Release Notes for *Cisco 3200 Series Mobile Access Routers* for Cisco IOS Release 12.2(11)YR

November 11, 2002

These release notes for the Cisco 3200 Series Mobile Access Routers describe the enhancements provided in Cisco IOS Release 12.2(11)YR. These release notes are updated as needed. Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* located on Cisco.com and the Documentation CD.

For a list of the software caveats that apply to Cisco IOS Release 12.2(11)YR, see the "Caveats" section on page 17 and *Caveats for Cisco IOS Release 12.2 T.* The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD.

Contents

This release note contains the following sections:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(11)YR and includes the following sections:

Memory Requirements

Table 1 provides the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.2(11)YR on the Cisco 3200 Series Mobile Access Router.

Table 1 Recommended Memory for the Cisco 3200 Series Mobile Access Router

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory	Runs from
Cisco 3200 Series Mobile Access Router	Cisco 3200 Series IOS IP	IP	c3200-i11-mz	32MB	128MB	RAM
Cisco 3200 Series Mobile Access Router	Cisco 3200 Series IOS IP Plus 3DES	IP PLUS/3DES	c3200-i11k9-mz	32MB	128MB	RAM

Hardware Supported

Cisco IOS Release 12.2(11)YR supports the Cisco 3200 Series Mobile Access Router. The Cisco 3200 Series Mobile Access Router includes the Cisco 3251 Mobile Access Router Card, Cisco 3201 Serial Mobile Interface Card, and the Fast Ethernet Switch Mobile Interface Card (FESMIC).

For detailed descriptions of new hardware features and which features are supported on each router, see the "New and Changed Information" section on page 10. For descriptions of existing hardware features and supported modules, see the configuration guides and additional documents specific to the Cisco 3200 Series Mobile Access Router, which are available on Cisco.com and the Documentation CD at the following location:
http://www.cisco.com/univercd/cc/td/doc/product/access/mar_3200/index.htm

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco router, log in to the router and enter the **show version** EXEC command. The following sample displays command output from a Cisco 3200 series router running Cisco IOS Release 12.2(11)YR:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 3200 Software (C3200-I11-M), Release 12.2(11)YR
! text deleted
Configuration register is 0x0
```

Upgrading to a New Software Release

Youcan download either a software image or a configuration file via TFTP or via the console port, a ROM monitor function over the router console port. After downloading, the file is saved to the Flash memory.

Use console download when you do not have access to a TFTP server.

If you are using a PC to download a Cisco IOS image over the router console port at 115,200 bps, ensure that the PC serial port is using a 16550 universal asynchronous transmitter/receiver (UART). If the PC serial port is not using a 16550 UART, we recommend using a speed of 38,400 or less when downloading an Cisco IOS image over the console port.

Configure the PC communications port to match the router console port as follows:

- 9600 baud
- 8 data bits
- no parity
- 1 stop bit

Follow the steps below to run Xmodem:

Step 1 Move the image file to the local drive where the **xmodem** will execute.

Step 2 Enter the **xmodem** command.

Following is the syntax and descriptions for the xmodem console download command:

xmodem [**-ucyrx**] *destination_file_name*

u	(Optional) Performs an upgrade of the ROMMON. System reboots after the file is upgraded.
c	(Optional) Performs the download using 16-bit cyclic redundancy check (CRC-16) error checking to validate packets. Default is 8-bit CRC.
y	(Optional) Sets the router to perform the download using Ymodem protocol. Default is Xmodem protocol. The protocols differ as follows: • Xmodem supports a 128-block transfer size. Ymodem supports a 1024-block transfer size. • Ymodem uses (CRC)-16 error checking to validate each packet. Depending on the device that the software is being downloaded from, this function might not be supported by Xmodem.
r	(Optional) Image is loaded into DRAM for execution. Default is to load the image into Flash memory.
x	(Optional) Image is loaded into DRAM without being executed.
destination_file_name	The name of the system image file or the system configuration file. In order for the router to recognize it, the name of the configuration file must be in the form of router_confg.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Cisco IOS Release 12.2(11)YR supports the same feature sets as Release 12.2 T, but Cisco IOS Release 12.2(11)YR can include new features supported by the Cisco 3200 series router.

Table 2 lists the features and feature sets supported in Cisco IOS Release 12.2(11)YR.

The table uses the following conventions:

- Platform and Feature Sets column
  - Yes—The feature is supported in the software image.
  - No—The feature is not supported in the software image.
- "In" column—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, "12.2(4)YA" indicates that a feature was introduced in 12.2(4)YA. If a cell in this column is empty, the feature was included in a previous release or the initial base release.

Note These feature set tables contain only list of selected features. These tables are not cumulative—nor do they comprehensively list all the features in each image.

Table 2 Feature List by Feature Set for the Cisco 3200 Series Mobile Access Router

Feature	In	Platform and Feature Set	
		IP	IP PLUS/IPSEC
AAA Server, RADIUS, TACACS			
RADIUS	12.2(11)YQ	Yes	Yes
TACACS	12.2(11)YQ	Yes	Yes
Quality of Service			
Generic Traffic Shaping (GTS)	12.2(11)YQ	Yes	Yes
Class-Based Weighted Fair Queuing (CBWFQ)	12.2(11)YQ	Yes	Yes
Committed Access Rate (CAR)	12.2(11)YQ	No	Yes
Diffserv Compliant WRED	12.2(11)YQ	Yes	Yes
Flow-Based WRED	12.2(11)YQ	Yes	Yes
Low Latency Queuing (LLQ)	12.2(11)YQ	Yes	Yes
Priority Queueing (PQ)	12.2(11)YQ	Yes	Yes
QoS Packet Marking	12.2(11)YQ	Yes	Yes
Random Early Detection (RED)	12.2(11)YQ	Yes	Yes
Weighted Fair Queueing (WFQ)	12.2(11)YQ	Yes	Yes
Weighted RED (WRED)	12.2(11)YQ	Yes	Yes
LFI	12.2(11)YQ	Yes	Yes
RSVP	12.2(11)YQ	No	Yes
Class-Based Ethernet CoS Matching and Marking (802.1p CoS)	12.2(11)YQ	Yes	Yes
802.1p CoS Features Service	12.2(11)YR	Yes	Yes
PPP and Related Protocols			
PPP	12.2(11)YQ	Yes	Yes
Multilink PPP	12.2(11)YQ	Yes	Yes
PPP over Frame Relay	12.2(11)YQ	Yes	Yes
Challenge Handshake Authentication Protocol (CHAP)	12.2(11)YQ	Yes	Yes
MS-CHAP Support	12.2(11)YQ	Yes	Yes
Password Authentication Protocol (PAP)	12.2(11)YQ	Yes	Yes
Easy IP, DHCP, AutoInstall			
Easy IP (Phase I)	12.2(11)YQ	Yes	Yes
DHCP Client	12.2(11)YQ	Yes	Yes
DHCP Relay	12.2(11)YQ	Yes	Yes
DHCP Relay Agent Support for Unnumbered I/F	12.2(11)YQ	Yes	Yes
DHCP Server	12.2(11)YQ	Yes	Yes

Table 2 Feature List by Feature Set for the Cisco 3200 Series Mobile Access Router (continued)

Feature	In	Platform and Feature Set	
		IP	IP PLUS/IPSEC
DHCP Server Options - Import and Autoconfig	12.2(11)YQ	Yes	Yes
DHCP Server - Easy IP Phase 2	12.2(11)YQ	Yes	Yes
AutoInstall using DHCP for LAN interfaces	12.2(11)YQ	Yes	Yes
HTTP Security	12.2(11)YQ	Yes	Yes
NAT			
NAT - Support for NetMeeting Directory (ILS)	12.2(11)YQ	Yes	Yes
Dialer			
Dial Backup	12.2(11)YQ	Yes	Yes
Dial-on Demand	12.2(11)YQ	Yes	Yes
Dialer Idle Timer Inbound Traffic Configuration	12.2(11)YQ	Yes	Yes
Dialer Profiles	12.2(11)YQ	Yes	Yes
Firewall			
Firewall Feature Set	12.2(11)YQ	No	Yes
Firewall Intrusion Detection System	12.2(11)YQ	No	Yes
Context-Based Access Control (CBAC)	12.2(11)YQ	No	Yes
Port to Application Mapping (PAM)	12.2(11)YQ	No	Yes
Frame Relay			
Frame Relay	12.2(11)YQ	Yes	Yes
Frame Relay Encapsulation	12.2(11)YQ	Yes	Yes
Frame Relay End-to-End Keepalive	12.2(11)YQ	Yes	Yes
Frame Relay Fragmentation (FRF.12)	12.2(11)YQ	Yes	Yes
Frame Relay FRF.9 Payload Compression	12.2(11)YQ	Yes	Yes
Frame Relay PVC Interface Priority Queuing	12.2(11)YQ	Yes	Yes
Frame Relay Switching Diagnostics and Troubleshooting	12.2(11)YQ	Yes	Yes
Frame Relay Traffic Shaping (FRTS)	12.2(11)YQ	Yes	Yes
IP Routing and Other Routing Protocols			
IPv4	12.2(11)YQ	Yes	Yes
IPv6	12.2(11)YQ	No	Yes
IP Enhanced IGRP Route Authentication	12.2(11)YQ	Yes	Yes
IP Named Access Control List	12.2(11)YQ	Yes	Yes
IP Precedence for GRE Tunnels	12.2(11)YQ	Yes	Yes
IP Summary Address for RIPv2	12.2(11)YQ	Yes	Yes
Cisco Discovery Protocol (CDP)	12.2(11)YQ	Yes	Yes
Open Shortest Path First (OSPF)	12.2(11)YQ	Yes	Yes

Table 2 Feature List by Feature Set for the Cisco 3200 Series Mobile Access Router (continued)

Feature	In	Platform and Feature Set	
		IP	IP PLUS/IPSEC
OSPF Flooding Reduction	12.2(11)YQ	Yes	Yes
OSPF Not-So-Stubby Areas (NSSA)	12.2(11)YQ	Yes	Yes
OSPF Packet Pacing	12.2(11)YQ	Yes	Yes
Routing Information Protocol (RIP)	12.2(11)YQ	Yes	Yes
Enhanced IGRP (EIGRP)	12.2(11)YQ	Yes	Yes
Enhanced IGRP Stub Routing	12.2(11)YQ	Yes	Yes
Generic Routing Encapsulation (GRE)	12.2(11)YQ	Yes	Yes
Hot Standby Router Protocol (HSRP)	12.2(11)YQ	Yes	Yes
HSRP support for ICMP Redirects	12.2(11)YQ	Yes	Yes
Integrated Routing and Bridging (IRB)	12.2(11)YQ	Yes	Yes
Internet Protocol Control Protocol (IPCP) Address Negotiation	12.2(11)YQ	Yes	Yes
Policy-Based Routing (PBR)	12.2(11)YQ	Yes	Yes
RTP Header Compression	12.2(11)YQ	Yes	Yes
STAC Compression	12.2(11)YQ	Yes	Yes
Transparent Bridging	12.2(11)YQ	Yes	Yes
UDLR Tunnel ARP & IGMP Proxy	12.2(11)YQ	Yes	Yes
Unidirectional Link Routing (UDLR)	12.2(11)YQ	Yes	Yes
IP CEF			
Cisco Express Forwarding (CEF) Support for IP Routing between IEEE 802.1Q VLANS.	12.2(11)YQ	Yes	Yes
Cisco Express Forwarding/distributed Cisco Express Forwarding (CEF/dCEF)	12.2(11)YQ	Yes	Yes
VLANS & Layer 2 Protocols			
Spanning-Tree Protocol (STP)	12.2(11)YR	Yes	Yes
Spanning-Tree Protocol (STP) Extension	12.2(11)YQ	Yes	Yes
Turbo Flooding of UDP Datagrams	12.2(11)YQ	Yes	Yes
IEEE 802.1Q VLAN Support	12.2(11)YQ	Yes	Yes
Virtual LAN	12.2(11)YR	Yes	Yes
Port-Based VLAN	12.2(11)YR	Yes	Yes
802.1q Trunking Support	12.2(11)YR	Yes	Yes
Inter-Virtual LAN Routing Support	12.2(11)YR	Yes	Yes
Virtual Terminal Protocol (VTP) Support	12.2(11)YR	Yes	Yes
IP Multicast			
PIM Version 1	12.2(11)YQ	Yes	Yes
PIM Version 2	12.2(11)YQ	Yes	Yes

Table 2 Feature List by Feature Set for the Cisco 3200 Series Mobile Access Router (continued)

Feature	In	Platform and Feature Set	
		IP	IP PLUS/IPSEC
IGMP Version 1	12.2(11)YQ	Yes	Yes
IGMP Version 2	12.2(11)YQ	Yes	Yes
IP Multicast Load Splitting Across Equal-Cost Paths	12.2(11)YQ	Yes	Yes
IGMP Snooping	12.2(11)YR	Yes	Yes
VPN			
Virtual Private Dial-Up Network (VPDN)	12.2(11)YQ	Yes	Yes
VPN Tunnel Management	12.2(11)YQ	Yes	Yes
L2TP Dial-Out	12.2(11)YQ	Yes	Yes
L2TP Layer2 Tunneling Protocol	12.2(11)YQ	Yes	Yes
L2TP Tunnel Preservation or IP Type of Service (ToS)	12.2(11)YQ	Yes	Yes
IPSEC			
IPSec Network Security	12.2(11)YQ	No	Yes
IPSec Triple DES (3DES)	12.2(11)YQ	No	Yes
IKE Extended Authentication (Xauth)	12.2(11)YQ	No	Yes
IKE Mode Configuration	12.2(11)YQ	No	Yes
IKE Security Protocol	12.2(11)YQ	No	Yes
IKE Shared Secret Using Authentication, Authorization, and Accounting (AAA) Server	12.2(11)YQ	No	Yes
Certification Authority Interoperability (CA)	12.2(11)YQ	No	Yes
Wildcard Pre-Shared key	12.2(11)YQ	No	Yes
Dynamic Crypto Map	12.2(11)YQ	No	Yes
Tunnel Endpoint Discovery	12.2(11)YQ	No	Yes
Manual Security Association	12.2(11)YQ	No	Yes
Secure Shell Version 1			
Secure Shell (SSH) Version 1 Integrated Client	12.2(11)YQ	No	Yes
SSH Version 1 Server Support	12.2(11)YQ	No	Yes
Mobile IP			
Mobile IP	12.2(11)YQ	Yes	Yes
Mobile Networks	12.2(11)YQ	Yes	Yes
Home Agent/Mobile Router Redundancy	12.2(11)YQ	No	No
Mobile Router Preferred Interfaces	12.2(11)YQ	Yes	Yes
Mobile Router Reverse Tunneling	12.2(11)YQ	Yes	Yes
Mobile Router Asymmetric Links	12.2(11)YQ	Yes	Yes
Mobile Router Static and Dynamic Networks	12.2(11)YQ	Yes	Yes

Table 2 Feature List by Feature Set for the Cisco 3200 Series Mobile Access Router (continued)

Feature	In	Platform and Feature Set	
		IP	IP PLUS/IPSEC
Static CCOA	12.2(11)YQ	Yes	Yes
AAA Server and Mobile IP	12.2(11)YQ	Yes	Yes
X.25			
X.25	12.2(11)YQ	Yes	Yes
X.25 Closed User Group	12.2(11)YQ	Yes	Yes
X.25 Failover	12.2(11)YQ	Yes	Yes
X.25 Load Balancing	12.2(11)YQ	Yes	Yes
X.25 over Frame Relay (Annex G)	12.2(11)YQ	Yes	Yes
X.25 over TCP (XOT)	12.2(11)YQ	Yes	Yes
X.25 Remote Failure Detection	12.2(11)YQ	Yes	Yes
X.25 Switch Local Acknowledgement	12.2(11)YQ	Yes	Yes
X.28 Emulation	12.2(11)YQ	Yes	Yes
PAD Sub-Addressing	12.2(11)YQ	Yes	Yes
CUG Selection Facility Suppress Option	12.2(11)YQ	Yes	Yes
X.25 Switch Function (routing/PVC)	12.2(11)YQ	Yes	Yes
SA Agent			
Service Assurance (SA) Agent	12.2(11)YQ	Yes	Yes
Response Time Reporter (RTR)	12.2(11)YQ	Yes	Yes
RTR Enhancements	12.2(11)YQ	Yes	Yes
SNMP			
SNMP	12.2(11)YQ	Yes	Yes
SNMP Support for VLAN Interfaces	12.2(11)YQ	Yes	Yes
SNMP Version 3.0	12.2(11)YQ	Yes	Yes
SNMPv2C	12.2(11)YQ	Yes	Yes
Interface Index Persistence	12.2(11)YQ	Yes	Yes
Network Management and MIB Support	12.2(11)YR	Yes	Yes
Miscellaneous Features			
NTP	12.2(11)YQ	Yes	Yes
Lock-and-Key	12.2(11)YQ	Yes	Yes
Standard IP Access List Logging	12.2(11)YQ	Yes	Yes
Time-Based Access List	12.2(11)YQ	Yes	Yes
Time-Based Access Lists Using Time Ranges	12.2(11)YQ	Yes	Yes
Command-Line Interface (CLI) String Search	12.2(11)YQ	Yes	Yes
Commented IP Access List Entries	12.2(11)YQ	Yes	Yes
Parser Cache	12.2(11)YQ	Yes	Yes

Table 2 Feature List by Feature Set for the Cisco 3200 Series Mobile Access Router (continued)

Feature	In	Platform and Feature Set	
		IP	IP PLUS/IPSEC
Basic Layer 2 Switching	12.2(11)YR	Yes	Yes
Switch-Based Broadcast/Multicast/Unicast Storm Control	12.2(11)YR	Yes	Yes
Source MAC Address/Secure Port	12.2(11)YR	Yes	Yes
Auto-Negotiation and Auto Media-Dependent Interface/Media Dependent Interface Crossed-Over (MDI/MDIX)	12.2(11)YR	Yes	Yes

New and Changed Information

The following section list the new software features supported by Cisco IOS Release 12.2(11)YR for the Cisco 3200 Series Mobile Access Router.

New Software Features in Cisco IOS Release 12.2(11)YR

The following sections list the new software features supported by Cisco IOS Release 12.2(11)YR for the Cisco 3200 Series Mobile Access Router.

Basic Layer 2 Switching

Switching is a technology that alleviates congestion in Ethernet LANs by reducing traffic and increasing bandwidth utilization. An Ethernet LAN switch improves bandwidth by separating collision domains and selectively forwarding traffic to the appropriate LAN segments.

Layer 2 switching is the method by which the Fast Ethernet Switching Mobile Interface Card (FESMIC) learns the source MAC address (6 bytes) of the packets coming in on each port and places them in the forwarding table denoting the port the address resides on. When any MAC frames come in destined for a MAC address that was learned to be residing on a FESMIC port (that is, the MAC address has an entry in the FESMIC authority revocation lists [ARL] table), the packet is forwarded to the port number where that MAC station resides. Note that the packet will only be forwarded to other ports on the switch that are resident in the same Virtual LAN (VLAN).

When MAC addresses come in with unknown destinations, they are flooded to the other ports on the same VLAN and to the Mobile Access Router Card (MARC) host. When the destination MAC replies on a particular port with its source address, the MAC is thus resolved and placed in the ARL table. In this method, bridging is called *plug and play* and as long as source and destination pairs coreside on the FESMIC-attached LAN segments, all the bridges will communicate in a seamless fashion.

The four 10/100 auto-sensing Fast Ethernet ports on FESMIC are automatically defaulted to Layer 2 switch ports once the system is booted up. The FESMIC is in effect a “learning bridge,” as defined in 802.1d, with the added VLAN capabilities of 802.1p/q. The FESMIC is fully capable of line-rate switching for all four FE ports.

Virtual LAN

Virtual LANs (VLANs) are created to provide the segmentation services traditionally provided by routers in LAN configurations. A VLAN consists of a single broadcast domain and solves the scalability problems of large flat networks by breaking a single broadcast domain into several smaller broadcast domains or VLANs. VLANs facilitate moves and changes in a network design more easily than traditional networks. VLANs improve security by isolating groups. High-security users can be grouped into a VLAN, possibly on the same physical segment, so that no users outside that VLAN can penetrate into the VLAN without appropriate routing into the VLAN via secure Layer 3 routing services.

- Broadcast Control

  Just as switches physically isolate collision domains for attached hosts and only forward traffic out a particular port, VLANs provide logical collision domains that confine broadcast and multicast traffic to the bridging domain.

- Security

  If you do not include a Layer 3 router for a VLAN, no users outside of that VLAN can communicate with the users inside the VLAN and vice versa. This extreme level of security is highly desirable for such applications as military applications.

- Performance

  You can assign users who require high-performance networking to their own VLANs. You might, for example, assign to a single VLAN both an engineer who is testing a multicast application and the servers that the engineer is using. The engineer experiences improved network performance by being on a “dedicated LAN,” and the rest of the engineering group experiences improved network performance because the traffic generated by the network-intensive application is isolated to another VLAN. This of course implies some areas of physical isolation of separate VLANs or prioritized service via tagging support and prioritized queuing classes within the switches/bridges of the 802.1q VLAN.

- Network Management

  Software on the switch allows you to assign users to VLANs and later reassign them to another VLAN. Recabling to change connectivity is no longer necessary in the switched LAN environment because network management tools allow you to reconfigure the LAN logically in seconds.

Port-Based Virtual LAN

By default the four FE ports on FESMIC are defaulted to Layer 2 switch ports and all four ports belong to VLAN 1. The user can partition the four switch ports so that they belong to different VLAN groups by using **switchport vlan access <vlan-id>** command.

Following are the brief functional description of FESMIC port-based VLAN:

- Packets received from a port are forwarded only to ports that are members of the same VLAN as the receiving port. VLAN partitions provide hard firewalls for all traffic in different VLANs. Each VLAN has its own MAC address table.
- A VLAN comes into existence when a local port is configured to be associated with the VLAN, or when a user adds a VLAN to the local VLAN database. A maximum of 32 VLANs having VLAN ID in the range of 1-1005 is supported.
- By default, a spanning-tree instance is created for each VLAN.

802.1q Trunking Support

The 802.1q trunk port support is mainly used for VLAN extension from one switch to another 802.1q-capable switch, and for an 802.1q-capable router for inter-VLAN routing. The FESMIC will support both the VLAN extension and inter-VLAN routing in one single module.

A trunk is a point-to-point link between one or more Ethernet switch ports and another networking device, such as a router or a switch. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network. The IEEE 802.1q protocol is an industry-standard trunking encapsulation and that allows multiple VLANS to be switched/multiplexed out to a trunk port destined for the network. The designation of trunk or access is denoted via CLI by the **show interface fastethernet** <*port number*> **switchport** command.

The 802.1q uses an internal tagging mechanism. A tag is inserted within the frame (with ISL, the frame is encapsulated instead). Note that on an 802.1q trunk, one VLAN is not tagged. This VLAN, named the *native* VLAN, must be configured the same on each side of the trunk. This way, we can determine to which VLAN a frame belongs to when we receive a frame without a tag. The EtherType field identifying the 802.1q frame is 0x8100. In addition to the 12-bit VLAN-ID, 3 bits are reserved for 802.1p priority tagging. Also, inserting a tag into a frame that already has the maximum Ethernet size creates a 1522 byte frame that can be considered as a “baby giant” by the receiving equipment.

The FESMIC is capable of 802.1q tagging only; it does not support the Cisco proprietary Inter-Switch Link (ISL) encapsulation, so the FESMIC trunk port would only support the 802.1q trunking encapsulation.

Inter-Virtual LAN Routing Support

In a VLAN network, traffic and stations for multiple network layer subnets (VLANs) can coexist on a single physical LAN segment. In practice, a single VLAN corresponds to a network subnet, and a VLAN trunking capable router such as the Cisco 1700 router is required to forward traffic from a first VLAN to a second VLAN for a Layer 2 switch device such as a Cisco 1900 or Cisco 2900.

The FESMIC will enable the Cisco 3250 MAR to become one of the first few Cisco IOS Ethernet switch routers to deliver the intelligent Layer 2 switching capability and Layer 3 inter-VLAN routing functionality in a single-box solution.

In a typical Cisco IOS manageable Layer 2 switch device such as the Cisco 1900, there would be one Layer 3 virtual interface (SVI) that allows the user to configure the box over a Layer 3 protocol like SNMP or via a Telnet application. This is referred to as the management VLAN for the switch. The default management VLAN is usually the native VLAN. The user configurable management VLAN device allows the user to configure any VLAN to be the management VLAN, but only one virtual Layer 3 interface can exist in one device.

A switch routing module, like FESMIC and the 3600 network module, allows the user to configure more than one virtual Layer 3 interface to support routing capability between the different VLANs and between the virtual Layer 3 interface and any other router interface in the system by using the switch virtual interface. The user can manage the switch router with any switch virtual Layer 3 interface created in the system. The router switch port is not supported in FESMIC. The router switch port is a switch port that is capable of handling Layer 3 switching functionality in hardware, the SVI architecture has the framework to support such a functionality.

- An SVI represents a VLAN of switch ports as one interface to the routing function in the system.
- There is at least one SVI associated with a VLAN.
- It is worth noting that it is not necessary to configure a SVI for every known VLAN. It is necessary to configure a SVI only when the user wishes to route between VLANs or to provide IP host connectivity to the designated management VLAN.

- On the management SVI, an interface VLAN is created at system initialization to permit remote box administration. Additional SVIs exist only when they are explicitly configured by a user.
- Routing protocol and bridging configuration are supported.

STP Support

Spanning-Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between any two stations. When two ports on a switch are detected to be in a loop, the spanning-tree port priority and port path cost setting determine which port is put in the forwarding state and which port is put in the blocking state.

Spanning-Tree Protocol provides a way for switches and bridges to maintain a loop-free topology and to avoid broadcast storms that can occur if loops exist in the topology. The algorithm is fairly complex, but all the bridges connected on the network initially boot into listening state, in which they exchange Bridged Protocol Data Units (BPDUs). These BPDUs are used to calculate the loop-free spanning-tree for the network topology. These BDPUs will set ports that cause loops to block based on a priority scheme. A single bridge will also be designated as the root bridge in the spanning-tree. Ports can be assigned priority that is utilized by the STP algorithm.

For example, connecting a cable in a loop on two ports that are in same VLAN should eventually result in one of the two ports being shut off by the spanning-tree algorithm. The Spanning-Tree Protocol runs on the MARC in Cisco IOS software. BPDUs are generated once every hello-timer interval.

Once the bridge listens, it will then move on to a learning state in which it will store all the SRC MAC addresses it can see on the port in the ARL. After a certain time, the topology converges, and the switch/bridge spanning-tree places all ports to forwarding (this is all ports that are not detected as causing loops), and then MAC packets are bridged normally between ports on the same VLANs.

The 802.1q standard defines the method for running multiple VLANs over a single or multiple physical LAN segments and defines a unique spanning-tree instance to be created on each of the VLAN instances for all the VLANs in a network. A Mono Spanning-Tree (MST) network lacks some flexibility compared to a Per VLAN Spanning-Tree (PVST) network, which runs one instance of Spanning-Tree Protocol (STP) per VLAN. One spanning-tree is created for every new VLAN created on the FESMIC ports. STP is enabled by default on the VLAN and on all newly created VLANs.

Cisco developed PVST+ to allow running several STP instances (even over an 802.1q network) by using a tunneling mechanism. PVST+ can be briefly described as utilizing a Cisco device to connect a MST zone (typically another vendor's 802.1q-based network) to a PVST zone (typically a Cisco 802.1q-based network). There is no specific configuration to enter in order to achieve this. PVST+ is a spanning-tree which allows the coexistence of both PVST and Shared Spanning-Tree (SST) in a mixed vendor environment.

The Spanning-Tree Protocol takes a substantial amount of time to converge to a loop free topology. It fails to take advantage of the point-to-point wiring in todays networks. PVST is Cisco proprietary Per VLAN Spanning-Tree. PVST is enabled on all switch platforms. Rapid Spanning-Tree Protocol (RSTP) aims to improve the operation of spanning-tree while maintaining compatibility with equipment based on the (original) 802.1d spanning-tree, which will be a standardized version of the PVST.

The Cisco Shared Spanning-Tree Architecture documents use the terms *MST* and *SST* to mean *Mono Spanning-Tree* and *Shared Spanning-Tree*, respectively. However, the IEEE 802.1s[10] uses the same terms with exactly opposite meanings; i.e., *MST* means *Multiple Spanning-Tree*, and *SST* is *Single Spanning-Tree*.

When you connect two Cisco switches through 802.1q trunks, the switches exchange spanning-tree BPDUs on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Cisco SST.

For more detailed information on how Spanning-Tree Protocols work, go to:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_6_2/confg_gd/spantree.htm#xtocid170356

802.1p CoS Features Support

The 802.1p class of service provides a simple mechanism to provide priority queuing/quality of service (QoS) to different packets by utilizing the 802.1q VLAN identifier (VID)/TAG field that is a 2-byte extension to the 802.1d MAC header. The 802.1p tag is mapped to different hardware queues in the FESMIC, with different queuing priorities associated with each queue.

The IEEE 802.1p specification defines eight levels of priority (0–7), with priority 7 being the highest priority. This information is carried in the 3-bit priority field of the VLAN tag header.

FESMIC supports up to two class of service (CoS) queues per egress port. For the tagged packets, the incoming packet priority can be mapped to one of the two queues, based on the priority field in the tag header or based on the result of filtering mechanism. For untagged packets, the CoS priority is derived either from a programmable field within the ARL (MAC address table) or from the result of filtering mechanism.

After the packets are mapped into a CoS queue, they are forwarded or conditioned using these scheduling algorithms:

- Strict Priority-Based Scheduling: In this policy, any packets in the two higher priority queues are transmitted first. Only when these queues empty are the packets of lower priority transmitted. The disadvantage of this scheme is potential starvation of packets in lower priority queues.
- Weighted Round-Robin Scheduling: This scheme alleviates the starvation of packets in lower priority queues by providing a certain minimum bandwidth to all queues for transmission. This bandwidth is programmable as the maximum number of packets of each CoS.

  The FESMIC FE ports are set by default to use the strict priority-based scheduling after system boots up, the user can enable the weighted round-robin scheduling via the CLI.

VTP Support

Virtual Terminal Protocol (VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain, also called a *VLAN management domain*, is made up of one or more switches that share the same VTP domain name and that are interconnected with trunks. VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations. The FESMIC supports both VTP version 1 and version 2. But VTP pruning mode is not supported.

- VTP server mode

  The user can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches, based on advertisements received over trunk links. VTP server is the default mode.

- VTP client mode

  This mode functions the same way as VTP server mode functions, but it does not create, change, or delete VLANs on a VTP client.

- VTP transparent mode

  Switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent switches do forward VTP advertisements that they receive from their trunk interfaces.

Switch-Based Broadcast/Multicast/Unicast Storm Control

A packet storm occurs when a large number of broadcast, unicast, or multicast packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is disabled.

Storm control uses high and low thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.

CLI commands are provided for enabling storm control thresholds, and the FESMIC is provisioned appropriately with thresholds for discarding excessive broadcast, multicast, and unicast MAC traffic in order to prevent the switch from being overwhelmed by traffic storms.

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host’s port number to the GDA list for that group. And, when the switch hears an IGMP leave, it removes the host’s port from the CAM table entry.

The purpose of the IGMP snooping is to restrain multicast traffic in a switched network. By default, a LAN switch floods multicast traffic within the broadcast domain, and this can consume a lot of bandwidth if many multicast servers are sending streams to the segment.

Multicast traffic is flooded because a switch usually learns MAC addresses by looking into the source address field of all the frames it receives. But, since a multicast MAC address is never used as source address for a packet and since multicast MAC address do not appear in the MAC address table, the switch has no method for learning them. The IGMP fast-leave snooping process is supported.

Secure MAC Address/Secure Port

Network security is implemented by providing the user with the option to make a port secure by allowing only well-known MAC addresses to send in data traffic or to filter undesired MAC addresses. These MAC addresses can be provisioned into the FESMIC's filter/forward tables as static bridge table entries. Secure MAC address/port security means that if you provision a source MAC address or destination MAC address into a ports ARL filter/forward table as a static bridge table filter entry, the FESMIC can disallow or allow traffic from that MAC address (in the case of a source address), or to that MAC address (in the case of destination address) from being switched between chip ports.

The VLAN provides an inherent level of port security in that if different ports are assigned to different VLANs, traffic will not be switched between these VLANs. It may be routed or trunked but only via appropriate entries in the routing table in the MARC or via trunk provisioning as desired.

Auto-Negotiation and Auto-MDI/MDIX

All of the Ethernet ports in the FESMIC support Ethernet auto-negotiation for the line transmission speed. Auto-negotiation is a feature in which both sides will configure automatically to either 10BASE-TX or 100BASE-TX without any need for provisioning by the user. Auto-negotiation is widely used on most Ethernet interfaces and is generally the default mode of operation. As a subset of the auto-negotiation phase, the FESMIC supports an initialization process called *HP Auto-MDI/MDIX*. HP Auto-MDI/MDIX is enabled whenever the FESMIC is configured for auto-negotiation and whenever HP Auto-MDI/MDIX is a subset of the auto-negotiation phase in any chips supporting it. (In order to have auto-MDIX you must have auto-negotiation)

When an Ethernet interface is enabled, one end of the link must perform MDI crossover so that the transmitter on one end of the data link is connected to the receiver on the other end of the data link (generally a crossover cable is used). The Auto-MDIX feature eliminates the need for this crossover/cross-wired cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase.

Auto-MDI/MDIX runs as a subset of the auto-negotiation phase. During auto-negotiation, the FESMIC transmits on TD+- and receives on RD+- (allowing the crossover detection during this sampling period). When connected via a straight-through cable to a device not supporting HP Auto-MDI/MDIX crossover, the FESMIC automatically switches its transmitter to RD+- and its receiver to TD+-, allowing communication to work correctly with the remote device without a crossover cable.

If both devices support HP Auto-MDI/MDIX crossover capability, a random algorithm in the HP Auto-MDI/MDIX algorithm selects only one of the two sides to perform the crossover function when required.

If the auto-negotiation feature is disabled, Auto-MDI/MDIX will not work since there is no signal transmission at initialization to sample the cabling with. Therefore, as in all systems not supporting HP Auto-MDIX, cabling will need to be correct for the devices being connected. The HP Auto-MDIX feature is disabled (via software which explicitly disables a bit in a register in the FESMIC) if the user selects the configuration of the line speed explicitly rather than leaving the default mode of auto-negotiation. Although it is possible to disable HP Auto-MDIX with auto-negotiation enabled, the current software does not implement an explicit CLI command that allows disabling of the Auto-MDIX during auto-negotiation.

Network Management and MIB Support

Cisco View is a web-based graphical device management application that provides monitoring and configuration features for Cisco Internetworking products (switches, routers, hubs, concentrators, and access servers). Cisco View aides network management by displaying a physical view of a Cisco device, allowing users to easily interact with device components to change configuration parameters or monitor statistics.

The following MIBs need to be added in Cisco IOS for FESMIC, so Cisco View can support VLAN creation and other switch functionality management effectively.

- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Caveats in Cisco IOS Releases 12.2 and 12.2 T are also in Cisco IOS Release 12.2(11)YR. For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*. For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*. These two documents list severity 1 and 2 caveats and are located on Cisco.com and the Documentation CD-ROM.

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in toCisco.com and click **Service & Support**: **Technical Assistance Center**: **Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats - Release 12.2(11)YR

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(11)YR. Only severity 1 through 3 caveats are included.

CSCdy55911

PIM router fails to receive (S,G) when **igmp join** command is used on VLAN.

Workaround:

use interface which is not configured with PIM sparse for debugging the multicast traffic flow as **igmp join** is used for debugging.

CSCdy73731

IP header checksum errors happen under heavy traffic when the interface FastEthernet interface0/0 is configured with the command **no ip mroute-cache**.

Workaround:

Under interface FastEthernet0/0, execute **ip mroute-cache**.

CSCdy74307

Query for ifDesc of IfTable does not show mobile interface.

CSCdy84122

Traceback happens while configuring VTP password.

Workaround:

Do not use the VTP domain name of " ".

CSCdy84519

VLANS cannot be added or deleted until a VTP domain name is configured.

Workaround:

Use the VTP domain name of "NULL" instead of " ".

CSCdy87996

Router crashes due to the **ip wccp version 1** and related commands.

CSCdz21667

After WRR bandwidth x y, not able to save WRR bandwidth 0 0 in NVRAM.

Workaround:

- Once the non-zero value is entered for the WRR feature, use **no wrr-queue bandwidth** *x y* and reload the router.
- Once the router is reloaded, use **wrr-queue bandwidth** *0 0* to turn off the CNG, and save it in the start-up configuration.

CSCin17221

vtpVlanISCRFBackpup object returns incorrect values.

- Returns 0 when CRF backup is not configured for this VLAN.
- Returns false(2) when CRF backup is enabled for the given VLAN.
- Returns true(1) when CRF backup is explicitly disabled for the given VLAN.

Related Documentation

The following sections describe the documentation available for the Cisco 3200 Series Mobile Access Routers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Documentation is available as electronic documents, except for feature modules and the Cisco IOS release notes, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Cisco IOS Release 12.2(11)YR. They are located on Cisco.com and the Documentation CD-ROM (under the heading **Service & Support)**:

- To reach the Release Notes for the Cisco 3200 Series Mobile Access Routers for Cisco IOS Release 12.2(11)YQ, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cisco 3200 Series Routers**: **Release Notes for Cisco 3200 Series Mobile Access Routers for Release 12.2(11)YR**

- To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T*, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2 T**

- To reach product bulletins, field notices, and other release-specific documents, click this path:

  Technical Documents: **Product Bulletins**

- The *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T* documents contain caveats applicable to all platforms for all maintenance releases of Release 12.2. To reach the caveats documents, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Caveats**

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in toCisco.com and click **Service & Support**: **Technical Assistance Center**: **Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents are available for the Cisco 3200 Series Mobile Access Routers on Cisco.com and the Documentation CD-ROM.

Cisco 3200 Series Mobile Access Routers

Documentation specific to the Cisco 3200 Series Mobile Access Routers is available on Cisco.com and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/mar_3200/index.htm

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the Related Documentation section.