

How to configure IGMP snooping with unregistered multicast addresses such as Service Location Protocol (SLP)

Introduction

IGMP snooping enables the switch to forward multicast traffic intelligently, instead of flooding all ports in the VLAN.

With IGMP snooping, the switch listens to IGMP membership reports, queries and leave messages to identify the switch ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

IGMP snooping is performed at Layer 2 on VLAN interfaces automatically. By default, the switch will only forward traffic out those ports with multicast listeners, therefore it will not act as a simple hub and flood all multicast traffic out all ports.

Multicast is sometimes used to learn, or advertise to users, services available on their network through Directory Agents (DAs) or directly with Service Agents (SAs) using Service Location Protocol (SLP). User Agents (UAs) and SAs send multicast requests (224.0.1.35), to locate DAs on the network. UAs and SAs learn of DAs via periodic multicast (224.0.1.34) advertisements. There is no need for IGMP-joins to these addresses with SLP.



Directory Agent (DA)

A process which collects information from Service Agents to provide a single repository of service information in order to centralise it for efficient access by User Agents.

Service Agent (SA)

Advertises the location and attributes on behalf of services.

User Agent (UA)

A process working on the user's behalf to acquire service attributes and configuration. The User Agent retrieves service information from the Service Agents or Directory Agents.

As these addresses are not within the reserved multicast range, (i.e. multicast IP addresses, x.0.0.x), IGMP snooping will snoop this traffic and not forward it to all ports within the VLAN unless the switch receives an IGMP-join for this group, or you statically add an IGMP entry for these addresses into the IGMP table.

With the implementation of IGMP snooping in software release 2.6.1 of AlliedWare for Rapiet i, AT-8800, and AT-8700XL series switches (release 2.6.2 for AT-9800 series switches and SwitchBlade), you may see that unregistered multicast traffic is no longer switched/flooded to all ports within a VLAN.

This can cause inconvenience if you are upgrading to software release 2.6.1 or later, and your service advertisements are no longer promulgated through the network.

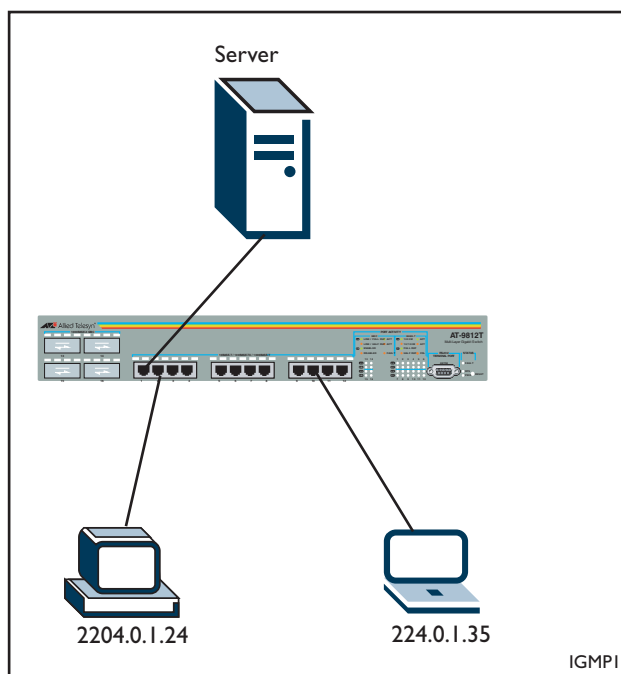
If you want to advertise or learn services via multicast and you still want to have IGMP snooping enabled to snoop other multicast traffic so it's not switched/flooded through your network then you need to configure static IGMP entries on the switch.

Configuration example

Figure 1 shows a server allowing two PCs access to Service Location Protocol addresses 224.0.1.24 and 224.0.1.35 by adding static IGMP entries to its table.

You have to have an IP interface associated with the VLAN that you are enabling IP IGMP on before you configure IP IGMP.

Figure 1: Illustration showing PCs having access to SLP addresses



1. Associate an IP interface with VLAN1

```
ADD IP INT=VLAN1 IP=x.x.x.x
```

2. Enable IGMP on the switch

```
ENABLE IP IGMP
```

3. Enable IGMP on VLAN1

This must be done before the static IGMP association is created.

```
ENABLE IP IGMP INTERFACE=VLAN1
```

4. Create the static IGMP association

The multicast data for the group specified by the DESTINATION parameter will be forwarded over the ports specified by the PORT parameter. If the PORT parameter is not entered, the association will default to all ports belonging to the interface.

```
CREATE IP IGMP DESTINATION=224.0.1.24 INTERFACE=VLAN1
```

```
CREATE IP IGMP DESTINATION=224.0.1.35 INTERFACE=VLAN1
```

