AX Series
Network Partition: Solution Guide
[Advanced]

for the Guaranteed Network

First Edition

Introduction

The *AX Series Network Partition: Solution Guide [Advanced]* provides system engineers with application technology information for system configuration using network partitions supported by AX6700S, AX6600S, and AX6300S switches from the proposal phase through stable operation.

Related material

- *AX Series Network Partition: Solution Guide [Basic]*
- *AX Series Network Partition: Solution Guide [For Authentication]*
- AX series product manuals (http://www.alaxala.com/en/techinfo/manual/index.html)

Cautions in using this guide

The basic operations described in this guide have been verified by ALAXALA Networks Corporation in a specific environment, and we do not guarantee correct function, performance, or reliability under all possible conditions. This document is intended only as a guide to help you configure your system using our products.
Unless otherwise specified, versions of the operating system software at the time of this guide's creation are as follows:

AX6700S, AX6600S, AX6300S - Ver11.1 (OP-NPAR license)
AX3600S, AX2400S - Ver11.1.A

Descriptions in this guide are subject to change without notice for improvement purposes.

Export notes

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

Table of Contents

1. Applications for Network Partitions

1.1 Reasons for introducing network partitions

As already discussed in the ***[Basic]*** and ***[For Authentication]*** versions of the ***AX Series Network Partition: Solution Guide***, a network partition is a system solution that can contain multiple logically independent networks within a minimal physical configuration. Considering its advantages, ALAXALA envisions three main scenarios in which network partitions can be recommended for production systems.

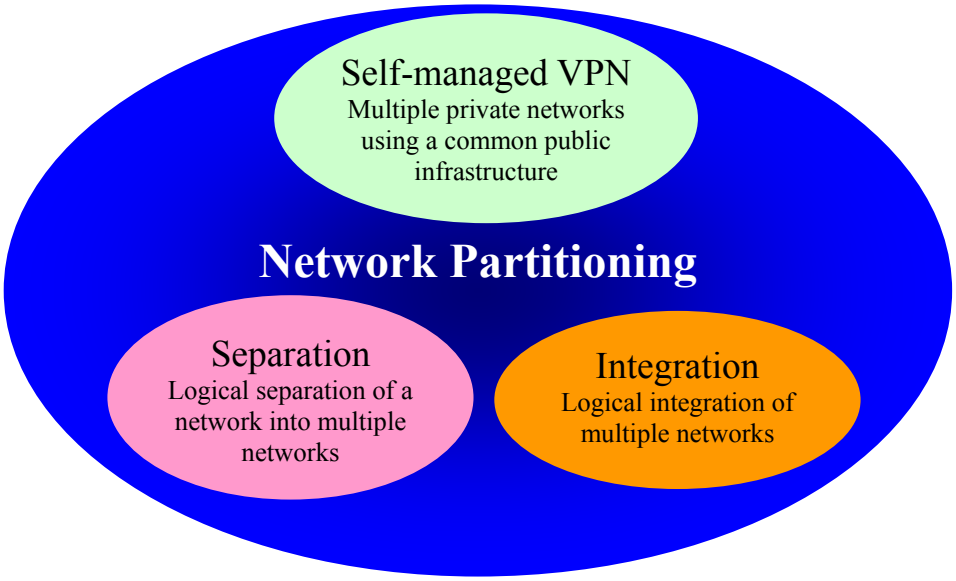


Figure 1.1-1 Three scenarios where a network partition is recommended

- **Self-managed VPN (Virtual Private Network)**
  This scenario applies when you want to configure a system with each connection target as a separate VPN, for example, if you want one single infrastructure but the users are from different organizations.

- **Separation**
  This scenario applies when you want to separate an existing network into several small networks or you want to extract a part of the network as a separate independent segment.

- **Integration**
  This scenario applies when you want to configure physically independent networks on a common infrastructure.

The following sections describe these scenarios.

1.2 Network partition as self-managed VPN

When configuring a new network system, if you need to set up a separate network for each organization, and you want to configure those networks on a common infrastructure to administer all of them collectively, a system configuration using network partitions may be recommended.

Such a requirement can be met with some existing technologies such as MPLS-VPN, however they require expensive special purpose equipment, or they might be complicated to set up. Network partitions are easier to deploy and are more appealing to users.

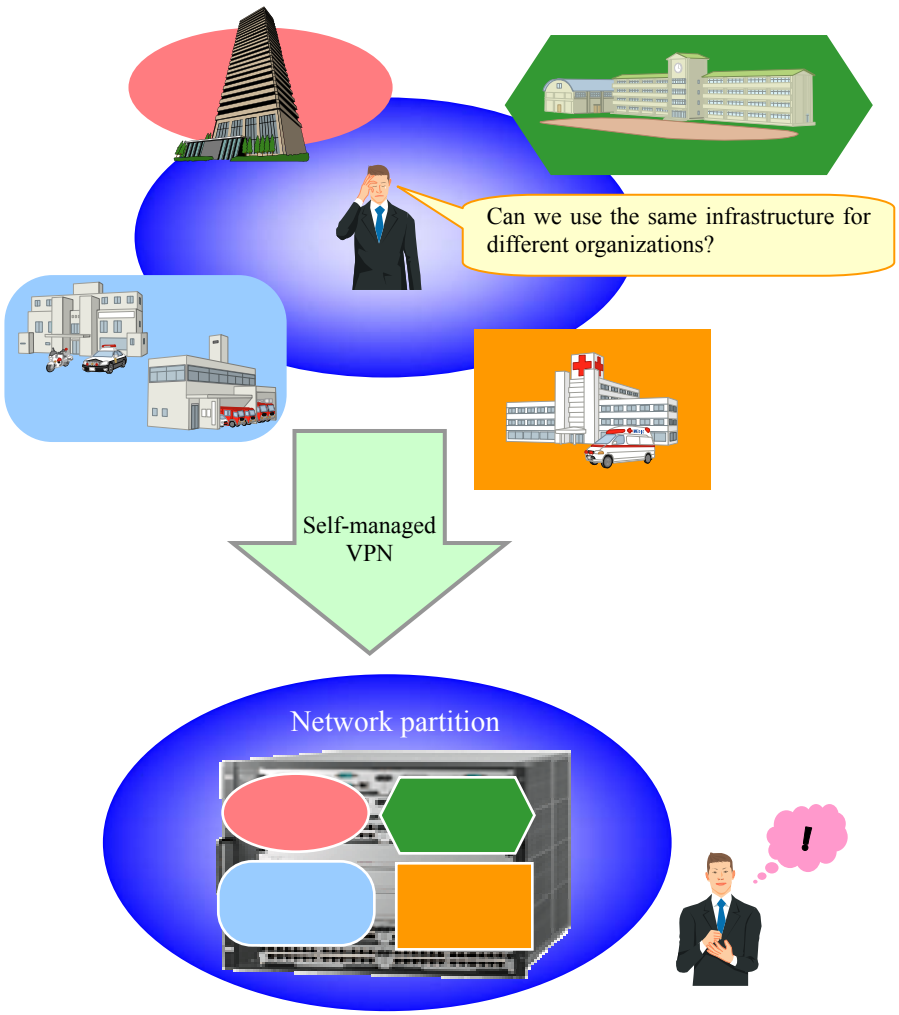


Figure 1.2-1 Using a self-managed VPN

A system tends to be configured when it is newly introduced. Therefore, you can design the system considering its capacity and the capacity of its devices, and thereby avoid any problems. However, in this case you need to define the boundaries of operation and administration responsibility. The boundaries between the organization coordinating the entire system and each organization using the network define the bounds of operation and administration.

1.3 Separating networks

When considering changes to the administration divisions associated with the expansion of an organization or enhancing the security between organizations, you might want to separate part of an existing network system or divide the system into groups. A system configuration using a network partition's logical network is recommended for such situations.

A logically separated network system can be configured while minimizing the effect on physical resources, such as the addition or expansion of devices. Additionally, you can easily configure the system to perform certain operations, such as the addition of a logical network, to flexibly support a gradual system transition.

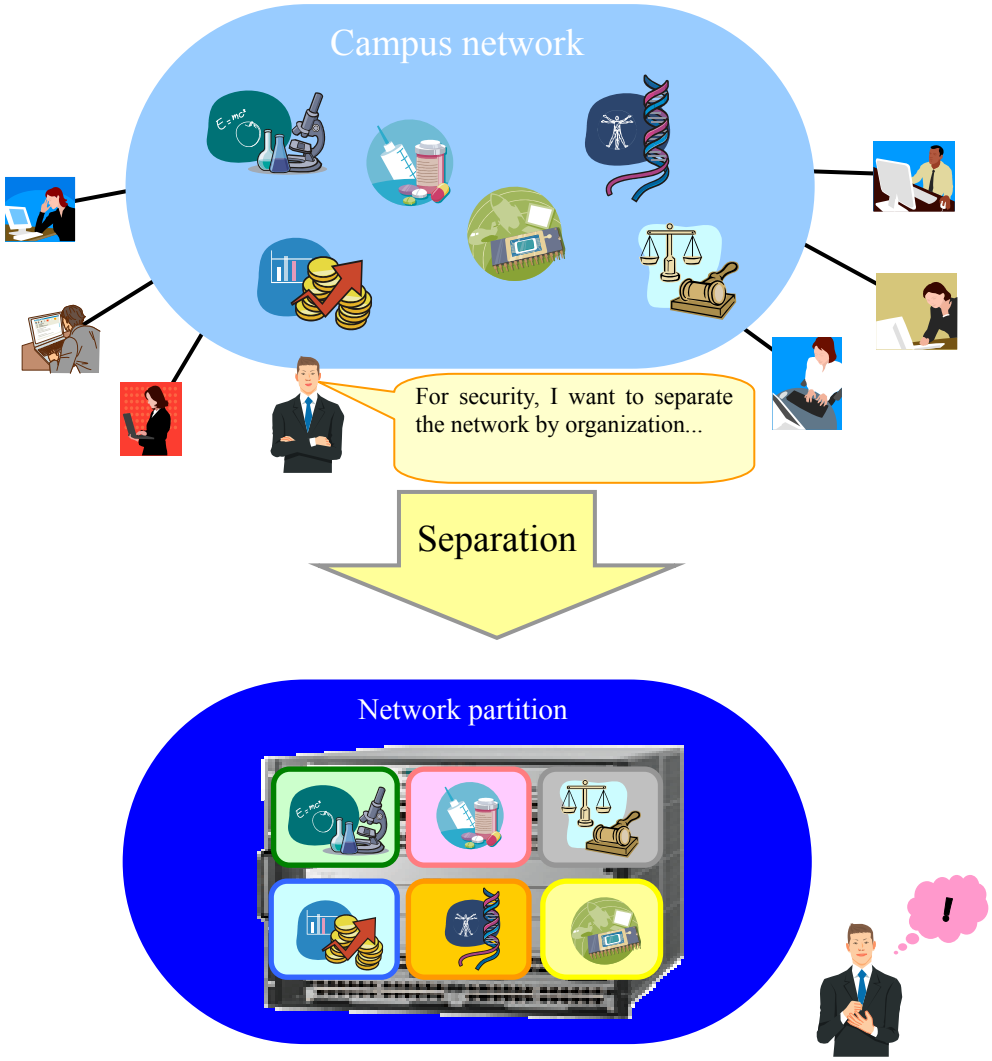


Figure 1.3-1 Separating networks

When separating networks, you must consider three requirements. First, you must preserve the user environment after the separation. Ideally, you should make the system change transparent to users, for example, by not changing the servers used or the address settings.

Next, you must preserve the independence of each separated network. Users should not be able to access one separated network from another. You must securely define the boundaries that determine what users, including end users, might access by some method such as combining network authentications.

Additionally, you must consider smooth system migration. When separating networks, it seems practical to separate a large operating network into several networks one by one. At this time, it is very important that the system be migrated without any extreme degradation of performance, such as long system downtime.

1.4 Integrating networks

System virtualization is now receiving attention as a technology for reducing the costs associated with operation, management, and hardware installation. System virtualization is based on system integration. Likewise, using network partitions to integrate network systems that are completely independent among multiple organizations can be an appropriate solution for reducing operation and management workload and costs. Such system integration might be adopted when one building or floor must contain multiple organizations.

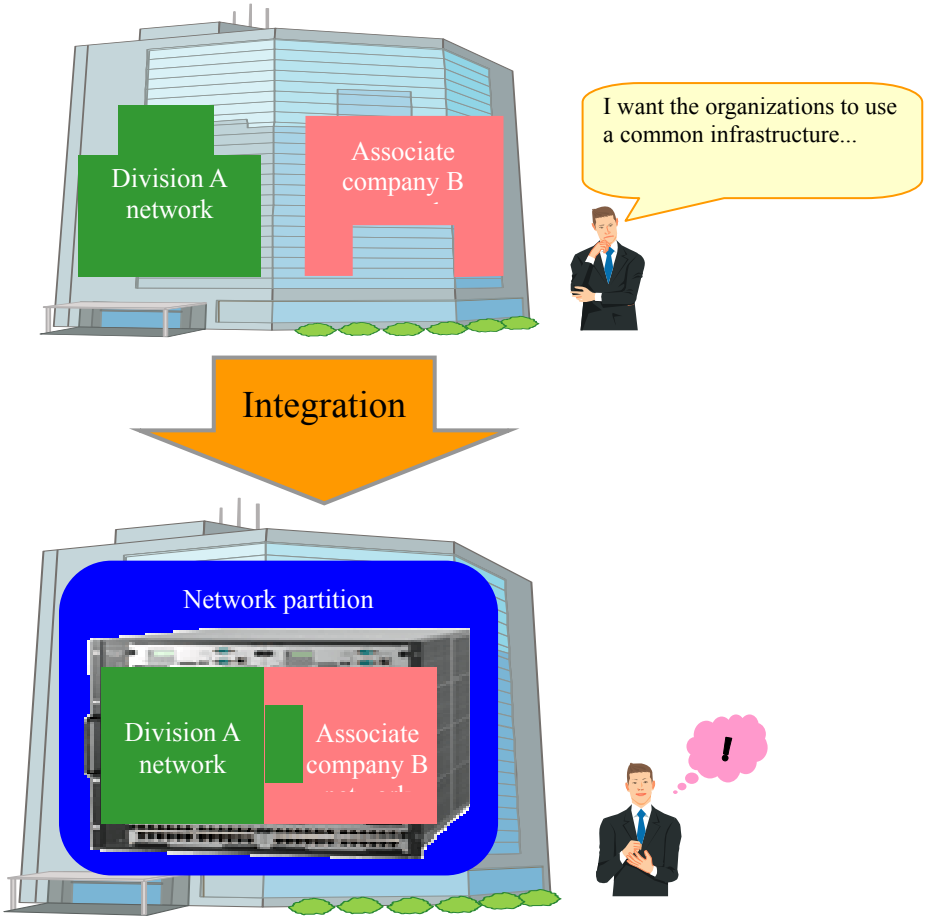


Figure 1.4-1 Integrating networks

When integrating networks, you must also consider whether the user environment can be preserved after the separation. Ideally, the system change is transparent to the end user. Additionally, by integrating networks, required network resources, such as transmission capability and capacity, should also increase. If you are going to integrate systems by using network partitions, you must consider beforehand if the requirements for network resources are also met.

2. Key Points When Introducing Network Partitions

This chapter describes the points to understand when designing systems using network partitions, such as the difference between such network systems and typical network systems.

2.1 Handling of VLANs

A logical network using network partitions is composed predominantly of the logical division of Layer 3 with the VRF technology and the logical division of Layer 2 with VLANs. However, the number of logical networks does not multiply the number of specifiable VLANs.
Therefore, an L2 switch that can handle VLANs can be used in the system with no consideration of a logical network using network partitions. When designing the system, you must fully understand this, as well as the correspondence between the logical network and the VLANs used in the logical network.

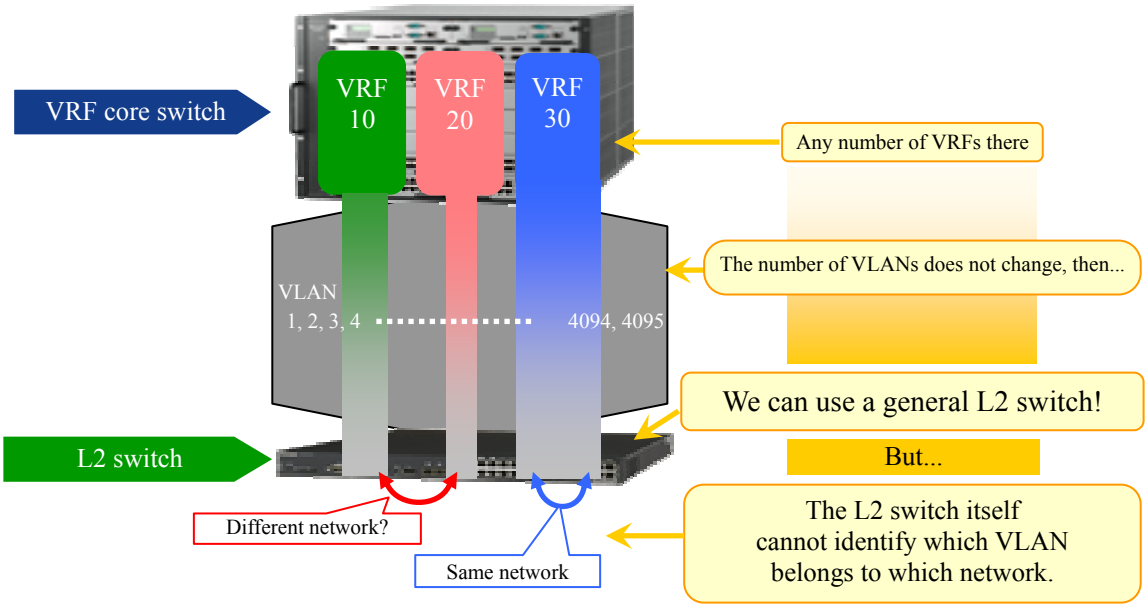


Figure 2.1-1 VLANs in a network partition

The major considerations relating to these points are described below.

(1) If an L3 switch without VRF is used for the distribution and access switch

In a general network, a VLAN boundary can be a subnet boundary. For a system using network partitions, a VLAN boundary must be a network boundary. Therefore, if you want to use an L3 switch without VRF as a distribution/access switch (like an L2 switch), you must make sure that a relay or a router between VLANs does not perform unnecessary network transmissions.

(2) If a switch itself performs transmissions

This condition applies to cases when the switches work as the endpoints of transmission, for example, when you perform a transmission with RADIUS using a switch for authentication, or when you operate and manage devices such as with syslog or telnet. In such cases, the switches themselves are generally assumed to exist in one network (for example, default gateway settings or the VLAN IP address settings). Therefore, if you want these switches to contain multiple networks, you must make sure that the desired transmissions are possible and that the functionality of the switches is not limited.

2.2 Shared network and duplicate IP address assignment

Two logical networks consisting of network partitions do not interfere with each other's IP address settings, and you can assign the same IP address to both logical networks.

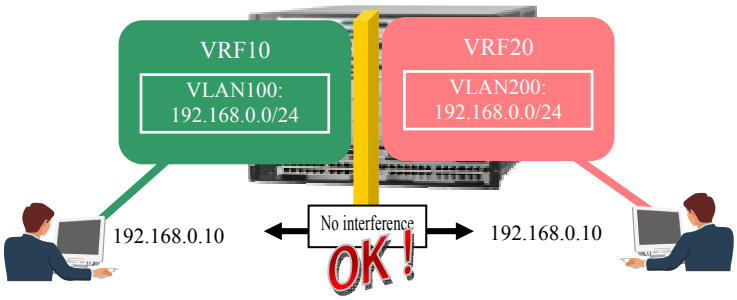


Figure 2.2-1 IP addresses can be identical

However, when you transmit between VRFs using an extranet, if the same IP address exists in both VRFs, there is no way to distinguish them from each other. Additionally, even when you configure a shared network, if both partitions can communicate with the shared network and each network in the partitions is using the same IP address, the shared network can identify the IP address of only one of the partitions. Therefore, if you use the extranet or build a shared network, using the same IP address for different partitions is prohibited.

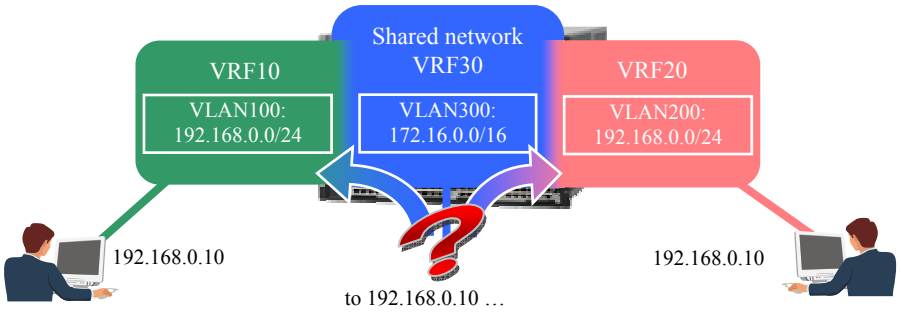


Figure 2.2-2 IP addresses cannot be identical when using a shared network

2.3 Using the network authentication function

As discussed in the ***AX Series Network Partition: Solution Guide [For Authentication]***, it is possible to use the network authentication function for network partition systems.

If a system configuration includes the authentication function, you can use the authentication switches within a logical network in the same way as typical switches. However, if you want a single authentication switch to handle multiple networks (each VLAN belongs to a different network), you must consider the following:

(1) Duplicate IP addresses are prohibited

You must assign an IP address to each VLAN in the authentication switch. However, the same IP address cannot be assigned to different VLANs within a single switch.

(2) Using RADIUS

You cannot use one single authentication switch to reference different RADIUS servers for multiple networks. For an authentication switch to handle multiple networks, you must consolidate the authentication information for all networks to configure the referenced RADIUS server.

(3) Maximizing the dynamic VLAN function

You can combine network partitions with the dynamic VLAN function of the authentication switch on AX series products to switch between the authenticated and unauthenticated environments of each network. In such a case, it is also possible to handle the DHCP servers independently for each logical network.

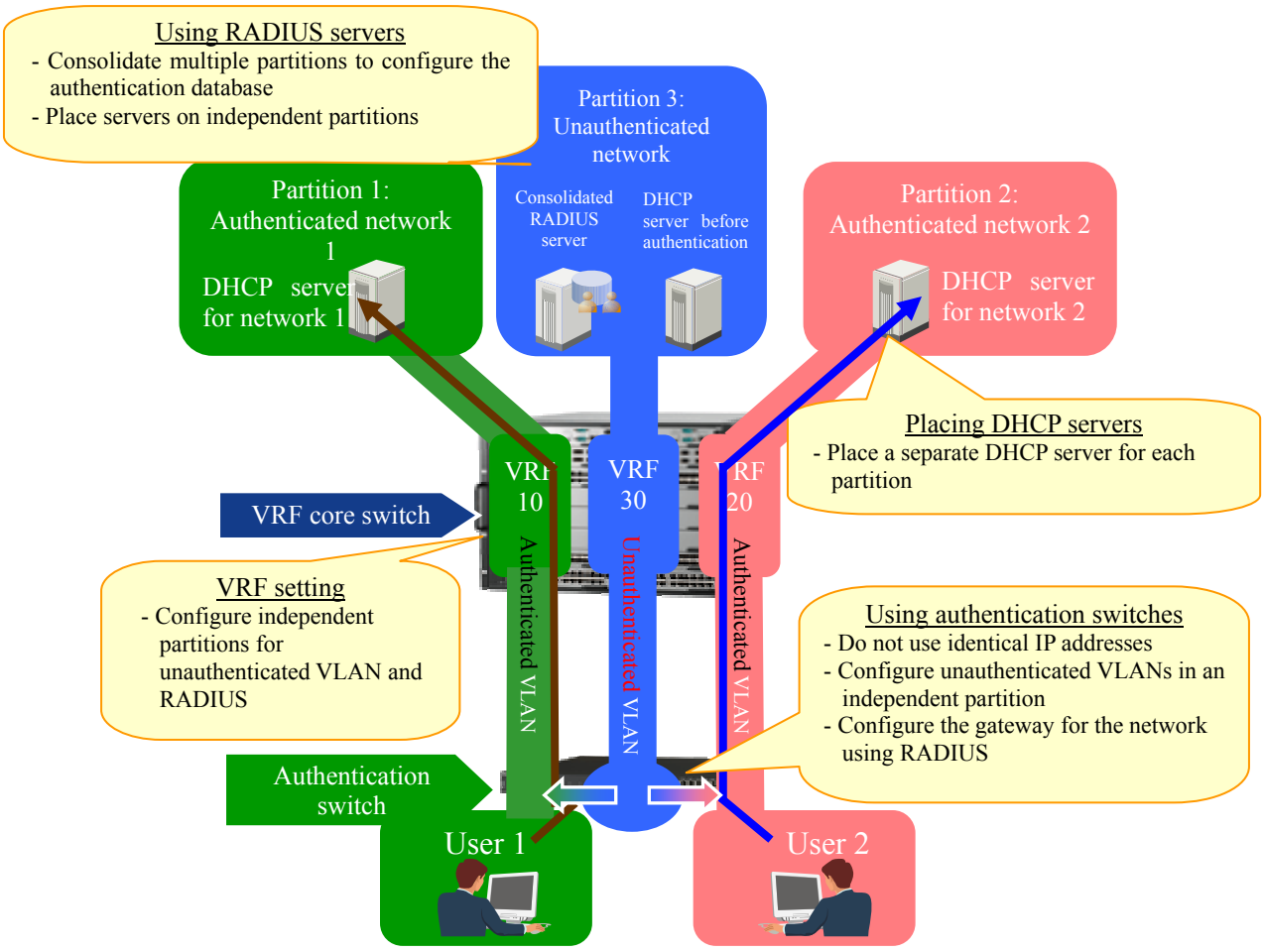


Figure 2.3-1 Recommended configuration for handling multiple networks with a single authentication switch

2.4 Operation management and the global network

In network partitions, if devices use the VRF function, most of the operation and management functions work on the global network. However, some of the functions can be used on networks using VRFs (partitions) other than the global network. See the table below for details.

Table 2.4-1 VRF device support for operation management functions

Functions for operations		Support		Remarks
		Global network	VRF other than global network	
General operation	show command	○	○	
	ping	○	○	
	traceroute	○	○	
	telnet command	○	○	
	Telnet server	○	x	
	ssh command	○	x	
	SSH server	○	x	
	ftp command	○	x	
	FTP server	○	x	
SNMP	Agent	○	○	
	MIB/Trap	○	○	- Information can be obtained per device. - VRF-enabled private MIB (IP, ARP, route).
syslog	Message transmission	○	x	

Legend: ○: Supported x: Not supported

For general switches other than VRF devices, you can use commands and functions for operation and management as on general networks, either on the global network or on each logical network.

Therefore, you must use the global network and adjust its coverage to operate and manage the entire system containing VRF devices.
If you are going to manage the operation of each logical network in the network partitions, you can do so in a way similar to general networks, except when there is a limitation on the VRF device's operation management function (only for monitoring functions such as SNMP, ping, and traceroute; see the table above).

2.5 Distributing resources

A network partition logically contains multiple networks. However, at its core, it is a single device. Therefore, the logical networks must share the resources of the device for transmissions. For example, the transmission capability of packets and frames or CPU processing capability must be shared among the logical networks as necessary. However, it is possible to limit the number of used IP routes and ARP tables per partition (see the table below).

Table 2.5-1 Resources limitable per logical network and execution command

Resource	Command	Unit of limitation	Remarks
Number of MAC address entries to be learned	`mac-address-table limit`	VLAN	
Number of registered ARP tables	`arp-limit`	VRF	
Number of IP routes	`maximum routes`	VRF	You can configure only the warning.
Number of IGMP groups	`ip igmp group-limit`	VRF	
Total number of IGMP sources	`ip igmp source-limit`	VRF	
Total number of PIM-SM/SSM multicast relay entries and negative cache entries	`ip pim mcache-limit`	VRF	
Number of PIM-SM/SSM multicast routing entries	`ip pim mroute-limit`	VRF	

On some occasions, such as network integration, you must make sure that the expected resources required for communication after the integration (that is, the total resources used by the networks before the integration) do not exceed the conditions and capacity for each device.

3. Configuring a Self-Managed VPN

This chapter describes a configuration example of a self-managed VPN and its specific configuration.

3.1 Background and system requirements

Assume that you will provide a network infrastructure in region "K" of a certain municipality, which can be shared by all organizations, agencies, and companies in that region. You want to make that infrastructure accessible to as many organizations as possible, both public and private. However, considering the wide variety of organizations, deploying the required infrastructure within a single network seems difficult.

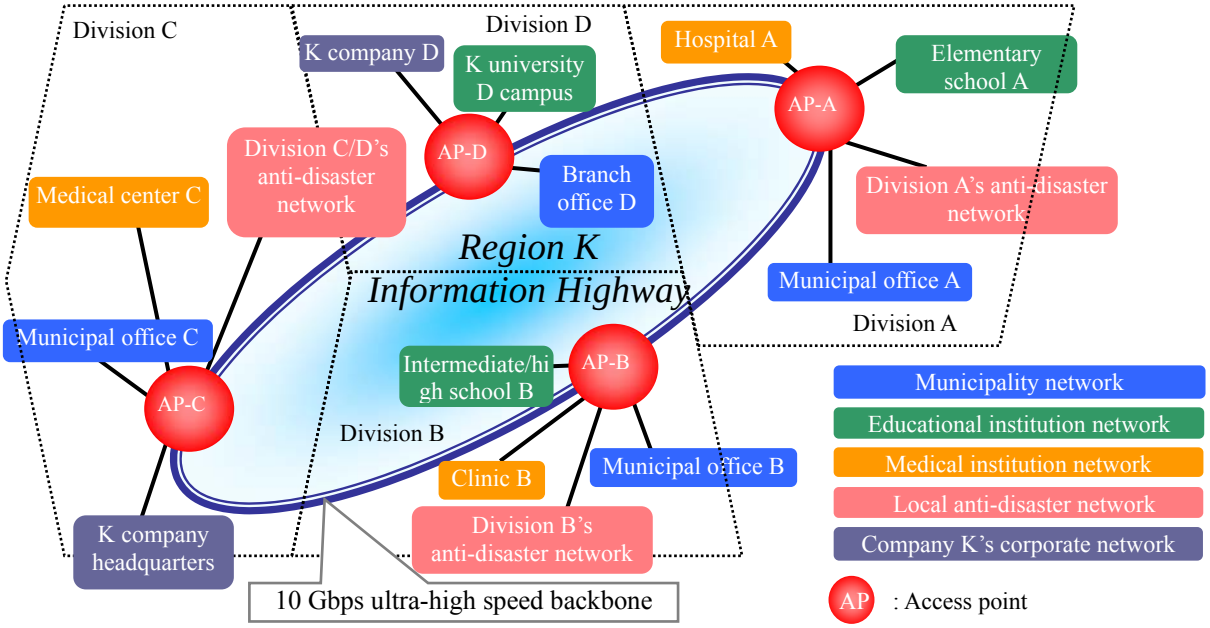


Figure 3.1-1 Network infrastructure in Region K

To meet these requirements, you are going to propose a comprehensive infrastructure using network partitions and containing a small VPN for each organization.

3.2 System design guidelines

This section lists some points to consider for system design, based on the example in this chapter.

(1) Make each user's network an exclusive configuration

We recommend that you configure the system to prevent communication between logical networks used by the respective users. By doing so, you can assign each logical network (that is, the IP address used by each user) without limitation, and as a result, you do not need to worry about duplicate IP addresses among the networks.

(2) Use the tag conversion function to avoid conflicts with user VLAN IDs

You can use the tag conversion function to prevent conflicts between user VLAN IDs used within an intra-organizational network and those used in the network partitions. This allows you to relax use restrictions for the respective intra-organizational networks.

(3) When administering and monitoring devices, their administration networks must be unified

When you are going to gather syslog and SNMP information, you need to specify the monitoring server. You can build a single network for such administration within the network for operation management, for example, the global network, to perform transmissions without L3 relay (within the same subnet). This allows you to use L2 switches, such as AX2400S series and AX1200S series, to perform remote administration using syslog and SNMP without specifying the gateway.

3.3 System configuration example

Considering the increase or decrease of organizations using the system and the addition of local access points, we recommend that you configure the networks so that devices can be easily added to the part beneath the distribution switches. For example, here is a configuration based on a ring network where devices can easily be added.

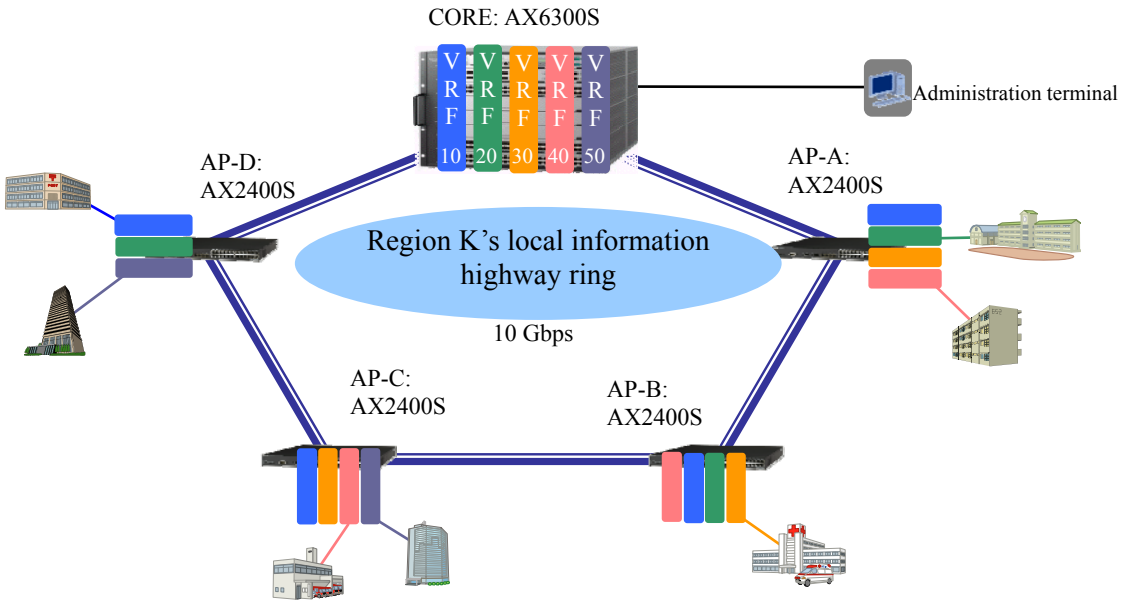


Figure 3.3-1 Self-managed VPN using network partitions and a ring network

Make the network partitions available by using AX6300S for the core of Region K's information highway and enabling the VRF function. In addition, configure the ring network as the backbone network of the information highway. This allows you to configure the backbone to support a maximum of 63 organizational networks.

Install an AX2400S at the access point of each division and open the ports for the network of each destination organization. Provide the modes described in the table below so that the destination organizations can select the appropriate infrastructure type.

Table 3.3-1 Infrastructure connection modes

Connection mode	Type of AP port	VLAN between APs	VLANs open to users[#1]	How users can see the infrastructure
L2 mode	Access	Same	-	Wide area Ethernet image
L3 mode	Access	Different	-	WAN image Routing is OSPF
L3 trunk mode	Trunk (802.1q tag VLAN)	Different	100 to 104	LAN image

AP: Access point

#1 VLAN IDs that users can configure and use for AP ports in the L3 trunk mode

The logical configuration of this system is as follows:

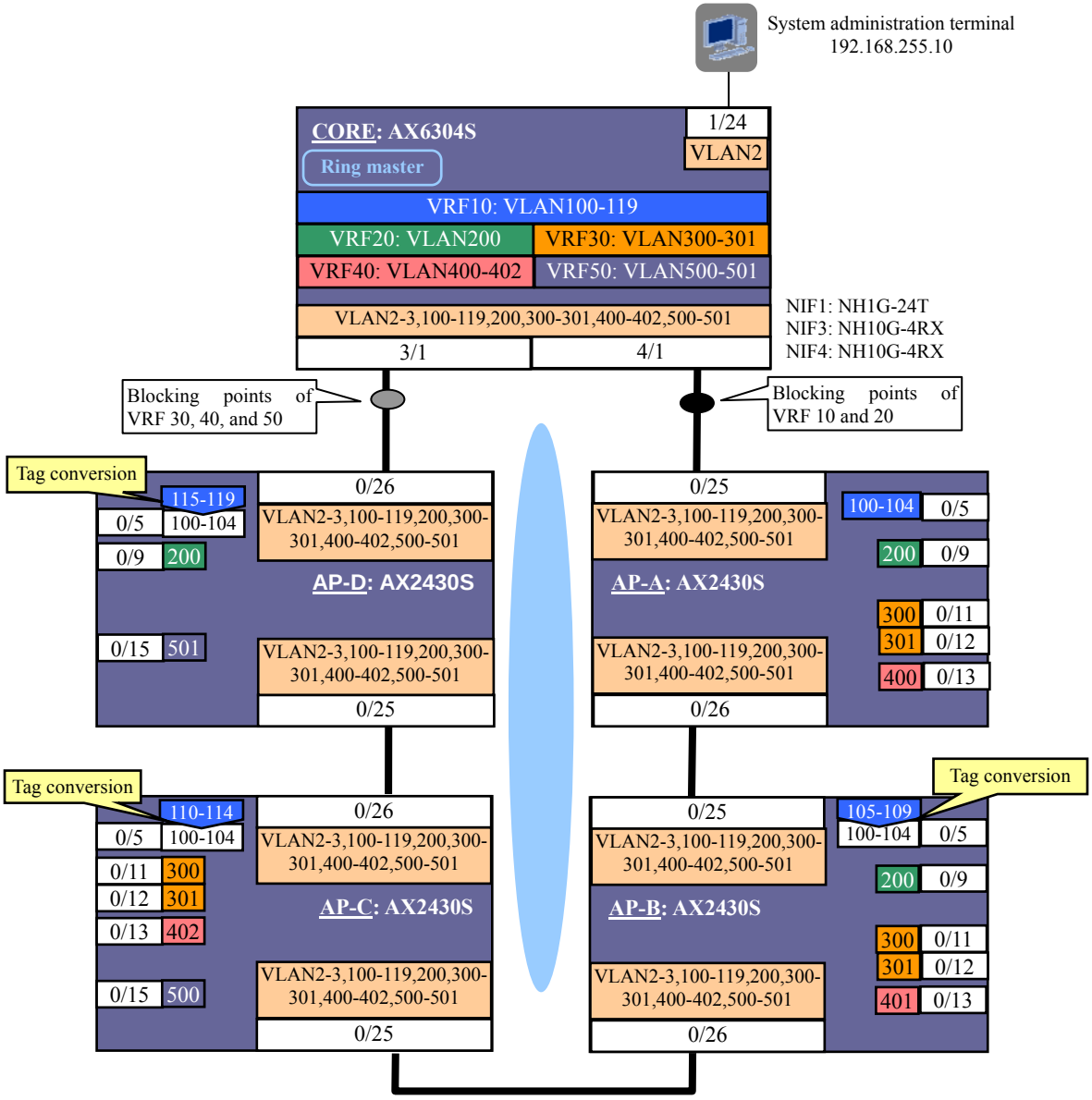


Figure 3.3-2 Logical configuration

For the assignment of partitions (VRF) and VLAN in this system, separate the partitions for each municipality network and user group as described in the table below.

Table 3.3-2 VRF/VLAN definitions

Partition name	VRF ID	AP mode	VLAN name	VLAN ID	IP address#1	Application
Administration	Global	–	Administration	2	192.168.255.0/24	Information highway administration
			Ring control	3	-	Ring control VLAN
Municipality network	10	L3 trunk	Municipal office A (AP-A)	100-104	192.168.100-104.0/24	Municipal office A subnet
			Municipal office B (AP-B)	105-109#2	192.168.115-119.0/24	Municipal office B subnet
			Municipal office C (AP-C)	110-114#2	192.168.110-114.0/24	Municipal office C subnet
			Municipal branch office D (AP-D)	115-119#2	192.168.115-119.0/24	Municipal branch office D subnet
Educational institution network	20	L2	Each site AP	200	-	Openness to users in each division
Medical institution network	30	L2	Each site AP	300	-	Openness to users in each division
			Each site AP	301	-	Openness to users in each division
Local anti-disaster network	40	L3	AP-A	400	192.168.40.0/24	Division A anti-disaster network
			AP-B	401	192.168.41.0/24	Division B anti-disaster network
			AP-C	402	192.168.42.0/24	Divisions C, D anti-disaster network
Company K's network	50	L3	AP-C	500	192.168.50.0/24	Headquarters
			AP-D	501	192.168.51.0/24	Branch D

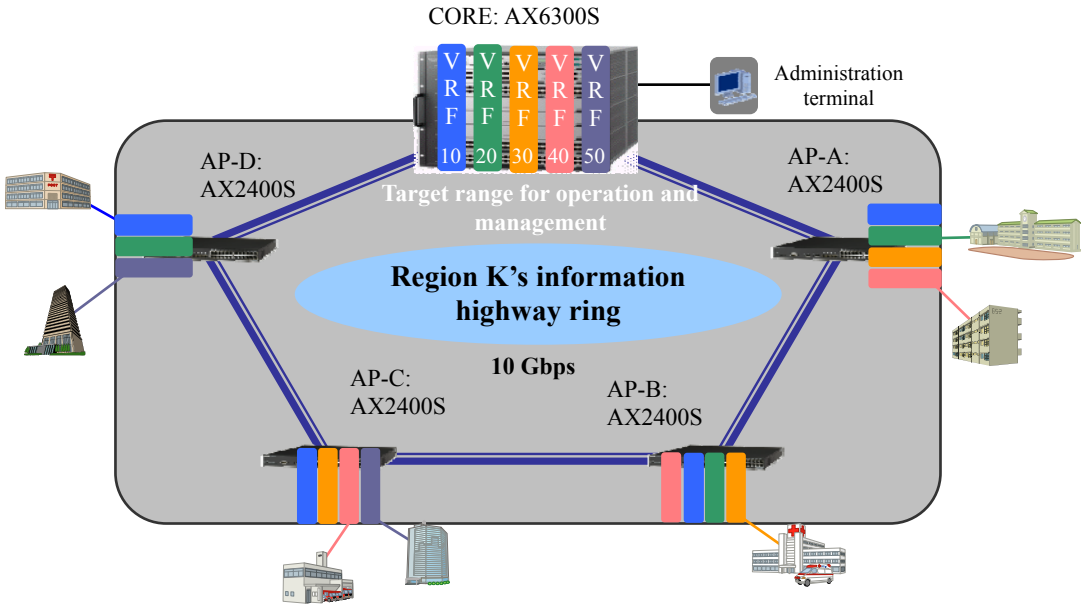
#1 The gateway addresses in L3 mode.
#2 Tag conversion function is configured. At the APs, users use VLANs 100 to 104.

In the network used by the municipality itself, 5 different VLANs are used for the sites. However, you must use the tag conversion function to assign IDs (100 to 104) to the VLANs for all the organizations that connect to each site AP. This allows you to standardize the settings for the L2 switches used by each of the organizations.
Use the APs in L2 mode for the educational institution and medical institution networks, and in L3 mode for the local anti-disaster and Company K networks.

The advantage of this system is that, by using network partitions, you can use a common infrastructure while setting up a separate L3 network for each organization, to easily configure small VPNs.
In case the system does not have the VRF function, the L3 core devices present all networks as subnets. Additionally, if Region K's ISP network and Company K's corporate network have their own routers or L3 switches, they might see a mixture of routes to each other's networks. This can cause many management and security problems for each organization.

3.4 Operation management

In this system, you operate and administer the network that is provided as the regional infrastructure, and the operation and administration of the networks configured by users are entrusted to the respective users. Therefore, you configure the global network for the devices within the range formed by the access points.



Monitored network	Monitored device	Information collected	Collection route
Entire regional infrastructure (global)	CORE	Global, VRF10, VRF20, VRF30, VRF40, VRF50	Global network
	AP-A	Global, VRF10, VRF20, VRF30, VRF40	
	AP-B	Global, VRF10, VRF20, VRF30	
	AP-C	Global, VRF10, VRF30, VRF40	
	AP-D	Global, VRF10, VRF20, VRF50	

Figure 3.4-1 System operation and management

3.5 Points for configuring devices

This section lists some points to consider for system design, based on the example in this chapter.

(1) Use the tag conversion function to relate the VLAN ID of the system to the VLAN ID of the user

If you want to separate the VLAN ID used in the intra-organizational networks and the VLAN ID used in the provided infrastructure system, use the tag conversion function to allocate the IDs.

(2) Specify an IP address for the VLAN that belongs to the administration network

To remotely operate and administer devices, assign an IP address for managing the devices to the VLAN that belongs to the administration network.

(3) See the *[Basic]* guide for VRF settings guidelines

For details about how to configure VRF settings, see the ***AX Series Network Partition: Solution Guide [Basic]***. Below are excerpts from ***3.2.1. Important points in the configuration*** in ***3.2 Network partitions in a ring network*** of the above guide. These excerpts contain information related to the sample system described here.

- **Points for configuring the ring network**

(2) Disable spanning trees
(3) Activate VRF in a mode using RingProtocol
(4) Assign VLANs to partitions (VRF)
(5) Match the VLAN mapping IDs with the VRF-IDs
(6) Routing protocols, if any, must be assigned to a partition (VRF) as an operating point
(7) Remote control must be via the global network

3.6 Sample configurations

This section provides examples of key configurations for implementing the core switch in the system and a device for the access point. See the *Appendix* for details about device configurations.

(1) L3 core switch: CORE (AX6304S)

CORE (AX6304S) configurations	
Disabling the spanning-tree	
(config)# **spanning-tree disable**	Disable PVST+, which is enabled by default. (Important point - *[Basic](2)*)
Configuring VRFs	
(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 (config)# **vrf definition 10** (config)# **vrf definition 20** (config)# **vrf definition 30** (config)# **vrf definition 40** (config)# **vrf definition 50**	Configure the VRF in combination with the ring protocol. (Important point - *[Basic](3)*) (You are prompted to restart the PSP. Enter y to restart.) Specify VRF 10 to be used. Specify VRF 20 to be used. Specify VRF 30 to be used. Specify VRF 40 to be used. Specify VRF 50 to be used.
Configuring VLANs	
(config)# **vlan 2-3,100-119,200,300-301,400-402,500-501**	Set the VLANs to be used.
Configuring the VLAN interface	
Configuring the VLAN for the global network	
(config)# **interface vlan 2** (config-if)# **ip address 192.168.255.1 255.255.255.0**	Specify VLAN 2 to be used in the global network for system administration. (Important point - *[Basic](7)*) Specify the IP address for VLAN 2. (Important point - *(2)*)
Configuring VLANs for VRF 10 (municipality network)	
(config)# **interface vlan 100** (config-if)# **vrf forwarding 10** (config-if)# **ip address 192.168.100.1 255.255.255.0** (config)# **interface vlan 101** (config-if)# **vrf forwarding 10** (config-if)# **ip address 192.168.101.1 255.255.255.0** : (omission) : (config)# **interface vlan 119** (config-if)# **vrf forwarding 10** (config-if)# **ip address 192.168.119.1 255.255.255.0**	Use VLANs 100 to119 for VRF 10. Specify the IP addresses for VLANs 100 to 119. (Important point - *[Basic](4)*)
Configuring VLANs for VRF 20 (educational institution network)	
(config)# **interface vlan 200** (config-if)# **vrf forwarding 20**	Use VLANs 200 and 201 for VRF 20. (Important point - *[Basic](4)*)
Configuring VLANs for VRF 30 (medical institution network)	
(config)# **interface range vlan 300-301** (config-if-range)# **vrf forwarding 30**	Use VLANs 300 and 301 for VRF 30. (Important point - *[Basic](4)*)
Configuring VLANs for VRF 40 (local anti-disaster network)	
(config)# **interface vlan 400** (config-if)# **vrf forwarding 40** (config-if)# **ip address 192.168.40.1 255.255.255.0** (config)# **interface vlan 401** (config-if)# **vrf forwarding 40** (config-if)# **ip address 192.168.41.1 255.255.255.0** (config)# **interface vlan 402** (config-if)# **vrf forwarding 40** (config-if)# **ip address 192.168.42.1 255.255.255.0**	Use VLANs 400 and 402 for VRF 40. Specify the IP addresses for VLANs 400 and 402. (Important point - *[Basic](4)*)
Configuring VLANs for VRF 50 (Company K's network)	

CORE (AX6304S) configurations	
(config)# **interface vlan 500** (config-if)# **vrf forwarding 50** (config-if)# **ip address 192.168.50.1 255.255.255.0** (config)# **interface vlan 501** (config-if)# **vrf forwarding 50** (config-if)# **ip address 192.168.51.1 255.255.255.0**	Use VLANs 500 and 501 for VRF 50. Specify the IP addresses for VLANs 500 and 501. (Important point - *[Basic](4)*)
Configuring the physical port interface	
Configuring the administration port	
(config)# **interface gigabitethernet 1/24** (config-if)# **switchport access vlan 2**	Specify port 1/24 as the VLAN 2 access port for administration.
Configuring ring ports	
(config)# **interface range tengigabitethernet 3/1, tengigabitethernet 4/1** (config-if-range)# **link debounce time 0** (config-if-range)# **switchport mode trunk** (config-if-range)# **switchport trunk allowed vlan 2-3,100-119,200,300-301,400-402,500-501** (config-if-range)# **axrp-ring-port 1**	Configure ports 3/1 and 4/1 for connecting to the ring network. Specify VLANs 2, 3, 100 to 119, 200, 201, 300, 301, 400 to 402, 500, and 501 as the trunk ports and enable their transmission. Specify as the ring port with RING ID=1.
Configuring the VLAN mapping	
(config)# **axrp vlan-mapping 1 vlan 2** (config)# **axrp vlan-mapping 10 vlan 100-119** (config)# **axrp vlan-mapping 20 vlan 200** (config)# **axrp vlan-mapping 30 vlan 300-301** (config)# **axrp vlan-mapping 40 vlan 400-402** (config)# **axrp vlan-mapping 50 vlan 500-501**	Specify the VLAN 2 used in the global network for the VLAN mapping 1 of the ring. (Important point - *[Basic](5)*) Specify the VLANs 100 to 119 used in VRF 10 for the VLAN mapping 10 of the ring. (Important point - *[Basic](5)*) Specify the VLAN 200 used in VRF 20 for the VLAN mapping 20 of the ring. (Important point - *[Basic](5)*) Specify the VLANs 300 and 301 used in VRF 30 for the VLAN mapping 30 of the ring. (Important point - *[Basic](5)*) Specify the VLANs 400 and 402 used in VRF 40 for the VLAN mapping 40 of the ring. (Important point - *[Basic](5)*) Specify the VLANs 500 and 501 used in VRF 50 for the VLAN mapping 50 of the ring. (Important point - *[Basic](5)*)
Configuring the ring protocol	
(config)# **axrp 1** (config-axrp)# **mode master** (config-axrp)# **control-vlan 3** (config-axrp)# **vlan-group 1 vlan-mapping 1,10,20** (config-axrp)# **vlan-group 2 vlan-mapping 30,40,50** (config-axrp)# **health-check interval 200** (config-axrp)# **health-check holdtime 600**	Specify the ring with RING ID=1. This node is set as the master node. Specify VLAN 3 to the control VLAN. Assign the VLAN mappings 1, 10, and 20 to VLAN group 1, and VLAN mappings 30, 40, and 50 to VLAN group 2. Set the health-check transmission interval to 200 ms and the health-check hold time to 600 ms.
Configuring the routing protocol	
(config)# **router ospf 1 vrf 40** (config-router)# **network 192.168.40.0 0.0.0.255 area 0** (config-router)# **network 192.168.41.0 0.0.0.255 area 0** (config-router)# **network 192.168.42.0 0.0.0.255 area 0** (config)# **router ospf 1 vrf 50** (config-router)# **network 192.168.50.0 0.0.0.255 area 0** (config-router)# **network 192.168.51.0 0.0.0.255 area 0**	Specify the OSPF for the routing protocol used in VRF 40. (Important point - *[Basic](6)*) Specify the OSPF for the routing protocol used in VRF 50. (Important point - *[Basic](6)*)
Configuring the syslog server	
(config)# **logging host 192.168.255.10**	Specify the IP address of the syslog server. (Important point - *[Basic Guide](7)*)

(2) Access point: AP-B (AX2430S)

AP-B (AX2430S) configurations	
Disabling the spanning–tree	
(config)# **spanning-tree disable**	Disable PVST+, which is enabled by default. (Important point - *[Basic](2)*)
Configuring VLANs	
(config)# **vlan 2-3,100-119,200,300-301,400-402,500-501**	Specify the VLANs to be used.
Configuring the VLAN interface	
(config)# **interface vlan 2** (config-if)# **ip address 192.168.255.3 255.255.255.0**	Specify the IP address to VLAN 2 for administration. (Important point - *(2)*)
Configuring the physical port interface	
Configuring the ring port	
(config)# **interface range tengigabitethernet 0/25-26** (config-if-range)# **link debounce time 0** (config-if-range)# **switchport mode trunk** (config-if-range)# **switchport trunk allowed vlan 2-3,100-119,200,300-301,400-402,500-501** (config-if-range)# **axrp-ring-port 1**	Configure ports 0/25 to 0/26 for connecting to the ring network. Specify VLANs 2-3, 100-104, 200, 300-301, 400-402, and 500-501 as the trunk ports and enable their transmission. Specify as the ring port with RING ID=1.
Configuring access ports	
(config)# **interface gigabitethernet 0/5** (config-if)# **switchport mode trunk** (config-if)# **switchport trunk allowed vlan 105-109** (config-if)# **switchport vlan mapping 100 105** (config-if)# **switchport vlan mapping 101 106** (config-if)# **switchport vlan mapping 102 107** (config-if)# **switchport vlan mapping 103 108** (config-if)# **switchport vlan mapping 104 109** (config-if)# **switchport vlan mapping enable** (config)# **interface gigabitethernet 0/9** (config-if)# **switchport mode access** (config-if)# **switchport access vlan 200** (config)# **interface gigabitethernet 0/11** (config-if)# **switchport mode access** (config-if)# **switchport access vlan 300** (config)# **interface gigabitethernet 0/12** (config-if)# **switchport mode access** (config-if)# **switchport access vlan 301** (config)# **interface gigabitethernet 0/13** (config-if)# **switchport mode access** (config-if)# **switchport access vlan 401**	Configure port 0/5 as the trunk port of VLANs 105 to 109. However, use tag conversion to convert VLANs 105 to 109 to VLANs 100 to 104 respectively. (Important point - *(1)*) Configure port 0/9 as the access port of VLAN 200. Configure port 0/11 as the access port of VLAN 300. Configure port 0/12 as the access port of VLAN 301. Configure port 0/13 as the access port of VLAN 401.
Configuring the VLAN mapping	
(config)# **axrp vlan-mapping 1 vlan 2** (config)# **axrp vlan-mapping 10 vlan 100-119** (config)# **axrp vlan-mapping 20 vlan 200** (config)# **axrp vlan-mapping 30 vlan 300-301** (config)# **axrp vlan-mapping 40 vlan 400-402** (config)# **axrp vlan-mapping 50 vlan 500-501**	Specify VLAN 2 for the VLAN mapping 1 of the ring. Specify VLANs 100 and 101 for the VLAN mapping 10 of the ring. Specify VLAN 200 for the VLAN mapping 20 of the ring. Specify VLANs 300 and 301 for the VLAN mapping 30 of the ring. Specify VLANs 400 and 402 for the VLAN mapping 40 of the ring. Specify VLANs 500 and 501 for the VLAN mapping 50 of the ring.
Configuring the ring protocol	
(config)# **axrp 1** (config-axrp)# **mode transit** (config-axrp)# **control-vlan 3** (config-axrp)# **vlan-group 1 vlan-mapping 1,10,20** (config-axrp)# **vlan-group 2 vlan-mapping 30,40,50**	Specify the ring with RING ID=1 as the transit node. Specify VLAN 3 for the control VLAN. Assign the VLAN mappings 1, 10, and 20 to VLAN group 1, and VLAN mappings 30, 40, and 50 to VLAN group 2.
Configuring the syslog server	
(config)# **logging host 192.168.255.10**	Specify the IP address of the syslog server.

4. Separating Networks

This chapter presents a step-by-step example of the procedure for separating networks.

4.1 Background and system requirements

X University distributes the devices to each campus or department and assigns a subnet to each department to operate the system. General information on the university is managed with a shared server in the data center, which is accessible from all departments. However, the departments also have their own servers for storing information that they want to restrict access to.

With the spread of wireless LANs, the campuses are worried about access from private PCs and unauthorized access by outsiders. Therefore, there is a growing demand to enhance each department's security.

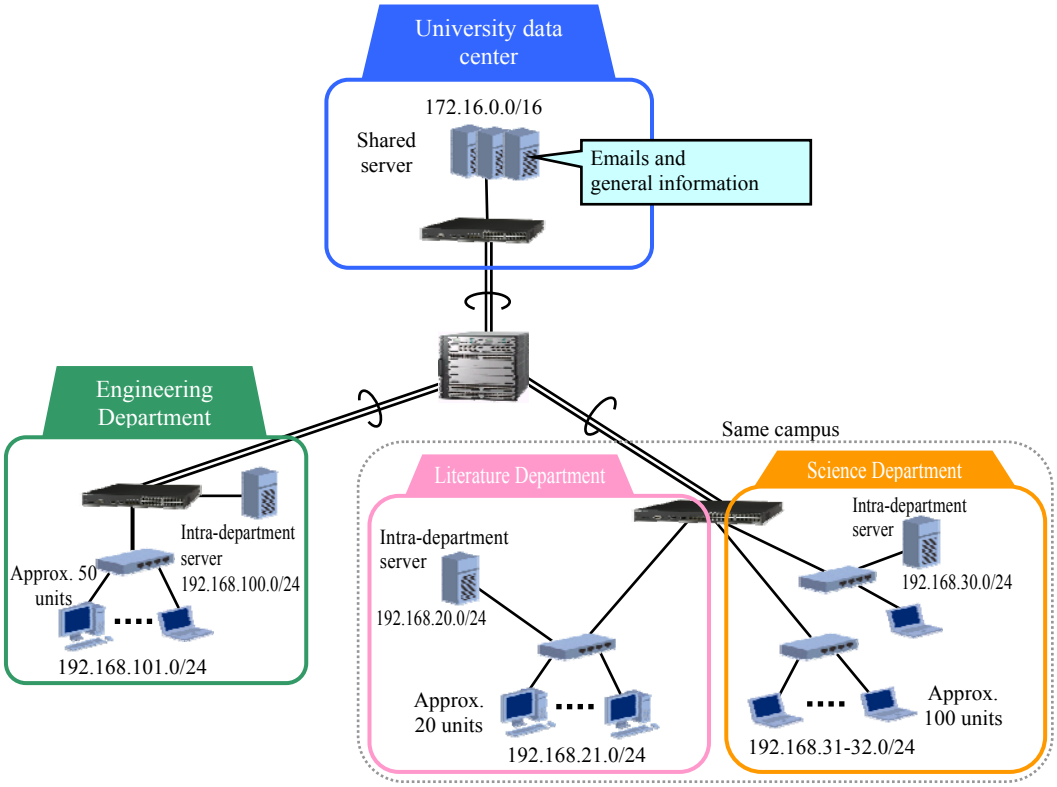


Figure 4.1-1 X University's campus network

You will introduce new network partitions to phase in the configuration of an independent network for each department, while preserving the basic infrastructure of the campus network. You will also build a shared network for accessing the common information of the university and for exchanging email. A network authentication system using Web authentication must also be installed to allow access only to the students and professors of each department.

4.2 System design guidelines

This section describes some tips for system design based on the example in this chapter.

(1) Inherit the address scheme before the separation

When you are separating existing networks, if you can inherit the assigned subnets before the separation to the respective networks after the separation, you do not need to modify the settings of the connected terminals and servers. Additionally, there will be no duplication of IP addresses between the networks after the separation, and this enables you to establish a new shared network. Considering these advantages, we recommend that you inherit the address scheme to the separated networks.

(2) Make use of a shared network

Even if you separate the networks and configure logical networks, if there is no duplication of IP addresses between those networks, you can configure a shared network. If there is any access target that is impossible to separate, such as a shared server (shared by all departments) in the example of this chapter, we recommend that you use a shared network.

If you are already aware of the necessity of using a shared network, we recommend that you separate the networks, including the shared network, during initial system modification, such as the first system modification described in this chapter.

If you are initially only going to separate an independent network without configuring a shared network, some settings, such as the filtering conditions for the global network, might be complicated. Therefore, if you are going to use a shared network, it is much easier to configure the settings when you first separate the shared part of the network.

(3) When administering and monitoring devices, their administration networks must be unified

When you are going to gather syslog and SNMP information, you need to specify the monitoring server. You can build a single network for such administration within the network for operation management, for example, the global network, to perform transmissions without L3 relay (within the same subnet). This might allow you to use L2 switches, such as those of the AX2400S series and AX1200S series, to perform remote administration using syslog and SNMP without specifying the gateway.

4.3 System configuration example

When using network partitions, the core switches must be replaced with AX6000 family switches (the AX6700S, AX6600S, and AX6300S series). If you use these switches to configure the network partition based on the fault-tolerant network, you can build the system with redundancy. It might also be possible to divert the devices that have been used for the existing networks to the L2 switches located on the access edge. (The devices must support link aggregation.)

The following diagram represents the separation of existing networks. In this case, there is no duplication of IP addresses among the networks after separation, and this enables you to establish a new shared network to handle the common data for all departments and the information you do not want to separate.

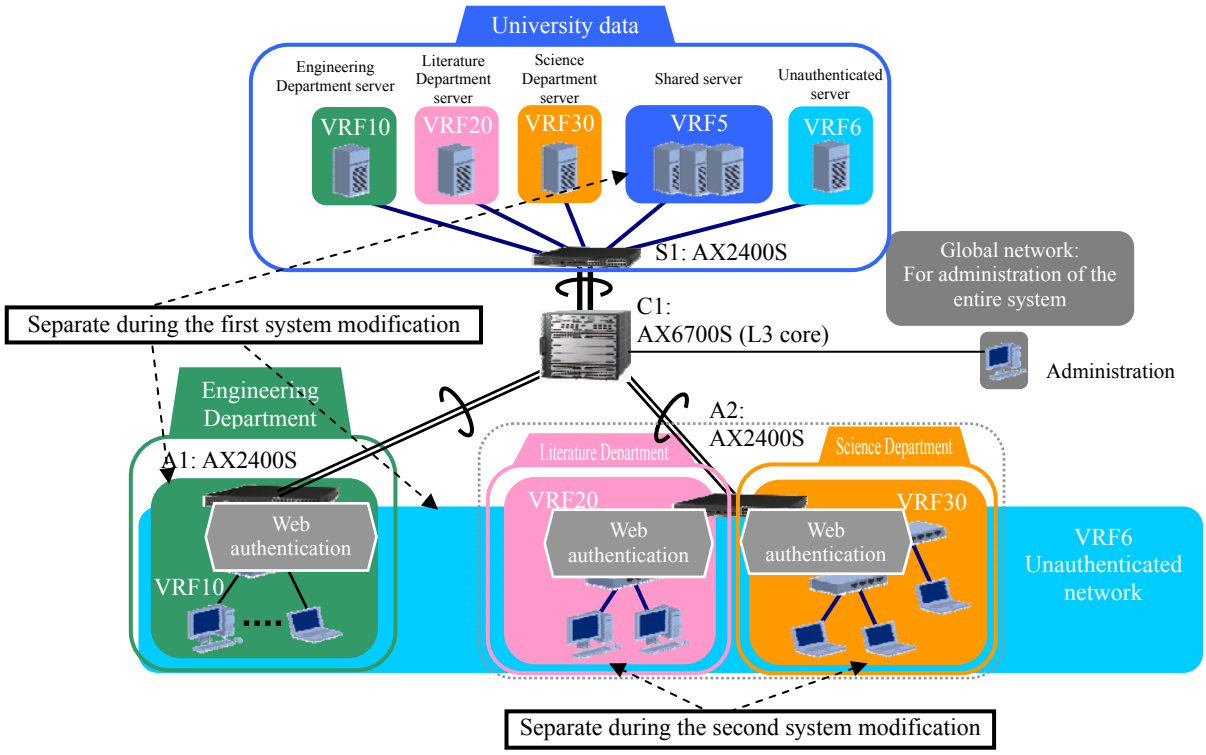


Figure 4.3-1 Separating the departments with network partitions

Install AX6700S as the core device of the backbone. Perform the first and second system modifications, and then use the VRF function to phase in the separation of three independent networks for the respective departments, the shared network which is accessible from these department networks, and the global network for administration. Configure a fault-tolerant network based on link aggregation, as a physical configuration, to divert the access switches AX2400S which had been used in the departments to those for the university data center and the departments. (The Literature Department and the Science Department will share the same switch.)

All servers that the departments had previously used will be moved to the university data center for integrated operation management, such as data backup. However, network partitions make the servers remain accessible only from their respective departments. The mail servers and general-purpose servers that the departments had previously shared will be located on the shared network, which is accessible by all departments.

The final logical configuration of the system after separating the networks is as follows:

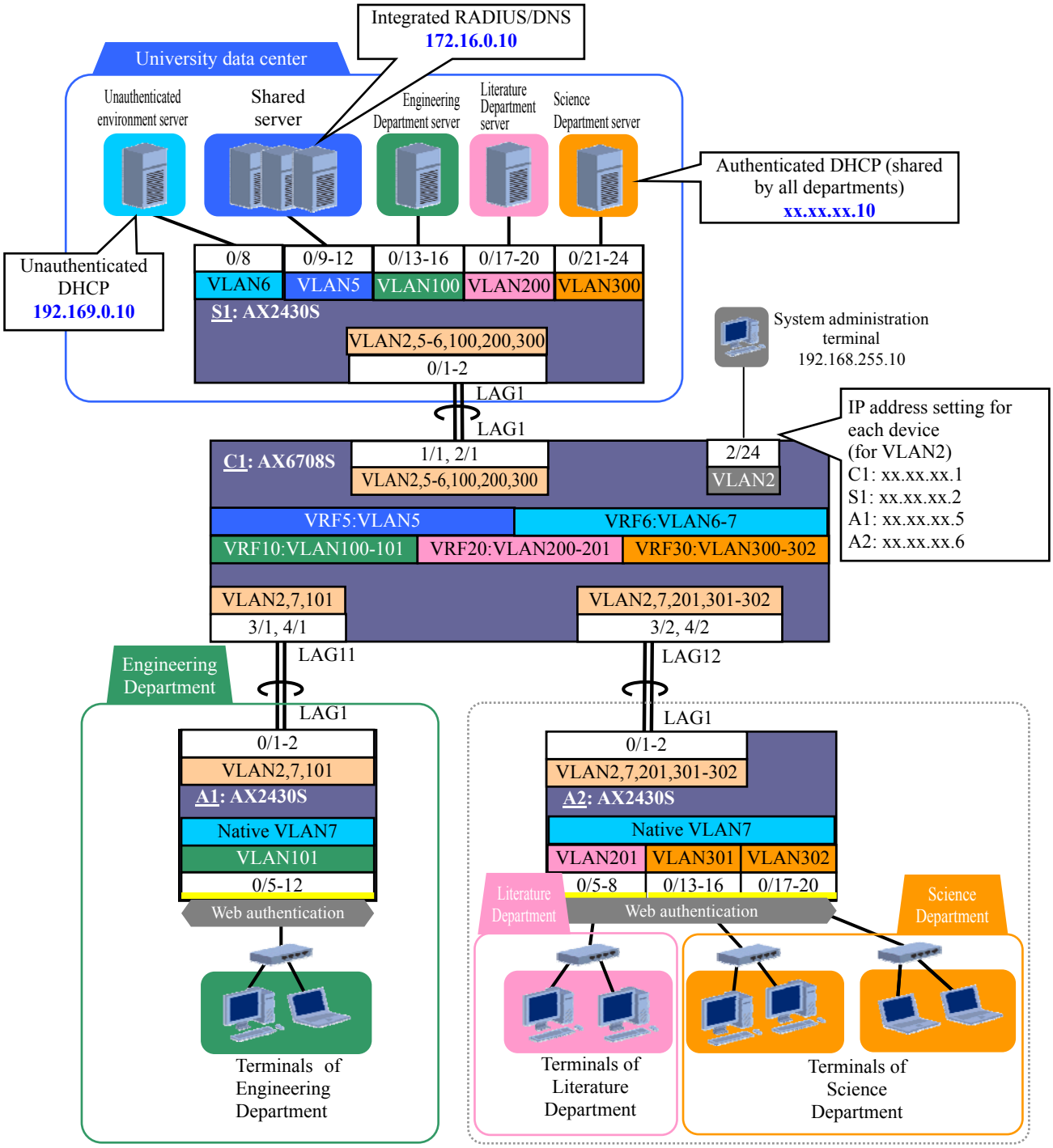


Figure 4.3-2 Logical configuration

Separate the networks step by step in the manner shown below.

System deployment: Deploy all the university facilities (without specifying VRFs) within the global network.

Table 4.3-1 VRF/VLAN definitions for system deployment

Partition name	VRF ID	VLAN name	VLAN ID	IP address	Application
Administration	Global	Administration	2	192.168.255.0/24	Entire network administration
Shared		Shared server	5	172.16.0.0/16	Shared server
Unauthenticated		Unauthenticated server	6	192.169.0.0/24	Unauthenticated environment server
		Unauthenticated	7	192.168.0.0/24	Unauthenticated terminal
Engineering Department		Intra-department server	100	192.168.100.0/24	Intra-department server
		Client 1	101	192.168.101.0/24	Engineering Department terminal
Literature Department		Intra-department server	200	192.168.20.0/24	Intra-department server
		Client	201	192.168.21.0/24	Literature Department terminal
Science Department		Intra-department server	300	192.168.30.0/24	Intra-department server
		Client	301	192.168.31.0/24	Science Department terminal 1
			302	192.168.32.0/24	Science Department terminal 2

First system modification: Separate the Shared, Unauthenticated, and Engineering Department partitions from the global network.

Table 4.3-2 VRF/VLAN definitions for the first system modification

Partition name	VRF ID	VLAN name	VLAN ID	IP address	Application
Administration	Global	Administration	2	192.168.255.0/24	Entire network administration
Literature Department		Intra-department server	200	192.168.20.0/24	Intra-department server
		Client	201	192.168.21.0/24	Literature Department terminal
Science Department		Intra-department server	300	192.168.30.0/24	Intra-department server
		Client	301	192.168.31.0/24	Science Department terminal 1
			302	192.168.32.0/24	Science Department terminal 2
Shared	5	Shared server	5	172.16.0.0/16	Shared server
Unauthenticated	6	Unauthenticated server	6	192.169.0.0/24	Unauthenticated environment server
		Unauthenticated	7	192.168.0.0/24	Unauthenticated terminal
Engineering Department	10	Intra-department server	100	192.168.100.0/24	Intra-department server
		Client 1	101	192.168.101.0/24	Engineering Department terminal

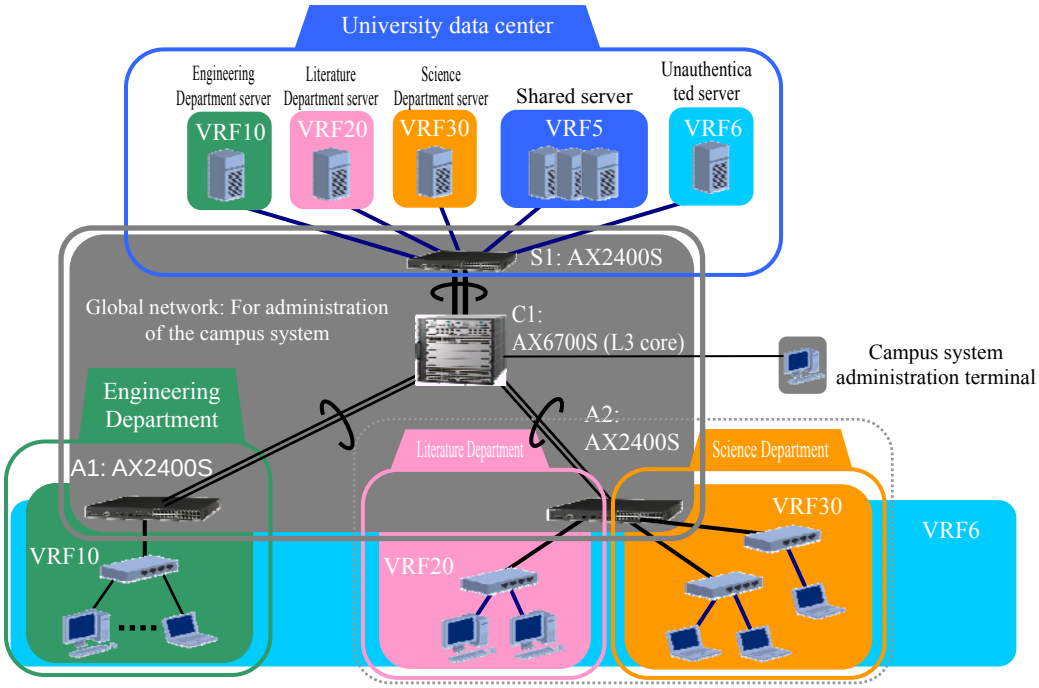
Second system modification: Separate the Literature Department and Science Department partitions from the global network.

Table 4.3-3 Final VRF/VLAN definitions

Partition name	VRF ID	VLAN name	VLAN ID	IP address	Application
Administration	Global	Administration	2	192.168.255.0/24	Entire network administration
Shared	5	Shared server	5	172.16.0.0/16	Shared server
Unauthenticated	6	Unauthenticated server	6	192.169.0.0/24	Unauthenticated environment server
		Unauthenticated	7	192.168.0.0/24	Unauthenticated terminal
Engineering Department	10	Intra-department server	100	192.168.100.0/24	Intra-department server
		Client 1	101	192.168.101.0/24	Engineering Department terminal
Literature Department	20	Intra-department server	200	192.168.20.0/24	Intra-department server
		Client	201	192.168.21.0/24	Literature Department terminal
Science Department	30	Intra-department server	300	192.168.30.0/24	Intra-department server
		Client	301	192.168.31.0/24	Science Department terminal 1
			302	192.168.32.0/24	Science Department terminal 2

4.4 Operation management

All the university facilities are to be centrally managed. To do this, the global network is expanded to include the access edge devices. Operation management, which is conducted within the global network, is not affected by the first or second system modification.



Monitored network	Monitored device	Information collected	Collection route
Entire campus system (Global)	C1	Global, VRF5, VRF6, VRF10, VRF20, VRF30	Global network
	S1	VRF5, VRF10, VRF20, VRF30	
	A1	VRF6, VRF10	
	A2	VRF6, VRF20, VRF30	

Figure 4.4-1 System operation management

4.5 Points for configuring devices

This section lists some points for configuring the devices used in the system.

(1) Specify the VRF operation mode before separating the networks

If in future you plan to separate the networks, as described in this chapter, we recommend that you enable the VRF operation mode (by using the vrf mode command) when you deploy each network. This is because when you enable the VRF operation mode, the BSU portion (for the AX6700S series) or PSP portion (for the AX6600S or AX6300S series) must be restarted, which causes all communication to stop temporarily.

(2) Use only VRF devices to separate the active networks

VRFs can be configured by performing a series of operations on the devices where the VRFs are active. The same is true for VRFs that must be configured in order to separate the active networks. There is no need to modify the settings for the distribution and access edge switches.

(3) Configure VRFs for active VLANs after deleting their IP addresses

Active networks are separated by adding VRF specifications to the VLANs that are currently used by the VRF devices. When adding the VRF specifications, make sure that you delete the IP addresses that are specified for these VLANs. After you finish adding the specifications, specify the addresses again. Communication via the VLANs stops after the IP addresses are deleted, and resumes when they are specified again.

In the example described in this chapter, the shared server and the Engineering Department network are temporarily stopped during the first system modification. The Literature Department and Science Department networks are temporarily stopped during the second system modification.

(4) Specify an IP address for the VLAN that belongs to the administration network

To remotely operate and administer devices, assign an IP address (for administering the devices) to the VLAN that belongs to the administration network.

(5) See the guide *[Basic]* for the VRF settings guidelines

For details about how to configure the VRF settings, see the ***AX Series Network Partition: Solution Guide [Basic]***. Below are excerpts from ***3.1.1. Important points in the configuration*** in ***3.1 Network Partition in an FT network*** of the guide above. These excerpts contain information related to the sample system described here.

- **Points for configuring the FT network**

(2) Disable spanning trees
(3) Activate VRF in a mode where no L2 protocol is enabled at the same time
(4) Assign VLANs to the partitions (VRF)
(6) Remote control must be via the global network

(6) See the guide [For Authentication] and AX Series Authentication Solution Guide for details about the authentication switch

For details about how to configure the VRF device to be equipped with authentication functions, see the ***AX Series Network Partition: Solution Guide [For Authentication]***. For details about how to configure the authentication function settings, see the ***AX Series Authentication Solution Guide***.

4.6 Sample configurations

This section provides examples of key configurations for implementing the core switch, distribution devices, and access edge devices in the system. See *Appendix* for details about the device configurations.

(1) L3 core switch for network deployment: C1 (AX6708S)

C1 (AX6700S) configurations for network deployment (without VRF separation)	
Disabling the spanning-tree	
(config)# **spanning-tree disable**	Disable PVST +, which is enabled by default. (Important point - *[Basic](2)*)
Configuring the VRF	
(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	Configure the VRF without using the L2 protocol. (Points for configuring - *(1)* and *[Basic](3)*) (You are prompted to restart the BSU. Enter y to restart.)
Configuring VLANs	
(config)# **vlan 2,5-7,100-101,200-201,300-302**	Specify the VLANs to be used.
Configuring the VLAN interface	
Configuring the VLAN for the system administration	
(config)# **interface vlan 2** (config-if)# **ip address 192.168.255.1 255.255.255.0**	Specify VLAN 2 to be used for system administration. (Important point - *[Basic](6)*) Specify the IP address for VLAN 2. (Important point - *(4)*)
Configuring the VLAN for the shared network	
(config)# **interface vlan 5** (config-if)# **ip address 172.16.0.1 255.255.0.0**	Specify VLAN 5. (Important point - *[Basic](4)*) Specify the IP address for VLAN 5.
Configuring the unauthenticated VLANs	
(config)# **interface vlan 6** (config-if)# **ip address 192.169.0.1 255.255.0.0** (config)# **interface vlan 7** (config-if)# **ip address 192.168.0.1 255.255.0.0** (config-if)# **ip helper-address 192.169.0.10**	Specify VLAN 6. (Important point - *[Basic](4)*) Specify the IP address for VLAN 6. Specify VLAN 7. (Important point - *[Basic](4)*) Specify the IP address for VLAN 7. Specify the transfer destination for the DHCP relay agent.
Configuring the Engineering Department VLANs	
(config)# **interface vlan 100** (config-if)# **ip address 192.168.100.1 255.255.255.0** (config)# **interface vlan 101** (config-if)# **ip address 192.168.101.1 255.255.255.0** (config-if)# **ip helper-address 192.168.100.10** (config-if)# **ip access-group bf_dhcp in layer3-forwarding**	Specify VLANs 100 and 101. (Important point - *[Basic](4)*) Specify the IP addresses for VLANs 100 and 101. Specify the following for VLAN 101: - Transfer destination for the DHCP relay agent - Access list used to deny access to the DHCP server for the unauthenticated VLAN
Configuring the Literature Department VLANs	
(config)# **interface vlan 200** (config-if)# **ip address 192.168.20.1 255.255.255.0** (config)# **interface vlan 201** (config-if)# **ip address 192.168.21.1 255.255.255.0** (config-if)# **ip helper-address 192.168.20.10** (config-if)# **ip access-group bf_dhcp in layer3-forwarding**	Specify VLANs 200 and 201. (Important point - *[Basic](4)*) Specify the IP addresses for VLANs 200 and 201. Specify the following for VLAN 201: - Transfer destination for the DHCP relay agent - Access list used to deny access to the DHCP server for the unauthenticated VLAN
Configuring the Science Department VLANs	
(config)# **interface vlan 300** (config-if)# **ip address 192.168.30.1 255.255.255.0**	Specify VLAN 300. (Important point - *[Basic](4)*) Specify the IP address for VLAN 300.

C1 (AX6700S) configurations for network deployment (without VRF separation)	
(config)# **interface vlan 301** (config-if)# **ip address 192.168.31.1 255.255.255.0** (config-if)# **ip helper-address 192.168.30.10** (config-if)# **ip access-group bf_dhcp in layer3-forwarding** (config)# **interface vlan 302** (config-if)# **ip address 192.168.32.1 255.255.255.0** (config-if)# **ip helper-address 192.168.30.10** (config-if)# **ip access-group bf_dhcp in layer3-forwarding**	Specify VLANs 300 and 301. (Important point - *[Basic](4)*) Specify the IP addresses for VLANs 300 and 301. Specify the following for VLANs 300 and 301: - Transfer destination for the DHCP relay agent - Access list used to deny access to the DHCP server for the unauthenticated VLAN
Configuring the physical port interface	
Configuring ports	
(config)# **interface gigabitethernet 2/24** (config-if)# **switchport access vlan 2** (config)# **interface range gigabitethernet 1/1, gigabitethernet 2/1** (config-if-range)# **link debounce time 0** (config-if-range)# **channel-group 1 mode on** (config)# **interface range gigabitethernet 3/1, gigabitethernet 4/1** (config-if-range)# **link debounce time 0** (config-if-range)# **channel-group 11 mode on** (config)# **interface range gigabitethernet 3/2, gigabitethernet 4/2** (config-if-range)# **link debounce time 0** (config-if-range)# **channel-group 12 mode on**	Specify port 2/24 as the VLAN 2 access port used for system administration. Specify ports 1/1 and 2/1 to implement channel group 1, which is used to connect to device S1. Specify ports 3/1 and 4/1 to implement channel group 11, which is used to connect to device A1. Specify ports 3/2 and 4/2 to implement channel group 12, which is used to connect to device A2.
Configuring port channels	
(config)# **interface port-channel 1** (config-if)# **switchport mode trunk** (config-if)# **switchport trunk allowed vlan 2,5-6,100,200,300** (config)# **interface port-channel 11** (config-if)# **switchport mode trunk** (config-if)# **switchport trunk allowed vlan 2,7,101** (config)# **interface port-channel 12** (config-if)# **switchport mode trunk** (config-if)# **switchport trunk allowed vlan 2,7,201,301-302**	Specify port channel 1 as the trunk port channel that allows transfer via VLANs 2, 5, 6, 100, 200, and 300. Specify port channel 11 as the trunk port channel that allows transfer via VLANs 2, 7, and 101. Specify port channel 12 as the trunk port channel that allows transfer via VLANs 2, 7, 201, 301, and 302.
Configuring the syslog server	
(config)# **logging host 192.168.255.10**	Specify the IP address of the syslog server.
Configuring the access list for denying access to the DHCP server for the unauthenticated VLAN	
(config)# **ip access-list extended bf_dhcp** (config-ext-nacl)# **deny udp any host 192.169.0.10 eq bootps** (config-ext-nacl)# **permit ip any any**	Define the access list bf_dhcp. This is the list used to deny access to the DHCP server for the unauthenticated VLAN.

(2) Data center access switch: S1 (AX2430S)

S1 (AX2430S) configurations * **These configurations are only to be specified when deploying a network.** (Important point - *(2)*)	
Disabling the spanning-tree	
(config)# **spanning-tree disable**	Disable PVST +, which is enabled by default.
Configuring VLANs	
(config)# **vlan 2,5-6,100,200,300**	Specify the VLANs to be used.
Configuring the physical port interface	
Configuring the access ports used to connect to the server	
(config)# **interface gigabitethernet 0/8** (config-if-range)# **switchport mode access** (config-if-range)# **switchport access vlan 6** (config)# **interface range gigabitethernet 0/9-12** (config-if-range)# **switchport mode access** (config-if-range)# **switchport access vlan 5** (config)# **interface range gigabitethernet 0/13-16** (config-if-range)# **switchport mode access** (config-if-range)# **switchport access vlan 100** (config)# **interface range gigabitethernet 0/17-20** (config-if-range)# **switchport mode access** (config-if-range)# **switchport access vlan 200** (config)# **interface range gigabitethernet 0/21-24** (config-if-range)# **switchport mode access** (config-if-range)# **switchport access vlan 300**	Specify port 0/8 as the VLAN 6 access port used to connect to the unauthenticated environment server. Specify ports 0/9 to 0/12 as the VLAN 5 access port used to connect to the shared server. Specify ports 0/13 to 0/16 as the VLAN 100 access port used to connect to the Engineering Department server. Specify ports 0/17 to 0/20 as the VLAN 200 access port used to connect to the Literature Department server. Specify ports 0/21 to 0/24 as the VLAN 300 access port used to connect to the Science Department server.
Configuring ports for communicating (uplinking) with higher-ranking switches	
(config)# **interface range gigabitethernet 0/1-2** (config-if-range)# **link debounce time 0** (config-if-range)# **channel-group 1 mode on**	Specify ports 0/1 and 0/2 to implement channel group 1, which is used to connect to device C1.
Configuring the port channel	
(config)# **interface port-channel 1** (config-if)# **switchport mode trunk** (config-if)# **switchport trunk allowed vlan 2,5-6,100,200,300**	Specify port channel 1 as the trunk port that allows transfer via VLANs 2, 5, 6, 100, 200, and 300.
Configuring the VLAN interface	
(config)# **interface vlan 2** (config-if)# **ip address 192.168.255.2 255.255.255.0**	Specify the interface IP address for VLAN 2, which is used to administer the system. (Important point - *(4)*)
Configuring the syslog server	
(config)# **logging host 192.168.255.10**	Specify the IP address of the syslog server.

(3) Distribution switch for the Literature/Science Department: A2 (AX2430S)

A2 (AX2430S) configurations * **These configurations are only to be specified when deploying a network.** (Important point - *(2)*)	
Disabling the spanning-tree	
(config)# **spanning-tree disable**	Disable PVST +, which is enabled by default.
Configuring VLANs	
(config)# **vlan 2,7**	Specify the VLANs to be used.
Configuring the MAC VLAN	
(config)# **vlan 201,301-302 mac-based**	Create a MAC VLAN to be used as the authenticated VLAN.
Configuring the physical port interface	
Configuring the access ports for the Literature Department	
(config)# **interface range gigabitethernet 0/5-8** (config-if-range)# **switchport mode mac-vlan** (config-if-range)# **switchport mac vlan 201** (config-if-range)# **switchport mac native vlan 7**	Specify ports 0/5 to 0/8 as the MAC VLAN port. Specify authenticated VLAN 201 as the MAC VLAN port. Specify unauthenticated VLAN 7 as the native VLAN.
Configuring the access ports for the Science Department	
(config)# **interface range gigabitethernet 0/13-16** (config-if-range)# **switchport mode mac-vlan** (config-if-range)# **switchport access vlan 301** (config-if-range)# **switchport mac native vlan 7** (config)# **interface range gigabitethernet 0/17-20** (config-if-range)# **switchport mode mac-vlan** (config-if-range)# **switchport mac vlan 302** (config-if-range)# **switchport mac native vlan 7**	Specify ports 0/13 to 0/16 as a MAC VLAN port. Specify authenticated VLAN 301 as the MAC VLAN port. Specify unauthenticated VLAN 7 as the native VLAN. Specify ports 0/17 to 0/20 as the MAC VLAN port. Specify authenticated VLAN 302 as the MAC VLAN port. Specify unauthenticated VLAN 7 as the native VLAN.
Configuring ports for communicating (uplinking) with higher-ranking switches	
(config)# **interface range gigabitethernet 0/1-2** (config-if-range)# **link debounce time 0** (config-if-range)# **channel-group 1 mode on**	Specify ports 0/1 and 0/2 to implement channel group 1, which is used to connect to device C1.
Configuring the port channel	
(config)# **interface port-channel 1** (config-if)# **switchport mode trunk** (config-if)# **switchport trunk allowed vlan 2,7,201,301-302**	Specify port channel 1 as the trunk port that allows transfer via VLANs 2, 7, 201, 301, and 302.
Configuring the VLAN interface	
(config)# **interface vlan 2** (config-if)# **ip address 192.168.255.6 255.255.255.0** (config)# **interface vlan 7** (config-if)# **ip address 192.168.0.6 255.255.255.0** (config)# **interface vlan 201** (config-if)# **ip address 192.168.21.6 255.255.255.0** (config)# **interface vlan 301** (config-if)# **ip address 192.168.31.6 255.255.255.0** (config)# **interface vlan 302** (config-if)# **ip address 192.168.32.6 255.255.255.0**	Specify the interface IP address for VLAN 2, which is used to administer the system. (Important point - *(4)*) Specify the interface IP address for unauthenticated VLAN 7. Specify the interface IP address for VLAN 201, which is used to connect to the Literature Department. Specify the interface IP address for VLANs 301 and 302, which are used to connect to the Science Department.
Configuring the default route	
(config)# **ip default-gateway 192.168.255.1**	Specify a default route used to communicate with the RADIUS server.
Configuring the RADIUS server	
(config)# **radius-server host 172.16.0.10 key xuniv**	Specify the IP address and key for the RADIUS server. This guide assumes that the key is "xuniv".
Configuring the syslog server	
(config)# **logging host 192.168.255.10** (config)# **logging event-kind aut**	Specify the IP address of the syslog server used for the entire system. Specify "aut" as the event type for log information.

A2 (AX2430S) Web authentication configurations	
Configuring the access lists used for Web authentication	
(config)# **ip access-list extended web-auth** (config-ext-nacl)# **permit udp any any eq bootps** (config-ext-nacl)# **permit udp any any eq domain**	Create the following access lists: - Access list that permits DHCP communication - Access list that permits DNS communication
Configuring the physical port interface	
Configuring access ports	
(config)# **interface range gigabitethernet 0/5-20** (config-if-range)# **web-authentication port** (config-if-range)# **authentication arp-relay** (config-if-range)# **authentication ip access-group web-auth**	Specify ports 0/5 to 0/20 as the Web-authenticated port. When ARP packets for a port other than the one described above are received from the unauthenticated terminal, the packets are output to a non-authenticated port. Apply the access list used for authentication.
Configuring RADIUS	
(config)# **aaa authentication web-authentication default group radius**	Specify user authentication to be performed on the RADIUS server.
Configuring Web authentication	
(config)# **web-authentication ip address 10.10.10.10** (config)# **web-authentication system-auth-control** (config)# **no web-authentication auto-logout** (config)# **web-authentication max-timer 60** (config)# **web-authentication jump-url http://xuniv.org/**	Specify the IP address dedicated to Web authentication. This guide assumes that the address is "10.10.10.10". Enable Web authentication. Disable automatic authentication logout. Specify 60 minutes as the maximum amount of time to remain connected after successful authentication. Specify the URL to be displayed after successful authentication. This guide assumes that “http://xuniv.org/” is the URL displayed.
Configuring the syslog server	
(config)# **web-authentication logging enable**	Output a Web authentication log to the syslog server.

(4) L3 core switch for the first system modification (separating the shared portion, unauthenticated VLAN, and the Engineering Department from the global network): C1 (AX6708S)

C1 (AX6700S) configurations for the first system modification (Important point - (2))	
Configuring VRFs	
(config)# **vrf definition global** (config)# **vrf definition 5** (config)# **vrf definition 6** (config)# **vrf definition 10**	Specify the global network. Specify VRF 5 to be used. Specify VRF 6 to be used. Specify VRF 10 to be used.
Configuring route filters (route-map) used to set up the shared network	
(config)# **route-map GLOBAL_IMPORT permit 10** (config-route-map)# **match vrf 5** (config)# **route-map VRF5_IMPORT permit 10** (config-route-map)# **match vrf global 6 10** (config)# **route-map VRF6_IMPORT permit 10** (config-route-map)# **match vrf 5** (config)# **route-map VRF10_IMPORT permit 10** (config-route-map)# **match vrf 5**	Define a route filter for GLOBAL_IMPORT. Permit all communications to and from VRF 5. Define a route filter for VRF5_IMPORT. Permit all communications to and from the global network, VRF 6, and VRF 10. Define a route filter for VRF6_IMPORT. Permit all communications to and from VRF 5. Define a route filter for VRF10_IMPORT. Permit all communications to and from VRF 5.
Configuring the shared network	
(config)# **vrf definition global** (config-vrf)# **import inter-vrf GLOBAL_IMPORT** (config)# **vrf definition 5** (config-vrf)# **import inter-vrf VRF5_IMPORT** (config)# **vrf definition 6** (config-vrf)# **import inter-vrf VRF6_IMPORT** (config)# **vrf definition 10** (config-vrf)# **import inter-vrf VRF10_IMPORT**	In global-network config mode, define GLOBAL_IMPORT as the route import filter condition. In VRF 5 config mode, define VRF5_IMPORT as the route import filter condition. In VRF 6 config mode, define VRF6_IMPORT as the route import filter condition. In VRF 10 config mode, define VRF10_IMPORT as the route import filter condition.
Configuring the VLAN interface	
Configuring VLANs for VRF 5 (shared network)	When these commands are executed, communication via VLAN 5 stops.
(config)# **interface vlan 5** (config-if)# **no ip address 172.16.0.1** (config-if)# **vrf forwarding 5** (config-if)# **ip address 172.16.0.1 255.255.0.0**	To use VLAN 5 for VRF 5, delete the IP address settings. (Important point - (3)) Specify VLAN 5 to be used for VRF 5. Specify the IP address for VLAN 5 again.
Configuring VLANs for VRF 6 (unauthenticated network)	When these commands are executed, communication via VLAN 6 stops.
(config)# **interface vlan 6** (config-if)# **no ip address 192.169.0.1** (config-if)# **vrf forwarding 6** (config-if)# **ip address 192.169.0.1 255.255.255.0**	To use VLAN 6 for VRF 6, delete the IP address settings. (Important point - (3)) Specify VLAN 6 to be used for VRF6. Specify the IP address for VLAN 6 again.
	When these commands are executed, communication via VLAN 7 stops.
(config)# **interface vlan 7** (config-if)# **no ip helper-address** (config-if)# **no ip address 192.168.0.1** (config-if)# **vrf forwarding 6** (config-if)# **ip address 192.168.0.1 255.255.0.0** (config-if)# **ip helper-address 192.169.0.10**	To use VLAN 7 for VRF 6, delete the IP address settings and the DHCP relay settings. (Important point - (3)) Specify VLAN 7 to be used for VRF 6. Specify the IP address and DHCP relay agent for VLAN 7 again.
Configuring VLANs for VRF 10 (Engineering Department)	When these commands are executed, communication via VLAN 100 stops.
(config)# **interface vlan 100** (config-if)# **no ip address 192.168.100.1** (config-if)# **vrf forwarding 10** (config-if)# **ip address 192.168.100.1 255.255.255.0**	To use VLAN 100 for VRF10, delete the IP address settings. (Important point - (3)) Specify VLAN 100 to be used for VRF 10. Specify the IP address for VLAN 100 again.
(config)# **interface vlan 101** (config-if)# **no ip helper-address** (config-if)# **no ip address 192.168.101.1** (config-if)# **vrf forwarding 10** (config-if)# **ip address 192.168.101.1 255.255.255.0** (config-if)# **ip helper-address 192.168.100.10**	To use VLAN 101 for VRF 10, delete the IP address and DHCP relay settings. (Important point - (3)) Specify VLAN 101 to be used for VRF 10. Specify the IP address and DHCP relay agent for VLAN 101 again.
	When these commands are executed, communication via VLAN 101 stops.

(5) L3 core switch for the second system modification (separating the Literature Department and Science Department from the global network): C1 (AX6708S)

C1 (AX6700S) configurations for the second system modification (Important point - *(2)*)	
Configuring VRFs	
(config)# **vrf definition 20** (config)# **vrf definition 30**	Specify VRF 20 to be used. Specify VRF 30 to be used.
Configuring route filters (route-map) used to set up the shared network	
(config)# **route-map VRF20_IMPORT permit 10** (config-route-map)# **match vrf 5** (config)# **route-map VRF30_IMPORT permit 10** (config-route-map)# **match vrf 5** (config)# **route-map VRF5_IMPORT permit 10** (config-route-map)# **match vrf 20 30**	Define a route filter for VRF20_IMPORT. Permit all communications to and from VRF 5. Define a route filter for VRF30_IMPORT. Permit all communications to and from VRF 5. Add a route filter for VRF5_IMPORT. Permit all communications to and from VRF 20 and VRF 30.
Configuring the shared network	
(config)# **vrf definition 20** (config-vrf)# **import inter-vrf VRF20_IMPORT** (config)# **vrf definition 30** (config-vrf)# **import inter-vrf VRF30_IMPORT**	In VRF 20 config mode, define VRF20_IMPORT as the route import filter condition. In VRF 30 config mode, define VRF30_IMPORT as the route import filter condition.
Configuring the VLAN interface	
Configuring VLANs for VRF 20 (Literature Department)	When these commands are executed, communication via VLAN 200 stops.
(config)# **interface vlan 200** (config-if)# **no ip address 192.168.20.1** (config-if)# **vrf forwarding 20** (config-if)# **ip address 192.168.20.1 255.255.0.0**	To use VLAN 200 for VRF 20, delete the IP address settings. (Important point - *(3)*) Specify VLAN 200 to be used for VRF 20. Specify the IP address for VLAN 200 again.
(config)# **interface vlan 201** (config-if)# **no ip helper-address** (config-if)# **no ip address 192.168.21.1** (config-if)# **vrf forwarding 20** (config-if)# **ip address 192.168.21.1 255.255.0.0** (config-if)# **ip helper-address 192.168.20.10**	To use VLAN 201 for VRF 20, delete the IP address and DHCP relay settings. (Important point - *(3)*) Specify VLAN 201 to be used for VRF 20. Specify the IP address and DHCP relay agent for VLAN 201 again.
Configuring VLANs for VRF 30 (Science Department)	When these commands are executed, communication via VLAN 201 stops.
(config)# **interface vlan 300** (config-if)# **no ip address 192.168.30.1** (config-if)# **vrf forwarding 30** (config-if)# **ip address 192.168.30.1 255.255.255.0**	To use VLAN 300 for VRF 30, delete the IP address settings. (Important point - *(3)*) Specify VLAN 300 to be used for VRF 30. Specify the IP address for VLAN 300 again.
	When these commands are executed, communication via VLAN 300 stops.
(config)# **interface vlan 301** (config-if)# **no ip helper-address** (config-if)# **no ip address 192.168.31.1** (config-if)# **vrf forwarding 30** (config-if)# **ip address 192.168.31.1 255.255.255.0** (config-if)# **ip helper-address 192.168.30.10**	To use VLANs 301 and 302 for VRF 30, delete the IP address and DHCP relay settings. (Important point - *(3)*) Specify VLANs 301 and 302 to be used for VRF 30. Specify the IP address and DHCP relay agent for VLANs 301 and 302 again.
	When these commands are executed, communication via VLAN 301 stops.
(config)# **interface vlan 302** (config-if)# **no ip helper-address** (config-if)# **no ip address 192.168.32.1** (config-if)# **vrf forwarding 30** (config-if)# **ip address 192.168.32.1 255.255.255.0** (config-if)# **ip helper-address 192.168.30.10**	When these commands are executed, communication via VLAN 302 stops.

5. Integrating Networks

This chapter provides an example that describes how to integrate multiple networks. In addition, it also provides specific information about how to configure the network devices.

5.1 Background and system requirements

Assume that a building is now under construction and that one office (A) and its partner company (C) and affiliate company (B) will all move into the building when it is completed. The employees of each are all using PCs and servers at their current work places. To avoid long-term suspension of business operations, A, C, and B wish to continue using their PCs and servers as they work at the new site, without having to change their respective configurations. Office A and its partner company C often work together on the same projects, so their employees want to work on the same floor. Because each of these companies will move to the same place, the information system managers want to use as few devices and materials as possible to manage the system.

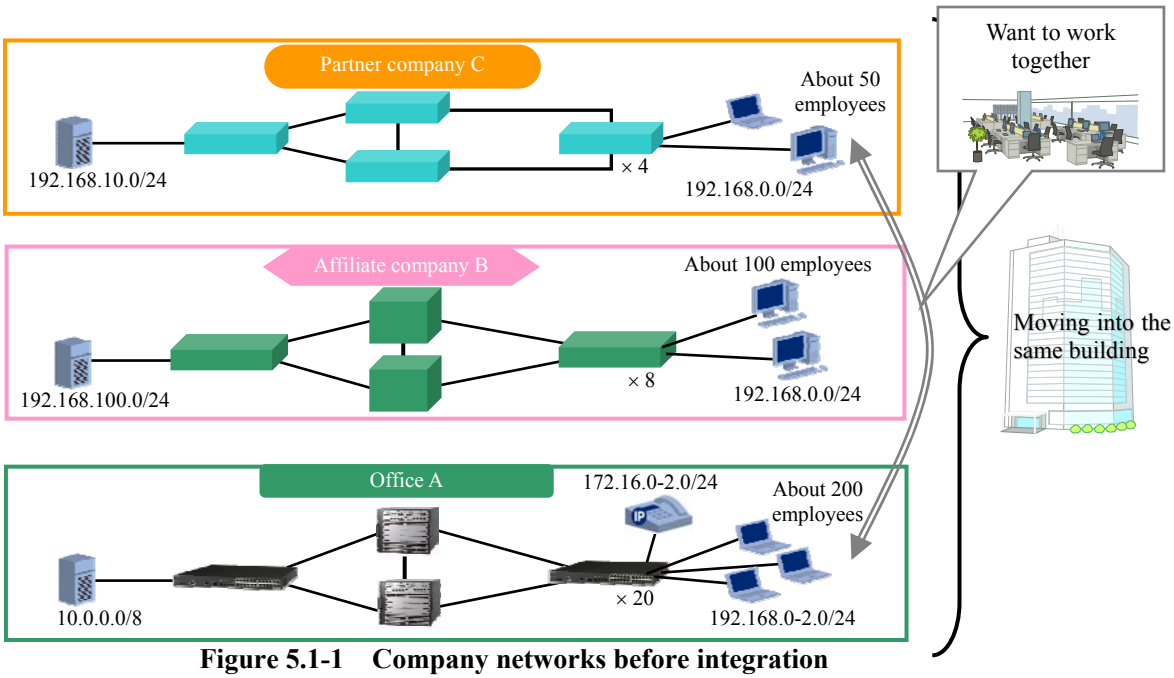


Figure 5.1-1 Company networks before integration

To satisfy these requirements, these companies have decided to implement network partition. This solution enables each company to establish a separate network while sharing the same infrastructure in the new building. For distribution and access switches, each company will use its own resources. In addition, they decided to use IP phones as the in-building phones and to incorporate them into the new system.

5.2 System design guidelines

This section lists some points to consider for system design, based on the example in this chapter.

(1) Make sure the VRF device can handle all the resources for the integrated network

The total number and capacity of the terminal and other devices for the networks before integration is assumed to be the number and transfer capacity of the terminal and other devices connected to the integrated system. The total number of devices and the capacity of the integrated system are not to exceed the limits of the core switches.

(2) The same IP addresses can be used as long as a shared network (or an extranet) is not created

Because independent networks are integrated, their IP addresses might be the same. When a network partition is used to integrate networks, we recommend that you avoid deploying a shared network or an extranet. This will allow the same IP address to be used.

(3) Efficiently use resource limitations

When there is an approximate number of devices for the system, such as IP phones, or when the number of devices is limited, we recommend that you limit the usage of the resources. Doing so prevents unnecessary communication from occupying resources, thereby making them more available for use by other networks.

(4) When administering or monitoring the devices of a logical network, specify an address for the VLAN of that network

To monitor or administer devices in a logical network, including those in the global network, you must assign an IP address to at least one of the VLANs that belong to the logical network. To collect syslog or SNMP information through a logical network, you must specify the monitoring server for that logical network. Note that some of the operation and management functions of a VRF device can only be used for communication through the global network. (For details, see *2.4 Operation management and the global network*.)

To operate, manage, and monitor devices, use a single network for the global network or each of the logical networks to perform transmissions without L3 relay (within the same subnet). As a result, an AX2400S series or AX1200S series L2 switch is able to remotely manage devices by using syslog or SNMP without needing to set up the gateway. However, make sure that you avoid using the same administration IP address if there is a distribution/access switch handling multiple networks, such as device D2F in the sample system described in the next section, and if monitoring is performed from each network.

5.3 System configuration example

To use a network partition for the sample system below, you must replace the core switch with an AX6000S series device. If this system is a fault-tolerant network, the L2 switch at the access edge can be the device currently used in the existing network. (This device must be able to support link aggregation.)

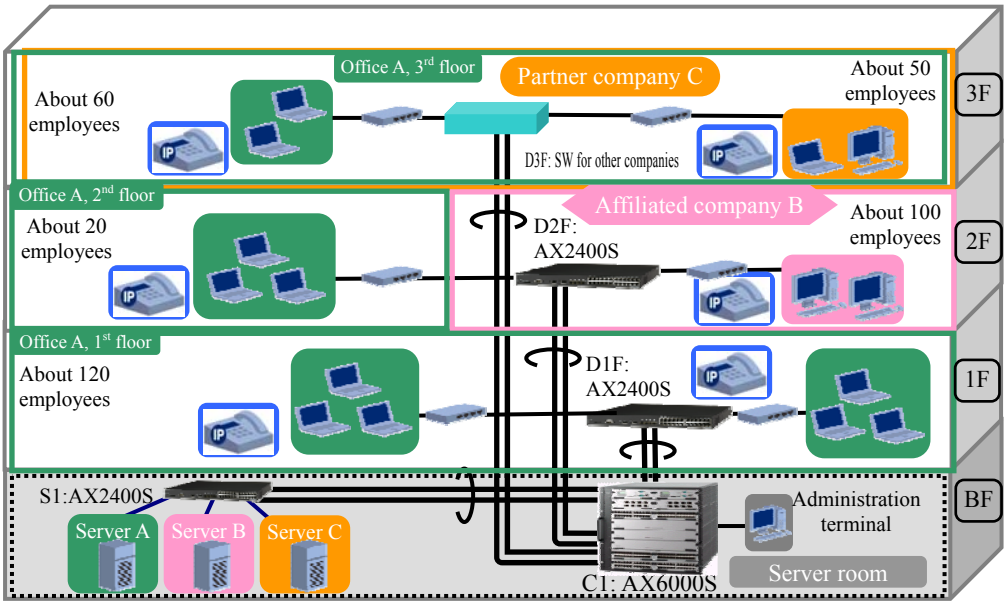


Figure 5.3-1 System integrating the company networks

Install the AX6700S as the core device, and use a network partition for the fault-tolerant network that uses link aggregation. There is no need to modify the access switches used in the departments when introducing the switches into the system. (These switches must be able to support link aggregation.)

By moving all the servers owned by each company to the common data center on the basement floor, the management of backup and other operations is centralized. At the same time, using a network partition maintains the functions of the dedicated servers used by each company. On the other hand, by newly installing a special partition for in-building IP phones, the functions of these phones are unified.

The logical configuration of the system is shown below.

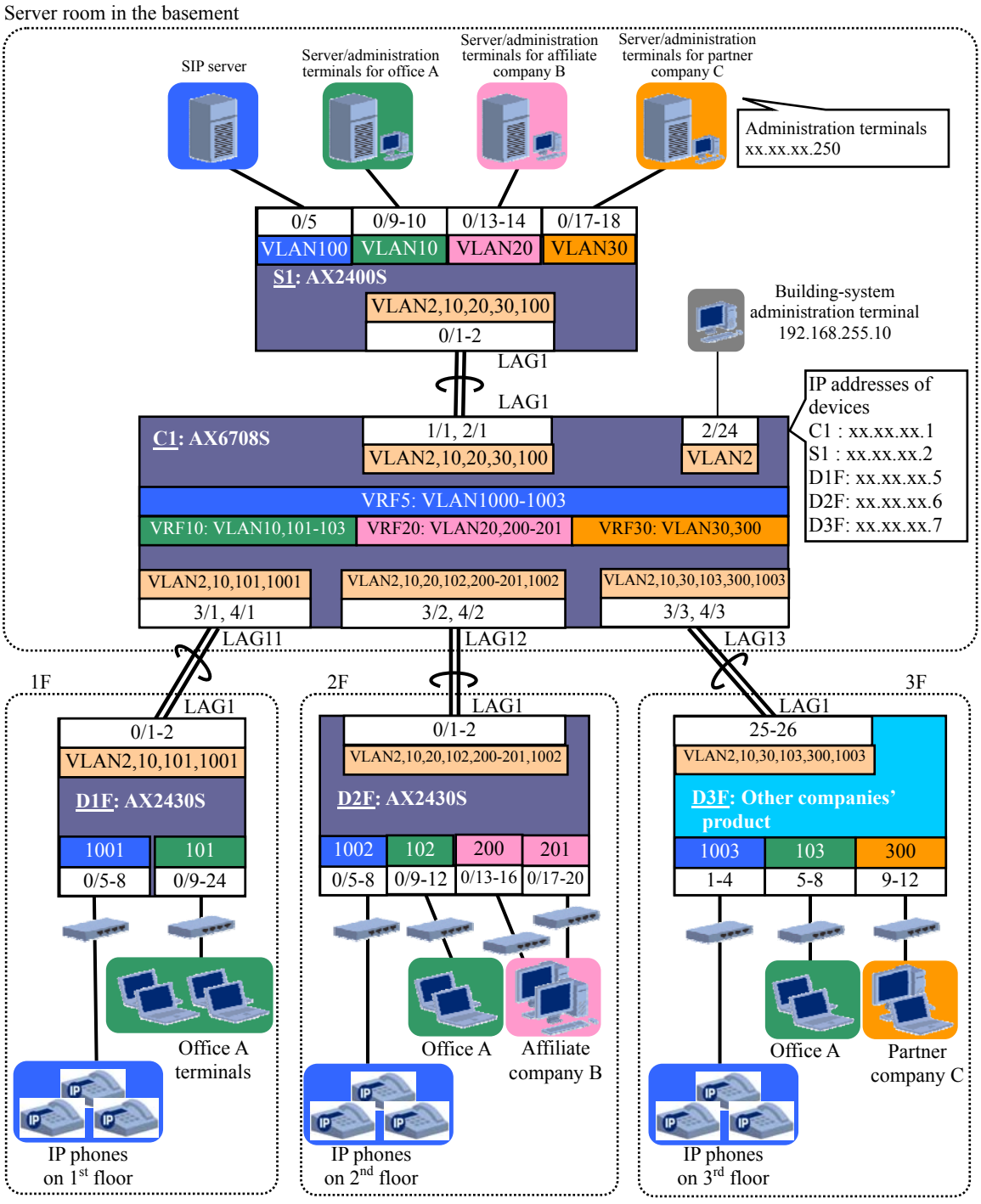


Figure 5.3-2 Logical configuration

The table below shows the definitions of the partitions and VLANs.

Table 5.3-1 VRF/VLAN definitions

Partition name	VRF ID	VLAN name	VLAN ID	IP address	Application
Administration	Global	Administration	2	192.168.255.0/24	Overall network administration
Intra-building IP phones	5	IP phone server	1000	172.16.0.0/24	Basement floor telephone/SIP server
		1st floor IP phones	1001	172.16.1.0/24	1st floor telephones (up to 150 units)
		2nd floor IP phones	1002	172.16.2.0/24	2nd floor telephones (up to 150 units)
		3rd floor IP phones	1003	172.16.3.0/24	3rd floor telephones (up to 150 units)
Office A	10	Server	10	10.0.0.0/8	Company A server for operation management
		1st floor client	101	192.168.0.0/24	Terminal
		2nd floor client	102	192.168.1.0/24	
		3rd floor client	103	192.168.2.0/24	
Affiliate company B	20	Server	20	192.168.100.0/24	Company B server for operation management
		Client 1	200	192.168.0.0/24	Terminal
		Client 2	201	192.168.1.0/24	
Partner company C	30	Server	30	192.168.10.0/24	Company C server for operation management
		Client	300	192.168.0.0/24	Terminal

There is a single partition for each company, plus an extra partition for IP phones. Because no shared network is deployed, the existing IP address for the respective partition assigned to each company will be used as is.

The IP phone network (VRF 5) will only be used for IP phones. It is assumed that there will be no significant change in the number of IP phones. Thus, to suppress the influence of improper connections or unexpected usage of facilities on other networks, the respective number of MAC address entries and ARP entries must be limited as follows:.

There will be about 120 employees on each floor, with one IP phone available to each person. Thus, the total number of IP phones to be installed on each floor is:

120 IP phones/floor

A total of four floors will be used, including the basement level. Thus, the total number of IP phones required is:

$120 \times 4 = 450$ IP phones

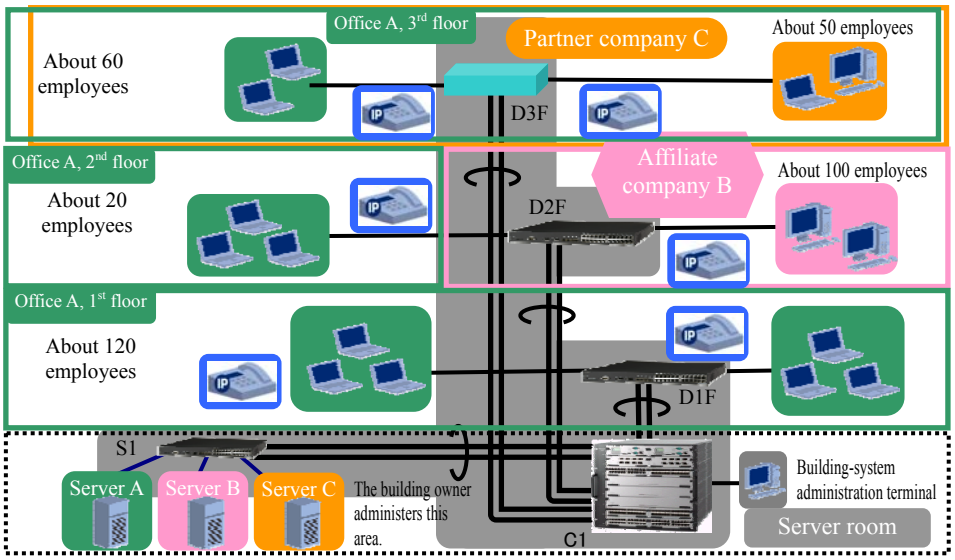
Considering the additional IP phones for the SIP server and underground server room, the limits on the number of MAC address entries and ARP entries are as follows:

Maximum number of MAC address entries = 150 for each VLAN
Maximum number of ARP entries = 600 for the IP phone network (VRF 5)

5.4 Operation management

Monitoring the entire system in the new building is made possible by expanding the global network to include the access edge devices. Because the global network is used, the core device can use all operation and management functions.

Each company must be able to operate and administer its own network. In this case, the functions provided by the core device are limited to those supported by VRF (such as SNMP, ping, and traceroute). If an address can be specified for a VLAN, the distribution and access edge devices can be operated and administered from the logical network to which the VLAN belongs. If devices are administered from multiple networks (including the global network), make sure that you avoid assigning the same IP administration address to different devices, as described *System design guidelines (4)* .



Monitored network	Monitored device	Information collected (information in parentheses is visible)	Collection route
System for the entire building (Global)	C1	Global, VRF5, VRF10, VRF20, VRF30	Global network
	S1	VRF5, VRF10, VRF20, VRF30	
	D1F	VRF10	
	D2F	VRF10, VRF20	
	D3F	VRF10, VRF30	
Office A (VRF10)	C1#1	VRF10 (Global, VRF5, VRF20, VRF30)	VRF10 network
	S1	VRF10 (VRF5, VRF20, VRF30)	
	D1F	VRF10 (VRF5)	
	D2F	VRF10 (VRF5, VRF20)	
	D3F	VRF10 (VRF5, VRF30)	
Affiliate company B (VRF20)	C1#1	VRF20 (Global, VRF5, VRF10, VRF30)	VRF20 network
	S1	VRF20 (VRF5, VRF10, VRF30)	
	D2F	VRF20 (VRF5, VRF20)	
Partner company C (VRF30)	C1#1	VRF30 (Global, VRF5, VRF10, VRF20)	VRF30 network
	S1	VRF30 (VRF5, VRF10, VRF20)	
	D3F	VRF30 (VRF5, VRF10)	

#1 Only provides the functions supported by VRF (such as SNMP, ping, and traceroute).

Figure 5.4-1 System operation management

5.5 Points for configuring devices

This section lists some points for configuring the devices used in the system.

(1) Specify the MAC address table limit for each VLAN and the ARP table limit for each VRF

To limit the resources for each network, specify the ARP table limit for each VRF. If necessary, specify the MAC address table limit for each VLAN that belongs to that network.

(2) Specify an IP address for the VLAN that belongs to the administration network

To remotely operate and administer devices, assign an IP address (for administering the devices) to the VLAN that belongs to the administration network.

(3) See *[Basic]* for the VRF settings guideline

For details about how to configure the VRF settings, see the ***AX Series Network Partition: Solution Guide [Basic]***. Below are excerpts from ***3.1.1. Important points in the configuration*** in ***3.1 Network partitions in an FT network*** of the guide above. These excerpts contain information related to the sample system described here.

- **Points for configuring the FT network**

(2) Disable spanning trees
(3) Activate VRF in a mode where no L2 protocol is enabled at the same time
(4) Assign VLANs to the partitions (VRF)
(6) Remote control must be via the global network

5.6 Sample configurations

This section provides examples of key configurations for implementing the core switch and distribution devices in the system. See the *Appendix* for details about the device configurations.

(1) L3 core switch: C1 (AX6708S)

C1 (AX6708S) configurations	
Disabling the spanning-tree	
(config)# **spanning-tree disable**	Disable PVST+, which is enabled by default. (Important point - *[Basic](2)*)
Configuring VRFs	
(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 (config)# **vrf definition 5** (config-vrf)# **arp-limit 600** (config)# **vrf definition 10** (config)# **vrf definition 20** (config)# **vrf definition 30**	Configure the VRF without using the L2 protocol. (Important point - *[Basic](3)*) (You are prompted to restart the BSU. Enter y to restart.) Specify VRF 5 to be used. Specify 600 as the maximum number of ARP entries for VRF 5. (Important point - *(1)*) Specify VRF 10 to be used. Specify VRF 20 to be used. Specify VRF 30 to be used.
Configuring VLANs	
(config)# **vlan 2,10,20,30,101-103,200-201,300,1000-1003**	Specify the VLANs to be used.
Configuring the maximum number of MAC addresses to be learned	
(config)# **mac-address-table limit vlan 1000 maximum 150** (config)# **mac-address-table limit vlan 1001 maximum 150** (config)# **mac-address-table limit vlan 1002 maximum 150** (config)# **mac-address-table limit vlan 1003 maximum 150**	Specify 150 as the maximum number of MAC addresses learned by VLANs 1000 to 1003. (Important point - *(1)*)
Configuring the VLAN interface	
Configuring VLANs for the global network	
(config)# **interface vlan 2** (config-if)# **ip address 192.168.255.1 255.255.255.0**	Specify VLAN 2 to be used in the global network for system administration. (Important point - *[Basic](6)*) Specify the IP address for VLAN 2. (Important point - *(2)*)
Configuring VLANs for VRF 10 (office A)	
(config)# **interface vlan 10** (config-if)# **vrf forwarding 10** (config-if)# **ip address 10.0.0.1 255.0.0.0** (config)# **interface vlan 101** (config-if)# **vrf forwarding 10** (config-if)# **ip address 192.168.0.1 255.255.255.0** (config)# **interface vlan 102** (config-if)# **vrf forwarding 10** (config-if)# **ip address 192.168.1.1 255.255.255.0** (config)# **interface vlan 103** (config-if)# **vrf forwarding 10** (config-if)# **ip address 192.168.2.1 255.255.255.0**	Use VLAN 10 for VRF10. (Important point - *[Basic](4)*) Specify the IP address for VLAN 10. Use VLAN 101 for VRF 10. (Important point - *[Basic](4)*) Specify the IP address for VLAN 101. Use VLAN 102 for VRF 10. (Important point - *[Basic](4)*) Specify the IP address for VLAN 102. Use VLAN 103 for VRF 10. (Important point - *[Basic](4)*) Specify the IP address for VLAN 103.
Configuring VLANs for VRF 20 (affiliate company B)	
(config)# **interface vlan 20** (config-if)# **vrf forwarding 20** (config-if)# **ip address 192.168.100.1 255.255.255.0** (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 VLAN 20 for VRF 20. (Important point - *[Basic](4)*) Specify the IP address for VLAN 20. Use VLAN 200 for VRF 20. (Important point - *[Basic](4)*) Specify the IP address for VLAN 200. Use VLAN 201 for VRF 20. (Important point - *[Basic](4)*) Specify the IP address for VLAN 201.
Configuring VLANs for VRF 30 (partner company C)	

C1 (AX6708S) configurations	
(config)# **interface vlan 30** (config-if)# **vrf forwarding 30** (config-if)# **ip address 192.168.10.1 255.255.255.0** (config)# **interface vlan 300** (config-if)# **vrf forwarding 30** (config-if)# **ip address 192.168.0.1 255.255.255.0**	Use VLAN 30 for VRF 30. (Important point - *[Basic](4)*) Specify the IP address for VLAN 30. Use VLAN 300 for VRF 30. (Important point - *[Basic](4)*) Specify the IP address for VLAN 300.
Configuring VLANs for VRF 5 (intra-building IP phones)	
(config)# **interface vlan 1000** (config-if)# **vrf forwarding 5** (config-if)# **ip address 172.16.0.1 255.255.255.0** (config)# **interface vlan 1001** (config-if)# **vrf forwarding 5** (config-if)# **ip address 172.16.1.1 255.255.255.0** (config)# **interface vlan 1002** (config-if)# **vrf forwarding 5** (config-if)# **ip address 172.16.2.1 255.255.255.0** (config)# **interface vlan 1003** (config-if)# **vrf forwarding 5** (config-if)# **ip address 172.16.3.1 255.255.255.0**	Use VLAN 1000 for VRF 5. (Important point - *[Basic](4)*) Specify the IP address for VLAN 1000. Use VLAN 1001 for VRF 5. (Important point - *[Basic](4)*) Specify the IP address for VLAN 1001. Use VLAN 1002 for VRF 5. (Important point - *[Basic](4)*) Specify the IP address for VLAN 1002. Use VLAN 1003 for VRF 5. (Important point - *[Basic](4)*) Specify the IP address for VLAN 1003.
Configuring the physical port interface	
Configuring ports	
(config)# **interface gigabitethernet 2/24** (config-if)# **switchport access vlan 2** (config)# **interface range gigabitethernet 1/1, gigabitethernet 2/1** (config-if-range)# **link debounce time 0** (config-if-range)# **channel-group 1 mode on** (config)# **interface range gigabitethernet 3/1, gigabitethernet 4/1** (config-if-range)# **link debounce time 0** (config-if-range)# **channel-group 11 mode on** (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**	Specify port 2/24 as the VLAN 2 access port used for system administration. Specify ports 1/1 and 2/1 to implement channel group 1, which is used to connect to device S1. Specify ports 3/1 and 4/1 to implement channel group 11, which is used to connect to device D1F. Specify ports 3/2 and 4/2 to implement channel group 12, which is used to connect to device D2F. Specify ports 3/3 and 4/3 to implement channel group 13, which is used to connect to device D3F.
Configuring the port channels	
(config)# **interface port-channel 1** (config-if)# **switchport mode trunk** (config-if)# **switchport trunk allowed vlan 2,10,20,30,1000** (config)# **interface port-channel 11** (config-if)# **switchport mode trunk** (config-if)# **switchport trunk allowed vlan 2,10,101,1001** (config)# **interface port-channel 12** (config-if)# **switchport mode trunk** (config-if)# **switchport trunk allowed vlan 2,10,20,102,200-201,1002** (config)# **interface port-channel 13** (config-if)# **switchport mode trunk** (config-if)# **switchport trunk allowed vlan 2,10,30,103,300,1003**	Specify port channel 1 as the trunk port that allows transfer via VLANs 2, 10, 20, 30, and 1000. Specify port channel 11 as the trunk port that allows transfer via VLANs 2, 10, 101, and 1001. Specify port channel 12 as the trunk port that allows transfer via VLANs 2, 10, 20, 102, 200, 201, and 1002. Specify port channel 13 as the trunk port that allows transfer via VLANs 2, 10, 30, 103, 300, and 1003.
Configuring the syslog server	
(config)# **logging host 192.168.255.10**	Specify the IP address of the syslog server. (Important point - *[Basic](6)*)

(2) Distribution switch: D1F (AX2430S)

D1F (AX2430S) configurations	
Disabling the spanning-tree	
(config)# **spanning-tree disable**	Disable PVST+, which is enabled by default.
Configuring VLANs	
(config)# **vlan 2,10,101,1001**	Specify the VLANs to be used.
Configuring the physical port interface	
Configuring the access ports	
(config)# **interface range gigabitethernet 0/5-8** (config-if-range)# **switchport mode access** (config-if-range)# **switchport access vlan 1001** (config)# **interface range gigabitethernet 0/9-24** (config-if-range)# **switchport mode access** (config-if-range)# **switchport access vlan 101**	Specify ports 0/5 to 0/8 as the VLAN 1001 access ports. Specify ports 0/9 to 0/24 as the VLAN 101 access ports.
Configuring ports for communicating (uplinking) with higher-ranking switches	
(config)# **interface range gigabitethernet 0/1-2** (config-if-range)# **link debounce time 0** (config-if-range)# **channel-group 1 mode on**	Specify ports 0/1 and 0/2 to implement channel group 1, which is used to connect to device C1.
Configuring the port channel	
(config)# **interface port-channel 1** (config-if)# **switchport mode trunk** (config-if)# **switchport trunk allowed vlan 2,101,1001**	Specify port channel 1 as the trunk port that allows transfer via VLANs 2, 101, and 1001.
Configuring the VLAN interface	
(config)# **interface vlan 2** (config-if)# **ip address 192.168.255.5 255.255.255.0** (config)# **interface vlan 10** (config-if)# **ip address 10.0.0.5 255.0.0.0**	Specify the IP address for VLAN 2, which is used to administer the building system. (Important point - *(2)*) Specify the IP address for VLAN 10, which is used to administer the office A network. (Important point - *(2)*)
Configuring the syslog servers	
(config)# **logging host 192.168.255.10** (config)# **logging host 10.0.0.250**	Specify the IP address of the syslog server used to administer the building system. Specify the IP address of the syslog server used to administer the office A network.

6. *Other reference examples*

This chapter introduces simple examples of systems implemented by using a network partition.

6.1 Adding VRFs for a ring network

To expand the system, you can use the ring protocol to increase the number of access devices in the system. However, the maximum number of logical networks (VRFs) is 63. If you want to have more than 63 VRFs, you must install additional devices, such as those shown below. In this case, however, there can be no more than 4,095 VLANs available for the entire system.

(1) Ring protocol installed

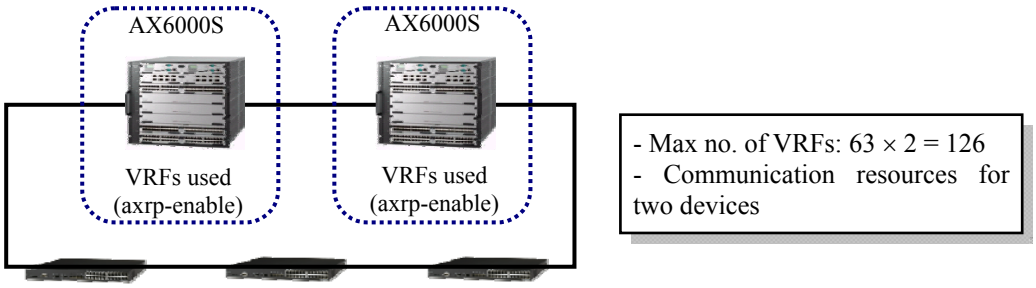


Figure 6.1-1 System with two VRF devices installed

You can double the number of available VRFs simply by installing an additional VRF device.

(2) Ring network separated from the system

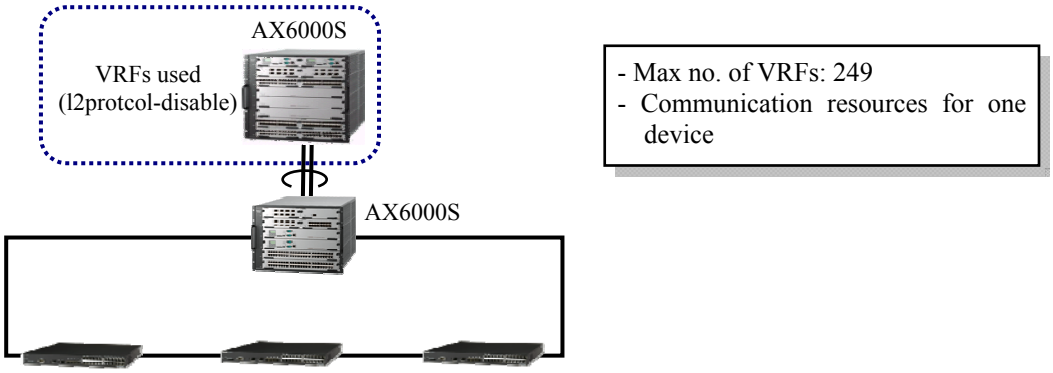


Figure 6.1-2 Ring separated from the system

In this system, the VRF device does not need to run the ring protocol. Although there is only one VRF device, up to 249 VRFs can be supported.

6.2 Using a network partition to integrate a DMZ into the system

In most cases there is a segment between internal networks and external networks, such as the Internet. This segment is called the Demilitarized Zone (DMZ). It is made up of Web servers, email servers, and DNS servers that are used to disclose information to the public. This segment can be deployed in a simple, straightforward manner using the shared network that is deployed by the network partition.

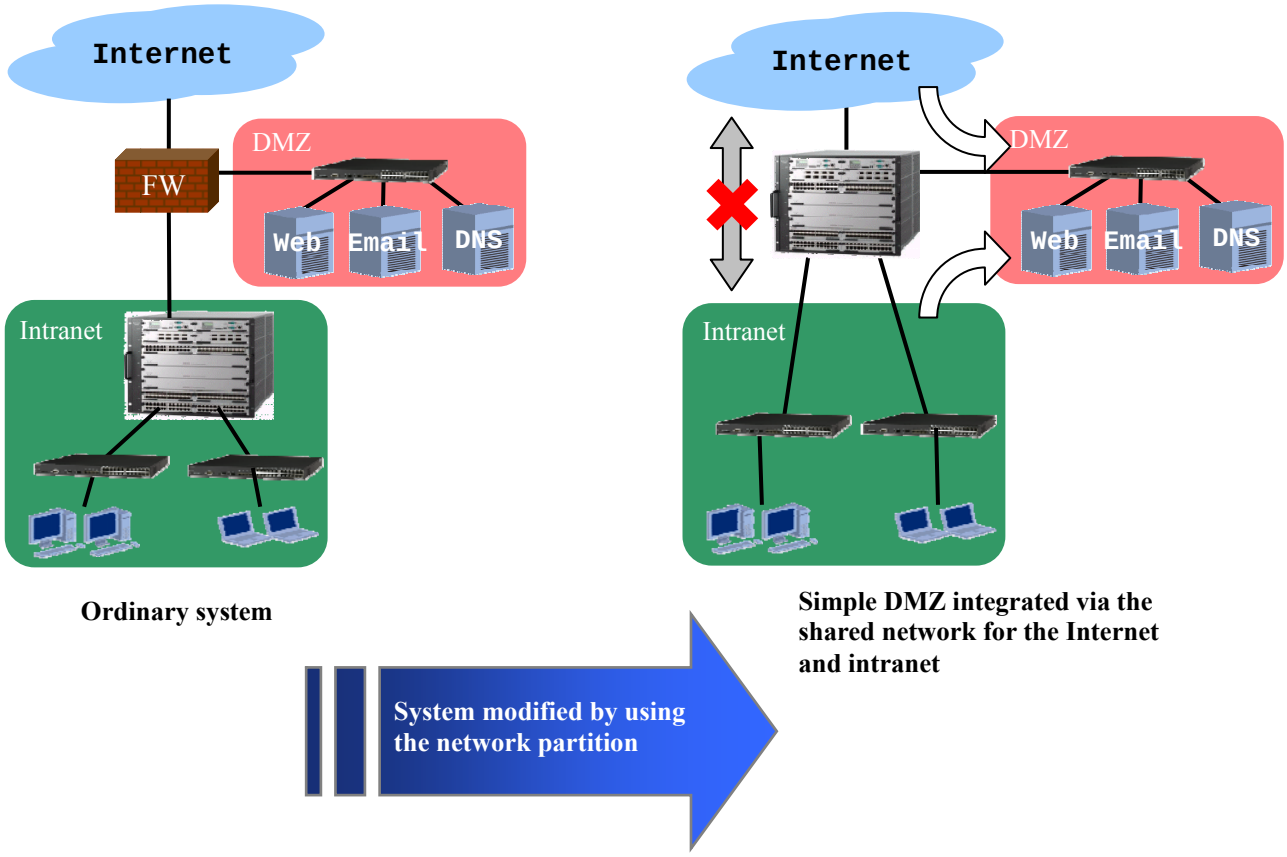


Figure 6.2-1 Using the network partition to integrate a DMZ into the system

If firewall or NAT functions are needed, make sure that you also deploy dedicated devices for these functions. As described in the figure above, using a network partition makes it possible to integrate a DMZ into the system.

7. Other Considerations

(1) Using multiple VRF devices does not cause the total number of VLANs to change

Regardless of whether the system contains one or several VRF devices for a larger number of VRFs (as described in *6.1 Adding VRFs for a ring network*), the range of VLAN IDs (2 to 4,095) available for each VRF device is the same. The VRF devices share the VLANs that are assigned VLAN IDs within that range.

(2) Watch out for routing loops when using a shared network made up of VRF devices

If you are using a shared network made up of multiple VRF devices, routing loops might occur in the network. You can prevent these loops from occurring by adding route filtering conditions.

Appendix: Configuration Files

The files that contain the configurations described in this guide are listed below.
In addition, there are also text files attached to this guide. These files contain all the configurations that apply to the AX series devices for the networks covered in *Chapter 3* through *Chapter 5*. (Adobe Acrobat 5.0 or later or Adobe Reader 6.0 or later is needed to view these files.)
For details about the configurations, see the corresponding files listed below.

3. Configuring a Self-Managed VPN

Device to be specified	Device name (related series)	Corresponding file
L3 core switch	CORE (AX6304S)	`3-MVPN-NP_CORE.txt`
Access point in Division A	AP-A (AX2430S-24X2)	`3-MVPN-NP_AP-A.txt`
Access point in Division B	AP-B (AX2430S-24X2)	`3-MVPN-NP_AP-B.txt`
Access point in Division C	AP-C (AX2430S-24X2)	`3-MVPN-NP_AP-C.txt`
Access point in Division D	AP-D (AX2430S-24X2)	`3-MVPN-NP_AP-D.txt`

4. Seperating Networks

Device to be specified		Device name (related series)	Corresponding file
L3 core switch	For system deployment	C1 (AX6708S)	`4-SEP-NP_C1_0.txt`
	For the first system modification		`4-SEP-NP_C1_0to1.txt`#1
			`4-SEP-NP_C1_1.txt`#2
	For the second system modification		`4-SEP-NP_C1_1to2.txt`#1
			`4-SEP-NP_C1_2.txt`#2
Access switch for the university data center#3		S1 (AX2430S-24)	`4-SEP-NP_S1.txt`
Distribution switch for the Engineering Department#3		A1 (AX2430S-24)	`4-SEP-NP_A1.txt`
Distribution switch for the Literature/Science Department#3		A2 (AX2430S-24)	`4-SEP-NP_A2.txt`

#1 File to which information is copied and pasted by using global config input mode.
#2 File that contains the complete configurations after system modification (i.e., a file which can be viewed by using show running-config after system modification).
#3 Configurations for devices (excluding the L3 core switch) do not need to be changed for the first or second system modification.

5. Integrating Networks

Device to be specified	Device name (related series)	Corresponding file
L3 core switch	C1 (AX6708S)	`5-INT-NP_C1.txt`
Access switch in the underground server room	S1 (AX2430S-24)	`5-INT-NP_S1.txt`
Distribution switch on the 1st floor	D1F (AX2430S-24)	`5-INT-NP_D1F.txt`
Distribution switch on the 2nd floor	D2F (AX2430S-24)	`5-INT-NP_D2F.txt`

This page has intentionally been left blank.

Edition 1 – May 21, 2009

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