to change a network configuration logically, from VLAN-based network division to subnet-based network division, without changing the configuration physically.

1.4 Inter-partition communication and shared networks

Network partition can be used to handle multiple logically distinguished networks. Basically, each partition has an independent network. Partitions, however, are able to communicate with each other.

Communications between partitions are achieved through route-filtering setting enhanced for VRF. It is also possible to use inter-partition communications to establish a separate network that can be connected from independent partitions. A network through such partitions is called a *shared network*. A network that permits inter-partition communication is also called an *extranet*.

A shared network effectively decreases the resources required for operation and administration of the entire network, and enables you to unify the administrative information of each partition and collect all the information on the shared network, while maintaining independence (access blocking) between partitions.

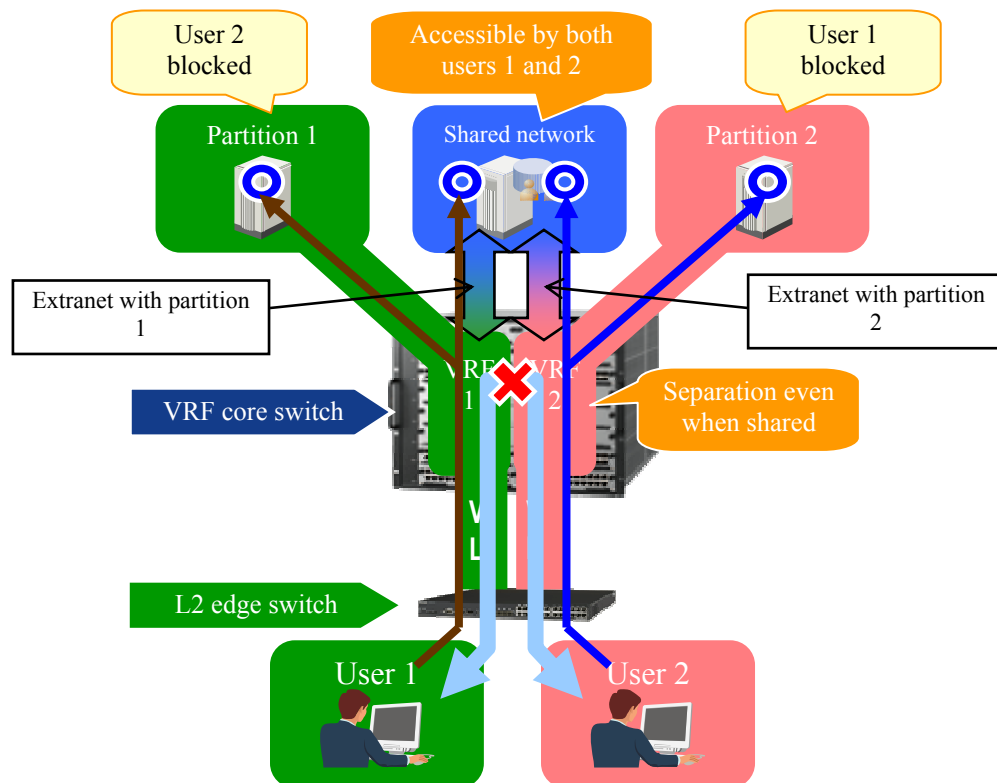


Figure 1.4-1 Concept of a shared network

2. Accommodating Conditions and Support Status

2.1 Accommodating conditions

This section describes the conditions that are specifically related to VRF in the manual (*AX6700S-AX6300S Software Manual Configuration Guide Vol.1, 3.2 Device Capacities*).

The other required conditions are regarded as common to any VRF.

(1) Number of table entries (common to the AX6700S, AX6600S, and AX6300S series)

The number of table entries for each route is shown in the tables in the manual. Please take careful note of the following when using VRF:

- The maximum number of entries when using VRF is the sum of the entries in all VRF instances.
- A route is added per VRF instance when using the loopback interface in the VRF instance.
- A route is added per VRF instance when using RIPv2 in the VRF instance.
- Two routes are added per VRF instance when using OSPF in the VRF instance.
- A route is consumed as device-specific information per VRF instance, if using VRF.

(29) Resources for unicast routing (common to the AX6700S, AX6600S, and AX6300S series)

When using OSPF with VRF, the maximum number of neighboring routers for a device is 200. In addition, make sure that the product of the number of LSAs retained by each VRF instance and the number of neighboring routers for each VRF instance does not exceed 200,000.

When using OSPFv3 with VRF, the maximum number of neighboring routers for a device is 100. In addition, make sure that the product of the sum of LSAs retained by all VRF instances and the number of neighboring routers for all VRF instances does not exceed 100,000.

(30) IPv4 multicast

When using IPv4 multicast for multiple VRF instances, the sum of the global network and VRF instances should not exceed the values specified by the accommodating conditions below.

Table 2.1-1 Maximum number of IPv4 multicasts

Item	AX6700S		AX6600S	AX6300S
	BSU-LA	BSU-LB	CSU-1B ^{#1}	MSU-1B ^{#1}
PIM-SM/SSM multicast interfaces	127 per device	255 per device		
Interfaces that support IGMP	127 per device	255 per device		
Message sources per group	256 per group			
PIM-SM/SSM multicast channel information entries ((S,G) entries, (*,G) entries, and negative caches; S = sender IP address, G = group address)	4,000 per device	8,000 per device		
Settings (pairs of source and group) of the coordination of PIM-SSM in IGMPv2/IGMPv3 (EXCLUDE mode)	256 per device			
Records processed per report in IGMPv3	32 records per message 32 sources per record			
IGMP Groups	256 per device			
Neighboring multicast routers	256 per device			
Rendezvous points	2 per group			
Groups available as rendezvous points per device ^{#2}	128 per device			
Total groups assigned to a rendezvous point per network (VPN)	128 per network (VPN) 256 per device ^{#3}			
BSR candidates per network (VPN)	16 per network (VPN) 256 per device ^{#3}			
Static groups	256 per device			
Static rendezvous point (RP) router addresses	16 per device			
Sources per IGMP group	256 per group			
Total number of downstream interfaces in the multicast relav entries	140,000 per device	280,000 per device		

Item	AX6700S		AX6600S	AX6300S
	BSU-LA	BSU-LB	CSU-1B ^{#1}	MSU-1B ^{#1}
Multicast-enabled VRF instances	127 per device	249 per device		

- #1 Support for VRF in the AX6600S series is active only when CSU-1B or CSU-1B1 is incorporated. Support for VRF in the AX6300S is active only when MSU-1B or MSU-1B1 is incorporated.
- #2 When a rendezvous point is set without specifying a group, the default group is assigned. When setting rendezvous points in the global network and VRF instances, you must meet the requirements for the total group count in a device or network (VPN), with the default group counted as one.
- #3 This indicates the total number in the global network and the networks connecting to all the VRF instances in a device.

(31) IPv6 multicast

When using IPv6 multicasts for multiple VRF instances, the sum of the global network and all VRF instances should not exceed the values specified by the accommodating conditions below.

Table 2.1-2 Maximum number of IPv6 multicasts

Item	AX6700S		AX6600S	AX6300S
	BSU-LA	BSU-LB	CSU-1B ^{#1}	MSU-1B ^{#1}
PIM-SM/SSM multicast interfaces	127 per device	255 per device		
MLD-enabled interface	127 per device	255 per device		
Communication sources per group	256 per group			
PIM-SM/SSM multicast channel information entries ((S,G) entries, (*,G) entries, and negative caches; S = sender IP address, G = group address)	1,000 per device	8,000 per device		
Settings (pairs of source and group) of the coordination of PIM-SSM in MLDv1/MLDv2 (EXCLUDE mode)	256 per device			
Records processed per report in MLDv2	32 records per message 32 sources per record			
MLD groups	256 per device			
Neighboring multicast routers	256 per device			
Rendezvous points	2 per group			
Groups available as rendezvous points per device ^{#2}	128 per device			
Total groups assigned to a rendezvous point per network (VPN)	128 per network (VPN) 256 per device ^{#3}			
BSR candidates per network (VPN)	16 per network (VPN) 256 per device ^{#3}			
Static groups	2,000 per device	4,000 per device		
Static rendezvous point (RP) router addresses	16 per device			
Sources per MLD group	256 per group			
Settings to handle remote multicast server addresses as directly connected servers	256 per device 16 per interface			
Total number of downstream interfaces in the multicast relay entries	140,000 per device	280,000 per device		
Multicast-enabled VRF instances	127 per device	249 per device		

- #1 Support for VRF in the AX6600S series is active only when CSU-1B or CSU-1B1 is incorporated. Support for VRF in the AX6300S series is active only when MSU-1B or MSU-1B1 is incorporated.
- #2 When a rendezvous point is set without specifying a group, the default group is assigned. When setting rendezvous points in the global network and VRF instances, you must meet the requirements for the total group count in a device or network (VPN), with the default group counted as one.
- #3 This indicates the total number in the global network and the networks connecting to all the VRF instances in a device.

(32) Number of configurable VRF instances (common to the AX6700S, AX6600S, and AX6300S series)

The number of VRF instances that can be configured is shown below. A global network is not included in the number of VRF instances that can be configured.

Table 2.1-3 Number of VRF instances that can be configured (common to the AX6700S/AX6300S)

VRF operation modes (parameters specified with the vrf mode command)	Number of specifiable VRF instances (VRF-IDs specified)
axrp-enable (Only IPv4 is available for configuring VRF instances and can be used with the ring protocol)	63 (VRF-ID: 2-64)
l2protocol-disable (Only IPv4 is available for configuring VRF instances and cannot be used with L2 redundancy protocols ^{#1})	249 (VRF-ID: 2-250)
axrp-enable-ipv4-ipv6 (IPv4 and IPv6 are available for configuring VRF instances and can be used with the ring protocol)	63 (VRF-ID: 2-64)
gsrp-enable-ipv4-ipv6 (IPv4 and IPv6 are available for configuring VRF instances and can be used with GSRP)	124 (VRF-ID: 2-125)
l2protocol-disable-ipv4-ipv6 (IPv4 and IPv6 are available for configuring VRF instances and cannot be used with L2 redundancy protocols ^{#1})	249 (VRF-ID: 2-250)

#1 Spanning trees, GSRP, and the ring protocol are included.

2.2 VRF support status

As with general networks, various protocols are available for logical networks (partitions) created using VRF. In contrast, the range of support for other functions depends on whether VRF is utilized (vrf mode is activated) in VRF-enabled devices. The details are described in the table below.

Table 2.2-1 Support for other functions in VRF-enabled devices

Item		When using VRF	Remarks
VLAN	Port VLAN	o	
	Protocol VLAN	o	
	MAC VLAN	o	
	Tag conversion	o	
	VLAN tunneling	o	
L2 protocol	Spanning trees	×	Excluding between the VRF and device
	Ring protocol	o	
IGMP snooping/MLD snooping		o	MLD querier is excluded
Filter	Filter	o	
	uRPF	o	Only for IPv4
QoS		o	
L2 Authentication	IEEE802.1X	×	Excluding between the VRF and device
	Web Authentication	×	
	MAC Authentication	×	
	Authenticated VLAN	×	
High reliability	Link aggregation	o	
	GSRP	o	
	VRRP	o	Only for IPv4
Fault detection	L2 loop detection	o	
	Storm control	o	
	IEEE802.3ah/UDLD	o	
Remote network management	SNMP	o	Only for IPv4
	syslog output	o	

Item		When using VRF	Remarks
	Email sending	●	
	sFlow statistics	△	Scope of the statistics covers VRF instances, although the router-type and gateway-type extended data formats collected at VRF-enabled interfaces are excluded. The collector only covers the global network.
Management of neighboring device information	LLDP	△	Organizationally defined TLV extensions are supported only by the global network
	OADP	△	No address info is included in VRF
Port mirroring		○	
L3 relay	IPv4 unicast relay	○	
	IPv4 unicast relay between VRF instances	○	
	IPv4 multicast relay	○	
	IPv4 multicast relay between VRF instances	○	
	IPv6 unicast relay	○	
	IPv6 unicast relay between VRF instances	○	
	IPv6 multicast relay	○	
	IPv6 multicast relay between VRF instances	×	
NULL interface		○	The global network and VRF instances share a single NULL interface
Policy-based routing		○	Inter-VRF routing enabled. Only for IPv4
DHCP/BOOTP relay agent		○	
DHCP server		●	
IPv4 static routing		○	Inter-VRF routing available.
IPv6 static routing		○	Inter-VRF routing available.
IPv4 unicast Routing protocol	RIP	○	
	OSPF	○	
	BGP4	○	
	Route filtering	○	
IPv6 unicast routing protocol		○	
IPv4 multicast Routing protocol	IGMP	○	
	PIM-SM	○	
	PIM-SSM	○	
IPv6 multicast routing protocol		○	
Operation & maintenance	ping/ping ipv6	○	
	tracert/tracert ipv6	○	
	Telnet client	○	
	Remote login via telnet	●	
	FTP	●	
	DNS resolver	●	
	NTP	○	

(Legend) ○: Available in both the VRF logical networks and the global network

△: Available in the VRF logical networks, with some limitations

●: Available only in the global network. Not available in the VRF logical networks.

×: Not available in either the VRF logical network or the global network

Note: These limitations do not apply if VRF is not used.

3. Examples of Configuring Systems with Network Partitions

As described in Chapter 1, the basic configuration of network partitions is a combination of VRF-enabled L3 core switches and L2 networks. This chapter describes how to **configure** a system using a detailed example.

3.1 Network partitions in an FT network

Given below is an example of a network partition system based on an FT network configured using an AX6700S L3 core switch as an FT switch.

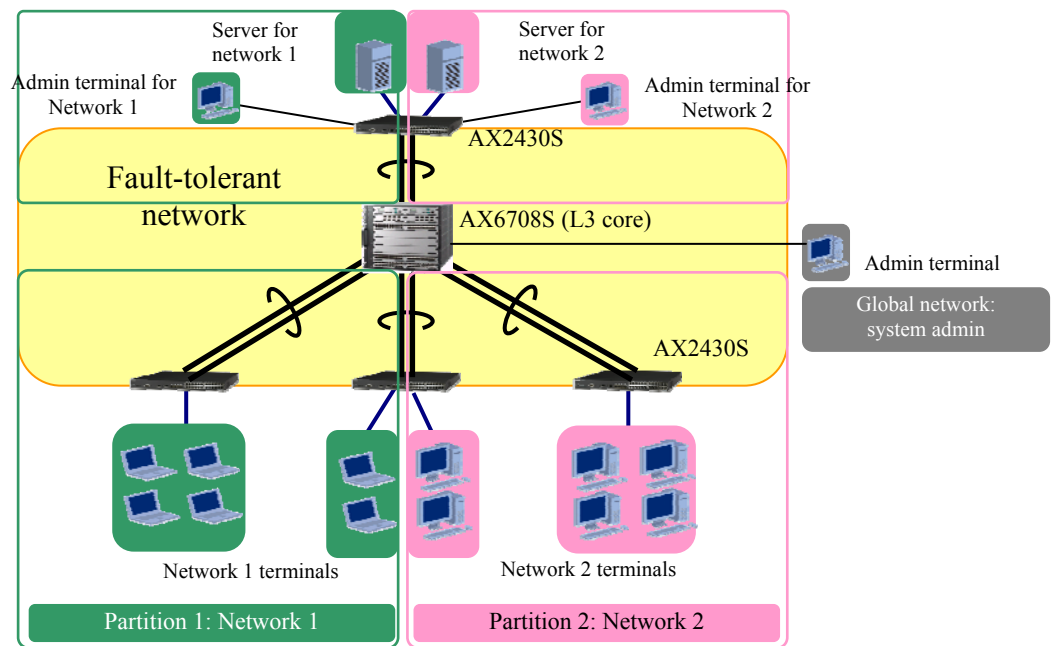


Figure 3.1-1 Network partitions in an FT network

The physical configuration appears to be similar to a normal FT network system without network partition. However, network partition enables you to establish multiple logically separated L3 network systems. This advantage allows you to integrate the stability of an FT network into multiple networks created using network partitions.

This configuration example shows two independent networks used in the system.

The logical configuration of the system is illustrated below:

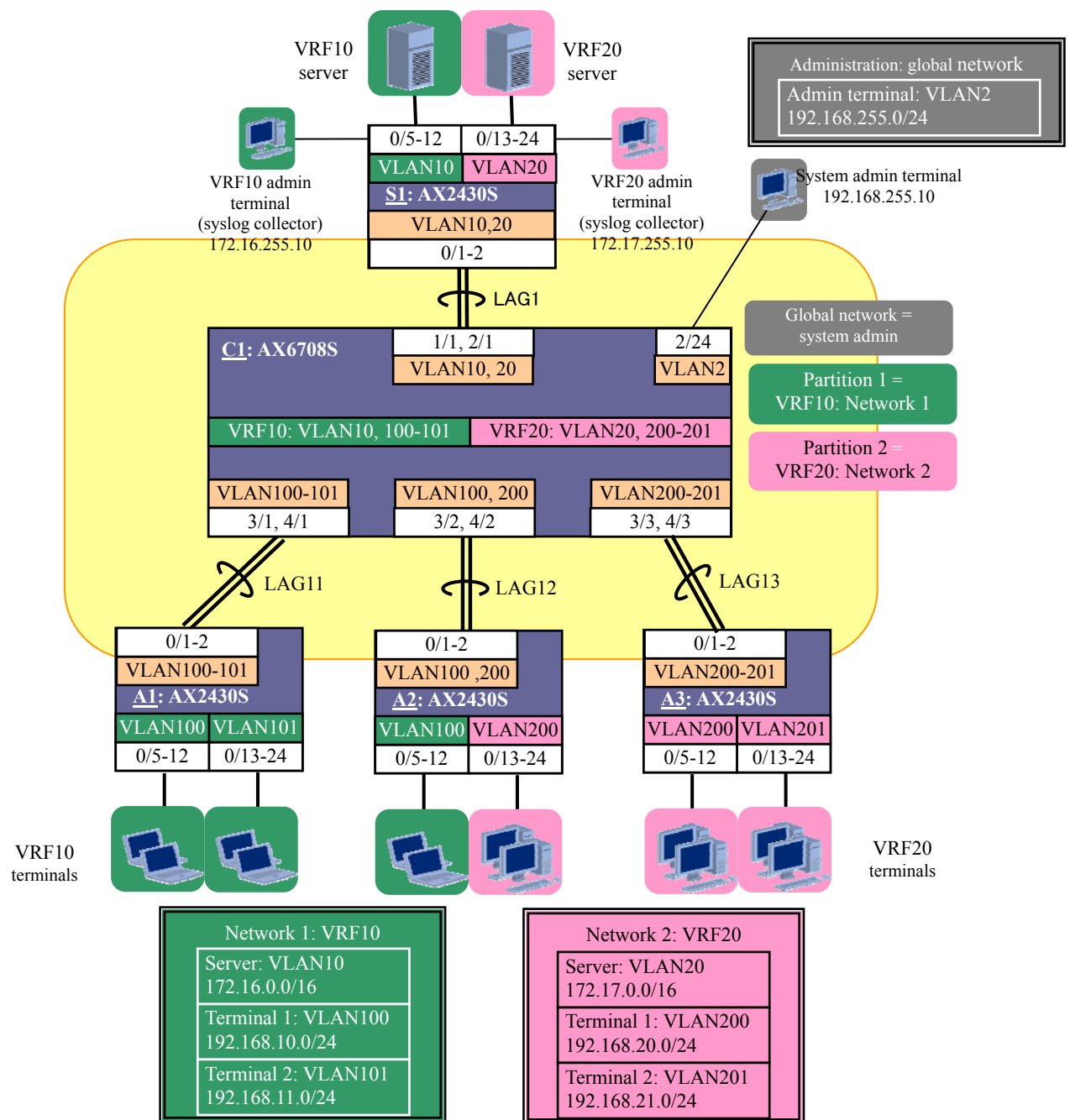


Figure 3.1-2 Logical configuration

Node C1 (core), with an AX6708S series switch configured as an FT switch, uses VRF to handle two independent networks, VRF10 for Network 1 and VRF20 for Network 2. Network 1 uses OSPF, and Network 2 uses RIP to inform its routes. System administration is maintained through the global network, enabling remote control of the overall system.

Access edge nodes, using AX2430S series L2 switches, connect with core node C1 via channel groups (link aggregation).

The important points and an example of the configuration for the devices are given below.

3.1.1 Important points in the configuration

(1) Assign the VRF configuration only to the L3 core device

Assign the VRF configuration only to the L3 core device. No VRF settings are needed for any peripherals consisting of L2 networks. VRF IDs, the identifiers for VRF instances, must be a number equal to or greater than 2. When L2 protocol is not used at the same time, as in this configuration, the maximum number cannot exceed 250.

(2) Disable spanning trees

Using VRF requires the prohibition of spanning trees. You need to disable spanning trees (PVST+), which are activated by default.

(3) Activate VRF in a mode where no L2 protocol is enabled at the same time

L2 protocol is not used simultaneously if the system is based on an FT network. This setting is performed using the vrf mode command. When using the vrf mode command to **change** the operation mode, some of the devices (the BSU in the AX6700S and the PSP in the AX6300S series) must be restarted. (A confirmation message will be displayed when the command is executed.)

(4) Assign VLANs to the partitions (VRF)

The vrf forwarding setting in the VLAN interfaces defines which partition is assigned to which VLAN. If this setting is omitted, the VLAN is assigned to the global network.

(5) Routing protocols, if any, must be assigned to a partition (VRF) as an operating point

As with VLANs, routing protocols must be assigned to one of the partitions. However, the method for specifying VRF is different according to the routing protocols used.

For OSPF, define VRF IDs using the router command, which specifies the use of OSPF. For RIP, define the VRF instance as one of the ipv4 address families.

If there is no VRF setting, the protocol will operate in the global network.

(6) Remote control must be via the global network

If you want to remotely control VRF-enabled devices via telnet or FTP, you must use the global network. Remote log collection (syslog) is available from any partition, starting from software ver.11.2.

3.1.2 Configuration example

Given below is a configuration example describing a starting point for system configuration. For the overall configuration, see [the Appendix](#).

(1) Configuration of the core node

C1 (AX6708S) configuration	
Prohibition of spanning trees	
(config)# spanning-tree disable	The AX series default value for PVST+ is enabled, therefore, disable PVST+. (Important point (2))
VRF configuration	
(config)# vrf mode l2protocol-disable All BSU will be restarted automatically when the selected mode differs from current mode. Do you wish to change mode (y/n): y	Set VRF so as to not be used with the L2 protocol. (Important point (3)) (A prompt for restarting the BSU is displayed. Enter Y if it is OK to restart.)
(config)# vrf definition 10 (config)# vrf definition 20	Declare that VRF10 is to be used. (Important point (1)) Declare that VRF20 is to be used. (Important point (1))
VLAN configuration	
(config)# vlan 2,10,20,100-101,200-201	Define the settings of the VLANs to be used.
VLAN interface configuration	
(config)# interface vlan 2 (config-if)# ip address 192.168.255.1 255.255.255.0	VLAN2 is used in the global network for system administration. (Important point (6)) Assign an IP address to VLAN2.
(config)# interface vlan 10 (config-if)# vrf forwarding 10 (config-if)# ip address 172.16.0.1 255.255.0.0	Use VLAN10 in VRF10. (Important point (4)) Assign an IP address to VLAN10.
(config)# interface vlan 20 (config-if)# vrf forwarding 20 (config-if)# ip address 172.17.0.1 255.255.0.0	Use VLAN20 in VRF20. (Important point (4)) Assign an IP address to VLAN20.
(config)# interface vlan 100 (config-if)# vrf forwarding 10 (config-if)# ip address 192.168.10.1 255.255.255.0	Use VLAN100 in VRF10. (Important point (4)) Assign an IP address to VLAN100.
(config)# interface vlan 101 (config-if)# vrf forwarding 10 (config-if)# ip address 192.168.11.1 255.255.255.0	Use VLAN101 in VRF10. (Important point (4)) Assign an IP address to VLAN101.
(config)# interface vlan 200 (config-if)# vrf forwarding 20 (config-if)# ip address 192.168.20.1 255.255.255.0	Use VLAN200 in VRF20. (Important point (4)) Assign an IP address to VLAN200.
(config)# interface vlan 201 (config-if)# vrf forwarding 20 (config-if)# ip address 192.168.21.1 255.255.255.0	Use VLAN201 in VRF20. (Important point (4)) Assign an IP address to VLAN201.
Configuration of physical port interfaces	
Port settings	
(config)# interface gigabitethernet 2/24 (config-if)# switchport access vlan 2	Define port 2/24 as the VLAN2 access port for system administration.
(config)# interface range gigabitethernet 1/1, gigabitethernet 2/1 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 1 mode on	Ports 1/1 and 2/1 form channel group 1 for connection with device S1.
(config)# interface range gigabitethernet 3/1, gigabitethernet 4/1 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 11 mode on	Ports 3/1 and 4/1 form channel group 11 for connection with device A1.

C1 (AX6708S) configuration	
<pre>(config)# interface range gigabitethernet 3/2, gigabitethernet 4/2 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 12 mode on (config)# interface range gigabitethernet 3/3, gigabitethernet 4/3 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 13 mode on</pre>	<p>Ports 3/2 and 4/2 form channel group 12 for connection with device A2.</p> <p>Ports 3/3 and 4/3 form channel group 13 for connection with device A3.</p>
Port channel settings	
<pre>(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 10,20 (config)# interface port-channel 11 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 100-101 (config)# interface port-channel 12 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 100,200 (config)# interface port-channel 13 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 200-201</pre>	<p>Define port channel 1 as the trunk port where forwarding to VLAN10 and 20 is permitted.</p> <p>Define port channel 11 as the trunk port where forwarding to VLAN100 and 101 is permitted.</p> <p>Define port channel 12 as the trunk port where forwarding to VLAN100 and 200 is permitted.</p> <p>Define port channel 13 as the trunk port where forwarding to VLAN200 and 201 is permitted.</p>
Routing protocol configuration	
<pre>(config)# router ospf 1 vrf 10 (config-router)# network 172.16.0.0 0.0.255.255 area 0 (config-router)# network 192.168.10.0 0.0.1.255 area 0 (config)# router rip (config-router)# address-family ipv4 vrf 20 (config-router-af)# network 172.17.0.0 0.0.255.255 (config-router-af)# network 192.168.20.0 0.0.1.255</pre>	<p>Specify OSPF as the routing protocol for VRF10. (Important point (5))</p> <p>Specify RIP as the routing protocol for VRF20. (Important point (5))</p>
Configuration for remote control of the device	
<pre>(config)# logging host 192.168.255.10 (config)# logging host 172.16.255.10 vrf 10 (config)# logging host 172.17.255.10 vrf 20 (config)# line vty 0 2 (config)# ftp-server</pre>	<p>Specify the host for collecting the syslog. Specify the host for collecting the syslog in VRF10. Specify the host for collecting the syslog in VRF20. (Important point (6))</p> <p>Permit telnet login (up to 2 users at a time).</p> <p>Activate the FTP server.</p>

(2) Configuration of access nodes

There are no VRF configuration items in the configuration of access nodes. The partition (VRF) to which an access node is related is determined by the partition to which the VLAN handled by the access node belongs. The L3 core node in which the VRF configuration is defined handles such settings.

S1 (AX2430S) configuration	
Prohibition of spanning trees	
(config)# spanning-tree disable	The AX series default value for PVST+ is enabled, therefore, disable PVST+.
VLAN configuration	
(config)# vlan 10,20	Define the settings of the VLANs to be used.
Configuration of physical port interfaces	
Port settings	
(config)# interface range gigabitethernet 0/1-2 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 1 mode on (config)# interface range gigabitethernet 0/5-12 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 10 (config)# interface range gigabitethernet 0/13-24 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 20	Ports 0/1-2 form channel group 1 for connection with device C1. Ports 0/5-12 form access ports for VLAN10 between the server/terminals and Network 1 (VRF10). Ports 0/13-24 form access ports for VLAN20 between the server/terminals and Network 2 (VRF20).
Port channel configuration	
(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 10,20	Define Port Channel 1 as the trunk port where forwarding to VLAN10 and 20 is permitted.

A1 (AX2430S) configuration	
Prohibition of spanning trees	
(config)# spanning-tree disable	The AX series default value for PVST+ is enabled, therefore, disable PVST+.
VLAN configuration	
(config)# vlan 100-101	Define the settings of the VLANs to be used ^{#1} .
Physical port interface configuration	
Port configuration	
(config)# interface range gigabitethernet 0/1-2 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 11 mode on (config)# interface range gigabitethernet 0/5-12 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 100 (config)# interface range gigabitethernet 0/13-24 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 101	Ports 0/1-2 form channel group 11 for connection with device C1. Ports 0/5-12 form access ports for use in the server/terminals of VLAN100 inside Network 1 (VRF10) ^{#1} . Ports 0/13-24 form access ports for use in the server/terminals of VLAN101 inside Network 1 (VRF10) ^{#1} .
Port channel configuration	
(config)# interface port-channel 11 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 100-101	Define port channel 11 as the trunk port where forwarding to VLAN100-101 is permitted ^{#1} .

#1 The configurations for devices A2 and A3 are the same as for A1, except for the VLAN configuration.

3.2 Network partitions in a ring network

This section shows an example of configuring network partitions in a network where AX6300S L3 core switches are used together with a ring protocol.

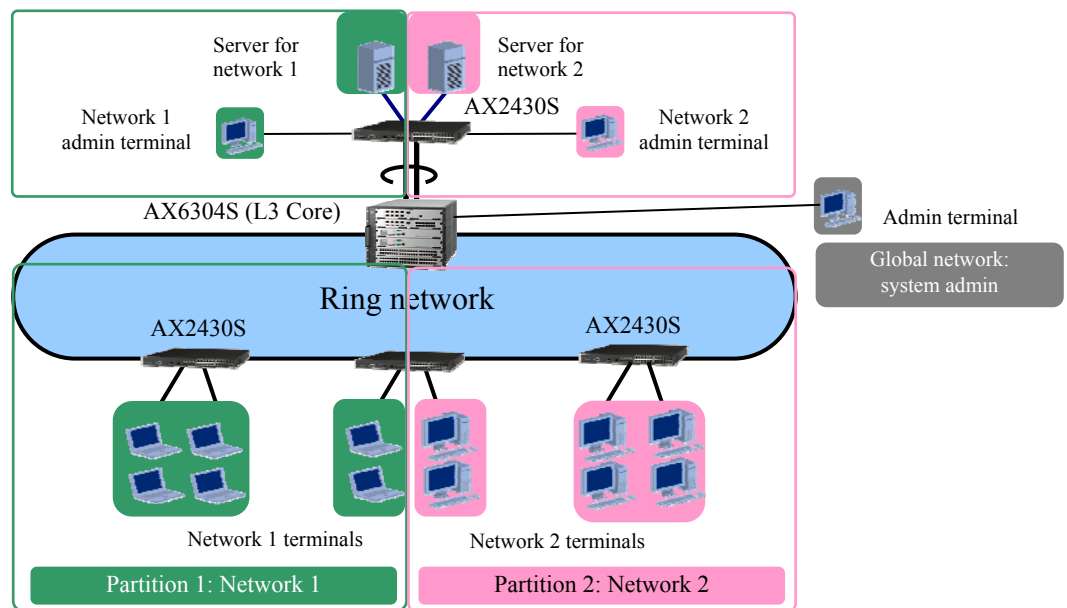


Figure 3.2-1 Network partitions in a ring network

Physically, the system uses a normal ring protocol in this configuration.

Using a ring protocol for the L2 networks makes the system scalable and flexible to the type of lines used. In particular, use in combination with network partition provides many advantages for systems requiring flexible settings for each network, such as easy addition and removal of partitions.

This configuration example shows two independent networks used in the system.

The logical configuration of the system is illustrated below:

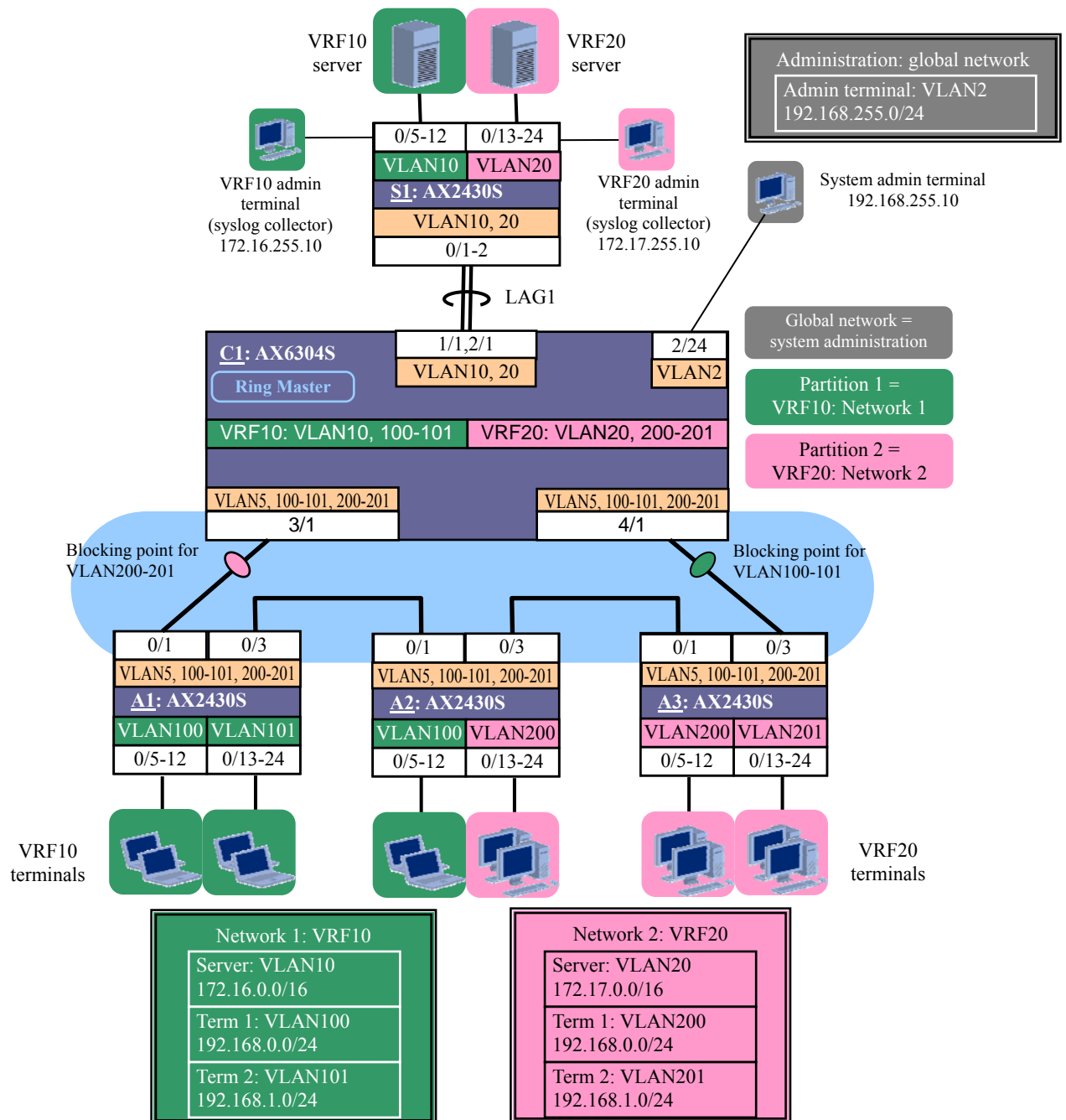


Figure 3.2-2 Logical configuration

Node C1 (core), configured with an AX6304S used as the FT switch, uses VRF to handle two independent networks, VRF10 for Network 1 and VRF20 for Network 2. Access edge nodes are configured using an AX2430S series switch, an L2 switch supporting ALAXALA's ring protocol. Node C1 and the edge nodes are connected via a ring network.

The ability of ring networks to assign different routes to each separate VLAN of the partitions is used. This enables the load balance per partition to reduce the load on the ring network.

System administration is maintained through the global network, enabling the remote control of the overall system.

The important points and an example of the configuration for the device are given below.

3.2.1 Important points in the configuration

(1) Assign the VRF configuration only to the L3 core device

Assign the VRF configuration only to the L3 core device. No VRF settings are needed for any peripherals (ring nodes, etc.) consisting of L2 networks. VRF IDs, the identifiers for VRF instances, must be a number equal to or greater than 2. The upper limit of the value is 64 if the ring protocol is used as the L2 protocol.

(2) Disable spanning trees

Using VRF requires the prohibition of spanning trees. You need to disable spanning trees (PVST+), which are activated by default.

(3) Activate VRF in a mode using the ring protocol

Specify the ring protocol as the L2 protocol if the system is based on a ring network. This setting is performed using the vrf mode command. When using the vrf mode command to **change** the operation mode, some of the devices (the BSU in the AX6700S series and the PSP in the AX6300S series) must be restarted. (A confirmation message will be displayed when the command is executed.) Parallel use of the ring protocol and STP or GSRP is not permitted in VRF-enabled devices^{#1}.

#1 In VRF-disabled ring nodes (L3 and L2 switches other than the core device), parallel use with STP and GSRP is permitted.

(4) Assign VLANs to partitions (VRF)

The vrf forwarding setting in the VLAN interfaces defines which partition is assigned to which VLAN. If this setting is omitted, the VLAN is assigned to the global network.

(5) Match the VLAN mapping IDs with the VRF-IDs

When you specify a VLAN used as an IP interface in VRF **for** VLAN ring mapping, make sure that the VRF-ID is identical to the VLAN mapping ID. Assign VLAN mapping ID 1 to the VLAN used for the global network when specifying the VLAN for VLAN mapping.

(6) Routing protocols, if any, must be assigned to a partition (VRF) as an operating point

As with VLANs, routing protocols must be assigned to one of the partitions. However, the method for specifying VRF is different according to the routing protocols used.

For OSPF, define VRF IDs using the router command, which specifies the use of OSPF. For RIP, define the VRF instance as one of the ipv4 address families.

If there is no VRF setting, the protocol will operate in the global network.

(7) Remote control must be via the global network

If you want to remotely control VRF-enabled devices via telnet or FTP, you must use the global network. Remote log collection (syslog) is available from any partition, starting from software ver.11.2.

3.2.2 Configuration example

Given below is a configuration example describing a starting point for system configuration. For the overall configuration, see [the Appendix](#).

(1) Configuration of the core node

C1 (AX6304S) configuration	
Prohibition of spanning trees	
(config)# spanning-tree disable	The AX series default value for PVST+ is enabled, therefore, disable PVST+. (Important point (2))
VRF configuration	
(config)# vrf mode axrp-enable PSP will be restarted automatically when the selected mode differs from current mode. Do you wish to change mode (y/n): y	Set VRF jointly with the ring protocol. (Important point (3)) (A prompt for restarting the PSP is displayed. Enter Y if it is OK to restart.)
(config)# vrf definition 10 (config)# vrf definition 20	Declare that VRF10 is to be used. (Important point (1)) Declare that VRF20 is to be used. (Important point (1))
VLAN configuration	
(config)# vlan 2,5,10,20,100-101,200-201	Define the settings of the VLANs to be used.
VLAN interface configuration	
(config)# interface vlan 2 (config-if)# ip address 192.168.255.1 255.255.255.0	Use VLAN2 in the global network for system administration. (Important point (7)) Assign an IP address to VLAN2.
(config)# interface vlan 10 (config-if)# vrf forwarding 10 (config-if)# ip address 172.16.0.1 255.255.0.0	Use VLAN10 in VRF10. (Important point (4)) Assign an IP address to VLAN10.
(config)# interface vlan 20 (config-if)# vrf forwarding 20 (config-if)# ip address 172.17.0.1 255.255.0.0	Use VLAN20 in VRF20. (Important point (4)) Assign an IP address to VLAN20.
(config)# interface vlan 100 (config-if)# vrf forwarding 10 (config-if)# ip address 192.168.0.1 255.255.255.0	Use VLAN100 in VRF10. (Important point (4)) Assign an IP address to VLAN100.
(config)# interface vlan 101 (config-if)# vrf forwarding 10 (config-if)# ip address 192.168.1.1 255.255.255.0	Use VLAN101 in VRF10. (Important point (4)) Assign an IP address to VLAN101.
(config)# interface vlan 200 (config-if)# vrf forwarding 20 (config-if)# ip address 192.168.0.1 255.255.255.0	Use VLAN200 in VRF20. (Important point (4)) Assign an IP address to VLAN200.
(config)# interface vlan 201 (config-if)# vrf forwarding 20 (config-if)# ip address 192.168.1.1 255.255.255.0	Use VLAN201 in VRF20. (Important point (4)) Assign an IP address to VLAN201.
Physical port interface configuration	
Ring port configuration	
(config)# interface gigabitethernet 3/1 (config-if)# link debounce time 0 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 5,100-101,200-201 (config-if)# axrp-ring-port 1	Define port 3/1 as a ring network connection. Define ports 5, 100-101, and 200-201 as the trunk ports where communication is permitted for the VLAN. Define RING ID = 1 for the ring port.
(config)# interface gigabitethernet 4/1 (config-if)# link debounce time 0 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 5,100-101,200-201 (config-if)# axrp-ring-port 1	Also define port 4/1 as a ring network connection. Define ports 5, 100-101, and 200-201 as the trunk ports where communication is permitted for the VLAN. Define RING ID = 1 for the ring port.
Port configuration	

C1 (AX6304S) configuration	
(config)# interface gigabitethernet 2/24 (config-if)# switchport access vlan 2	Define port 2/24 as the VLAN2 access port for system administration.
(config)# interface range gigabitethernet 1/1, gigabitethernet 2/1 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 1 mode on	Define ports 1/1 and 2/1 to form channel group 1 for connection with device S1.
Port channel configuration	
(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 10,20	Define port channel 1 as the trunk port where forwarding to VLAN10 and 20 is permitted.
VLAN mapping configuration	
(config)# axrp vlan-mapping 10 vlan 100-101 (config)# axrp vlan-mapping 20 vlan 200-201	Define VLAN mapping 10 of the ring as VLAN100-101 used in VRF10. (Important point (5)) Define VLAN mapping 20 of the ring as VLAN200-101 used in VRF20. (Important point (5))
Ring protocol configuration	
(config)# axrp 1 (config-axrp)# mode master (config-axrp)# control-vlan 5 (config-axrp)# vlan-group 1 vlan-mapping 10 (config-axrp)# vlan-group 2 vlan-mapping 20	Define RING ID = 1. Define this node as a master node. Define VLAN5 as the control-VLAN. Assign VLAN mapping 10 to VLAN group 1. Assign VLAN mapping 20 to VLAN group 2.
Routing protocol configuration	
(config)# router ospf 1 vrf 10 (config-router)# network 172.16.0.0 0.0.255.255 area 0 (config-router)# network 192.168.0.0 0.0.1.255 area 0	Specify OSPF as the routing protocol for VRF10. (Important point (6))
(config)# router rip (config-router)# address-family ipv4 vrf 20 (config-router-af)# network 172.17.0.0 0.0.255.255 (config-router-af)# network 192.168.0.0 0.0.1.255	Specify RIP as the routing protocol for VRF20. (Important point (6))
Configuration for remote control of the device	
(config)# logging host 192.168.255.10 (config)# logging host 172.16.255.10 vrf 10 (config)# logging host 172.17.255.10 vrf 20	Specify the host for collecting the syslog. Specify the host for collecting the syslog in VRF10. Specify the host for collecting the syslog in VRF20. (Important point (7))
(config)# line vty 0 2 (config)# ftp-server	Permit telnet login (up to 2 users at a time). Activate the FTP server.

(2) Configuration of access nodes

There is no VRF-related setting required for configuration of access nodes. A partition (VRF) to be associated with an access node is the one to which the VLAN handled by the access node belongs. The L3 core node in which the VRF configuration is defined handles such settings.

S1 (AX2430S) configuration	
Prohibition of spanning trees	
(config)# spanning-tree disable	The default value for PVST+ is enabled, therefore, disable PVST+.
VLAN configuration	
(config)# vlan 10,20	Define the settings of the VLANs to be used.
Physical port interfaces configuration	
Port configuration	
(config)# interface range gigabitethernet 0/1-2 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 1 mode on	Define ports 0/1-2 of channel group 1 for connection with device C1.
(config)# interface range gigabitethernet 0/5-12 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 10	Define ports 0/5-12 to form access ports for VLAN10 between the server/terminals and network 1 (VRF10).
(config)# interface range gigabitethernet 0/13-24 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 20	Define ports 0/13-24 to form access ports for VLAN20 between the server/terminals and network 2 (VRF20).
Port channel configuration	
(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 10,20	Define port channel 1 as the trunk port where forwarding to VLAN10 and 20 is permitted.

A1 (AX2430S) configuration	
Prohibition of spanning trees	
(config)# spanning-tree disable	The default value for PVST+ is enabled, therefore, disable PVST+.
VLAN configuration	
(config)# vlan 5,100-101,200-201	Define the settings of the VLANs to be used.
Physical port interface configuration	
Ring port configuration	
(config)# interface gigabitethernet 0/1 (config-if)# link debounce time 0 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 5,100-101,200-201 (config-if)# axrp-ring-port 1	Define port 0/1 as a ring network connection. Define ports 5, 100-101, 200-201 as the trunk ports where communication is permitted for the VLAN. Define RING ID = 1 for the ring port.
(config)# interface gigabitethernet 0/3 (config-if)# link debounce time 0 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 5,100-101,200-201 (config-if)# axrp-ring-port 1	Also define port 0/3 as a ring network connection. Define ports 5, 100-101, 200-201 as the trunk ports where communication is permitted for the VLAN. Define RING ID = 1 for the ring port.
Access port configuration	
(config)# interface range gigabitethernet 0/5-12 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 100	Define ports 0/5-12 as the access ports for the connection of the VLAN100 server or terminal in network 1 (VRF10) ^{#1} .
(config)# interface range gigabitethernet 0/13-24 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 101	Define ports 0/13-24 as the access ports for the connection of the VLAN101 server or terminal in network 1 (VRF10) ^{#2} .
VLAN mapping configuration	
(config)# axrp vlan-mapping 10 vlan 100-101 (config)# axrp vlan-mapping 20 vlan 200-201	Define VLAN mapping 10 of the ring as VLAN100-101 used in VRF10. Define VLAN mapping 20 of the ring as VLAN200-101 used in VRF20.
Ring protocol configuration	
(config)# axrp 1 (config-axrp)# mode transit (config-axrp)# control-vlan 5 (config-axrp)# vlan-group 1 vlan-mapping 10 (config-axrp)# vlan-group 2 vlan-mapping 20	Define RING ID = 1. Define this node as a transient node. Define VLAN5 as the control-VLAN. Assign VLAN mapping 10 to VLAN group 1. Assign VLAN mapping 20 to VLAN group 2.

#1 Devices A2 and A3 are configured in the same way as device A1, except when the VLAN to be handled is different.

3.3 Network partition using GSRP

The following shows an example of configuring a network partition system with GSRP in a network that uses the AX6300S as the L3 core switch.

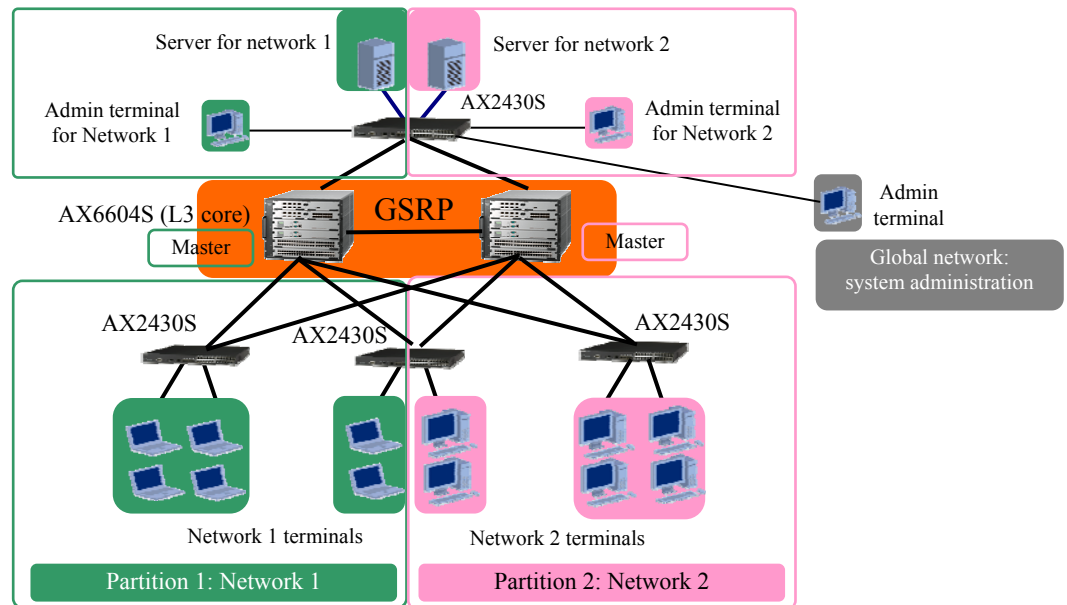


Figure 3.3-1 GSRP-configured network partitions

In this configuration as well, the system is a redundant system that is physically configured using ordinary GSRP. One of the advantages of GSRP is that a redundant system based on VRRP and STP can be replaced without physically changing the configuration. Additionally, in software ver.11.2, a VRF function can be used together with GSRP. Therefore, a network partition can be easily established without significantly changing the physical configuration of the redundant system previously configured using VRRP and STP.

This example shows how to configure a system composed of two independent networks, based on a redundant configuration system consisting of two existing switch devices.

The logical configuration in this example is as shown below.

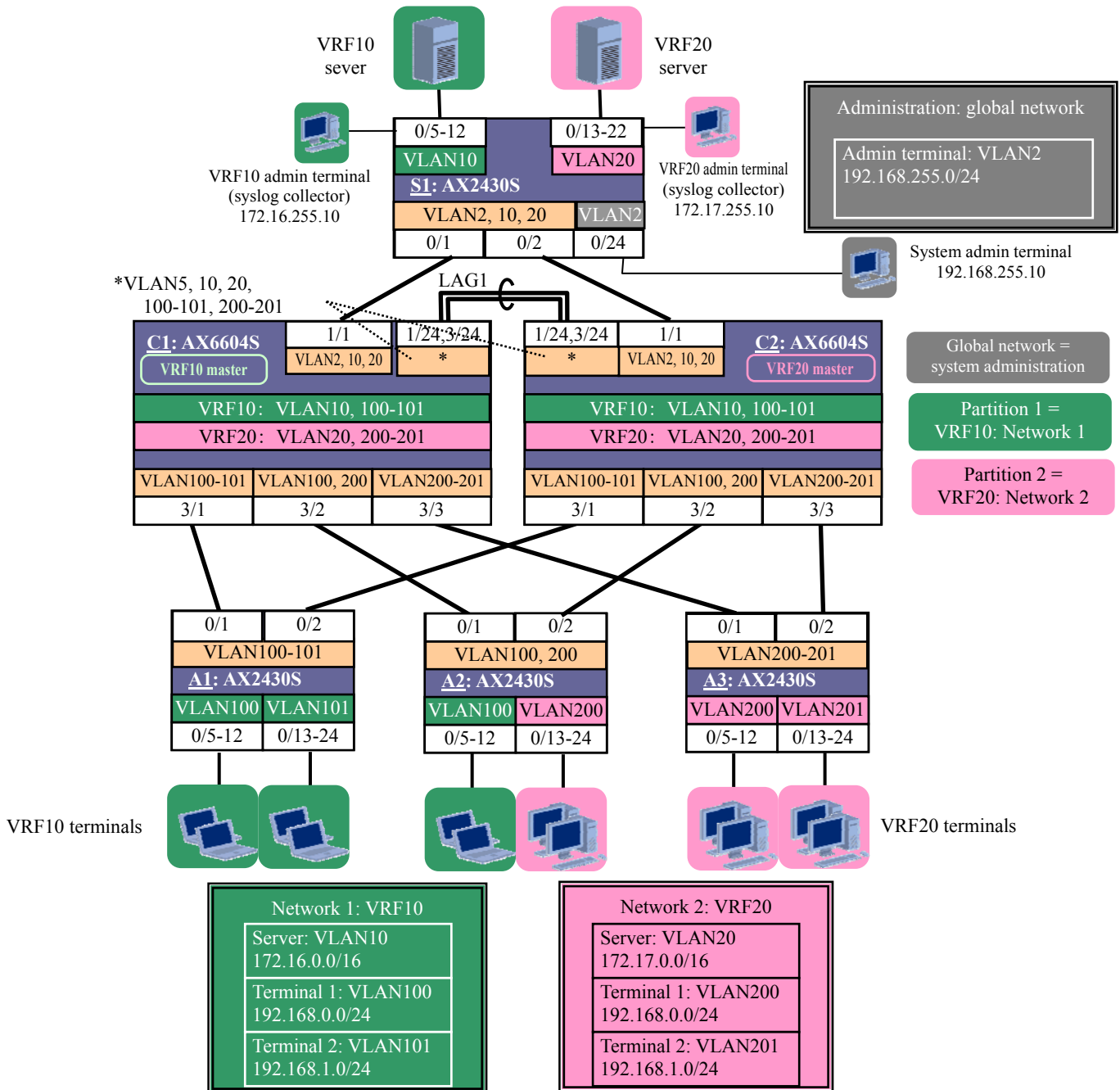


Figure 3.3-2 Logical configuration

Nodes C1 and C2, which function as the core, use an AX6604S series switch and constitute a GSRP switch, while handling two independent networks using a VRF function with network 1 as VRF10 and another independent network 2 as VRF20. The AX2430S series switch, which is the L2 switch, is used for the access edge node.

In this configuration, the GSRP features are put to practical use and GSRP masters are divided for each VLAN used in the partitions. As a result, the load can be distributed across partitions and the system can be easily configured based on a minimum of settings, without considering the routing between GSRP devices.

Moreover, system administration is maintained through the global network, enabling the remote control of the overall system. Configuration points and examples are given below for configuring the devices used as described above.

3.3.1 Important points in the configuration

(1) Assign the VRF configuration only to the L3 core device

Assign the VRF configuration only to the L3 core device. No VRF setting is needed for any peripherals (ring nodes, etc.) consisting of L2 networks. VRF IDs must be a number equal to or greater than 2. The upper limit of the value is 125 when using GSRP.

(2) Disable spanning trees

Using VRF and GSRP requires the prohibition of spanning trees. You need to disable spanning trees (PVST+), which are enabled by default.

(3) Activate VRF in the mode that uses GSRP

When configuring a system using GSRP, specify that GSRP is used for the L2 protocol.

This setting is performed using the vrf mode command. However, part of the devices (the BSU section of the AX6700S and the PSP section for the AX6600S/AX6300S) must be restarted when changing the operating mode using the vrf mode command. (A confirmation message will be displayed when the command is executed.)

(4) Assign VLANs to partitions (VRF)

The vrf forwarding setting in the VLAN interfaces defines which partition is assigned to which VLAN. If this setting is omitted, the VLAN is assigned to the global network.

(5) Combine the use of the VLAN group and VLAN used in a partition to simplify configuration

In GSRP, a VLAN in the VLAN group can be set without depending on VRF, and various configurations can be implemented, such as a system in which load balance is taken into consideration. However, the routing between devices configured for GSRP requires an accurate design. When a network partition is combined with GSRP, one of the ways to simplify such a design is to set the VLAN group used in VRF to the same VLAN group used for GSRP. This method is beneficial, as the logical configuration of the system or operation during switching is easy to understand.

(6) Use the GSRP Layer 3 redundant switching function

The two GSRP switches must have the same address as the server or terminal default gateway. Therefore, enable the Layer 3 redundancy function.

(7) Specify the type of partition in which the routing protocol operates

As with VLANs, routing protocols must be assigned to one of the partitions. However, the method for specifying VRF is different according to the routing protocols used.

For OSPF, define the VRF IDs using the router command, which specifies the use of OSPF. For RIP, define the VRF instance as one of the ipv4 address families.

If there is no VRF setting, the protocol will operate in the global network.

(8) Remote control must be via the global network

If you want to remotely control VRF-enabled devices via telnet or FTP, you must use the global network. Remote log collection (syslog) is available from any partition on a global network, starting from software ver.11.2.

3.3.2 Configuration example

Given below is a configuration example describing a starting point for system configuration. For the overall configuration, see [the Appendix](#).

(1) Configuration of the core node

C1 (AX6604S) configuration	
Prohibition of spanning trees	
(config)# spanning-tree disable	The AX series default value for PVST+ is enabled, therefore, disable PVST+. (Important point (2))
VRF configuration	
(config)# vrf mode gsrp-enable-ipv4-ipv6 PSP will be restarted automatically when the selected mode differs from current mode. Do you wish to change mode (y/n): y	Set VRF together with GSRP. (Important point (3)) (A prompt for restarting the PSP is displayed. Enter Y if it is OK to restart.)
(config)# vrf definition 10 (config)# vrf definition 20	Declare that VRF10 is to be used. (Important point (1)) Declare that VRF20 is to be used. (Important point (1))
VLAN configuration	
(config)# vlan 2,5,10,20,100-101,200-201	Define the settings of the VLANs to be used.
VLAN interface configuration	
(config)# interface vlan 2 (config-if)# ip address 192.168.255.1 255.255.255.0 (config)# interface vlan 10 (config-if)# vrf forwarding 10 (config-if)# ip address 172.16.0.1 255.255.0.0 (config)# interface vlan 20 (config-if)# vrf forwarding 20 (config-if)# ip address 172.17.0.1 255.255.0.0 (config)# interface vlan 100 (config-if)# vrf forwarding 10 (config-if)# ip address 192.168.0.1 255.255.255.0 (config)# interface vlan 101 (config-if)# vrf forwarding 10 (config-if)# ip address 192.168.1.1 255.255.255.0 (config)# interface vlan 200 (config-if)# vrf forwarding 20 (config-if)# ip address 192.168.0.1 255.255.255.0 (config)# interface vlan 201 (config-if)# vrf forwarding 20 (config-if)# ip address 192.168.1.1 255.255.255.0	Use VLAN2 in the global network for system administration. (Important point (8)) Assign an IP address to VLAN2 ^{#1} . Use VLAN10 in VRF10. (Important point (4)) Assign an IP address to VLAN10 Use VLAN20 in VRF20. (Important point (4)) Assign an IP address to VLAN20. Use VLAN100 in VRF10. (Important point (4)) Assign an IP address to VLAN100. Use VLAN101 in VRF10. (Important point (4)) Assign an IP address to VLAN101. Use VLAN200 in VRF20. (Important point (4)) Assign an IP address to VLAN200. Use VLAN201 in VRF20. (Important point (4)) Assign an IP address to VLAN201.
Physical port interfaces configuration	
Access switch port configuration	
(config)# interface gigabitethernet 1/1 (config-if)# link debounce time 0 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 2,10,20 (config)# interface gigabitethernet 3/1 (config-if)# link debounce time 0 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 100-101 (config)# interface gigabitethernet 3/2 (config-if)# link debounce time 0 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 100,200	Define port 1/1 for server access switch connection. Define ports 2, 10, and 20 as the trunk ports where communication is permitted for the VLAN. Define port 3/1 for the access switch connection. Define ports 100-101 as the trunk ports where communication is permitted for the VLAN. Also define port 3/2 for the access switch connection. Define ports 100 and 200 as the trunk ports where communication is permitted for the VLAN.
C1 (AX6604S) configuration	

(config)# interface gigabitethernet 3/3 (config-if)# link debounce time 0 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 200-201	Also define port 3/3 for the access switch connection. Define ports 200-201 as the trunk ports where communication is permitted for the VLAN.
GSRP direct link configuration	
(config)# interface range gigabitethernet 1/24, gigabitethernet 3/24 (config-if-range)# link debounce time 0 (config-if-range)# channel-group 1 mode on (config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 5,10,20,100-101,200-201 (config-if)# gsrp 1 direct-link	Define ports 1/24 and 2/24 as channel group 1 for the GSRP direct link. Define port channel 1 as the trunk port where transfer is permitted for VLAN5, VLAN10, VLAN20, VLAN100-101, and VLAN-200-201. Define it as the direct link for GSRP1.
GSRP configuration	
(config)# gsrp 1 (config-gsrp)# gsrp-vlan 5 (config-gsrp)# layer3-redundancy (config-gsrp)# vlan-group 1 vlan 10,100-101 (config-gsrp)# vlan-group 2 vlan 20,200-201 (config-gsrp)# vlan-group 1 priority 120 (config)# gsrp limit-control	Define GSRP when GSRP ID = 1. Define VLAN5 as the GSRP control VLAN. Define Layer 3 redundant switching for GSRP (Important point (6)) Assign VLAN10 and VLAN100-101 to VLAN group 1. Assign VLAN20 and VLAN200-201 to VLAN group 2. (Important point (5)) Specify the priority level of VLAN group 1 as 120, so that this device becomes the preferential master ^{#1} . Enable the GSRP VLAN group-restricted control function for remote management of the device.
Routing protocol configuration	
(config)# router ospf 1 vrf 10 (config-router)# network 172.16.0.0 0.0.255.255 area 0 (config-router)# network 192.168.0.0 0.0.1.255 area 0 (config)# router rip (config-router)# address-family ipv4 vrf 20 (config-router-af)# network 172.17.0.0 0.0.255.255 (config-router-af)# network 192.168.0.0 0.0.1.255	Specify OSPF as the routing protocol for VRF10. (Important point (7)) Specify RIP as the routing protocol for VRF20. (Important point (7))
Configuration for remote control of the device	
(config)# logging host 192.168.255.10 (config)# logging host 172.16.255.10 vrf 10 (config)# logging host 172.17.255.10 vrf 20 (config)# line vty 0 2 (config)# ftp-server	Specify the host for collecting the syslog. Specify the host for collecting the syslog in VRF10. Specify the host for collecting the syslog in VRF20. (Important point (8)) Permit telnet login (up to 2 users at a time). Activate the FTP server.

- #1 The configuration for device C2 is the same as for device C1, except that the IP address assigned to the device (VLAN2) and the priority setting on the GSRP VLAN group are different from those for device C1. For more details, see the attached configuration.

(2) Configuration of access nodes

There is no VRF-related setting required for configuration of access nodes. A partition (VRF) to be associated with an access node is the one to which the VLAN handled by the access node belongs. The L3 core node in which the VRF configuration is defined handles such settings.

S1 (AX2430S) configuration	
Prohibition of spanning trees	
(config)# spanning-tree disable	In a system in which GSRP is used, a spanning tree is not used. In the AX series, however, the default value for PVST+ is enabled, therefore, disable PVST+.
VLAN configuration	
(config)# vlan 2,10,20	Define the settings of the VLANs to be used.
Physical port interface configuration	
Port configuration	
(config)# interface range gigabitethernet 0/1-2 (config-if-range)# link debounce time 0 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 2,10,20	Define ports 0/1-2 for connection with devices C1 and C2.
(config)# interface range gigabitethernet 0/5-12 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 10	Define ports 0/5-12 to form access ports for VLAN10 for connection of a network 1 (VRF10) server or terminal.
(config)# interface range gigabitethernet 0/13-22 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 20	Define ports 0/13-22 to form access ports for VLAN20 for connection of a network 2 (VRF20) server or terminal.
(config)# interface gigabitethernet 0/24 (config-if)# switchport mode access (config-if)# switchport access vlan 2	Define port 0/24 to form an access port for VLAN2 for a system management terminal.

A1 (AX2430S) configuration	
Prohibition of spanning trees	
(config)# spanning-tree disable	In a system in which GSRP is used, a spanning tree is not used. In the AX series, however, the default value for PVST+ is enabled, therefore, disable PVST+.
VLAN configuration	
(config)# vlan 100-101	Define the settings of the VLANs to be used.
Physical port interface configuration	
Port configuration	
(config)# interface range gigabitethernet 0/1-2 (config-if-range)# link debounce time 0 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 100-101	Define ports 0/1-2 for connection with devices C1 and C2.
(config)# interface range gigabitethernet 0/5-12 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 100	Define ports 0/5-12 as access ports for connection of the VLAN100 server or terminal in network 1 (VRF10) ^{#1} .
(config)# interface range gigabitethernet 0/13-24 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 101	Define ports 0/13-24 as access ports for connection of the VLAN101 server or terminal in network 1 (VRF10) ^{#1} .

#1 The settings of devices A2 and A3 are the same as for device A1, except that the VLANs to be handled are different among them.

3.4 Configuration method for shared networks

An example for extending the system of a network partition based on an FT network as explained in [section 3.1](#) and newly adding and configuring a shared network is described below.

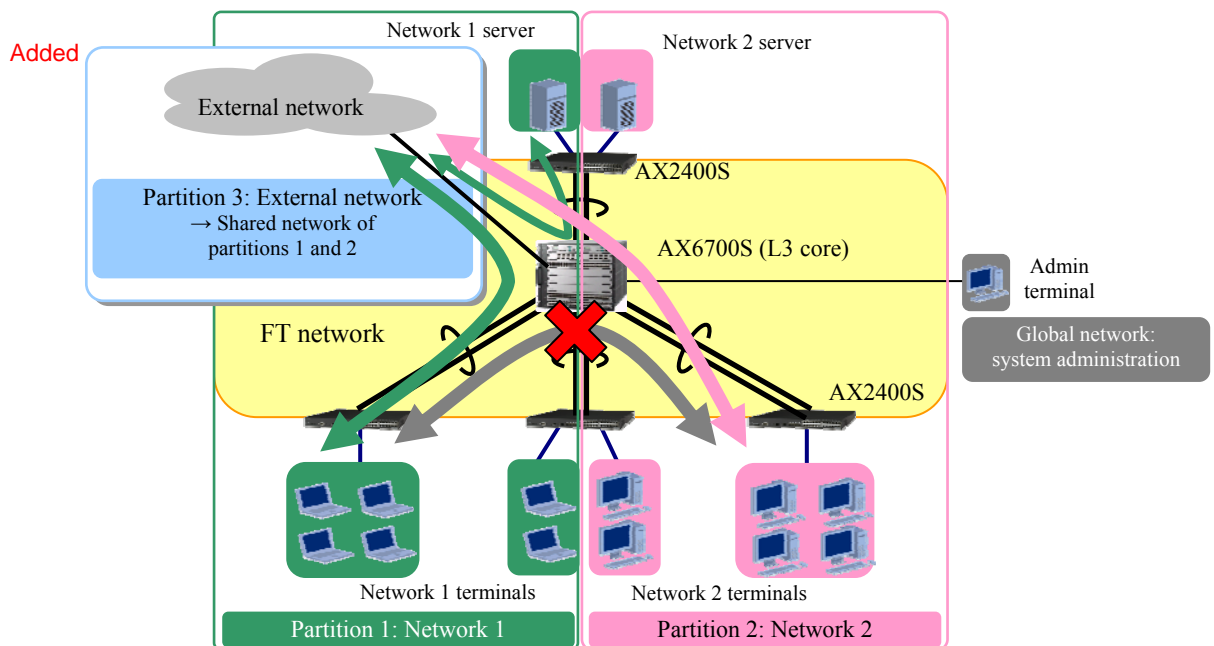


Figure 3.4-1 FT network-based configuration with a shared network

The configuration example above assumes a system in which an external network, which is accessible from two previously independent networks, was added as a shared network. However, networks 1 and 2 cannot communicate directly. Network 2 can communicate with an external network from only the IP address assigned to the terminal side.

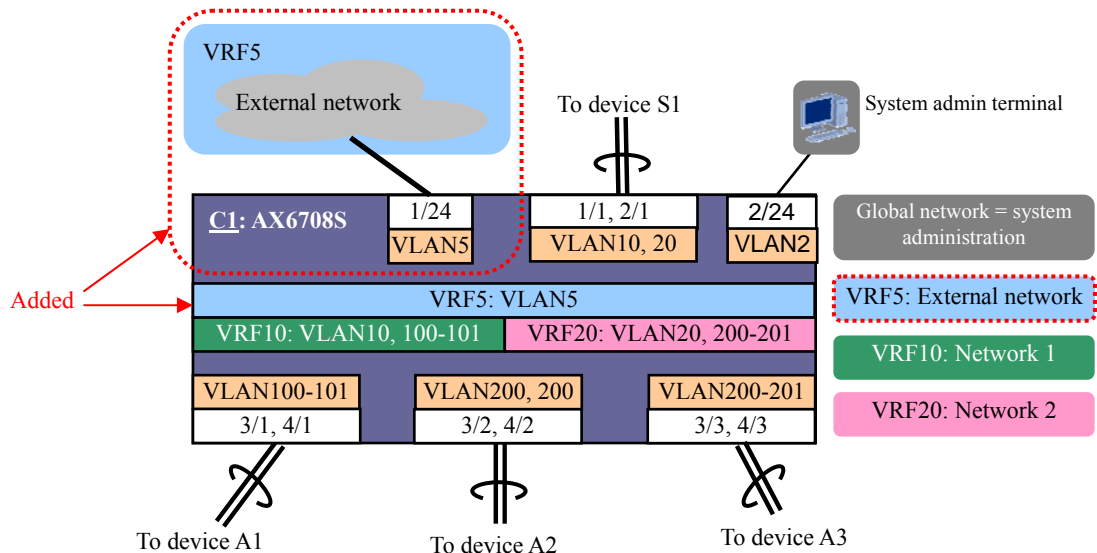


Figure 3.4-2 Logical configuration with a shared network

In node C1, the core, VRF5 for the external network connection is added in addition to the configuration described in section 3.1.

After the settings described above are complete, route filtering is used to achieve a shared network. Remote VRF is mutually specified between VRFs that permit communication. More detailed filter conditions can be also created using a prefix list. Route filtering in this example configuration is described below.

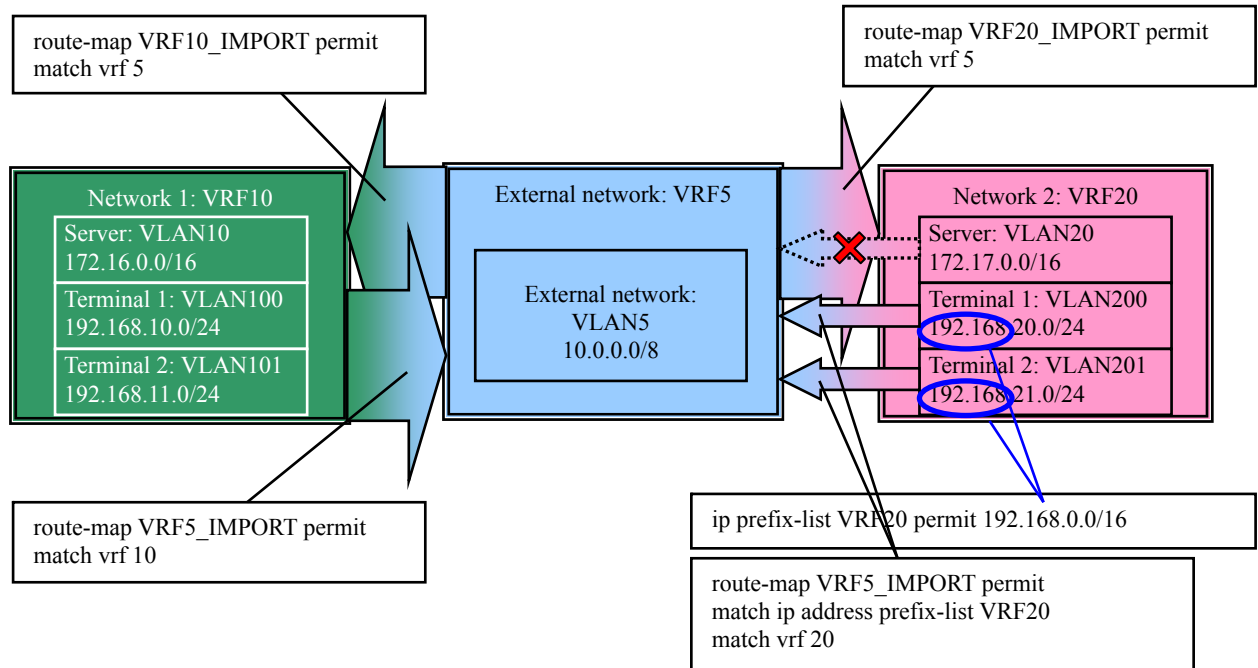


Figure 3.4-3 Description of route filter for configuring a shared network

Filters permitting communication from VRF10 to VRF5 and from VRF5 to VRF10 are defined between external network VRF5 and network 1 VRF10.

A filter permitting communication from VRF5 to VRF20 is defined between external network VRF5 and network 2 VRF20. For communication from VRF20 to VRF5, the range of the network that enables communication using a prefix list is limited to 192.168.x.0/24, in addition to a filter permitting VRF20.

Important points and configuration examples for the above are described below.

3.4.1 Important points in the configuration

As described above, an extra network is achieved by inter-VRF route filtering.

(1) Configure the route-map identifier when setting VRF.

To use route filtering, a route filter identifier is configured for each VRF to be treated as an extra network.

(2) Configure remote VRF permitting communication by using route filtering

In a system in which VRF is used, like the setting of ordinary route filtering, VRF can be added to the filter conditions. This enables transfer control between VRFs.

Therefore, mutual VRF is permitted as a filter condition between VRFs that permit communication during execution of an extra network. Furthermore, detailed control can also be done through the combined use of other filter conditions.

3.4.2 Configuration example

For the overall configuration including the description below, see [the Appendix](#).

(1) Additional core node configuration

Additional C1 (AX6708S) configuration	
Additional VRF configuration	
<pre>(config)# vrf definition 5 (config-vrf)# import inter-vrf VRF5_IMPORT (config)# vrf definition 10 (config-vrf)# import inter-vrf VRF10_IMPORT (config)# vrf definition 20 (config-vrf)# import inter-vrf VRF20_IMPORT</pre>	<p>Enter the VRF5 configuration mode. Define “VRF5_IMPORT” as the route-map identifier for VRF5. (Important point (1))</p> <p>Enter the VRF10 configuration mode. Define “VRF10_IMPORT” as the route-map identifier for VRF10. (Important point (1))</p> <p>Enter the configuration mode of VRF20. Define “VRF20_IMPORT” as the route-map identifier for VRF20. (Important point (1))</p>
Additional VLAN configuration	
<pre>(config)# vlan 5</pre>	Define additional VLANs for the shared network.
Additional VLAN interface configuration	
<pre>(config)# interface vlan 5 (config-if)# vrf forwarding 5 (config-if)# ip address 10.1.2.3 255.255.255.0</pre>	<p>Define VLAN5 to be used in VRF5. Assign an IP address to VLAN5.</p>
Route filter (route-map) configuration	
<pre>(config)# ip prefix-list VRF20 seq 10 permit 192.168.0.0/16 (config)# route-map VRF5_IMPORT permit 10 (config-route-map)# match vrf 10 (config)# route-map VRF5_IMPORT permit 20 (config-route-map)# match ip address prefix-list VRF20 (config-route-map)# match vrf 20 (config)# route-map VRF10_IMPORT permit 10 (config-route-map)# match vrf 5 (config)# route-map VRF20_IMPORT permit 10 (config-route-map)# match vrf 5</pre>	<p>Define a prefix list that conforms to 192.168/16 for VRF20. Define the route filter applied to “VRF5_IMPORT”. Define all communications with (VRF5 and) VRF10 to be permitted in sequence 10. Define all communication with (VRF5 and) VRF20 that satisfies prefix list “VRF20” conditions defined above to be permitted in sequence 20. (Important point (2))</p> <p>Define the route filter applied to “VRF10_IMPORT”. Define all communications with (VRF10 and) VRF5 to be permitted. (Important point (2))</p> <p>Define the route filter applied to “VRF20_IMPORT”. Define all communications with (VRF20 and) VRF5 to be permitted. (Important point (2))</p>

4. Network Partition Operations

4.1 System log

In the device that uses a VRF function, VRF information is added to the event information on the routing protocol, such as RIP, OSPF, BGP4, or PIM-SM, to identify a VRF for which each routing protocol has been used. VRF information is also added partially in the device-related event protocol (location of event occurrence = IP) or in software (multicast-related).

```
C1>show logging
KEY 12/20 12:10:00 operator(tty00):C1> show logging
RTM 12/20 12:03:14 OSPF SENT 192.168.10.1 -> 224.0.0.5      (VRF 10): Network is down.
...
```

See AX6700S-AX6300S *Software Manual Message/Log Reference* for the displayed log information and other details.

4.2 Operational commands

In the device that uses a VRF function, the parameters below that identify VRF can be added to almost all operational commands related to Layer 3 relay. This enables the selection of the VRF to be displayed.

(vrf not specified)	Only information on the global network
vrf <vrf id>	Information on the specified VRF
vrf all	Total VRF information, including the global network

(Note: There are also some commands with which “all” cannot be specified.)

For example, a “show ip route” command that displays route information is shown below.

- vrf is not specified. (Route display of the global network)

```
C1>show ip route
Date 2008/12/20 12:00:00 UTC
Total: 4 routes
Destination      Next Hop      Interface      Metric  Protocol  Age
127/8            ----          localhost      0/0     Connected 2h 14m
127.0.0.1/32     127.0.0.1     localhost      0/0     Connected 2h 14m
192.168.255/24   192.168.255.1 VLAN0002       0/0     Connected 2h 14m
192.168.255.1/32 192.168.255.1 VLAN0002       0/0     Connected 2h 14m
```

- vrf 10 is specified.

```
C1>show ip route vrf 10
Date 2008/12/20 12:00:00 UTC
VRF: 10 Total: 8 routes
Destination      Next Hop      Interface      Metric  Protocol  Age
127/8            ----          localhost      0/0     Connected 2h 14m
127.0.0.1/32     127.0.0.1     localhost      0/0     Connected 2h 14m
172.16/16        172.16.0.1    VLAN0010       0/0     Connected 2h 14m
172.16.0.1/32    172.16.0.1    VLAN0010       0/0     Connected 2h 14m
192.168.10/24    192.168.10.1  VLAN0100       0/0     Connected 2h 14m
192.168.10.1/32  192.168.10.1  VLAN0100       0/0     Connected 2h 14m
192.168.11/24    192.168.11.1  VLAN0101       0/0     Connected 2h 14m
192.168.11.1/32  192.168.11.1  VLAN0101       0/0     Connected 2h 14m
```

- vrf all is specified.

<pre> Cl>show ip route vrf all Date 2008/12/20 12:00:00 UTC VRF: global Total:4 routes Destination Next Hop Interface Metric Protocol Age 127/8 ---- localhost 0/0 Connected 2h 14m 127.0.0.1/32 127.0.0.1 localhost 0/0 Connected 2h 14m 192.168.255/24 192.168.255.1 VLAN0002 0/0 Connected 2h 14m 192.168.255.1/32 192.168.255.1 VLAN0002 0/0 Connected 2h 14m VRF: 5 Total: 14 routes Destination Next Hop Interface Metric Protocol Age 10/8 10.1.2.3 VLAN0005 0/0 Connected 2h 14m 10.1.2.3/32 10.1.2.3 VLAN0005 0/0 Connected 2h 14m 127/8 ---- localhost 0/0 Connected 2h 14m 127.0.0.1/32 127.0.0.1 localhost 0/0 Connected 2h 14m 172.16/16 172.16.0.1 VLAN0010 0/0 Extra-VRF 2h 14m 172.16.0.1/32 172.16.0.1 VLAN0010 0/0 Extra-VRF 2h 14m 192.168.10/24 192.168.10.1 VLAN0100 0/0 Extra-VRF 2h 14m 192.168.10.1/32 192.168.10.1 VLAN0100 0/0 Extra-VRF 2h 14m 192.168.11/24 192.168.11.1 VLAN0101 0/0 Extra-VRF 2h 14m 192.168.11.1/32 192.168.11.1 VLAN0101 0/0 Extra-VRF 2h 14m 192.168.20/24 192.168.20.1 VLAN0200 0/0 Extra-VRF 2h 14m 192.168.20.1/32 192.168.20.1 VLAN0200 0/0 Extra-VRF 2h 14m 192.168.21/24 192.168.21.1 VLAN0201 0/0 Extra-VRF 2h 14m 192.168.21.1/32 192.168.21.1 VLAN0201 0/0 Extra-VRF 2h 14m VRF: 10 Total: 8 routes Destination Next Hop Interface Metric Protocol Age 127/8 ---- localhost 0/0 Connected 2h 14m 127.0.0.1/32 127.0.0.1 localhost 0/0 Connected 2h 14m 172.16/16 172.16.0.1 VLAN0010 0/0 Connected 2h 14m 172.16.0.1/32 172.16.0.1 VLAN0010 0/0 Connected 2h 14m 192.168.10/24 192.168.10.1 VLAN0100 0/0 Connected 2h 14m 192.168.10.1/32 192.168.10.1 VLAN0100 0/0 Connected 2h 14m 192.168.11/24 192.168.11.1 VLAN0101 0/0 Connected 2h 14m 192.168.11.1/32 192.168.11.1 VLAN0101 0/0 Connected 2h 14m VRF: 20 Total: 8 routes Destination Next Hop Interface Metric Protocol Age 127/8 ---- localhost 0/0 Connected 2h 14m 127.0.0.1/32 127.0.0.1 localhost 0/0 Connected 2h 14m 172.17/16 172.17.0.1 VLAN0020 0/0 Connected 2h 14m 172.17.0.1/32 172.17.0.1 VLAN0020 0/0 Connected 2h 14m 192.168.20/24 192.168.20.1 VLAN0200 0/0 Connected 2h 14m 192.168.20.1/32 192.168.20.1 VLAN0200 0/0 Connected 2h 14m 192.168.21/24 192.168.21.1 VLAN0201 0/0 Connected 2h 14m 192.168.21.1/32 192.168.21.1 VLAN0201 0/0 Connected 2h 14m </pre>						
Route of the global network						
Indicates the route of an extra network (between other partitions)						
Route of VRF5 (the external network)						
Route of VRF10 (network 1)						
Route of VRF20 (network 2)						

As shown above, the information for each VRF or the information for the entire system can be selected for display.

Regarding the relationship between VLAN and VRF, you can use the show vlan command to display the information that indicates which VLAN is used in which VRF.

```

Cl>show VLAN 100
Date 2008/12/20 12:00:00 UTC
VLAN counts:1
VLAN ID:100 Type:Port based Status:Up
Learning:On Tag-Translation:
BPDU Forwarding: EAPOL Forwarding:
Router Interface Name:VLAN0100
VRF:10
IP Address:192.168.10.1/24
Source MAC address: 0012.e2e0.2a00(System)
Description:VLAN0100
Spanning Tree:
AXRP RING ID: AXRP VLAN group:
GSRP ID: GSRP VLAN group: L3:
IGMP snooping: MLD snooping:
Flow mode:
Tagged(4) :3/1-2
4/1-2

```

Use the show ip vrf detail command or the show ip interface command when examining the type of VLAN assigned to VRF.

- Example of show ip interface command execution

```

Cl>show ip interface vrf 10
Date 2008/12/20 12:00:00 UTC
VLAN0010: flags=8863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST>
mtu 1500
inet 172.16.0.1/16 broadcast 172.16.255.255
NIF01/Port01: UP media 1000BASE-T full(auto) 0012.e2e0.2a00 ChGr:1 (UP)
NIF02/Port01: UP media 1000BASE-T full(auto) 0012.e2e0.2a00 ChGr:1 (UP)
Time-since-last-status-change: 00:44:23
Last down at: -----
uRPF(IPv4): Disable
VLAN : 10 VRF : 10
VLAN0100: flags=8863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST>
mtu 1500
inet 192.168.10.1/24 broadcast 192.168.10.255
NIF03/Port01: UP media 1000BASE-T full(auto) 0012.e2e0.2a00 ChGr:11 (UP)
NIF03/Port02: UP media 1000BASE-T full(auto) 0012.e2e0.2a00 ChGr:12 (UP)
NIF04/Port01: UP media 1000BASE-T full(auto) 0012.e2e0.2a00 ChGr:11 (UP)
NIF04/Port02: UP media 1000BASE-T full(auto) 0012.e2e0.2a00 ChGr:12 (UP)
Time-since-last-status-change: 00:44:23
Last down at: -----
uRPF(IPv4): Disable
VLAN : 100 VRF : 10
VLAN0101: flags=8863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST>
mtu 1500
inet 192.168.11.1/24 broadcast 192.168.11.255
NIF03/Port01: UP media 1000BASE-T full(auto) 0012.e2e0.2a00 ChGr:11 (UP)
NIF04/Port01: UP media 1000BASE-T full(auto) 0012.e2e0.2a00 ChGr:11 (UP)
Time-since-last-status-change: 00:44:25
Last down at: -----
uRPF(IPv4): Disable
VLAN : 101 VRF : 10

```

These three VLANs were assigned to VRF 10.

See AX6700S-AX6300S Software Manual, Operation Command Reference Vol.1 and Vol.2 for details on operational commands.

5. Cautions

(1) Use of the VRF function requires a separate optional license (OP-NPAR).

The VRF function is indispensable when constructing a network partition system. However, an optional license (OP-NPAR) is separately required for the device that is configured for VRF.

(2) MSU-1B or MSU-1B1 is required to use the VRF function in the AX6300S. CSU-1B or CSU-1B1 is required to use the VRF function in the AX6600S.

MSU-1B or MSU-1B1 is required as the configuration condition for the device when using the VRF function in the AX6300S. The VRF function cannot be used in the MSU-1A or MSU-1A1.

CSU-1B or CSU-1B1 is required as the configuration condition for the device when using the VRF function in the AX6600S. The VRF function cannot be used in the CSU-1A or CSU-1A1.

With the AX6700S, there are no conditions for device configuration.

(3) Make sure that IP addresses do not overlap when configuring a shared network.

In a network partition system, there is no problem even if the IP addresses used overlap between independent mutual partitions. However, make sure that IP addresses do not overlap between mutual partitions when communication between partitions is permitted in an extra network or shared network.

(4) Remote login to a device that enables the VRF function can only be done from a global network.

Use the global network when remotely logging in to a device in which the VRF function is used, using telnet or transfer of a file using FTP. Remote operation cannot be performed from other partitions (VRF).

Appendix: Configuration Files

Examples of the configurations introduced in this guide are described below.

Configurations for each device in each network configuration in Chapter 3 are attached to these files as text files. (Adobe Acrobat 5.0 and later or Adobe Reader 6.0 and later are required to extract the attached files.)

For details on each configuration, see the attached files with the same names as the file names below.

3. Examples of Implementing Systems with Network Partitions

3.1. Network partitions in an FT network

	Device name and target device	Target file
L3 core switch ^{#1}	C1 (AX6708S)	3-1_FTN-NP_C1.txt
L2 access switch	S1 (AX2430S-24)	3-1_FTN-NP_S1.txt
	A1 (AX2430S-24)	3-1_FTN-NP_A1.txt
	A2 (AX2430S-24)	3-1_FTN-NP_A2.txt
	A3 (AX2430S-24)	3-1_FTN-NP_A3.txt

(*1) BSU mounts the BSU-LA.

3.2. Network partitions in a ring network

	Device name and target device	Target file
L3 core switch	C1 (AX6304S)	3-2_RING-NP_C1.txt
L2 access switch	S1 (AX2430S-24)	3-2_RING-NP_S1.txt
	A1 (AX2430S-24)	3-2_RING-NP_A1.txt
	A2 (AX2430S-24)	3-2_RING-NP_A2.txt
	A3 (AX2430S-24)	3-2_RING-NP_A3.txt

3.3. Network partition using GSRP

	Device name and target device	Target file
L3 core switch	C1 (AX6604S)	3-3_GSRP-NP_C1.txt
	C2 (AX6604S)	3-3_GSRP-NP_C2.txt
L2 access switch	S1 (AX2430S-24)	3-3_GSRP-NP_S1.txt
	A1 (AX2430S-24)	3-3_GSRP-NP_A1.txt
	A2 (AX2430S-24)	3-3_GSRP-NP_A2.txt
	A3 (AX2430S-24)	3-3_GSRP-NP_A3.txt

3.4. Configuration method for shared networks

	Device name and target device	Target file
L3 core switch ^{#1}	C1 (AX6708S)	3-4_FTN-NP-EX_C1.txt
L2 access switch ^{#2}	S1 (AX2430S-24)	(3-1_FTN-NP_S1.txt)
	A1 (AX2430S-24)	(3-1_FTN-NP_A1.txt)
	A2 (AX2430S-24)	(3-1_FTN-NP_A2.txt)
	A3 (AX2430S-24)	(3-1_FTN-NP_A3.txt)

#1 BSU mounts the BSU-LA.

#2 The access switch configuration is the same as for the switch in section 3.1, described above.

This page has intentionally been left blank.



Edition 2 – February 19, 2010

Network Technical Support
ALAXALA Networks Corporation

Shin-Kawasaki Mitsui Bldg West Tower, 890
Kashimada, Saiwai-ku, Kawasaki-shi,
Kanagawa 212-0058, JAPAN
<http://www.alaxala.com/en/index.html>