



Release Notes for Cisco 3200 Series Mobile Access Routers for Cisco IOS Release 12.3(8)YD1

November 2, 2005

These release notes describe new features and significant software components for the Cisco 3200 Series Mobile Access Router that support the Cisco IOS Release 12.3(8)T, up to and including Release 12.3(8)YD1. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with [Cross-Platform Release Notes for Cisco IOS Release 12.3T](#) located on [Cisco.com](#).

For a list of the software caveats that apply to Release 12.3(8)YD1, see the “Caveats” section on [page 11](#) and [Caveats for Cisco IOS Release 12.3\(8\)T](#). The online caveats document is updated for every maintenance release and is located on [Cisco.com](#).

Contents

- [System Requirements, page 2](#)
- [New and Changed Information, page 9](#)
- [Important Notes, page 10](#)
- [Caveats, page 11](#)
- [Related Documentation, page 13](#)
- [Obtaining Documentation, page 18](#)
- [Documentation Feedback, page 19](#)
- [Cisco Product Security Overview, page 19](#)
- [Obtaining Technical Assistance, page 20](#)
- [Obtaining Additional Publications and Information, page 21](#)



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

© 2005 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(8)YD1 and includes the following sections:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 2](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 3](#)
- [Feature Set Tables, page 3](#)

Memory Requirements

[Table 1](#) describes the memory requirements for the Cisco IOS feature sets supported by the Cisco IOS Release 12.3(8)YD1 on the Cisco 3200 series routers.

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

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory	Runs from
Cisco 3250 Mobile Access Router	Cisco 3250 Mobile Access Router IOS ENTERPRISE BASE	ENTERPRISE BASE	c3250-entbase-mz	32 MB	128 MB	RAM
Cisco 3250 Mobile Access Router	Cisco 3250 Mobile Access Router IOS ADVANCED ENTERPRISE	ADVANCED ENTERPRISE	c3250-adventerprisek9-mz	32 MB	128 MB	RAM

Hardware Supported

The Cisco IOS Release 12.3(8)YD1 supports the Cisco 3200 Series Mobile Access Router.

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 at the following location:

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

This URL is subject to change without notice. If it changes, point your web browser to [Cisco.com](http://www.cisco.com), and click the following path:

Technical Documentation: Access Servers & Routers: Mobile Access Router

Determining the Software Version

To determine which version of Cisco IOS software is currently running on your Cisco 3200 series router, log in to the router and enter the **show version** command in privileged EXEC mode. The following sample output from the **show version** command indicates the version number.

```
router> show version
Cisco IOS Software, 3200 Software (C3250-ENTBASE-M), Version 12.3(8)YD1, RELEASE SOFTWARE (fc1)
Synched to technology version 12.3(10.3)T2
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see [Cisco IOS Software Releases 12.3 T Installation and Upgrade Procedures](#) located on Cisco.com.

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. Release 12.3(8)YD includes new features supported by the Cisco 3200 Series Mobile Access Router. These features are also in Cisco IOS Release 12.3(8)YD1.



Caution

The Cisco IOS images with strong encryption (including, but not limited to, 168-bit [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States will likely require an export license. Customer orders can be denied or subject to delay as a result of United States government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

[Table 2](#) lists the features and feature sets supported in Release 12.3(8)YD1.

The table uses the following conventions:

- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, “12.3(8)YD” indicates that the feature was introduced in Release 12.3(8)YD. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.
- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.



Note

This feature set table contains only a list of selected features, which are cumulative for Release 12.3(7)nn early deployment releases only (*nn* identifies each early deployment release). The table does not list all features in each image; additional features are listed in [Cross-Platform Release Notes for Cisco IOS Release 12.3T](#) and in Release 12.3(8)T Cisco IOS documentation.

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

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
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 Interface	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 Routers (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 Interior Gateway Routing Protocol (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

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

Feature	In	Platform and Feature Set	
		IP	IP PLUS/IPSec
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
Stacker (STAC) Compression	12.2(11)YQ	Yes	Yes
Transparent Bridging	12.2(11)YQ	Yes	Yes
UDLR Tunnel Address Resolution Protocol (ARP) and Interior Gateway Management Protocol (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 and 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

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

Feature	In	Platform and Feature Set	
		IP	IP PLUS/IPSec
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
Virtual Private Network (VPN)			
Virtual Private Dial-Up Network (VPDN)	12.2(11)YQ	Yes	Yes
VPN Tunnel Management	12.2(11)YQ	Yes	Yes
Layer 2 Tunneling Protocol (L2TP)	12.2(11)YQ	Yes	Yes
L2TP Dial-Out	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
Internet Key Exchange (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

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

Feature	In	Platform and Feature Set	
		IP	IP PLUS/IPSec
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
Mobile Router Static Collocated Care-of Address (CCoA)	12.2(11)YQ	Yes	Yes
AAA Server and Mobile IP	12.2(11)YQ	Yes	Yes
Mobile IP - Mobile Networks Deployment MIB	12.3(2)XF	Yes	Yes
Mobile IP - Mobile Router DHCP Support for DCCoA and FA Processing	12.3(7)XR	Yes	Yes
Foreign Agent Route Optimization	12.3(8)YD	Yes	Yes
X.25			
X.25	12.2(11)YQ	Yes	Yes
X.25 Closed User Group (CUG)	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) Subaddressing	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			
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

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

Feature	In	Platform and Feature Set	
		IP	IP PLUS/IPSec
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
Autonegotiation and Auto-Media-Dependent Interface/Media-Dependent Interface Crossover (MDI/MDIX)	12.2(11)YR	Yes	Yes
NetFlow	12.3(2)XF	Yes	Yes
Class Based Traffic Shaping with Hierarchical Policy Map Support on Cisco 3200 MAR FESMIC Interfaces	12.3(7)XS	Yes	Yes
Declassification or Zeroization	12.3(8)YD	Yes	Yes

New and Changed Information

The following sections list the new information about the Cisco 3200 Series Mobile Access Routers for Cisco IOS Release 12.3(8)YD. This information also applies to Cisco IOS Release 12.3(8)YD1.

New Software Features in Release 12.3(8)YD

The following sections describe the new software features supported by the Cisco 3200 Series Mobile Access Routers for Release 12.3(8)YD.

Foreign Agent Route Optimization

The Mobile IP Protocol version 4 does not allow direct routing from one mobile node to another mobile node or to a mobile network behind a mobile router. The protocol requires the traffic to go through the home agent (HA), creating the problem of triangular routing.

The Foreign Agent (FA) Route Optimization feature *injects* mobile network routes into a foreign agent routing table, enabling routing directly from one mobile network to another mobile network. The resulting route optimization improves deployments that are running latency-sensitive applications.

Declassification or Zeroization

Declassification, sometimes referred to as *zeroization*, erases all potentially sensitive information in the router memory. This includes the erasure of the main memory, cache memories and other memories containing packet data, NVRAM, and selected files in Flash, such as crash dumps. Declassification is launched by taking an action. The action is determined by the configuration of the router.

New Software Features in Release 12.3(8)T

For information regarding the features supported in Cisco IOS Release 12.3(8)T, see the Cross-Platform Release Notes and New Feature Documentation links at the following location on [Cisco.com](http://www.cisco.com):

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/index.htm>

This URL is subject to change without notice. If it changes, point your web browser to [Cisco.com](http://www.cisco.com), and click the following path:

Service & Support: Technical Documents: Cisco IOS Software: Release 12.3: Release Notes: Cross-Platform Release Notes (Cisco IOS Release 12.3(8)T)

Important Notes

The following sections contain important notes concerning the new software features supported by the Cisco 3200 Series Mobile Access Router for Release 12.3(8)YD. These notes also apply to Cisco IOS Release 12.3(8)YD1.

Foreign Agent Route Optimization

When the Foreign Agent Route Optimization feature is configured on a Cisco 3200 router, the home agent must be running Cisco IOS Software Release 12.3(11)T or later. Older releases may result in double encapsulation failures.

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 12.3(8)T are also in Release 12.3(8)YD. For information on caveats in Cisco IOS Release 12.3(8)T, see the *Caveats for Cisco IOS Release 12.3(8)T* document. This document lists severity 1 and 2 caveats; the documents is located on [Cisco.com](http://www.cisco.com).



Note

If you have an account with [Cisco.com](http://www.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](http://www.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.

Resolved Caveats - Release 12.3(8)YD1

This section documents possible unexpected behavior by Cisco IOS Release 12.3(8)YD1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei61732

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

- CSCef43691—L2TPv3 and UTI sessions doing PMTUD vulnerable to spoofed ICMP paks.

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef44225—IPSec (ESP-AH) doing PMTUD vulnerable to spoofed ICMP packets.
See note for CSCef43691 above.
- CSCef44699—GRE and IPinIP doing PMTUD vulnerable to spoofed ICMP packets.
See note for CSCef43691 above.
- CSCef60659—More stringent checks required for ICMP unreachable.
See note for CSCef43691 above.
- CSCsa59600—IPSec PMTUD not working [after CSCef44225].
See note for CSCef43691 above.

Open Caveats - Release 12.3(8)YD

This section documents possible unexpected behavior by Cisco IOS Release 12.3(8)YD and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef88449—Traceback is displayed after bootup.
- CSCef91557—UT can not pass traffic with packet size 256 B with IPSec.
- CSCin82407

Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory will be posted to

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>

Resolved Caveats - Release 12.3(8)YD

There are no resolved caveats specific to Cisco IOS Release 12.3(8)YD that require documentation in these release notes.

Related Documentation

The following sections describe the documentation available for the Cisco 3200 series routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on [Cisco.com](http://www.cisco.com) and <http://www.cisco.com/univercd/home/index.htm>.

Use these release notes with these documents:

- [Release-Specific Documents](#)
- [Platform-Specific Documents](#)
- [Cisco Feature Navigator](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3 and are located on [Cisco.com](http://www.cisco.com) and <http://www.cisco.com/univercd/home/index.htm>:

- [Cross-Platform Release Notes for Cisco IOS Release 12.3\(7\)T](#)

On [Cisco.com](http://www.cisco.com) at:

Products and Solutions: Cisco IOS Software: Cisco IOS Software Releases 12.3: Instructions and Guides: Release Notes

On <http://www.cisco.com/univercd/home/index.htm> at:

Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes



Note Cross-Platform Release Notes for Cisco IOS Release 12.3T are located on [Cisco.com](http://www.cisco.com) or on <http://www.cisco.com/univercd/home/index.htm> at **Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Cisco IOS Release 12.3T**.

- Product bulletins, field notices, and other release-specific documents at <http://www.cisco.com/univercd/home/index.htm>
- [Caveats for Cisco IOS Release 12.3](#)

As supplements to the caveats listed in these release notes, see [Caveats for Cisco IOS Release 12.3](#) and [Caveats for Cisco IOS Release 12.3T](#), which contain caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.3 and Cisco IOS Release 12.3T.

On [Cisco.com](http://www.cisco.com) at:

Products & Services: IOS Software: Cisco IOS Software Releases 12.3: Instructions and Guides: Release Notes: Release Notes for Cisco IOS Release 12.3, Part 5: Caveats

On <http://www.cisco.com/univercd/home/index.htm> at:

Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Caveats

- If you have an account on [Cisco.com](http://www.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](http://www.cisco.com) and click **Products and Solutions: Cisco IOS Software: Cisco IOS Software Releases 12.3: Troubleshooting: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

Documentation specific to the Cisco 3200 Series Mobile Access Router 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

On [Cisco.com](http://www.cisco.com) at:

Products and Solutions: Routers: All Routers: Cisco 3200 Series Mobile Access Routers

On <http://www.cisco.com/univercd/home/index.htm> at:

Technical Documentation: Access Servers & Routers: Mobile Access Router

Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on [Cisco.com](http://www.cisco.com). If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with [Cisco.com](http://www.cisco.com). If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on [Cisco.com](http://www.cisco.com) by following the directions found at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On [Cisco.com](http://www.cisco.com) at:

Products and Solutions: Cisco IOS Software: Cisco IOS Releases 12.3: Instructions and Guides

On <http://www.cisco.com/univercd/home/index.htm> at:

Cisco IOS Software: Cisco IOS Release 12.3: Configuration Guides and Command References

Cisco IOS Release 12.3 Documentation Set Contents

[Table 3](#) lists the contents of the Cisco IOS Release 12.3 software documentation set, which is available in electronic form and in printed form if ordered.

On [Cisco.com](http://www.cisco.com) at:

Products and Solutions: Cisco IOS Software: Cisco IOS Releases 12.3: Instructions and Guides

On <http://www.cisco.com/univercd/home/index.htm> at:

Cisco IOS Software: Cisco IOS Release 12.3

Table 3 *Cisco IOS Release 12.3 Documentation Set*

Books	Major Topics
<ul style="list-style-type: none"> <i>Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i> <i>Cisco IOS Configuration Fundamentals and Network Management Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2: Bridging</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2: IBM Networking</i> 	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSw+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server

Table 3 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Technologies Configuration Guide</i> • <i>Cisco IOS Dial Technologies Command Reference</i> 	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface and Hardware Component Configuration Guide</i> • <i>Cisco IOS Interface and Hardware Component Command Reference</i> 	LAN Interfaces Serial Interfaces Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP Configuration Guide</i> • <i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i> • <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> • <i>Cisco IOS IP Command Reference, Volume 3 of 4: Multicast</i> • <i>Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility</i> 	IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Voice Configuration Library</i> • <i>Cisco IOS Voice Command Reference</i> 	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms

Table 3 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Cisco IOS Mobile Wireless Configuration Guide</i> • <i>Cisco IOS Mobile Wireless Command Reference</i> 	General Packet Radio Service
<ul style="list-style-type: none"> • <i>Cisco IOS Terminal Services Configuration Guide</i> • <i>Cisco IOS Terminal Services Command Reference</i> 	ARA LAT NAS1 Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Software System Messages</i> 	

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. 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/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.