Technical Guide

WAN-LAN PIM Multicast Routing and LAN IGMP

FEATURE OVERVIEW AND CONFIGURATION GUIDE

Introduction

This guide describes WAN-LAN PIM Multicast Routing and IGMP on the LAN and how to configure WAN-LAN PIM multicast routing and LAN IGMP snooping.

The Allied Telesis Next Generation Firewalls (NGFWs) can perform routing of IPv4 and IPv6 multicast, using PIM-SM and PIM-DM. Also, switching interfaces of the NGFWs are IGMP aware, and will only forward multicast steams to these switch ports that have received reports.

IGMP snooping allows a device to only forward multicast streams to the links on which they have been requested.

PIM Sparse mode requires specific designated routers to receive notification of all streams destined to specific ranges of multicast addresses. When a router needs to get hold of a given group, it sends a request to the designated Rendezvous Point for that group. If there is a source in the network that is transmitting a stream to this group, then the Rendezvous Point will be receiving it, and will forward it to the requesting router.

AlliedWare Plus™ OPERATING SYSTEM

Contents

Products and software version that apply to this guide

This guide applies to AlliedWare Plus™ Firewall, running version **5.4.5** or later.

However, implementation varies between products. To see whether a product supports a feature or command, see the following documents:

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

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

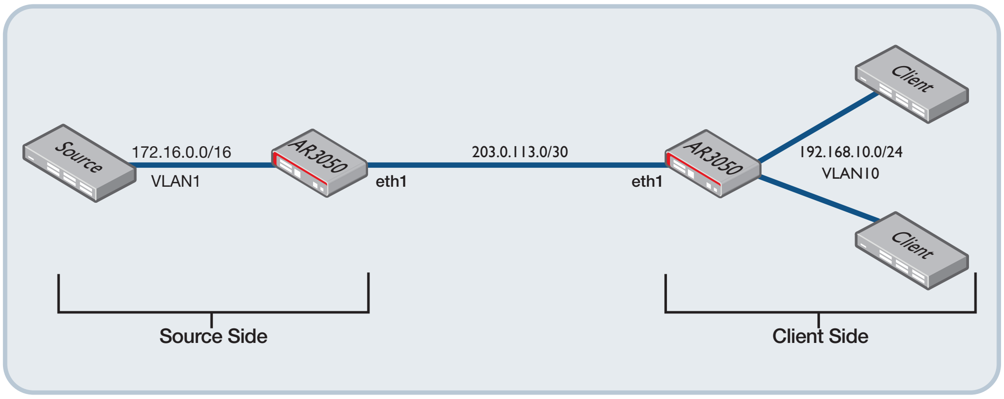
Feature support may change in later software versions. For the latest information, see the above documents.

Configuring WAN-LAN PIM Multicast Routing and LAN IGMP Snooping

Topology

The diagram below shows two Allied Telesis NGFWs, connected via an Ethernet link. One of the NGFWs is attached to a multicast source, and the other is attached to two clients that wish to receive streams from that source.

Figure 1: Topology of Allied Telesis NGFWs



Configuration notes

Before multicast routing using PIM-SM can work, there must be full unicast connectivity throughout the network. Since a static rendezvous point (RP) will be used here, a loopback interface is configured to provide the RP's IP address. Any interface address reachable throughout the network can be used for the RP address, but best practice is to use a loopback as loopback interfaces are always up and reachable through any physical interface (when combined with a suitable unicast routing design). In this example static routes are used for simplicity.

Multicast traffic can be routed via VLAN, Virtual Tunnel Interface (VTI), and Ethernet interfaces. IGMP (including querrier and Snooping) is supported via VLAN interfaces only.

Basic configuration of client side NGFW:

```
vlan database
 vlan 10 state enable
!
interface port1.0.1-1.0.2
 switchport access vlan 10
!
interface eth1
 ip address 203.0.113.2/30
!
interface vlan10
 ip address 192.168.10.1/24
!
ip route 0.0.0.0/0 203.0.113.1
```

Basic configuration of source side NGFW:

```
interface eth1
 ip address 203.0.113.1/30
!
interface vlan1
 ip address 172.16.0.1/16
!
interface lo
 ip address 10.0.0.1/32
!
ip route 192.168.0.0/16 203.0.113.2
```

Multicast configuration

Client side

Step 1: Enable Layer 3 IP multicast routing.

```
awplus#configure terminal
awplus(config)#ip multicast-routing
```

Step 2: Enable PIM Sparse-Mode multicast routing on eth1.

```
awplus(config)#interface eth1
awplus(config-if)#ip pim sparse-mode
awplus(config-if)#exit
```

Step 3: Enable IGMP querier on VLAN10.

```
awplus(config)#interface vlan10
awplus(config-if)#ip igmp
```

Step 4: Enable PIM Sparse-Mode multicast routing on VLAN10.

```
awplus(config-if)#ip pim sparse-mode
awplus(config-if)#exit
```

Step 5: Specify a static Rendezvous Point (RP) address to be used for PIM.

```
awplus(config)#ip pim rp-address 10.0.0.1
```

Source side

Step 1: Enable Layer 3 IP multicast routing.

```
awplus(config)#ip multicast-routing
```

Step 2: Enable PIM Sparse-Mode multicast routing on eth1.

```
awplus(config)#interface eth1
awplus(config-if)#ip pim sparse-mode
```

Step 3: Enable PIM Sparse-Mode multicast routing on interface vlan1.

```
awplus(config)#interface vlan1
awplus(config-if)#ip pim sparse-mode
```

Step 4: Specify a static Rendezvous Point (RP) address on the local interface.

```
awplus(config)#interface lo
awplus(config-if)#ip pim sparse-mode
```

Step 5: Specify the static Rendezvous Point (RP) address to be used for PIM.

```
awplus(config)#ip pim rp-address 10.0.0.1
```

Show information

To see which interfaces are enabled for PIM, enter the **show ip pim sparse-mode interface** command.

Here is an example output.

```
awplus#show ip pim sparse-mode interface
Total configured interfaces: 3   Maximum allowed: 100
Total active interfaces:     2

Address          Interface VIFindex Ver/   Nbr    DR          DR
                                   Mode   Count  Prior
203.0.113.2      eth1      2        v2/S   1     1       203.0.113.2
192.168.10.1     vlan10    4         v2/S  0     1       192.168.10.1
```

To see which interfaces are enabled for IGMP, enter the **show ip igmp interface** command. On the 172.16.0.0/16 subnet on the source side, NGFW is a multicast server which is sending a UDP multicast stream to 224.1.1.1.

Using the **show ip pim sparse-mode mroute detail** command on the source side NGFW shows this multicast stream has been received:

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

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

(172.16.0.2, 224.1.1.1) Uptime: 00:03:01
  Flags/Ext-Flags: 0x04/0x03
  RPF nbr: None, RPF idx: None
  Upstream:
   State: JOINED, SPT Bit: on, JT: off, KAT Expiry: 29 secs
   Macro state: Join Desired,
  Downstream:
  Interop    listener    rx-data     flags (ES,EDW,RXD,DAJ,EOE)
             0x00000000  0x00000000  0x00000001
(172.16.0.2, 224.1.1.1, rpt) Uptime: 00:03:01
  Flags/Ext-Flags: 0x08/0x00
  RP: 0.0.0.0, RPF nbr: None, RPF idx: None
  Upstream:
   State: RPT NOT JOINED, OT: off
   Macro state:
  Downstream:
  Interop    listener    rx-data     flags (ES,EDW,RXD,DAJ,EOE)
             0x00000000  0x00000000  0x00000001
```

The client side device has not learned of the stream yet because the rendezvous point is on the source side NGFW. Because the client side NGFW has not yet sent a PIM join message to the source side NGFW, the source side NGFW is not sending multicast across the link to the client side NGFW. Even though a large number of multicast packets have been received on VLAN1, none have been transmitted on eth1.

```
awplus#show interface vlan1 | include input
   input packets 2574156, bytes 648687312, dropped 0, multicast packets
2574156
awplus#
awplus#show interface eth1 | include output
    output packets 57, bytes 9052
```

To trigger PIM to route the multicast through, a client needs to report its interest in the stream via an IGMP Report packet. If a client attached to the VLAN10 interface of the client side NGFW sends a report for group 224.1.1.1, then this can be seen in the **show ip igmp groups** command:

```
awplus#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface          Uptime   Expires  Last Reporter
224.1.1.1        vlan10             00:00:06 00:04:14 192.168.10.10
```

This IGMP Report triggers PIM on the client side NGFW to add a (*,G) entry for the multicast group, and send the PIM join message to the source side NGFW, which will trigger it to send the multicast.

Output of the **show ip pim sp mroute detail** command is shown below:

```
awplus#show ip pim sp mroute detail
IP Multicast Routing Table

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

(*, 224.1.1.1) Uptime: 00:00:17
  Flags/Ext-Flags: 0x02/0x00
  RP: 10.0.0.1, RPF nbr: 203.0.113.1, RPF idx: eth1
  Upstream:
   State: JOINED, SPT Switch: Enabled, JT Expiry: 43 secs
   Macro state: Join Desired,
  Downstream:
   vlan10:
     State: NO INFO, ET: off, PPT: off
     Assert State: NO INFO, AT: off
      Winner: 0.0.0.0, Metric: INF, Pref: INF, RPT bit: on
     Macro state: Could Assert, Assert Track
  Local Olist:
   vlan10
  Interop    listener    rx-data     flags (ES,EDW,RXD,DAJ,EOE)
             0x00000000  0x00000000  0x00000001
(172.16.0.2, 224.1.1.1) Uptime: 00:00:17
  Flags/Ext-Flags: 0x04/0x03
  RPF nbr: 203.0.113.1, RPF idx: eth1
  Upstream:
   State: JOINED, SPT Bit: on, JT Expiry: 43 secs, KAT Expiry: 193 secs
   Macro state: Join Desired,
  Downstream:
  Inherited Olist:
   vlan10
  Interop    listener    rx-data     flags (ES,EDW,RXD,DAJ,EOE)
             0x00000000  0x00000000  0x00000001
(172.16.0.2, 224.1.1.1, rpt) Uptime: 00:00:17
  Flags/Ext-Flags: 0x08/0x00
  RP: 10.0.0.1, RPF nbr: 203.0.113.1, RPF idx: eth1
  Upstream:
   State: NOT PRUNED, OT: off
   Macro state: RPT Join,
  Downstream:
  Interop    listener    rx-data     flags (ES,EDW,RXD,DAJ,EOE)
             0x00000000  0x00000000  0x00000001
```

The source side device can be seen now forwarding the multicast streams to the client side device, as shown by the output multicast packets on eth1, towards the client side device:

```
awplus#show interface vlan1 | include input
    input packets 10898140, bytes 2746331280, dropped 0, multicast
packets 10898140
awplus#show interface eth1 | include output
    output packets 414040, bytes 104321206
```

IGMP snooping

The functionality of IGMP snooping (enabled by default) can also be seen here. There are two clients in VLAN 10, but only one of them has reported interest in the 224.1.1.1 multicast stream. The behaviour of an Ethernet switch without IGMP snooping is to flood multicast streams to all ports in a VLAN, similar to broadcasts. IGMP snooping prevents this by limiting the transmission of multicast streams only to the interested client.

```
awplus#show ip igmp snooping statistics interface vlan10
IGMP Snooping statistics for vlan10
Interface:      vlan10
Group:          224.1.1.1
Flags:
Uptime:         00:00:19
Group mode:     Exclude (Expires: 00:04:00)
Last reporter:  192.168.10.10
Source list is empty

Port member list:
port1.0.1 - 241 secs (if)
```

This ensures that only the client that requested the stream, (the client attached to port1.0.1) receives the stream, and not the client that has not requested any streams (the one attached to port1.0.2), as shown by the output packet counters for these two ports:

```
awplus#show interface port1.0.1 | include output
    output packets 1573994, bytes 402730688, multicast packets 1573991
broadcast packets 3
awplus#
awplus#show interface port1.0.2 | include output
    output packets 1127, bytes 76812, multicast packets 1124 broadcast
packets 3
```

The role of maintaining IGMP group membership falls on the querier. This is elected based on the highest IP address of the IGMP-enabled routers on a given Layer 2 domain. In this case the client-side device is the querier because it is the only IGMP enabled router on VLAN 10:

```
awplus#show ip igmp interface vlan10

Interface vlan10 (Index 310)
 IGMP Enabled, Active, Querier, Version 3 (default)
 Internet address is 192.168.10.1
 <output omitted>
```

C613-22042-00 REV A

Allied Telesis the **solution :** the **network**

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