The Guaranteed Network

Closer to you, Further into the future.

AX Series
Surveillance Camera Network: Solution Guide

Edition 1

Document No. NTS-11-R-050

ALAXALA Networks Corporation

Preface

This manual provides system engineers with basic technical information for integrating network systems mainly for surveillance cameras (hereinafter the "surveillance camera network") using multicast routing, by taking advantage of the functionalities of the AX series of ALAXALA Networks Corporation. This information helps system engineers to understand overall operation, build systems, and ensure stable operation.

Related documents

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

Notes on using this document

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

AX6600S	Ver. 11.7
AX2430S	Ver. 11.7
AX1240S	Ver. 2.3

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

Export restrictions

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

Trademarks

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

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

Revision history

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

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

Contents

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

1. Networks Systems for Surveillance Cameras

1.1 Network systems that support security

In recent years, surveillance cameras are increasingly being installed at important locations to observe events directly in order to prevent crimes and accidents. The targets of surveillance are also expanding in size and scope, from individual buildings to entire organizations containing such buildings—even to entire regions.

Footage taken by surveillance cameras placed at various locations is used for real-time monitoring and also needs to be archived. Video data is usually collectively stored on an online server, because it is inefficient to store data on separate cameras. Thus, a security surveillance system also requires a highly functional and stable network system

ALAXALA provides highly functional and stable network systems for surveillance cameras through its various advanced technologies and expertise.

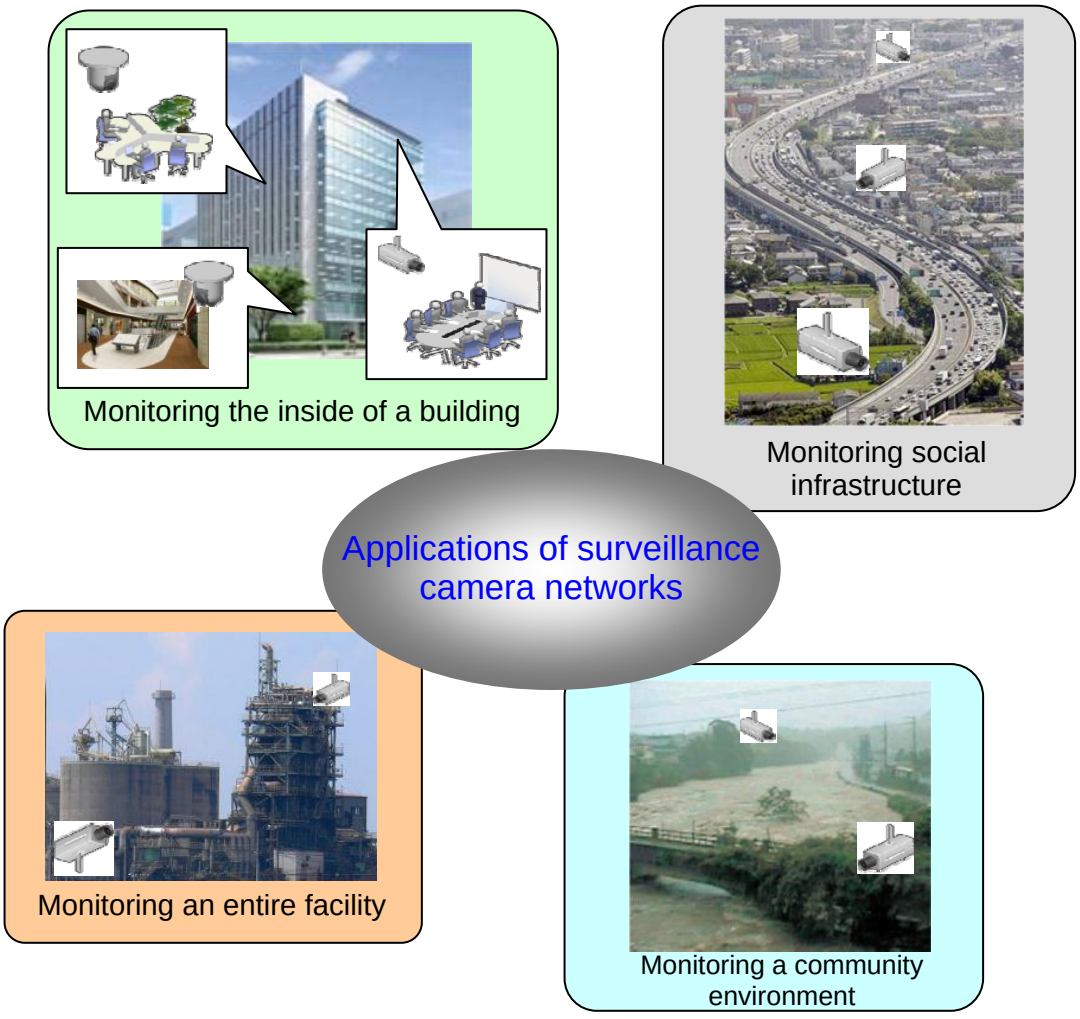


Figure 1.1-1: Applications of surveillance camera networks

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

1.2 Example applications of surveillance camera networks

1.2.1 Building surveillance systems

Surveillance cameras can serve in the place of human eyes for various applications, including the security surveillance of rooms within office buildings, 24/7 support of hospital patients, and monitoring physically inaccessible areas in factories. Even for a single building, dozens of cameras can be necessary to monitor all the rooms. The most common practice is to integrate a network to accommodate all such cameras.

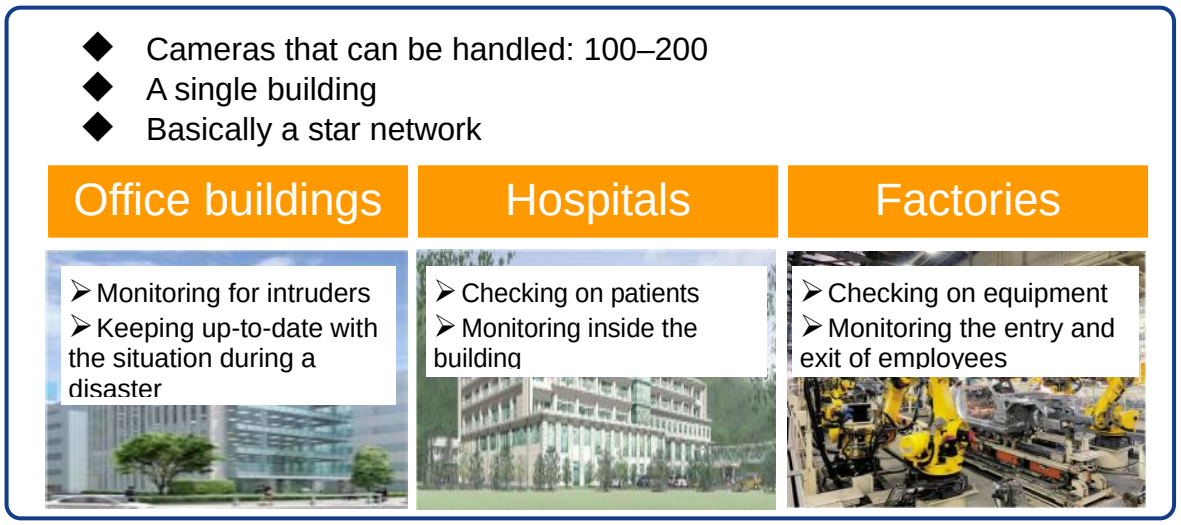


Figure 1.2-1: Applications in buildings and general facilities

1.2.2 Surveillance systems of large-scale facilities

Surveillance cameras play a significant role in monitoring various locations within large-scale facilities such as large shopping centers that house multiple stores, airports, and theme parks. Many more cameras are still necessary to extensively cover entire areas within a facility, so surveillance networks also require greater capacity limits and stability.

Figure 1.2-2: Applications in large-scale facilities

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

1.2.3 Surveillance system of wider areas and regions

It is now also common to use surveillance cameras to better understand situations remotely, for example in important social infrastructure and public facilities such as railways, roads, rivers, and dams, as well as to manage community environments. In addition to the large numbers of cameras necessary to cover extensive areas, it is imperative to be able to easily integrate a reliable wide-area network.

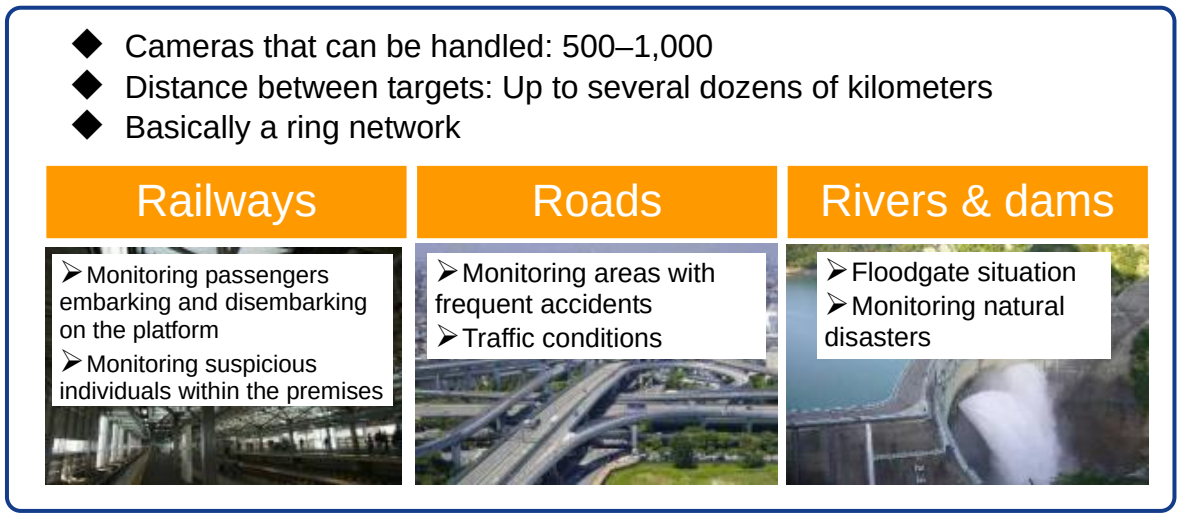


Figure 1.2-3: Applications in wide-area monitoring systems

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

2. Capabilities That Support Surveillance Camera Networks

The main capabilities of the AX series, which can support surveillance camera networks, are explained below.

2.1 Fault-tolerant network: A highly reliable technology that ensures stable and continuous distribution

Surveillance cameras must be able to monitor continuously for long periods, which means that surveillance camera networks must also be highly reliable, continuously functioning systems.

ALAXALA's AX series incorporates high-reliability technologies and capabilities that support non-stop networks, which are represented by the fault-tolerant network.

- Simple protocol-less network
- The route switching time of the highly reliable FT switches is as short as 50 ms.

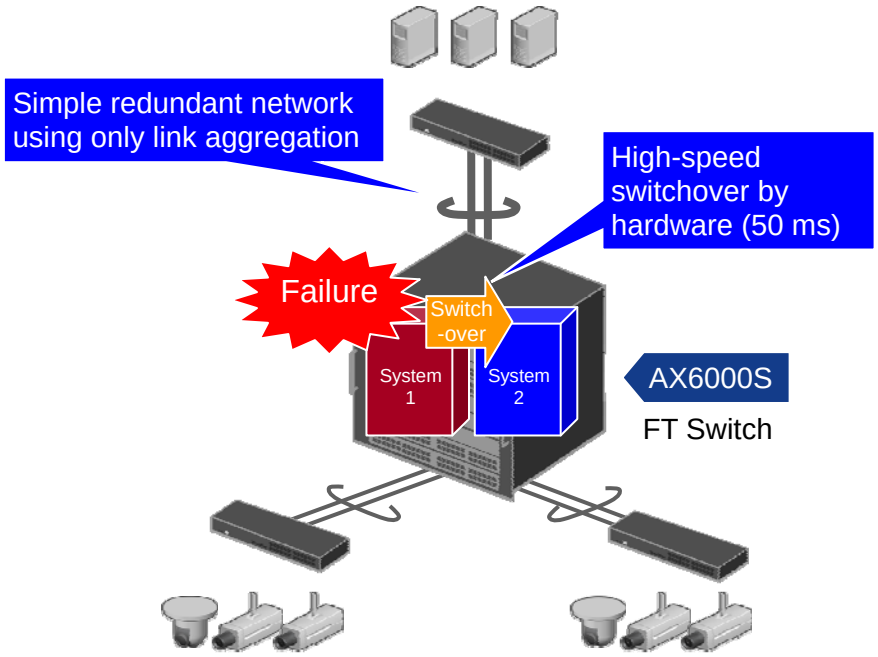


Figure 2.1-1: Fault-tolerant network

By using the AX6000S family, which delivers high-speed and stable switchovers of operation systems through hardware, as a core switch, and combining the lines using a link aggregation connection, you can integrate a highly available, operable, and protocol-less network.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

2.2 Multicasts that efficiently connect and manage many cameras

A surveillance camera system typically handles dozens to several hundreds of cameras, depending on the size of the monitored facility. Therefore, the ability to efficiently handle enough terminal devices (that is, surveillance cameras) is another important requirement of switches that constitute a surveillance camera network.

The receiving side of the footage sent from surveillance cameras usually has multiple servers that record the video data and multiple monitoring PCs for viewing the video, and when the scope of the monitoring target is extensive, the data might be recorded and monitored at several sites.

This is why the larger the surveillance camera system, the more the system tends to employ multicast routing to deliver data. This means that to integrate a surveillance camera network, it is imperative to be able to build a multicast network with a high capacity limit.

The multicast routing supported by ALAXALA's AX series not only supports both IPv4 and IPv6, but can also handle thousands of terminals.

Table 2.2-1: Supported capabilities and capacity limits for multicasts

Supported capabilities and capacity limit		Chassis-type switch[#1]	Box-type switches				
		AX6000S	AX3800S	AX3600S	AX2500S	AX2400S	AX1200S
Multicast group management							
	IGMP	○ v2/v3	○ v2/v3	○ v2/v3	--	--	--
	MLD	○ v1/v2	○ v1/v2	○ v1/v2	--	--	--
	Number of IGMP groups	2000 Standard 3000 Extended	256	256	--	--	--
	Number of MLD groups	256 Standard 256 Extended	256	256			
Multicast routing protocol							
	Supported protocols	PIM-SM/ PIM-SSM/ PIM-DM[#2]	PIM-SM/ PIM-SSM	PIM-SM/ PIM-SSM	--	--	--
	Maximum routes (IPv4)	4000 Standard 8000 Extended	1024	1024	--	--	--
	Maximum routes (IPv6)	1000 Standard 8000 Extended	128	128[#3]/ 768[#4]	--	--	--
Layer 2 multicast cooperation functions							
	IGMP snooping	○ v1/v2/v3	○ v1/v2/v3	○ v1/v2/v3	○ v1/v2/v3	○ v1/v2/v3	○ v1/v2
	MLD snooping	○ v1/v2	○ v1/v2	○ v1/v2	○ v1/v2	○ v1/v2	○ v1/v2
	Number of VLANs supported	256	32	32	32	32	32
	Number of VLAN ports	4096	512	512	512	512	512
	Number of IGMP/MLD snooping entries	1000 Standard 2000 Extended	500	500	1000	500	500

[#]1: For chassis-type switches, *(Standard)* signifies that BSU-LA/CSU-1A/MSU-1A1 is used; *(Extended)* means that BSU-LB/CSU-1B/MSU-1B1 is used.
[#]2: PIM-DM supports IPv4 only.
[#]3: For AX3640S/AX3630S

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

[#]4: For AX3650S

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

2.3 Ring Protocols that allow wide-area networks to be built reliably and easily

Systems that monitor extensive areas such as entire regions (including railways and roads) must be able to integrate a network system that provides stable coverage of wide areas. Another requirement is easy operation, considering the sheer size of some network areas.

Ring network topologies are one possibility for integrating wide-area networks, a single ring design results in a single network with only an L2 layer, which has some drawbacks including vulnerability to bandwidth occupation caused by flooding, which can increase load on an entire network even if it occurs at a single point; and the increase in latency the larger the ring becomes.

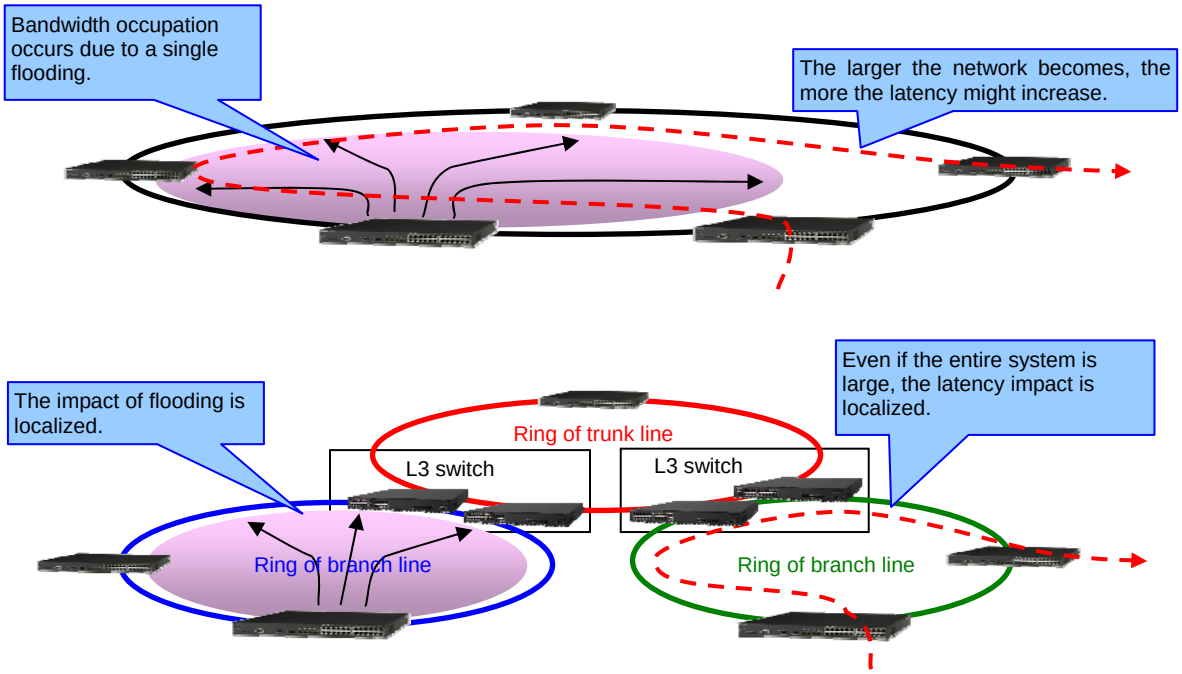


Figure 2.3-1: Hierarchical ring network

The AX series allows for integrating L2/L3 layered networks using L3 switches. By dividing a network at the L3 layer, load increase due to flooding and communication latency between locations can be minimized. Each ring can be also configured as a simple assembly of single L2 rings, thus ensuring easy operation.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

3. System Integration and Configuration Examples

This chapter describes how to configure a surveillance camera network that takes advantage of the various functionalities of the AX series.

3.1 Surveillance system of a typical building

Below we provide an example of integrating a surveillance camera network configured within a typical building using an FT switch as the core switch.

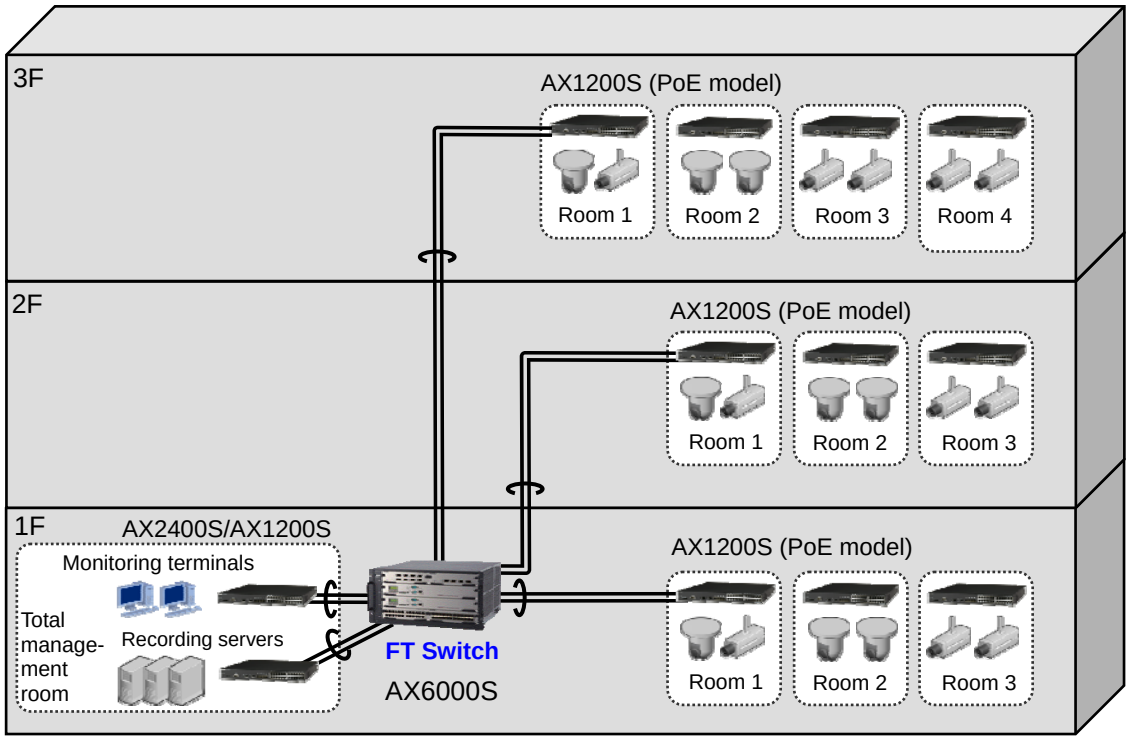


Figure 3.1-1: Surveillance camera network in a building using an FT switch as the core switch

The first floor houses the total management room that monitors the entire building, and houses servers that record all the monitoring data and the terminals that can monitor areas within the building.

Surveillance cameras are installed in each room on each floor, and an access switch such as the AX1200S switch aggregates the cameras. For aggregating surveillance cameras, we recommend that you use PoE model switches that can power the cameras. PoE model switches can eliminate the need to use separate cables for power and data transmission.

The access switch in each room is then connected to the AX6000S FT switch configured as the core switch.

This configuration can easily build a surveillance camera network that can handle enough cameras installed in a typical building and ensure high availability.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

As a specific example of a device configuration, consider the configuration shown in Figure 3.1-2 as part of the entire system.

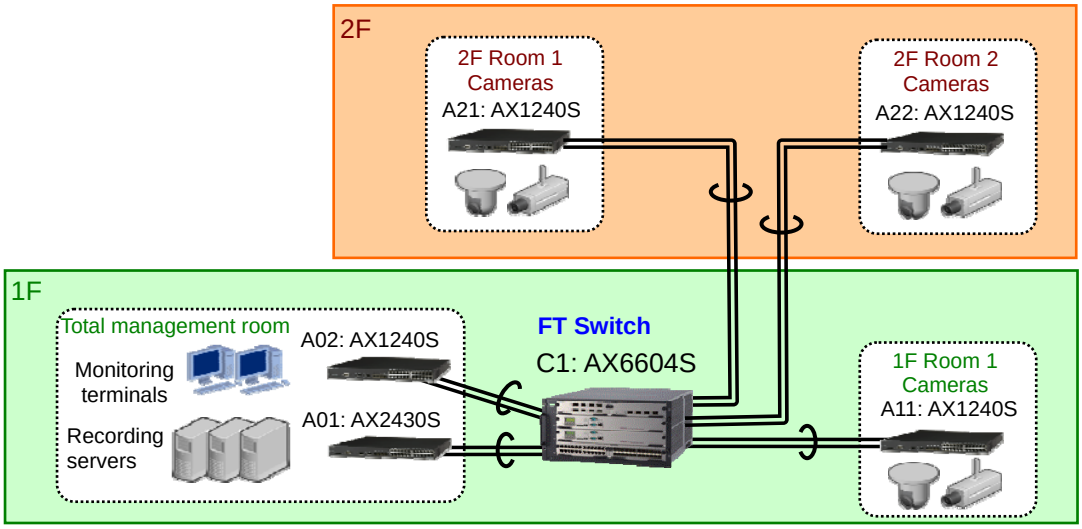
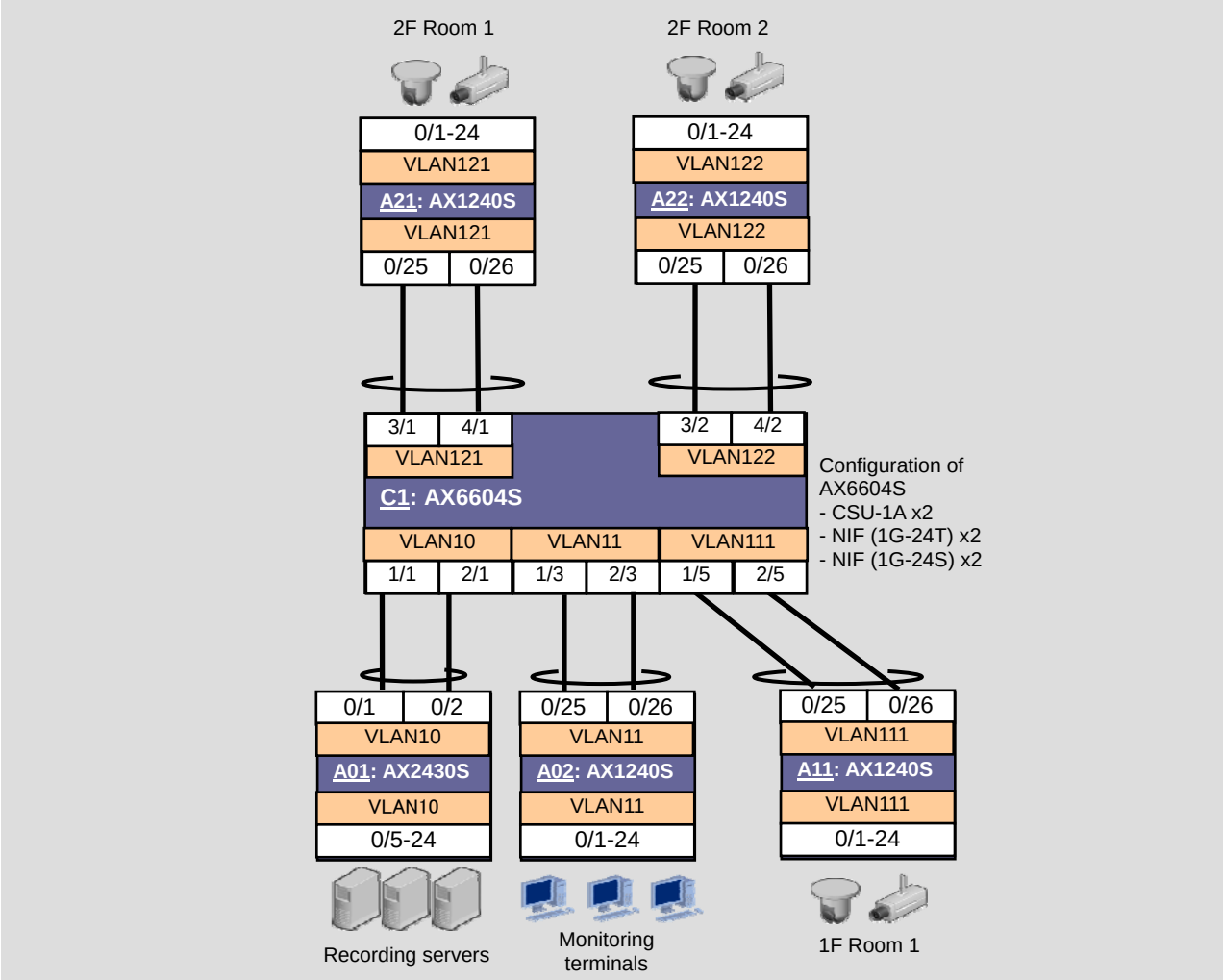


Figure 3.1-2: Configuration of a surveillance camera network as used in the examples in this document

Figure 3.1-2 shows a simplified image of the entire system shown in Figure 3.1-1. An AX6604S switch is used as the core switch that directly accommodates the access switches (AX2430S and AX1240S) that are placed in the total management room and general-use rooms on the first and second floors.

Figure 3.1-3 below provides the logical configuration of the system.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.



		VLAN ID	IP address	Multicast group address
1F of the building	Recording servers	10	10.0.0.0/24	225.10.0.1
	Monitoring terminals	11	11.0.0.0/24	225.11.0.1
	Room 1	111	192.168.11.0/24	-
2F of the building	2F Room 1	121	192.168.21.0/24	-
	2F Room 2	122	192.168.22.0/24	-

Figure 3.1-3: Logical configuration

The logical configuration shows a network consisting of two different segments: one for recording servers and monitoring terminals, and the other for the general-use rooms on the first and second floors. In this configuration, recording servers and monitoring terminals are the receiving side, and thus the respective servers and terminals have unique multicast group addresses; and on the switches (A01 and A02) that accommodate them, IGMP snooping is enabled.

PIM-SM is used as the multicast routing protocol. Note that because Switch C1 is the only L3 switch that functions as a multicast router, C1 is specified as a static rendezvous point.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

3.1.1 Configuration key points

(1) Three major categories of configuration for multicast routing

To configure a network that supports multicast routing, you need to set the items below.
Configure the L3 switch/router in the network as follows:

- Multicast group management functionality
  In a multicast network system, multiple recipients are handled as a group, called a *multicast group*, and the recipients that belong to the group are called *multicast group members*. Common functionality to manage and control multicast group members includes IGMP for IPv4 and MLD for IPv6.

- Multicast routing protocols
  Protocols that efficiently select routes for multicast traffic (for both IPv4 and IPv6) include PIM-SM, PIM-SSM, and PIM-DM. You need to select one of these protocols taking into consideration the size of the system and placement of the multicast group members. Note that all of these protocols are designed to select appropriate routes for multicast traffic based on unicast traffic routes, so normal unicast routes must be correctly established.

In addition, in order to use the entire network system efficiently, configure the L2 switch (and the L3 switch that does not perform multicast control) in the network as follows:

- Multicast cooperation functionality (IGMP/MLD snooping feature)
  Although the L2 switch normally forwards multicast traffic to all the ports of the VLAN, this functionality allows multicast traffic to be forwarded only to ports to which multicast group members are connected. As a result, unnecessary multicast traffic can be minimized for more efficient use of the network.

(2) Generally, consider using v2 of IPv4 IGMP.

IGMP provides the ability to manage and control multicast group members for IPv4 networks. There are two main versions of IGMP, IGMPv2 and IGMPv3. If you do not specify a version, the AX series operates in a mode that allows a combination of both versions.

This means that as long as you use the L3 switch of the AX series to manage IGMP, you do not need to be aware of the IGMP version; but if you want to use the IGMP snooping feature concurrently on the surrounding L2 switches and if you are unsure whether IGMP is supported by the recipient hosts of multicast traffic, we recommend that you use IGMPv2 to ensure versatility.

(3) PIM-SM is recommended as the multicast routing protocol.

Common multicast routing protocols include PIM-SM, PIM-SSM, and PIM-DM.

You can use PIM-SSM in surveillance camera networks because the multicast sources are usually fixed cameras, but due to some restrictions for using PIM-SSM, multicast group member hosts and the switch that performs IGMP snooping should support IGMPv3. Thus, PIM-SM is recommended in systems that might use devices that do not support IGMPv3.

Another reason that we recommend PIM-SM is that IPv4 PIM-SM supports non-stop communication on system switchover in AX6000S-family products (FT switches), and therefore improves the availability of the system.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

(4) Make four configurations to use PIM-SM.

To use PIM-SM, make the following configurations:

- Configuration of IPv4 multicast routing
- Configuration of IPv4 PIM-SM
- Configuration of IPv4 PIM-SM rendezvous point candidates
- Configuration of IPv4 PIM-SM BSR (bootstrap router) candidates or a static rendezvous point

Note, however, that you must configure the static rendezvous point without setting up rendezvous point candidates because the example in this section has only one L3 switch (core switch).
If multiple L3 devices serve as multicast routers, configure rendezvous point candidates, and then set up BSR candidates or a static rendezvous point.

(5) Configure the PIM-SM, and IGMP will also become operable.

To use PIM-SM, you need to set up the `ip pim sparse-mode` command on the VLAN interface to which you want to apply PIM-SIM, making IGMP also operable on that interface (equivalent to `ip igmp router`).
Therefore, on an interface that uses PIM-SM, you need not make a separate configuration for IGMP.

(6) When using PIM-SM on an FT switch, enable non-stop communication on system switchover.

If you set up a BCU/CSU/MSU redundant configuration and use IPv4 PIM-SM with AX6000S, you can use `ip pim nonstop-forwarding` to specify to temporarily prevent multicast forwarding from stopping during the system switchover of BCU/CSU/MSU (except when you use IPv4 PIM-SM on a VRF interface).

We also recommend using this command to enhance system availability.

(7) Enable IGMP snooping on L2 switches that reside on the routes leading to the multicast recipient hosts.

Multicast cooperation functions include IGMP snooping for IPv4 networks. For this function to work effectively, make sure that IGMP snooping is enabled on all the L2 switches to which the multicast recipient hosts (multicast group members) are connected and that reside on the routes leading to the multicast router.

These configurations prevent unnecessary multicast traffic from flowing to the ports and lines that do not reach the multicast group members, and thus can avoid consuming the bandwidth of switches and lines outside of the multicast routes.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

3.1.2 Configuration examples

Configuration examples are shown below.

(1) Configuration of Core Switch C1

Configuration of C1 (AX6604S)	
Configuration of the Spanning Tree Protocol	
`(config)# spanning-tree disable`	Disable the Spanning Tree Protocol.
Configuration of VLANs	
`(config)# vlan 10-11,111,121-122` `(config-vlan)# exit`	Configure the VLANs that are to be used.
Configuration of multicast routing (Configuration key point (4))	
`(config)# ip multicast-routing` `(config)# ip pim nonstop-forwarding`	Enable IPv4 multicast routing functionality. Enable non-stop communication during system switchover for IPv4 PIM-SM. (Configuration key point (6))
Configuration of VLAN interfaces	

`(config)# interface vlan 10`
`(config-if)# ip address 10.0.0.1 255.255.255.0`
`(config-if)# ip pim sparse-mode`
`(config-if)# exit`
	Assign the IP address `10.0.0.1` to VLAN `10` and enable PIM-SM and IGMP.
	(Configuration key points (2), (3), and (4))

`(config)# interface vlan 11`
`(config-if)# ip address 11.0.0.1 255.255.255.0`
`(config-if)# ip pim sparse-mode`
`(config-if)# exit`
	Assign the IP address `11.0.0.1` to VLAN `11`, and enable PIM-SM and IGMP.
	(Configuration key points (2), (3), and (4))

`(config)# interface vlan 111`
`(config-if)# ip address 192.168.11.1`
`255.255.255.0`
`(config-if)# ip pim sparse-mode`
`(config-if)# exit`
	Assign the IP address `192.168.11.1` to VLAN `111`.
	Enable PIM-SM and IGMP.
	(Configuration key points (2), (3), and (4))

`(config)# interface vlan 121`
`(config-if)# ip address 192.168.21.1`
`255.255.255.0`
`(config-if)# ip pim sparse-mode`
`(config-if)# exit`
	Assign the IP address `192.168.21.1` to VLAN `121`.
	Enable PIM-SM and IGMP.
	(Configuration key points (2), (3), and (4))

`(config)# interface vlan 122`
`(config-if)# ip address 192.168.22.1`
`255.255.255.0`
`(config-if)# ip pim sparse-mode`
`(config-if)# exit`
	Assign the IP address `192.168.22.1` to VLAN `122`.
	Enable PIM-SM and IGMP.
	(Configuration key points (2), (3), and (4))

Configuration of the IPv4 PIM-SM rendezvous point (Configuration key point (4))	

`(config)# interface loopback 0`
`(config-if)# ip address 1.1.1.10`
`(config-if)# exit`
	Set the loopback address to `1.1.1.10`.

`(config)# access-list 1 permit 225.10.0.0`
`0.0.0.255`
`(config)# access-list 1 permit 225.11.0.0`
`0.0.0.255`
	Create an access list that assigns `225.10.0.0/24` and `225.11.0.0/24` as the addresses of the multicast group to be managed.

`(config)# ip pim rp-address 1.1.1.10 1`	Assign `1.1.1.10` to the static rendezvous point that controls multicast group using access list `1`.
Configuration of physical interfaces	

`(config)# interface range gigabitethernet 1/1,`
`gigabitethernet 2/1`
`(config-if-range)# channel-group 10 mode on`
`(config-if-range)# exit`
	Add ports `1/1` and `2/1` to port channel `10` as a static link aggregation.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

Configuration of C1 (AX6604S)	
(config)# interface range gigabitethernet 1/3, gigabitethernet 2/3 (config-if-range)# channel-group 11 mode on (config-if-range)# exit	Add ports 1/3 and 2/3 to port channel 11 as a static link aggregation.
(config)# interface range gigabitethernet 1/5, gigabitethernet 2/5 (config-if-range)# channel-group 12 mode on (config-if-range)# exit	Add ports 1/5 and 2/5 to port channel 12 as a static link aggregation.
(config)# interface range gigabitethernet 3/1, gigabitethernet 4/1 (config-if-range)# channel-group 21 mode on (config-if-range)# exit	Add ports 3/1 and 4/1 to port channel 21 as a static link aggregation.
(config)# interface range gigabitethernet 3/2, gigabitethernet 4/2 (config-if-range)# channel-group 22 mode on (config-if-range)# exit	Add ports 3/2 and 4/2 to port channel 22 as a static link aggregation.
(config)# interface port-channel 10 (config-if)# switchport access vlan 10 (config-if)# exit	Set port channel 10 as the access port of VLAN 10.
(config)# interface port-channel 11 (config-if)# switchport access vlan 11 (config-if)# exit	Set port channel 11 as the access port of VLAN 11.
(config)# interface port-channel 12 (config-if)# switchport access vlan 111 (config-if)# exit	Set port channel 12 as the access port of VLAN 111.
(config)# interface port-channel 21 (config-if)# switchport access vlan 121 (config-if)# exit	Set port channel 21 as the access port of VLAN 121.
(config)# interface port-channel 22 (config-if)# switchport access vlan 122 (config-if)# exit	Set port channel 22 as the access port of VLAN 122.

(2) Configuration of Access Switch A01

Configuration of A01 (AX2430S)	
Configuration of the Spanning Tree Protocol	
(config)# spanning-tree disable	Disable the Spanning Tree Protocol.
Configuration of the VLAN	
(config)# vlan 10 (config-vlan)# exit	Configure the VLAN that is to be used.
Configuration of physical interfaces	
(config)# interface range gigabitethernet 0/1-2 (config-if-range)# channel-group 1 mode on (config-if-range)# exit	Add ports 0/1-2 to channel group 1.
(config)# interface port-channel 1 (config-if)# switchport access vlan 10 (config-if)# exit	Set port channel 1 as an access port of VLAN 10.
(config)# interface range gigabitethernet 0/5-24 (config-if-range)# switchport access vlan 10 (config-if-range)# exit	Set ports 0/5-24 as access ports of VLAN 10.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

Configuration of A01 (AX2430S)	
Configuration of VLAN interfaces	
(config)# interface vlan 10 (config-if)# ip igmp snooping (config-if)# ip igmp snooping mrouter interface port-channel 1 (config-if)# exit	Enable IGMP snooping on VLAN 10 and set port channel 1 as the multicast router port. (Configuration key point (7))

(3) Configuration of access switch A02

Configuration of A02 (AX1240S)	
Configuration of the Spanning Tree Protocol	
(config)# spanning-tree disable	Disable the Spanning Tree Protocol.
Configuration of the VLAN	
(config)# vlan 11 (config-vlan)# exit	Configure the VLAN that is to be used.
Configuration of physical interfaces	
(config)# interface range gigabitethernet 0/25-26 (config-if-range)# channel-group 1 mode on (config-if-range)# exit (config)# interface port-channel 1 (config-if)# switchport access vlan 11 (config-if)# exit (config)# interface range fastethernet 0/1-24 (config-if-range)# switchport access vlan 11 (config-if-range)# exit	Configure channel group 1 with ports 0/25-26. Set port channel 1 as an access port of VLAN 11. Set ports 0/1-24 as access ports of VLAN 11.
Configuration of VLAN interfaces	
(config)# interface vlan 11 (config-if)# ip igmp snooping (config-if)# ip igmp snooping mrouter interface port-channel 1 (config-if)# exit	Enable IGMP snooping on VLAN 11 and set port channel 1 as the multicast router port. (Configuration key point (7))

(4) Configuration of access switches A11, A21, and A22

Configuration of A11 (AX1240S)	
Configuration of the Spanning Tree Protocol	
(config)# spanning-tree disable	Disable the Spanning Tree Protocol.
Configuration of the VLAN	
(config)# vlan 111 (config-vlan)# exit	Configure the VLAN that is to be used.
Configuration of physical interfaces	
(config)# interface range gigabitethernet 0/25-26 (config-if)# channel-group 1 mode on (config-if)# exit (config)# interface port-channel 1 (config-if)# switchport access vlan 111 (config-if)# exit (config)# interface range fastethernet 0/1-24 (config-if-range)# switchport access vlan 111 (config-if-range)# exit	Set ports 0/25-26 as access ports of VLAN 111. Set ports 0/1-24 as access ports of VLAN 111.

#1: The configuration of switches A21 and A22 will be same as that of A11, except that the VLANs handled by the switches are different (A21: VLAN ID=121, A22: VLAN ID=122).

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

4. Checking the System

In a surveillance camera network system that uses multicast routing, you can check the operation of multicast routing to confirm that the surveillance cameras operate properly. This chapter mainly discusses multicast-related operation commands.

4.1 Checking with the core switch (L3 switch)

The L3 switch controls the multicast group and multicast routes to provide multicast routing. Related operation commands are shown below.

(1) Checking multicast forwarding

You can use the `show ip mcache` command to check whether multicast communications are correctly performed. This command shows the multicast group that currently performs multicast forwarding, its transmission sources, and its VLAN interfaces used for forwarding.

```
C1# show ip mcache
Date 2012/03/27 10:28:40 JST
Total: 2 routes
- Forwarding entry
-----------------------------------------------------------
Group Address   Source Address  Flags  Uptime   Expires
225.10.0.1      192.168.21.10           04:52    03:30
     incoming:
         VLAN0121(192.168.21.1)
     outgoing:
         VLAN0010(10.0.0.1)
225.11.0.1      192.168.21.10           04:51    03:30
     incoming:
         VLAN0121(192.168.21.1)
     outgoing:
         VLAN0011(11.0.0.1)
C1#
```

Figure 4.1-1: Execution result of the show ip mcache command

This example shows the following two multicast entries that currently perform forwarding:

From 192.168.21.10 to group address 225.10.0.1
From 192.168.21.10 to group address 225.11.0.1

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

(2) Checking multicast routes

To check information on the multicast routes, you can use the `show ip mroute` command regardless of the type of multicast routing protocol. This operation command shows detailed information, including: multicast routes for each combination of source and multicast group known as *(S,G)* entries, the type of multicast routing protocol that is used, the connection status of senders/recipients, the status of the forwarding routes (via the rendezvous point/shortest path), and the various aging timer values.

```
C1# show ip mroute
Date 2012/03/27 10:28:26 JST
Total: 4 routes, 2 groups, 1 source

(S,G) 2 routes ------------------------------------------------------------
Group Address    Source Address   Protocol Flags  Uptime   Expires  Assert
225.10.0.1       192.168.21.10    SM       FLT    05:12    03:10    00:00
    incoming: VLAN0121(192.168.21.1)     upstream: Direct  reg-sup: 0s
    outgoing: VLAN0010(10.0.0.1)         uptime 05:13  expires --:--

225.11.0.1       192.168.21.10    SM       FLT    05:11    03:10    00:00
    incoming: VLAN0121(192.168.21.1)     upstream: Direct  reg-sup: 0s
    outgoing: VLAN0011(11.0.0.1)         uptime 05:13  expires --:--

(*,G) 2 routes ------------------------------------------------------------
Group Address    RP Address       Protocol Flags  Uptime   Expires  Assert
225.10.0.1       1.1.1.10         SM       LR     05:13    03:04    00:00
    incoming: register                   upstream: This System
    outgoing: VLAN0010(10.0.0.1)         uptime 05:13  expires --:--

225.11.0.1       1.1.1.10         SM       LR     05:13    02:59    00:00
    incoming: register                   upstream: This System
    outgoing: VLAN0011(11.0.0.1)         uptime 05:13  expires --:--
C1#
```

Figure 4.1-2: Execution result of the show ip mroute command

This example shows that the following two multicast entries operate using the PIM-SM protocol, and that both senders and recipients are connected to the switch directly:

- (192.168.21.10, 225.10.0.1)
- (192.168.21.10, 225.11.0.1)

In addition, because the operation uses PIM-SM, the result shows that for the route from the rendezvous point (shared tree: (*,G) entry), two similar entries exist that designate this Switch as the rendezvous point (upstream: This System).

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

(3) Checking IGMP information

When the IGMP functionality is enabled with the L3 switch, you can use the `show ip igmp interface` command to check if the IGMP functionality functions properly.

```
C1# show ip igmp interface
Date 2012/03/27 10:30:28 JST
Total: 5 Interfaces
Address         Interface       Version  Flags  Querier         Expires    Group Count  #1 Notice
10.0.0.1        VLAN0010              3         10.0.0.1              -              1    Q
11.0.0.1        VLAN0011              3         11.0.0.1              -              1
192.168.11.1    VLAN0111              3         192.168.11.1          -              0
192.168.21.1    VLAN0121              3         192.168.21.1          -              0
192.168.22.1    VLAN0122              3         192.168.22.1          -              0
C1#
```

Version of target IGMP
Snooping flag
IGMP querier aging time
#1 Alert info
VLAN that operates IGMP
Address of querier
Number of groups joined

#1: This column appears when any notice exists (since it is generated until the General Query is sent or received twice).

Figure 4.1-3: Execution result of the show ip igmp interface command

This example shows that the five VLAN interfaces operate with both IGMPv2 and v3 enabled. (In the `Version` column, a "2" appears when only v2 is used, and a "3" appears when only v3 is used.)
Also shown is that a multicast group is registered with each VLAN, whether VLAN `10` or VLAN `11`. You can also check any notices for the interface (IGMP version discrepancies, maximum number of information items exceeded, etc.).

In addition, you can use the `show ip igmp group` command to check details for each multicast group registered on the switch where IGMP is enabled.

```
C1# show ip igmp group
Date 2012/03/27 10:30:37 JST
Total: 2 groups
Group Address/Source Address  Interface       Version  Mode     Last Reporter   Uptime
Expires  IGMPv1Time IGMPv2Time IGMPv3Time
225.10.0.1                    VLAN0010            2     EXCLUDE  10.0.0.10       06:08
03:14     --:--      03:10      --:--
225.11.0.1                    VLAN0011            2     EXCLUDE  11.0.0.10       06:08
03:19     --:--      03:15      --:--
C1#
```

(Upper row) multicast group address
VLAN to which the group belongs
Version of IGMP in use
Address of the host that last participated in the group

Figure 4.1-4: Execution result of the show ip igmp group command

This example shows that two multicast groups are registered to the switch, that they belong to VLAN `10` and VLAN `11` respectively, and that the version of IGMP that is used is "2" for both. It also shows the IP address of the host that last participated in the group, the elapsed time since each group was generated, and the aging time values.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

4.2 Checking with the distribution and access switches (IGMP snooping)

For a multicast network, it is also important to prevent the generation of unnecessary multicast traffic. The functionality used to control this traffic is IGMP/MLD snooping, and in the AX series it is also supported by the L2 switches that are used as distribution or access switches. You can use the following commands to check the operation status of this functionality.

(1) Checking the settings of IGMP snooping and the operation status

You can use the `show igmp-snooping` command to check the settings of IGMP snooping and the operation status.

```
A01# show igmp-snooping
Date 2012/03/27 10:49:36 JST
VLAN counts: 1
VLAN: 10   VLAN where IGMP snooping operates
  IP address:      Querier: disable
  IGMP querying system:
  Querier version: V2  Version of IGMP querier
  Fast-leave: Off
  Port(22): 0/1-2,0/5-24   Target ports and number of ports
  Mrouter-port: 0/1-2      Ports that have a route to the multicast router
  Group Counts: 1          Detected number of multicast groups
A01#
```

Figure 4.2-1: Execution result of the show igmp-snooping command

This example shows that IGMP snooping operates on IGMPv2 with VLAN `10`. It also shows that a total of 22 physical ports (`0/1-2` and `0/5-24`) are configured to be subject to IGMP snooping in VLAN `10`, that the ports that have a route to the multicast router are `0/1-2`, and that, currently, IGMP traffic to one multicast group is being detected.

(2) Checking the status of multicast delivery

By checking the detailed operation of IGMP snooping, you can confirm the following items:

- Which group uses which port
- Which group's traffic reaches which ports

You can use the `show igmp-snooping group` command for the former and the `show igmp-snooping port` command for the latter.

```
A01# show igmp-snooping group
Date 2012/03/27 10:49:50 JST
Total Groups: 1
VLAN counts: 1
VLAN: 10  Group counts: 1
  Group Address       MAC Address          Version        Mode
  225.10.0.1          0100.5e0a.0001       V2             -
    Port-list:0/23
A01#
```

Figure 4.2-2: Execution result of the show igmp-snooping group command

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

This example shows that the multicast forwarding to group address 225.10.0.1 uses IGMPv2 and that the communication goes through port 0/23.

```
A01# show igmp-snooping port 0/23
Date 2012/03/27 10:49:55 JST
Port  0/23  VLAN counts: 1
  VLAN: 10  Group counts: 1
    Group Address       Last Reporter       Uptime     Expires
    225.10.0.1          10.0.0.10           00:20      04:03
A01#
```

Figure 4.2-3: Execution result of the show igmp-snooping port command

This example shows that multicast forwarding to group address 225.10.0.1 is handled at port 0/23 and that the host that most recently issued an IGMP Report (the host that last participated in the multicast group) is 10.0.0.10.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

5. Considerations

Below we provide you with some points that you must be aware of when you use the multicast routing functionality.

5.1 Notes on multicast group management functionality (IGMP/MLD)

Here we explain the most common issues. For details about the following notes and other considerations, see chapters *Description of IPv4 Multicasting* and *Description of IPv6 Multicasting* in the *Software Manual Configuration Guide Vol. 3* of the AX6000S family or the AX3600S series.

(1) Time for creating a (*,G) or a (S,G) entry for static group joins

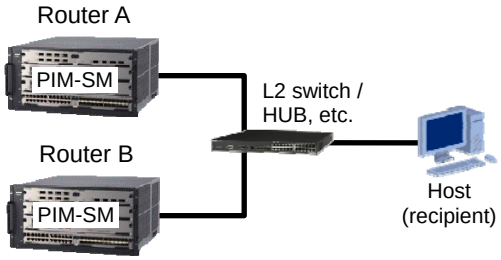
When static group joining is set due to a configuration change, as long as 125 seconds might be needed to create a (*,G) entry for a PIM-SM group, or a (S,G) entry for a PIM-SSM group.

5.2 Notes on the multicast routing protocol PIM-SM

Here we will mainly explain the most common issues related to PIM-SM. For details about the following notes and other considerations, see chapters *Description of IPv4 Multicasting* and *Description of IPv6 Multicasting* in the *Software Manual Configuration Guide Vol. 3* of the AX6000S family or the AX3600S series.

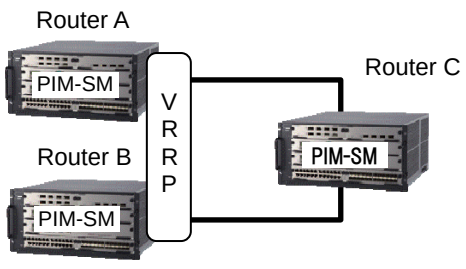
(1) Configurations requiring special attention when using PIM-SM

- In configurations such as the one in the figure below, in which two or more routers connected directly to the host exist on the same network, make sure that you enable PIM-SM.



If only IGMP operates while PIM-SM does not operate at the interface where multiple routers exist in the same network, multicast data might be forwarded twice.

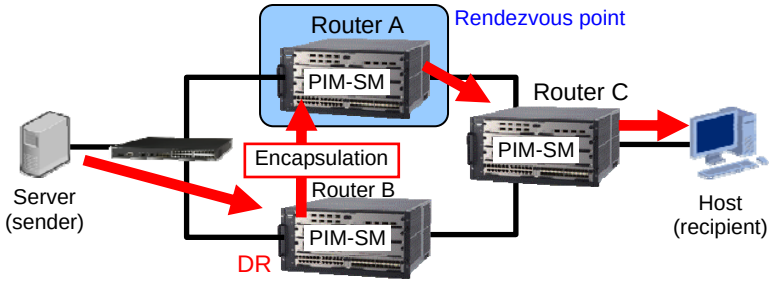
- In configurations such as the one in the figure below, in which the PIM protocol cannot detect the upstream router, multicast communication cannot be performed because the environment has a static route as the gateway, for which Router C has set the virtual interface with VRRP set for Router A and Router B.



Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

To use multicast communication in such a configuration, you need to set a static route to Router C using any of the following as the real address of Router A or Router B:
- Rendezvous point address
- BSR address
- Gateway address to the multicast data source address

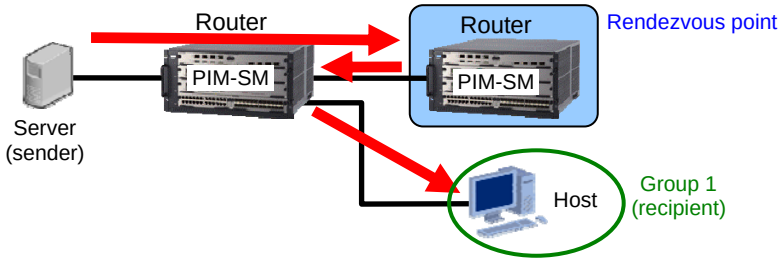
- In a configuration in which two or more routers connected directly to the sender exist on the same network, when choosing one as the rendezvous point, make sure that the DR (designated router) and the rendezvous point are the same.



If a router other than the rendezvous point is the DR, as shown in the above figure, the load on Routers A and B increases because PIM-Register messages are sent from the DR to the rendezvous point. In addition, when multicast packets within the PIM-Register messages are forwarded, packet loss might occur on the rendezvous point.
Note that if the rendezvous point is the DR, encapsulation is not performed using PIM-Register messages.

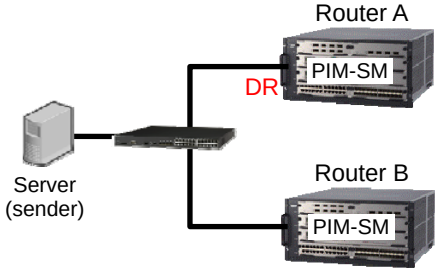
(2) Inappropriate configurations for using PIM-SM

- Configuration in which a recipient is between the sender and the rendezvous point



Forwarding via the rendezvous point cannot be performed efficiently.

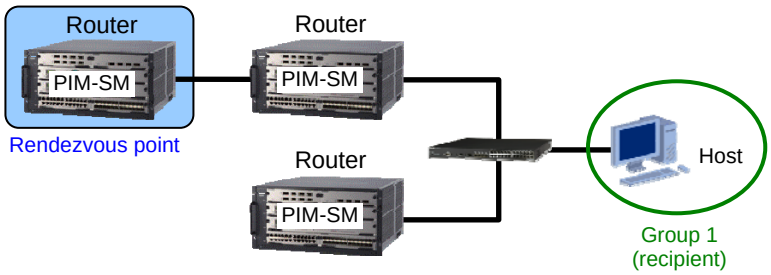
- Configuration in which multiple PIM-SM routers that are not rendezvous points are running on the same line as the sender



In the configuration as shown in the above figure, excessive load is placed on the PIM-SM router (Router B) that is not the DR, which might significantly impact other functionality in the device. In this case, split the line as appropriate.

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

- Configuration in which multiple PIM-SM routers are running on the same line as the multicast group (recipient), and when one of the PIM-SM routers does not connect to the rendezvous point



The shortest path between the sender and group 1 might not be established.

5.3 Notes on using IGMP/MLD snooping

Here we explain some of the most common issues. For details about the following notes and other considerations, see the section *Notes on using IGMP snooping and MLD snooping* of the chapter *Description of IGMP Snooping and MLD Snooping* in the *Software Manual Configuration Guide Vol. 1* of the respective AX series.

(1) Control packet flooding

Because multicast traffic that is subject to suppression by IGMP snooping or MLD snooping is data traffic, flooding needs to be performed within a VLAN to enable the routing protocol and other control packets to be received by all routers and all hosts. Thus the AX-series switch forwards packets with destination IP addresses contained in the address ranges shown in Table 5.3-1 below to all ports on the VLAN.

Table 5.3-1: Control packet flooding

Protocol	Address range
IGMP snooping	From 224.0.0.0 to 224.0.0.255
MLD snooping	ff02::/16

Note that some multicast group addresses that duplicate multicast MAC addresses for control packets cannot be used. The following table lists multicast group addresses that cannot be used for addresses outside the address ranges shown in the above Table 5.3-1.

Table 5.3-2: Multicast group addresses that cannot be used

AX series	Protocol	Address range
AX6000S family	IGMP	224.128.0.0/24
AX3800S, AX3650S, AX2530S, AX2400S, AX1200S series	IGMP	224.128.0.0/24, [225-239].0.0.0/24, [225-239].128.0.0/24

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

Appendix: Configuration Files

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

3.1 Surveillance system of a typical building

	Name of the switch and the target switch	Target file
Core switch	C1 (AX6604S)	`3-1_MCN_C1.txt`
Access switch	A01 (AX2430S-24T)	`3-1_MCN_A01.txt`
	A02 (AX1240S-24T2C)	`3-1_MCN_A02.txt`
	A11 (AX1240S-24P2C)	`3-1_MCN_A11.txt`
	A21 (AX1240S-24P2C)	`3-1_MCN_A21.txt`
	A22 (AX1240S-24P2C)	`3-1_MCN_A22.txt`

Copyright © 2012, ALAXALA Networks Corporation. All rights reserved.

Edition 1 issued on March 29, 2012
Document No. NTS-11-R-050

ALAXALA Networks Corporation
Network Technical Support

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