



ADVANCED
NETWORK DEVICES

Multicast Network Configuration

Version 1.0

6/18/2025

© 2025 ADVANCED NETWORK DEVICES

3820 NORTH VENTURA DR.

ARLINGTON HEIGHTS, IL 60004

U.S.A

ALL RIGHTS RESERVED

Proprietary Notice and Liability Disclaimer

The information disclosed in this document, including all designs and related materials, is the valuable property of Digital Advanced Network Devices and/or its licensors. Advanced Network Devices and/or its licensors, as appropriate, reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use, and sales rights thereto, except to the extent said rights are expressly granted to others.

The Advanced Network Devices product(s) discussed in this document are warranted in accordance with the terms of the Warranty Statement accompanying each product. However, actual performance of each product is dependent upon factors such as system configuration, customer data, and operator control. Since implementation by customers of each product may vary, the suitability of specific product configurations and applications must be determined by the customer and is not warranted by Advanced Network Devices.

To allow for design and specification improvements, the information in this document is subject to change at any time, without notice. Reproduction of this document or portions thereof without prior written approval of Advanced Network Devices is prohibited.

Static Electric Warning



TROUBLESHOOTING AND ADDITIONAL RESOURCES

User Support: <https://www.anet.com/user-support/>
Technical Resources: <https://www.anetd.com/user-support/technical-resources/>
AND Legal Disclaimer: <https://www.anetd.com/legal/>

OVERVIEW

Multicast is a bandwidth-efficient method of delivering the same data to multiple receivers simultaneously. Our application, ClockWise Campus, leverages multicast to transmit audio streams to ANetD devices for playback during Notifications and Live Audio as well as auto-discover devices on the network. This app note provides general guidance to configuring multicast on Cisco devices.

While many managed switches support the multicast features and commands shown in this document, it is important to consult the documentation for your specific network hardware to ensure compatibility and correct implementation.

CLOCKWISE MULTICAST OPERATION

ClockWise Campus transmits multicast audio streams to ANetD devices for use in campus-wide Notifications and Live Audio. These streams fall into two main categories:

- **Dynamic Streams:** Created on demand by ClockWise Campus for Notifications and Live Audio. These streams are ephemeral and only active during the duration of the event. ClockWise uses multicast addresses 239.2.2.30 and 239.2.2.31 to generate Dynamic Streams.
- **Custom Permanent Streams:** Configured by administrators and can be used to serve specific zones, buildings, or use cases. These streams are persistent and assigned fixed multicast addresses and ports. ANetD devices will always listen for audio from defined Permanent Streams.
- ANetD devices come preconfigured with a Factory Default Permanent Stream, which uses multicast address 239.9.10.11:23456.

ClockWise Campus auto-discovers devices on the network using the multicast address 227.75.76.77 over UDP port 5543.

ESSENTIAL LAYER 2 CONFIGURATION FOR MULTICAST

The following subsections cover configuration and considerations for: IGMP Snooping, IGMP Snooping Per VLAN, and IGMP Querier.

IGMP SNOOPING

IGMP snooping allows for the switch to listen in on IGMP traffic between hosts and multicast routers, so it only forwards multicast traffic to ports where devices have explicitly joined a group.

To enable IGMP snooping globally use the *"ip igmp snooping"* command from global config mode.

To verify IGMP snooping is enabled globally on the switch, use the “*show ip igmp snooping*” command from user exec mode or “*do show ip igmp snooping*” command from global config mode:

```
SW2(config)#do sh ip igmp snoopin
Global IGMP Snooping configuration:
-----
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000
```

To verify if IGMP snooping is functioning, use command “*sh ip igmp snooping groups*”.

```
SW2#show ip igmp snooping groups
Vlan      Group                Type      Version  Port List
-----
30        224.0.1.116              igmp      v2       Fa1/0/31, Fa1/0/48
30        224.0.1.120              igmp      v2       Fa1/0/31, Fa1/0/48
30        224.20.20.20             igmp      v2       Fa1/0/31, Fa1/0/48
30        224.110.110.100          igmp      v2       Fa1/0/41, Fa1/0/48
30        227.75.76.77             igmp      v2       Fa1/0/31, Fa1/0/39,
                                   Fa1/0/41, Fa1/0/48
30        227.77.77.77            igmp      v2       Fa1/0/27, Fa1/0/48
30        232.9.10.11             igmp      v2       Fa1/0/31, Fa1/0/41,
                                   Fa1/0/48
30        239.2.2.30              igmp      v2       Fa1/0/31, Fa1/0/48
30        239.255.255.250         igmp      v2       Fa1/0/27, Fa1/0/48
```

IGMP SNOOPING PER VLAN

Multicast efficiency is typically managed per VLAN. Ensure snooping is enabled on the VLAN used by the ANetD devices.

Use the “*ip igmp snooping vlan {vlan_ID}*” command to enable IGMP Snooping Per VLAN.

Note: The Cisco devices being used in this document do not support this command. Instead, IGMP snooping can be enabled globally to accomplish the same result.

To verify configuration per VLAN use “*do show ip igmp snooping vlan {vlan_ID}*” from global config mode:

```
Vlan 30:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave  : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Robustness variable     : 2
Last member query count  : 2
Last member query interval : 1000
```

IGMP QUERIER

IGMP queries are needed to maintain multicast group membership. In most networks, a Layer 3 device—such as a router or a switch with an IP interface in the multicast VLAN—automatically serves as the IGMP querier. If one is present, no querier configuration is needed on the access switch.

In flat Layer 2 networks without a router or Layer 3 interface in the VLAN, multicast traffic may stop after a few minutes due to IGMP timeouts. To prevent this, the switch can act as a querier—but only if it has a VLAN interface (SVI) with an IP address and at least one active port in that VLAN.

To globally configure an IGMP querier, use the “*ip igmp snooping querier*” command from global config mode.

To verify IGMP querier configuration, use the “*show ip igmp snooping querier*” command.

```
SW2#sh ip igmp snooping querier
Vlan      IP Address      IGMP Version  Port
-----
30        10.10.200.254    v2            Fa1/0/48
110       10.10.200.254    v2            Switch
```

ESSENTIAL LAYER 3 CONFIGURATION FOR MULTICAST

The following subsections detail the configuration and key considerations for the multicast protocols used in Layer 3 networks: IGMPv2, IGMPv3, PIM, RPF, and RP. While IGMPv2 and IGMPv3 primarily handle group membership, they depend on other multicast protocols for full functionality, particularly for multicast routing and efficient traffic forwarding. Each protocol subsection will provide an overview of its purpose, key configurations, and considerations. The final subsection will explain how all the protocols integrate to enable efficient Layer 3 multicast routing and provide the necessary configurations for optimal multicast performance.

IGMPV2 AND IGMPV3 (INTERNET GROUP MANAGEMENT PROTOCOL)

IGMP manages multicast group membership by allowing hosts to signal their local router which multicast groups they wish to join or leave. This ensures that multicast traffic is only delivered to interested receivers, optimizing network bandwidth.

IGMPv2: Introduces Leave messages, enhancing group membership management by allowing hosts to notify routers when they no longer wish to receive multicast traffic for a group.

IGMPv3: Adds support for Source-Specific Multicast (SSM), enabling receivers to join multicast groups from specific sources only, providing more precise traffic filtering.

Considerations:

IGMPv2 is typically enabled by default on most Layer 3 devices.

Both IGMPv2 and IGMPv3 require IGMP Snooping to be enabled on Layer 2 switches to optimize multicast traffic forwarding.

PIM (PROTOCOL INDEPENDENT MULTICAST)

PIM is a multicast routing protocol that uses the unicast routing table to forward multicast traffic efficiently. It operates independently of any specific unicast routing protocol. There are two main PIM modes:

PIM Sparse Mode (PIM-SM): Uses a Shared Distribution Tree. It requires a Rendezvous Point (RP) to manage multicast group memberships prior to the sender multicasting data on the network. If the RP is missing, the Designated Router (DR) on the sender's local subnet will drop the traffic. Only routers with interested receivers forward multicast traffic. This quickly establishes an optimal path to forward multicast traffic.

Note: Cisco recommends using PIM Sparse Mode for new deployments and whenever possible.

PIM Dense Mode (PIM-DM): Uses a Source Distribution Tree. It initially floods multicast traffic from the sender to all routers in the topology which can result in the receiver getting two copies of the same multicast data. The routers that don't have receivers connected send prune messages to other routers in the topology to stop receiving multicast data. Eventually, an optimal path is built to forward multicast traffic. This process repeats whenever a multicast source starts streaming. This is referred to as, "flood and prune behavior" which can have an impact on network performance.

Consideration:

The command "*ip pim-sparse-dense-mode*" can also be issued to a router interface. This command tells the interface on the router to operate in sparse mode if possible. If it cannot, it will operate in dense mode. The purpose of this mode is to operate in dense mode just long enough to learn the IP address of the RP. Once the

RP is learned, the interface will operate in sparse mode. This is because the routers need to use multicast to identify the RP. However, the router can't learn the address of the RP if it's not running multicast.

RP (RENDEZVOUS POINT)

The RP is a key element in PIM Sparse Mode (PIM-SM). It serves as a central point where multicast sources and receivers meet to establish a multicast routing path. The RP helps manage group memberships and ensures multicast traffic is only sent to receivers that need it. The RP can be manually configured on every router interface in the multicast topology, or an Auto RP can be configured.

Why RP is Needed:

Multicast Group Management: The RP helps routers know where to send multicast traffic based on group memberships.

Traffic Forwarding: It sets up the initial multicast path (Shared Tree) before traffic is forwarded directly to receivers (Shortest Path Tree).

Required in PIM-SM: If the RP is missing, the DR on the sender's local subnet will drop the traffic.

Auto RP requires an RP and a Mapping Agent. A Mapping Agent listens to group 224.0.1.39 for any router announcing itself as an RP. The Mapping Agent then resolves any conflicts that might exist among the routers that want to become RPs and the Mapping Agent announces the multicast group RP mapping to the group 224.0.1.40. Auto RP requires router interfaces in the multicast topology to use the *"ip pim-sparse-dense-mode"* command.

RPF (REVERSE PATH FORWARDING)

RPF is a built-in check that makes sure multicast traffic is received on the correct interface—specifically, the one the router would use to reach the source. This helps prevent routing loops and ensures efficient forwarding. It's used automatically by multicast protocols like PIM and no manual configuration is typically needed.

LAYER 3 MULTICAST NETWORK CONFIGURATION

This final subsection covers the layer 3 multicast network configuration required to ensure efficient flow of multicast traffic on the network. This section assumes that IGMP Snooping and, if needed, an IGMP querier are setup in addition to unicast routing.

1. Enable multicast routing on all routers in the multicast routing topology with the *"ip multicast routing"* command. Use the *"show ip mroute"* command to verify the multicast routing table is built.

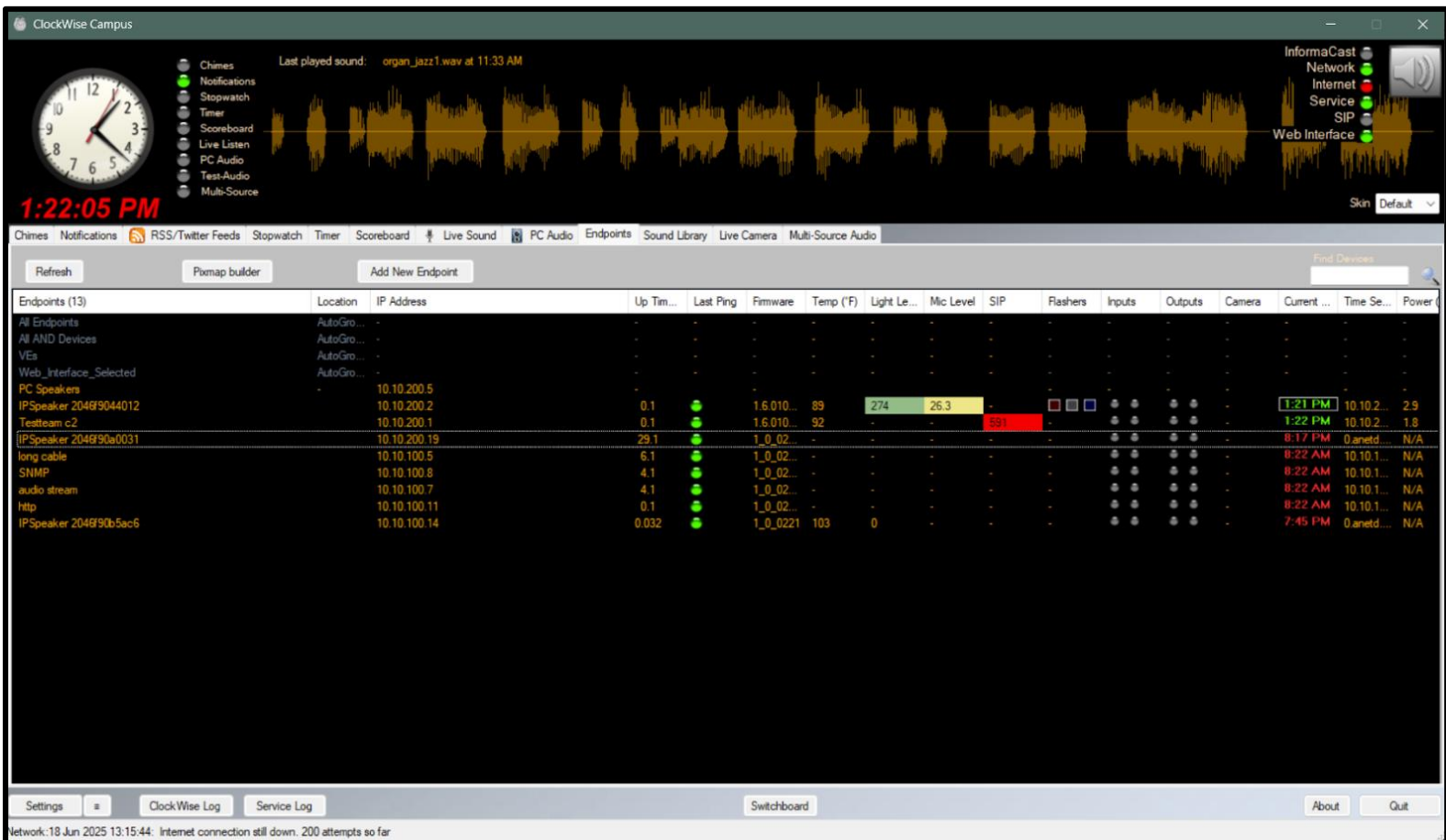
2. Apply PIM Sparse Mode to all Layer 3 interfaces that will participate in multicast routing (toward sources, receivers, and between routers). Use command *"ip pim sparse-mode"*.

```
interface GigabitEthernet0/0
ip address 10.10.10.2 255.255.255.252
ip pim sparse-mode
ip ospf network point-to-point
duplex auto
speed auto
```

3. Define the RP with command *"ip pim rp-address x.x.x.x"*. Ensure the RP is reachable by all routers that will be routing multicast traffic. Configure a static RP or use Auto-RP/BSR (Bootstrap Router) if needed.

```
ip pim rp-address 2.2.2.2
```

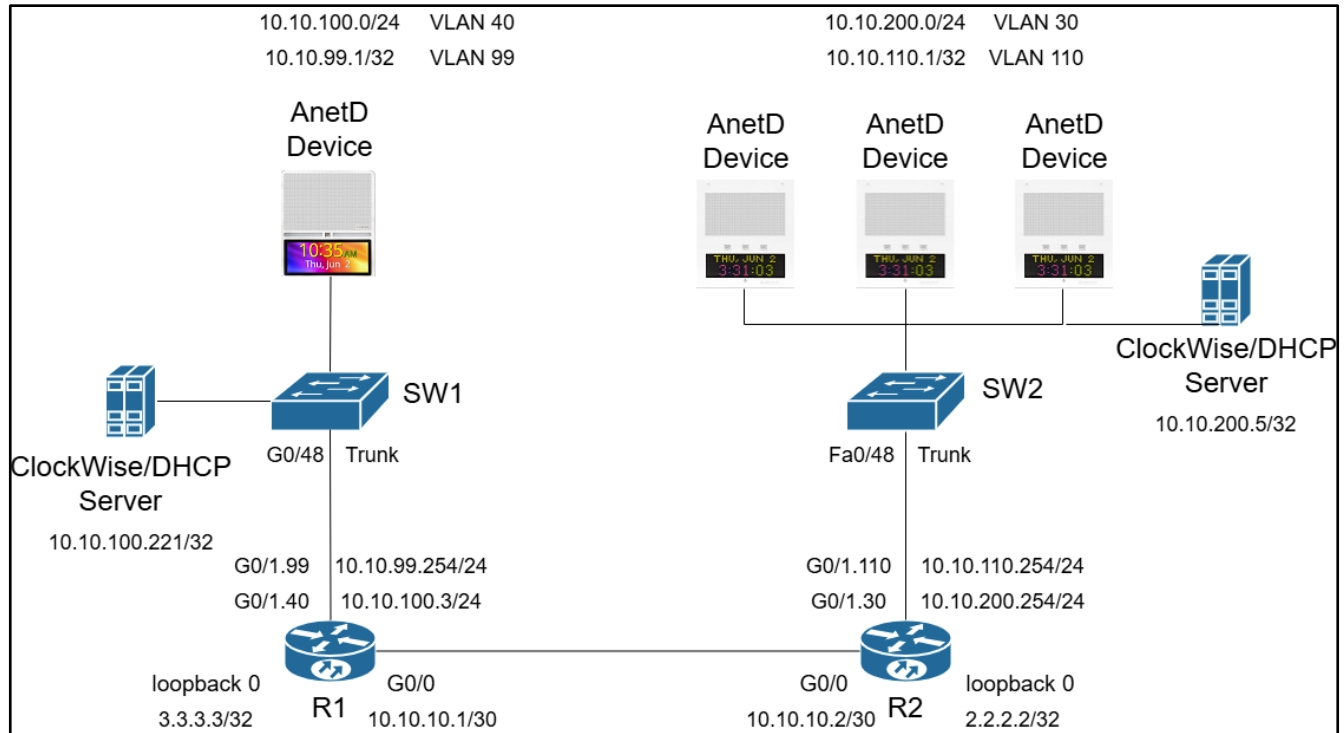
4. Once multicast routing has been configured properly, devices should auto populate in ClockWise from different subnets.



The screenshot displays the ClockWise Campus web interface. At the top, there's a clock showing 1:22:05 PM and a status bar with various icons like Chimes, Notifications, Stopwatch, Timer, Scoreboard, Live Listen, PC Audio, Test-Audio, and Multi-Source. A large audio waveform is visible in the background. Below the status bar, there's a navigation menu with options like Chimes, Notifications, RSS/Twitter Feeds, Stopwatch, Timer, Scoreboard, Live Sound, PC Audio, Endpoints, Sound Library, Live Camera, and Multi-Source Audio. The main content area shows a table of endpoints with columns for Location, IP Address, Up Time, Last Ping, Firmware, Temp (F), Light Le..., Mic Level, SIP, Flashers, Inputs, Outputs, Camera, Current ..., Time Se..., and Power. The table lists 13 endpoints, including various speakers and network devices. At the bottom, there are buttons for Settings, ClockWise Log, Service Log, Switchboard, About, and Quit. A status message at the very bottom indicates a network connection issue: "Network: 18 Jun 2025 13:15:44: Internet connection still down. 200 attempts so far".

Endpoints (13)	Location	IP Address	Up Tim...	Last Ping	Firmware	Temp (F)	Light Le...	Mic Level	SIP	Flashers	Inputs	Outputs	Camera	Current ...	Time Se...	Power (
All Endpoints	AutoGro...	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
All AND Devices	AutoGro...	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
VEs	AutoGro...	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Web_Interface_Selected	AutoGro...	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
PC Speakers	-	10.10.200.5	-	-	-	-	-	-	-	-	-	-	-	-	-	-
IPSpeaker 2048/9044012	-	10.10.200.2	0.1	1:21 PM	1.6.010...	89	274	26.3	-	-	-	-	-	1:21 PM	10.10.2...	2.9
Testteam c2	-	10.10.200.1	0.1	1:22 PM	1.6.010...	92	-	-	531	-	-	-	-	1:22 PM	10.10.2...	1.8
IPSpeaker 2048/90a0031	-	10.10.200.19	29.1	8:17 PM	1.0_02...	-	-	-	-	-	-	-	-	8:17 PM	0.anetd...	N/A
long cable	-	10.10.100.5	6.1	8:22 AM	1.0_02...	-	-	-	-	-	-	-	-	8:22 AM	10.10.1...	N/A
SNMP	-	10.10.100.8	4.1	8:22 AM	1.0_02...	-	-	-	-	-	-	-	-	8:22 AM	10.10.1...	N/A
audio stream	-	10.10.100.7	4.1	8:22 AM	1.0_02...	-	-	-	-	-	-	-	-	8:22 AM	10.10.1...	N/A
http	-	10.10.100.11	0.1	8:22 AM	1.0_02...	-	-	-	-	-	-	-	-	8:22 AM	10.10.1...	N/A
IPSpeaker 2048/90b5ac6	-	10.10.100.14	0.032	7:45 PM	1.0_0221	103	0	-	-	-	-	-	-	7:45 PM	0.anetd...	N/A

Below is a reference image of the network topology used:



To learn more, below is a link to Cisco's IP Multicast Quick-Start Configuration Guide:

<https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/9356-48.html>

Summary of multicast related commands issued to the network devices in the topology:

SW1:

ip igmp snooping

ip igmp snooping querier 10.10.100.3

SW2:

ip igmp snooping

ip igmp snooping querier 10.10.200.254

R2:

```
ip multicast-routing
```

```
interface GigabitEthernet0/0
```

```
ip pim sparse-mode
```

```
interface GigabitEthernet0/1.30
```

```
ip pim sparse-mode
```

```
ip pim rp-address 2.2.2.2
```

R1:

```
ip multicast-routing
```

```
interface GigabitEthernet0/0
```

```
ip pim sparse-mode
```

```
interface GigabitEthernet0/1.40
```

```
ip pim sparse-mode
```

```
ip pim rp-address 2.2.2.2
```