Release Notes for *Cisco 3200 Series Mobile Access Routers* for Cisco IOS Release 12.2(15)ZL

June 21, 2004

These release notes for the Cisco 3200 Series Mobile Access Routers describe the enhancements provided in Cisco IOS Release 12.2(15)ZL. These release notes are updated as needed. Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2(15)T* located on Cisco.com and the Documentation CD.

For a list of the software caveats that apply to Cisco IOS Release 12.2(15)ZL, see the "Caveats" section on page 13 and *Caveats for Cisco IOS Release 12.2(15)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(15)ZL 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(15)ZL 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	Runs from
Cisco 3200 Series Mobile Access Router	Cisco 3200 Series IOS IP	IP	c3200-i11-mz	32 MB	128 MB	RAM
Cisco 3200 Series Mobile Access Router	Cisco 3200 Series IOS IP Plus 3DES	IP PLUS/3DES	c3200-i11k9-mz	32 MB	128 MB	RAM

Hardware Supported

Cisco IOS Release 12.2(15)ZL 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 Cisco 3201 FESMIC, 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 the 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(15)ZL:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 3200 Software (C3200-I11-M), Release 12.2(15)ZL
! text deleted
Configuration register is 0x0
```

Upgrading to a New Software Release

You can 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 are 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(15)ZL supports the same feature sets as Release 12.2(15)T, but Cisco IOS Release 12.2(15)ZL 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(15)ZL.

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 Queuing (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 Queuing (WFQ)	12.2(11)YQ	Yes	Yes
Weighted RED (WRED)	12.2(11)YQ	Yes	Yes
Link Fragmentation and Interleaving (LFI)	12.2(11)YQ	Yes	Yes
Resource Reservation Protocol (RSVP)	12.2(11)YQ	No	Yes
Class-Based Ethernet CoS Matching and Marking (802.1p CoS)	12.2(11)YQ	Yes	Yes
Traffic Policing	12.2(11)YQ	Yes	Yes
Custom Queing	12.2(11)YQ	Yes	Yes
Network Based Application Recognition (NBAR)	12.2(15)ZL	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

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 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
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			
Network Address Translation (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 Payload Compression FRF.9	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

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
IP Enhanced Interior Gateway Routing Protocol (EIGRP) Route Authentication	12.2(11)YQ	Yes	Yes
IP Named Access Control List	12.2(11)YQ	Yes	Yes
IP Precedence for Generic Routing Encapsulation (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
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 Internet Control Message Protocol (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
Unidirectional Link Routing (UDLR) Tunnel Address Resolution Protocol (ARP) and Internet Group Management Protocol (IGMP) Proxy	12.2(11)YQ	Yes	Yes
UDLR	12.2(11)YQ	Yes	Yes
Border Gateway Protocol (BGP)	12.2(15)ZL	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

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
Spanning-Tree Protocol (STP) Extension	12.2(11)YQ	Yes	Yes
Turbo Flooding of User Datagram protocol (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
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
Virtual Private Network (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

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
Tunnel Endpoint Discovery	12.2(11)YQ	No	Yes
Manual Security Association	12.2(11)YQ	No	Yes
IPSec Advanced Encryption Standard (AES)	12.2(15)ZL	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
Static Collocated Care-of Address (CCoA)	12.2(11)YQ	Yes	Yes
AAA Server and Mobile IP	12.2(11)YQ	Yes	Yes
Dynamic CCoA	12.2(15)ZL	Yes	Yes
Preferred Home Agent	12.2(15)ZL	Yes	Yes
IPSec over Mobile IP	12.2(15)ZL	Yes	Yes
Quality of Service (QoS) in Mobile IP Environment	12.2(15)ZL	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
Packet Assembler/Disassembler (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			

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
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			
Simple Network Management Protocol (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			
Network Time Protocol (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
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 Crossover (MDI/MDIX)	12.2(11)YR	Yes	Yes
External Modem Support	12.2(15)ZL	Yes	Yes

New and Changed Information

The following section identifies the new software features supported by Cisco IOS Release 12.2(15)ZL for the Cisco 3200 Series Mobile Access Router.

New Software Features in Cisco IOS Release 12.2(15)ZL

The following sections list the new software features supported by Cisco IOS Release 12.2(15)ZL for the Cisco 3200 Series Mobile Access Router.

Dynamic CCoA

Dynamic collocated care-of address (CCoA) allows a mobile router to roam to foreign networks in which foreign agents are not deployed. A roaming interface with CCoA attempts to find foreign agents on the link by soliciting and listening for agent advertisements. If a foreign agent is found, the mobile router attempts to register the foreign agent CCoA, and thereafter tries to register only the foreign agent CCoA. If foreign agent is not found, the mobile router tries to register its CCoA and thereafter tries to register only its CCoA.

CCoA support is essential and must be manually enabled on each roaming interface. By default, only foreign agent CCoA processing is enabled by using the **ip mobile router-service** command.

Preferred Home Agent

Home agent (HA) for the mobile router was previously pre-configured and allowed only one usable home agent configuration. When roaming, a home agent closer to the mobile router may be preferred. This feature will allow a home agent to be selected which is closer to the mobile router.

The HA list is configured on the mobile router. Each HA is configured with a priority. HAs are tried, commencing with the highest priority. If the HA explicitly denies the registration, or if the maximum retry count is exceeded, the mobile router attempts the next highest priority HA.

If the lowest priority HA fails, the mobile router waits until a HA advertisement is received, and then tries to register again starting with the highest priority HA.

IPSec in the Mobile IP Environment

Security associations (SAs) establish trust between two devices in a peer-to-peer relationship. There are two types of security association.

The first is Internet Key Exchange (IKE), which provides negotiation, peer authentication, key management, and key exchange. IKE provides a secure communication channel between two devices that is used to negotiate an encryption algorithm, a hash algorithm, an authentication method, and any relevant group information.

The second type of security association is IPSec Security Association (IPSec SA). Because IPSec SA is unidirectional, it requires separate IPSec SAs be established in each direction to provide non-repudiation, data integrity, and payload confidentiality. Non-repudiation is often necessary to verify that a transaction has taken place, such as a financial exchange between parties. Data integrity verifies that packets are not altered in transit by a third party. Payload confidentiality is provided by encryption.

It might be necessary to protect certain traffic on the mobile network. This is accomplished by enabling IPSec between the mobile router and an IPSec gateway located behind the home agent. Because an IPSec tunnel is established within the Mobile IP tunnel, IKE renegotiation is unnecessary while the mobile router moves about. The result is a secure, scalable mobile networks that is based on standards.

The IPSec encryption algorithm that runs between the mobile router and the IPSec gateway can be either Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES). Note that AES provides greater security than DES and is more efficient than 3DES.

QoS in Mobile IP Environment

Quality of Service (QoS) is a measure of performance that reflects router transmission quality and service availability. The mobile router supports the following QoS features in both static and mobile environments:

- Class Based Weighted Fair Queuing (CBWFQ)
- Network Based Application Recognition (NBAR)
- Class Based Packet Marking—Setting IP Precedence bits
- Class Based Packet Marking—QoS Group Value
- Class Based Packet Marking—Differentiated Services Code Point (DSCP)
- Class Based Policer for the DSCP
- Class Based Ethernet Class of Service (CoS) Matching and Marking (802.1p COS)
- Priority Queuing
- Traffic Policing
- Class Based Policer for the DiffServ Assured Forwarding (AF) Per Hop Behavior
- Link Fragmentation and Interleaving (LFI)
- Weighted Random Early Detection (WRED)
- DiffServ Compliant WRED
- Flow Based WRED
- Random Early Detection (RED)
- Low Latency Queuing (LLQ)
- LLQ for Frame Relay
- Custom Queuing
- Weighted Fair Queuing (WFQ)
- Committed Access Rate (CAR)
- General Traffic Shaping (GTS)

Note None of the Layer3 QoS features, such as Priority Queuing, Custom Queuing, are supported on Virtual Local Area Network (VLAN)–based switched virtual interfaces (SVIs) due to limitations in the Cisco 3201 FESMIC.

For more details on QoS, refer to the following URL:

http://www.cisco.com/en/US/tech/tk543/tech_topology_and_network_serv_and_protocol_suite_home.html

BGP

The Border Gateway Protocol (BGP) provides loop-free interdomain routing between autonomous systems. It exchanges network information with other BGP systems by creating a TCP connection to its peers and exchanging routing updates over this connection, including information about the list of autonomous system paths. (An autonomous system [AS] is a set of routers that operate under the same

administration.) This information can be used to construct a graph of autonomous system connectivity from which routing loops can be pruned and with which autonomous system-level policy decisions can be enforced. BGP is often run among the networks of Internet service providers (ISPs).

External Modem Support

The external general packet radio service/code division multiple access (GPRS/CDMA) modems provide the mobile access router with a Layer 2 roaming interface. The Mobile IP stack would allow Layer 3 roaming IP connectivity for the mobile access router. These external modems will be connected to a serial interface of the mobile access router; the serial interface of the mobile access router will be running in asynchronous mode.

MIB Support for Mobile IP

The following Management Information Bases (MIBs) are supported in Cisco IOS Release 12.2(15)ZL in addition to those supported in Cisco IOS Release 12.2(11)YQ and Cisco IOS Release 12.2(11)YR.

- CISCO-BGP4-MIB
- BGP4-MIB
- CISCO-NBAR-PROTOCOL-DISCOVERY-MIB

For more details on the MIB Support for Mobile IP feature, and for a list of the MIBs supported, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/mar_3200/mar_conf/m010intr.htm#1035866

New Software Features in Release 12.2(15)T

For information regarding the features supported in the Cisco IOS Release 12.2(15)T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/index.htm

This URL is subject to change without notice. If it changes, point your web browser to Cisco.com, and click the following path:

Service & Support: **Technical Documents**: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cross-Platform Release Notes (Cisco IOS Release 12.2(15)T)**

Caveats

Caveats describe unexpected behavior or defects in the 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 Release 12.2(15)T are also in Cisco IOS Release 12.2(15)ZL. For information on caveats in Cisco IOS Release 12.2(15)T, refer to the *Caveats for Cisco IOS Release 12.2(15)T* document. For information on caveats in Cisco IOS Release 12.2, refer to the *Caveats for Cisco IOS Release 12.2* document. These documents list severity 1 and 2 caveats; the documents are located on Cisco.com and the Documentation CD.

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(15)ZL

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(15)ZL. This section includes severity 1 through 3 caveats.

- CSCea68991—NBAR classifies tunneled traffic incorrectly.

  When a service policy with NBAR is applied to an interface configured for Mobile IP roaming with reverse tunneling, the tunneled packets are not classified correctly although QoS Preclassify feature is enabled on the tunnel interface.

  Workaround

  Apply the service policy on the tunnel interface used as the template for Mobile IP tunnels.

- CSCea17729—Pings to a mobile router fail when the mobile router that is acting as foreign agent uses same care-of address (CoA) for mobile node as CCoA.

  Workaround

  Use an address for the foreign agent's CoA that is different from the CCoA.

- CSCea86245—To track the known modem issues in supported modems.
  - When the Wavecom modem connected to the serial interface of the Cisco 3200 router is powered down, the serial interface will not go down and the PPP connection will remain if keepalives are disabled on the serial interface.

    Workaround

    Enable keepalives on the serial interface.
  - When the antenna of the Anydata modem connected to the serial interface of the Cisco 3200 router is detached, the serial interface will not go down and the Point to Point Protocol (PPP) connection will remain if keepalives are disabled on the serial interface.

    Workaround

    Enable keepalives on the serial interface.
  - When the antenna of the Anydata modem connected to the serial interface of the Cisco 3200 router with keepalive enabled is detached or reattached, the PPP connection will go down and fail thereafter due to CHAP authentication failure.

    Workaround

    Power-cycle the Anydata modem.
  - When the antenna of the Airlink Raven Modem connected to the serial interface of the Cisco 3200 router with **dialer persistence** command enabled is detached, the Cisco 3200 router will try to dial out and establish PPP connection although the DCD/DSR signals are down.

    Workaround

    Configure the **modem printer** command on the line corresponding to the serial interface.

  - When the Sony Ericsson handset connected to the serial interface of the Cisco 3200 router is idle for a day, the Cisco 3200 router will no longer be able to communicate with the handset.

    Workaround

    The communication can be restored either by disconnecting and then reconnecting the handset end of the serial cable, or by power-cycling the handset.

  - When the antenna of the Siemens M35 modem connected to the serial interface of the Cisco 3200 router is detached, the Cisco 3200 router will maintain PPP connection although IP traffic cannot be send or received.

    Workaround

    Configure the **register lifetime** <*x*> command under **ip mobile router**. Set *x* to a lesser value if the modem has to be disconnected.

- CSCeb06521—Two mobile tunnels may be created pointing to different home agents.

  When the Priority HA feature is configured and connectivity to registered HA is lost, a CCoA-registered mobile router may not delete its Mobile IP tunnel to that HA after that HA registration is deleted. This may cause problems for traffic passing though the mobile router when it subsequently registers with another HA.

  Workaround

  None.

- CSCeb06827—Europe Vodafone wireless does not work on Mobile IP.

  Vodafone uses Network Address Translation (NAT)/Port Address Translation (PAT) in its network, which causes problems for Mobile IP, because Mobile IP uses either generic routing encapsulation (GRE) or IP encapsulation that lacks a port to translate.

  Workaround

  None.

- CSCdy79531—Layer 3 QoS features will not work on switched virtual interfaces.

  Workaround

  None.

Resolved Caveats - Release 12.2(15)ZL

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(15)ZL. This section includes severity 1 through 3 caveats.

- CSCdu53656

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCea28131

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

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(15)ZL. 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(15)ZL, 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(15)ZL**

- To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.2(15)T*, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2(15)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(15)T* documents contain caveats that apply 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 to Cisco.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.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private Internets and Intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

---

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