Multicast Network Management

Multicast Architecture
Agenda

- IP Multicast MIBs
- IP Multicast Syslogs
- IP Multicast NetFlow
- Network Management Systems for IP Mcast
- Monitoring and Trouble shooting Examples
What Is Network Management?

Practically, many people say:

- **Fault Detection and Isolation**
  
  Are any WAN links flapping?
  
  How long has that been happening?

- **Monitoring**
  
  Do you know what your network is doing right now?
  
  Do you know where your packets are?

- **Configuration Management**
  
  Which routers are included in that routing domain?
  
  Are there any obvious misconfigurations?
IP Multicast Net Mgmt Challenges

- Multicast forwarding state is dynamic
- Best Effort Delivery
- No Congestion control
  
  Requires External Monitoring
  
  Applications may have feedback mechanism (e.g. Tibco, PGM)
What Is Network Management for IPmc?

- Some people may say....
  How any active mroutes do we have now?
  What data rates are they running at?
  Where are the receivers for that group?
  Is the traffic behaving as expected?
  Which RP supports that group?
  How does the multicast traffic flow affect other traffic?

- What do you think it includes?
Multicast MIBs
Multicast MIBS

MIBs come in 4 main flavors:

Draft
  - MIBs based on IETF draft

RFC: Experimental
  - MIBs based on IETF RFC that is experimental

RFC: Proposed Standard
  - MIBs based on IETF RFC that is a proposed standard

Cisco specific MIBs
  - Extend the capabilities of IP multicast beyond what is defined in the IETF MIBs
  - For example, Cisco specific configuration and feature elements.
# Multicast MIBS

<table>
<thead>
<tr>
<th>Category</th>
<th>MIBs</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP</td>
<td>IGMP-MIB.my, IGMP-STD-MIB.my</td>
</tr>
<tr>
<td>IGMP Snooping</td>
<td>CISCO-IGMP-SNOOPING-MIB.my (CatOS only)</td>
</tr>
<tr>
<td>Mroute</td>
<td>IPMROUTE-MIB.my, IPMROUTE-STD-MIB.my, CISCO-IPMROUTE-MIB.my</td>
</tr>
<tr>
<td>PIM</td>
<td>PIM-MIB.my, CISCO-PIM-MIB.my</td>
</tr>
<tr>
<td>MSDP</td>
<td>MSDP-MIB.my</td>
</tr>
<tr>
<td>mVPN</td>
<td>CISCO-MVPN-MIB.my</td>
</tr>
</tbody>
</table>
## Multicast MIBS IOS Support

<table>
<thead>
<tr>
<th>MIB</th>
<th>12.1E</th>
<th>12.2SX</th>
<th>12.3</th>
<th>12.4</th>
<th>12.0S</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP-MIB</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>IGMP-STD-MIB (RFC 2933)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MROUTE-MIB</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MROUTE-STD-MIB (RFC 2932)</td>
<td>No</td>
<td>Yes¹</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CISCO-IPMROUTE-MIB</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PIM-MIB (RFC 2934)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CISCO-PIM-MIB</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MSDP-MIB (RFC 4624)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CISCO-MVPN-MIB</td>
<td>No</td>
<td>Yes¹</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

¹ The CISCO-MVPN-MIB and MROUTE-STD-MIB are available in 12.2(33)SXH and 12.2(33)SRB
IOS-XR MIB Support

- 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
IGMP-STD-MIB

- Based on RFC 2933
- Contains information for IPv4 Multicast Routers, e.g.:
  - Address of IGMP Querier
  - IGMP version configured on int
  - IGMP cache
- Does not fully support IGMPv3
  CSCek28502 fixed igmpInterfaceVersion
- Cisco implementation does support set/create of config objects
PIM-MIB

- Based on RFC 2934
- Contains PIM Interface info, neighbors and RP info
  - `pimRPState`
    - active RPs in system
    - similar to “show ip pim rp”
  - `pimRPSetTable`
    - mapping info for PIMv2
    - similar to “show ip pim rp mapping”
- Does not support Static RP ranges – but active groups will show up in `pimRPState`
- Auto-RP group ranges are included in `pimRPSetTable`
IP-MROUTE-STD-MIB

- Based on RFC 2932
- Contains information about the status of multicast routing
- Traffic statistics
  - Packet counters per mroute
  - Packet counters per mroute, per outbound interface
    - NextHopPkts
  - Octet counters per mroute
  - Octet counters per interface – in/out
CISCO-IPMROUTE-MIB

Contains information about mroutes such as flags and traffic counters

- The IPMROUTE-STD-MIB contains counters that are not available in the IPMROUTE-MIB

- IPMROUTE-STD-MIB has these objects additional as compared to the IPMROUTE-MIB:
  1. ipMRouteEntryCount
  2. ipMRouteHCOctets
  3. ipMRouteInterfaceHCInMcastOctets
  4. ipMRouteInterfaceHCOutMcastOctets
  5. ipMRouteScopeNameTable (has 7 objects)

- These are available in the CISCO-IPMROUTE-MIB as:
  1. ciscoIpMRouteNumberOfEntries
  2. ciscoIpMRouteOctets
  3. ciscoIpMRouteIfInMcastOctets
  4. ciscoIpMRouteIfOutMcastOctets
  5. Only available in IPMROUTE-STD-MIB
Packet Counters

**IF-MIB (RFC1213)**
- ifInMulticastPkts
- ifOutMulticastPkts
- ifHCInMulticastPkts
- ifHCOOutMulticastPkts

**CISCO-IPMROUTE-MIB**
- ciscolpMRoutelfInMcastPkts
- ciscolpMRoutelfHCInMcastPkts
- ciscolpMRoutelfOutMcastPkts
- ciscolpMRoutelfHCOOutMcastPkts

**Multicast In/Out Packets At Interface Level**

**Pax** – all L2 packets are P2P not Mcast

**USE New Counters**

**Most Int Types Counters are fine (e.g. GE)**

Similar output as:
```show ip pim int count```
CISCO-MVPN-MIB

- Based on draft-svaidya-mcast-vpn-mib to be re-submitted as L3VPN WG draft

- Includes:
  
  **Generic Info**
  - Names of Multicast-enabled VRFs
  - Number of active multicast enabled interfaces per VRF
  - Object to control trap generation per-mVRF
  - Last Config Event in each mVRF

  **Per-MVRF Information**
  - MDT default group address
  - MDT Data Groups and related Variables
  - Dynamic mapping between customer multicast groups and Default/Data MDT groups
  - Mapping between mVRF and MDT tunnel interface
  - MDT Join TLVs being sent by a device,
  - MDT-SAFI NLRI (BGP advertisements of MDT groups)
Traffic Reporting on 6500/7600

- Cat6500 traffic statistics are collected by hardware counters and updated periodically to MSFC
- Native IOS updates 25% of mroutes every 25 seconds
  - worse case stats can be 100 seconds old
  - in 12.2(18)SX this was changed to 10% with a default of 9 seconds – worse case 90 secs
- The stat update time can be adjusted with `mls ip multicast flow-stat-timer <secs>`
- May cause increase in CPU utilization depending on number of mroutes. Use with care.
# Multicast Notifications (Traps)

<table>
<thead>
<tr>
<th>Mroute</th>
<th>ciscoIpMRouteMissingHeartBeats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PIM</strong></td>
<td></td>
</tr>
<tr>
<td>pimNeighborLoss</td>
<td></td>
</tr>
<tr>
<td>ciscoPimRPMappingChange</td>
<td></td>
</tr>
<tr>
<td>ciscoPimInvalidRegister</td>
<td></td>
</tr>
<tr>
<td>ciscoPimInvalidJoinPrune</td>
<td></td>
</tr>
<tr>
<td>ciscoPimInterfaceUp</td>
<td></td>
</tr>
<tr>
<td>ciscoPimInterfaceDown</td>
<td></td>
</tr>
<tr>
<td><strong>MSDP</strong></td>
<td></td>
</tr>
<tr>
<td>msdpEstablished¹</td>
<td></td>
</tr>
<tr>
<td>msdpBackwardTransition</td>
<td></td>
</tr>
<tr>
<td><strong>mVPN</strong></td>
<td></td>
</tr>
<tr>
<td>ciscoMvpnMvrfChange</td>
<td></td>
</tr>
</tbody>
</table>

¹Supported in latest images – 12.4T, 12.0S, 12.2SXH, 12.2SRB. CSCek00661 has details.
Multicast Traps - Enabling

Traps are enabled by these commands:

```
snmp-server enable traps pim
  invalid-pim-message     Enable invalid pim traps
  neighbor-change         Enable neighbor change trap
  rp-mapping-change       Enable rp mapping change trap

snmp-server enable traps ipmulticast

snmp-server enable traps msdp

snmp-server enable traps mvpn

or

snmp-server enable traps
```

Will enable **ALL** traps
Multicast Traps – Enabling (Cont.)

Traps are enabled by these commands:

```
snmp-server enable traps pim invalid-pim-message
ciscoPimInvalidRegister
ciscoPimInvalidJoinPrune
snmp-server enable traps pim neighbor-change
pimNeighborLoss
ciscoPimInterfaceUp
ciscoPimInterfaceDown
snmp-server enable traps pim rp-mapping-change
ciscoPimRPMappingChange
snmp-server enable traps pim
   Everything above
snmp-server enable traps ipmulticast
   ciscoIpMRRouteMissingHeartBeats
snmp-server enable traps msdp
   msdpBackwardTransition
snmp-server enable traps mvpn
ciscoMvpnMvrfChange
```
Multicast Heartbeat

- Sends an SNMP trap when traffic stops for critical group

Troubleshooting Usage:

Confirm traffic stream activity

Requires that downstream router or host has joined group or that a static IGMP has been set – e.g. data path must be through the router configured with heartbeat monitor
Multicast Heartbeat

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

```
snmp-server enable traps ipmulticast
ip multicast heartbeat 224.0.1.53 1 1 10
```
Multicast VPN (MVPN) Concept and Fundamentals

- Customer CE devices joins the MPLS Core through provider’s PE devices
- The MPLS Core forms a Default MDT for a given Customer
- A High-bandwidth source for that customer starts sending traffic
- Interested receivers 1 & 2 join that High Bandwidth source
- Data-MDT is formed for this High-Bandwidth source
What Is VRF Aware?

If a MIB is VRF aware then:

- SNMP gets and sets can be made to the individual VRFs
- The MIB will have the ability to detect conditions for a trap inside of a VRF and lookup the additional information in the VRF context
- Traps will be sent to a manager located inside a VRF

```bash
snmp-server host 1.1.1.1 vrf blue
```
NOTE: VRF Aware and MIBs

MIBs that are not VRF aware will not be able to report on an event that occurs in a VRF. They will only report on events in the default/global routing tables.

Only PE routers need to be VRF Aware.

- These MIBs are **NOT** VRF Aware:
  - Mroute, PIM, MSDP, IGMP, IGMP Snooping
- The mVPN MIB is VRF independent and can be used to access information about each VRF.
New IETF Work on MIBs

- **New PIM MIB**
  
  Current draft: draft-ietf-pim-mib-v2-10.txt
  
  Working its way through the standards process

- **New Support**
  
  Static RP group ranges
  
  Auto-RP group ranges
  
  Embedded RP
  
  PIM-Bidir – DF election table
  
  IPv6 Multicast
New IETF Work on MIBs (Cont.)

- **IP Multicast MIB**
  
  Replaces IPMROUTE-STD-MIB

  Current Draft: draft-ietf-mboned-ip-mcast-mib-05.txt

  Working its way through the standards process

- **New Support**

  SSM Range Definitions

  PIM-Bidir mroute types

  IPv6 (Address Family Independent)

  Local host information – the mib will report on which groups are joined by router/host
New IETF Work on MIBs (Cont.)

- **BSR MIB**
  
  Current Draft: draft-ietf-pim-bsr-mib-03

  BSR info that has been pulled out of the PIM MIB

- **Supports**
  
  Candidate-RP info

  Elected BSR info

  Supports IPv4 and IPv6
New IETF Work on MIBs (Cont.)

- **Multicast Group Membership Discovery MIB**
  
  Current Draft: draft-ietf-magma-mgmd-mib-08.txt

- **Supports**
  
  IGMPv1, IGMPv2, IGMPv3
  MLDv1, MLDV2
  IPv4 and IPv6 membership in one MIB
  Support for hosts and routers
More Info

- For more information about IP Multicast MIBs:
  Search on CCO for “Multicast Network Management”

Or

- [http://www.cisco.com/go/ipmulticast](http://www.cisco.com/go/ipmulticast)

White Papers

IP Multicast Network Management
Multicast Syslog Messages
Multicast Syslogs

- There are dozens of multicast Syslog messages in these categories:
  - Mroute Messages
  - MDS Messages
  - PIM Messages
  - AUTORP Messages
  - MDT Messages
  - MSDP Messages
  - DVMRP Messages
  - MCAST Messages - Layer 2 Multicast

- Many customers use a correlation engine to collect and process Syslog messages – such as CNS Notification Engine
Useful Multicast Syslogs

Invalid RP Register Syslog:

```
%PIM-1-INVALID_RP_REG: Received Register from 210.0.1.202 for 239.3.3.3 not willing to be RP
```

This message indicates that an edge router is configured with the wrong RP address. DR addr is 210.0.1.202

Some users confuse the DR addr with the source addr. New format will make the message more readable. Adding address of RP from Reg msg:

```
%PIM-1-INVALID_RP_REG: Received Register from router 210.0.1.202 for group 239.3.3.3, 210.1.1.3 not willing to be RP
```
New Syslog Command

Global command:

ip pim log-neighbor-changes

Alerts when the status of a PIM neighbor changes – similar to existing log messages for OSPF and BGP

Integrated into recent releases of 12.3, 12.3T, 12.0S, 12.2S. See CSCee02125.
NOTE: VRF Aware and Syslogs

All the Syslog messages ARE VRF aware. They report the name of the VRF in the error message. Available in 12.2SX, 12.3T but not 12.0S images.

Examples of syslogs with VRF information:

```plaintext
%PIM-1-INVALID_RP_REG: VRF red: Received Register from 200.1.1.201 for 226.6.6.6, not willing to be RP

%PIM-5-NBRCHG: neighbor 126.1.5.14 UP on interface GigabitEthernet3/38 (vrf default)
```

Sometimes the VRF info:
- Is at the beginning of the message, sometimes end
- Identifies the default domain, sometimes not

This has been fixed in latest releases. See CSCei50781 and CSCek46450 for 12.0S
mVPN Management – Data MDT Reuse

mVPN has the option of using a different Data MDT for each high bandwidth customer stream.

SPs would like to monitor their VPNs to determine which ones may need more addresses for Data MDTs. This can be done with the mdt reuse syslog:

```
ip vrf blue
  mdt default 232.1.1.1
  mdt data 232.1.200.0 0.0.0.255
  mdt log-reuse
```

The config will enable this syslog message:

```
%MDT-5-DATA_MDT_REUSED: VRF blue: Data MDT 232.1.200.0 is reused in VRF blue
```
Multicast NetFlow
NetFlow Origination

- Developed by Darren Kerr and Barry Bruins at Cisco Systems in 1996
  US Patent 6,243,667

- The value of information in the cache was a secondary discovery
  Initially designed as a switching path

- NetFlow is now the **primary network accounting technology** in the industry

- Answers questions regarding IP traffic: **who, what, where, when, and how**
**Principle NetFlow Benefits**

<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Peering arrangements</td>
<td>- Internet access monitoring (protocol distribution, where traffic is going/coming)</td>
</tr>
<tr>
<td>- Network planning</td>
<td>- User monitoring</td>
</tr>
<tr>
<td>- Traffic engineering</td>
<td>- Application monitoring</td>
</tr>
<tr>
<td>- Accounting and billing</td>
<td>- Charge back billing for departments</td>
</tr>
<tr>
<td>- Security monitoring</td>
<td>- Security monitoring</td>
</tr>
</tbody>
</table>
What is a Traditional IP Flow?

1. Inspect a packet’s 7 key fields and identify the values
2. If the set of key field values is unique create a flow record or cache entry
3. When the flow terminates export the flow to the collector
NetFlow Principles

- Unidirectional flow
- Accounts for both transit traffic and traffic destined for the router
- Works with Cisco Express Forwarding or fast switching
  - Not a switching path
- Supported on all interfaces and Cisco IOS® Software platforms
- Returns the subinterface information in the flow records
- Cisco Catalyst® 6500 Series and Cisco 7600 Series enables NetFlow on all interfaces by default
### Traditional Layer 3 NetFlow Cache

1. **Create and update flows in NetFlow cache**

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPadd</th>
<th>DstIf</th>
<th>DstIPadd</th>
<th>Protocol</th>
<th>TOS</th>
<th>Flgs</th>
<th>Src Port</th>
<th>Src AS</th>
<th>Dst Port</th>
<th>Dst AS</th>
<th>NextHop</th>
<th>Bytes/Pkt</th>
<th>Active</th>
<th>Idle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa1/0</td>
<td>173.100.21.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>11000</td>
<td>A2</td>
<td>/24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1528</td>
<td>1745</td>
<td>4</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.3.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>6</td>
<td>40</td>
<td>0</td>
<td>2491</td>
<td>15</td>
<td>/26</td>
<td>196</td>
<td>15</td>
<td>10.0.23.2</td>
<td>740</td>
<td>41.5</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.20.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>10000</td>
<td>A1</td>
<td>/24</td>
<td>180</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1428</td>
<td>1145.5</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.6.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>6</td>
<td>40</td>
<td>0</td>
<td>2210</td>
<td>19</td>
<td>/30</td>
<td>180</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1040</td>
<td>24.5</td>
</tr>
</tbody>
</table>

2. **Expiration**

- Inactive timer expired - 15 sec is default
- Active timer expired - 30 min (1800 sec) is default
- NetFlow Cache is Full – oldest flows are Expired
- RST or FIN TCP Flag

3. **Export version**

   Non- Aggregated Flows—Export **Version 5 or 9**

4. **Transport protocol**

   - **30 Flows per 1500 byte export packet**

   - **Export Packet**
     - **Header**
       - **Payload (Flows)**
Flow Timers and Expiration

1st & 3rd Flows – Src 10.1.1.1, Dst 20.2.2.2, Prot 6, Src & Dst port 15, InIF FE0/0, ToS 128
2nd Flow – Src 10.1.1.1, Dst 20.2.2.2, Prot 6, Src & Dst port 15, InIF FE0/0, ToS 192

- SysUptime - Current time in milliseconds since router booted
- UTC - Coordinated Universal Time can be synchronized to NTP (Network Time Protocol)
Multicast NetFlow — Timers

- IP Multicast uses UDP
- UDP flows do not terminate like TCP flows with a RST or a FIN
- UDP flows depend on the aging timers to be exported
- On SW platforms this is controlled by the active timer

```plaintext
ip flow-cache timeout active 1
```
Minimum setting is 1 minute

- On 6500/7600 this is controlled by long aging timer

```plaintext
mls aging long 64
```
Minimum setting is 64 seconds
# NetFlow Export Versions

<table>
<thead>
<tr>
<th>NetFlow Version</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Original</td>
</tr>
<tr>
<td>5</td>
<td>Most Common</td>
</tr>
</tbody>
</table>
| 7               | Specific to Cisco C6500 and 7600 Series Switches  
|                 | Similar to Version 5, but Does Not Include AS, Interface, 
|                 | TCP Flag and ToS Information |
| 8               | Choice of Eleven Aggregation Schemes  
|                 | Reduces Resource Usage |
| 9               | Flexible, Extensible Export Format to Enable Easier Support  
|                 | of Additional Fields and Technologies e.g. MPLS, Multicast, 
NetFlow v9 Principles

- Version 9 is an export format
- Still a push model
- Send the templates regularly (configurable)
- Independent of the UDP transport protocol, it is ready for any reliable transport protocol e.g. TCP, SCTP,…
- Advantage: we can add new technologies/data types very quickly
  
  e.g. MPLS, IPv6, BGP Next Hop, Multicast,…
Multicast NetFlow

Three Types of NetFlow Implementations for Multicast Traffic:

1. Traditional Ingress NetFlow
2. Multicast NetFlow Ingress
3. Multicast NetFlow Egress
Switching Path Implications for NetFlow Multicast

- Does each outgoing interface generate a separate flow?
- Do the bytes and packets reflect input or output numbers?

Switching Vector:
- FAST + FLOW (Fast)
- dCEF (mdfs)

Multicast Route Lookup
- MFIB
- Source AS

Add Input Flow Fields

Multicast Packets
- Input

Packet Buffer

Input Interface Feature Check
- ACL
- Policy
- WCCP

Multicast Replication
- Ethernet 1
- Ethernet 2
- Ethernet 3

Output Interface Feature Check
- Qos
- CAR
- Crypto

Add Output Flow Fields

Bytes Packets

Output Interface Feature Check

Multicast 224.0.0.0 through 239.255.255

• Ethernet 1
• Ethernet 2
• Ethernet 3

Passed

Fast + FLOW (Fast)

dCEF (mdfs)
Multicast: Traditional NetFlow

Traditional NetFlow Configuration

- Interface Ethernet 0
  - ip route-cache flow
  - ip flow ingress
- ip flow-export version 9
- ip flow-export destination 10.255.1.1 9995

Flow Record Created in NetFlow Cache

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPAdd</th>
<th>DstIf</th>
<th>DstIPAdd</th>
<th>Protocol</th>
<th>TOS</th>
<th>Flgs</th>
<th>SrcPort</th>
<th>DstPort</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Null</td>
<td>224.10.10.100</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>00A2</td>
<td>00A2</td>
<td>23100</td>
<td>21</td>
</tr>
</tbody>
</table>

- There is only one flow per NetFlow configured input interface
- Destination interface is marked as “Null”
- Bytes and Packets are the incoming values
**Multicast NetFlow Ingress (v9)**

**Multicast NetFlow Ingress Configuration**

- Interface Ethernet 0
  - `ip flow ingress`
  - `ip multicast netflow ingress`
- `ip flow-export version 9`
- `ip flow-export destination 10.255.1.1 9995`

**Flow Record Created in NetFlow Cache**

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIpAdd</th>
<th>DstIf</th>
<th>DstIpAdd</th>
<th>Protocol</th>
<th>TOS</th>
<th>Flgs</th>
<th>SrcPort</th>
<th>DstPort</th>
<th>Bytes</th>
<th>Packets</th>
<th>Obytes</th>
<th>Opackets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Null</td>
<td>224.10.10.100</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>00A2</td>
<td>00A2</td>
<td>23100</td>
<td>21</td>
<td>69300</td>
<td>63</td>
</tr>
</tbody>
</table>

- There is only one flow per NetFlow configured input interface
- Destination interface is marked as “Null”
- Bytes and Packets are the **incoming** values
- Obytes and Opackets are **outgoing** values across all interfaces – sw based routers only
**Multicast NetFlow Egress (v9)**

**Multicast NetFlow Egress Configuration**

- Interface Ethernet 1
  - ip multicast netflow egress
- Interface Ethernet 2
  - ip multicast netflow egress
- Interface Ethernet 3
  - ip multicast netflow egress

- ip flow-export version 9
- ip flow-export destination 10.255.1.1 9995

**Flow Records Created in NetFlow Cache**

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddr</th>
<th>DstIf</th>
<th>DstIPaddr</th>
<th>Protocol</th>
<th>TOS</th>
<th>Flgs</th>
<th>SrcPort</th>
<th>DstPort</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Eth1*</td>
<td>224.10.10.100</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>00A2</td>
<td>00A2</td>
<td>23100</td>
<td>21</td>
</tr>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Eth2*</td>
<td>224.10.10.100</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>00A2</td>
<td>00A2</td>
<td>23100</td>
<td>21</td>
</tr>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Eth3*</td>
<td>224.10.10.100</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>00A2</td>
<td>00A2</td>
<td>23100</td>
<td>21</td>
</tr>
</tbody>
</table>

- There is one flow per Multicast NetFlow Egress configured output interface
- One of the Key fields that define a unique flow has changed from source interface to destination interface
- Bytes and Packets are the outgoing values
Multicast NetFlow: config anomalies

- `ip multicast netflow ingress`
  - enabled by default
  - is not nvgened
  - if `ip flow ingress` is enabled, multicast netflow will be enabled

- `ip multicast netflow egress`
  - disabled by default
  - Unicast netflow must be enabled on at least one interface
Multicast NetFlow: Minimum Config - Ingress

Software Based Routers (e.g. 7200)

interface Ethernet 0
  ip flow ingress
    ip multicast netflow ingress

ip flow-export version 9
ip flow-export destination 10.255.1.1 9995

*ip multicast netflow ingress* is not nvgened and not required
Multicast NetFlow: Minimum Config - Egress

Software based routers (e.g. 7200)

interface Ethernet 0
  ip flow ingress
  ip multicast netflow egress

ip flow-export version 9
ip flow-export destination 10.255.1.1 9995
Multicast NetFlow: Minimum Config - Ingress

6500/7600 - Ingress

```bash
mls flow ip interface-full
mls nde sender
!
interface Vlan10
  ip flow ingress
    ip multicast netflow ingress
!
ip flow-export version 9
ip flow-export destination 10.255.1.1 9995
```

*ip multicast netflow ingress* is not nvgened and not required
Multicast NetFlow: Minimum Config - Egress

6500/7600 - Egress

mls flow ip interface-full
mls nde sender
!
interface Vlan10
  ip flow ingress  # can be configured on any interface
  ip multicast netflow egress
!
ip flow-export version 9
ip flow-export destination 10.255.1.1 9995
### Multicast NetFlow: Export Format

#### Summary

**Software Based Router (e.g. 7200) – Ingress Accounting**

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPadd</th>
<th>DstIf</th>
<th>DstIPadd</th>
<th>Bytes</th>
<th>Packets</th>
<th>Obytes</th>
<th>Opackets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Null</td>
<td>224.1.1.10</td>
<td>23100</td>
<td>21</td>
<td>69300</td>
<td>63</td>
</tr>
</tbody>
</table>

**Software Based Router (e.g. 7200) – Egress Accounting**

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPadd</th>
<th>DstIf</th>
<th>DstIPadd</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Eth1</td>
<td>224.1.1.10</td>
<td>23100</td>
<td>21</td>
</tr>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Eth2</td>
<td>224.1.1.10</td>
<td>23100</td>
<td>21</td>
</tr>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Eth3</td>
<td>224.1.1.10</td>
<td>23100</td>
<td>21</td>
</tr>
</tbody>
</table>

**6500/7600 – Ingress Accounting**

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPadd</th>
<th>DstIf</th>
<th>DstIPadd</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Null</td>
<td>224.1.1.10</td>
<td>23100</td>
<td>21</td>
</tr>
</tbody>
</table>

**6500/7600 – Egress Accounting**

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPadd</th>
<th>DstIf</th>
<th>DstIPadd</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>10.0.0.2</td>
<td>Eth1</td>
<td>224.1.1.10</td>
<td>23100</td>
<td>21</td>
</tr>
<tr>
<td>Null</td>
<td>10.0.0.2</td>
<td>Eth2</td>
<td>224.1.1.10</td>
<td>23100</td>
<td>21</td>
</tr>
<tr>
<td>Null</td>
<td>10.0.0.2</td>
<td>Eth3</td>
<td>224.1.1.10</td>
<td>23100</td>
<td>21</td>
</tr>
</tbody>
</table>
Multicast NetFlow: RPF (Reverse Path Forwarding) Failures

- If “ip multicast netflow rpf-failure” is configured globally, packets that have fields that should come from another input interface are blocked e.g. source IP and input interface doesn’t agree with the routing table.

- When this feature is enabled globally:

  ```
  Router(config)# ip multicast netflow rpf-failure
  ```

  the RPF failures are recorded as flows in the NetFlow cache.

- Once configured, there will be a new field in the NetFlow cache called “RPF Fail” to count flows that fail and how many times.
NetFlow MIB

- Snapshot of current ‘Top Talkers’ NetFlow cache via SNMP – **Works with PIM-Bidir**
- Administration and configuration of NetFlow using the MIB interface
- NetFlow MIB cannot be used to retrieve all flow information due to scalability
- Example objects available:
  - Protocol distribution
  - Number of bytes/flows exported
  - Number of flows in cache
- This is targeted at Denial of Service (DoS) attacks, security monitoring and remote locations where export to a local NetFlow collector is not possible
- Available now in Release 12.3(7)T and 12.2(25)S and 12.2(33)SXH
Multicast NetFlow: Summary

- Supported via NetFlow version 9 export format
- Performance: Ingress vs. Egress
  
  Multicast NetFlow Ingress and traditional NetFlow will have similar performance numbers

  Multicast NetFlow Egress will have performance impact that is proportional to the number of interfaces on which it is enabled (include input interfaces)

- Availability
  
  Cisco IOS Software Release 12.3(1)
  
  Cisco 12000 Series Internet Router – see next slide

- Cisco Cisco Catalyst 6500 Series and Cisco 7600 Series
  
  Multicast NetFlow Ingress is supported on the PFC3A, PFC3B or PFC3B-XL in 12.2(18)SXF
  
  Multicast NetFlow Egress will require a PFC3B or PFC3B-XL
Multicast NetFlow: 12000 Series

- **Ingress, Non-Sampled**
  Engines 3 and 5 (aggregated NetFlow only)
  (reporting pre-replication counters only and output i/f Null)

- **Ingress, Sampled mode**
  Engines 2, 3, 4+, 5, 6
  (reporting pre-replication counters only and output i/f Null)

- **Egress, Non-Sampled**
  multicast packets are not reported by any engine

- **Egress, Sampled mode**
  Engines 3, 5
  (reporting flows for each replica, i.e. post replication flows)

- **Netflow on Engine 0 and 1 are not recommended**
Egress Netflow on the 12K may report the wrong ingress interface

– Eng 3, 5 and 6 do not retain the ingress interface information after replication

– However, the incoming slot information is known

– Instead of returning NULL as the ingress interface the netflow record is created with the ingress interface as the first interface on the linecard

– Therefore, a netflow collector may account for packets against the wrong interface

– More information can be found in CSCek47890
## Multicast NetFlow 6500/7600 Support

Support added in 12.2(18)SXF

<table>
<thead>
<tr>
<th>Multicast replication mode</th>
<th>NetFlow Accounting Mode</th>
<th>NetFlow v9 Export</th>
<th>View records at CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ingress</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Egress</td>
<td>Yes*</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Requires PFC3B/3B-XL

** Available for 12.2(33)SXH
# Multicast NetFlow Capacity – 6500/7600

<table>
<thead>
<tr>
<th></th>
<th>Size</th>
<th>Efficiency</th>
<th>Effective Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sup2/PFC2</strong></td>
<td>Multicast NetFlow Not Supported</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sup720/PFC3A</strong></td>
<td>128K entries</td>
<td>50%</td>
<td>64K entries</td>
</tr>
<tr>
<td><strong>Sup720/PFC3B</strong></td>
<td>128K entries</td>
<td>90%</td>
<td>115K entries</td>
</tr>
<tr>
<td><strong>Sup720/PFC3BXL</strong></td>
<td>256K entries</td>
<td>90%</td>
<td>230K entries</td>
</tr>
</tbody>
</table>
More Info

For more information about netflow:

http://www.cisco.com/go/netflow
Network Mgmt for PIM-SM

- RPs can be discovered through PIM MIB
- RP Group Ranges can be discovered for Auto-RP and BSR through PIM MIB
- RP knows about all active groups
- Mroute MIB can retrieve the entire forwarding table
- MSDP MIB can show which RPs are running MSDP and their peering status
- IGMP MIB can show you which groups have receivers on which interfaces
- Multicast NetFlow can be used for traffic analysis
Network Mgmt for PIM-SSM

- No RP
  No central place to check for all S,Gs
- S,G mroutes can be tracked, measured with IP Mroute MIB
- IGMP MIB can give you group membership information
  IGMPv3 is not supported
  No source information
- Multicast NetFlow can be used for traffic analysis
Network Mgmt for PIM-Bidir

- RP knows about all active groups
- No S,G Entries
  Mroute MIB and ‘show ip mroute count’ will not be able to give any info on sources
- *,G still there – MIBs OK
  Traffic info is aggregated on a group
  Source only branches
  Use show mls ip multicast rp-mapping gm-cache
- Need Source info? – Use NetFlow
  Multicast NetFlow will have all S,G info with traffic rates
Network Mgmt for mVPN

- CE routers use same mgmt tools – no change
- On 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 P Domain S,Gs are being used for each MDT
  - Which P Domain S,Gs are being used for each C Domain mroute

- The P Domain S,G can be looked up in the IPMROUTE-MIB or IPMROUTE-STD-MIB to collect statistics
- P Domain groups can be managed with normal methods
- Data MDT reuse can be tracked with Syslog
Network Management Systems (NMS) for IP Multicast
Some Multicast NMS Products

- Cisco Multicast Manager
- HP OpenView NNM Smart Plug-in for IP Multicast
- InCharge™ IP Multicast Manager
- SPECTRUM® Multicast Manager
Cisco NetFlow Applications and Partners

Traffic Analysis

- AdventNet
- HP
- InfoVista
- IBM
- Evident
- CA
- Valencia Systems
- Caligare
- NetQoS
- wiredcity
- Netmon
- PARRESSLER
- isarNet
- Arbor Networks
- nentusage

Open Source
- Flow-Tools
- FlowMon
- Flowd

Denial of Service

- Cisco Systems
- ARBOR Networks
- CS-Mars
- Lancope

Billing

- Evident
- Portal
- NetQoS

Multicast VPN Provisioning

- Internet Solutions Center (ISC) – MPLS VPN Management
- Multicast Address Pools associated to Provider
  Each Pool can be used for Default, Data or both types of MDTs (Multicast Distribution Tree)
- VPNs enabled for multicast
  Default and Data MDTs associated with VPN
- ISC Configures
  VRF associated to the multicast VPN
  PE and CE interfaces to enable multicast
  Enables multicast routing for VRF
- Assumption
  Provider core and Customer sites are pre-setup for multicast
Cisco Multicast Manager

- Web based software application
- Monitor all critical components of the multicast infrastructure
- Simplifies troubleshooting tasks
- In-depth multicast diagnostics
- Trending and analysis
Cisco Multicast Manager

- **Monitor** – RP’s, Sources and Groups, DR’s, Throughput and Multicast Trees
- **Diagnose** – list all active sources and groups, plot trees, interrogate multicast routing, IGMP and MSDP tables. Locate hosts, gather traffic samples, look at layer2 switch tables.
Custom Built 6500 Multicast Troubleshooting

Automatically:
Issues and stores relevant commands
Draws Graphical Tree
Plots packet throughputs

Cisco Multicast Manager 2.4 (Beta 0.005)

Diagnostics:
- Show All Groups
- Locate Host
- Network Status
- RP Status
- RP Summary
- IGMP Diagnostics
- MSDP Status
- Layer 2 Switches
- Health Check
- 6500 Troubleshooting

6500 Troubleshooting

Router: es1-7606-sd2
Username
Password:
Enable:
Packing interval: 5

Source: 126.32.2.234
Group: 232.1.1.2
Command: `sh ip mroute`

Clear Output | E-mail output to TAC

-- 7/14/2006 10:09:22 -- es1-7606-sd2 -- 'sh ip mroute'
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected, L - Local, P - Pruned, R - RI-bit set, F - Register flag,
### Table 1: Device Information

<table>
<thead>
<tr>
<th>Device</th>
<th>IP</th>
<th>DR</th>
</tr>
</thead>
<tbody>
<tr>
<td>es1-7606-sd2</td>
<td>126.0.1.12</td>
<td>126.32.2.12</td>
</tr>
<tr>
<td>Source</td>
<td>Group</td>
<td>RPF</td>
</tr>
<tr>
<td>126.32.2.33</td>
<td>239.254.1.0</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

### Table 2: Incoming Interface Information

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>Packets Received</th>
<th>Outgoing Interfaces</th>
</tr>
</thead>
</table>

### Table 3: Outgoing Interface Information

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>Packets Received</th>
<th>Outgoing Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>es1-7606-c4</td>
<td>GigabitEthernet3/14</td>
<td>977249019 (1000.28566666666666 Gbps)</td>
<td>GigabitEthernet3/15</td>
</tr>
</tbody>
</table>

### Diagram Information

- **RP**
- **es1-7606-c2**
- **es1-7606-c4**
- **es1-7606-d2**
- **es1-7606-w2**
- **es1-7606-w5**
- **es1-7606-w4**
- **es1-7606-w1**

- **esi-7606-c3**
- **esi-7606-d3**
- **esi-7606-w1**
- **esi-7606-d2**

**Connection Details**

- **esi-7606-w5** (126.1.52.48)
- **esi-7606-w4** (126.1.33.47)
- **esi-7606-w1** (126.3.1.31)
- **esi-7606-w2** (126.3.1.31)

- **esi-7606-c3** (126.1.17.13)
- **esi-7606-c4** (126.1.11.16)
- **esi-7606-d2** (126.1.17.13)
- **esi-7606-d4** (126.1.11.16)
- **esi-7606-d2** (126.1.17.13)
- **esi-7606-d3** (126.1.11.16)

- **esi-7606-w1** (126.1.17.13)
- **esi-7606-w4** (126.1.11.16)
- **esi-7606-w3** (126.1.17.13)
- **esi-7606-w2** (126.1.11.16)

**Clear Output | E-mail output to TAC**

- **esi-7606-w5** (126.1.52.48)
- **esi-7606-w4** (126.1.33.47)
- **esi-7606-w1** (126.3.1.31)
- **esi-7606-w2** (126.3.1.31)

(*) , 239.254.1.0, 18w6d/00:03:24, RF 126.0.2.1, flags: S
Incoming interface: GigabitEthernet3/13, EDP nbr 126.1.6.12, EDP-MFD
Outgoing interface list:
  - GigabitEthernet3/14, Forward/Sparse, 2w6d/00:02:37, H
  - GigabitEthernet1/1, Forward/Sparse, 18w6d/Static, H

(*) , 239.254.2.2, 18w6d/00:02:49, RF 126.0.4.1, flags: S
Incoming interface: GigabitEthernet3/14, EDP nbr 126.1.11.16, EDP-MFD
Outgoing interface list:
  - GigabitEthernet3/1, Forward/Sparse, 18w6d/Static, H
Dynamically Updating Top Talkers

<table>
<thead>
<tr>
<th>Source</th>
<th>Group</th>
<th>Short Term</th>
<th>Medium Term</th>
<th>Long Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>126.32.2.33</td>
<td>239.254.1.0</td>
<td>500 pps/1098 kbps(1sec)</td>
<td>1098 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.9</td>
<td>500 pps/1100 kbps(1sec)</td>
<td>1100 kbps(last 10 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.33</td>
<td>239.254.1.7</td>
<td>500 pps/1108 kbps(1sec)</td>
<td>1108 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.33</td>
<td>239.254.1.5</td>
<td>500 pps/1107 kbps(1sec)</td>
<td>1107 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.4</td>
<td>500 pps/1094 kbps(1sec)</td>
<td>1094 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.33</td>
<td>239.254.1.2</td>
<td>500 pps/1100 kbps(1sec)</td>
<td>1100 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.4</td>
<td>500 pps/1100 kbps(1sec)</td>
<td>1100 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.0</td>
<td>500 pps/1096 kbps(1sec)</td>
<td>1096 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.2</td>
<td>500 pps/1101 kbps(1sec)</td>
<td>1101 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.33</td>
<td>239.254.1.8</td>
<td>500 pps/1097 kbps(1sec)</td>
<td>1097 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.3</td>
<td>500 pps/1106 kbps(1sec)</td>
<td>1106 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.1</td>
<td>500 pps/1103 kbps(1sec)</td>
<td>1103 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.3</td>
<td>500 pps/1099 kbps(1sec)</td>
<td>1099 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.33</td>
<td>239.254.1.8</td>
<td>500 pps/1106 kbps(1sec)</td>
<td>1106 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.6</td>
<td>500 pps/1114 kbps(1sec)</td>
<td>1114 kbps(last 10 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.7</td>
<td>500 pps/1101 kbps(1sec)</td>
<td>1101 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.6</td>
<td>500 pps/1095 kbps(1sec)</td>
<td>1095 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
<tr>
<td>126.32.2.34</td>
<td>239.254.1.5</td>
<td>500 pps/1109 kbps(1sec)</td>
<td>1109 kbps(last 0 secs)</td>
<td>1103 kbps(life avg)</td>
</tr>
</tbody>
</table>

Output taken from ‘show ip mroute active’ displayed in a table
CMM Support for mVPN

New

VRFs discovered from PEs
CMM Support for mVPN

New

PE routers with VRFs configured

<table>
<thead>
<tr>
<th>Device</th>
<th>Multicast Enabled</th>
<th>Route Distinguisher</th>
<th>Default Group</th>
<th>Data Group</th>
<th>Data Group Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>ent-a</td>
<td>yes</td>
<td>100:100</td>
<td>232.1.100.0</td>
<td>232.1.100.16</td>
<td>0.0.0.15</td>
</tr>
<tr>
<td>ent-b</td>
<td>yes</td>
<td>201:201</td>
<td>232.2.100.0</td>
<td>232.2.100.16</td>
<td>0.0.0.15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device</th>
<th>Multicast Enabled</th>
<th>Route Distinguisher</th>
<th>Default Group</th>
<th>Data Group</th>
<th>Data Group Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>ent-a</td>
<td>yes</td>
<td>100:100</td>
<td>232.1.100.0</td>
<td>232.1.100.16</td>
<td>0.0.0.15</td>
</tr>
<tr>
<td>ent-b</td>
<td>yes</td>
<td>200:200</td>
<td>232.2.100.0</td>
<td>232.2.100.16</td>
<td>0.0.0.15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device</th>
<th>Multicast Enabled</th>
<th>Route Distinguisher</th>
<th>Default Group</th>
<th>Data Group</th>
<th>Data Group Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>ent-a</td>
<td>yes</td>
<td>100:100</td>
<td>232.1.100.0</td>
<td>232.1.100.16</td>
<td>0.0.0.15</td>
</tr>
<tr>
<td>ent-b</td>
<td>yes</td>
<td>200:200</td>
<td>232.2.100.0</td>
<td>232.2.100.16</td>
<td>0.0.0.15</td>
</tr>
</tbody>
</table>
CMM Support for mVPN

New

RD and RT info
MDT info
VRF/MDT Mapping info
New Features in 2.3(4)

- Static RPs
- Support for SSM
- Simplified Polling Configuration
- Scheduling of Health Checks
- Email reports for Health Checks
- Monitoring of % multicast traffic on an interface
- Reporting of % multicast traffic on an interface
- PIM Neighbor Report
- Interface errors on multicast tree traces
CMM 2.4

- MVPN
- CRS/IOS-XR support
- Video Delivery Networks
  IneoQuest probes based on RFC 4445
  MDI – Media Delivery Index
Benefits of Deploying CMM

- **Monitoring**
  Rendezvous Points, Designated Routers, Sources and Groups, Layer2 Ports, Multicast Trees, Interface Bandwidth

- **Reporting**
  Latest Alerts, Specific Alerts, Historical S,G, Historical Interface Traffic

- **Diagnostics**
  Active Sources/Groups, Detailed Multicast Trees, Actual PPS through tree, IGMP Information, MSDP Information

- **Health Check**
  Ability to check and report on the status of overall network
Monitoring and Troubleshooting Examples
Using CMM to Detect Multicast Faults

- Many types of multicast networks have fairly static distribution trees during normal operation
  
  Finance – Market Data
  Video Distribution for cable TV

- Network state can be captured and monitored for changes

- CMM can send alerts when unexpected changes occur
Monitoring

CMM can monitor:

- Availability of RP’s
- Selected Sources and Groups
- Multicast Trees
- Designated Routers (DRs)
- Layer2 Ports

High/Low data rate thresholds
Monitoring — RPs

CMM can monitor the RPs:

- Is the RP up and available
- Set a threshold on the number of sources and groups that are registered
- Track all sources and groups that join and leave
- Report any rogue sources and groups joining
Monitoring — S,Gs

- CMM can find all of the active sources and groups
- The S,Gs can be monitored with thresholds for low and high pps
- Start with a large high threshold and a small low threshold number
- CMM will start to monitor the traffic sent by these sources to these groups at the routers you selected
- You can now use the historical reporting function to start base-lining more intelligent thresholds
## Polling Configuration

Configure polling intervals by time and day.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Run Times</th>
<th>Start Time</th>
<th>Stop Time</th>
<th>Days</th>
<th>Max Threads</th>
<th>Max Days</th>
<th>Max Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Run Times</td>
<td>Use Defaults</td>
<td>00</td>
<td>00</td>
<td>23</td>
<td>59</td>
<td>M-F</td>
<td></td>
</tr>
<tr>
<td>DR Polling Interval</td>
<td>5 Min</td>
<td>00</td>
<td>00</td>
<td>23</td>
<td>59</td>
<td>M-F</td>
<td></td>
</tr>
<tr>
<td>Layer 2 Polling Interval</td>
<td>20 Sec</td>
<td>00</td>
<td>00</td>
<td>23</td>
<td>59</td>
<td>M-F</td>
<td></td>
</tr>
<tr>
<td>Route Monitor Polling Interval</td>
<td>1 Min</td>
<td>00</td>
<td>00</td>
<td>23</td>
<td>59</td>
<td>M-F</td>
<td></td>
</tr>
<tr>
<td>Specific Route Monitor Polling Interval</td>
<td>1 Min</td>
<td>00</td>
<td>00</td>
<td>23</td>
<td>59</td>
<td>M-F</td>
<td></td>
</tr>
<tr>
<td>RP/SG Cache Polling Interval</td>
<td>3 Min</td>
<td>00</td>
<td>00</td>
<td>23</td>
<td>59</td>
<td>M-F</td>
<td>10</td>
</tr>
<tr>
<td>RP Status Polling Interval</td>
<td>3 Min</td>
<td>00</td>
<td>00</td>
<td>23</td>
<td>59</td>
<td>M-F</td>
<td></td>
</tr>
<tr>
<td>RPF Failure Polling Interval</td>
<td>1 Min</td>
<td>00</td>
<td>00</td>
<td>23</td>
<td>59</td>
<td>M-F</td>
<td></td>
</tr>
<tr>
<td>Threshold Polling Interval</td>
<td>1 Min</td>
<td>00</td>
<td>00</td>
<td>23</td>
<td>59</td>
<td>M-F</td>
<td></td>
</tr>
<tr>
<td>Multicast Topology Polling Interval</td>
<td>24 Hrs</td>
<td>04</td>
<td>00</td>
<td>07</td>
<td>00</td>
<td>M-F</td>
<td></td>
</tr>
<tr>
<td>Tree Polling Interval</td>
<td>2 Min</td>
<td>00</td>
<td>00</td>
<td>23</td>
<td>59</td>
<td>M-F</td>
<td></td>
</tr>
</tbody>
</table>
Monitoring — Multicast Trees

- CMM can monitor multicast trees and report any changes.
- Within CMM you can draw the graphical trees that you want to monitor and save them.
- These saved trees will then appear under the monitoring trees drop down box. Select the trees that you want to monitor and the polling period.
Using CMM to Detect Multicast Faults

CMM can discover the active sources and groups
Using CMM to Detect Multicast Faults

The Tree trace produces a text based table and a graphic diagram

The text table is used to compare traces to detect changes
Using CMM to Detect Multicast Faults

The graphic can be used to quickly identify:
- RPs
- Routers
- Forwarding state
- Interfaces
CMM: Health Checks

- Ability to run pre-configured scripts to check the status of:
  - RP’s
    - `sysUpTime` is checked
  - S,G’s
    - S,G is checked if it exists
  - MSDP
    - Peering sessions are checked for “established”
  - Multicast Trees
    - Tree is compared against baseline
CMM: Health Checks

- Health checks can check the status of RP’s, MSDP peering, the presence of sources and groups and the status of multicast trees.
- Configure a Health Check to check and report upon the critical components of your network
- Create a Health Check for every important source and group
- In the event of problems run the health checks immediately
Health Check: Configuration

Add RP’s to check

Add MSDP checks

Add S,G’s to check
## Health Check: Configuration

### Cisco Tool Administration

<table>
<thead>
<tr>
<th>Configuration:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Domain Management</td>
</tr>
<tr>
<td>- Admin Utilities</td>
</tr>
<tr>
<td>- System Security</td>
</tr>
<tr>
<td>- User Management</td>
</tr>
<tr>
<td>- Discovery</td>
</tr>
<tr>
<td>- Device Configuration</td>
</tr>
<tr>
<td>- Global Polling Configuration</td>
</tr>
<tr>
<td>- Address Management</td>
</tr>
<tr>
<td>- Multicast Manager</td>
</tr>
<tr>
<td>- RP Polling</td>
</tr>
<tr>
<td>- SG Polling</td>
</tr>
<tr>
<td>- L2 Polling</td>
</tr>
<tr>
<td>- Tree Polling</td>
</tr>
<tr>
<td>- Health Check</td>
</tr>
<tr>
<td>- Route Manager</td>
</tr>
<tr>
<td>- QoS Monitor</td>
</tr>
</tbody>
</table>

### Management Domain: entsol

<table>
<thead>
<tr>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
</tr>
<tr>
<td>224.0.1.39</td>
</tr>
</tbody>
</table>

### Current Source/Group Polling Configuration

<table>
<thead>
<tr>
<th>Source</th>
<th>Group</th>
<th>Router</th>
<th>Remove</th>
</tr>
</thead>
</table>

### Forwarding Trees

- Select Baseline: fix-income-tree1.trace
- Add

### Trees to be Polled

<table>
<thead>
<tr>
<th>Baseline</th>
<th>Source</th>
<th>Group</th>
<th>FHR</th>
<th>LHR</th>
<th>Remove</th>
</tr>
</thead>
</table>
Troubleshooting with CMM

Health Check immediately points out changes from baseline
Bidir Troubleshooting with NetFlow

- **Problem**: A particular Bidir group’s traffic levels have jumped dramatically
- Might be a misconfigured source
  But Bidir sources can’t be seen with MIBs
- **Solution**: Use Multicast NetFlow
  Individual sources can be tracked
  Collectors can point out high traffic source
Bidir Troubleshooting with NetFlow

- Cisco NFC can capture all traffic to a mcast dest addr
- All sources for a group can be sorted by data rate
- One source is sending significantly more traffic than others
- This host is either misconfigured or its an application problem
Questions?