Multicast Listener Discovery (MLD)

FEATURE OVERVIEW AND CONFIGURATION GUIDE

Introduction

Multicast Listener Discovery (MLD) is used to exchange membership status information between members of IPv6 multicast groups on a network segment and IPv6 routers that support multicasting.

Host membership in a multicast group is reported by individual member hosts, and membership status is periodically polled by multicast routers.

- MLD is defined in RFC 2710, Multicast Listener Discovery (MLD) for IPv6.
- MLDv2 is defined in RFC 3810, Multicast Listener Discovery Version 2 (MLDv2) for IPv6.

AlliedWare Plus supports both RFC 2710 for MLD and RFC 3810 for MLDv2.

Products and software version that apply to this guide

This guide applies to all AlliedWare Plus™ products, running version 5.4.4 or later.

Feature support may change in later software versions. For the latest information, 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.
Contents

Introduction............................................................................................................................................................................. 1
  Products and software version that apply to this guide................................................................................................. 1
  Related documents................................................................................................................................................................. 2
MLD Overview........................................................................................................................................................................ 3
  MLDv1 packets......................................................................................................................................................................... 4
MLD Snooping........................................................................................................................................................................... 4
  AlliedWare Plus switches support MLD Snooping........................................................................................................... 5
  Limitation of MLD on AlliedWare Plus switches............................................................................................................ 5
Configuration Examples .......................................................................................................................................................... 6
  Simple MLD configuration..................................................................................................................................................... 6
  MLD Snooping configuration examples............................................................................................................................ 6
  Configuring a multicast router port statically................................................................................................................... 7
  Enabling MLD Snooping fast-leave processing on an interface........................................................................................ 8
  Configuring MLD Snooping report suppression on an interface.................................................................................... 8

Related documents

The following documents give more information about the IPv6 multicasting features on AlliedWare Plus products:

- the Multicasting Feature Overview and Configuration Guide
- the Command Reference for each product

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

Multicast Listener Discovery (MLD) is the IPv6 equivalent of Internet Group Management Protocol (IGMP). Fortunately, as with most aspects of IPv6 routing, the features and operation of MLD closely resembles those of its IPv4 equivalent. In fact, the RFCs defining MLD quite explicitly state that they are adaptations of IGMP to IPv6.

The packet types, timers, actions etc. in MLD are very much the same as those in IGMP.

As with IGMP, there are multiple versions of MLD. Because MLD has been defined more recently than IGMP, the version numbers of MLD are actually one behind the version numbers of IGMP.

This means that:
- MLDv1 (RFC2710) is equivalent to IGMPv2.
- MLDv2 (RFC3810) is equivalent to IGMPv3.

The basic actions that occur in the MLD protocol are:
1. Hosts that wish to receive certain multicast groups send out MLD reports requesting the groups.
2. Routers and switches that receive these reports create forwarding entries to forward the groups in question out via the interface on which the report was received.
3. Routers send out MLD queries at intervals, to find out who still wants to receive each group.
4. If a router or switch has not recently seen any reports requesting a given group on a given interface, it will remove the forwarding entry that is delivering that group to that interface.

In the actions above, a router is an MLD querier. The other switches in the network (i.e. those between the listening hosts and the querier) will perform MLD snooping.

The main duties of an MLD querier are to:
- Send general queries, to find out who is still listening.
- Handle incoming reports, creating forwarding entries for the groups requested in those reports. If the MLD querier is also acting as a Layer 3 router of IPv6 multicast (using PIMv6 or similar), the MLD query process also needs to tell the Layer 3 multicast routing process to send upstream requests for the groups being requested in incoming MLD reports.
- Handle incoming Done messages. Removing the forwarding entry for the groups specified in the Done message, after first checking that no other host on the same interface is still listening to that group.
In addition, a querier has to:

- Listen for incoming queries from other queriers that might be operating in the same Layer 2 network. If the querier receives a query from a device with a lower IP address, then it has to stop operating as a querier, and let the lower-address device operate as the querier for the local network.
- Time out forwarding entries for which no reports have been received recently.

As with a lot of the signaling packets in IPv6, MLD packets are ICMPv6 packets. The different types of MLD packets have different ICMPv6 type values, as shown in the table below.

The source address of MLD packets is the link-local address of the device sending the packet (in MLDv2, it is actually permissible to send MLD packets with an all-zeros source address if the link-local address has not yet been calculated).

MLD packets always have a hop-count of 1.

MLD packets contain a Hop-by-Hop Options extension header that includes the Router Alert Option. The effect of this option is that all routers need to process MLD packets, irrespective of whether the router believes it is actively listening for the multicast address to which the MLD packet is destined.

### MLDv1 packets

Table 1: MLDv1 packet types and address information

<table>
<thead>
<tr>
<th>PACKET TYPE</th>
<th>SOURCE ADDRESS</th>
<th>DEST ADDRESS</th>
<th>ICMP TYPE</th>
<th>MULTICAST ADDRESS IN PACKET</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Query</td>
<td>Sender’s link-local address</td>
<td>FF02::1</td>
<td>130</td>
<td>::</td>
</tr>
<tr>
<td>Multicast address-and-source-specific Query</td>
<td>Sender’s link-local address</td>
<td>The specific group address being queried about</td>
<td>130</td>
<td>The specific group address being enquired about</td>
</tr>
<tr>
<td>Multicast address-and-source-specific Query</td>
<td>Sender’s link-local address</td>
<td>The specific group address being queried about</td>
<td>130</td>
<td>The specific group address being enquired about</td>
</tr>
<tr>
<td>Report</td>
<td>Sender’s link-local address</td>
<td>FF02::16</td>
<td>143</td>
<td>Multiple multicast addresses</td>
</tr>
</tbody>
</table>
MLD Snooping

As mentioned above, the switches that lie on the path between the hosts and the MLD router also have a role in controlling the forwarding of IPv6 multicast. A goal with multicast forwarding is always to forward the multicast packets only to those network segments where they are required.

Hence, it is valuable if the switches on the path between a multicast router and the listening hosts know which of their ports are directed towards the hosts that are members of given multicast groups. Then, they can forward the data for those groups only out the relevant ports, and not waste bandwidth on the links connected to ports that are not directed towards members of the group in question.

To achieve this, the switches keep track of the MLD packets passing through them - they note when a request to join a given group arrives on a given port, and when hosts announce their intention to leave given groups. Based on the information they glean from these passing MLD packets, they can maintain a table of which groups need to be forwarded out which ports. This process is known as MLD Snooping.

AlliedWare Plus switches support MLD Snooping

MLD Snooping is enabled by default globally for the switch. It can be enabled and disabled on a per-VLAN basis.

MLD Snooping makes a distinction between Member ports, which are ports connected to members hosts, and Router ports, which are ports connected to, or directed towards, a Layer 3 router or a Layer 3 switch.

Limitation of MLD on AlliedWare Plus switches

There is a 100 MLD interface limit when applying MLD commands to multiple VLANs. Only the first 100 VLANs have the required multicast structures added to the interfaces that allow multicast routing.

MLD requires memory for storing data structures, as well as the hardware tables to implement hardware routing. As the number of ports, VLANs, static and dynamic groups increases then more memory is consumed. You can track the memory used for MLD with the command:

```
awplus# show memory pools nsm | grep MLD
```

Static and dynamic Link Aggregation groups, ports and VLANs are not limited for MLD. For VLANs, this allows you to configure MLD across more VLANs with fewer ports per VLAN, or fewer VLANs with more ports per VLAN. For dynamic (LACP) LAGs, you can configure MLD across more LAGs with fewer ports per LAG, or fewer LAG groups with more ports per LAG.
Configuration Examples

Simple MLD configuration

Configuring MLD on interface vlan2

```
! ipv6 forwarding 
!
interface vlan2
  ipv6 address 2001:0db8::12:252/64
  ipv6 enable
  ipv6 mld
!
```

Note: IPv6 must be enabled on an interface with the `ipv6 enable` command, IPv6 forwarding must be enabled globally for routing IPv6 with the `ipv6 forwarding` command.

Note: The IPv6 addresses shown use the address space 2001:0db8:/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical networks (other than for testing purposes) nor should they appear on any public network.

MLD Snooping configuration examples

Enabling the MLD Snooping Querier on an interface

Use the MLD Snooping Querier feature to provide an MLD Querier in a VLAN where PIM-SMv6 and MLD are not configured and whenever you do not need to route IPv6 multicast traffic. You can configure the switch to generate MLD queries on a VLAN interface if multicast routing is not enabled. For each VLAN that is connected to switches that use MLD Snooping to control multicast traffic, configure one switch as the MLD Snooping Querier.

To enable and show MLD Snooping Querier on VLAN interface vlan2, enter the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping querier
awplus(config-if)# exit
awplus(config)# exit
awplus# show ipv6 mld interface vlan2
```

Note that the MLD Snooping Querier is configured in Interface Configuration mode only. You cannot configure MLD Snooping Querier globally for all VLAN interfaces on a switch.
Enabling MLD Snooping globally and on an interface

To globally enable and show MLD Snooping on the switch, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 mld snooping
awplus(config)# exit
awplus# show ipv6 mld interface
```

Note that entering the command `show ipv6 mld interface` without an optional interface parameter displays MLD information for all configured interfaces globally on the switch.

To enable and show MLD Snooping on VLAN interface vlan2, enter the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping
awplus(config-if)# exit
awplus(config)# exit
awplus# show ipv6 mld interface vlan2
```

Note that entering the command `show ipv6 mld interface vlan2` with the optional interface parameter displays MLD information for that specified configured interface on the switch.

Configuring a multicast router port statically

MLD snooping will learn which ports are connected to IPv6 Multicast routers (by recognizing incoming packets that are characteristic of IPv6 routers - MLD queries, PIMv6 packets, OPSFv3 packets, and so on). Such ports are designated as Router Ports, and ALL IPv6 multicast groups are forwarded to these ports. For various reasons, there may be cases where you do not simply want to rely on the learning of MLD Router ports, but wish to explicitly designate one or more ports to be MLD Router Ports.

To configure and show a static MLD Router port on VLAN interface vlan2, enter the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping mrouter interface port1.0.2
awplus(config-if)# exit
awplus(config)# exit
awplus# show ipv6 mld interface vlan2
```

Note the VLAN interface to the Multicast Router must be administratively up and the line protocol must be up to configure a static connection to a Multicast Router on the VLAN.
Enabling MLD Snooping fast-leave processing on an interface

MLD fast-leave is a mode whereby MLD (and snooping) decides to stop forwarding a given group to a given port as soon as the port receives an announcement that a host connected to the port is leaving the group. By default, the switch follows the standard group-specific query process, to decide if any other hosts downstream of the port are still listening for the group in question.

However, if you know that there is only one host downstream of a port, there is no need to query whether any other hosts on that are still listening to the group, as there are no other hosts on that port. Hence, fast-leave can be used in that case, to speed up the reaction to MLD leave announcements.

To enable and show MLD Snooping Fast-Leave Processing on VLAN interface vlan2, enter the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping fast-leave
awplus(config-if)# exit
awplus(config)# exit
awplus# show ipv6 mld interface vlan2
```

Configuring MLD Snooping report suppression on an interface

MLD snooping report suppression is a feature that increases the extent to which MLD snooping interferes with the flow of MLD packets. If report suppression is not enabled, then MLD snooping simply lets MLD packets pass through, and keeps note of which packets have passed through. When report suppression is enabled, MLD snooping actively works to reduce the number of MLD packets that are forwarded to the querier (to take load off the querier).

If the snooper sees multiple reports arrive from downstream hosts, requesting membership of the same group, it will forward just one of these requests to the querier, and drop the rest - i.e. suppress the duplicated reports. Similarly, if the snooper receives a leave announcement on a port, but knows that there are other downstream hosts that are still members of the group in question, it will not forward the leave to the querier.
To enable and show MLD Snooping Report Suppression on VLAN interface vlan2, enter the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping report-suppression
awplus(config-if)# exit
awplus(config)# exit
awplus# show ipv6 mld interface vlan2
```