Technical Guide

Protocol Independent Multicast - Source Specific Multicast (PIM-SSM) - IPv4 and IPv6

Feature Overview and Configuration Guide

Introduction

This guide provides information about the multicast protocol know as Protocol Independent Multicast - Source Specific Multicast (PIM-SSM).

PIM-SSM is a multicast routing protocol designed to optimize the delivery of data from a single source to multiple receivers. It is derived from Protocol Independent Multicast - Sparse Mode (PIM-SM) and is a simplified version of PIM-SM.

Benefits of PIM-SSM

- Simpler setup – No need for complex routing structures.
- Efficient delivery – Data goes straight from the source to the receivers.
- Better security – Only traffic from the chosen source is accepted.
- Ideal for streaming – Perfect for IPTV, live broadcasts, and real-time data.

AlliedWare Plus routers - command support and considerations

The following multicast commands are supported on AlliedWare Plus routers:

```
ip pim ssm default
ipv6 pim ssm default
```

Please note: **SSM Mapping is not supported** on these devices. As a result, multicast hosts must use the following protocols:

- IPv4 hosts: IGMPv3 (not IGMPv1 or IGMPv2)
- IPv6 hosts: MLDv2

This ensures proper operation of Source-Specific Multicast (SSM) on these platforms.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus™ products that support PIM-SSM, running version **5.5.5-1.2** or later.

To see whether your product supports PIM-SSM, see the following documents:

- The product's Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Feature support may change in later software versions. For the latest information, see the above documents.

Content

PIM-SSM

PIM-SSM simplifies multicast routing by eliminating the need for a rendezvous point and reducing control plane complexity. It is particularly useful in applications like IPTV, live video streaming, and financial data distribution, where the source of the multicast stream is known and fixed.

Unlike traditional multicast models, PIM-SSM uses a source-specific model where receivers explicitly request data from a known source using IGMPv3 or MLDv2.

- IGMPv3 is used in IPv4 networks.
- MLDv2 is used in IPv6 networks.

The key feature that makes IGMP and MLD suitable for PIM-SSM is their support for source filtering. This means a host can specify not just the multicast group it wants to join, but also the specific source it wants to receive traffic from.

For details of the commands used to configure PIM-SSM, see the PIM-SM and IGMP chapters of your switch's Command Reference. The Command Reference is available on our website at alliedtelesis.com.

Background

One of the significant characteristics of PIM Sparse Mode and PIM Dense Mode is the fact that hosts, and most of the routers, in the network do not know the source address of the multicast groups they wish to join.

Keeping the network in the dark about the source addresses of the groups makes the network management a bit simpler.

The advantages are:

- You don't need a process to inform hosts of the source addresses of the streams in advance. However, this is only a minor advantage, since you still need a process to inform hosts of the group addresses beforehand.
- You can freely change the multicast servers without needing to notify all hosts about the new server addresses.

Disadvantages:

- It complicates the multicast routing protocol. Much of the functionality in PIM Sparse Mode and PIM Dense Mode exists because hosts and routers don't know the source of a requested group. Features like Rendezvous Points in Sparse Mode and State Refreshes in Dense Mode are designed to handle this limitation.
- If you're receiving multicast feeds from multiple external content providers, you must ensure that their group addresses don't overlap, which requires careful coordination.
- It introduces vulnerability to multicast denial-of-service (DoS) attacks. If an attacker knows the group address of an active stream, they can send multicast packets to that address. These packets will be forwarded to all listening hosts, regardless of the source IP, potentially disrupting the legitimate stream.

In light of these disadvantages, a variant of Multicast routing, called **Source Specific Multicast** (**SSM**), was defined.

In SSM routing:

- The hosts requesting streams need to know the source address of the stream they are requesting, and must specify the source in their request.
- SSM routers differentiate between streams that go to the same group address but come from different source addresses. If they have been requested to send a stream from source 1 (S1,G), they will forward that (S1,G) stream. But they will not forward a stream to the same group from a different source, such as (S2,G).
- The Rendezvous Point (RP)—a central concept in PIM Sparse Mode—is not needed in SSM because:
  - In traditional multicast models like PIM-SM, the RP acts as an initial meeting point for multicast traffic. Receivers send join messages to the RP, which then helps them discover the actual source of the stream.
  - In SSM, receivers already know the source IP address and can join the stream directly using the (S,G) format, bypassing the RP entirely.
  - This direct join mechanism eliminates the need for RP discovery, shared trees, and source registration processes, making PIM-SSM simpler, faster, and more secure.

Here's a simple comparison between PIM-SSM and PIM-SM:

FEATURE	PIM-SSM	PIM-SM
Source Discovery	Receiver knows the source in advance	Source discovery via Rendezvous Point
Rendezvous Point (RP)	Not required	Required
Receiver Join info	Receiver joins using (S,G) - Source and Group	Receiver joins using (*,G) - any source for Group
Security	More secure - only traffic from a known source	Less secure - can receive traffic from any source
Complexity	Simpler setup and management	More complex due to RP and source discovery
Scalability	Highly scalable	Less scalable in large networks
Use case	Ideal for streaming from known sources (e.g. IPTV, financial feeds, security cameras)	Better for dynamic or unknown sources (e.g., video conferencing)

PIM-SSM IP address ranges

The Internet Assigned Numbers Authority (IANA) has reserved the **IPv4** address range 232.0.0.0 through 232.255.255.255 for SSM applications. Although PIM-SSM can technically be configured to use the entire 224/4 multicast address range, PIM-SSM operation is guaranteed only in the 232.0.0.0/8 range, except 232.0.0.0/24, which is reserved.

For **IPv6**, IANA has reserved the address range ff3x::/96 for Source-Specific Multicast (SSM).The ff3x::/96 range is used exclusively for SSM.

The x in ff3x represents the scope of the multicast (e.g., link-local, site-local, global). Just like in IPv4 where 232.0.0.0/8 is reserved for SSM, in IPv6, only the ff3x::/96 range is guaranteed to work for SSM.

How PIM-SSM processes join requests

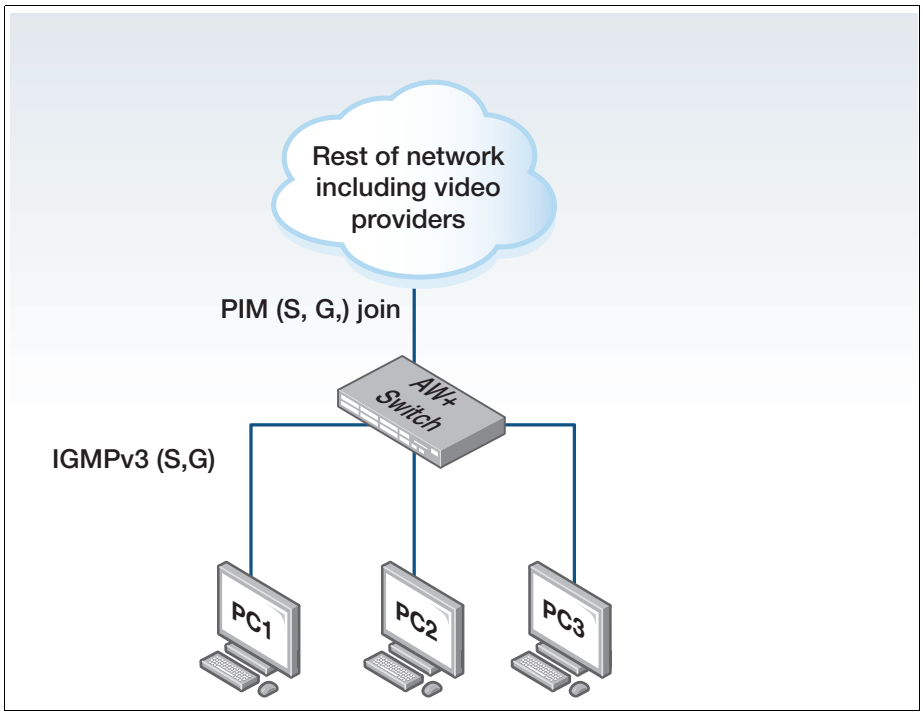
To join a multicast group using PIM-SSM, the client sends an IGMPv3 or MLDv2 join with the source IP address specified.

For example, to join multicast group **232.1.1.1** each PC must send an IGMPv3 join with the source IP address specified. The join will be a (S,G) join. For example, the join (192.168.1.1,232.1.1.1) requests the group 232.1.1.1 from the source 192.168.1.1.

The router will receive the join and check if the group address is in the SSM range.

Then:

- If the group address is in the SSM range, the router will verify that a specific source or sources have been included in the IGMP join.
- If a specific source or sources has been included in the IGMP join, then the router will forward a PIM (S,G) join towards the source IP address.
- If the source IP address is not specified, then the router will discard the IGMP join and the PC will not join the group.
- If an IGMPv2 join is received for the SSM range, then by default the join is discarded because no source IP address is specified.



Older versions of IGMP and MLD require SSM Mapping

A restriction of PIM-SSM is that it requires a “Source, Group” (S,G) join and only IGMPv3/MLDv2 support this. Earlier versions of IGMP and MLD only use “Any, Group” (*,G) joins.

This can be a problem if you have older multicast client devices that do not support IGMPv3/MLDv2.

If the router receives an IGMPv1, IGMPv2 or MLDv1 join request for an SSM group, then by default the router discards it.

To resolve this issue, you can use a feature called **SSM Mapping**. This feature allows you to statically map IGMPv1/v2 (*,G) joins into PIM (S,G) joins, which in turn allows the router to talk to an upstream PIM-SSM network.

With SSM Mapping, you use software **ACLs** to statically configure the router with source IP addresses for each group address or range of group addresses. This allows the router to receive a (*,G) join, match (map) the group address, and based on this, insert the matching source IP address. The router then treats the join as a normal (S,G) join.

If the ACL doesn’t match the source/group address pair, then the router doesn’t change the (*,G) entry. If the group address is in the SSM range, then the router discards the join. If the group address is not in the SSM range, then it attempts to process it with PIM-SM.

Note that SSM Mapping cannot map IGMPv3/MLDv2 (*,G) joins.

For more detail see "Using SSM Mapping and PIM-SSM to work with older multicast client devices" on page 10.

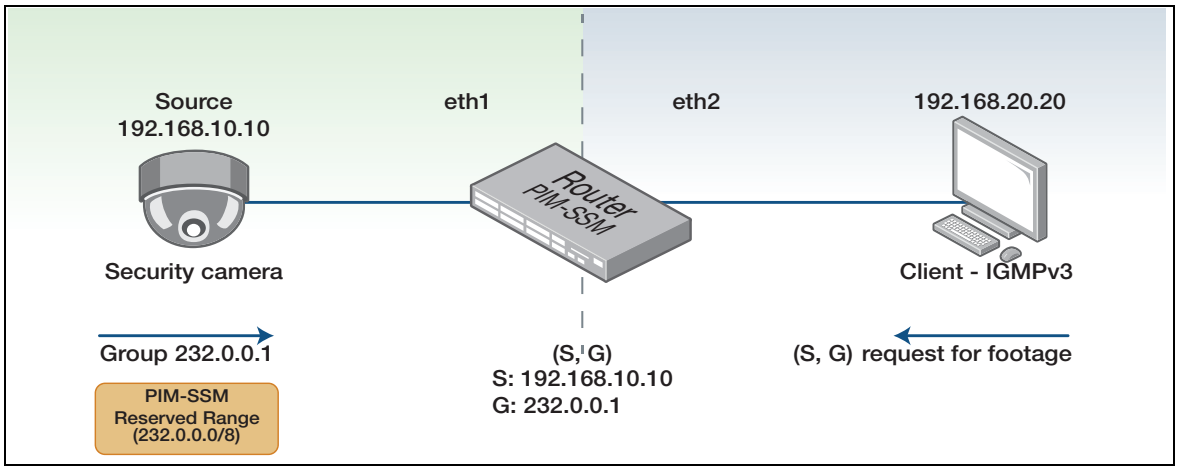
Configuring PIM-SSM multicast groups with IGMPv3

You can set up either default or non-default multicast groups:

- **Default Configuration**: Uses IANA-reserved SSM ranges (IPv4: 232.0.0.0/8, excluding 232.0.0.0/24; IPv6: ff3x::/96). No access list needed—ideal for standard SSM set-ups.
- **Non-Default Configuration**: Supports custom multicast ranges outside the default. Requires access lists and is useful for legacy systems or specific applications.

Configuring PIM-SSM with a default multicast group and IGMPv3

AlliedWare Plus supports PIM-SSM on switches, and—starting from version 5.5.5-1.1—also on firewalls and routers. Firewalls and routers support only the default PIM-SSM group range.



The example below shows how to configure PIM-SSM using the default group range on a router. To configure a switch, use VLANs instead of Ethernet ports.

1. Enable the PIM service and multicasting

```
awplus# configure terminal
awplus# service pim
awplus# ip multicast-routing
```

2. Enable PIM on eth1 and then enable PIM and IGMP on eth2

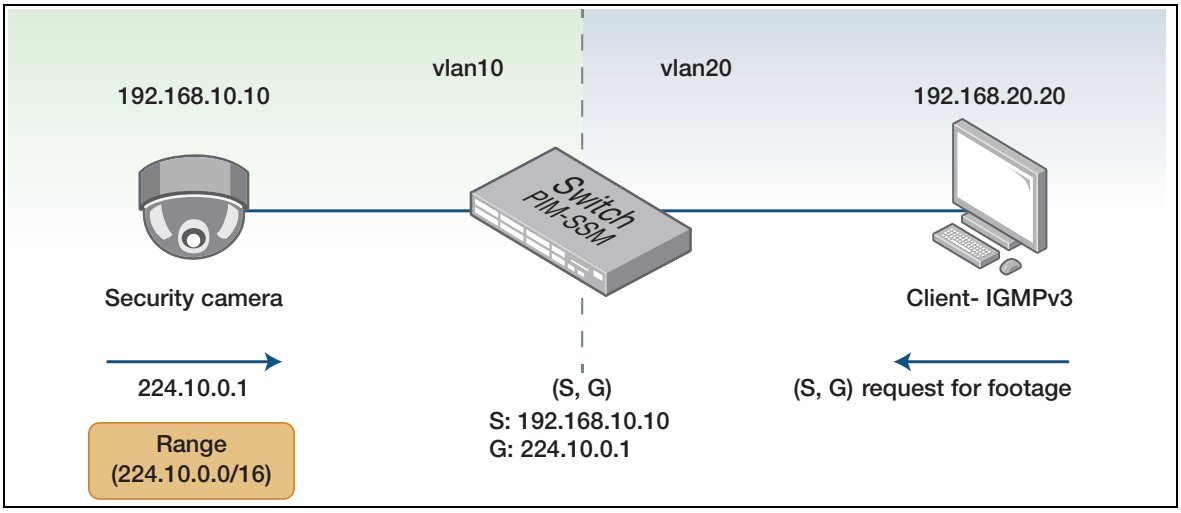
```
awplus(config)# int eth1
awplus(config-if)# ip pim sparse-mode
awplus(config-if)# exit
awplus(config)# int eth2
awplus(config-if)# ip pim sparse-mode
awplus(config-if)# ip igmp
awplus(config-if)# exit
```

3. Define the default address range of PIM-SSM

```
awplus(config)# ip pim ssm default
```

Configuring PIM-SSM with a non-default multicast group and IGMPv3

AlliedWare Plus switches support user-specified (non-default) multicast group addresses. The following example shows how to do this.



Before you start, create VLAN10 and VLAN20 and add them to the desired switchports.

1. Enable the PIM service and multicasting

```
awplus# configure terminal
awplus# service pim
awplus# ip multicast-routing
```

2. Enable PIM on VLAN10 and then enable PIM and IGMP on VLAN20

```
awplus(config)# int vlan10
awplus(config-if)# ip pim sparse-mode
awplus(config-if)# exit
awplus(config)# int vlan20
awplus(config-if)# ip pim sparse-mode
awplus(config-if)# ip igmp version 2
awplus(config-if)# exit
```

3. Specify the multicast group address range and camera source address

```
awplus(config)# access-list standard V4-SSM-RANGE permit 224.10.0.0/16

awplus(config)# ip igmp ssm range V4-SSM-RANGE
awplus(config)# ip pim ssm range V4-SSM-RANGE
```

Using SSM Mapping and PIM-SSM to work with older multicast client devices

This section explains how to configure **SSM Mapping**, which is necessary when supporting older multicast client devices that do not use IGMPv3 or MLDv2. These legacy clients, running IGMPv1 or IGMPv2, cannot natively support Source-Specific Multicast (SSM) because they only send (*,G) join requests — meaning “any source for group G.”

To enable these clients to receive video streams in a PIM-SSM environment, you need a mechanism called **SSM Mapping**. SSM Mapping translates the (*,G) join requests from IGMPv1/v2 clients into (S,G) joins, where S is the known source IP address. This allows the clients to participate in SSM even though they don’t support it directly.

How it works:

1. The client sends an IGMPv1/v2 join for group G (e.g., 232.0.0.1) without specifying a source.
2. The local device (typically the first-hop device) maps group G to a known source using a predefined table or policy (ACL).
3. The device then creates a (S,G) join internally and forwards it using PIM-SSM.

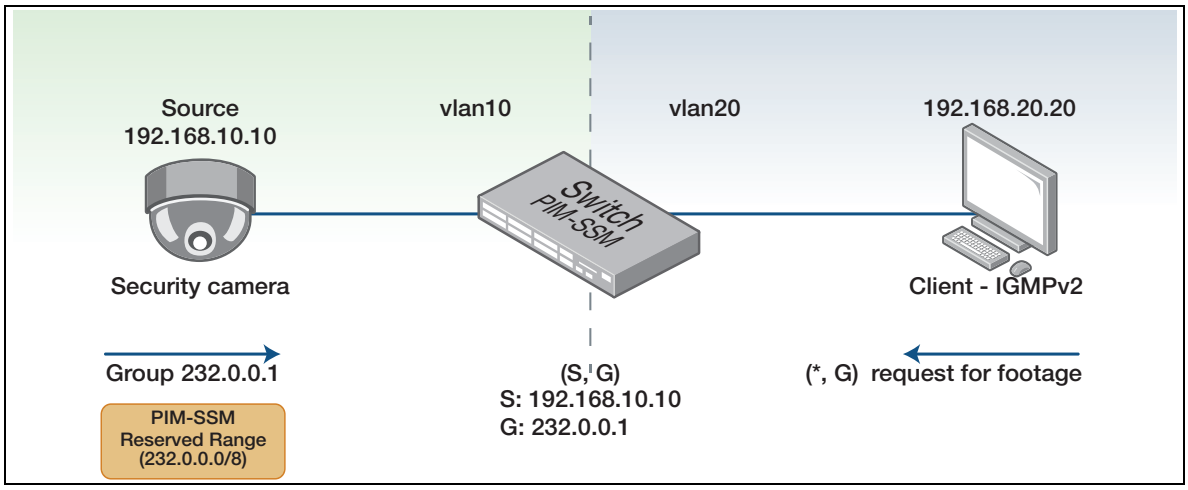
Requirements for this to work:

- The device must support SSM Mapping.
- The source IP must be known and trusted.
- The group must be in the SSM range (e.g., 232.0.0.0/8 for IPv4).

The next section explains how to configure PIM-SSM multicast groups with legacy clients, running IGMPv1 or IGMPv2. You can configure a default multicast group, or a non-default multicast group.

Configuring PIM-SSM with a default multicast group and IGMPv1 or IGMPv2

AlliedWare Plus switches support PIM-SSM with IGMPv1 and IGMPv2. The following example shows how to configure this when using the default PIM-SSM group address range.



Before you start, create VLAN10 and VLAN20 and add them to the desired switchports.

1. Enable the PIM service and multicasting

```
awplus# configure terminal
awplus# service pim
awplus# ip multicast-routing
```

2. Enable PIM on VLAN10 and then enable PIM and IGMPv2 on VLAN20

```
awplus(config)# int vlan10
awplus(config-if)# ip pim sparse-mode
awplus(config-if)# exit
awplus(config)# int vlan20
awplus(config-if)# ip pim sparse-mode
awplus(config-if)# ip igmp version 2
awplus(config-if)# exit
```

3. Enable SSM Mapping on the device

```
awplus(config)# ip pim ssm-map enable
```

4. Use an ACL to define the group address

```
awplus(config)# access-list 1 permit 232.0.0.1/32
```

5. In IGMP, associate the group address with the camera's source address

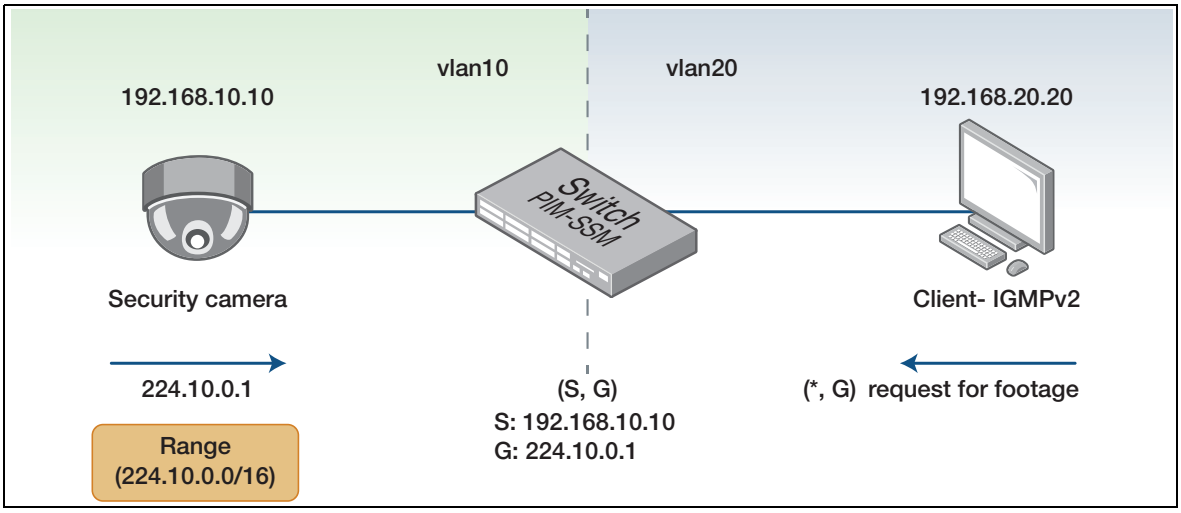
```
awplus(config)# ip igmp ssm-map static 1 192.168.10.10
```

6. Use the default PIM-SSM address range

```
awplus(config)# ip pim ssm default
```

Configuring PIM-SSM with a non-default multicast group and IGMPv1 or IGMPv2

AlliedWare Plus switches support PIM-SSM with IGMPv1 and IGMPv2. The following example shows how to configure this when using a user-specified (non-default) PIM-SSM group address range.



Before you start, create VLAN10 and VLAN20 and add them to the desired switchports.

1. Enable the PIM service and multicasting

```
awplus# configure terminal
awplus# service pim
awplus# ip multicast-routing
```

2. Enable PIM on VLAN10 and then enable PIM and IGMP on VLAN20

```
awplus(config)# int vlan10
awplus(config-if)# ip pim sparse-mode
awplus(config-if)# exit
awplus(config)# int vlan20
awplus(config-if)# ip pim sparse-mode
awplus(config-if)# ip igmp
awplus(config-if)# exit
```

3. Enable SSM Mapping on the device

```
awplus(config)# ip pim ssm-map enable
```

4. Use an ACL to specify the multicast group address range

```
awplus(config)# access-list 2 permit 224.10.0.0/16
```

5. Use that range in PIM-SSM and IGMP

```
awplus(config)# ip pim ssm range 2
awplus(config)# ip igmp ssm range 2
```

6. Use an ACL to define the non-default group address

```
awplus(config)# access-list 3 permit 224.10.0.1/32
```

7. Associate the non-default group address with the camera's source address'

```
awplus(config)# ip igmp ssm-map static 3 192.168.10.10
```

Example Configurations

This section provides some example configurations for the following:

PIM-SSM with the default multicast group and IGMPv3

```
service pim
!
ip domain-lookup
!
no service dhcp-server
!
ip multicast-routing
!
spanning-tree mode rstp
!
no lacp global-passive-mode enable
!
switch 1 provision x950-28
switch 1 bay 1 provision xem2-12
!
vlan database
 vlan 10,20 state enable
!
ip igmp ssm-map static SSM-camera-1 192.168.10.10
!
ip pim ssm default
!
interface port1.0.1
 switchport
 switchport mode access
 switchport access vlan 10
!
interface port1.0.2
 switchport
 switchport mode access
 switchport access vlan 20
!
interface port1.0.3-1.0.37
 switchport
 switchport mode access
!
interface port1.1.1-1.1.12
 switchport
 switchport mode access
!
interface vlan10
 ip address 192.168.10.1/24
 ip pim sparse-mode
!
interface vlan20
 ip address 192.168.20.1/24
 ip igmp
 ip pim sparse-mode
!
line con 0
line vty 0 7
!
end
```

PIM-SSM with a non-default multicast group and IGMPv3

```
access-list standard V4-SSM-RANGE permit 224.10.0.1/16
!
service pim
!
vlan database
 vlan 10,20 state enable
!
ip igmp ssm range V4-SSM-RANGE
!
ip pim ssm range V4-SSM-RANGE
!
ip multicast-routing
!
vlan database
 vlan 10,20 state enable
!
ip igmp ssm range V4-SSM-RANGE
!
ip pim ssm range V4-SSM-RANGE
!
interface port1.0.1
 switchport
 switchport mode access
 switchport access vlan 10
!
interface port1.0.2
 switchport
 switchport mode access
 switchport access vlan 20
!
interface vlan10
 ip address 192.168.10.1/24
 ip pim sparse-mode
!
interface vlan20
 ip address 192.168.20.1/24
 ip igmp
 ip pim sparse-mode
```

SSM default configuration IPv6

```
service password-encryption
!
hostname multicast-router
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
ipv6 access-list standard ssm-camera-1 permit ff35::1/128
!
no service ssh
!
autoboot enable
!
no service telnet
!
service http
!
no clock timezone
!
snmp-server
!
aaa authentication enable default local
aaa authentication login default local
!
stack virtual-chassis-id 2124
!
service pim6
!
ip domain-lookup
!
no service dhcp-server
!
ip multicast-routing
!
ipv6 multicast-routing
!
spanning-tree mode rstp
!
service power-inline
no lacp global-passive-mode enable
!

#[continued on next page...]
```

```
#[config continues...]

switch 1 provision x930-52
!
vlan database
 vlan 10,20 state enable
!
ipv6 pim ssm default
!
interface port1.0.1
 switchport
 switchport mode access
 switchport access vlan 10
!
interface port1.0.2
 switchport
 switchport mode access
 switchport access vlan 20
!
interface port1.0.3-1.0.50
 switchport
 switchport mode access
!
interface port1.0.51-1.0.52
 stackport
!
interface vlan10
 ipv6 address 2001:abcd:cafe:1a::1/64
 ipv6 pim sparse-mode
!
interface vlan20
 ipv6 address 2001:abcd:cafe:1b::1/64
 ipv6 mld
 ipv6 pim sparse-mode
!
ipv6 forwarding
ipv6 mld ssm-map static ssm-camera-1 2001:abcd:cafe:1a::10
!
line con 0
line vty 0 7
!
end
```

SSM non-default configuration IPv6

```
service password-encryption
!
hostname multicast-router
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
ipv6 access-list standard V6-SSM-RANGE permit ff03::/16
!
!
no service ssh
!
autoboot enable
!
no service telnet
!
service http
!
no clock timezone
!
snmp-server
!
aaa authentication enable default local
aaa authentication login default local
!
stack virtual-chassis-id 2124
!
service pim6
!
ip domain-lookup
!
no service dhcp-server
!
ip multicast-routing
!
ipv6 multicast-routing
!
spanning-tree mode rstp
!
no ipv6 mld ssm-map enable
service power-inline
no lacp global-passive-mode enable
!
switch 1 provision x930-52
!
vlan database
 vlan 10,20 state enable
!
ipv6 pim ssm range V6-SSM-RANGE
!
interface port1.0.1
 switchport
 switchport mode access
 switchport access vlan 10

#[continued on next page...]
```

```
#[config continues...]

!
interface port1.0.2
 switchport
 switchport mode access
 switchport access vlan 20
!
interface port1.0.3-1.0.50
 switchport
 switchport mode access
!
interface port1.0.51-1.0.52
 stackport
!
interface vlan10
 ipv6 address 2001:abcd:cafe:1a::1/64
 ipv6 pim sparse-mode
!
interface vlan20
 ipv6 address 2001:abcd:cafe:1b::1/64
 ipv6 mld
 ipv6 pim sparse-mode
!
ipv6 forwarding
!
line con 0
line vty 0 7
!
end
```

Monitoring

Here's some example output for the commands: **show ip pim sparse-mode mroute** and **show ip igmp groups detail**

```
awplus# show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 1
(S,G,rpt) Entries: 0
FCR Entries: 0
MRIB Msg Cache Hit: 0

(192.168.10.10, 224.10.0.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
 Local            1
 Joined           0
 Asserted Winner  0
 Asserted Loser   0
 Outgoing         1
  Interop    listener    rx-data     flags (ES,EDW,RXD,DAJ,EOE)
             0x00000000  0x00000000  0x00000001

multicast-router#show ip igmp groups detail

Interface:      vlan20
Group:          224.10.0.1
Flags:
Uptime:         00:01:38
Group mode:     Include ()
Flags:          00000084
Last reporter:  192.168.20.10
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)

Include Source List :
  Source Address  Uptime    v3 Exp    Fwd  Flags
  192.168.10.10   00:01:38  stopped   Yes
```

For information on PIM-SM monitoring commands, see the Protocol Independent Multicast - Sparse Mode (PIM-SM) Feature Overview and Configuration Guide

References

[1] S. Bhattacharyya, Ed., "An Overview of Source-Specific Multicast (SSM)," RFC 3569, Internet Engineering Task Force, July 2003. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc3569

C613-22137-00-REV A

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com