

# BrainBuzz

## Cramsession

Last updated June, 2000. Click [here](#) for updates.

Click [here](#) to see additional documents related to this study guide. Click [here](#) to receive free practice questions for Cisco exams.

### Contents

Contents .....	1
LAN Segmentation .....	2
Terms in Switching Technology.....	2
Virtual LANs .....	3
VTP .....	4
LAN Emulation .....	5
Model Specific Information .....	6
Catalyst 1900 Switch.....	8
Catalyst 2820 Switch.....	8
Catalyst 3000 Series Switches .....	9
DDR .....	9
QOS Quality of Service .....	10
Tag Switching .....	11
MLS Multi Layer Switching ..	11
Multi-Casting .....	13
TAC Technical Assistance Center .....	16

## Cramsession™ for Cisco CCNP 2.0 BCMSN

### Abstract:

This Cramsession will help you to prepare for Cisco exam 640-504, CCNP 2.0, Building Cisco Multilayer Switch Networks. Exam topics include Building a Campus Network, Managing Campus Traffic Network and Basic Router and Switch Configuration, Spanning Tree Protocol and VLAN.



Notice: While every precaution has been taken in the preparation of this material, neither the author nor BrainBuzz.com assumes any liability in the event of loss or damage directly or indirectly caused by any inaccuracies or incompleteness of the material contained in this document. The information in this document is provided and distributed "as-is", without any expressed or implied warranty. Your use of the information in this document is solely at your own risk, and Brainbuzz.com cannot be held liable for any damages incurred through the use of this material. The use of product names in this work is for information purposes only, and does not constitute an endorsement by, or affiliation with BrainBuzz.com. Product names used in this work may be registered trademarks of their manufacturers. This document is protected under US and international copyright laws and is intended for individual, personal use only. For more details, [visit our legal page](#).

---

# **Cisco CCNP 2.0**

## **LAN Segmentation**

### **Why we need LAN segmentation?**

- deliver more bandwidth per user (fewer user per segment) and at the same time enable traffic between same-segment nodes

### **LAN segmentation with bridges**

- layer 2
- store and forward all frames (including multicast frames)
- easy to set up
- protocol-independent
- replaced by switches

### **LAN segmentation with routers**

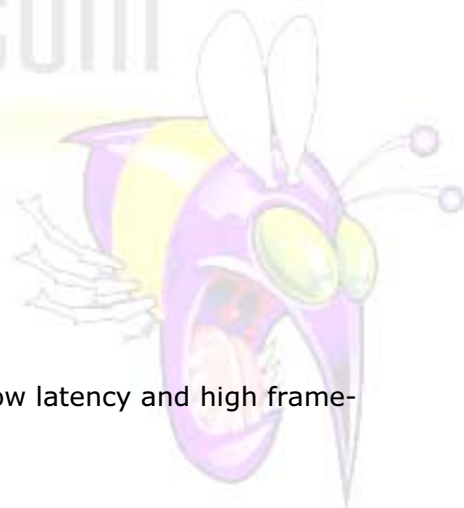
- layer 3
- multiple active paths
- requires configuration

### **LAN segmentation with switches**

- multiple high-speed data exchanges with low latency and high frame-forwarding rates
- expensive but popular

### **Terms in Switching Technology**

- Store-and-forward method – receives the complete frame before forwarding
- Cut-through method –checks the destination address as soon as the header is received and immediately forwards it out
- Source-route switching method – used by Token Ring to forward frames that contain RIFs based on the next ring number
- Rings that are source-route switched have the same ring number, and the switch learns the MAC addresses and Route Descriptors (which is a portion of a RIF that indicates a single hop)
- Switch with only source-route switching could not be used to replace existing source-route bridges, unless you renumber the existing rings



- Fast switching - the default switching type, can be manually enabled using the command: ip route-cache. The first packet is copied into packet memory, while the destination network or host information is located in the fast-switching cache
- Process Switching - slow as there is NO route cache, but slow usually means SAFE. To enable use the command "no protocol route-cache"
- Distributed Switching - to enable use the command "protocol route-cache distributed". Also it requires a second generation VIP line cards
- Optimum Switching - on 7500 this is the default. From its name you can understand what it is – high performance!
- FIFO Queuing – packets leave in first in first out order
- Weighted Fair Queuing – default for all interfaces slower than 2.048Mb; uses session weight as measurement; the higher the weight the lower the priority
- Priority Queuing - allocates a percentage of bandwidth for a specified traffic via protocol or custom queue lists
- Custom Queuing - packets are forwarded based on an assigned priority determined by administrator defined priority lists and groups

## **Virtual LANs**

- logically segment the physical LAN infrastructure into different subnets so that broadcast frames are switched only between ports within the same VLAN
- switches are used in VLANs to act as entry points for end-station devices into switched fabric, and to provide intelligence to group users, ports, or logical addresses and to make filtering and forwarding decisions. Switches also communicate with other switches and router to update themselves
- most VLANs use frame filtering (frame tagging) to examine particular information about each frame based on user-defined offsets, and uniquely assign a user-defined ID to each frame header. This technique is used by the Catalyst 3000 and 5000 series switches for multi-VLAN
- each hub segment connected to a switch port can be assigned to only one VLAN
- VLANs ports on a switch can be assigned statically using a VLAN management application or by working directly within the switch. A more convenient approach, Dynamic VLANs are ports on a switch that can automatically determine their VLAN assignments
- Lane Emulation (LANE) standard provides VLAN communication across shared FDDI backbones, and is supported on the Catalyst 5000 family switches, with each allowing a single link to carry information from multiple VLANs
- VLAN Trunk Protocol (VTP) is a software feature on the Catalyst 5000 that allows mapping of trunking protocols together to create integrated VLAN across management domain

## **VLAN commands**

- Vlan database - enter into VLAN configuration mode
- Vtp domain domain-name - configure a VTP administrative-domain's name
- Vtp password password-value - set the password for the VTP domain
- Vtp server - configure the switch as a server
- Vtp client - put the switch in VTP client mode
- Vtp transparent - put the switch in VTP transparent mode
- Show vtp status - show VTP configuration
- No vtp v2-mode: disable VTP version 2

## **VTP**

- Stands for VLAN Trunk Protocol
- Works at Layer 2
- Nature: Messaging Protocol
- Manages the adding, deleting, and renaming of VLAN management domain
- To Enable a VTP management domain, use the command Set vtp
- VTP information can be distributed to all stations throughout the network, as long as that those stations participate as VLAN configurator
- VTP provides auto intelligence for configuring switches across the network

## **Switch Modes in VTP**

When network has more than 250 VLANs, the switch will change from server to client mode, or from client mode to transparent mode:

- VTP servers advertise their VLAN configurations to switches in the same VTP domain and synchronize. Please note that VLAN configurations are saved on NVRAM
- VTP client acts like VTP servers except they cannot create, edit, or delete VLANs, and that VLAN configurations are NOT saved in NVRAM
- VTP transparent does not participate in VTP, does not advertise its VLAN configuration, and does not synchronize. However, it does forward VTP advertisements that it receives, and can create, edit, and delete VLANs

## **Configuring VTP**

- Global Information in a VTP Advertisement includes VTP Domain Name, VTP Configuration Revision Number, Update Identity, Update Timestamp, MD5 Digest
- VLAN Information in a VTP Advertisement includes VLAN ID, VLAN Name, VLAN Type, VLAN State

- VTP Version 2 has features not supported in VTP version 1, including Token Ring LAN Switching and VLANs, unrecognized Type Length Value, Version Dependent Transparent Mode and Consistency Checks. Please note that all the switches in the VTP domain must run the same VTP version
- In general, don't enable VTP version 2 in the VTP domain unless all the switches are running version 2 as well. However, if the network is Token Ring, you must enable VTP version 2
- VTP Pruning increases bandwidth by controlling traffic flow to the vital trunk links and to block flooded traffic to VLANs in the pruning eligible list. Enabling VTP pruning on a VTP server will enable it on the entire management domain

### **Configuration Guidelines**

- Max 250 active VLANs supported by a switch. Watch out though, as some switch models only support 6 VLANs ...
- When creating a VLAN the switch must be in VTP server or transparent mode
- Default VLAN Configurations - Ethernet Parameters has an ID Range 1-1005. No limit on VLAN Name, and the MTU Size is 1500

### **LAN Emulation**

- Emulated LAN is a group of ATM-attached devices treated as an independent broadcast domain, and can be thought of as a single Ethernet segment or independent Token Ring
- Two components: the LAN Emulation Client (LEC) and LAN Emulation Services
- LEC can be located in the same device(s) as the LANE Services
- LANE services made up of LAN Emulation Configuration Server (LECS), the LAN Emulation Server (LES), and the Broadcast and Unknown Server (BUS), and all of them can be located in the same device or distributed among one, two, or three devices
- To join an emulated LAN, LEC needs to contact the LECS in order to obtain its ATM address, via reconfigured address for the LECS, ILMI or the well-known address of the configuration service
- When two systems are in the same emulated LAN, switches are enough for data transmissions
- When two systems reside in different emulated LANs, a Layer 3 router / switch must be used to interconnect them, regardless of the physical connection
- SSRP for LAN Emulation in Cisco IOS software release 11.2 adds fault tolerance to the standard LAN Emulation and is enabled with LANE / used by redundant server configurations

---

## Model Specific Information

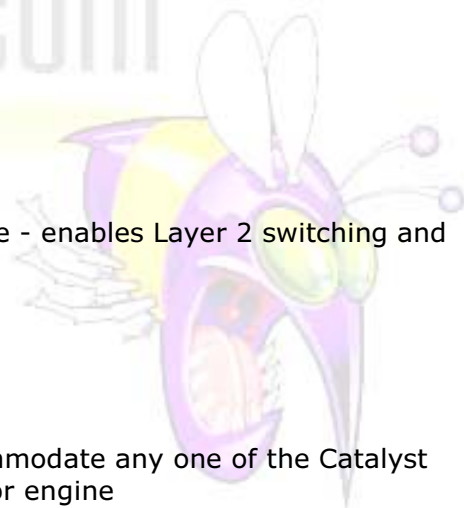
### Catalyst 5000 Series Switches

#### Node

- Demand nodes include Workstations, Personal Computers, Client applications and Terminal Servers
- Resource Nodes include Servers, Network backbone, WAN routers, Minicomputer or mainframe hosts
- Guideline: always place resource nodes on dedicated, not shared links and place local resource nodes close to associated demand nodes
- Local resource means resource node in the same collision domain as the demand node
- Remote resource means resource node located in a different collision domain
- Guideline: always place local resource on segments with high user access, and place global resources on their own segment

#### Architecture

- Modular
- Rack-mounted chassis
- One slot dedicated to the Supervisor engine - enables Layer 2 switching and network management
- High-density switched interfaces
- Two Fast Ethernet interfaces
- 1.2 Gbps backplane
- Catalyst 5002 has two-slots and can accommodate any one of the Catalyst 5000 switching modules and one Supervisor engine
- 5002 uses non swappable power supply redundancy, meaning the power supplies are not hot swappable
- Catalyst 5500 = Catalyst 5000 + LS1010 products + 13 slots + 3.6 Gbps backplane + 5.0Gbps LS1010 bus
- EARL - Encoded Address Recognition Logic. Used to listen and learn MAC addresses and to determine where to send frames
- NMP - Network Management Processor. Used to perform system control, system configuration, system diagnostics, spanning tree per VLAN, and network management
- MCP - Master Control Processor. Used to communicate information between the NMP and the line module communications processors
- LCP - Line Module Communications Processor. Used to process information from MCP across the management bus



- LTL - Local Target Logic. Used for port selection
- CBL - Color Blocking Logic. Used to block in out VLAN traffic
- ARB - Arbiter, one for each line card and on each Supervisor engine Control arbitration for each bus, with different levels of priorities
- SAINT - Synergy Advance Interface and Network Termination with Ethernet MAC
- SAGE - Synergy Advanced Gate Array Engine, = SAINT without Ethernet MAC
- SAMBA - Synergy Advanced Multipurpose Bus Adaptor, used to provide arbitration to the switching bus among the ports and among the line modules
- SAMBA ASIC - works in master mode (supports 13 line cards) or slave mode (supports 48)
- FDDI Module conforms to IEEE 802.10 interoperable LAN/MAN Security (SLS) standard which defines a single protocol data unit known as a Secure Data Exchange (SDE) PDU at MAC-layer
- Security Association Identifier (SAID) is being used as VLAN ID

## **Management & Troubleshooting**

- Out-of-band management - via console port direct connection to the Supervisor module
- In-band management – via SNMP network connection through modem or line module, with a max limit of 8 telnet connections
- RMON has 4 groups, including the Statistics Group for port utilization and error statistics, the History Group for periodic statistics, the Alarm Group for sampling interval and threshold, and the Event Group for logging events to network management station
- SPAN is the Enhanced Switched Port Analyzer that monitors traffic for analysis by other tools
- CWSI CiscoWorks Switched Internet Solutions is a management suite that consists of CiscoView, VlanDirector, and TrafficDirector
- Most of the time cabling is the problem. You can use cable tester device to look for cable breaks. Time Domain Reflectometer measures cable length and impedance. Loose or incorrect device connection can also be a potential source of problems
- Always isolate network segment problems by checking the devices on the same segment to see if they can communicate. In an IP environment, try to use “ping” command to achieve this
- Switch LEDs indicate problem based on color: red = failure, orange = less severe problem. If the Output Fail LED = Red, check the power supply
- To troubleshoot other problems, try using the show commands to find out what is going on: Sh config, Sh int, Sh module, Sh spantree, Sh trunk, Sh vlan, Sh port, Sh mac, Show test and Show log ...etc.

- Protocol Analyzer can capture and display protocol information, while Network monitors can continuously monitor network traffic
- ATM LANE Module - Regarding addressing, every LEC must have a MAC address and every LANE component (LECS, LES, BUS, and LEC) must have a unique ATM address
- Keep in mind that all LECs on the same ATM interface must have the same MAC address being assigned automatically, meaning that LEC MAC addresses are not unique, while all ATM addresses are unique
- A pool of 16 MAC addresses are reserved to be assigned to each LANE module

### **Catalyst 1900 Switch**

- 24 switched 10BaseT ports + 25th AUI port + 1 or 2 fixed 100BaseT ports
- No expansion slots available
- Can be managed via CiscoView or Telnet, CDP and CGMP
- ClearChannel comprises the following components: packet exchange bus (X-bus), forwarding engine, embedded control unit(ECU), management interface, share buffer memory, and switched ports. Also, a 1-Gbps packet exchange bus is deployed
- Supported switching modes include FastForward (cut-through), Fragment Free (cut-through but no collision packet) and Store-and-Forward
- Virtual LANs support - four VLANs supported per switch configurable on a per-port basis, with each VLAN owning bridge MIB and spanning tree
- Support Multicast packet filtering and registrations plus broadcast storm control

### **Catalyst 2820 Switch**

- 24 switched 10BaseT ports + 25th AUI port + 2 expansion slots for high-speed modules like 100BaseT, FDDI, and ATM
- 2048 or 8192 MAC addresses
- Cut-through or store-and-forward switching
- Can be managed via CiscoView or Telnet
- Clear channel architecture
- Supported switching modes include FastForward (cut-through), Fragment Free (cut-through but no collision packet) and Store-and-Forward
- Virtual LANs support - four VLANs supported per switch configurable on a per-port basis, with each VLAN owning bridge MIB and spanning tree
- Support Multicast packet filtering and registrations plus broadcast storm control
- 2820 CLI lets you enter Cisco IOS software commands to configure the LANE client software on the ATM module. It can be accessed from the Catalyst 2820 management console

- Use Port status information for troubleshooting. If status is Enabled, this means the port is active, and is receiving and transmitting packets. Suspended means the port is not active but will become active later. Disabled means the port is inactive and must be manually returned to enabled state

### **Catalyst 3000 Series Switches**

- Designed to work in conjunction with the Catalyst Matrix in stack
- Advanced Feature Set for VLANs, EtherChannel, and full-duplex port operation
- 16 10BaseT port + 4MB / 8MB of memory + 1 MB of Flash memory, real-time clock, console port, SwitchProbe port, AUI port, and 2 slots for operational modules

### **DDR**

- Stands for Dial-on-Demand Routing
- Often used as backup to standard connection methods
- spoofs routing tables to provide the image of full-time connectivity using Dialer interfaces
- filters out interesting packets for establishing, maintaining, and releasing switched connections
- maintains connection using PPP or other WAN encapsulation techniques
- dialer cloud -network formed by the interconnected DDR devices (bundles of potential and active point-to-point connections) , and includes only the intended interconnected devices but not the entire switched media
- Topologies for include Point-to-point, Fully meshed and Hub-and-spoke
- Point-to-Point Topology - two sites are connected to each other, each with a dialer interface and maps the other site's address to a telephone number
- Fully Meshed Topology - recommended for very small DDR networks as it is complex and costly to set up - any-to-any connectivity as each site can call any other site directly
- Hub-and-Spoke- central site is connected to several remote sites, while the remote sites do not call any of the other remote sites.
- Asynchronous connections - used by communication servers or through the auxiliary port on a router, and can be used to support multiple network layer protocols
- Encapsulation Methods for DDR
- PPP -recommended as it supports multiple protocols and is used for synchronous, asynchronous, or ISDN connections. It is also interoperable with different vendors
- HDLC -supported on synchronous serial lines and ISDN connections only, and supports multiple protocols, with NO authentication though
- SLIP - works on asynchronous interfaces and is IP only, with NO authentication

- X.25 - works on synchronous serial lines and a single ISDN B channel

## **QoS Quality of Service**

- refers to the capability of a network to provide better service to selected network traffic over various technologies
- primary goals include dedicated bandwidth, controlled jitter and latency and improved loss characteristics
- 3 fundamental pieces for QoS implementation:
  - within a single network element - queuing, scheduling, and traffic shaping tools
  - signaling techniques for coordinating QoS from end to end between network elements
  - QoS policy, management, and accounting functions to control and administer end-to-end traffic across a network
- 3 basic levels of end-to-end:
  - Best-effort service - basic connectivity with no guarantees
  - Differentiated service - soft QoS - Some traffic is treated better than the rest via statistical preference
  - Guaranteed service - hard QoS - absolute reservation of network resources for specific traffic
- primary Cisco IOS congestion avoidance tool is weighted random early detection - monitoring traffic load at points in the network and stochastically discarding packets if the congestion begins to increase - selectively discard lower priority traffic and provide differentiated performance characteristics for different classes of service
- 2 traffic shaping tools---generic traffic shaping (GTS) and Frame Relay traffic shaping(FRTS)
  - GTS reduces outbound traffic flow by constraining specified traffic to a particular bit rate while queuing bursts of the specified traffic
  - FRTS provides parameters useful for managing network traffic congestion: committed information rate (CIR), FECN and BECN, and DEbit
- 2 link efficiency mechanisms---Link Fragmentation and Interleaving (LFI) and Real-Time Protocol Header Compression(RTP-HC)
  - LFI is designed for low speed links in which serialization delay is significant. It requires that multilink Point-to-Point Protocol (PPP) be configured on the interface with interleaving turned on
  - Real-Time Transport Protocol is for carrying newer multimedia application traffic, including packetized audio and video, over an IPnetwork
- QoS Policy Setting + Policy-Based Routing(PBR)
  - classify traffic based on extended access list criteria, set IP precedence bits, and even route to specific traffic
  - set precedence levels on incoming traffic and using them in combination with queuing tools

- SNAToS + data-link switching plus(DLSw+)
- allows mapping of traditional SNA class of service (CoS) into IP differentiated service

## **Tag Switching**

- 2 principal components: forwarding and control
- forwarding component - uses tag information carried by packets and the tag-forwarding information maintained by a tag switch to perform packet forwarding
- label swapping - when a packet with a tag is received, the switch uses the tag as an index in its Tag Information Base (TIB). If the switch finds a matching entry, then for each component in the entry the switch replaces the tag in the packet with the outgoing tag, and also replaces the link-level information in the packet with the outgoing link-level
- control component - maintaining correct tag-forwarding information among a group of interconnected tag switches
- Tag information can be carried in a packet in many ways, such as a small "shim" tag header inserted between the Layer 2 and the network-layer headers, as part of the Layer 2 header (eg. ATM), as part of the network-layer header (eg. Ipv6). This is why tag switching can be implemented over any media type
- as tag-switching forwarding paradigm is based on label swapping, which is the same as in AT forwarding, tag-switching technology can be applied to ATM switches
- Tag switches support multicast by utilizing data link layer multicast capabilities: all tag switches that are part of a given multicast tree on a common subnetwork must agree on a common tag so that forwarding of multicast packet to all downstream switches on that subnetwork is possible
- Tag switching can mark packets as belonging to a particular class after they have been classified the first time, which is an important aspect of QOS

## **MLS Multi Layer Switching**

### **Definition**

- high-performance hardware-based Layer 3 switching - switches unicast IP data packet flows between subnets using ASIC switching hardware, offloading processor-intensive packet routing from network routers - packet forwarding function is moved to Layer3
- currently for Catalyst 5000 and 2926G series LAN switches
- standard routing protocols including Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), and Intermediate System-to-Intermediate System (IS-IS) are used for route determination

## Components

- MultilayerSwitching-Switching Engine (MLS-SE)--- Catalyst 2926G series switch, or Catalyst5000 series switch with the NFFC or NFFCII
- MultilayerSwitching-Route Processor (MLS-RP)---Catalyst 5000 series Route Switch Module(RSM) or an externally connected Cisco 7500, 7200, 4500, or 4700 series router with software that supports MLS
- MultilayerSwitching Protocol (MLSP)---protocol running between the MLS-SE and MLS-RP
- when MLS is enabled, the RSM or externally attached router continues to handle all non-IP protocols while offloading the switching of IP packets to the MLS-SE

## Flows

- based only on Layer 3 addresses
- NFFC (or NFFC II) maintains Layer 3 switching table (i.e. the MLS cache) for the Layer3-switched flows
- whenever the Layer 3-switching entry for a flow ages out, the flow statistics will be exported to a flow collector application
- maximum MLS cache size is 128K
- cache larger than 32K increases the likelihood that a flow will get forwarded to the router
- when a layer 3 packet is switched from source to destination, the switch performs a packet rewrite based on information learned from the router and stored in the MLS cache
- if Host A and B are on different virtual LANs, when Host A sends a packet to the MLS-RP to be routed to Host B, the MLS-SE recognizes that the packet was sent to the MAC address of the MLS-RP, and will check the MLS cache to find the matching entry
- MLS-SE uses flow mask modes to determine how MLS entries are created, in which the flow mask mode is based on the access lists configured on the MLS router interfaces
- Use the command "show mls entry" to display the mls entry - MLS entries are exported at a burst rate of 1,213 datagrams of 27 flows each. Keep in mind that export rates for MLS entries are depending on the traffic pattern: no typical packet rate
- to specify the minimum flow mask, use the "set mls flow" command

## Implementation

- when using an external router, the ideal set up is one directly attached external router per switch to ensure proper caching
- You can use Cisco high-end routers for MLS when they are externally attached to the switch, make the attachment with multiple Ethernet connections on an

one per subnet basis or by using Fast or Gigabit Ethernet with Inter-Switch Link encapsulation

- End hosts can be connected through any media
- connection between external router and switch must be through standard 10/100 Ethernet interfaces or ISL links
- Router interfaces with input access lists or reflexive access lists cannot participate in MLS. However, you can translate input access lists to output access lists to provide the same effect
- When an output access list is applied, the MLS cache entries for that interface are purged. However, entries associated with other interfaces are not affected at all
- Output access list with log, precedence, tos, or establish options cannot participate in MLS
- Flow mask mode is destination-ip when there is no access list on any MLS-RP interface. When there is a standard access list, the mode is source-destination-ip. When there is an extended access list, the mode is ip-flow

### **Multi-Casting**

- Switches use CGMP, IGMP snooping and GMRP to manage multicast by allowing directed switching of multicast traffic, and also to dynamically configure switch ports so that IP multicast traffic is forwarded only to the appropriate ports
- CGMP and IGMP software components run on both the Cisco router and the switch
- When CGMP/IGMP-capable router receives IGMP control packet, it creates a CGMP or IGMP packet that contains the request type, the multicast group address, and the MAC address of the host
- Request type can either be join or leave
- Router sends the packet to a well-known address to which all switches listen, so that the supervisor engine module interprets the packet and modifies the forwarding table automatically
- To statically configure multicast groups, use the "set cam static" command. Keep in mind that Multicast groups learned through CGMP or IGMP snooping are dynamic, and that static setting supersedes the dynamic settings
- If a spanning-tree VLAN topology changes, the CGMP/IGMP-learned multicast groups on the VLAN are purged and the CGMP/IGMP-capable router generates new multicast group information
- If a CGMP/IGMP-learned port link is disabled, the corresponding port is removed from any multicast group
- To join an IP multicast group, a host sends an IGMP join message specifying its MAC address and the IP multicast group it wants to join. The CGMP/IGMP-capable router builds and multicasts the join message to the well-known address to which the switches listen. Upon receipt of the join message, each switch searches its Enhanced Address Recognition Logic (EARL) table to

determine if it contains the MAC address of the host asking to join the multicast group. If found, the switch creates a multicast forwarding entry in the EARL forwarding table

- EARL automatically learns MAC addresses and port numbers of the IP multicast hosts
- CGMP/IGMP-capable router sends periodic multicast group queries, so that if a host wants to remain in a multicast group, it must respond to the query.
- If after a number of queries the router receives no reports from any host in a multicast group, the router sends a CGMP/IGMP command to the switch to remove the group from the forwarding tables
- CGMP fast-leave-processing allows the switch to detect IGMP version 2 leave messages sent to the all-routers multicast address by hosts on any of the supervisor engine module ports
- GARP Multicast Registration Protocol (GMRP) - Generic Attribute Registration Protocol (GARP) application that provides constrained multicast flooding facility - register and de-register multicast group addresses at the MAC layer throughout Layer 2 connected network. Since it is Layer 3-protocol independent, it can support the multicast traffic of any Layer 3 protocol
- Display information on dynamically learned and manually configured multicast router ports - show multicast router [mod\_num/port\_num][vlan\_id]
- Display total number of multicast addresses groups in each VLAN - show multicast group count [vlan\_id]
- Normal registration mode (the default) - allows dynamic GMRP multicast registration and deregistration on the port
- Fixed registration mode - port ignores any subsequent registrations or de-registrations on other ports, but continues to register multicast groups that are specific to the port
- CGMP Commands:
  - Enable CGMP on the switch - set cgmpenable
  - Verify that CGMP is enabled - show cgmp statistics [vlan\_num]
  - Enable CGMP fast-leave processing on the switch - set cgmp leave enable
  - Verify that CGMP fast-leave processing is enabled - show cgmp leave
  - Display information on those multicast router ports learned dynamically using CGMP - show multicast router cgmp [mod\_num/port\_num][vlan\_id]
  - Display information about multicast groups learned dynamically through CGMP - show multicast group cgmp [mac\_addr][vlan\_id]
  - Display total number of multicast addresses groups in each VLAN that were learned dynamically through CGMP - show multicast group count cgmp [vlan\_id]
  - Display CGMP statistics - show cgmp statistics [vlan\_id]

- Disable CGMP fast-leave processing on the switch - set cgmp leave disable
- Disable CGMP on switch - set cgmpdisable
- IGMP Commands:
  - Enable IGMP snooping on the switch - set igmpenable
  - Verify that IGMP snooping is enabled - show igmp statistics [vlan\_num]
  - Enable IGMP fast-leave processing on the switch - set igmp fastleaveenable
  - Verify that IGMP fast-leave processing is enabled - show igmpleave
  - Display information only on those multicast router ports learned dynamically using IGMP snooping - show multicast router igmp [mod\_num/port\_num][vlan\_id]
  - Disable IGMP snooping on the switch - set igmpdisable
  - GMRP Commands:
    - Enable GMRP on the switch - set gmrpenable
    - Verify GMRP configuration - show gmrp configuration
    - Disable GMRP on individual switch ports - set port gmrp disable[mod\_num/port\_num]
    - Enable the GMRP forward-all option on a switch port - set gmrp fwdall enablemod\_num/port\_num
    - Disable the GMRP forward-all option on a port - set gmrp fwdall disablemod\_num/port\_num
- PIM Protocol Independent Multicast
- You must enable PIM for an interface to perform IP multicast routing
- Enable PIM on an Interface also enables IGMP operation on an interface
- Interface can be configured to be in dense mode, sparse mode, or sparse-dense mode - the modes determine how the router populates its multicast routing table and how the router forwards multicast packets it receives from its directly connected LANs
- For PIM to work it must be in one mode, although there is no default mode setting as multicast routing is disabled on an interface by default
- Dense-mode interfaces are always added to the table
- Sparse-mode interfaces are added to the table only when periodic Join messages are received from downstream routers, or when there is a directly connected member on the interface
- Rather than to enabling only dense mode or only sparse mode you can enable sparse-dense mode- the interface is treated as dense mode if the group is in dense mode, or in sparse mode if the group is in sparse mode

- Commands:
  - ip pim dense-mode - Enable dense-mode PIM on the interface
  - Ip pim sparse-mode - Enable sparse-mode PIM on the interface

### **TAC Technical Assistance Center**

- Staffed by Customer Support Engineers (CSEs)
- Problem report or user question begins when you open a case through Cisco Connection Online, phone or email
- When you contact a TAC, your case is logged, given a call number, and assigned to a CSE who will work with you to answer the question, give advice on system use, help with system configuration, or correct a system malfunction
- 4 priorities
  - Priority 1- existing network is "down", which is critical
  - Priority 2 - network is severely degraded, which has a significant impact
  - Priority 3 -operational performance of the network is impaired, although business operations remain functional
  - Priority 4- little or no impact to the business operation at this moment

Special Thanks to Michael Yu for contributing material for this Cramsession. Make sure to visit his site at:  
<http://michaelyu.freesevers.com>