IP Multicast Network Management Overview

Last updated: August 2007

This paper provides an overview of the instrumentation, tools, and solutions that enable the management of Cisco® IP multicast deployments. It is assumed that the reader is familiar with network management in general. Please visit www.cisco.com for additional information relating to the topics covered in this overview.

Introduction

The Cisco IP Next-Generation Network (IP NGN) architecture simplifies the development and deployment of advanced services while enabling service providers to lower capital and operational expenditures. The inherent efficiencies of a converged network reduce administrative overhead, and the architecture facilitates the integration of intelligence and instrumentation for efficient management. The Cisco IP NGN and Cisco networking solutions complement industry best practices and approaches encompassed by the OSI model for network management, which is sometimes referred to as the FCAPS model. The five facets of network management included in the FCAPS model are:

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management

The management of an IP multicast deployment, like any other network, requires that network managers have the tools and solutions to address these five facets. This paper overviews the underlying instrumentation built into Cisco IP multicast platforms to enable all five FCAPS categories. The Cisco tools and solutions that interface with the Cisco instrumentation, and are relevant to the management of IP multicast deployments, are also overviewed.

This paper focuses on the areas of fault, configuration, and performance management. The methods and solutions employed to monitor and control resource-usage accounting and security for an IP multicast deployment do not differ from any other network, and are, therefore, covered in other Cisco reference documents.

Instrumentation

Today's network devices include the intelligence to respond to queries from network management systems. Cisco devices support the Simple Network Management Protocol (SNMP), a part of the TCP/IP protocol suite, to access and collect information about network device status and performance, and support queries using MIB modules. For a complete explanation and illustration of MIB "trees," please refer to the Cisco paper, "IP Multicast Network Management," at: http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a00800d6b62.shtml.

Note that all standard management solutions, including many freeware programs and utilities, can poll MIBs and take advantage of information returned by syslogs.

Multicast MIBs

MIBs are standardized by the Internet Engineering Task Force (IETF). The three categories of IETF MIBs include:

- Standard MIBs, based on the current IETF draft
- Request for Comments (RFC) Experimental, based on a new idea that is under consideration (prior to a formal proposal)
- RFC Proposed Standard, based on a proposal that is being considered for inclusion in the standard

In addition to the IETF MIBs, Cisco Systems® has defined and implemented Cisco MIBs. These extend the management capabilities for IP multicast beyond the standard IETF capabilities. Cisco tools and management solutions use Cisco multicast MIBs to provide users with enhanced configuration and monitoring capabilities that take advantage of proprietary Cisco device features.

Cisco IOS® XR Software supports the MIBs listed below. Eventually, Cisco will offer MIB feature parity between Cisco IOS and Cisco IOS XR operating environments:

- CISCO-IETF-IPMROUTE-MIB, based on RFC 2932 with IPv6 support
- CISCO-IETF-PIM-MIB, based on RFC 2934 with IPv6 support
- CISCO-IETF-PIM-EXT-MIB, extensions to the PIM MIB to support Bidir, DR Priority
- IPV6-MLD-MIB, based on RFC 3019

The following MIBs are of particular interest for managing Cisco IP multicast networks:

- IGMP-STD-MIB: Based on RFC 2933, this MIB contains information for IPv4 multicast routers, such as:
  - IP address of Internet Group Management Protocol (IGMP) querier
  - IGMP version configured on the interface
  - IGMP cache
  - The hosts that are subscribed on a router interface

  The Cisco implementation of the IGMP-STD-MIB is one of the few Cisco MIBs that does support set/create configuration objects.
- PIM-MIB: Based on RFC 2934, PIM-MIB contains Protocol Independent Multicast (PIM) interface information, PIM neighbors, and rendezvous point (RP) information.
- IP-MROUTE-STD-MIB: Based on RFC 2932, it contains information about the status of multicast routing. The traffic statistics that can be collected using this MIB include packet counters per multicast route (in and out), and octet counters (in and out) per route.
- CISCO-IPMROUTE-MIB: Contains additional information (compared to the IP-MROUTE-STD-MIB) about multicast routes, such as event flags and traffic counters.
- CISCO-MVPN-MIB: Contains configuration and state information for multicast VPNs such as the name of multicast enabled VRFs and the dynamic mapping between customer multicast groups and Default/Data MDT groups.

Table 1 summarizes the multicast MIBs supported by Cisco devices. The “STD” MIBs are part of the IETF standard. The “CISCO” MIBs are Cisco extensions to the standard. Other MIBs are experimental or proposed IETF MIBs. Table 2 shows which releases of Cisco IOS Software support each of these MIBs.

Table 1. Cisco Supported Multicast MIBs

Category	MIBs	Features and Functions
IGMP	IGMP-MIB.my IGMP-STD-MIB.my	Status and usage for interfaces (each interface for which IGMP is enabled) and caches (for each IP multicast group).
IGMP Snooping	CISCO-IGMP-SNOOPING-MIB.my (Cisco Catalyst® OS only)	Status of IGMP Snooping protocol usage. A switch that implements IGMP Snooping listens to IGMP messages exchanged between hosts and routers, then provides selective transmission of multicast traffic based on the multicast group contained within each message.
Multicast Routing (Mroute)	IPMROUTE-MIB.my IPMROUTE-STD-MIB.my CISCO-IPMROUTE-MIB.my	Information about IP multicast groups (interfaces, number of packets sent to the group, timers, etc.).
Protocol Independent Multicast (PIM)	PIM-MIB.my CISCO-PIM-MIB.my	PIM interfaces, IP addresses, and status (frequency of joins and prunes, neighbors).
Multicast Source Discovery Protocol (MSDP)	MSDP-MIB.my	Objects used to remotely monitor MSDP speakers.
Multicast VPN (mVPN)	CISCO-MVPN-MIB.my	Multicast VPN configuration and state information such as the name of multicast enabled VRFs and the dynamic mapping between customer multicast groups and Default/Data MDT groups.

Table 2. Cisco IOS Software Support of Multicast MIBs

Cisco IOS Software Release	12.1E	12.2SX	12.3	12.4	12.0S
IGMP-MIB	Yes	Yes	No	No	Yes
IGMP-STD-MIB	No	No	Yes	Yes	No
MROUTE-MIB	Yes	No	No	No	No
MROUTE-STD-MIB[1]	No	Yes	Yes	Yes	Yes
CISCO-IPMROUTE-MIB	Yes	Yes	Yes	Yes	Yes
PIM-MIB	Yes	Yes	Yes	Yes	Yes
CISCO-PIM-MIB	Yes	Yes	Yes	Yes	Yes
MSDP-MIB	No	Yes	Yes	Yes	Yes
CISCO-MVPN-MIB[1]	No	Yes	No	Yes	Yes

Multicast MIBs and VRF Aware

MIBs that are not “VRF aware” will not be able to report on any Virtual Routing and Forwarding (VRF) events; they will only report on events in the default and global routing tables. Only provider-edge routers need to be VRF aware. These MIBs are not VRF aware: Mroute, PIM, MSDP, IGMP, and IGMP Snooping.

The mVPN MIB is VRF-independent and can be used to access VRF information.

Multicast Traps

SNMP traps are generated by managed devices to asynchronously report the occurrence of a specific event to a network management station (NMS). The multicast notification traps supported by Cisco devices fall into four categories (see Table 3).

[1] The CISCO-MVPN-MIB and MROUTE-STD-MIB are available in 12.2(33)SXH and 12.2(33)SRB

Table 3. Multicast Traps

Mroute	ciscoIpMRouteMissingHeartBeats
PIM	pimNeighborLoss ciscoPimRPMappingChange ciscoPimInvalidRegister ciscoPimInvalidJoinPrune ciscoPimInterfaceUp ciscoPimInterfaceDown
MSDP	msdpEstablished[2] msdpBackwardTransition
mVPN	ciscoMvpnMvrfChange

Traps can be enabled individually, or collectively, using SNMP commands.

Multicast Heartbeat

The Cisco Multicast Heartbeat monitoring utility provides a simple-to-use tool for confirming the basic status of a multicast network. Routers in the multicast network can be configured to send a trap when traffic stops within a critical group. The Heartbeat monitor confirms traffic stream activity.

The syntax for invoking the utility includes two instructions:

```
snmp-server enable traps ipmulticast
ip multicast heartbeat 224.0.1.53 1 1 10
```

The utility allows the user to:

- Set the router to send the traps.
- Set the group.
- Set the minimum number of intervals that must have traffic.
- Set the number of intervals to monitor.
- Set the length of intervals in seconds.

Syslogs

Cisco devices generate syslog messages. Defined by an industry standard, syslogs capture information for devices on a network, usually using UDP Port 514. A central syslog server aggregates all device messages and alerts, and stores them or prints them using a simple configuration file format. Cisco devices can send messages to a UNIX-style syslog service. Syslog information is useful both in routine troubleshooting and for handling incidents on the network. Many service providers use syslog messages to monitor capacity (by customer or by network connection) as part of their routine capacity planning and adjustment efforts. For example, the “MDT reuse” syslog lets providers monitor VPNs to determine the ones that may need more addresses for data multicast distribution trees (MDTs).

There are dozens of multicast syslog messages in these categories:

- Mroute (multicast routes), used to detect when the number of multicast routes exceeds a specified threshold
- MDS (Multicast Distributed Switching)

[2] Supported in latest images. 12.4T, 12.0S, 12.2SXH, 12.2SRB. See CSCek00661 using the Cisco.com Bug Toolkit on Cisco.com for more details: http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

- PIM (Protocol Independent Multicast)
- AUTORP (automatic rendezvous point)
- MDT (multicast distribution tree)
- MSDP (Multicast Source Discovery Protocol)
- DVMRP (Distance Vector Multicast Routing Protocol)
- MCAST (Layer 2 multicast)

Service providers can use a correlation engine to collect and process syslog messages.

The PIM-1-INVALID_RP_REG syslog is particularly useful for Multicast networks. This message indicates that a designated router (DR) is trying to register a source with a router that is not configured to be the RP. Either the DR has the wrong RP address configured or the RP is not configured correctly.

A new syslog command—the “ip pim log-neighbor-changes” command—creates an alert when the status of a PIM neighbor changes (similar to the existing log messages for OSPF, EIGRP and BGP). This command is supported by the most recent releases of Cisco IOS Software.

Note that all syslog messages are “VRF aware” and the name of the VRF is included in the error message.

Monitoring Tool: Netflow

The Cisco IP multicast instrumentation provides network managers with in-depth information about the status of the network. To efficiently collect and analyze this information, network managers can take advantage of the NetFlow tool or the Multicast Management solution (described in the next section).

Background

Developed in 1996 by Darren Kerr and Barry Bruins at Cisco Systems, the patented NetFlow utility is now the primary network accounting technology in the industry. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing. Cisco provides a set of NetFlow applications to collect information about traffic, process the collected data, and provide end-user applications with easy access to the data.

NetFlow includes three key components that perform the following capabilities:

- **Flow Caching** analyzes and collects IP data flows entering router or switch interfaces and prepares data for export. It enables the accumulation of data on flows with unique characteristics, such as IP addresses, application, and class of service (CoS). Flexible flow data is now available using the latest NetFlow v.9 export data format. NetFlow supports key technologies, including IPv4, IPv6, Multicast, and Multiprotocol Label Switching (MPLS).
- **FlowCollector** and **Data Analysis** components capture exported data from multiple routers and filter and aggregate the data according to customer policies. This summarized or aggregated data is then stored for analysis. Users can utilize Cisco NetFlow as a flow collector, or they can opt for a variety of third-party partner products. A graphical user interface displays and analyzes NetFlow data collected from FlowCollector files. This allows users to complete near-real-time visualization or trending analysis of recorded and aggregated flow data. Users can specify the router and aggregation scheme and desired time interval.

Typical flow analysis information found in a NetFlow data record includes:

- Source and destination IP address
- Source and destination TCP/User Datagram Protocol (UDP) ports
- Type of service (ToS)
- Packet and byte counts
- Start and end timestamps
- Input and output interface numbers
- TCP flags and encapsulated protocol (TCP/UDP)
- Routing information (next-hop address, source autonomous system (AS) number, destination AS number, source prefix mask, destination prefix mask)

Cisco Support for NetFlow

Cisco supports two types of NetFlow options for multicast that each generates a different flow record in the NetFlow cache (see Figures 1 and 2):

- Multicast NetFlow Ingress: incoming and outgoing values (bytes and packets) are both counted and stored. Note: only software-based routers (for example, the Cisco 7200 Series) can provide the outgoing values in this mode.
- Multicast NetFlow Egress: bytes and packets are the outgoing values.

NetFlow can optionally count and report Reverse Path Forwarding (RPF) failures in a multicast network. This capability is enabled when the “ip multicast netflow rpf-failure” feature is globally enabled on the routers in the network.

For more information about NetFlow, visit: http://www.cisco.com/go/netflow, or refer to the white paper at: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.shtml.

Figure 1. Multicast NetFlow Cache Examples

Software-Based Router (Such as Cisco 7200 Series) – Ingress

SrcIf	SrcIPadd	DstIf	DstIPadd	Bytes	Packets	Obytes	Opackets
Eth0	10.0.0.2	Null	224.1.1.10	23100	21	69300	63

Software-Based Router – Egress

SrcIf	SrcIPadd	DstIf	DstIPadd	Bytes	Packets
Eth0	10.0.0.2	Eth1	224.1.1.10	23100	21
Eth0	10.0.0.2	Eth2	224.1.1.10	23100	21
Eth0	10.0.0.2	Eth3	224.1.1.10	23100	21

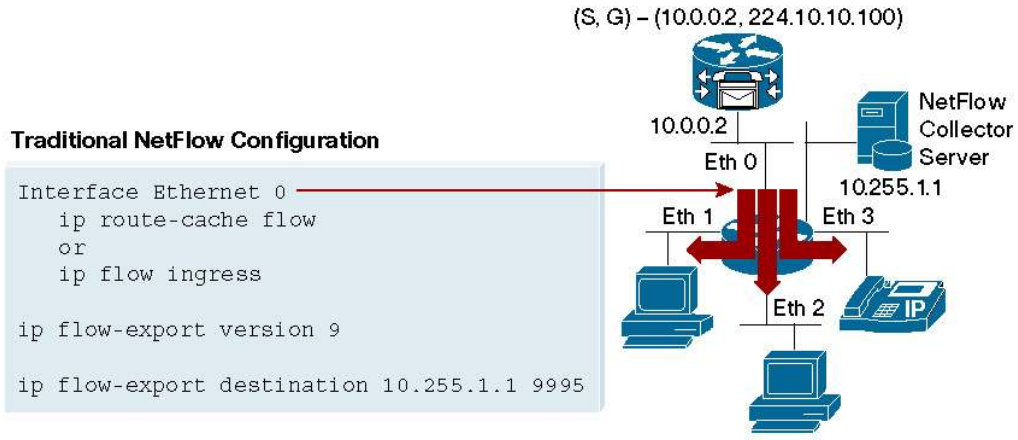
Cisco Catalyst 6500/Cisco 7600 – Ingress Accounting

SrcIf	SrcIPadd	DstIf	DstIPadd	Bytes	Packets
Eth0	10.0.0.2	Eth1	224.1.1.10	23100	21

Cisco Catalyst 6500/Cisco 7600 – Egress Accounting

SrcIf	SrcIPadd	DstIf	DstIPadd	Bytes	Packets
Null	10.0.0.2	Eth1	224.1.1.10	23100	21
Null	10.0.0.2	Eth2	224.1.1.10	23100	21
Null	10.0.0.2	Eth3	224.1.1.10	23100	21

Figure 2. Configuration for Multicast NetFlow Ingress (Version 9)



Summary: Instrumentation and NetFlow

For PIM-SM, the multicast instrumentation and NetFlow tool capabilities include:

- The discovery of RPs using MIBs
- The discovery of RP group ranges for Auto-RP PIMv2 Bootstrap Router (BSR)
- The identification of all active groups (RP know about all active multicast groups)
- Retrieving the entire forwarding table using Mroute MIB
- Using MSDP MIB to show which RPs are running MSDP, and check their peering status
- Using IGMP MIB to show which groups have receivers on which interfaces
- Analyzing traffic using NetFlow

For PIM-SSM:

- No discovery of RPs (no central place to check for all sources or groups)
- Source and group Mroutes can be tracked and measured with IP Mroute MIB
- Access group membership information with IGMP MIB (IGMPv3 is not supported)
- Multicast NetFlow can be used for traffic analysis

For Bidir:

- RP knows about all active groups
- No source or group entries (Mroute MIB and “show ip mroute count” will not provide source information)
- *,G supported; MIBs work; traffic information is aggregated on a group; for source-only branches use the “**show mls ip multicast rp-mapping gm-cache**”
- For source information, use NetFlow (Multicast NetFlow will have all source and group information with traffic rates)

For mVPN:

- Customer Edge (CE) routers use the same management tools (no change)
- On Provider Edge (PE) routers, the CISCO-MVPN-MIB can provide:
  - A list of all active multicast VRFs
  - How many interfaces are configured for each VRF

- Which default and data MDTs are in use for each VRF
- Which provider domain sources and groups are being used for each MDT
- Which provider domain sources and groups are being used for each customer domain Mroute

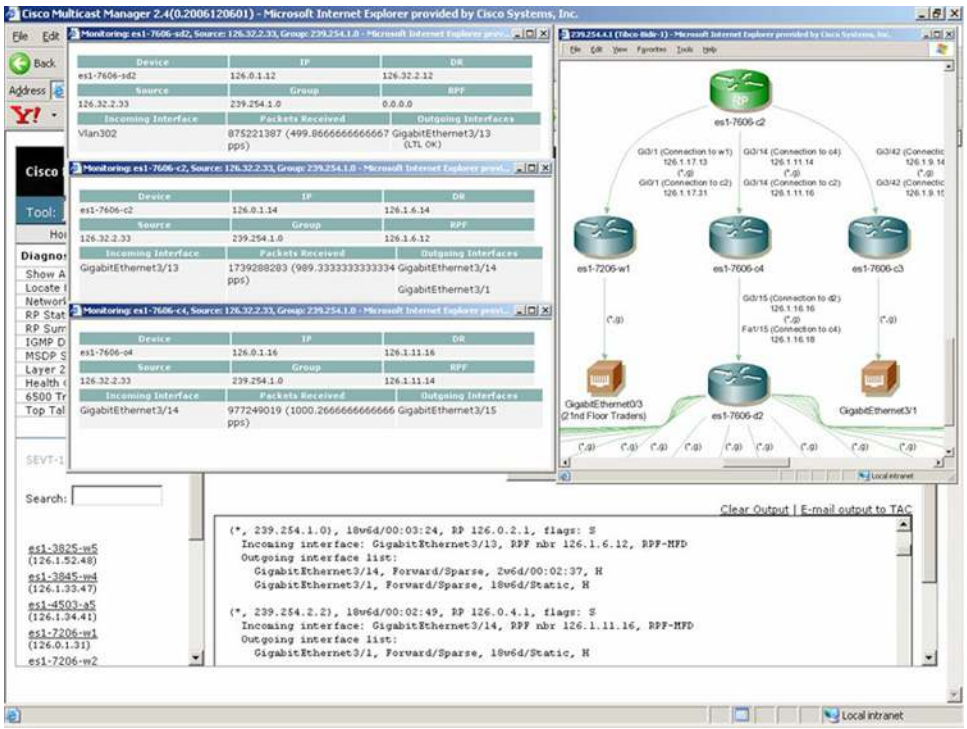
- The provider domain source and group can be looked up in the IPMROUTE-MIB or IPMROUTE-STD-MIB to collect statistics
- Provider domain groups can be managed with normal methods

Cisco Multicast Manager

The Cisco Multicast Manager is a Web-based software application that allows Service Providers and Enterprise customers to monitor all critical components of the multicast network (see Figure 3). It includes in-depth multicast diagnostics, network health checks, reports for trending and analysis, and tools for simplifying troubleshooting tasks. Some of the capabilities supported by the browser-based interface include:

- Monitoring of RPs (sources and groups), DRs, throughput, and multicast trees
- Listing of all active sources and groups
- Plotting trees
- Interrogating multicast routing, IGMP, and MSDP tables
- Locating hosts
- Gathering traffic samples
- Looking at Layer 2 switch tables

Figure 3. Cisco Multicast Manager Web Interface



The benefits of using Cisco Multicast Manager include a greatly enhanced user experience since problems can be proactively discovered before they become major outages. The monitoring capabilities allow the support staff a comprehensive view of the network and operation, and provide alerts of any events or performance that exceeds specified limitations. These capabilities include monitoring:

- RPs
- Sources and groups
- DRs
- Throughput
- Multicast trees

The diagnostic capabilities speed the time required for troubleshooting:

- List all active sources and groups
- Plot trees
- Interrogate multicast routing
- Review IGMP and MSDP tables
- Locate hosts
- Gather traffic samples
- Review Layer 2 switch tables

For more information about Cisco Multicast Manager visit http://www.cisco.com/go/cmm

Further Reading

Developing IP Multicast Networks, 1999, Cisco Press: http://www.ciscopress.com/title/1578700779

Multicast: http://www.cisco.com/go/multicast

NetFlow: http://www.cisco.com/go/netflow

IP Multicast Network Management:
http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a00800d6b62.shtml

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-361110-03 8/07