New and Changed Information

This section lists the new hardware and software features that are supported in Cisco IOS Release 12.4 and contains the following sections:

Note A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp.

New Hardware Features Supported in Cisco IOS Release 12.4(25)

There are no new hardware features in Cisco IOS Release 12.4(25).

New Software Features Supported in Cisco IOS Release 12.4(25)

There are no new software features in Cisco IOS Release 12.4(25).

New Hardware Features Supported in Cisco IOS Release 12.4(23)

This section describes new and changed features in Cisco IOS Release 12.4(23). Some features may be new to Cisco IOS Release 12.4(23) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(23). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Sync/Async/T1DSU HWICS (HWIC-1T, HWIC-2T, HWIC-2A/S, HWIC-1DSU)

For detailed information about this feature, see the following documents:

Connecting Cisco Serial High-Speed WAN Interface Cards at http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/1_2T_2AS_HWIC.html

Connecting Cisco DSU/CSU High-Speed WAN Interface Cards at http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/DSU_T1_HWIC.html

New Software Features Supported in Cisco IOS Release 12.4(23)

There are no new software features in Cisco IOS Release 12.4(23).

New Hardware Features Supported in Cisco IOS Release 12.4(21)

There are no new hardware features in Cisco IOS Release 12.4(21).

New Software Features Supported in Cisco IOS Release 12.4(21)

This section describes new and changed features in Cisco IOS Release 12.4(21). Some features may be new to Cisco IOS Release 12.4(21) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(21). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

- Debug Commands for Voice Fastpath and VoIP Fastpath
- SNMP—IP Precedence and DSCP Support

Debug Commands for Voice Fastpath and VoIP Fastpath

The **debug voice fastpath** and **debug voip fastpath** commands have been added to monitor and better understand voice fastpath and VoIP fastpath activity on the Cisco AS5350XM and Cisco AS5400XM platforms. For more information about these commands, see the *Cisco IOS Debug Command Reference* at the following URL:

http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html

SNMP—IP Precedence and DSCP Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_snmp_ip_prec_dscp.html

New Hardware Features Supported in Cisco IOS Release 12.4(19)

There are no new hardware features in Cisco IOS Release 12.4(19).

New Software Features Supported in Cisco IOS Release 12.4(19)

There are no new software features in Cisco IOS Release 12.4(19).

New Hardware Features Supported in Cisco IOS Release 12.4(18)

There are no new hardware features in Cisco IOS Release 12.4(18).

New Software Features Supported in Cisco IOS Release 12.4(18)

This section describes new and changed features in Cisco IOS Release 12.4(18). Some features may be new to Cisco IOS Release 12.4(18) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(18). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

SSH Keyboard Interactive Authentication

The SSH Keyboard Interactive Authentication feature is a generic authentication method that can be used to implement different types of authentication mechanisms. Basically, any currently supported authentication method that requires only user input can be performed with this feature. No additional user input is required.

New Hardware Features Supported in Cisco IOS Release 12.4(17)

There are no new hardware features in Cisco IOS Release 12.4(17).

New Software Features Supported in Cisco IOS Release 12.4(17)

There are no new software features in Cisco IOS Release 12.4(17).

New Hardware Features Supported in Cisco IOS Release 12.4(16)

This section describes new and changed features in Cisco IOS Release 12.4(16). Some features may be new to Cisco IOS Release 12.4(16) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(16). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

HWIC-1B-U

A BRI U interface module provides a single basic rate ISDN U WAN interface. The HWIC-1B-U is a replacement interface card of the WIC- 1B-U-V2 WAN Module.

New Software Features Supported in Cisco IOS Release 12.4(16)

There are no new software features in Cisco IOS Release 12.4(16).

New Hardware Features Supported in Cisco IOS Release 12.4(13)

There are no new hardware features in Cisco IOS Release 12.4(13).

New Software Features Supported in Cisco IOS Release 12.4(13)

This section describes new and changed features in Cisco IOS Release 12.4(13). Some features may be new to Cisco IOS Release 12.4(13) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(13). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

- isis metric and isis ipv6 metric Commands
- show pppoe throttled mac Command
- timing wink-duration Command
- vlan ifdescr detail Command
- VRF Aware System Message Logging (Syslog)

isis metric and isis ipv6 metric Commands

The **maximum** keyword has been added to the **isis metric** and **isis ipv6 metric** commands so that you can set the Intermediate System-to-Intermediate System (IS-IS) metric to the maximum link metric. Entering the **maximum** keyword excludes the link from the SPF calculation. If a link is advertised with the maximum link metric, the link is not considered during the normal SPF calculation. When the link is excluded from the SPF, it is not advertised for calculating the normal SPF. An example is a link that is available for traffic engineering, but not for hop-by-hop routing.

For the **isis metric** command, the **maximum** keyword is available under the subinterface configuration mode.

For more details regarding the **maximum** keyword for the **isis metric** command, see the “IS-IS Commands” chapter of the *Cisco IOS Routing Protocols Command Reference* at the following URL:

http://www.cisco.com/en/US/docs/ios/iproute_isis/command/reference/irs_is1.html

For more details regarding the **maximum** keyword for the **isis ipv6 metric** command, see the *Cisco IOS IPv6 Command Reference* at the following URL:

http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_09.html

show pppoe throttled mac Command

The **show pppoe throttled mac** command displays information about MAC addresses from which PPP over Ethernet (PPPoE) sessions are throttled, that is, not currently accepted. PPPoE connection throttling limits the number of PPPoE session requests that can be made from a MAC address within a specified period of time. Use the **show pppoe throttled mac** command to display MAC addresses and ingress ports of users that exceed connection throttling limits that you configured using the **sessions throttle** command.

The following is sample output from the **show pppoe throttled mac** command:

```
Router# show pppoe throttled mac

MAC(s) throttled
MAC                 Ingress Port
00c1.00aa.006c          ATM1/0/0.101
007c.009e.0070          ATM1/0/0.101
0097.009d.007a          ATM1/0/0.101
008c.0077.0082          ATM1/0/0.101
00b5.00a8.009f          ATM1/0/0.101
00a4.0088.00b5          ATM1/0/0.101
```

timing wink-duration Command

The **timing wink-duration** command has been enhanced with the addition of the **receive** keyword and *minimum* and *maximum* arguments. You can specify the timing range for a receive wink-signal duration for a voice port. The syntax for this command is as follows:

timing wink-duration {**time** | **receive** *minimum maximum*}

vlan ifdescr detail Command

The **vlan ifdescr detail** command displays details of the VLAN interfaces. When **vlan ifdescr detail** is configured and a new **encapsulation dot1q** is configured, you see the detail description. The **getmany** command output displays the interface and subinterface. If the router is reloaded saving the configuration, all subinterfaces appear in the detail output.

The following example shows how to enable the display of interface and subinterface details:

```
Router# vlan ifdescr detail
```

interface e0/0.1

encapsulation dot1q 100

interface eo/0.2

encapsulation dot1Q 200

The following is sample output from the **getmany** command:

```
Router# getmany
```

ifDescr.1 = ethernet0/0.1

ifDescr.2 = ethernet0/0.1-802.1QVLAN

VRF Aware System Message Logging (Syslog)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2sr/12_2sra/feature/guide/srvrfslg.html

New Hardware Features Supported in Cisco IOS Release 12.4(12)

There are no new hardware features in Cisco IOS Release 12.4(12).

New Software Features Supported in Cisco IOS Release 12.4(12)

This section describes new and changed features in Cisco IOS Release 12.4(12). Some features may be new to Cisco IOS Release 12.4(12) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(12). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

- Configuring the MWAM Memory Allocation
- IP-RIP Delay Start

Configuring the MWAM Memory Allocation

By default, 32MB is allocated for IO memory on each processor of a Cisco MWAM router. However, the **memory-size iomem** command can be used to reallocate the IO memory from the total available DRAM space, The **no** form of the **memory-size iomem** command is used to revert to the default memory allocation

IP-RIP Delay Start

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_4/12_4_mainline/ipripds.html

New Hardware Features Supported in Cisco IOS Release 12.4(10)

There are no new hardware features in Cisco IOS Release 12.4(10).

New Software Features Supported in Cisco IOS Release 12.4(10)

This section describes new and changed features in Cisco IOS Release 12.4(10). Some features may be new to Cisco IOS Release 12.4(10) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(10). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature

does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

CLI for particle clone and particle pool tuning

The **buffers** command has been enhanced by adding the following keywords:

- **particle-clone**—This keyword enables you to set the number of particle clones in the initial buffer pool settings.
- **header**—This keyword enables you to set the number of particles in the header particle pool.
- **fastswitching**—This keyword enables you to set the number of particles in the fastswitching particle pool.
- **minimum**—This keyword enables you to set the number of minimum buffer elements.

The new syntax is as follows:

buffers {{{**small** | **middle** | **big** | **verybig** | **large** | **huge** | **particle-clone** | **header** | **fastswitching** | *interface-type interface-number*} {**permanent** | **max-free** | **min-free** | **initial**} *number-of-buffers*} | **element** {**permanent** | **minimum**} *elements* | **tune automatic**}

The buffers command has been updated in the Cisco IOS Network Management Command Reference, Release 12.4 at

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_02.html

Configuring the Source IP Address for SNTP Packets

When the system sends an SNTP packet, the source IP address is normally set to the address of the interface through which the SNTP packet is sent. Use the **sntp source-interface** command in global configuration mode if you want to configure a specific interface from which the IP source address will be taken.

GKTMP version Subcommand

The GKTMP **version** subcommand configures the GKTMP version on the Cisco IOS gatekeeper.

For detailed information about this command, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/gktmpv4_3/guide/gk_cli.html

show snmp sysobjectid Command

The **show snmp sysobjectid** command was added to Cisco IOS Release 12.4(10) and is included in the Cisco IOS Network Management Command Reference, Release 12.4 at
http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_16.html

Using the **show snmp sysobjectid** command is a quick way to identify a device. The system object ID is the identifier of the network management subsystem, which is SNMP, and is typically the starting point at which network management applications try to discover a device.

New Hardware Features Supported in Cisco IOS Release 12.4(8)

There are no new hardware features in Cisco IOS Release 12.4(8).

New Software Features Supported in Cisco IOS Release 12.4(8)

This section describes new and changed features in Cisco IOS Release 12.4(8). Some features may be new to Cisco IOS Release 12.4(8) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(8). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

- Chunk Validation During Scheduler Heapcheck
- Cisco High-Speed Intrachassis Module Interconnect (HIMI)
- Selection of Redirecting Number IE

Chunk Validation During Scheduler Heapcheck

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_4/12_4_mainline/cvdsh.html

Cisco High-Speed Intrachassis Module Interconnect (HIMI)

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/serdescn.html

http://www.cisco.com/en/US/docs/ios/12_4/12_4_mainline/srdesfm1.html

Selection of Redirecting Number IE

Prior to the 12.4(8) mainline release, when multiple redirect numbers (IEs) were received on an incoming ISDN call, the last RDN was automatically selected. The **redirecting-selection** keyword has been added to the **isdn incoming ie** command to provide the option of selecting either the first or last RDN when multiple RDN IEs are received. See the following new syntax for the **isdn incoming ie** command:

isdn incoming ie {**channel-id** [**accept-qsig-variant**] | **display** {**dms250** | **transparent**}} [**redirecting-selection** {**first** | **last**}]

The **first** keyword selects the first RDN received; the **last** keyword selects the last RDN received. The **first** and **last** keywords are available only when the **redirecting-selection** keyword is entered.

New Hardware Features Supported in Cisco IOS Release 12.4(7)

This section describes new and changed features in Cisco IOS Release 12.4(7). Some features may be new to Cisco IOS Release 12.4(7) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(7). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Port Adapter Jacket Card

The Port Adapter Jacket Card is used in the I/O controller slot of a Cisco 7200 VXR router with an NPE-G1 or NPE-G2 installed and allows a port adapter to be installed. The NPE-G1 as well as NPE-G2 incorporates I/O controller functionality, so that the I/O controller slot is available for the Port Adapter Jacket Card. The NPE-G1 and NPE-G2 have a third dedicated peripheral component interconnect (PCI) bus that provides additional bandwidth to the chassis. The third PCI bus allows a port adapter with a high bandwidth point requirement to be used with the Port Adapter Jacket Card in the I/O controller slot.

Note The Port Adapter Jacket Card is supported on Cisco IOS Release 12.4 starting with Cisco IOS Release 12.4(7). On Cisco IOS Release 12.4, the Port Adapter Jacket Card works only on Cisco 7200 VXR routers with an NPE-G1 installed since NPE-G2 is not supported in Cisco IOS Release 12.4.

New Software Features Supported in Cisco IOS Release 12.4(7)

This section describes new and changed features in Cisco IOS Release 12.4(7). Some features may be new to Cisco IOS Release 12.4(7) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(7). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

- Alcatel Callback on Busy is Failing Due to Bad Channel_id IE (CSCsc03531)
- Enhance Nextport CLI to Display IFD Queues (CSCei12295)
- IP SLAs Responder

Alcatel Callback on Busy is Failing Due to Bad Channel_id IE (CSCsc03531)

Some ISDN callback signaling-only calls on Alcatel switches were failing. Q.931 debugs showed that the Channel_id IE was malformed (lack of the D-channel selector). Support was added for the malformed Channel_id IE used by Alcatel in a signaling-only setup. The following command syntax is required to enable the feature:

isdn incoming ie channel-id accept-qsig-variant

Enhance Nextport CLI to Display IFD Queues (CSCei12295)

The **show nextport ifd queue** command has been enhanced to obtain and display interface driver (IFD) queue information and statistics to identify audio problems efficiently. The new syntax is as follows:

show nextport ifd queue *slot/port* [**voice** | **data** | **gdb** | **est** | **control**]

IP SLAs Responder

Cisco IOS IP Service Level Agreements (SLAs) is a capability embedded in Cisco IOS software that allows Cisco customers to understand IP service levels, increase productivity, lower operational costs, and reduce the frequency of network outages. In Cisco IOS Release 12.4(7), the Cisco IOS IP SLAs Responder has been added to the IP Base Cisco IOS Packaging. The IP SLAs Responder provides the capability to easily obtain precision network response time measurements between Cisco IOS source and destination devices. In the IP Base feature set, the IP SLAs Responder supports the User Datagram Protocol (UDP) echo, UDP jitter, and Transmission Control Protocol (TCP) connect operations.

For information on Cisco IOS IP SLAs configuration tasks, see the *Cisco IOS IP SLAs Configuration Guide*, Release 12.4. For information on Cisco IOS IP SLAs commands, see the *Cisco IOS IP SLAs Command Reference*, Release 12.4.

New Hardware Features Supported in Cisco IOS Release 12.4(5)

This section describes new and changed features in Cisco IOS Release 12.4(5). Some features may be new to Cisco IOS Release 12.4(5) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(5). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Single Port G.SHDSL WAN Interface Card (WIC-1SHDSL-V3)

A single port multi line G.SHDSL WAN interface card (WIC), or WIC-1SHDSL-V3, provides Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature support for two-wire mode and four-wire mode for SHDSL on the Cisco 1700 series, Cisco 1800 series, Cisco 26xxXM, Cisco 2691, Cisco 2800, Cisco 3700 series, and Cisco 3800 series modular access routers. The WIC-1SHDSL-V3 incorporates the latest firmware and the latest circuitry. For more information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt4wire.html

New Software Features Supported in Cisco IOS Release 12.4(5)

This section describes new and changed features in Cisco IOS Release 12.4(5). Some features may be new to Cisco IOS Release 12.4(5) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(5). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature

does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

- Additional Baud Rates for Serial CEM Network Module
- Gigabit EtherChannel

Additional Baud Rates for Serial CEM Network Module

On a Serial CEM Network Module, you can now use the **clock rate** (interface serial) command to set additional baud rates of 300, 600, 1792K, and 1920K bps. The new values are documented at the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/bbfeamod.html

Gigabit EtherChannel

Gigabit EtherChannel (GEC) allows gigabit per second transmission rates and provides flexible, scalable bandwidth with resiliency and load sharing across links for switches, router interfaces, and servers. GEC combines multiple physical Gigabit Ethernet links into one channel, which manages load sharing of traffic among the links in the channel as well as redundancy if one or more links in the channel should fail; Unicast, broadcast, and multicast traffic is distributed across the links, providing higher performance and redundant parallel paths. If a link fails, traffic is redirected to remaining links within the EtherChannel without user intervention.

Based on the functionality, the GEC is the same as the Fast EtherChannel (FEC) except for the following:

- The interfaces added to the channel are Gigabit Ethernet interfaces.
- Because the onboard Gigabit Ethernet supports jumbo frames, there is a difference in the range of the MTU supported.

On the Cisco 7200, native (onboard) Gigabit Ethernet supports jumbo frames. The maximum transmission unit (MTU) supported on native Gigabit Ethernet ports is 9216. By default, the EtherChannel takes an MTU size in the range of 1500 to 10240 bytes. Once the first interface is added to the channel and an MTU is configured on it, the MTU range of the EtherChannel changes from its default value to the range supported by the first interface added to the channel.

New Hardware Features Supported in Cisco IOS Release 12.4(3)

This section describes new and changed features in Cisco IOS Release 12.4(3). Some features may be new to Cisco IOS Release 12.4(3) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(3). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

- ATM-OC3
- Cisco Small Business 100 Series Routers
- Dial-Only Dial Feature Card for Cisco AS5350XM and Cisco AS5400XM Universal Gateways

ATM-OC3

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_4/12_4_mainline/atm_oc3.html

Cisco Small Business 100 Series Routers

Cisco Small Business Series secure broadband routers are fixed-configuration, small-office routers that support up to five users. They provide the required performance to run basic, secure services in small offices, including firewall and support for Multiprotocol Label Switching (MPLS)-based VPNs. In addition, an easy-to-use configuration tool, Cisco Router and Security Device Manager (SDM), allows nontechnical users to quickly set up the router and its firewall configuration, while remote management capabilities in Cisco IOS software facilitate easy deployment and centralized management for service providers or value-added resellers.

Dial-Only Dial Feature Card for Cisco AS5350XM and Cisco AS5400XM Universal Gateways

The new dial-only dial feature card (DFC) supports 60 (DL-60) to 108 (DL-108) dial calls in a Cisco AS5350XM and Cisco AS5400XM universal gateway. Dial services include modem calls (all modulations), ISDN digital calls, V.110 data calls, and V.120 data calls. Modem pass-through calls are not included in dial services. The dial-only DFC does not support voice or fax services.

For more information about the dial-only DFC, see the following URLs:

http://www.cisco.com/en/US/products/hw/univgate/ps501/prod_installation_guides_list.html

http://www.cisco.com/en/US/products/hw/univgate/ps505/prod_installation_guides_list.html

New Software Features Supported in Cisco IOS Release 12.4(3d)

This section describes new and changed features in Cisco IOS Release 12.4(3d). Some features may be new to Cisco IOS Release 12.4(3d) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(3d). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

MIB Enhancement for MGCP Statistics and Connections

The CISCO-XGCP-MIB is enhanced to generate connection and statistical information for display as part of output for the **show mgcp connection** and **show mgcp statistics** commands.

The following shows relevant sample output for the two commands:

```
Router# show mgcp connection

Endpoint        Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (CO)dec (E)vent[SIFL]
(R)esult[EA] Encryption(K)
1. S1/DS1-0/1   C=2,1,2  I=0x2  P=18204,0  M=2  S=4,4 CO=1 E=0,0,0,0  R=0,0 K=1


Router# show mgcp statistics
```

```
UDP pkts rx 8, tx 9
Unrecognized rx pkts 0, MGCP message parsing errors 0
Duplicate MGCP ack tx 0, Invalid versions count 0
CreateConn rx 4, successful 0, failed 0
DeleteConn rx 2, successful 2, failed 0
ModifyConn rx 4, successful 4, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 4, failed 0
AuditConnection rx 0, successful 0, failed 0
AuditEndpoint rx 0, successful 0, failed 0
RestartInProgress tx 1, successful 1, failed 0
Notify tx 0, successful 0, failed 0
ACK tx 8, NACK tx 0
ACK rx 0, NACK rx 0
IP address based Call Agents statistics:
IP address 10.24.167.3, Total msg rx 8, successful 8, failed 0
```

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

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

New Software Features Supported in Cisco IOS Release 12.4(3)

This section describes new and changed features in Cisco IOS Release 12.4(3). Some features may be new to Cisco IOS Release 12.4(3) but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4(3). To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

- Cisco Communication Media Module Voice Features
- MPLS Label Distribution Protocol
- Scalability for Stateful NAT

Cisco Communication Media Module Voice Features

Support for Non-Facility Associated Signaling (NFAS) and Secure Real-Time Transport Protocol (SRTP)/Secure SRST (SSRST) was added to the Cisco Communication Media Module:

- Secure SRST (SSRST)
- Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways
- ISDN-NFAS with D Channel Backup

For detailed information about these features, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xy/archive/gtcmm.html

MPLS Label Distribution Protocol

The default MPLS label distribution protocol changed from TDP to LDP. If no protocol is explicitly configured by the **mpls label protocol** command, LDP is the default label distribution protocol. See the **mpls label protocol** (global configuration) and **mpls label protocol** (interface configuration) commands for more information.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ldpmib13.html

Note Use caution when upgrading the image on a router that uses TDP. Ensure that the TDP sessions are established when the new image is loaded. You can accomplish this by issuing the **mpls label protocol tdp** global configuration command. Issue this command and save it to the startup configuration before loading the new image. Alternatively, you can enter the command and save the running configuration immediately after loading the new image.

Scalability for Stateful NAT

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_4/12_4_mainline/snatsca.html

New Hardware Features Supported in Cisco IOS Release 12.4

This section describes new and changed features in Cisco IOS Release 12.4. Some features may be new to Cisco IOS Release 12.4 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4. To determine if a feature is new or changed, see the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature oes not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

- 1-Port ADSL WAN Interface Card
- 1-Port DSU/CSU T1 WIC for the Cisco 1700, Cisco 2600, Cisco 3600, and Cisco 3700 Series Routers
- 2-Port GigE/POS
- 8-Port Foreign Exchange Office MRP for the United States with Battery Reversal (MRP3-8FXOM1)
- 16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series (NM-16ESW)
- 256-MB Memory Capacity Enhancement
- ADSL Broadband Router
- ADSL over POTS WIC with Dying Gasp Support (WIC-1ADSL-DG)
- AIM-CUE
- AIM-VPN-HPII-PLUS
- Circuit Emulation over IP (CEoIP)
- Cisco 1711 and Cisco 1712 Security Access Routers

- Cisco 1800 Series Routers (Modular)
- Cisco 2800 Series Routers
- Cisco 3200 Series Mobile Access Routers
- Cisco 3800 Series Routers
- Cisco AS5350XM Universal Gateway
- Cisco AS5400XM Universal Gateways
- Cisco Communication Media Module Voice Features
- Cisco Gigabit Ethernet High-Speed WAN Interface Cards (HWIC-1GE-SFP)
- Cisco IAD2430 Series IOS Reduced IP Subset/Voice
- Cisco Intrusion Detection System (IDS) Network Module (NM-CIDS-K9)
- Cisco MWR 1900 Series Routers
- Cisco Small Business 100 Series Routers
- Cisco SOHO 90 Series and Cisco 830 Series Routers
- Cisco VG224 24-Port Analog Phone Gateway
- Data Compression AIM for the Cisco 2600 Series Routers
- Enhanced Route Switch Controller (ERSC)
- EtherSwitch Service Modules
- High-Density Analog (FXS/DID/FXO) and Digital (BRI) Extension Module for Voice/Fax (EVM-HD)
- HWIC-4ESW
- HWIC-9ESW
- ILPM-4 and ILPM-8
- IP Communications High-Density Digital Voice/Fax Network Module
- IP Communications Voice/Fax Network Module
- Network Analysis Module (NM-NAM)
- NM-1FE-SMF
- NM-8AM-V2, NM-16AM-V2
- NM-16A/S
- NM-CUE-EC
- PWLAN Access Routers
- Serial HWICs
- Single-Port Multiline G.SHDSL WIC
- VIC-4FXS/DID
- VPN Acceleration Module 2+ (VAM2+)
- WIC-4ESW (4-Port Ethernet Switch WIC)

1-Port ADSL WAN Interface Card

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a008017c4a2.html

1-Port DSU/CSU T1 WIC for the Cisco 1700, Cisco 2600, Cisco 3600, and Cisco 3700 Series Routers

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2/12_2z/12_2zl/feature/guide/t1dsu.html

2-Port GigE/POS

The 2-Port Gigabit Ethernet (GigE) feature refers to the MGX-2GE backcard that is controlled and monitored by the MGX-2GE driver. The MGX-2GE driver is a Cisco IOS software subsystem that provides high-speed transport of IP packets at Gigabit Ethernet (GE) rates on each port.

The 2-Port Packet over SONET (POS) feature refers to the MGX-2POS backcard that is controlled and monitored by the MGX-2GE driver. The MGX-2POS driver is a Cisco IOS software subsystem that provides high-speed transport of IP packets at OC-12 rates on each port.

The MGX-2GE driver has the following features:

- Small Form Factor Pluggable (SFP) security
- Link management (auto negotiation)
- Flow control between gigabit links
- Interface MAC address assignment
- MAC address filtering
- Card online insertion and removal (OIR) support
- SFP hot swapping

The MGX-2GE driver performs the following tasks:

- Initializing the GE driver subsystem at Cisco IOS boot time
- Initializing and configuring the GE backcard
- Downloading the GE backcard firmware images
- Collecting statistics for the CLI and SNMP
- Managing alarm and trap events after insertion, removal, and hot swap
- Managing interface status and configuration changes
- Processing events and alarms
- Monitoring data path hardware failures
- Controlling front card and backcard port and card status LEDs

The MGX-2POS driver has the following features:

- SONET alarms processing
- SFP security
- Card OIR support

- SFP Hot Swapping
- Internal and external loopback
- Internal and external clock source

The MGX-2POS driver performs the following tasks:

- Initializing the POS driver subsystem at Cisco IOS boot time
- Initializing and configuring the GE backcard
- Downloading the POS backcard firmware images
- Collecting statistics for the CLI and SNMP
- Managing alarm and trap events after insertion, removal, and hot swap
- Managing interface status and configuration changes
- Processing events and alarms
- Monitoring data path hardware failures
- Controlling front card and backcard port and card status LEDs

8-Port Foreign Exchange Office MRP for the United States with Battery Reversal (MRP3-8FXOM1)

The Cisco ICS 7750 now supports a Multiservice Route Processor (MRP) with eight FXO-M1 ports (MRP3-8FXOM1), which you can use to connect to PBXs or key systems and to provide off-premise connections in the United States, Canada, and other countries. FXO-M1 is an enhancement of FXO with battery reversal and caller ID features. Like the MRP3-8FXS, the MRP3-8FXOM1 also includes an open slot (slot 1) that accepts all voice interface cards (VICs), WAN interface cards (WICs), and Voice/WAN interface cards (VWICs) that are supported on the Cisco ICS 7750.

Note You can use H.323 with the caller ID and battery reversal answer supervision features on the MRP3-8FXOM1. Media Gateway Control Protocol (MGCP) on the MRP3-8FXOM1 is supported, but not with caller ID or battery reversal detection.

16- and 36-Port Ethernet Switch Module for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series (NM-16ESW)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2/12_2z/12_2zj/feature/guide/fz1636nm.html

256-MB Memory Capacity Enhancement

The new 128-MB synchronous dynamic RAM (SDRAM) dual in-line memory module (DIMM) is available for use in all new and existing Cisco 2600XM series routers. This new 128-MB DIMM offers higher-density memory, providing the ability to support memory increases to 256 MB of DRAM. For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/hw/routers/ps259/products_qanda_item0900aecd800f71dd.shtml

ADSL Broadband Router

The Cisco 1701 router (part number CISCO1701-K9) is an ADSL security access router. It is a fixed configuration dual-port router, designed in a desktop form factor, that provides primary WAN access through ADSL (ADSL over plain old telephone service [POTS]) and a backup link through ISDN (BRI-S/T). It also provides standard Cisco IOS security capabilities through support for IPSec Virtual Private Network (VPN), stateful inspection firewall, and intrusion detection system.

The Cisco 1701 ADSL security router is ideal for providing secure, reliable Internet and corporate network connectivity to enterprise small branch offices and small- and medium-sized businesses. It offers business-class ADSL over POTS service with a redundant ISDN WAN link to ensure high availability of critical business applications. The Cisco 1701 router also supports a wide range of integrated security services, as well as advanced quality of service (QoS) features to prioritize mission-critical data traffic.

ADSL over POTS WIC with Dying Gasp Support (WIC-1ADSL-DG)

The ADSL over POTS WIC with dying gasp support (part number WIC-1ADSL-DG) conforms to Cisco WICs/VICs and enables ADSL services to be deployed. The WIC supports the Annex A, G.992.1 technical specifications and complies with ANSI T1.413 Issue 2. It targets the business ADSL over POTS service worldwide. This ADSL over POTS WIC supports a dying gasp message that is sent by the customer premises equipment device (for example, a Cisco 1760 access router with an installed WIC-1ADSL-DG) to the digital subscriber line access multiplier (DSLAM) when a power outage occurs (that is, the WIC-1ADSL-DG supports DSLAM notification on power loss).

AIM-CUE

The AIM-CUE Advanced Integrated Module provides support for Cisco Unity Express voice mail and auto attendant for either Cisco CallManager or Cisco CallManager Express IP Communications networks. The AIM-CUE is supported on the Cisco 2600XM, Cisco 2691, and Cisco 3700 series voice gateway routers on an AIM form factor. For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/2600/hardware/module/installation/guide/aims_ins.html

AIM-VPN-HPII-PLUS

Cisco 3825 and Cisco 3845 Integrated Services Routers with the AIM-VPN-HPII-PLUS will be supported with IPSec stateful failover. Cisco 3800 on-board crypto is not supported with IPSec stateful failover at this time.

Circuit Emulation over IP (CEoIP)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_4/interface/configuration/guide/hbbfeamo.html

Cisco 1711 and Cisco 1712 Security Access Routers

Cisco IOS Release 12.3(7)T provides support for the Cisco 1711 and Cisco 1712 Security Access routers. The Cisco 1711 and Cisco 1712 are fixed configuration routers that provide secure Internet connectivity and dial backup using the analog modem port (on the Cisco 1711) or the ISDN port (on the Cisco 1712) if your primary connection fails. These routers include an integrated 4-port 10/100-Mbps Ethernet switch in WIC slot 0, an onboard Fast Ethernet port external interface, and a Virtual Private Network (VPN) module in the router's internal slot. These ports enable you to configure a demilitarized zone (DMZ) using VLANs and Cisco IOS firewall features.

Cisco 1800 Series Routers (Modular)

Cisco IOS Release 12.3(8)T4 introduces and supports the Cisco 1800 series routers (modular). The Cisco 1800 series routers (modular) include the Cisco 1841 in this release. The Cisco 1841 router is a data-only router with two HWIC/WIC/VWIC slots, capable of supporting single-wide HWICs, and one advanced integration module (AIM) slot. It can be placed on a desktop or wall-mounted. The Cisco 1841 does not provide inline power support.

For detailed information about these new routers, see the "Cisco 1800 Series Routers (Modular)" section on page 31.

Cisco 2800 Series Routers

Cisco IOS Release 12.3(8)T4 introduces and supports the Cisco 2800 series integrated services routers. The Cisco 2800 series integrated services routers include the Cisco 2801, Cisco 2811, Cisco 2821, and Cisco 2851 routers.

For detailed information about these new routers, see the "Cisco 2800 Series Routers" section on page 46.

Cisco 3200 Series Mobile Access Routers

Cisco IOS Release 12.3(11)T introduces and supports the Cisco 3200 series of mobile access routers, which includes the Cisco 3220 and the Cisco 3250.

For detailed information about these new routers, see the "Cisco 3200 Series Mobile Access Routers" section on page 53 and the documents at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps272/products_technical_reference_chapter09186a008022b2dc.html

Cisco 3800 Series Routers

Cisco IOS Release 12.3(11)T introduces and supports the Cisco 3800 series routers, which include the Cisco 3825 and the Cisco 3845.

For detailed information about these new routers, see the "Cisco 3800 Series Routers" section on page 70 and the documents at the following location:

http://www.cisco.com/en/US/products/ps5855/index.html

Cisco AS5350XM Universal Gateway

The Cisco AS5350XM universal gateway is a one rack unit (1RU) universal gateway that provides best of class voice, fax, and remote access services at densities up to 8T1/7E1. The Cisco AS5350XM universal gateway has three feature card slots and two 10/100/1000 Ethernet LAN ports.

For more information about the Cisco AS5350XM universal gateway, see the following URL:

http://www.cisco.com/en/US/products/ps6268/index.html

Cisco AS5400XM Universal Gateways

The Cisco AS54000XM universal gateway is a one rack unit (1RU) universal gateway that provides best of class voice, fax, and remote access services at densities up to CT3. The Cisco AS5400XM universal gateway has seven feature card slots and two 10/100/1000 Ethernet LAN ports.

For more information about the Cisco AS5400XM universal gateway, see the following URL:

http://www.cisco.com/en/US/products/ps6269/index.html

Cisco Communication Media Module Voice Features

Cisco IOS Release 12.3(14)T introduces and supports the Catalyst 6500 Series and Cisco 7600 Series Communication Media Module with SNMP, MLPP, MCID, HW-MTP with RFC 2833, enhanced QSIG, and native T.l38 fax relay.

Cisco Gigabit Ethernet High-Speed WAN Interface Cards (HWIC-1GE-SFP)

The Cisco Gigabit Ethernet high-speed WAN interface card (HWIC-1GE-SFP) is a high-speed interface card providing copper and optical Gigabit Ethernet connectivity for Cisco modular access routers.

Cisco IAD2430 Series IOS Reduced IP Subset/Voice

The Cisco IAD2430 is the next generation integrated voice and data services platform for service providers, building on the industry leading Cisco IAD2420 series IAD. The Cisco IAD2430 series offers a major leap forward in price performance and enhanced software functionality such as MGCP SRST used to accelerate the migration from TDM to VoIP cost efficiently. The Cisco IAD2430 series harnesses the maturity of the Cisco IAD2420 series software and enhances functionality by providing more capabilities such as denser interfaces (up to 24 FXS or up to 2 voice and 2 data T1s), encryption, and DC power backup while maintaining its 1-RU form factor for space saving Service Provider Managed Services deployment.

Cisco Intrusion Detection System (IDS) Network Module (NM-CIDS-K9)

The Cisco Intrusion Detection System (IDS) network module is installed in any one of the network module slots on the Cisco 2600XM, Cisco 3600, and Cisco 3700 series routers to provide full-featured intrusion-protection services within the router. The Cisco IDS network module provides the ability to:

- Inspect all traffic traversing the router.
- Identify malicious activity.
- Terminate illegitimate traffic.
- Integrate the Cisco IDS functionality into the branch office router.

- Implement full-featured Cisco IDS at your remote branch offices.
- Install the Cisco IDS network module in any one of the network module slots on the Cisco 2600XM, Cisco 3600, and Cisco 3700 series routers.

Note The IDS network module is not supported on the Cisco 3620, Cisco 3631, Cisco 3640, and Cisco 3640A modular access routers.

The Cisco IDS network module provides up to 45 Mbps of intrusion detection capability. Only one Cisco IDS network module is supported per router, and it is not hot-swappable. The network module runs the latest version of the Cisco IDS software, version 4.1.

You can manage and retrieve events from the Cisco IDS network module through Cisco IOS CLI or through one of these Cisco IDS managers—IDS Device Manager or Management Center for IDS Sensors.

The Cisco IDS network module supports the following interfaces:

- One internal 10/100 Ethernet port—connects to the router's backplane.
- One external 10/ 100-based Ethernet port—used for device management (management of other routers and/or PIX Firewalls to perform shunning) and command and control of the Cisco IDS network module by the Cisco IDS manager.

For instructions on accessing the Cisco IDS documentation on Cisco.com, see the *Cisco Intrusion Detection System (IDS) Hardware and Software Version 4.1 Documentation Guide* that shipped with your IDS router module. It is at the following URL:

https://www.cisco.com/en/US/docs/security/ips/4.1/installation/guide/hwguide.html

For basic installation information, see "Connecting Cisco Intrusion Detection System Network Modules" in the *Cisco Network Modules Hardware Installation Guide* at the following URL:

https://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/securenm.html

Cisco MWR 1900 Series Routers

Cisco IOS Release 12.3(11)T introduces and supports the Cisco MWR 1900 series routers, which include the Cisco MWR 1941-DC Mobile Wireless Edge Router.

For detailed information about these new routers, see the "Cisco MWR 1900 Series Routers" section on page 33 and the documents at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/ipran/2_0/1941/index.htm

Cisco Small Business 100 Series Routers

Cisco IOS Release 12.3(14)T introduces and supports the Cisco Small Business 100 Series Routers.

Cisco SOHO 90 Series and Cisco 830 Series Routers

The Cisco SOHO 91, SOHO 97, 831, and 837 have the following additional features over existing broadband routers:

- A 4-port Ethernet switch
- A hardware encryption coprocessor

- A virtual aux port that uses the same physical port as the console port
- A newer MPC857DSL processor

Cisco VG224 24-Port Analog Phone Gateway

The Cisco VG224 is a 24-port analog phone gateway based on Cisco IOS software. The platform has 24-port FXS through an RJ-21 connector and two 10/100BASE-T interfaces. The Cisco VG224 is supported on CCM Release 3.2 or later. For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/hw/gatecont/ps2250/ps5627/index.html

Data Compression AIM for the Cisco 2600 Series Routers

The AIM-COMPR2-V2 provides hardware compression for up to two full-duplex E1 links. Supported are the industry standard Limpel Zif Stac (LZS) and Microsoft Point-to-Point Compression (MPPC) compression algorithms over Point-to-Point Protocol (PPP) or Frame Relay. High-Level Data Link Control (HDLC) is not supported.

The new AIM-COMPR2-V2 card replaces the AIM-COMPR2 compression AIM for the Cisco 2600XM series routers.

Enhanced Route Switch Controller (ERSC)

The enhanced route switch controller is a faster route switch controller (RSC) card that supports more calls, better redundancy, and stratum 3 clocking. The RSC is a printed circuit board that connects to the server backplane and performs routing functions. It also supports environmental monitoring and board initialization at power up.

EtherSwitch Service Modules

Cisco IOS Release 12.3(14)T provides support for four new EtherSwitch service network modules for the following routers:

- Cisco 2691
- Cisco 2811
- Cisco 2821
- Cisco 2851
- Cisco 3700 series
- Cisco 3800 series

The new Cisco EtherSwitch service modules greatly expand the capabilities of integrated switching within Cisco routers by providing support for new features such as IEEE 802.3af Power over Ethernet (PoE), local Layer 3 switching, Cisco Network Administrator and Cisco Emergency Responder, and Cisco StackWise interfaces (available on NME-XD-24ES-1S-P only), as well as software feature parity with Cisco Catalyst 3750 series switches. Additionally, the new Cisco EtherSwitch service modules are the first modules that can take full advantage of the increased performance capabilities and new form factors of the enhanced network module slot on Cisco integrated service routers.

The following Cisco EtherSwitch network modules are supported in Cisco IOS Release 12.3(14)T:

- NME-16ES-1G-P—One 16-port 10/100 Cisco EtherSwitch service module w/802.3af, 1 10/100/1000 port, and IP Base.
- NME-X-23ES-1G-P—One 23-port 10/100 Cisco EtherSwitch service module w/802.3af, 1 10/100/1000 port w/ 802.3af, and IP Base.
- NME-XD-24ES-1S-P—One 24-port 10/100 Cisco EtherSwitch service module w/802.3af, 1 SFP, Cisco StackWise connectors, and IP Base.
- NME-XD-48ES-2S-P—One 48-port 10/100 Cisco EtherSwitch service module w/ 802.3af, 2 SFPs, and IP Base.

High-Density Analog (FXS/DID/FXO) and Digital (BRI) Extension Module for Voice/Fax (EVM-HD)

For detailed information about this feature, refer to the following document:

http://www.cisco.com/en/US/products/hw/modules/ps2617/products_configuration_example09186a0080513001.shtml

HWIC-4ESW

The HWIC-4ESW is a 4-port 10/100 Ethernet switch that is capable of providing inline power to IP phones and access points on all 4 ports when used in conjunction with the ILPM-4 daughter card.

HWIC-9ESW

The HWIC-9ESW is a 9-port 10/100 Ethernet switch that is capable of providing inline power to IP phones and access points on 8 ports (not 9) when used in conjunction with the ILPM-8 daughter card. The HWIC-D-9ESW is in a doublewide form factor and is usable only in those routers that can provide doublewide interface card slots: the Cisco 2800 series and Cisco 3800 series, so far.

ILPM-4 and ILPM-8

The ILPM-4 and ILPM-8 are optional daughter cards to be used in conjunction with the HWICs to provide inline power on those ports that can carry power. These daughter cards require that the router have installed in it an optional –48 volt power supply. The daughter cards use this supply to provide inline power. The ILPM-4 is used only with the HWIC-4ESW, and the ILPM-8 is used only with the HWIC-D-9ESW.

IP Communications High-Density Digital Voice/Fax Network Module

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/hdd_vfnm.html

IP Communications Voice/Fax Network Module

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2/12_2z/12_2zj/feature/guide/flex_dsp.html

Network Analysis Module (NM-NAM)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xd/feature/guide/nm_nam.html

NM-1FE-SMF

The 100BASE-FX SMF Network Module expands fiber Ethernet connectivity options for the Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, Cisco 3725, and Cisco 3745 routers. This network module can transmit at distances of up to 10 kilometers and supports the IEEE 802.3ah Ethernet standard.

NM-8AM-V2, NM-16AM-V2

The NM-8AM-V2 and NM-16AM-V2 network modules (NMs) serve as integrated analog modem network modules for the modular access routers. These network modules terminate either eight or sixteen analog modem connections through POTS interfaces.

Hardware Specifications

Each network module consists of eight or sixteen analog modems.

Table 15 Hardware Specifications for Analog Modems: Cisco 2600XM Series and Cisco 3600 Series Routers

Characteristic	Description
Number of supported NMs	• Cisco 2610XM, 2620XM, 2650XM: 1 • Cisco 2691: 1 • Cisco 3660: Up to 6 • Cisco 3725: Up to 2 • Cisco 3745: Up to 4
Dial-related	• Autosensing International Pocket Exchange (IPX), TCP/IP, AppleTalk Remote Access (ARA), AppleTalk Control Protocol (ATCP) • Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP), Multilink PPP (MP) • Reverse Telnet support for LAN-based dial-out • Domain Name System (DNS) Domain Name Server support • MNP 2-4 for high performance under all line conditions

Table 15 Hardware Specifications for Analog Modems: Cisco 2600XM Series and Cisco 3600 Series Routers (continued)

Characteristic	Description
Carrier protocols	• BELL 103, and 212a • ITU-T V.21 at 300 bps • ITU-T V.22 A/B • ITU-T V.22bis (with V.54 loop back) • ITU-T V.23 at 75/1200 bps • ITU-T V.32 • ITU-T V.32 turbo up to 19,200 bps • ITU-T V.32bis • ITU-T V.34 • ITU-T V.34+ up to 33,600 bps • ITU-T V.34bis • ITU-T V.90 • V.92 Quick Connect
Error-correcting link access protocols	V.42 Link Access Procedure for Modems (LAPM), MNP 2-4
Fax protocols	• EIA 578 Class 2 Fax • Group 3 Class 1 and Class 2 Fax • ITU-T V.17 • ITU-T V.21 channel 2 • ITU-T V.27ter • ITU-T V.29
Compression protocols	V.42bis (includes MNP 5)
Cables	16 RJ-11 connectors

NM-16A/S

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtnm16as.html

NM-CUE-EC

Cisco IOS Release 12.4(1) introduces support for the NM-CUE-EC, Cisco Unity Express Network Module with Enhanced Capacity. This network module provides increased capacity compared with the NM-CUE and supports Cisco Unity Express Release 2.1 and later releases. The NM-CUE-EC supports up to 16 ports of concurrent voice mail or automated attendant sessions.

PWLAN Access Routers

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xd/feature/guide/PWLANar.html

Serial HWICs

Cisco IOS Release 12.3(14)T supports five new serial and asynchronous high-speed WAN interface cards (HWICs). Serial HWICs provide highly flexible connections for Cisco 1800, Cisco 2800, and Cisco 3800 Integrated Services routers. These HWICs allow customers to easily enable applications such as WAN aggregation, legacy protocol transport, console server, and dial access server. Customers can mix and match HWICs to tailor cost-effective solutions for common networking problems such as remote network management, external dial modem access, low density WAN aggregation, legacy protocol transport, and high port density support.

There are five serial and asynchronous HWICs:

1. HWIC-4T—Four high-speed serial ports
2. HWIC-4A/S—Four low-speed synchronous/asynchronous serial ports
3. HWIC-8A/S-232—Eight low-speed synchronous/asynchronous serial ports, EIA-232 only
4. HWIC-8A—Eight async EIA-232 serial ports
5. HWIC-16A—Sixteen async EIA-232 serial ports

Single-Port Multiline G.SHDSL WIC

A single-port multiline G.SHDSL WAN interface card (WIC), or WIC-1SHDSL-V2, provides Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature support for two-wire mode and four-wire mode for SHDSL on the Cisco 2600XM series, Cisco 2691, Cisco 3600 series, and Cisco 3700 series modular access routers. The WIC-1SHDSL-V2 incorporates the latest firmware and the latest circuitry.

VIC-4FXS/DID

The VIC-4FXS/DID feature supports the 4-port Foreign Exchange Station/Direct Inward Dialing (FXS/DID) voice interface card (VIC) on the Cisco 1751 and Cisco 1760 routers. The 4-port FXS/DID VIC provides both FXS and DID functionality on a single VIC. The Cisco 1751 router can support three 4-port FXS/DID VICs, up to a maximum of four DID ports. The Cisco 1760 router can support four 4-port FXS/DID VICs, up to a maximum of eight DID ports.

VPN Acceleration Module 2+ (VAM2+)

The VPN Acceleration Module 2+ (VAM2+) is supported with IPSec Stateful Failover for the Cisco 7200 and Cisco 7301 routers.

WIC-4ESW (4-Port Ethernet Switch WIC)

The Cisco 4-port 10/100BASE-T Fast Ethernet Switch WAN Interface Card (WIC-4ESW) for Cisco 1700 series modular access routers is an intelligent managed switch, offering small businesses and enterprise small branch office customers the option to integrate LAN switching and routing into one platform. The advanced capabilities of the WIC, including VLAN support, Spanning Tree Protocol, and traffic prioritization, provide the flexibility for customers to deploy different network configurations.

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/release/notes/rn1700xc.html

New Software Features Supported in Cisco IOS Release 12.4

This section describes new and changed features in Cisco IOS Release 12.4. Some features may be new to Cisco IOS Release 12.4 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 12.4. To determine if a feature is new or changed, refer to the feature history table at the beginning of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided

- AAA Double Authentication Secured by Absolute Timeout
- AAA IPv6 Attributes Support
- AAL1 CES on AIM-ATM
- ACL IP Options Selective Drop
- ACL—Named ACL Support for Noncontiguous Ports on an Access Control Entry
- ACL Performance Enhancement
- ACL Support for Filtering IP Options
- ACL Support for TCP Flags Filtering
- Administrative Secure Device Provisioning Introducer
- Advanced Encryption Standard (AES)
- Analog Centralized Automatic Message Accounting (CAMA) E911 Trunk
- Any Transport over MPLS (AToM) SCR VC Mode for PA-A3-T1/E1-IMA
- APS Support on Cisco AS5850 STM-1 Interfaces
- ARP-Auto Logoff
- Asynchronous Point of Sale-to-IP Conversion
- ATM Mode for Two-Wire or Four-Wire SHDSL
- Attribute Screening for Access Requests
- Authorization for Protocol Translation
- AutoQoS for the Enterprise
- AutoQoS—VoIP
- AutoSecure
- BCP Support

- BGP Configuration Using Peer Templates
- BGP Convergence Optimization
- BGP Cost Community
- BGP Cost Community Support for EIGRP MPLS VPN PE-CE with Backdoor Links
- BGP Dynamic Update Peer-Groups
- BGP MIB Support Enhancements
- BGP Policy Accounting Output Interface Accounting
- BGP Route-Map Continue
- BGP Support for Dual AS Configuration for Network AS Migrations
- BGP Support for Fast Peering Session Deactivation
- BGP Support for IP Prefix Import from Global Table into a VRF Table
- BGP Support for Named Extended Community Lists
- BGP Support for Next-Hop Address Tracking
- BGP Support for Sequenced Entries in Extended Community Lists
- BGP Support for TTL Security Check
- Blinking LEDs to Indicate DSL Line Training
- Call Admission Control for IKE
- Call Application HTTP Client Cookie Support
- Call Failure Recovery (Rotary) on the Cisco Multiservice IP-to-IP Gateway
- Call Routing Enhancements to the H.323 Gatekeeper and GKTMP (GK API)
- Calling Line Identification for Spain and Austria
- CEF Support for Dialer Profiles on Cisco 7500 Routers
- CEF Support for NAT-PT
- Certificate Server Auto Archive
- Certificate to ISAKMP Profile Mapping
- Circuit Emulation over IP (CEMoIP)
- Cisco 1700 Series Voice Features
- Cisco 1700 Series Voice Features for Cisco IOS Release 12.3(2)T
- Cisco 7200 Series and Cisco 7301 Routers—Enhanced MIB Support
- Cisco 7301 Router Support for IPSec Stateful Failover
- Cisco CallManager Express 3.3
- Cisco Communication Media Module Voice Features
- Cisco Conferencing and Transcoding for Voice Gateway Routers
- CISCO-CONFIG-COPY-MIB: FTP and rcp Support
- CISCO-CONFIG-COPY-MIB: Secure Copy Support
- Cisco Easy VPN Remote
- Cisco Easy VPN Remote Enhancements
- Cisco Enhanced Conferencing and Transcoding for Cisco Voice Gateway Routers

- Cisco Extension to the Interfaces MIB (CISCO-IF-EXTENTION-MIB)
- CISCO-FLASH-MIB Enhancements
- Cisco General Packet Radio Service (GPRS) Gateway Support Node (GGSN)
- Cisco IOS 802.1x Supplicant
- Cisco IOS Certificate Server
- Cisco IOS IPv6 Configuration Library
- Cisco IOS IPv6 Configuration Library
- Cisco IOS Login Enhancements
- Cisco IOS MGCP Gateway Support for Cisco CallManager Network Specific Facilities
- Cisco IOS Resilient Configuration
- Cisco IOS Software Feature Removal: Token Ring Inter-Switch Link
- CISCO-IP-LOCAL-MIB-Support
- Cisco Multipath Channel (CMPC)
- Cisco NM-8AM-V2 and NM-16AM-V2 Analog Modem Network Modules with V.92
- Cisco Survivable Remote Site Telephony (SRST), V3.0
- Cisco Transaction Connection (CTRC)
- Cisco Unique Device Identifier
- Cisco VG224 24-Port Analog Phone Gateway
- Cisco VoIP Internal Error Codes
- Cisco IOS Intrusion Prevention System
- Cisco IOS IPv6 Configuration Library
- Class-Based Packet Marking Enhancements
- Class-Based QoS MIB (CBQoSMIB)
- Class-Based QoS MIB (CBQoSMIB) Enhancements
- Class-Based QoS MIB (CBQoSMIB) Enhancements III
- Class-Based Traffic Policing with CLP Tagging
- Clear Certificate Server Enrollment Request Database
- CLNS Support for GRE Tunneling of IPv4 and IPv6 Packets
- CNS Frame Relay Zero Touch
- Combined Packet Protocol (CPP)
- Conferencing and Transcoding for Voice Gateway Routers
- Configurable DHCP Client
- Configurable MAC Address for PPPoE
- Configuration Change Notification and Logging
- Configuration Change Notification and Logging—EAL4+ Certification Enhancements
- Configuring Fast Secure Roaming
- Configuring Remote Site IEEE 802.1X Local Authentication Service
- Configuring SIP Header Passing

- Contextual Configuration Diff Utility
- Control Plane Policing
- CPU Thresholding Notification
- Crypto Access Check on Clear-Text Packets
- Crypto Conditional Debug Support
- Custom Tone Download to Cisco IOS MGCP Gateways from Cisco CallManager
- Default Route on a PPP Virtual Access Interface
- Default Session Application Enhancements
- Demilitarized Zone (DMZ) Port
- DHCP Address Allocation Using Option 82
- DHCP Authorized ARP
- DHCP Enhancements for Edge-Session Management
- DHCP Lease Limit per ATM RBE Unnumbered Interface
- DHCP ODAP Server Support
- DHCP Relay—MPLS VPN Support
- DHCP Release and Renew CLI in EXEC Mode
- DHCP—Static Mapping
- DHCP—Statically Configured Routes Using a DHCP Gateway
- DHCP—Subscriber Identifier Suboption of Option82
- DHCPv6 Prefix Delegation via AAA
- Dial-Out Trunk Group
- Digital Private Network Signaling System (DPNSS) Backhaul
- Direct HTTP Enroll with CA Servers
- Distributed Dial-on-Demand Routing
- Distributed Multilink Frame Relay (FRF.16)
- DNS Proxy
- DNS Spoofing
- Dynamic DNS Support for Cisco IOS
- Dynamic Multipoint VPN (DMVPN)
- Easy Secure Device Deployment AAA Integration
- Easy VPN Client RSA Signature Support
- Easy VPN Server
- EIGRP MPLS VPN PE-CE Site of Origin (SoO)
- EIGRP Prefix Limit Support
- EIGRP SNMP Support
- EIGRP Support for Route Map Filtering
- E-mail Inspection Engine
- Embedded Event Manager 1.0

- Embedded Event Manager 2.1
- Embedded Resource Manager (ERM)
- Embedded Syslog Manager
- Enabling OSPFv2 on an Interface Using the ip ospf area Command
- Encrypted Preshared Key
- End-of-Record Function for DCNs
- Enhanced Conferencing and Transcoding for Voice Gateway Routers
- Enhanced Crashinfo File Collection Method
- Enhanced cRTP for Links with High Delay, Packet Loss, and Reordering
- Enhanced Debug Capabilities for Cisco Voice Gateways
- Enhanced ITU-T G.168 Echo Cancellation
- Enhanced Object Tracking
- Enhanced Object Tracking of Service Assurance Agent (SAA) Operations
- Enhanced Voice and QoS for ADSL and G.SHDSL
- ESMTP Support for Cisco IOS Firewall
- ETSI Call Transfer
- Exclusive Configuration Change Access
- Extended ACL Support for IGMP to Support SSM in IPv4
- Extended Prepaid Tariff Switch with SSG
- FACILITY Debug Enhancement
- FHRP—VRRP Enhancements
- File Download Using HTTP
- Firewall ACL Bypass
- Firewall Authentication Proxy for FTP and Telnet Sessions
- Firewall Intrusion Detection System (IDS) Enhancements
- Firewall N2H2 Support
- Firewall Support for SIP
- Firewall Support of SSL Encrypted HTTP Authentication Proxy Sign-On
- Firewall Websense URL Filtering
- Four-Wire Mode for SHDSL
- Framed-Route in RADIUS Accounting
- Frame Relay—Multilink (MLFR-FRF.16)
- Frame Relay Switched Virtual Circuits (SVC) over ISDN
- Gatekeeper Prefix Selection for Hair-Pinned Calls
- Generic Routing Encapsulation Tunnel IP Source and Destination VRF Membership
- GGSN R3.1
- GLBP MD5 Authentication
- Granular Protocol Inspection

- Health Monitor and Diagnostic Monitor for the Cisco AS5850
- Hookflash and DTMF Relay Transfer
- Hot Standby Router Protocol (HSRP)
- Hot Standby Router Protocol Version 2
- HSRP MD5 Authentication
- HTTP Client API for TCL IVR
- HTTP Inspection Engine
- IEEE 802.1Q Tunneling
- IGMPv3 Host Stack
- Image Verification
- Implementing RIP for IPv6
- Import of RSA Keypair and Certificates in PEM Format
- Inspection of Router-Generated Traffic
- Integrated IS-IS Global Default Metric
- Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters
- Integrated Routing and Bridging (IRB) Support for the Cisco MGX-RPM-XF-512
- Interoperability Enhancements to the Cisco Multiservice IP-IP Gateway
- Intrusion Prevention System (IPS) - Signature Enhancements
- Invalid Security Parameter Index Recovery
- IOS Embedded Event Manager 2.1
- IP Security VPN Monitoring
- IP Side Answer Tone Detection for Echo Canceller Control
- IP SLAs Sub-millisecond Accuracy Improvements
- IP SLA—VoIP Call Setup (Post Dial Delay) Monitoring
- IP SLA—VoIP Gatekeeper Registration Delay Monitoring
- IP Source Tracker
- IP to ATM CoS Enhancements
- IPHC (cRTP/cUDP/cTCP)
- IPSec and Quality of Service
- IPSec Anti-Replay Window: Expanding and Disabling
- IPSec Dead Peer Detection Periodic Message Option
- IPsec NAT Transparency
- IPSec Preferred Peer
- IPSec Virtual Tunnel Interface
- IPv6 BSR Bi-Directional Support
- IPv6 IOS Firewall FTP Application Support
- IPv6 Multicast: Bootstrap Router (BSR)
- IPv6 Support for AS5850 Dial

- ISDN Backup in MPLS Core
- ISDN Calling Name Display
- ISDN Type of Number to RADIUS Server
- IS-IS Caching of Redistributed Routes
- IS-IS Fast-Flooding of LSPs Using the fast flood Command
- IS-IS Incremental SPF
- IS-IS Limit on Number of Redistributed Routes
- IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements
- IS-IS Support for Priority-Driven IP Prefix RIB Installation
- IS-IS Support for Route Tags
- Key Rollover for Certificate Renewal
- L2TP Client-Initiated Tunneling
- L2TP Tunnel Connection Speed Labeling
- L2TPv3: Layer 2 Tunnel Protocol Version 3
- LAN Network Manager (LNM)
- Land Mobile Radio (LMR) over IP
- LFI
- Loadsharing IP Packets Over More Than Six Parallel Paths
- Local AAA Server
- Login Password Retry Lockout
- Lossless Compression R1, ATM Cell Switching, External BITS Clocking Source
- Low Latency Queueing
- MAC Address Based Authorization with SSG
- Malicious Caller Identification Invocation Support for Enterprise Networks
- Managed LAN Switch
- MCID for Cisco IOS Voice Gateways
- Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways in SRST Mode
- Media Inactive Call Detection
- Memory and CPU Measurement
- Memory Threshold Notifications
- Memory Thresholding Infrastructure
- MGCP-Controlled Backhaul of BRI Signaling in Conjunction with Cisco CallManager
- MGCP Fax Rate Control
- MGCP Line Control Signaling Package
- MGCP Support for CallManager (IP-PBX)
- MIB Enhancements for H.323, SIP, and MGCP
- Minimal Disruptive Restart of VIP Cards

- MLPP for Analog and BRI Endpoints on Cisco IOS Voice Gateways
- MLPP for Cisco IOS Voice Gateways
- Mobile IP
- Mobile IP CPS Improvement at FA
- Mobile IP Dynamic Security Association and Key Distribution
- Mobile IP—Foreign Agent Local Routing to Mobile Networks
- Mobile IP—Generic Routing Encapsulation for Cisco Mobile Networks
- Mobile IP Home Agent Redundancy for Dynamic Mobile Networks
- Mobile IP MIB for Reverse Tunnel, Challenge, and VSEs
- Mobile IP—Mobile IPv6 Home Agent
- Mobile IP—Mobile Router DHCP Support for Dynamic CCoA and Foreign Agent Processing
- Mobile IP—Support for RFC 3519 NAT Traversal
- Mobile Networks Deployment MIB
- Mobile Networks Dynamic Collocated Care-of-Address
- Modem Calls over QSIG
- Monitoring and Retraining on Reception of Loss of Margin Messages
- Monitoring Control Characters on Async Lines
- MPLS-aware NetFlow
- MPLS DiffServ-Aware Traffic Engineering (DS-TE)
- MPLS Enhancements to Interfaces MIB
- MPLS Label Distribution Protocol MIB Version 8 Upgrade
- MPLS Label Switch Controller and Enhancements
- MPLS LDP Autoconfiguration
- MPLS LDP Graceful Restart
- MPLS LDP-IGP Synchronization
- MPLS LDP Inbound Label Binding Filtering
- MPLS LDP Session Protection
- MPLS—Multilink PPP Support
- MPLS Quality of Service (QoS)
- MPLS QoS—DiffServ Tunneling Modes
- MPLS Traffic Engineering (TE)
- MPLS Virtual Private Networks
- MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution
- MPLS VPN—Explicit Null Label Support with BGP IPv4 Label Session
- MPLS VPN Half-Duplex VRF (HDVRF) Support
- MPLS VPN—Inter-AS—IPv4 BGP Label Distribution
- MPLS VPN—MIB Notifications
- MPLS VPN—MIB Support

- MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge
- MPLS VPN VRF Selection Using Policy Based Routing
- MSDP Compliance with IETF MSDP Draft 20
- Multicast Fast Switching Performance Improvement
- Multicast VPN
- Multicast VPN MIB
- Multiprotocol Label Switching (MPLS)
- Multi-VRF CE (VRF-lite) Updated Performance
- NAT—dCEF Support
- NAT—H.245 Tunneling Support
- NAT Integration with MPLS VPNs (VRF-NAT)
- NAT–Performance & Scalability Enhancement–Timer Wheel
- NAT–Performance Enhancement–CEF Switching Support
- NAT Routemaps Outside-to-Inside Support
- NAT RTSP Support Using NBAR
- NAT—SIP Support
- NAT Stateful Failover for Application Layer Gateway (ALG) Support
- NAT Stateful Failover for Asymmetric Outside-to-Inside Support
- NAT—Static IP
- NAT Support for H.323 Fragmented Control Messages
- NAT—Support for H.323 v3 and v4 in v2 Compatibility Mode
- NAT—Support of IP Phone to Cisco CallManager
- NAT Virtual Interface (NVI)
- NBAR Multiple Applications per Port Capability
- NetFlow
- NetFlow Egress Support
- NetFlow Layer 2 and Security Monitoring Exports
- NetFlow MIB
- NetFlow Top Talkers
- Network Admission Control
- Network-based Application Recognition (NBAR)
- New Features in Cisco CallManager
- New Voice Features
- NextPort Voice Tuning and Background Noise Statistics with NextPort Dual-Filter G.168 Echo Cancellation
- No Service Password-Recovery
- OER Policy-Rules Configuration and Port-Based Prefix Learning
- OER Support for Cost-Based Optimization and Traceroute Reporting

- Online Certificate Status Protocol (OCSP)
- Optimized Edge Routing (OER)
- Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine
- OSPF Area Transit Capability
- OSPF Incremental SPF
- OSPF Limit on Number of Redistributed Routes
- OSPF Link-State Advertisement (LSA) Throttling
- OSPF Link State Database Overload Protection
- OSPF MIB Support of RFC 1850 and Latest Extensions
- OSPF per-Interface Link-Local Signaling
- OSPF Sham-Link MIB Support
- OSPF Sham-Link Support for MPLS VPN
- OSPF Support for Unlimited Software VRFs per Provider Edge (PE) Router
- Outbound Control Packet Decoding Implemented for VPDN Debug Output Using the L2TP Protocol
- Out-of-Band to In-Band DTMF Relay for Cisco IOS Voice Gateways
- Overlap Signaling Processing on H.323 Terminating Gateways
- PAD Subaddress Formatting Option
- PA-POS-1OC3: 1-port Packet over SONET OC3c/STM1 Port Adapter
- PCR Support for the Cisco Signaling Link Terminal
- Per Interface mroute State Limit
- Per-VRF AAA
- Per VRF for TACACS+ Servers
- Periodic MIB Data Collection and Transfer Mechanism
- Persistent Self-Signed Certificates
- Persistent TDM Switched Circuits
- PKI AAA Authorization Using the Entire Subject Name
- PKI: Query Multiple Servers During Certificate Revocation Check
- PKI Status
- Policy Based Routing: Recursive Next Hop
- Port Translation for Windows Clients and Cisco IOS LNS Support
- PPP/MLP MRRU Negotiation Configuration
- PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support
- PPPoE Session Recovery After Reload
- Protected Private Key Storage
- Protocol Translation Aggregation
- QoS Bandwidth Estimation
- QoS: Classification, Policing, and Marking on LAC

- QSIG Supplementary Features for Cisco IOS Voice Gateways
- Quality of Service for Virtual Private Networks
- Query Mode Definition Per Trustpoint
- Quick Autoenroll
- RADIUS Attribute 104
- RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level
- RADIUS NAS-IP-Address Configurability
- Random Sampled NetFlow
- Rate Based Satellite Control Protocol
- Rate Limiting NAT Translation
- RAW IP Traffic Export
- Real-time Resolution for IPSec Tunnel Peer
- Re-enroll Using Existing Certificate
- Regex Engine Performance Enhancement
- Reliable Static Routing Backup Using Object Tracking
- Reverse Route Injection
- Reverse SSH Enhancements
- RFC 2867—RADIUS Tunnel Accounting
- Role-Based CLI Access
- Route Processor Redundancy Plus (RPR+)
- RSVP Refresh Reduction and Reliable Messaging
- RTP Header Compression over Satellite Links
- SAA Support for Frame Relay, VoIP, and MPLS VPN Monitoring
- SafeNet IPSec VPN Client Support
- SEAL Encryption
- Second-Generation 1- and 2-Port T1/E1 Multiflex Trunk Voice/WAN Interface Cards
- Secure Device Provisioning Certificate-Based Authorization
- Secure Shell Version 2 Support
- Secure SNMP Views
- Selective Enabling of Applications Using an HTTP or Secure HTTP Server
- Service Assurance Agent (SAA)—MPLS VPN Path Jitter
- Service Assurance Agent (SAA) Multiple Operation Scheduling
- Service Assurance Agency (SAA) VoIP UDP Operation
- Service Selection Gateway (SSG)
- Service Selection Gateway (SSG) Features in Release 12.3(4)T
- Session Initiation Protocol (SIP)
- SHDSL—Auto Detection of 2 Wire Versus 4 Wire Line Mode
- Show Command Section Filter

- Show Version Enhancements
- Signal ISDN B-Channel ID to Enable Application Control of Voice Gateway Trunks
- SIP Audible Message-Waiting Indicator for FXS Phones
- SIP: Cisco IOS Gateway HTTP Digest Authentication and Registration
- SIP: Cisco IOS Gateway Reason Header and Buffered Calling Name Completion
- SIP Debug Output Filtering Support
- SIP Gateway Support Enhancements to the bind Command
- SIP Header Support and Subscribe and Notify for External Triggers
- SIP: RFC 3261 Enhancements
- Skip FA/HA-CHAP at Mobile IP Lifetime Renewals
- SNA Switching Services Enterprise Extender for IP Version 6
- SNMP linkDown Trap Limiting
- SNMP over IPv6 Support
- SNMP Support for Named Access Lists
- SNMP Support over VPNs—Context Based Access Control
- SNMP v1/v2c PDU Conversions for Proxy Forwarder (RFC 2576)
- Source Specific Multicast (SSM) Mapping
- SSG 3-Key Authentication
- SSG AAA Transaction Enhancements
- SSG Aware On-Demand IP Address Renewal
- SSG Complete ID
- SSG Default DNS Redirection
- SSG Default Quota for Prepaid Billing Server Failure
- SSG Enhancements to SSG-SESM Interaction and Service Logon
- SSG Interface Redundancy
- SSG MIB Extensions
- SSG Open Garden Configuration Enhancements
- SSG Permanent TCP Redirection
- SSG Support for Dynamic Load Balancing
- SSG Support for Overlapping Subscriber IP Addresses
- SSG Support for RADIUS Attributes 27 and 29
- SSG Support for Subnet Based Authentication
- SSG TCP Redirect Access Control Lists
- SSG Transparent Autologon
- SSM Channel (S,G) Based Filtering for Multicast Boundaries
- Stateful Failover for IPSec
- Subordinate Certificate Server
- Subscriber Service Support

- Support for AAA Attributes MN-HA-SPI and MN-HA Shared Key
- Survivable Remote Site Telephony (SRST) 3.2
- Survivable Remote Site Telephony (SRST) 3.3
- System Logging—EAL4 Certification Enhancements
- T1/E1 Mode for SHDSL
- T.37 Fax Status Notification Enhancement in an MTA Environment
- T.38 Fax Relay on the Cisco Catalyst 6000 and Cisco 7600 Communication Media Module
- T.38 Fax Statistics
- TCP Congestion Avoidance
- TCP Explicit Congestion Notification
- Token Ring Inter-Switch Link (TRISL)
- Token Ring LAN Emulation (TR-LANE)
- Transient Memory Management
- Transparent Cisco IOS Firewall
- Troubleshooting Enhancements for Multilink PPP over ATM Link Fragmentation and Interleaving
- Tunnel Authentication via RADIUS on Tunnel Terminator
- Turbo-Classification for QoS
- Two-Wire Mode over SHDSL
- Upgrade Secondary ROMmon CLI
- Upstream PPPoX Connection Speed Transfer at LAC
- USB Storage
- Using Certificate ACLs to Ignore Revocation Check and Expired Certificates
- V.120 Support Network Access Server (NAS)
- Videoconferencing on the Cisco Multiservice IP-to-IP Gateway
- Virtual Auxiliary Port Feature and Configuration of DSL Settings
- Virtual Fragmentation Reassembly
- VLANs over IP Unnumbered Interfaces
- Voice Application Enhancements, Phase 4a
- Voice Application Monitoring and Troubleshooting Enhancements
- Voice Call Debug Filtering on Cisco Voice Gateways
- Voice Performance Statistics on Cisco Gateways
- VoiceXML Store and Forward
- VoIP Alternate Path Fallback SNMP Trap
- VPDN MIB Enhancements for per-VRF Session Counting
- VPN Access Control Using 802.1X Authentication
- VRF and MQC Hierarchical Shaping in PXE
- VRF Aware Cisco IOS Firewall
- VRF Aware Dialer Watch

- VRF-Aware IPSec
- VRF Aware MPLS Static Labels
- VRF Aware Multicast Error Messages
- VRRP MIB—RFC 2787
- VRRP Object Tracking
- VRRP—Virtual Router Redundancy Protocol
- VTMS
- Warm Reload
- Warm Upgrade
- WCCP Enhancements
- WCCP Version 2
- WebVPN
- X.25 Call Confirm Packet Address Control
- X.25 Data Display Trace
- X.25 Station Type for ISDN D-Channel Interface
- X.25 Version Configuration

AAA Double Authentication Secured by Absolute Timeout

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_dasat.html

AAA IPv6 Attributes Support

For detailed information about this feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_aaaip.htm

AAL1 CES on AIM-ATM

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_aal1.html

ACL IP Options Selective Drop

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/sel_drop.html

ACL—Named ACL Support for Noncontiguous Ports on an Access Control Entry

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtaclace.html

ACL Performance Enhancement

An IP access control list (ACL) is a Cisco IOS software feature that allows an administrator to configure a network to permit and deny packets based on a set of ACL entries, thus improving security and control within a network. These lists contain entries that are searched sequentially for matches among certain fields in Layer 3 and Layer 4 packet headers.

Before Cisco IOS Release 12.3(2)T, ACL entries were sequentially configured and stored. This implementation caused the first match in a search to be the first ACL entry in a given list, not the entry that provided the best match. Although this implementation was straightforward and logical, it did not scale well with the number of ACL entries in an ACL.

Cisco IOS Release 12.3(2)T implements ACLs using hierarchical radix tries (sometimes called multilevel tries, backtracking tries, or tries-of-tries) to improve matching performance. Individual tries are made for the source prefix and the destination prefix, with additional ACL entry information such as TCP ports, TCP flags, and time ranges being held at the nodes. Cisco IOS software performs a best match lookup for the given set of prefixes. This new implementation is an internal improvement that supports all existing functionality, and the sequential searching properties that cause ACLs to check the entries from start to end and stop searching for a match as soon as one is found are still valid.

The benefits of implementing of ACLs using hierarchical radix tries are as follows:

- Memory usage is made more efficient.
- Less system resources are required to maintain the tries information.
- Performance of ACL matching is improved for larger access lists.

ACL Support for Filtering IP Options

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtipofil.html

ACL Support for TCP Flags Filtering

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/sel_drop.html

Administrative Secure Device Provisioning Introducer

This feature was introduced in Cisco IOS Release 12.3(8)T. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtadintr.html

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) feature adds support for the new encryption standard AES, with cipher block chaining (CBC) mode, to IP Security (IPSec). AES is a privacy transform for IPSec and Internet Key Exchange (IKE) that has been developed to replace the Data Encryption Standard (DES). AES is designed to be more secure than DES: AES offers a larger key size, while ensuring that the only known approach to decrypt a message is for an intruder to try every possible key. AES has a variable key length—the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.

For more details on this feature, see the following URL:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_aes.html

Analog Centralized Automatic Message Accounting (CAMA) E911 Trunk

The Cisco 1751 and Cisco 1760 routers now support analog centralized automatic message accounting (CAMA) trunks on the two- and four-port Foreign Exchange Office (FXO) cards. The VIC2-2FXO and VIC2-4FXO cards are now user configurable for CAMA mode operation on a port-by-port basis. For example, on the VIC2-2FXO card, port 0 can be configured for CAMA, and port 1 can be configured for FXO-M1 operation.

The CAMA feature offers the following benefits:

- Direct connection to the E911 network
- Compliance with current legislation requiring enterprises to connect directly to the E911 network
- Trunk capabilities to emergency services that are not currently supported on any Cisco product
- Configuration on H.323 Voice over IP (VoIP)

Any Transport over MPLS (AToM) SCR VC Mode for PA-A3-T1/E1-IMA

You can configure AToM ATM Single Cell Relay (VC mode) on the following port adapters: PA-A3-8T1IMA and PA-A3-8E1IMA.

APS Support on Cisco AS5850 STM-1 Interfaces

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gt_aps58.html

ARP-Auto Logoff

This feature was introduced in Cisco IOS Release 12.3(8)XX. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xx/gtarpal.html

Asynchronous Point of Sale-to-IP Conversion

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_apos.html

ATM Mode for Two-Wire or Four-Wire SHDSL

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt4wire.html

Attribute Screening for Access Requests

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3b/feature/guide/gt_asfar.html

Authorization for Protocol Translation

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gttpadta.html

AutoQoS for the Enterprise

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/ft_aqose.html

AutoQoS—VoIP

The AutoQoS—VoIP feature allows you to automate the delivery of quality of service (QoS) on your network and provides a means for simplifying the implementation and provisioning of QoS for Voice over IP (VoIP) traffic.

For additional information about this feature, see the following documents:

- *AutoQoS—VoIP*
- *Quality of Service for Voice*

AutoSecure

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/feature/guide/ftatosec.html

BCP Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_bcp.html

BGP Configuration Using Peer Templates

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_bgpct.html

BGP Convergence Optimization

BGP convergence optimization introduces a new algorithm for update generation that reduces the amount of time that is required for Border Gateway Protocol (BGP) convergence. Neighbor update messages are optimized before they are forwarded to neighbors. Updates are optimized and forwarded based on peer groups and per-individual neighbors. This enhancement improves BGP convergence, router boot time, and transient memory usage. This enhancement is not user configurable.

BGP Cost Community

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_bgpcc.html

BGP Cost Community Support for EIGRP MPLS VPN PE-CE with Backdoor Links

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgpcce.html

BGP Dynamic Update Peer-Groups

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtbgpdpg.html

BGP MIB Support Enhancements

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_bmibe.html

BGP Policy Accounting Output Interface Accounting

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_bgpdpg.html

BGP Route-Map Continue

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_brmcs.html

BGP Support for Dual AS Configuration for Network AS Migrations

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtbgpdas.html

BGP Support for Fast Peering Session Deactivation

This feature was introduced in Cisco IOS Release 12.0(29)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/cs_bsfda.html

BGP Support for IP Prefix Import from Global Table into a VRF Table

This feature was introduced in Cisco IOS Release 12.0(29)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_bgivt.html

BGP Support for Named Extended Community Lists

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtnextcl.html

BGP Support for Next-Hop Address Tracking

This feature was introduced in Cisco IOS Release 12.0(29)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_bnht.html

BGP Support for Sequenced Entries in Extended Community Lists

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtextseq.html

BGP Support for TTL Security Check

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_btsh.html

Blinking LEDs to Indicate DSL Line Training

The ADSL LED Blinking feature provides information on the status of a DSL line. ADSL Tx/Rx is used for this purpose. There are three distinct blinking patterns that indicate the various states of a DSL line when it is training.

1. When the firmware is being downloaded within the router, the LED remains on for 700 ms and goes off for 300 ms.
2. When the modem state is MODEM_ACT_ACK (0x8), the router is waiting to hear from the central office (CO) and is not yet seeing an incoming signal. During this time, the LED will be on and off for 50 ms each.
3. When the modem state is MODEM_TRAINING (0x10), the LED will always be on. This means that the DSL line is training.

Shortly after the DSL line has started training, the modem state changes to SHOWTIME, and then the router is successfully trained with the DSLAM.

Note The CD LED on the front panel will be off during the DSL line training process. This is different from the normal operation when packets are being transmitted or received.

Call Admission Control for IKE

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtcallik.html

Call Application HTTP Client Cookie Support

For detailed information about this feature, see the "Configuring Basic Functionality for TCL IVR and VoiceXML Applications" chapter in the *Cisco IOS TCL IVR and VoiceXML Application Guide*.

Call Failure Recovery (Rotary) on the Cisco Multiservice IP-to-IP Gateway

The Call Failure Recovery feature eliminates the need for identical codec capabilities for all dial peers in the rotary group and allows the IP-to-IP gateway to restart the codec negotiation process with the originating endpoint on the basis of the codec capabilities of the next dial peer in the rotary group.

For detailed information about this feature, see the *Cisco Multiservice IP-to-IP Gateway Application Guide* at the following URL:

http://www.cisco.com/en/US/partner/docs/ios/voice/cube/configuration/guide/vb-gw-roadmap.html

Call Routing Enhancements to the H.323 Gatekeeper and GKTMP (GK API)

These features improve routing flexibility in customer networks in which an external route server is used to select potential endpoints for call completion.

- Nonblocking GKTMP (GK API): Timing changes are associated with recovery processing when socket errors occur.
- Separate DNIS for Alternate Endpoints: It is now possible to associate a unique DNIS with each alternate endpoint.
- Support for "z" Tag in RESPONSE xRQ: This support enhances the responses that a route server can provide to the H.323 gatekeeper to allow greater flexibility for combinations of gateway endpoints and gatekeepers.

Calling Line Identification for Spain and Austria

Caller ID (sometimes called *CLID* or *ICLID* for incoming call line identification) is an analog service offered by a central office (CO), that supplies calling party information to subscribers. Typically, the calling party number, and sometimes the name, appears on a station (also called *extension*) device such as a PC telephony software application screen or the display on a telephone. Type 1 Caller ID show the calling party information while the call is ringing, and Type 2 Caller ID shows the calling number display while the recipient is on another call. Type 1 Caller ID is supported in this release.

The Caller ID feature supports the sending of calling party information from Foreign Exchange Station (FXS) loop-start and ground-start ports into a Caller-ID-equipped telephone device. The FXS port emulates the extension interface of a PBX or the subscriber interface for a CO switch.

Spain and Austria both use the ETSI-FSK method for sending the caller number to the analog phone.

CEF Support for Dialer Profiles on Cisco 7500 Routers

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtcefrsp.html

CEF Support for NAT-PT

This feature adds support for Cisco Express Forwarding (CEF) switching on Network Address Translation-Protocol Translation (NAT-PT) interfaces. Use the **ip cef** and **ipv6 cef** commands to configure the feature.

Certificate Server Auto Archive

For detailed information about this feature, see the *Cisco IOS Certificate Server* document:

http://www.cisco.com/en/US/partner/docs/ios/12_3t/12_3t4/feature/guide/gt_ioscs.html

Certificate to ISAKMP Profile Mapping

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_isakp.html

Circuit Emulation over IP (CEMoIP)

The Circuit Emulation over IP (CEMoIP) feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2691 Multiservice routers
- Cisco 3725 Modular Access routers
- Cisco 3745 Modular Access routers
- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

Cisco 1700 Series Voice Features

The following is a list of Cisco IOS voice features that have been introduced in various Cisco IOS releases and that are now supported on the Cisco 1700 series platforms as part of Cisco IOS Release 12.3(11)T.

The following Cisco IOS VoIP features are supported on the Cisco 1700 series platforms for Cisco IOS Release 12.3(11)T:

- H.323v4: Enhanced Call Usage Reporting
- H.323v4 Gateway Zone Prefix Registration Enhancements
- SIP Call Transfer and Call Forwarding
- VoIP and Cisco Express Forwarding (CEF) Interoperability
- VoIP and Policy Based Routing (PBR) Interoperability

H.323v4: Enhanced Call Usage Reporting

This feature provides H.323v4 enhancements that provide standards-based call usage reporting to the gatekeeper from an H.323 gateway. This information is used by the gatekeeper to generate call detail records (CDRs).

For more information, see the following documents:

- The "Cisco IOS Call Control Technology" section in the *Cisco IOS Voice Configuration Library*:

  http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm
- The *VoIP Gateway Trunk and Carrier Based Routing Enhancements* document:

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t11/feature/guide/ftgwrepg.html
- The *VoIP Gatekeeper Trunk and Carrier Based Routing Enhancements* document:

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t11/feature/guide/ftgkrenb.html

H.323v4 Gateway Zone Prefix Registration Enhancements

This feature provides support for two capabilities included in H.323, version 4: additive registration and dynamic zone prefix registration. Additive registration allows a gateway to add to or modify a list of aliases contained in a previous registration without first unregistering from the gatekeeper. Dynamic zone prefix registration allows a gateway to register actual PSTN destinations served by the gateway with its gatekeeper.

For more information, see the following documents:

- The "Cisco IOS Call Control Technology" section in the *Cisco IOS Voice Configuration Library*:

  http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm
- The *H.323v4 Gateway Zone Prefix Registration Enhancements* document:

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftgwzpre.html

SIP Call Transfer and Call Forwarding

This feature introduces the ability of Session Initiation Protocol (SIP) gateways to initiate blind or attended call transfers. Release Link Trunking (RLT) functionality is also added. With RLT, SIP blind call transfers can now be triggered by channel-associated signaling (CAS) trunk signaling. This feature also implements SIP support of call forwarding requests from a Cisco IOS gateway.

For more information, see the *Cisco IOS SIP Configuration Guide*:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/12_4t/sip_12_4t_book.html

VoIP and Cisco Express Forwarding (CEF) Interoperability

This functionality enables Cisco Express Forwarding of VoIP signaling and payload packets that originate from voice interfaces and interactive voice response (IVR) applications.

This feature modifies the Voice over IP (VoIP) and IVR programming so that they can interoperate with features that are supported only in the CEF path (not in the fast-switching path that VoX uses). Voice and IVR work only in the fast path on the routers where they are originated and terminated (voice and IVR on "transit" routers are just data packets and of course can be CEF-switched).

This feature enables policy-based routing of VoIP traffic that originates or terminates on the specified voice gateways and introduces voice packet differentiated services code point (DSCP) marking for Media Gateway Control Protocol (MGCP) voice gateways.

For more information, see the *VoIP Interoperability with Cisco Express Forwarding and Policy-Based Routing* document:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vclcef.html

VoIP and Policy Based Routing (PBR) Interoperability

PBR gives you a flexible means of routing packets by allowing you to configure a defined policy for traffic flows, lessening reliance on routes derived from routing protocols. To this end, PBR gives you more control over routing by extending and complementing the existing mechanisms provided by routing protocols. PBR allows you to set the IP precedence. It also allows you to specify a path for certain traffic, such as priority traffic over a high-cost link.

PBR allows you to perform the following tasks:

- Classify traffic according to extended access list criteria. Access lists, then, establish the match criteria.
- Set IP precedence bits, giving the network the ability to enable differentiated classes of service.
- Route packets to specific traffic-engineered paths; you might need to route them to allow a specific QoS through the network.

For more information, see the *VoIP Interoperability with Cisco Express Forwarding and Policy-Based Routing* document:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vclcef.html

Cisco 1700 Series Voice Features for Cisco IOS Release 12.3(2)T

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/1700voip.html

Cisco 7200 Series and Cisco 7301 Routers—Enhanced MIB Support

This feature greatly expands and updates the support for SNMP MIBs for Cisco 7200 series routers and Cisco 7301 routers. Improved inventory, asset, and fault management capabilities are provided by this feature, with a focus on consistent manageability of Cisco network elements.

The 7200 MIB Improvement feature greatly expands and updates the support for SNMP MIBs for Cisco 7200 series routers. This feature provides:

- Cisco 7200 series additional port adapter support.
- Support for DS1 and DS3 MIBs is implemented as defined by RFC 2495 and RFC 2496, respectively.
- A standards-based technology (SNMP) for monitoring faults and performance on the router.
- Support for all SNMP versions (SNMPv1, SNMPv2c, and SNMPv3).
- Notification of faults, alarms, and conditions that might affect services.

For detailed information about MIB support on the Cisco 7200 series, see the *Cisco 7200 Series Router MIB Specifications Guide*, available at:

http://www.cisco.com/en/US/partner/products/hw/routers/ps341/prod_technical_reference_list.html

The 7301 MIB Support feature greatly expands and updates the support for Cisco 7301 routers because this feature:

- Provides core enhancements to network management capabilities.
- Supports the Cisco 7301 port adapter.
- Manages and monitors Cisco 7301 resources through an SNMP-based network management system (NMS).
- Reduces the amount of time and system resources required to perform functions such as inventory management and bulk data transfers.

For detailed information about MIB support on Cisco 7301 routers, see the *Cisco 7301 Router MIB Specifications Guide*, available at:

http://www.cisco.com/en/US/partner/products/hw/routers/ps352/prod_technical_reference_list.html

Cisco 7301 Router Support for IPSec Stateful Failover

Cisco IOS Release 12.3(11)T2 introduces support for IPSec stateful failover on the Cisco 7301 router. For detailed information on IPSec stateful failover beginning in Cisco IOS Release 12.3(11)T, see the following document:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00802d03f2.html

Cisco CallManager Express 3.3

Cisco CME Basic Automatic Call Distribution and Auto-Attendant Service (Cisco CME B-ACD) has been updated to allow multiple auto-attendant services and a drop-through mode that sends callers directly to a hunt group without encountering an interactive menu. Improvements have also been made to hunt groups and overlay ephone-dns. For detailed information about these features, see the Cisco CallManager Express 3.3 documentation at http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/requirements/guide/cme33spc.html

Cisco Communication Media Module Voice Features

This feature brings additional support for the Cisco Catalyst 6500 series and Cisco 7600 series Communication Media Module with SNMP, MLPP, MCID, HW-MTP with RFC 2833, enhanced QSIG, and native T.l38 fax relay.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xy/archive/gtcmm.html

Cisco Conferencing and Transcoding for Voice Gateway Routers

The Cisco Conferencing and Transcoding for Voice Gateway Routers feature enables voice conferencing among conferees at small, remote branch offices or distributed sites using local resources, without calls having to traverse the company WAN to the central site that supports such services.

The feature also provides transcoding at the remote site. Different IP telephony devices support different codecs, and, for communications to be enabled between them, transcoding is required. The feature provides transcoding at the remote site, without having to access transcoding services at the central site.

To provide these services, the feature takes advantage of unused DSP resources on a network module in an already existing small or midsize Cisco router at the remote site. The collection of DSP resources so made available is called a DSP farm. The DSP farm is managed at a central office or branch office by Cisco CallManager, the software-based call-processing component of the Cisco IP telephony solution.

The Cisco Conferencing and Transcoding for Voice Gateway Routers feature was originally supported in Cisco IOS Release 12.2(13)T. This feature is now supported on the Cisco Catalyst 4000 Access Gateway Module (AGM). See the following document for additional information:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_dsp.html

CISCO-CONFIG-COPY-MIB: FTP and rcp Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtrcpmib.html

CISCO-CONFIG-COPY-MIB: Secure Copy Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_cpmib.html

Cisco Easy VPN Remote

For detailed information about this feature, see the following document:

https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftezvpnr.html

Cisco Easy VPN Remote Enhancements

For detailed information about this feature, see the following document:

https://www.cisco.com/en/US/docs/ios/12_3/featlist/sec_vcg.html

Cisco Enhanced Conferencing and Transcoding for Cisco Voice Gateway Routers

For detailed information about this feature, see the "Configuring Conferencing and Transcoding for Voice Gateway Routers" chapter in the *Cisco CallManager and Cisco IOS Interoperability Guide*:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/interop/interovr.html

Cisco Extension to the Interfaces MIB (CISCO-IF-EXTENTION-MIB)

The CISCO-IF-EXTENTION-MIB implements Cisco specific extensions to the Interface MIB (RFC 2233). These extensions are, specifically, two tables that provide information about interface packet statistics and interface properties.

CISCO-FLASH-MIB Enhancements

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_fcmib.html

Cisco General Packet Radio Service (GPRS) Gateway Support Node (GGSN)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/GGSN40/ggsn40.html

Cisco IOS 802.1x Supplicant

For detailed information about this feature, see the *VPN Access Control Using 802.1X Authentication* document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xa/gt_802_1.html

Cisco IOS Certificate Server

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ioscs.html

Cisco IOS Intrusion Prevention System

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_fwids.html

Cisco IOS IPv6 Configuration Library

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html

Cisco IOS Login Enhancements

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_login.html

Cisco IOS MGCP Gateway Support for Cisco CallManager Network Specific Facilities

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_nsf.html

Cisco IOS Resilient Configuration

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtrescfg.html

Cisco IOS Software Feature Removal: Token Ring Inter-Switch Link

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_jncrg.html

CISCO-IP-LOCAL-MIB-Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_ipmib.html

Cisco Multipath Channel (CMPC)

As of Cisco IOS Release 12.3(4)T, the Cisco Multipath Channel (CMPC) feature has been removed from Cisco IOS software.

Cisco NM-8AM-V2 and NM-16AM-V2 Analog Modem Network Modules with V.92

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtnmam.html

Cisco Survivable Remote Site Telephony (SRST), V3.0

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_configuration_guide_chapter09186a0080557e96.html

Cisco Transaction Connection (CTRC)

As of Cisco IOS Release 12.3(4)T, the Cisco Transaction Connection feature has been removed from Cisco IOS software.

Cisco Unique Device Identifier

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtpepudi.html

Cisco VG224 24-Port Analog Phone Gateway

The Cisco VG224 is a 24-port analog phone gateway based on Cisco IOS software. The Cisco VG224 enables a hybrid of VoIP technology (AVVID based architectures with Cisco CallManager as call control) with TDM analog endpoints (analog phones, fax machines, analog modems). The Cisco VG224 is supported on Cisco CallManager Release 3.2 or later.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/ps9810/index.html

Cisco VoIP Internal Error Codes

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/monitor/configuration/guide/vt_voip_err_cds.html

Class-Based Packet Marking Enhancements

With Release Cisco IOS Release 12.3, the Class-Based Packet Marking feature (first introduced in Cisco IOS Release 12.1(2)T) has been enhanced to support packet marking at any level of a hierarchical policy map. With this enhancement, customers can now use the **set** command to configure packet marking actions in the child classes as well as in the parent classes of a hierarchical policy map.

For more information about class-based packet marking, see the "Classification" part of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

For more information about the **set** command, see the *Cisco IOS Quality of Service Solutions Command Reference*, Cisco IOS Release 12.3T.

Class-Based QoS MIB (CBQoSMIB)

The Class-Based Quality of Service Management Information Base (CBQoS MIB) provides access to quality of service (QoS) configuration information and statistics. The CBQoS MIB allows service providers to monitor their QoS offerings. This MIB gives router QoS configuration such as ClassMap, PolicyMap, Match Statements, and Feature Actions configuration parameters. The MIB also contains counter objects that give statistics such as the number of packets traversed conforming to a policing feature. The MIB uses several indexes to identify QoS features and to distinguish among instances of those features. The MIB provides information about marking and policing done using IP precedence and differentiated services code point (DSCP).

Class-Based QoS MIB (CBQoSMIB) Enhancements

This feature enhances the Class-Based Quality of Service (QoS) MIB (CBQoSMIB) in Cisco IOS software. For information about the CBQoSMIB and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

Class-Based QoS MIB (CBQoSMIB) Enhancements III

Several MIB objects and tables have been added to the CBQoSMIB to reflect the enhanced functionality of the modular QoS CLI (MQC). These MIB objects and tables provide enhanced traffic policing, shaping, and marking functionality.

The following MIB objects and tables were added to the CBQoSMIB:

- Two time-based MIB objects, burst ms and excess burst ms, used when you are configuring traffic policing.

  These parameters were added to allow you to specify the appropriate burst values to be used for policing traffic. However, these two parameters can be used when you are configuring traffic policing on the basis of a percentage of bandwidth *only*.

  For more information about configuring traffic policing on the basis of a percentage of bandwidth, see the Percentage-Based Policing and Shaping feature at the following URL:

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftpctpol.html

- Two time-based MIB objects, sustained burst size in ms and excess burst size in ms, used when you are configuring traffic shaping.

  These parameters were added to allow you to specify the appropriate burst values to be used for shaping traffic. However, these parameters can be used when you are configuring traffic shaping (either average-rate traffic shaping or peak-rate traffic shaping) on the basis of a percentage of bandwidth *only*.

  Note The sustained burst size in ms and excess burst size in ms objects are not currently supported on the Cisco 7500 series router. Therefore, on the Cisco 7500 series router, the counters for these two MIB objects will display zeros.

  For more information about configuring traffic shaping on the basis of a percentage of bandwidth, see the Percentage-Based Policing and Shaping feature at the following URL:

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftpctpol.html

- One table used to count statistical data associated with the various **set** commands available in Cisco IOS software.

  For more information about the Cisco IOS **set** commands, see the Cisco command reference publications for the Cisco IOS release that you are using.

- Three tables used to support the Enhanced Packet Marking feature available with Cisco IOS Release 12.2(13)T.

  For more information about the Enhanced Packet Marking feature, see the following URL:

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftenpkmk.html

For more information about the CBQoSMIB, the MIB objects and tables listed above, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

Class-Based Traffic Policing with CLP Tagging

When configured on the router, the Class-Based Traffic Policing with CLP Tagging feature polices the flow of cells in the forward (into the network) direction of a virtual connection. The traffic policing mechanism determines whether received cells comply with the negotiated traffic management values and tags the cell with a CLP bit value of 1. The purpose of this feature is to mark traffic that does not meet the traffic management values so that packets that exceed the set values can be dropped by the network if the network is congested.

Clear Certificate Server Enrollment Request Database

For detailed information about this feature, see the *Cisco IOS Certificate Server* document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ioscs.html

CLNS Support for GRE Tunneling of IPv4 and IPv6 Packets

GRE tunneling of IPv4 and IPv6 packets through CLNS networks enables Cisco tunnels to interoperate with networking equipment from other vendors. This feature provides compliance with RFC 3147.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclnsv6.html

CNS Frame Relay Zero Touch

For detailed information about this feature, see the following document:

https://www.cisco.com/en/US/docs/ios/12_3/feature/guide/g_zerot.html

Combined Packet Protocol (CPP)

As of Cisco IOS Release 12.3(4)T, the Combined Packet Protocol (CPP) feature has been removed from Cisco IOS software.

Conferencing and Transcoding for Voice Gateway Routers

This feature provides conferencing and transcoding capability in Cisco IOS gateways using packet voice data modules (PVDMs). This feature is delivered in Cisco IOS software and operates in conjunction with Cisco CallManager to provide enhanced multiservice support for Cisco routers in a Cisco CallManager network.

For more information about this featurese, see the following documentation:

- *Conferencing and Transcoding for Voice Gateway Routers*
- *Cisco CallManager and Cisco IOS Interoperability Guide*

Configurable DHCP Client

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtdhcpcf.html

Configurable MAC Address for PPPoE

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gt_cmppp.html

Configuration Change Notification and Logging

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtconlog.html

Configuration Change Notification and Logging—EAL4+ Certification Enhancements

Note Official EAL4+ certification is not claimed by Cisco. This feature is part of current and planned enhancements that may qualify Cisco IOS software for future certification.

This feature enhances the configuration change logging process in Cisco IOS software. The system logging process can now provide a log of configuration changes, and commands are provided to configure, view, and clear configuration logs. This feature is disabled by default.

For detailed information about this feature, see the *Configuration Change Notification and Logging* document at:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtconlog.html

Configuring Fast Secure Roaming

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/fastroam.html

Configuring Remote Site IEEE 802.1X Local Authentication Service

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/locauth.html

Configuring SIP Header Passing

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/sip/configuration/guide/sipftgde.html

Contextual Configuration Diff Utility

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_diff.html

Control Plane Policing

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

CPU Thresholding Notification

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cpu_thresh_notif.html

Crypto Access Check on Clear-Text Packets

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_crpks.html

Crypto Conditional Debug Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_dbcry.html

Custom Tone Download to Cisco IOS MGCP Gateways from Cisco CallManager

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_tones.html

Default Route on a PPP Virtual Access Interface

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtdfltrt.html

Default Session Application Enhancements

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtsesapp.html

Demilitarized Zone (DMZ) Port

This feature was introduced in Cisco IOS Release 12.3(7)XR1. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xr/dmz_port.html

DHCP Address Allocation Using Option 82

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gdhcpopt.html

DHCP Authorized ARP

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtautarp.html

DHCP Enhancements for Edge-Session Management

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_iedge.html

DHCP Lease Limit per ATM RBE Unnumbered Interface

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtdhcpls.html

DHCP ODAP Server Support

The DHCP ODAP Server Support feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

DHCP Relay—MPLS VPN Support

The DHCP Relay— MPLS VPN Support feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

DHCP Release and Renew CLI in EXEC Mode

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtdhcprr.html

DHCP—Static Mapping

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtdhcpsm.html

DHCP—Statically Configured Routes Using a DHCP Gateway

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtddgtwy.html

DHCP—Subscriber Identifier Suboption of Option82

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_opt82.html

DHCPv6 Prefix Delegation via AAA

For detailed information about this feature, see the "Implementing ADSL and Deploying Dial Access for IPv6" module in the *Cisco IOS IPv6 Configuration Library* located at:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-adsl_dial.html

Dial-Out Trunk Group

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtdltrgp.html

Digital Private Network Signaling System (DPNSS) Backhaul

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/ftdpnss.html

Direct HTTP Enroll with CA Servers

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gthttpca.html

Distributed Dial-on-Demand Routing

In previous Cisco IOS software releases, distributed Cisco Express Forwarding (dCEF) is not supported for dialer interfaces on the Cisco 7500 series router. The Distributed Dial-on-Demand Routing (DDR) feature introduces the ability for the Cisco 7500 series router to perform dCEF switching on dialer interfaces. dCEF switching increases the performance of the router by moving processing from the Route Processor (RP) to the line card (LC).

The Distributed DDR feature can be used with all current dialer configurations—dialer profile interfaces, legacy dialer interfaces, and Multilink PPP on dialer interfaces. All pool members of the dialer interface must share the same Versatile Interface Processor (VIP) and the same type of port adaptor (PA). Quality of service (QoS) is not currently supported for the Distributed DDR feature. A VIP2-50 or higher is recommended for running the Distributed DDR feature.

No configuration commands are required to enable the Distributed DDR feature; however dCEF must be enabled. If dCEF is not enabled, processing will occur on the RP as it would in previous releases of Cisco IOS software that lack the Distributed DDR feature. The Distributed DDR feature can be disabled by globally disabling dCEF or by configuring the **no ip route-cache distributed** command on the dialer interface or D-channel interface.

Distributed Multilink Frame Relay (FRF.16)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/dmfr.html

DNS Proxy

In Virtual Private Network (VPN) or PPP over Ethernet (PPPoE) scenarios, the router on the LAN may act as a local Dynamic Host Configuration Protocol (DHCP) server and may receive requests for Domain Name System (DNS) server IP addresses from devices on the LAN. The DNS Proxy feature allows the router to send its own LAN address to devices that request DNS server IP addresses and to forward DNS queries to the real DNS servers after the WAN connection is established. The router can thus act as a proxy for devices on the LAN.

In forwarding DNS queries, the router caches the responses from the real DNS servers. Over time, the router's cache accumulates the DNS information most often requested, enabling the router to respond to most DNS queries coming from the LAN and reducing the packet overhead on the WAN interface.

In order for the DNS Proxy feature to work, the router must obtain the IP address of the real DNS server from the WAN when the WAN connection is established.

The **ip dns server** global configuration command enables DNS proxy server functionality on the router and causes the router to forward DNS queries to the actual DNS servers. The **dns-server** *address* global configuration command causes the router to respond to DNS queries with its own IP address.

DNS Spoofing

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtdnsspf.html

Dynamic DNS Support for Cisco IOS

This feature was introduced in Cisco IOS Release 12.3(8)YA. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3y/12_3ya8/gt_ddns.html

Dynamic Multipoint VPN (DMVPN)

The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IP Security (IPSec) Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IPSec encryption, and Next Hop Resolution Protocol (NHRP).

Benefits of the DMVPN feature are as follows:

- Hub router configuration reduction
- Automatic IPSec encryption initiation
- Support for dynamically addressed spoke routers
- Dynamic tunnel creation for spoke-to-spoke tunnels

Easy Secure Device Deployment AAA Integration

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtezsddi.html

Easy VPN Client RSA Signature Support

The Easy VPN Client RSA Signature Support feature provides for the support of Rivest, Shamir, and Adelman (RSA) signatures on Easy VPN remote devices. The support is provided through RSA certificates that can be stored on or off the remote device.

Easy VPN Server

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ftunity.html

EIGRP MPLS VPN PE-CE Site of Origin (SoO)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtmvesoo.html

EIGRP Prefix Limit Support

This feature was introduced in Cisco IOS Release 12.0(29)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_epls.html

EIGRP SNMP Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_epls.html

EIGRP Support for Route Map Filtering

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gteigrpr.html

E-mail Inspection Engine

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_email.html

Embedded Event Manager 1.0

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtioseem.html

Embedded Event Manager 2.1

This feature was introduced in Cisco IOS Release 12.0(26)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gteem21.html

Embedded Resource Manager (ERM)

The Embedded Resource Manager (ERM) feature allows you to impose and monitor an upper limit of usage for resources such as buffer, memory, and CPU. This feature monitors system resource usage to better understand scalability needs by allowing you to configure threshold values for the CPU, buffer and memory resource owners. This check helps prevent catastrophic system failures due to high levels of resource depletion:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_rmimg.html

Embedded Syslog Manager

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_esm.html

Enabling OSPFv2 on an Interface Using the ip ospf area Command

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospfarea.html

Encrypted Preshared Key

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_epsk.html

End-of-Record Function for DCNs

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gteordcn.html

Enhanced Conferencing and Transcoding for Voice Gateway Routers

The Enhanced Conferencing and Transcoding for Voice Gateway Routers feature provides enhanced multiservice support for Cisco routers in a Cisco CallManager network. This is accomplished by enabling audio conference and transcode functions in access routers. This single-package solution simplifies deployments and eases administration. Tangible cost savings are realized with the location of conference resources in the branch to reduce WAN utilization. Costs are further reduced with the use of transcode services to reduce bandwidth needs. This feature requires the PVDM2 and is also supported on the NM-HD.

Note This feature requires Cisco CallManager 4.0 or a later release.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/sw/voicesw/ps4952/index.html

Enhanced Crashinfo File Collection Method

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gt_cricm.html

Enhanced cRTP for Links with High Delay, Packet Loss, and Reordering

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gt_ecrtp.html

Enhanced Debug Capabilities for Cisco Voice Gateways

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt17004t.html

Enhanced ITU-T G.168 Echo Cancellation

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vclport.html

Enhanced Object Tracking

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/fthsrptk.html

Enhanced Object Tracking of Service Assurance Agent (SAA) Operations

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtfhrp.html

Enhanced Voice and QoS for ADSL and G.SHDSL

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtevqos.html

ESMTP Support for Cisco IOS Firewall

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_esmtp.html

ETSI Call Transfer

For detailed information about this feature, see the "Configuring Telephony Call-Redirect Features" chapter in the *Cisco IOS TCL IVR and VoiceXML Application Guide*.

Exclusive Configuration Change Access

This feature provides a configuration locking mechanism for exclusive change access to the configuration for the duration of the lock. Two new commands are provided to enable or disable the configuration lock: **configuration mode exclusive** and **configure terminal lock**.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_exclu.html

Extended ACL Support for IGMP to Support SSM in IPv4

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtmcxacl.html

Extended Prepaid Tariff Switch with SSG

The Extended Prepaid Tariff Switch with SSG feature is used to measure the usage of specific services at various times, even when the monetary value of the volume quota does not change at the time of tariff switching. In such a scenario, the remaining amount of a user's pre-tariff-switch quota continues as

post-tariff-switch quota. Information can be collected about how much quota was used before a particular time and how much was used after, providing a usage profile of specific services at various times.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/sgbacctg.html

FACILITY Debug Enhancement

Overview

This feature enables display of ASN.1-encoded ISDN FACILITY Information Element (IE) contents. All supported operations of the ISDN supplementary services—Advice of Charge (AOC), Two B-Channel Transfer (TBCT), Explicit Call Transfer (ECT), and Malicious Call Identification (MCID)—are now included as part of the debug messages. Prior to this enhancement, the **debug isdn q931** command displayed the contents of the FACILITY IE in its raw hexadecimal format. Now, the parameters of FACILITY IE are displayed in text format along with parameter values where they are applicable and as they are relevant to the operation. In addition, the ASN.1-encoded Notification structure of the Notification-Indicator IE is also decoded. This debugging information is available for both incoming and outgoing FACILITY IEs in any message over an ISDN interface.

The **debug isdn q931** command must be enabled to display the contents of the FACILITY IE. Following are examples of new messages displayed in the **debug isdn q931** command output. See the **debug isdn q931** command page for more details about the information displayed by the FACILITY IE.

Output for Invoke Component Debug Message with MCID Operation: Example

Old output:

```
07:20:21: ISDN Se7/4:23 Q931: TX -> FACILITY pd = 8  callref = 0x8001
    Facility i = 0x91A106020107020103
-   ETSI Supplementary Service, Invoke, Malicious Call ID
```

New output:

```
07:20:21: ISDN Se7/4:23 Q931: TX -> FACILITY pd = 8  callref = 0x8001
    Facility i = 0x91A106020107020103
        Protocol Profile = Remote Operations Protocol
        A106020107020103
        Component = Invoke Component
            Invoke Id = 07 (MCID)
            Operation = McidRequest
```

Output for Return Result Component Debug Message for TBCT: Example

Old output:

```
02:05:33: ISDN Se7/4:23 Q931: RX <- FACILITY pd = 8  callref = 0x01
        Facility i = 0x91A203020105A113020101800105060 72A8648CE15000A81020164
```

New output:

```
02:05:33: ISDN Se7/4:23 Q931: RX <- FACILITY pd = 8  callref = 0x01
        Facility i = 0x91A203020105A113020101800105060 72A8648CE15000A81020164
        Protocol Profile = Remote Operations Protocol
        A203020105
        Component = Return Result Component
            Invoke Id = 05 (TBCT)

        A113020101800105060 72A8648CE15000A81020164
        Component = Invoke Component
```

```
            Invoke Id = 01 (unknown)
            Linked Id = 05
            Operation = SetCallTag
                Call Tag = 356
```

Output for Return Error Component Debug Message: Example

Old output:

```
16:27:07: ISDN Se1:23 Q931: RX <- FACILITY pd = 8  callref = 0x01
        Facility i = 0x91A306020107020109
        - ETSI Supplementary Service, Return Error
```

New output:

```
16:27:07: ISDN Se1:23 Q931: RX <- FACILITY pd = 8  callref = 0x01
        Facility i = 0x91A306020107020109
        Protocol Profile = Remote Operations Protocol
        A306020107020109
        Component = Return Error Component
            Invoke Id = 07 (MCID)
            Error = Not Incoming Call
```

Output for Reject Component Debug Message: Example

Old output:

```
03:09:17: ISDN Se7/4:23 Q931: RX <- FACILITY pd = 8  callref = 0x01
    Facility i = 0x91A406020109800102
```

New output:

```
03:09:17: ISDN Se7/4:23 Q931: RX <- FACILITY pd = 8  callref = 0x01
    Facility i = 0x91A406020109800102
        Protocol Profile = Remote Operations Protocol
        A406020109800102
        Component = Reject Component
            Invoke Id = 09 (Unknown)
            Problem = General Problem; Badly structured Component
```

Output for Notification-Indicator IE Component Debug Message: Example

Old output:

```
Mar  1 01:48:26.543: ISDN Se1/0:23 Q931: RX <- NOTIFY pd = 8  callref = 0x00
Notification Ind i = 0x83300C06072A8648CE15020181010D
```

New output:

```
Mar  1 01:48:26.543: ISDN Se1/0:23 Q931: RX <- NOTIFY pd = 8  callref = 0x00
Notification Ind i = 0x83300C06072A8648CE15020181010D
                Notification = Transferred Call Clearing
                Call Tag = 13
```

FHRP—VRRP Enhancements

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtvrrpen.html

File Download Using HTTP

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_hcopy.html

Firewall ACL Bypass

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_aclby.html

Firewall Authentication Proxy for FTP and Telnet Sessions

The authentication proxy in the Cisco IOS firewall feature set currently supports only the HTTP protocol. Authentication proxy support has been extended to the FTP/Telnet protocols with this release. This release also introduces absolute timeout functionality to the authentication proxy feature. The absolute timeout sets a time window during which the authentication proxy on the enabled interface is active. As the absolute timer expires, the authentication proxy will be disabled. The addition of the absolute timeout upgrades the functionality of the authentication proxy and also meets the firewall requirements.

Firewall Intrusion Detection System (IDS) Enhancements

The Cisco IOS Intrusion Detection System (IDS) feature supports intrusion detection technology on all the Cisco IOS–based router platforms when the Cisco IOS firewall is present. The Cisco IOS IDS feature identifies 101 of the most common attacks, using signatures to detect patterns of misuse in network traffic. The Cisco IOS IDS acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router, scanning each to match any of the IDS signatures. When the Cisco IOS IDS detects suspicious activity, it responds before network security can be compromised, and it logs the event through the Cisco IOS syslog or the Cisco Secure Intrusion Detection System (Cisco Secure IDS, formerly known as NetRanger) Post Office Protocol. The network administrator can configure the IDS system to choose the appropriate response to various threats.

Firewall N2H2 Support

N2H2 is globally deployed third-party URL filtering software that can filter HTTP requests, based on destination hostname, destination IP address, username, and password. It relies on a sophisticated URL database of more than 15 million sites organized into more than 40 categories using both Internet technology and human review. This feature enables the Cisco IOS firewall to do URL filtering based on the N2H2 server. When a Cisco 800 router receives an HTTP request, it sends a query request to the N2H2 server with the requested URL. The N2H2 server does some necessary lookups for the URL and sends back a query response. Based on the N2H2 server's response, the router either blocks the HTTP request by redirecting the browser to a block page or proceeds with normal HTTP processing.

For more information on this feature, see the following URL:

http://www.cisco.com/en/US/partner/docs/ios/12_2t/12_2t15/feature/guide/ft_n2h2.html

Firewall Support for SIP

This feature allows Session Initiation Protocol (SIP) signaling requests to traverse directly between gateways or through a series of proxies to the destination gateway or phone. After the initial request, if the Record-Route header field is not used, subsequent requests can traverse directly to the destination gateway address as specified in the Contact header field. Thus, the Cisco IOS firewall is aware of all surrounding proxies and gateways and allows the following functionality:

- SIP signaling responses can travel the same path as SIP signaling requests.
- Subsequent signaling requests can travel directly to the endpoint (destination gateway).
- Media endpoints can exchange data.

For more information on this feature, see the following URL:

http://www.cisco.com/en/US/partner/docs/ios/12_2t/12_2t15/feature/guide/ft_fwsip.html

Firewall Support of SSL Encrypted HTTP Authentication Proxy Sign-On

The Firewall Support of SSL Encrypted HTTP Authentication Proxy Sign-On feature allows a user to encrypt the change of the username and password between the HTTP client and the Cisco IOS router via Secure Socket Layer (SSL) when authentication proxy is enabled on the Cisco IOS firewall, thereby ensuring confidentiality of the data passing between the HTTP client and the Cisco IOS router.

Firewall Websense URL Filtering

Websense is a third-party URL filtering software program that can filter HTTP requests, based on destination hostname, destination IP address, keywords, and username. Websense maintains a URL database of more than 20 million sites organized into more than 60 categories and subcategories. This feature enables the Cisco IOS firewall to do URL filtering based on the Websense server. When a Cisco 800 router receives an HTTP request, it sends a query request to the Websense server with the requested URL. The Websense server does some necessary lookups for the URL and sends back a query response. Based on the Websense server's response, the router either blocks the HTTP request by redirecting the browser to a block page or proceeds with normal HTTP processing.

For more information on this feature, see the following URL:

http://www.cisco.com/en/US/partner/docs/ios/12_2t/12_2t15/feature/guide/ftwebsen.html

Four-Wire Mode for SHDSL

The Four-Wire Mode for SHDSL feature adds four-wire support in fixed line-rate mode only on a single-port multiline G.SHDSL WIC or WIC-1SHDSL-V2. This feature builds on the existing features of the Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature supported on the 1-port G.SHDSL WIC (WIC-1SHDSL). Four-Wire Mode for SHDSL supports the Cisco 2600XM series, Cisco 2691, Cisco 3600, and Cisco 3700 series routers and incorporates the latest firmware and the latest circuitry. The four-wire feature of G.991.2 doubles the bandwidth in ATM mode and increases usable distance over two pairs of wires.

This feature supports ATM in four-wire mode. Embedded Operation Channel (EOC) messages support for customer premise equipment (CPE) is provided for two-wire and four-wire modes.

Framed-Route in RADIUS Accounting

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_fra22.html

Frame Relay—Multilink (MLFR-FRF.16)

The Multilink Frame Relay feature introduces functionality based on the Frame Relay Forum Multilink Frame Relay UNI/NNI Implementation Agreement (FRF.16). This feature provides a cost-effective way to increase bandwidth for particular applications by enabling multiple serial links to be aggregated into a single bundle of bandwidth. Multilink Frame Relay is supported on User-to-Network Interfaces (UNIs) and Network-to-Network Interfaces (NNIs) in Frame Relay networks.

Frame Relay Switched Virtual Circuits (SVC) over ISDN

The Frame Relay Switched Virtual Circuits over ISDN feature provides support for Frame Relay switched virtual circuits (SVCs) over ISDN BRI lines. Before the introduction of this feature, Frame Relay over ISDN supported Frame Relay permanent virtual circuits (PVCs) only. Frame Relay SVCs can be configured on dialer or BRI interfaces in the same way that SVCs are configured on serial interfaces.

For additional information on configuring Frame Relay and Frame Relay SVCs, see the "Configuring Frame Relay" chapter of the *Cisco IOS Wide-Area Networking Configuration Guide* at the following location:

http://www.cisco.com/en/US/docs/ios/12_3/featlist/wan_vcg.html

Gatekeeper Prefix Selection for Hair-Pinned Calls

The Gatekeeper Prefix Selection for Hair-Pinned Calls feature enables an H.323 gatekeeper to terminate/hairpin calls from a TDM/PSTN endpoint back through the same originating gateway on the basis of priority/zone prefix values.

For detailed information about this feature, see the *Cisco Multiservice IP-to-IP Gateway Application Guide*:

http://www.cisco.com/en/US/docs/ios/12_3/multiservice_ip2ip/guide/ipipgw_2.html

Generic Routing Encapsulation Tunnel IP Source and Destination VRF Membership

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtgrevrf.html

GGSN R3.1

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2/12_2y/12_2yy/ggsn31/31cmd/ggsn31_r.html

http://www.cisco.com/en/US/docs/ios/12_2/12_2y/12_2yy/ggsn31/31cfg/ggsn31_c.html

GLBP MD5 Authentication

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtglbpau.html

Granular Protocol Inspection

The Granular Protocol Inspection feature adds flexibility to the Cisco IOS Firewall by allowing it to perform a higher degree of inspection of TCP and User Data Protocol (UDP) traffic for most RFC 1700 application types.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtgpinsp.html

Health Monitor and Diagnostic Monitor for the Cisco AS5850

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/feature/guide/ft585hm.html

Hookflash and DTMF Relay Transfer

Hookflash and DTMF Relay Transfer is a cost-effective way to transfer customer calls from first-level technical support to other agent groups for second-level support. The circuit between the transferrer and the transferee is released after the transferrer initiates the transfer and the remote switch connects the transferee and the transfer target.

Hot Standby Router Protocol (HSRP)

Hot Standby Router Protocol (HSRP) enables a set of routers to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. HSRP is particularly useful in environments in which critical applications are running and fault-tolerant networks have been designed. By sharing an IP address and a MAC address, two or more routers that are acting as one virtual router are able to seamlessly assume the routing responsibility in the case of a defined event or an unexpected failure. This enables hosts on a LAN to continue forwarding IP packets to a consistent IP and MAC address so that the changeover of devices that are doing the routing is transparent to them and their sessions.

The routers in an HSRP configuration are known as an HSRP group or standby group. A single router selected from the group is responsible for forwarding the packets that hosts send to the virtual router. This router is known as the active router. Another router is selected as the standby router. If the active router fails, the standby router assumes the packet forwarding duties of the active router. Although an arbitrary number of routers may run HSRP, only the active router forwards the packets sent to the virtual router.

HSRP uses a priority scheme to determine which HSRP-configured router is to be the default active router. To configure a router as an active router, the router is assigned a priority that is higher than the priority of all the other HSRP-configured routers. The default priority is 100. If any of the routers is configured with a higher priority, those routers will be the active router.

HSRP works by the exchange of multicast messages that advertise priority among HSRP-configured routers. When the active router fails to send a hello message within a configured period of time, the standby router with highest priority becomes the active router. The transition of the packet-forwarding function between routers is completely transparent to all the hosts on the network.

HSRP-configured routers exchange three types of multicast messages.

- Hello—The hello messages convey to other HSRP routers the router's HSRP priority and state information. By default, an HSRP router sends hello messages every 3 seconds.
- Coup—When a standby router assumes the function of the active router, it sends a coup message.
- Resign—A router that is the active router sends this message when it is about to shut down or when a router with a higher priority sends a hello message.

At any time, HSRP-configured routers will be in one of the following states:

- Active—The router is performing packet-transfer functions.
- Standby—The router is ready to assume packet-transfer functions if the active router fails.
- Speaking and listening—The router is sending and receiving hello messages.
- Listening—The router is receiving hello messages.

Hot Standby Router Protocol Version 2

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gthsrpv2.html

HSRP MD5 Authentication

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gthsrpau.html

HTTP Client API for TCL IVR

The HTTP Client API for TCL IVR feature enables TCL IVR applications to retrieve data from or post data to an external HTTP server. Also introduces a new command-line-interface structure for configuring voice applications and support for additional TCL 8.3.4 commands.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_http_api_tclivr.html

HTTP Inspection Engine

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_fwapc.html

IEEE 802.1Q Tunneling

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_qinq.html

IGMPv3 Host Stack

The IGMPv3 Host Stack feature enables routers and switches to function as multicast network endpoints or hosts. The feature adds INCLUDE mode capability to the Internet Group Management Protocol (IGMP) version 3 host stack for Source Specific Multicast (SSM) groups.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtigmpv3.html

Image Verification

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtigmpv3.html

Implementing RIP for IPv6

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-rip.html

Import of RSA Keypair and Certificates in PEM Format

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrsapem.html

Inspection of Router-Generated Traffic

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_insrg.html

Integrated IS-IS Global Default Metric

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtisglob.html

Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtisprot.html

Integrated Routing and Bridging (IRB) Support for the Cisco MGX-RPM-XF-512

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_irb.html

Interoperability Enhancements to the Cisco Multiservice IP-IP Gateway

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6968/ps6441/product_bulletin_c25-409474.html#wp9005754

Intrusion Prevention System (IPS) - Signature Enhancements

The IPS Signature Enhancements feature expands the number and type of virus and attack signatures currently available in the Intrusion Detection System/Intrusion Prevention System (IDS/IPS) Sensor database. These signatures are specific to TCP, UDP, and ICMP intrusions.

For detailed information about this feature, see the *Cisco IOS Intrusion Prevention System (IPS)* document at:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_fwids.html

Invalid Security Parameter Index Recovery

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_ispir.html

IOS Embedded Event Manager 2.1

This feature was introduced in Cisco IOS Release 12.0(26)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gteem21.html

IP Security VPN Monitoring

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ipsvm.html

IP Side Answer Tone Detection for Echo Canceller Control

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/as5350/software/release/notes/echocan.html

IP SLAs Sub-millisecond Accuracy Improvements

This feature enhances the granularity and accuracy of IP SLA measurements. For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/ps6350/prod_bulletin09186a0080457b39.html

IP SLA—VoIP Call Setup (Post Dial Delay) Monitoring

The IP SLA VoIP Call Setup Monitoring operation measures the call setup time using H.323/SIP signaling protocol over IP networks. The typical setup time measured is from the setup/INVITE message sent to alert/ringing message received.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtslapdd.html

IP SLA—VoIP Gatekeeper Registration Delay Monitoring

The IP SLA Gatekeeper Registration Delay Monitoring operation measures the light weight registration time from H.323 Gateways to Gatekeepers.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtslagkd.html

IP Source Tracker

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ipst.html

IP to ATM CoS Enhancements

The IP to ATM CoS feature implements a solution for coarse-grained mapping of quality of service (QoS) characteristics between IP and ATM, using Cisco Enhanced ATM port adapters (PA-A3) on Cisco 7200 and Cisco 7500 series routers. This category of coarse-grained QoS is often referred to as class of service (CoS). The resulting feature makes it possible to support differential services in network service provider environments.

With the Cisco IOS Release 12.3(4)T, the IP to ATM CoS feature has been enhanced to include support for the Cisco 7500 series router with either the PA-A3-8T1 IMA or PA-A3-8E1 IMA port adapters.

For more information about the IP to ATM CoS feature, see the “Quality of Service Solutions” section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

IPHC (cRTP/cUDP/cTCP)

Internet Protocol Header Compression (IPHC) includes compressed Routing Table Protocol (cRTP), compressed User Datagram Protocol (cUDP), and compressed Transport Control Protocol (cTCP) and allows low speed links to run more efficiently when IP headers are extremely large or of comparable size to the payload.

An IPHC-enabled interface sends only changes to the header instead of sending the entire header with every packet.

At the beginning of a transmission, the transmitting end (the compressor) sends a full header packet to the receiving end (the decompressor). After this initial packet, the compressor sends all other packets with headers that contain only the differences between them and the original full header. The decompressor maintains a copy of the original full header and reconstructs all the other packet headers by adding the changes to them.

IPSec and Quality of Service

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtqosips.html

IPSec Anti-Replay Window: Expanding and Disabling

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_iarwe.html

IPSec Dead Peer Detection Periodic Message Option

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtdpmo.html

IPsec NAT Transparency

The IPSec NAT Transparency feature introduces support for IP Security (IPSec) traffic to travel through the Network Address Translation (NAT) or Point Address Translation (PAT) point in the network by addressing many known incompatibilities between NAT and IPSec. This feature encapsulates IPSec packets in a User Datagram Protocol (UDP) wrapper, which allows the packets to travel across NAT devices.

A standard IPSec Virtual Private Network (VPN) tunnel would not work if there are one or more NAT or PAT points in the delivery path of the IPSec packet. This feature makes NAT IPSec aware, thereby allowing remote access users to build IPSec tunnels to home gateways.

IPSec Preferred Peer

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_ipspp.html

IPSec Virtual Tunnel Interface

The IPSec Virtual Tunnel Interface feature:

- Provides a routable interface for terminating IPSec tunnels.
- Provides ease of configuration.
- Provides facility of routing.
- Supports multicast.
- Supports aspects like Network Management, HA, and Load Balancing.

IPv6 BSR Bi-Directional Support

This feature was introduced in Cisco IOS Release 12.3(2)T. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html#wp1055997

IPv6 IOS Firewall FTP Application Support

Cisco IOS IPv6 Firewall FTP application support is provided by port-to-application mapping (PAM). PAM allows you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application.

For more information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-sec_trfltr_fw.html

IPv6 Multicast: Bootstrap Router (BSR)

For Cisco IOS IPv6 multicast implementations, PIM routers in a domain must be able to map each multicast group to the correct RP address. The BSR protocol for PIM-SM provides a dynamic, adaptive mechanism to distribute group-to-RP mapping information rapidly throughout a domain. With the IPv6 BSR feature, if an RP becomes unreachable, it will be detected and the mapping tables will be modified so that the unreachable RP is no longer used, and the new tables will be rapidly distributed throughout the domain.

For more information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html#wp1055997

IPv6 Support for AS5850 Dial

As of Cisco IOS Release 12.3(11)T, Cisco IOS IPv6 is supported on the Cisco AS5850 platform. For detailed information about Cisco IOS IPv6, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html

ISDN Backup in MPLS Core

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_isdn_backup_mpls.html

ISDN Calling Name Display

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/sip/configuration/guide/sipftgde.html

ISDN Type of Number to RADIUS Server

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_isdnt.html

IS-IS Caching of Redistributed Routes

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/isredrib.html

IS-IS Fast-Flooding of LSPs Using the fast flood Command

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fstfld.html

IS-IS Incremental SPF

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/isisispf.html

IS-IS Limit on Number of Redistributed Routes

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsiredis.html

IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsisiadv.html

IS-IS Support for Priority-Driven IP Prefix RIB Installation

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fslocrib.html

IS-IS Support for Route Tags

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtisitag.html

Key Rollover for Certificate Renewal

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtkyroll.html

L2TP Client-Initiated Tunneling

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtvoltun.html

L2TP Tunnel Connection Speed Labeling

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtclabel.html

L2TPv3: Layer 2 Tunnel Protocol Version 3

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtl2tpv3.html

Note The L2TPv3: Layer 2 Tunnel Protocol Version 3 feature is not currently supported on the Cisco 7200 NPE-G1 in Cisco IOS Release 12.3T.

LAN Network Manager (LNM)

As of Cisco IOS Release 12.3(4)T, the LAN Network Manager (LNM) feature has been removed from Cisco IOS software.

Land Mobile Radio (LMR) over IP

This feature was introduced in Cisco IOS Release 12.3(4)XD. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtlmrip.html

LFI

Link Fragmentation Interleaving (LFI) allows a large packet to be divided into smaller fragments so that excessive head of line blocking can be avoided for smaller packets such as Voice over IP (VoIP) packets.

On slow speed interfaces (slower than T1), a packet with maximum transmission unit (MTU) can cause excessive head of line blocking in low latency priority queues (LLQs) especially in VoIP applications. The solution is to implement LFI on these interfaces.

The RPM-XF supports LFI on MLPPP interfaces and supports up to 200 LFI-enabled interfaces. LFI and PPP interfaces use the Multilink PPP (MLPPP) long sequence number fragment format headers.

LFI over multiple links in an MLPPP bundle is not supported. Receiving and reassembling out of sequence fragments is also not supported.

Loadsharing IP Packets Over More Than Six Parallel Paths

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_mpg6.html

Local AAA Server

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_laas.html

Login Password Retry Lockout

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/g_cilprl.html

Lossless Compression R1, ATM Cell Switching, External BITS Clocking Source

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vclfeat.html

Low Latency Queueing

Low latency queueing (LLQ) provides a low-latency, strict-priority transmit queue for Voice over IP (VoIP) traffic.

MAC Address Based Authorization with SSG

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/sgbmaca.html

Malicious Caller Identification Invocation Support for Enterprise Networks

The Malicious Caller Identification (MCID) Invocation Support for Enterprise Networks feature extends support for MCID service in the public service telephone network (PSTN) to the Cisco 2801.

This feature was introduced in Cisco IOS Release 12.2(15)T. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the Malicious Caller Identification Invocation Support for Enterprise Networks document:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftmcid.html

Managed LAN Switch

The Managed LAN Switch feature enables the control of the four switch ports in Cisco 831, 836, and 837 routers. Each switch port is associated with a Fast Ethernet interface. The output of the command **show controllers fastEthernet** *<1-4>* displays the status of the selected switch port. The Managed LAN Switch feature allows setting and display of the following parameters for each of the switch ports:

- Speed
- Duplex

It also allows display of the link state of a switch port—that is, whether a device is connected to that port or not.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xc/feature/guide/mlans.html

MCID for Cisco IOS Voice Gateways

The MCID for Cisco IOS Voice Gateways feature supports the Malicious Call Identification (MCID) supplementary service that enables Cisco CallManager 4.0 to identify the source of malicious calls.

For detailed information about this feature, see the "Configuring MCID for Cisco IOS Voice Gateways" chapter in the *Cisco CallManager and Cisco IOS Interoperability Guide*:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/interop/int_mcid.html

Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways in SRST Mode

For detailed information about this feature, see the Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways in SRST Mode document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtsecure.html

Media Inactive Call Detection

For detailed information about this feature, see the following document:

https://www.cisco.com/en/US/docs/ios/voice/ivr/configuration/guide/ivrapp07.html

Memory and CPU Measurement

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_mmeas.html

Memory Threshold Notifications

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_memnt.html

Memory Thresholding Infrastructure

For detailed information about this feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_thres.htm

MGCP-Controlled Backhaul of BRI Signaling in Conjunction with Cisco CallManager

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftbribkh.html

MGCP Fax Rate Control

To establish the maximum fax rate for Media Gateway Control Protocol (MGCP) T.38 sessions, use the **mgcp fax rate** command in global configuration mode. To reset MGCP endpoints to their default fax rate, use the **no** form of this command.

mgcp fax rate {**2400** | **4800** | **7200** | **9600** | **12000** | **14400** | **voice**}

no mgcp fax rate

For detailed information about this feature, see the "Configuring T.38 Fax Relay" section in the Cisco Fax Services over IP Application Guide.

MGCP Line Control Signaling Package

The **mgcp package-capability** command has been modified. The **lcs-package** keyword has been added to the list of package selections.

The line control signaling (LCS) package supports the transport of line supervision signals in the media stream using RFC-2833 event packets in PacketCable GR303-switched IP systems. When the **lcs-package** keyword is used, the named telephony events (NTEs) associated with the LCS package are enabled automatically. The following telephone events are supported by devices that implement the LCS package:

- Ring (RFC-2833 event 144)
- On-hook (RFC-2833 event 149)
- Open signal interval (RFC-2833 event 159)

For detailed information about this feature, see the "Basic MGCP Configuration" chapter of the *Cisco IOS MGCP and Related Protocols Configuration Guide.*

MGCP Support for CallManager (IP-PBX)

The MGCP Support for CallManager (IP-PBX) feature enables the Cisco IOS software on the Cisco 1751 and Cisco 1760 to interact with Cisco CallManager using Media Gateway Control Protocol (MGCP). It provides MGCP-based supplementary services, failover, redundancy, and multicast music on hold (MoH) support for CallManager.

MIB Enhancements for H.323, SIP, and MGCP

The MIB Enhancements for H.323, SIP, and MGCP feature provides SNMP MIB enhancements on the following platforms:

- Cisco AS5350 universal gateways
- Cisco AS5400 series universal gateways
- Cisco AS5850 universal gateways

The MIBs contain objects that represent active H.323, SIP, and MGCP calls and also include call details. For definitions of the H.323, SIP, and MGCP MIB objects, see the following MIBs:

- CISCO-H225-MIB
- CISCO-MEDIA-GATEWAY-MIB
- CISCO-MGC-MIB
- CISCO-SIP-CALLS-MIB
- CISCO-TC
- CISCO-XGCP-CAPABILITY
- CISCO-XGCP-EXT-CAPABILITY
- CISCO-XGCP-EXT-MIB
- CISCO-XGCP-MIB

To locate and download MIBs, use Cisco MIB Locator found at the following URL:

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

Minimal Disruptive Restart of VIP Cards

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtmdrvip.html

MLPP for Analog and BRI Endpoints on Cisco IOS Voice Gateways

Provides the capability for Cisco IOS voice gateways to present analog and basic rate interface (BRI) phones to be controlled by the Cisco CallManager as though they were Cisco IP phones, enabling the following:

- Line-side support for the Multilevel Precedence and Preemption (MLPP) feature
- Cisco CallManager registration of analog and Basic Rate Interface (BRI) endpoints
- Cisco CallManager endpoint auto configuration support
- Modem pass-through support
- Cisco Survivable Remote Site Telephony (SRST) support

For detailed information about this feature, see the MLPP for Analog and BRI Endpoints on Cisco IOS Voice Gateways document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtstcapp.html

MLPP for Cisco IOS Voice Gateways

The MLPP for Cisco IOS Voice Gateways feature supports Multilevel Precedence and Preemption (MLPP) service, allowing authorized users to preempt lower priority voice calls using Cisco CallManager 4.0.

For detailed information about this feature, see the "Configuring MGCP Gateway Support for Cisco CallManager" chapter in the *Cisco CallManager and Cisco IOS Interoperability Guide*:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/interop/intcnf1.html

Mobile IP

Mobile IP is an open standard, defined by the Internet Engineering Task Force (IETF) RFC 2002, that allows users to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks. Mobile IP is scalable for the Internet because it is based on IP—any media that can support IP can support Mobile IP.

Cisco IOS software and its support for Mobile IP provide the technology that enables an IP node's ability to retain the same IP address and maintain existing communications while traveling from one network to another.

Mobile IP eliminates a stop-and-start approach to IP connectivity that is required with network location changes, thus enabling users to maintain the same IP address regardless of their point of attachment to the network.

Mobile IP has the following three components:

1. Mobile Node

   The Mobile Node is a device such as a cell phone, PDA, or laptop whose software enables network roaming capabilities.

2. Home Agent

   The Home Agent is a router on the home network that serves as the anchor point for communication with the Mobile Node; it tunnels packets from a device on the Internet, called a Correspondent Node, to the roaming Mobile Node. (A tunnel is established between the Home Agent and a reachable point for the Mobile Node in the foreign network.)

3. Foreign Agent

   The Foreign Agent is a router that can function as the point of attachment for the Mobile Node when it roams to a foreign network, delivering packets from the Home Agent to the Mobile Node.

The care-of address is the termination point of the tunnel toward the Mobile Node when it is on a foreign network. The Home Agent maintains an association between the home IP address of the Mobile Node and its care-of address, which is the current location of the Mobile Node on the foreign or visited network.

The Mobile IP process has three main phases:

1. Agent Discovery—A Mobile Node discovers its Foreign Agent and Home Agent during agent discovery.
2. Registration—The Mobile Node registers its current location with the Foreign Agent and Home Agent during registration.
3. Tunneling—A reciprocal tunnel is set up by the Home Agent to the care-of address (current location of the Mobile Node on the foreign network) to route packets to the Mobile Node as it roams.

Mobile IP uses a strong authentication scheme for security purposes. All registration messages between a Mobile Node and a Home Agent are required to contain the Mobile-Home Authentication Extension (MHAE).

Mobile IP CPS Improvement at FA

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/wireless/pdsn/12.311t/MoipCPS.html

Mobile IP Dynamic Security Association and Key Distribution

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtmipsec.html

Mobile IP—Foreign Agent Local Routing to Mobile Networks

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtfamoip.html

Mobile IP—Generic Routing Encapsulation for Cisco Mobile Networks

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtgremip.html

Mobile IP Home Agent Redundancy for Dynamic Mobile Networks

With the introduction of the Mobile IP Home Agent Redundancy for Dynamic Mobile Networks feature, the mobile router is capable of dynamically registering network(s) (or subnet) with its home agent. This functionality greatly simplifies deployment and provisioning.

To achieve this functionality, extra information is stored in the mobility binding. However, this extra information was not passed to the standby home agent in case of a redundant home agent configuration. Thus, the standby home agent would not know of a dynamically registered network and the stateful switchover was compromised. If the active home agent went down and the standby home agent took over, the dynamic network information was lost and the entire dynamic network would lose connectivity.

The Mobile IP Home Agent Redundancy for Dynamic Mobile Networks feature provides a solution to this problem by keeping the mobility bindings synchronized between the active and standby home agents. Now the standby home agent will have dynamic mobile network information stored in its mobility binding table ensuring a successful stateful switchover.

Dynamic network support for Cisco Mobile Networks was added in Cisco IOS Release 12.2(13)T. See "Cisco Mobile Networks" feature documentation for more information on this feature at the following location:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t4/feature/guide/ftmbrout.html

Mobile IP MIB for Reverse Tunnel, Challenge, and VSEs

Reverse tunnel, challenge, and vendor specific extensions (VSEs) have been added to Mobile IP functionality. The Mobile IP MIB for Reverse Tunnel, Challenge, and VSEs feature provides MIB objects for this functionality. These features can now be managed and monitored via Simple Network Management Protocol (SNMP).

Mobile IP—Mobile IPv6 Home Agent

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con_ps6441_TSD_Products_Configuration_Guide_Chapter.html

Mobile IP—Mobile Router DHCP Support for Dynamic CCoA and Foreign Agent Processing

The Mobile Router DHCP Support for Dynamic Collocated Care-of Address (DCCoA) and Foreign Agent (FA) Processing feature adds support for mobile router roaming on Ethernet interfaces that acquire an IP address dynamically via the Dynamic Host Configuration Protocol (DHCP). The interface can register using this acquired IP address as a DCCoA or register using a CoA acquired from a foreign agent. This behavior is true for all platforms that support Mobile IP beginning with Cisco IOS Release 12.3(14)T.

This feature adds support for FA processing of advertisements and registrations on DHCP roaming interfaces.

A Simple Network Management Protocol (SNMP) signaling capability is also added to support this feature on the Cisco 3200 Series Mobile Access Router with a Wireless Mobile Interface Card (WMIC). The WMIC uses SNMP trap messages to signal the mobile router that the Layer 2 wireless local-area network (WLAN) is either up or down.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtdhcpm.html

Mobile IP—Support for RFC 3519 NAT Traversal

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtnatmip.html

Mobile Networks Deployment MIB

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtmdebug.html

Mobile Networks Dynamic Collocated Care-of-Address

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtcolloc.html

Modem Calls over QSIG

Some Cisco customers require that their routers connect to their PBXs and be capable of making modem calls with Q signaling (QSIG). This capability would allow them to continue using their internal private telecommunications network and to migrate from leased lines to Voice over IP (VoIP) topologies. The ISDN software in Cisco IOS Release 12.3(7)T supports modem calls with QSIG signaling. QSIG is one form of the common channel signaling (CCS) protocol used for PBX interconnection and is based on International Telecommunication Union ITU-T Recommendation Q.931.

Monitoring and Retraining on Reception of Loss of Margin Messages

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/feat_lom/dsllom.html

Monitoring Control Characters on Async Lines

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtasyncl.html

MPLS-aware NetFlow

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_mnf.html

MPLS DiffServ-Aware Traffic Engineering (DS-TE)

The MPLS DiffServ-Aware Traffic Engineering (DS-TE) feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers

- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

MPLS Enhancements to Interfaces MIB

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/ftifemib.html

MPLS Label Distribution Protocol MIB Version 8 Upgrade

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/ftldpv8.html

MPLS Label Switch Controller and Enhancements

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/ftlsc32t.html

MPLS LDP Autoconfiguration

The MPLS LDP Autoconfiguration feature was introduced in Cisco IOS Release 12.0(30)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsldpaut.html

MPLS LDP Graceful Restart

The MPLS LDP Graceful Restart feature was introduced in Cisco IOS Release 12.0(29)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsgr29s.html

MPLS LDP-IGP Synchronization

The MPLS LDP-IGP Synchronization feature was introduced in Cisco IOS Release 12.0(30)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsldpsyn.html

MPLS LDP Inbound Label Binding Filtering

This feature was introduced in Cisco IOS Release 12.0(26)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsinbd4.html

MPLS LDP Session Protection

This feature was introduced in Cisco IOS Release 12.0(30)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fssespro.html

MPLS—Multilink PPP Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/mplsdmlp.html

MPLS Quality of Service (QoS)

The MPLS Quality of Service (QoS) feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

MPLS QoS—DiffServ Tunneling Modes

The MPLS QoS—DiffServ Tunneling Modes feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2691 Multiservice routers
- Cisco 3725 Modular Access routers
- Cisco 3745 Modular Access routers
- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

MPLS Traffic Engineering (TE)

The MPLS Traffic Engineering (TE) feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers

- Cisco 3845 Series Integrated Services routers

MPLS Virtual Private Networks

The MPLS Virtual Private Networks (VPNs) feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution

The MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2691 Multiservice routers
- Cisco 3725 Modular Access routers
- Cisco 3745 Modular Access routers
- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

MPLS VPN—Explicit Null Label Support with BGP IPv4 Label Session

The MPLS VPN—Explicit Null Label Support with IPv4 BGP Label Session feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2691 Multiservice routers
- Cisco 3725 Modular Access routers
- Cisco 3745 Modular Access routers
- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

MPLS VPN Half-Duplex VRF (HDVRF) Support

The MPLS VPN Half-Duplex (HDVRF) Support feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2691 Multiservice routers
- Cisco 3725 Modular Access routers
- Cisco 3745 Modular Access routers
- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

The MPLS VPN—Inter-AS—IPv4 BGP Label Distribution feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2691 Multiservice routers
- Cisco 3725 Modular Access routers
- Cisco 3745 Modular Access routers
- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

MPLS VPN—MIB Notifications

The MPLS VPN—MIB Notifications feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2691 Multiservice routers
- Cisco 3725 Modular Access routers
- Cisco 3745 Modular Access routers
- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

MPLS VPN—MIB Support

The MPLS VPN—MIB Support feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2691 Multiservice routers
- Cisco 3725 Modular Access routers

- Cisco 3745 Modular Access routers
- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge

The MPLS VPN support for EIGRP between Provider Edge and Customer Edge feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

MPLS VPN VRF Selection Using Policy Based Routing

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_pbrsv.html

MSDP Compliance with IETF MSDP Draft 20

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_msdp.html

Multicast Fast Switching Performance Improvement

The Multicast Fast Switching Performance Improvement feature provides improvement of up to 100 percent of the existing multicast path packet throughput. This feature targets software forwarding-based platforms for IPv4 multicast only.

Multicast VPN

Multicast Virtual Private Network (VPN) provides the ability to transport multicast traffic inside an MPLS-VPN using multicast tunneling. A single MPLS-VPN endpoint can send a multicast packet to all other destination endpoints in the MPLS-VPN.

A customer edge (CE) router sends a multicast packet customer packet (C-packet) to a provider edge (PE) router. The PE router creates a provider packet (P-packet) by adding either a GRE-IP header or an IP-IP header to this packet. The PE router then sends the P-packet to one or more provider routers (P routers) using multicast processing.

Multicast VPN supports only MPLS frame-based encapsulation.

Multicast VPN MIB

The Multicast VPN MIB feature was introduced in Cisco IOS Release 12.0(29)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/mcvpnmib.html

Multiprotocol Label Switching (MPLS)

The Multiprotocol Label Switching (MPLS) feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

Multi-VRF CE (VRF-lite) Updated Performance

The Multi-VRF (VRF-lite) feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

NAT—dCEF Support

The NAT—dCEF Support feature enhances the overall performance of Route Switch Processors on Cisco 7500 series routers by enabling line cards to perform address translation. Without this feature, any Distributed Cisco Express Forwarding (dCEF) switched packet that needs address translation must be switched by the RSC (Route Switch Controller), which increases load and reduces system performance and throughput. With the NAT—dCEF Support feature, Network Address Translation (NAT) is implemented on the line card level so that address translation is carried out at the switching path.

In distributed switching, the switching process occurs on versatile interface processor (VIP) and other interface cards that support switching. When dCEF is enabled, line cards, such as VIP line cards or Gigabit Switch Router line cards, maintain an identical copy of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters, relieving the RSC of involvement in the switching operation. dCEF uses an interprocess communication (IPC) mechanism to ensure synchronization of FIBs and adjacency tables on the RSC and line cards. The NAT—dCEF Support feature also enables line cards to maintain a subset of the RSC NAT table. This enables the line cards to switch packets and perform express forwarding within and between port adapters. Because embedded address translation cannot occur at the line card level, packets that require payload translation are punted to the next higher-level switching mechanism in the RSC.

NAT—H.245 Tunneling Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/nat245tl.html

NAT Integration with MPLS VPNs (VRF-NAT)

The NAT Integration with MPLS VPNs (VRF-NAT) feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

NAT–Performance & Scalability Enhancement–Timer Wheel

The NAT–Timer Wheel Enhancement feature reduces CPU utilization in cases where routers must manage large numbers of NAT Network Address Translation (NAT) entries, and eliminates the performance bottleneck caused by the previous timer tree model. By using a more efficient data structure and a priority queue to sort the timer and eliminate the sorting operation during a timer insertion, the NAT–Timer Wheel Enhancement Feature speeds the process of inserting and removing a timer, which improves the scalability of a router running NAT.

NAT–Performance Enhancement–CEF Switching Support

The NAT–CEF Switching Support feature enhances router performance by optimizing packet processing. Through Cisco Express Forwarding (CEF), decisions to translate, punt, drop, or forward a packet are made with a single lookup. To improve performance, packets that do not require translation and fragmented packets are not punted to the process level. Those packets that have special flags, such as TCP syn/fin/reset, are processed in the CEF path itself. Any action that is CPU-intensive is performed by a background process or by process-level NAT code.

NAT Routemaps Outside-to-Inside Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtnato2n.html

NAT RTSP Support Using NBAR

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtnrtsp.html

NAT—SIP Support

Session Initiation Protocol (SIP) is an application-layer signaling protocol for creating and controlling multimedia sessions with two or more participants and a client/server protocol transported over TCP or UDP. The messages in the protocol might have IP addresses embedded in the packet payload. If a message passes through a router configured with NAT, the embedded information is translated and encoded back to the packet.

No configurations changes are needed for this feature. However, the SIP proxy server or user agent may sometimes listen to SIP messages in the nonstandard ports. The following global configuration command is used to change the configuration:

ip nat service sip tcp port *number*

The *number* argument is the port number on which the SIP proxy server will listen for SIP messages.

NAT Stateful Failover for Application Layer Gateway (ALG) Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtsnatay.html

NAT Stateful Failover for Asymmetric Outside-to-Inside Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtsnatay.html

NAT—Static IP

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/gt_ntsip.html

NAT Support for H.323 Fragmented Control Messages

Control messages for most multimedia applications such as H.323 messages can arrive at a router as fragments. IP-level fragmentation is common and well understood, but some applications have control messages that can span across several IP datagrams, causing the control message of an application that uses TCP to arrive at a router running Network Address Translation (NAT) as multiple IP packets that are not fragmented.

Prior to the introduction of the NAT Support for H.323 Fragmented Control Messages feature, NAT required the entire control message to be present in a single IP packet. If NAT received a control message that was fragmented, the packet was dropped. This feature enables NAT to perform address translation against fragmented packets, and it provides support for H.323 packets that arrive in different TCP segments.

NAT—Support for H.323 v3 and v4 in v2 Compatibility Mode

H.323 is an ITU-T specification for transmitting audio, video, and data across a packet network. Four versions of the H.323 protocols are currently in use: v1, v2, v3, and v4. The NAT—Support for H.323 v3 and v4 in v2 Compatibility Mode feature enables Cisco Network Address Translation (NAT) routers

to support messages coded in H.323 v3 and v4 when those messages contain fields compatible with H.323 v2. This feature does not add support for H.323 capabilities introduced in v3 and v4, such as new message types or new fields that require address translation.

NAT—Support of IP Phone to Cisco CallManager

Cisco IP phones use the Selsius Skinny Station Protocol to connect with and register to the Cisco CallManager. Messages flow back and forth that include IP address and port information used to identify other IP phone users with which a call can be placed.

To deploy Cisco IOS Network Address Translation (NAT) between the IP phone and the Cisco CallManager in a scalable environment, NAT needs to be able to detect the Selsius Skinny Station Protocol and understand the information passed within the messages.

When an IP phone attempts to connect to the Cisco CallManager and it matches the configured NAT translation rules, NAT will translate the original source IP address and replace it with one from the configured pool. This new address will be reflected in the Cisco CallManager and be visible to other IP phone users.

NAT listens on the default port of the Cisco CallManager to translate the Skinny messages. If the call manager uses a port other than the default port, that port needs to be configured, using the **ip nat service skinny tcp port** global configuration command. To disable the port, use the **no** form of this command. The syntax of this command is shown below:

ip nat service skinny tcp port *number*

no ip nat service skinny tcp port *number*

NAT Virtual Interface (NVI)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtnatvi.html

NBAR Multiple Applications per Port Capability

For detailed information about this feature, see the *Network-Based Application Recognition and Distributed Network-Based Application Recognition* document:

http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsnbarad.html

NetFlow

Cisco IOS Release 12.3(11)T supports NetFlow on the Cisco 3200 series mobile access routers.

NetFlow Egress Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/nflowegr.html

NetFlow Layer 2 and Security Monitoring Exports

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/nflwsec1.html

NetFlow MIB

This release adds MIB support to NetFlow. NetFlow cache information, current NetFlow configuration, and statistics can now be monitored using the Simple Network Management Protocol (SNMP).

For more information about CISCO-NETFLOW-MIB, the MIB objects for the functionality described above, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

NetFlow Top Talkers

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/cfg_nflow_top_talk.html

Network Admission Control

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_nac.html

Network-based Application Recognition (NBAR)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsnbarad.html

New Features in Cisco CallManager

For detailed information about this feature, see the following documents:

www.cisco.com/en/US/products/sw/voicesw/ps556/index.html

New Voice Features

Cisco IOS 12.3(4) T supports the following new voice features:

- Accounting Server Connectivity Failure and Recovery Detection
- Cisco CallManager Express 3.0
- Cisco IOS MGCP Gateway Support for Cisco CallManager Network Specific Facilities
- Cisco Survivable Site Remote Telephony, V3.0
- Customizable Tone Download to Cisco IOS MGCP Gateways from Cisco Call Manager
- Default Session Application Enhancements
- DES/3DES/AES VPN Encryption Module (AIM-VPN/BPII)

- DPNSS Backhaul
- Enhanced ITU-T G.168 Echo Cancellation
- H.323v4 Gateway Zone Prefix Registration Enhancements
- Inactive Call Detection
- ISDN Calling Name Display for SIP
- Media Inactive Timer
- NextPort Voice Tuning and Background Noise Statistics
- PLAR (Private Line Automatic Ring-down) for Trading Turrets
- SIP 300 Multiple Choice Messages
- SIP Gateway Support Enhancements to the bind Command
- SIP Debug Output Filtering Support
- SIP Header Support and SUBSCRIBE and NOTIFY for External Triggers
- SIP NOTIFY-Based Out-of-Band DTMF Relay Support
- SIP Redirect Processing
- SIP Register Support
- SIP RFC 3261 Enhancements
- SIP Survivable Remote Site Telephony (SRST)
- VIC2-2FXS, VIC2-2E/M, VIC2-2FXO, VIC2-4FXO, VIC2-2CAMA, VIC2-2BRI-NT/TE
- Videoconferencing for the Cisco Multiservice IP-to-IP Gateway Feature
- Voice Application Enhancements, Phase 4a
- Voice DSP Crash Dump Analysis
- Voice Performance Statistics on Cisco Gateways
- VoIP Debug Filtering
- VoIP Internal Error Codes

NextPort Voice Tuning and Background Noise Statistics with NextPort Dual-Filter G.168 Echo Cancellation

This feature allows you to dynamically configure voice services on the NextPort-based platforms: the Cisco AS5350, Cisco AS5400, Cisco AS5400HPX, and Cisco AS5850. This feature also provides improved voice quality and statistics reporting and adds dual-filter G.168 echo canceller capability in NextPort SPE firmware (SPEware) version 10.2.2 and later with Cisco IOS Release 12.3(11)T.

Dual-filter G.168 echo canceller capability has been added to the CSMV6 dial feature card (DFC) for NextPort platforms. The NextPort dual-filter G.168 echo canceller (EC) improves voice quality in VoIP connections by providing relatively less residual echo leakage, better non-linear processing (NLP) timing, less clipping, and better comfort noise generation (CNG) in most environments.

The dual-filter G.168 echo canceller features two concurrently operating adaptive filters (which control echo tail coverage) and two double-talk detection functions. In addition, the comfort noise model uses “Hoth noise” spectrum shaping to better replicate the true noise spectrum.

The NextPort dual-filter G.168 echo canceller uses the same voice-tuning (VCtune) interface for configuring voicecap parameters as the Cisco-proprietary G.164 echo canceller. Adjusting the dual-filter echo canceller is carried out by using a voicecap or by using the Cisco IOS command-line interface (CLI) during configuration.

For more information, see the *NextPort Voice Tuning and Background Noise Statistics with NextPort Dual-Filter G.168 Echo Cancellation* document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtvctune.html

No Service Password-Recovery

The No Service Password-Recovery feature was introduced in Cisco IOS Release 12.3(8)YA. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3y/12_3ya8/gtnsvpwd.html

OER Policy-Rules Configuration and Port-Based Prefix Learning

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gt_oer2.html

OER Support for Cost-Based Optimization and Traceroute Reporting

The OER Support for Cost-Based Optimization and Traceroute Reporting feature provides outbound traffic optimization based on financial link cost (i.e., fixed cost versus tier based cost). This feature also adds support for traceroute reporting.

Online Certificate Status Protocol (OCSP)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_ocsp.html

Optimized Edge Routing (OER)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_oer1.html

Option to Disable Hardware Crypto Engine Failover to Software Crypto Engine

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_dhcef.html

OSPF Area Transit Capability

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospfatc.html

OSPF Incremental SPF

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospfispf.html

OSPF Limit on Number of Redistributed Routes

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsoredis.html

OSPF Link-State Advertisement (LSA) Throttling

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsolsath.html

OSPF Link State Database Overload Protection

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospfopro.html

OSPF MIB Support of RFC 1850 and Latest Extensions

This release updates the OSPF MIB support to the latest RFC 1850 and adds the latest draft extensions. For more information regarding the definitions of the draft extensions, see the CISCO-OSPF-MIB.my and CISCO-OSPF-TRAP-MIB.my files that are available through the Cisco MIB FTP site at the following URL:

ftp://ftp.cisco.com/pub/mibs/v2/

For routers that are running Cisco IOS Release 12.0(26)S and later releases, the OSPF MIB and CISCO OSPF MIB will be supported only for the first OSPF process (except for MIB objects that are related to virtual links and sham links). SNMP Traps will be generated for OSPF events that are related to any of the OSPF processes. There is no workaround for this situation.

Note The CISCO-OSPF-MIB.my is a read-only MIB.

OSPF per-Interface Link-Local Signaling

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospflls.html

OSPF Sham-Link MIB Support

The OSPF Sham-Link MIB Support feature was introduced in Cisco IOS Release 12.0(30)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospfslms.html

OSPF Sham-Link Support for MPLS VPN

For more information about the OSPF Sham-Link Support for MPLS VPN feature, see the documentation at the following URL:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ospfshmk.html

OSPF Support for Unlimited Software VRFs per Provider Edge (PE) Router

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtospfvf.html

Outbound Control Packet Decoding Implemented for VPDN Debug Output Using the L2TP Protocol

Before Cisco IOS Release 12.3(14)T, only incoming Layer 2 Transport Protocol (L2TP control packets were decoded and displayed in the output of virtual private dialup network (VPDN) **debug** command data with the **debug vpdn l2x-packets** EXEC command enabled. To create L2TP tunnels and sessions, the software sends control packets to the peer. If you had wanted to troubleshoot the sessions effectively during the control-channel establishment phase of those sessions, it was necessary to review debug data from both outgoing and incoming control packets, on both the LAC and LNS. Also, for outgoing L2TP control packets, the hexadecimal packet dump was displayed on the screen only, which made it difficult to troubleshoot interoperability issues that required packet analyzers, or to use data from peer or vendor devices to analyze the outgoing L2TP control packets.

To be consistent with other protocol-level debug output in the Cisco IOS software, L2TP control packet **debug** command output needed to show bidirectional protocol packet decode data, rather than just the incoming only data that had been displayed.

Cisco IOS Release 12.3(14)T implements the decoding of outgoing L2TP hexadecimal control messages, which includes the L2TP headers and the attribute-value pairs that are transacted in each outgoing control message. VPDN debug data can also be directed into a file so that packet analyzers can be used on the data.

To use this feature, you must enable the **debug vpdn l2x-packets** command on the router in which the decoded outgoing control packets debug data needs to be shown.

Note The **debug vpdn l2x-packets** command can result in a large number of debug messages and should be used only on a debug chassis with a single active session.

Following is sample decoded debug output, followed by a list of the attribute-value pairs that are supported in the enhanced **debug** command output:

```
Router#
3d22h: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
3d22h:  Tnl 29029 L2TP: O SCCRQ
3d22h:  Tnl 29029 L2TP: Parse AVP 0, len 8, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Parse SCCRQ
3d22h:  Tnl 29029 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Protocol Ver 256
3d22h:  Tnl 29029 L2TP: Parse  AVP 6, len 8, flag 0x0
3d22h:  Tnl 29029 L2TP: Firmware Ver 0x1130
3d22h:  Tnl 29029 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Hostname LAC-tunnel
3d22h:  Tnl 29029 L2TP: Parse  AVP 8, len 25, flag 0x0
3d22h:  Tnl 29029 L2TP: Vendor Name Cisco Systems, Inc.
3d22h:  Tnl 29029 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
```

```
3d22h:  Tnl 29029 L2TP: Rx Window Size 20050
3d22h:  Tnl 29029 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Chlng
         B1 E9 3B 84 72 66 19 B1 C5 46 8F E7 31 A8 3B BC
3d22h:  Tnl 29029 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Assigned Tunnel ID 29029
3d22h:  Tnl 29029 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Framing Cap 0x0
3d22h:  Tnl 29029 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Bearer Cap 0x0
3d22h:  Tnl 29029 L2TP: Parse Cisco AVP 110, len 6, flag 0x0
3d22h:  Tnl 29029 L2TP: PPPoE Relay Forward Capable
3d22h:  Tnl 29029 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0, ns 0, nr 0
         C8 02 00 8D 00 00 00 00 00 00 00 80 08 00 00
         C8 02 00 8D 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
         6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
         53 79 73 74 65 6D 73 ...
3d22h:  Tnl 29029 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Parse SCCRP
3d22h:  Tnl 29029 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Protocol Ver 256
3d22h:  Tnl 29029 L2TP: Parse  AVP 6, len 8, flag 0x0
3d22h:  Tnl 29029 L2TP: Firmware Ver 0x1120
3d22h:  Tnl 29029 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Hostname LNS-tunnel
3d22h:  Tnl 29029 L2TP: Parse  AVP 8, len 25, flag 0x0
3d22h:  Tnl 29029 L2TP: Vendor Name Cisco Systems, Inc.
3d22h:  Tnl 29029 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Rx Window Size 20050
3d22h:  Tnl 29029 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Chlng
         7F 8B 30 8C 1D CD 44 49 CA 71 C3 6F 45 C2 89 B1
3d22h:  Tnl 29029 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Chlng Resp
         C3 A8 1B 39 6B 42 82 A5 AC A1 11 36 94 97 A2 1D
3d22h:  Tnl 29029 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Assigned Tunnel ID 18566
3d22h:  Tnl 29029 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Framing Cap 0x0
3d22h:  Tnl 29029 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Bearer Cap 0x0
3d22h:  Tnl 29029 L2TP: Parse Cisco AVP 110, len 6, flag 0x0
3d22h:  Tnl 29029 L2TP: PPPoE Relay Forward Capable
3d22h:  Tnl 29029 L2TP: No missing AVPs in SCCRP
3d22h:  Tnl 29029 L2TP: I SCCRP, flg TLS, ver 2, len 163, tnl 29029, ns 0, nr 1
contiguous pak, size 163
         C8 02 00 A3 71 65 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 20 80 10 00 00 00 07 4C 4E 53 2D 74 75
         6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
         53 79 73 74 65 6D 73 2C ...
3d22h:  Tnl 29029 L2TP: I SCCRP from LNS-tunnel
3d22h:  Tnl 29029 L2TP: O SCCCN  to LNS-tunnel tnlid 18566
3d22h:  Tnl 29029 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Parse SCCCN
3d22h:  Tnl 29029 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
3d22h:  Tnl 29029 L2TP: Chlng Resp
         3B 74 77 E8 DD 30 64 48 C2 63 42 D5 37 C3 B9 F2
3d22h:  Tnl 29029 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl 18566, ns 1, nr 1
         C8 02 00 2A 48 86 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 3B 74 77 E8 DD 30
         64 48 C2 63 42 D5 37 C3 B9 F2
```

```
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: O ICRQ to LNS-tunnel 18566/0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse ICRQ
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 15, len 10, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Serial Number 1563200007
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 14, len 8, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Assigned Call ID 61
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 18, len 10, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Bearer Type 2
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse Cisco AVP 100, len 15, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Client NAS Port
         53 65 72 69 61 6C 33 2F 30
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: O ICRQ, flg TLS, ver 2, len 63, tnl 18566,
lsid 61, rsid 0, ns 2, nr 1
         C8 02 00 3F 48 86 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 0A 00 00 00 0F 5D 2C 8A 07 80 08
         00 00 00 0E 00 3D 80 0A 00 00 00 12 00 00 00 02
         00 0F 00 09 00 64 53 65 72 69 61 6C 33 2F 30
3d22h:  Tnl 29029 L2TP: I ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 29029, ns
1, nr 2
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse ICRP
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 14, len 8, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Assigned Call ID 9
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: No missing AVPs in ICRP
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: I ICRP, flg TLS, ver 2, len 28, tnl 29029,
lsid 61, rsid 0, ns 1, nr 3
contiguous pak, size 28
         C8 02 00 1C 71 65 00 3D 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 09
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: O ICCN to LNS-tunnel 18566/9
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse ICCN
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 24, len 10, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Connect Speed 1544000
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 19, len 10, flag 0x8000 (M)
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Framing Type 1
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 27, len 17, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Last Sent LCPREQ
         03 05 C2 23 05 05 06 1D 9C 69 09
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 28, len 12, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Last Rx LCPREQ
         05 06 1F 19 E3 07
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 31, len 22, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Proxy Auth Chal
         FF 0D CB C7 E4 07 74 9F 43 0C 82 B5 17 69 4D 9E
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 32, len 8, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Proxy Auth ID 60
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 30, len 22, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Proxy Auth Name client@cisco.com
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 33, len 22, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Proxy Auth Resp
         80 45 E2 C5 A7 D0 8C C1 0F 0A 14 F8 9E F7 21 F3
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Parse  AVP 29, len 8, flag 0x0
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: Proxy Auth Type 2
3d22h: Se3/0 Tnl/Sn 29029/61 L2TP: O ICCN, flg TLS, ver 2, len 151, tnl 18566,
lsid 61, rsid 9, ns 3, nr 2
         C8 02 00 97 48 86 00 09 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 00 17 8F 40 80 0A
         00 00 00 13 00 00 00 01 00 11 00 00 00 1B 03 05
         C2 23 05 05 06 1D 9C 69 09 00 0C 00 00 00 1C 05
         06 1F 19 E3 07 00 16 ...
3d22h:  Tnl 29029 L2TP: I ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 29029, ns 2, nr 4
3d22h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up
```

List of Supported L2TP Attribute Values

- L2TP_VENDOR_IETF:
  - L2TP_AVP_RESULT_CODE
  - L2TP_AVP_PROTOCOL_VERSION
  - L2TP_AVP_FRAMING_CAP
  - L2TP_AVP_BEARER_CAP
  - L2TP_AVP_TIE_BREAKER
  - L2TP_AVP_FIRMWARE_REV
  - L2TP_AVP_HOST_NAME
  - L2TP_AVP_VENDOR_NAME
  - L2TP_AVP_ASSIGNED_TUNNEL_ID
  - L2TP_AVP_REC_WINDOW_SIZE
  - L2TP_AVP_CHALLENGE
  - L2TP_AVP_Q931_CAUSE_CODE
  - L2TP_AVP_CHALLENGE_RESPONSE
  - L2TP_AVP_ASSIGNED_SESSION_ID
  - L2TP_AVP_CALL_SERIAL_NUM
  - L2TP_AVP_MINIMUM_BPS
  - L2TP_AVP_MAXIMUM_BPS
  - L2TP_AVP_BEARER_TYPE
  - L2TP_AVP_FRAMING_TYPE
  - L2TP_AVP_CALLED_NUMBER
  - L2TP_AVP_CALLING_NUMBER
  - L2TP_AVP_SUB_ADDRESS
  - L2TP_AVP_TX_CONNECT_SPEED
  - L2TP_AVP_PHYSICAL_CHANNEL_ID
  - L2TP_AVP_INITIAL_LCP_CONFREQ
  - L2TP_AVP_LAST_SENT_LCP_CONFREQ
  - L2TP_AVP_LAST_RECV_LCP_CONFREQ
  - L2TP_AVP_PROXY_AUTHEN_TYPE
  - L2TP_AVP_PROXY_AUTHEN_NAME
  - L2TP_AVP_PROXY_AUTHEN_CHALLENGE
  - L2TP_AVP_PROXY_AUTHEN_ID
  - L2TP_AVP_PROXY_AUTHEN_RESPONSE
  - L2TP_AVP_CIRCUIT_ERRORS
  - L2TP_AVP_ACCM
  - L2TP_AVP_RANDOM_VECTOR
  - L2TP_AVP_PRIVATE_GROUP_ID

  - L2TP_AVP_RX_CONNECT_SPEED
  - L2TP_AVP_SEQUENCING_REQUIRED
  - L2TP_AVP_IETF_PPP_DISC_CAUSE
- SMI_CISCO_ENTERPRISE_CODE:
  - L2TP_AVP_ASSIGNED_CC_ID
  - L2TP_AVP_PW_CAP_LIST
  - L2TP_AVP_LOCAL_SESSION_ID
  - L2TP_AVP_REMOTE_SESSION_ID
  - L2TP_AVP_ASSIGNED_COOKIE
  - L2TP_AVP_END_IDENTIFIER
  - L2TP_AVP_PW_TYPE
  - L2TP_AVP_CIRCUIT_STATUS
  - L2TP_AVP_SESSION_TIE_BREAKER
  - L2TP_AVP_CISCO_DRAFT_AVP_VERSION
  - L2TP_AVP_CLIENT_NAS_PORT
  - L2TP_AVP_HOPCOUNT
  - L2TP_AVP_USERNAME
  - L2TP_AVP_ORIG_NAS_IP_ADDR
  - L2TP_AVP_CISCO_PPP_DISC_CAUSE
  - L2TP_AVP_VENDOR_ERROR_CODE
  - L2TP_AVP_FIXED_CHALLENGE_ID
  - L2TP_AVP_FIXED_CHALLENGE
  - L2TP_AVP_REDIRECT_CAPABLE
  - L2TP_AVP_REDIRECT_ID
  - L2TP_AVP_PPPOE_RLYFWD_CAPABLE
  - L2TP_AVP_PPPOE_RLYRSP_CAPABLE
  - L2TP_AVP_PPPOE_PAD
- SMI_REDBACK_ENTERPRISE_CODE
  - L2TP_AVP_NAS_PORT_TYPE_LIST

Out-of-Band to In-Band DTMF Relay for Cisco IOS Voice Gateways

This feature provides RFC 2833 capability, enabling DTMF relay communication between SIP devices and non-SIP endpoints using Cisco CallManager 4.0.

For detailed information about this feature, see the Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers chapter in the *Cisco CallManager and Cisco IOS Interoperability Guide*:

http://www.cisco.com/en/US/docs/ios/voice/cminterop/configuration/guide/vc_enh_confr_vgr.html

Overlap Signaling Processing on H.323 Terminating Gateways

In an overlap signaling scenario, the called number in the SETUP message does not contain enough digits to match the incoming dial peer for the dial peer to select the right application. With this change, the H.323 layer determines if a partial match is detected and appends the called number with the needed digits. The new called number is checked to see if it matches any of the incoming dial peers. If either full match or no match is returned, the call will proceed with a SETUP procedure.

For detailed information about this feature, see the *Cisco Multiservice IP-to-IP Gateway Application Guide*:

http://www.cisco.com/en/US/docs/ios/12_3/multiservice_ip2ip/guide/ipipgw_2.html

PAD Subaddress Formatting Option

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtpadsfo.html

PA-POS-1OC3: 1-port Packet over SONET OC3c/STM1 Port Adapter

The 1-port Packet over SONET OC3c/STM1 Port Adapter feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 7200 FlexWAN systems.
- Cisco 7300 FlexWAN systems.
- Cisco 7400 FlexWAN systems.
- Cisco 7500 FlexWAN systems.
- Cisco 7600 FlexWAN systems.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/interfaces_modules/port_adapters/install_upgrade/multichannel_serial/pa-pos-1oc3_install_config/6514_1oc.html

PCR Support for the Cisco Signaling Link Terminal

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/ftsltpcr.html

Per Interface mroute State Limit

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtmrtlim.html

Per-VRF AAA

The Per-VRF AAA feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers

- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

Per VRF for TACACS+ Servers

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_pvt.html

Periodic MIB Data Collection and Transfer Mechanism

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gdatacol.html

Persistent Self-Signed Certificates

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtpsscer.html

Persistent TDM Switched Circuits

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gttdmsw.html

PKI AAA Authorization Using the Entire Subject Name

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gt_dnall.html

PKI: Query Multiple Servers During Certificate Revocation Check

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtcertrc.html

PKI Status

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtpkista.html

Policy Based Routing: Recursive Next Hop

The Policy Based Routing: Recursive Next Hop feature was introduced in Cisco IOS Release 12.0(28)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12s_pbr.html

Port Translation for Windows Clients and Cisco IOS LNS Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/pt_wnlns.html

PPP/MLP MRRU Negotiation Configuration

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtmpmrru.html

PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtvlansc.html

PPPoE Session Recovery After Reload

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtppprec.html

Protected Private Key Storage

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_ppkey.html

Protocol Translation Aggregation

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_ptagg.html

QoS Bandwidth Estimation

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtcbandw.html

QoS: Classification, Policing, and Marking on LAC

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtqoslac.html

QSIG Supplementary Features for Cisco IOS Voice Gateways

This feature supports Q Signaling (QSIG) over PRI backhaul interfaces on MGCP gateways to Cisco CallManager 4.0.

For detailed information about this feature, see the Configuring MGCP PRI Backhaul and T1 CAS Support for Cisco CallManager chapter in the *Cisco CallManager and Cisco IOS Interoperability Guide*:

http://www.cisco.com/en/US/docs/ios/voice/cminterop/configuration/guide/vc_mgcp_t1cas.html

Quality of Service for Virtual Private Networks

This feature allows the customer to configure Quality of Service (QoS) features and tunneling/crypto on the same interface.

As VPNs grow to include data, voice, and video traffic, the different types of traffic need to be handled differently in the network. QoS and bandwidth management features allow a VPN to deliver high transmission quality for time-sensitive applications such as voice and video. Each packet is tagged to identify the priority and time sensitivity of its payload, and traffic is sorted and routed based on its delivery priority. Cisco VPN solutions support a wide range of QoS features.

For more details on this feature, see the following URL:

http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800b3d15.shtml

Query Mode Definition Per Trustpoint

Certificates and certificate revocation lists (CRLs) are used by your router when a CA is used. Normally certain certificates and all CRLs are stored locally in the router's NVRAM, and each certificate and CRL uses a moderate amount of memory. The Query Mode Definition Per Trustpoint allow you to define a query for a specific trustpoint or for the trustpoints defined on a particular router.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_qerym.html

Quick Autoenroll

The Autoenroll feature enables a router to automatically trigger an enrollment when the elapsed lifetime of an existing certificate has reached a certain percentage (for example, after 70 percent of the lifetime has passed, the router automatically enrolls for a new certificate). When no certificate exists, a 1-minute timer is set to trigger autoenrollment as soon as the clock has been set manually or by using Network Time Protocol (NTP).

The Quick Autoenroll feature shortens the 1-minute time when no certificate exists. Instead of having to wait 1 minute, an enrollment will occur after 15 seconds. This feature applies to manually configured autoenroll using the current **auto-enroll** command. No new or additional commands or keywords are necessary for this feature to work. This feature also applies when the configuration sent to the device

includes autoenroll (that is, to any subsystem that calls for the “parse_configure() with RES_MANUAL” flag to enter the **auto-enroll** command, for example, during a Trusted Transitive Introduction [TTI] exchange).

When the configuration is read from NVRAM or copied from file systems, autoenroll will still have a 1-minute timer. The 1-minute timer prevents the read-in of multiple trustpoints from configuration and trigger enrollments that occur simultaneously.

RADIUS Attribute 104

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_ra104.html

RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/ra5f.html

RADIUS NAS-IP-Address Configurability

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3b/feature/guide/gt_siara.html

Random Sampled NetFlow

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/nfstatsa.html

Rate Based Satellite Control Protocol

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_rbscp.html

Rate Limiting NAT Translation

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_natrl.html

RAW IP Traffic Export

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_rawip.html

Real-time Resolution for IPSec Tunnel Peer

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrlres.html

Re-enroll Using Existing Certificate

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_enroll_pki.html

Regex Engine Performance Enhancement

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_rexpe.html

Reliable Static Routing Backup Using Object Tracking

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xe/feature/guide/dbackupx.html

Reverse Route Injection

The Reverse Route Injection feature was introduced in Cisco IOS Release 12.1(9)E. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_rrie.html

Reverse SSH Enhancements

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gt_rssh.html

RFC 2867—RADIUS Tunnel Accounting

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2/12_2b/12_2b8/feature/guide/ft_tnact.html

Role-Based CLI Access

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.html

Route Processor Redundancy Plus (RPR+)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_rpr2.html

RSVP Refresh Reduction and Reliable Messaging

The RSVP Refresh Reduction and Reliable Messaging feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

RTP Header Compression over Satellite Links

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/ftcrtprf.html

SAA Support for Frame Relay, VoIP, and MPLS VPN Monitoring

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t2/feature/guide/ft1csaa.html

SafeNet IPSec VPN Client Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_scse.html

SEAL Encryption

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_se.html

Second-Generation 1- and 2-Port T1/E1 Multiflex Trunk Voice/WAN Interface Cards

The Second-Generation 1- and 2-Port T1/E1 Multiflex Trunk Voice/WAN Interface Cards feature enables T1/E1 multiflex voice/WAN interface cards to support enhanced voice and data applications in Cisco multiservice routers. This feature provides the following:

- Flexible T1 and E1 support.
- Drop-and-insert multiplexing capability on all versions.
- Support for a dedicated hardware echo-cancellation module.
- On 2-port cards, capability for each port to be clocked from an independent clock source.

This feature was introduced in Cisco IOS Release 12.3(13)T. For more information, see the Configuring Hardware Echo Cancellation chapter in the *Voice Port Configuration Guide*. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the *Second-Generation 1- and 2-Port T1/E1 Multiflex Trunk Voice/WAN Interface Cards* document:

http://www.cisco.com/en/US/docs/ios/12_2/12_2z/12_2zj/feature/guide/gthwecan.html

Secure Device Provisioning Certificate-Based Authorization

The Secure Device Provisioning (SDP) Certificate-Based Authorization feature allows certificates issued by other authority (CA) servers to be used for SDP introductions. For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtcbauth.html

Secure Shell Version 2 Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ssh2.html

Secure SNMP Views

The USM, VACM and Community MIBs have information that can potentially be used to gain access to the router using SNMP. Therefore, the USM, VACM, and Community MIBs are excluded from the default SNMP access view so as not to allow remote access unless specifically configured. However, when an SNMP view is created with any parent object identifier (OID) of these MIBs included (for example “internet included”), these MIBs also get included in the view. To increase security, the Secure SNMP Views enhancement excludes these MIBs from SNMP access views even when parent OIDs are included in the view. Prior to this release, when configuring SNMP views with parent OIDs that include the USM, VACM, or Community OIDs, the user was required to explicitly exclude them. For example, the following configuration can be used for excluding security-sensitive MIBs from the SNMP view named “test”:

! – include all MIBs under the parent tree “internet” snmp-server view test internet included

! -- exclude snmpUsmMIB snmp-server view test 1.3.6.1.6.3.15 excluded

! -- exclude snmpVacmMIB snmp-server view test 1.3.6.1.6.3.16 excluded

! -- exclude snmpCommunityMIB snmp-server view test 1.3.6.1.6.3.18 excluded

Beginning in Cisco IOS Releases 12.0(26)S and 12.2(2)T, the USM, VACM, and Community MIBs are excluded from any parent OIDs in a configured view by default. If you wish to include these MIBs in a view, you must now explicitly include them.

Selective Enabling of Applications Using an HTTP or Secure HTTP Server

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_httpe.html

Service Assurance Agent (SAA)—MPLS VPN Path Jitter

The Service Assurance Agent (SAA)—MPLS VPN Path Jitter feature supports the use of the ICMP Path Jitter probe operation in an MPLS/VPN environment. ICMP Path Echo operations record statistics for each hop along the path that the operation takes to reach it destination. The ICMP Path Echo operation computes this hop-by-hop response time between a Cisco router and any IP device on the network by discovering the path using traceroute. ICMP Path Jitter uses multiple ICMP packets to determine jitter and packet loss on a hop-by-hop basis.

This feature allows you to specify a Virtual Private Network (VPN) forwarding table for a Path Echo operation using the **vrfName** command in SAA PathJitter configuration mode. The ICMP Path Jitter operation records statistics for each hop along the path to the destination.

Service Assurance Agent (SAA) Multiple Operation Scheduling

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_saams.html

Service Assurance Agency (SAA) VoIP UDP Operation

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtsaamos.html

Service Selection Gateway (SSG)

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as digital subscriber lines (DSL), cable modems, or wireless to allow simultaneous access to network services. The Service Selection Gateway MIB enables network administrators to use Simple Network Management Protocol (SNMP) to monitor and manage SSG. The SSG MIB contains objects that correspond to and allow the monitoring of several important SSG features, including SSG AutoDomain, SSG Port-Bundle Host Key, and SSG TCP Redirect for Services. For detailed definitions of MIB objects, see the CISCO-SSG-MIB.

Service Selection Gateway (SSG) Features in Release 12.3(4)T

For detailed information about this feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/ssg/index.htm

Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) is an ASCII-based, application-layer control protocol (defined in RFC 2543) that can be used to establish, maintain, and terminate calls between endpoints.

Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

This feature is supported on the Cisco 827-4V router beginning with this release. The SIP feature on Cisco 827-4V router supports only basic calls between two end points. Supplementary services like call waiting, call forwarding, etc. are not supported on the Cisco 827-4V router.

For more details on this feature, see the following URL:

http://www.cisco.com/en/US/tech/tk652/tk701/tk587/tsd_technology_support_sub-protocol_home.html

SHDSL—Auto Detection of 2 Wire Versus 4 Wire Line Mode

For detailed information about this feature, see the *ATM Mode for Two-Wire or Four-Wire SHDSL* document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt4wire.html

Show Command Section Filter

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtshfltr.html

Show Version Enhancements

The output of the commonly used **show version** command has been modified slightly to reflect general updates to Cisco IOS software. If you are currently using any automated tools (such as scripts) that parse the output of the **show version** command, you should review the new output format and make changes as needed.

For more information, see the following:

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_s4.html

Signal ISDN B-Channel ID to Enable Application Control of Voice Gateway Trunks

This feature enables call management applications to identify specific ISDN bearer (B) channels used during a voice gateway call for billing purposes. With the identification of the B channel, SIP and H.323 gateways can enable port-specific features such as voice recording and call transfer.

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-isdn_ps6350_TSD_Products_Configuration_Guide_Chapter.html

SIP Audible Message-Waiting Indicator for FXS Phones

For detailed information about this feature, see the "Configuring SIP MWI Support" chapter of the *Cisco IOS SIP Configuration Guide*.

SIP: Cisco IOS Gateway HTTP Digest Authentication and Registration

For detailed information about this feature, see the *Cisco IOS SIP Configuration Guide*.

SIP: Cisco IOS Gateway Reason Header and Buffered Calling Name Completion

For detailed information about this feature, see the *Cisco IOS SIP Configuration Guide*.

SIP Debug Output Filtering Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/voice_troubleshooting/old/vts_filt.html

SIP Gateway Support Enhancements to the bind Command

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/sip/configuration/guide/sipftgde.html

SIP Header Support and Subscribe and Notify for External Triggers

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/sip/configuration/guide/sipftgde.html

SIP: RFC 3261 Enhancements

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/sip/configuration/guide/sipftgde.html

Skip FA/HA-CHAP at Mobile IP Lifetime Renewals

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/wireless/home_agent/12.311t/feature_modules/spi_shared.html#wp1263745

SNA Switching Services Enterprise Extender for IP Version 6

SNA Switching Services (SNASw) announces hostname configuration support for Enterprise Extender (EE) connections. This allows SNASw EE links over an IP Version 6 backbone, and also enables Global Connection Network (also known as GVRN - Global Virtual Routing Node) to work when Network Address Translation (NAT) is in place between the connecting networks (IP Version 4 or IP Version 6). This feature adds an IPv6 keyword to the **snasw link** and **snasw port** commands.

For detailed information on configuring IPv6, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_c.html

For detailed information on configuring SNASw, see the following document:

http://www.cisco.com/en/US/docs/ios/bridging/configuration/guide/br_ctc.html

For detailed information on the **snasw link** and **snasw port** commands, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/ibm2/command/reference/ib2_s4gt.html

SNMP linkDown Trap Limiting

This enhancement provides for the correlation of linkDown traps based on layering. When a channelized interface goes down, in addition to the linkDown trap on the main channelized interface, there will be a flood of linkDown traps of all channel interfaces configured on the main channelized interface. A new command line interface (CLI) command, **snmp ifmib trap throttle**, limits the linkDown Simple Network Management Protocol (SNMP) notifications that are generated for a channel group.

SNMP over IPv6 Support

For detailed information about this feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_mgev6.htm

SNMP Support for Named Access Lists

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtsnmpal.html

SNMP Support over VPNs—Context Based Access Control

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtsnmpvp.html

SNMP v1/v2c PDU Conversions for Proxy Forwarder (RFC 2576)

The SNMP v1/v2c PDU Conversions for Proxy Forwarder feature brings all images and platforms that include the SNMP Proxy subsystem (sub_snmp_proxy.o) into partial compliance with RFC 2576. RFC 2576 defines coexistence between three versions of the Internet-standard Network Management Framework: SNMPv3, SNMPv2, and SNMPv1. The only exception to full compliance with RFC 2576 is that this release of Cisco IOS software does not yet support version translations for Simple Network Management Protocol (SNMP) notifications.

Source Specific Multicast (SSM) Mapping

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtssmma.html

SSG 3-Key Authentication

The SSG 3-Key Authentication feature enables Service Selection Gateway (SSG) to authenticate Cisco Subscriber Edge Services Manager (SESM) users on the basis of three keys: username, password, and mobile station integrated services digital network (MSISDN) number. Before the introduction of this feature, users logging into SESM were authenticated on the basis of username and password only (2-key authentication).

When SSG 3-key authentication is used, users are required to provide their MSISDN number (which is typically their phone number), in addition to username and password, at SESM login. RADIUS attribute 31 (calling-station ID) is used to communicate the MSISDN number in account logon requests sent from SESM to SSG and in access requests sent from SSG to a AAA server. When 3-key authentication is used, all host and connection accounting packets for the user contain the MSISDN number. SSG 3-key authentication is performed for account logon only, not for service logon; however, SSG will include the MSISDN number in the access requests for service logons.

SSG AAA Transaction Enhancements

The Service Selection Gateway (SSG) AAA transactions for host logon and service profile downloading have been enhanced. The AAA server can now handle multiple SSG host logon and service profile download requests concurrently without stopping SSG processes.

SSG Aware On-Demand IP Address Renewal

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/sgb_odip.html

SSG Complete ID

The SSG Complete ID feature provides enhancements to the interaction between Service Selection Gateway (SSG) and Cisco Subscriber Edge Services Manager (SESM) by allowing SSG to pass along the following information where available:

- Client IP address
- Client MAC address
- Subinterface
- Virtual path identifier/virtual channel identifier (VPI/VCI)
- Mobile station integrated services digital network (MSISDN) number

This feature provides a more flexible way of identifying a client, which can be a single user on a PC, a site managing many users, or a transit user at a wireless (WLAN) hot spot location. The SSG Complete ID feature also enables SESM to offer greater customization of Web portals, specifically by location; so, for example, each WLAN hot spot can have its own branded portal.

SSG Default DNS Redirection

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3b/feature/guide/gbdefdns.html

SSG Default Quota for Prepaid Billing Server Failure

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtssgdfq.html

SSG Enhancements to SSG-SESM Interaction and Service Logon

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3bw/feature/guide/ssg-enhn.html

SSG Interface Redundancy

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtssgifr.html

SSG MIB Extensions

The Service Selection Gateway MIB enables network administrators to use Simple Network Management Protocol (SNMP) to monitor and manage SSG. The SSG MIB contains objects that correspond to various SSG features and that allow the collection of statistics and management of certain SSG configurations.

In Cisco IOS Release 12.3(8)T, the SSG MIB has been enhanced to provide statistics and the ability to manage the configuration of the SSG Transparent Autologon feature. The SSG Transparent Autologon feature enables SSG to authenticate and authorize users based on IP packets received from users. SSG authorizes users based on the source IP address received on the downlink interface. The SSG MIB includes objects for reporting transparent autologon statistics such as the current number of transparent passthrough, suspect, waiting-for-authorization, and unidentified users. The MIB also includes read-write objects that allow certain SSG transparent autologon thresholds and values to be configured in the MIB in addition to configuration using the command-line interface.

For detailed definitions of the SSG MIB objects, see the CISCO-SSG-MIB. To locate and download MIBs, use Cisco MIB Locator found at the following URL:

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

SSG Open Garden Configuration Enhancements

A Service Selection Gateway open garden is a collection of websites or networks that subscribers can access as long as they have physical access to the network. Subscribers do not have to provide authentication information before accessing the websites in an open garden. Before the introduction of this feature, open garden services had to be configured in local service profiles. The SSG Open Garden Enhancements allows service profiles for open garden services to be defined and managed locally or remotely on the RADIUS server.

SSG Permanent TCP Redirection

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3b/feature/guide/gtTCPred.html

SSG Support for Dynamic Load Balancing

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtssgdfp.html

SSG Support for Overlapping Subscriber IP Addresses

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtssgovr.html

SSG Support for RADIUS Attributes 27 and 29

The SSG Support for Radius Attributes 27 and 29 feature introduces SSG compliance with RFC 3580 with respect to RADIUS attributes 27 (Session-Timeout) and 29 (Termination-Action). RFC 3580 recommends using attributes 27 and 29 in Access-Accept packets during authentication to enforce periodic reauthentication of users. For details, see RFC 3580, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines."

For instances that indicate reauthentication after the session timeout, SSG uses the cached username and password while performing reauthentication. If SSG does not have these credentials, the session is brought down as if reauthentication had failed. If a particular deployment makes use of one-time passwords for authenticating users, SSG reauthentication will fail and the session will be brought down.

For SSG transparent autologon (TAL) hosts (TAL users who have host objects created on SSG), SSG will perform TAL reauthorization upon session timeout whenever attribute 29 is present in the RADIUS profile of the user. (Note that for TAL users, SSG performs reauthorization, not reauthentication, because the user profile is downloaded on the basis of the IP address and service password.)

In SSG RADIUS proxy deployments, SSG will not perform session timeout processing when attribute 29 is present in the Access-Accept packet and is set to reauthenticate.

SSG Support for Subnet Based Authentication

The Subnet-Based Authentication for SSG feature allows a service provider to identify subscribers to services by their subnet, rather than by a subscriber's IP address.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/sgbsubnt.html

SSG TCP Redirect Access Control Lists

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3bw/feature/guide/tcprdrct.html

SSG Transparent Autologon

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3bw/feature/guide/autologn.html

SSM Channel (S,G) Based Filtering for Multicast Boundaries

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtmcbnd.html

Stateful Failover for IPSec

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gt_topht.html

Subordinate Certificate Server

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_scs.html

Subscriber Service Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtsubspt.html

Support for AAA Attributes MN-HA-SPI and MN-HA Shared Key

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/wireless/home_agent/12.311t/feature_modules/spi_shared.html

Survivable Remote Site Telephony 3.1

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs31spc.htm

Survivable Remote Site Telephony (SRST) 3.2

SRST adds a number of key telephony features:

- alias Command
- Call Pickup Ringing Extension
- COR List
- External Music on Hold Source
- Japanese Katakana Localization
- Number of Phones Supported on an Access Server
- Option to Disable H.225 TCP Timer from Phone to Gateway to Maintain Calls in Progress During WAN Outage
- RFC 2833 DTMF Support from SCCP Devices to Cisco Unity Express
- Translation Profiles Support (CME and SRST)

alias Command

The **alias** command is enhanced as follows:

- The **cfw** keyword is added, providing call forward no-answer/busy capabilities.
- The maximum number of **alias** commands that are used for creating calls to telephone numbers that are unavailable during Cisco CallManager fallback is increased from 10 to 50.
- The *alternate-number* argument can be used in multiple **alias** commands.

For detailed information about this feature, see the **alias** command in the *Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference*:

http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srsa_a_m.html

Call Pickup Ringing Extension

The **pickup** command is introduced to enable the PickUp soft key on all Cisco IP phones, allowing an external Direct Inward Dialing (DID) call coming into one extension to be picked up from another extension during SRST.

For detailed information about this feature, see the **pickup** command in the *Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference*:

http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srsa_n_z.html#wp1213470

COR List

The maximum number of class of restriction (COR) lists is increased from 10 to 20.

For detailed information about this feature, see the **cor** command in the *Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference*:

http://www.cisco.com/en/US/tech/tk652/tk90/technologies_configuration_example09186a008019d649.shtml

External Music on Hold Source

Cisco SRST has been enhanced with the **moh-live** command. The **moh-live** command provides live-feed MOH streams from an audio device connected to an E&M or FXO port to Cisco IP phones in SRST mode. Music from a live feed is from a fixed source and is continuously fed into the MOH playout buffer instead of being read from a flash file. Live-feed MOH can also be multicast to Cisco IP phones.

For detailed information about this feature, see the *Integrating Cisco CallManager and Cisco SRST to Use Cisco SRST as a Multicast MOH Resource* document:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00802d1c31.html

Japanese Katakana Localization

Japanese Katakana is now supported with the **JP** keyword and is available to Cisco SRST systems running under Cisco CallManager V4.0.

For detailed information about this feature, see the **user-locale** command in the *Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference*:

http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srsa_n_z.html#wp1267971

Number of Phones Supported on an Access Server

The number of phones that are supported on a Cisco 3845 is increased from 240 to 720 and up to 960 ephone-dns or virtual ports.

Option to Disable H.225 TCP Timer from Phone to Gateway to Maintain Calls in Progress During WAN Outage

To preserve existing H.323 calls on the branch in the event of an outage, disable the H.225 keepalive timer by entering the **no h225 timeout keepalive** command.

For detailed information about this feature, see the "Overview of Cisco IOS SRST" chapter in the *Cisco IOS Survivable Remote Site Telephony Version 3.2 System Administrator Guide*:

http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/srst/configuration/guide/srs_over.html

RFC 2833 DTMF Support from SCCP Devices to Cisco Unity Express

Cisco Skinny Client Control Protocol (SCCP) phones, such as those used with Cisco SRST systems, provide only out-of-band DTMF digit indications. To enable SCCP phones to send digit information to remote SIP-based IVR and voice-mail applications, Cisco SRST 3.2 and later versions provide conversion from the out-of-band SCCP digit indication to the SIP standard for DTMF relay, which is RFC 2833. You select this method in the SIP VoIP dial peer using the **dtmf-relay rtp-nte** command.

For detailed information about this feature, see the "Preparing Cisco SRST Support for SIP" chapter in the *Cisco IOS Survivable Remote Site Telephony Version 3.2 System Administrator Guide*:

http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/srst/configuration/guide/srstsa.html

Translation Profiles Support (CME and SRST)

Cisco SRST 3.2 supports translation profiles. Translation profiles allow you to group translation rules and to associate translation rules with the following:

- Called numbers
- Calling numbers
- Redirected called numbers

For detailed information about this feature, see the "Setting Up Call Handling" chapter in the *Cisco IOS Survivable Remote Site Telephony Version 3.2 System Administrator Guide*:

http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/srst/configuration/guide/srs_call.html

Also, see the **translation-profile** command in the Cisco IOS Voice Command Reference:

http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_t3.html#wp1651612

Survivable Remote Site Telephony (SRST) 3.3

Secure Cisco IP phones that are located at remote sites and that are attached to gateway routers can communicate securely using the WAN with Cisco CallManager. But if the WAN link or Cisco CallManager goes down, all communication through the remote phones becomes nonsecure. To overcome this situation, gateway routers can now function in secure SRST mode, which activates when the WAN link or Cisco CallManager goes down. When the WAN link or Cisco CallManager is restored, Cisco CallManager resumes secure call-handling capabilities.

Secure SRST provides new SRST security features such as authentication, integrity, and media encryption. Authentication provides assurance to one party that another party is whom it claims to be. Integrity provides assurance that the given data has not been altered between the entities. Encryption

implies confidentiality; that is, that no one can read the data except the intended recipient. These security features allow privacy for SRST voice calls and protect against voice security violations and identity theft.

For detailed information about this feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/voice/srst/srst33/srst33ad/index.htm

System Logging—EAL4 Certification Enhancements

Note Official EAL4 certification is not claimed by Cisco. This feature is part of current and planned enhancements which may qualify Cisco IOS Software for future certification.

This feature includes the following enhancements:

- The system logging process will now generate 'audit start' and 'audit stop; messages.
- The system logging process will now generate messages that include the date and time of an event, the type of event, the subject identity, and the outcome (success or failure) of an event.
- Changes to logging parameters will be logged.
- Further enhancements to minimize lost audit records.

T1/E1 Mode for SHDSL

The T1/E1 Mode for SHDSL feature was introduced in Cisco IOS Release 12.3(4)XD. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtgshdsl.html

T.37 Fax Status Notification Enhancement in an MTA Environment

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_fax_services_over_ip_application_guide/t37.html

T.38 Fax Relay on the Cisco Catalyst 6000 and Cisco 7600 Communication Media Module

The T.38 Fax Relay on the Cisco Catalyst 6000 and Cisco 7600 Communication Media Module feature provides support for T.38 fax relay on the Cisco Catalyst 6000 and Cisco 7600.

For detailed information about this feature, see the Configuring T.38 Fax Relay chapter in the *Cisco Fax Services over IP Application Guide*:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_fax_services_over_ip_application_guide/t38.html

T.38 Fax Statistics

The T.38 Fax Statistics feature enables access servers with NextPort digital signal processors to gather detailed statistics about T.38 fax-relay calls. Statistics can be compiled into detailed call-detail records for diagnostic and billing purposes.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/t38fxsta.html

TCP Congestion Avoidance

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gttcpca.html

TCP Explicit Congestion Notification

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gttcpecn.html

Token Ring Inter-Switch Link (TRISL)

As of Cisco IOS Release 12.3(2)T, the Token Ring Inter-Switch Link (TRISL) feature has been removed from Cisco IOS software.

Token Ring LAN Emulation (TR-LANE)

As of Cisco IOS Release 12.3(4)T, the Token Ring LAN Emulation (TR-LANE) feature has been removed from Cisco IOS software.

Transient Memory Management

Transient memory is that memory which is allocated and de-allocated within a short period of time. When these type of memory allocations are free and interleaved with 'static' memory allocations, it leads to memory fragmentation. This enhancement helps to minimize memory fragmentation issues. This enhancement is especially effective for devices in BGP networks. The feature is enabled by default: no user configuration is required. Detailed information on transient memory pools, if used on your device, can be viewed using the **show memory transient** command.

Transparent Cisco IOS Firewall

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_trans.html

Troubleshooting Enhancements for Multilink PPP over ATM Link Fragmentation and Interleaving

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gttrbmlp.html

Tunnel Authentication via RADIUS on Tunnel Terminator

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2/12_2b/12_2b8/feature/guide/ftunauth.html

Turbo-Classification for QoS

The Turbo-Classification for QoS feature provides support for using turbo access control lists (ACLs) when you configure quality of service (QoS) functionality. Turbo ACLs compile the ACLs into a set of lookup tables, while maintaining the first packet-matching requirements. Packet headers are used to access these tables in a small, fixed, number of lookups, independent of the existing number of ACL entries.

Turbo ACLs process ACLs more expediently, providing faster functionality for routers. For more information about turbo ACLs, see the *Turbo Access Lists* feature at the following URL:

http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dttacl.html

For information on access control lists, see the *Access Control Lists: Overview and Guidelines* document at the following URL:

http://www.cisco.com/en/US/docs/ios/11_3/security/configuration/guide/scacls.html

Two-Wire Mode over SHDSL

The Two-Wire Mode over SHDSL feature adds ATM, E1 and T1 support on a single port multiline G.SHDSL WIC, or WIC-1SHDSL-V2, to build on the existing features of the Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature supported on the 1-port G.SHDSL WAN interface card. Frame Mode TDM over G.SHDSL supports Cisco 2600XM series, Cisco 2691, and Cisco 3700 series routers and incorporates the latest firmware and the latest circuitry.

Two-Wire Mode over SHDSL supports ATM, E1 and T1 in two-wire mode. Embedded Operations Channel (EOC) message support for customer premise equipment (CPE) is provided for two-wire and four-wire modes. Some central office (CO) messages are also supported.

Upgrade Secondary ROMmon CLI

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12S28FUR.html

Upstream PPPoX Connection Speed Transfer at LAC

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtupppox.html

USB Storage

The USB Storage feature enables certain models of Cisco routers to support universal serial bus (USB) Flash modules and provide secure access to a router.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_etokn.html

Using Certificate ACLs to Ignore Revocation Check and Expired Certificates

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ircec.html

V.120 Support Network Access Server (NAS)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt120nas.html

Videoconferencing on the Cisco Multiservice IP-to-IP Gateway

For detailed information about this feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/ipipgw/index.htm

Virtual Auxiliary Port Feature and Configuration of DSL Settings

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/vauxdsl.html

Virtual Fragmentation Reassembly

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_vfrag.html

VLANs over IP Unnumbered Interfaces

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtunvlan.html

Voice Application Enhancements, Phase 4a

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/ivr/configuration/guide/tcl_c.html

Voice Application Monitoring and Troubleshooting Enhancements

For detailed information about this feature, see the "Monitoring and Troubleshooting Voice Applications" chapter in the *Cisco IOS TCL IVR and VoiceXML Application Guide*.

Voice Call Debug Filtering on Cisco Voice Gateways

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/voice_troubleshooting/old/voipt_c.html

Voice Performance Statistics on Cisco Gateways

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_th.html

VoiceXML Store and Forward

Voice extensible markup language (VXML) capability has been added to the Cisco 2691 router and Cisco 37xx series routers.

VoIP Alternate Path Fallback SNMP Trap

The VoIP Alternate Path Fallback SNMP Trap feature enhances support for the PSTN Fallback feature by providing the capability to generate Simple Network Management Protocol (SNMP) traps when the fallback subsystem redirects or rejects an H.323 VoIP call because a network condition fails to meet a configured threshold. See the Trunk-Management Features document for configuring information.

For detailed information about this feature, see theVoIP Alternate Path Fallback SNMP Trap document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/pstntrap.html

VPDN MIB Enhancements for per-VRF Session Counting

An extension has been added to the virtual private dialup network (VPDN) CISCO-VPDN-MGMT-MIB that returns the total number of active sessions for each VPDN template. For customers that associate a VPDN template to each VPN routing and forwarding (VRF) instance, this MIB extension provides a way to monitor session usage per VRF.

Service providers can terminate sessions from multiple customer accounts on the same L2TP network server (LNS). The sharing of the LNS is done by creating one VRF per customer. Session limits on VPDN templates and VPDN groups are configured to control the allocation of sessions among customers and among users within the same customer account. A VPDN template is associated with each VRF, and its session limit restricts the total number of sessions for a customer account. Within that account, users may be assigned to different VPDN groups as their access requirements dictate. Session limits on VPDN groups further control the allocation of customer sessions among its users. In such a setup, the service provider must use the Simple Network Management Protocol (SNMP) to retrieve the total number of active sessions per customer to monitor their usage on the LNS.

Prior to the introduction of this MIB enhancement, only the total number of sessions on the LNS across all customer accounts could be retrieved through SNMP. This enhancement extends the CISCO-VPDN-MGMT-MIB to include a read-only table of VPDN template entries, with each entry reporting the number of active sessions across all VPDN groups that are associated with that template. The table entries can be accessed individually using GET requests or consecutively using repeated GET-NEXT requests.

VPN Access Control Using 802.1X Authentication

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xa/gt_802_1.html

VRF and MQC Hierarchical Shaping in PXE

For detailed information about this feature, see the following document

http://www.cisco.com/en/US/docs/ios/12_2/12_2b/12_2b8/feature/guide/12b_pxf.html

VRF Aware Cisco IOS Firewall

VRF Aware Cisco IOS Firewall applies Cisco IOS Firewall functionality to VRF (Virtual Routing and Forwarding) interfaces when the firewall is configured on a service provider (SP) or large enterprise edge router.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_vrfaw.html

VRF Aware Dialer Watch

For detailed information about this feature, see the following:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtdwvrfa.html

VRF-Aware IPSec

The VRF-aware IPSec feature was integrated into the Cisco IOS Release 12.3(14)T and implemented on the following platforms:

- Cisco 2811 Series Integrated Services routers
- Cisco 2821 Series Integrated Services routers
- Cisco 2851 Series Integrated Services routers
- Cisco 3825 Series Integrated Services routers
- Cisco 3845 Series Integrated Services routers

VRF Aware MPLS Static Labels

The VRF-Aware MPLS Static Labels feature was introduced in Cisco IOS Release 12.0(23)S. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vrf_aware_static.html

VRF Aware Multicast Error Messages

Multicast error messages that are associated with a particular multicast VPN customer in an MPLS VPN environment can be tracked.

VRRP MIB—RFC 2787

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtvrrpmb.html

VRRP Object Tracking

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtvrrptk.html

VRRP—Virtual Router Redundancy Protocol

The Virtual Router Redundancy Protocol (VRRP) feature can solve the static configuration problem. VRRP enables a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.

VRRP is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, and on MPLS VPNs and VLANs.

For more details on this feature, see the following URL:

http://www.cisco.com/en/US/docs/ios/12_0st/12_0st18/feature/guide/st_vrrpx.html

VTMS

Versatile Traffic Management System (VTMS) on the RPM-XF allows bandwidth sharing between virtual channels (VCs). When a VC is idle, its bandwidth can be used by other VCs. It allows all VCs to share the same VTMS link and supports ATM and either Packet Over SONET (POS) or GigE links.

VTMS on the RPM-XF uses a bandwidth divisor of 65535, making it considerably more powerful than P5 VTMS which uses a bandwidth divisor of 255.

VTMS on the RPM-XF uses dummy full queues to handle traffic congestion and allows packet dropping, including undefined bit rate (UBR) packet dropping.

Warm Reload

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtwrmrbt.html

Warm Upgrade

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtwarmup.html

WCCP Enhancements

The WCCP Enhancements feature was introduced in Cisco IOS Release 12.3(7)T. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtwccpis.html

WCCP Version 2

This release adds support for version 2 of the Web Cache Communication Protocol (WCCP) for the Cisco 830 Series (Cisco 831, 836, and 837 Platforms). WCCP, developed by Cisco Systems, specifies interactions between one or more routers (or Layer 3 switches) and one or more web-caches. The purpose of the interaction is to establish and maintain the transparent redirection of selected types of traffic flowing through a group of routers. The selected traffic is redirected to a group of web-caches with the aim of optimizing resource usage and lowering response times. For information on configuring WCCP, see the following document:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf018.html

WebVPN

The Cisco WebVPN feature provides remote access to enterprise sites by users from anywhere on the Internet.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/g_sslvpn.html

X.25 Call Confirm Packet Address Control

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtx25adc.html

X.25 Data Display Trace

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtx25ddt.html

X.25 Station Type for ISDN D-Channel Interface

The X.25 Station Type for ISDN D-Channel Interface feature was introduced in Cisco IOS Release 12.3(7)XR. For detailed information about changes and enhancements to this feature in Cisco IOS Release 12.3(14)T, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3/12_3x/12_3xr/x25enc_d.html

X.25 Version Configuration

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtx25ver.html

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on 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. 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 by following the directions found at this URL:

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

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 16.

Table 16 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Limitations and Restrictions

The following sections contain limitations and restrictions that apply to Cisco IOS Release 12.4.

Cisco IOS IP SLAs Proactive Threshold Monitoring Limitation

It has been observed that when trying to configure proactive threshold monitoring for a Cisco IOS IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) echo operation, the **rtr reaction-configuration** *operation-number* **threshold-type consecutive** *consecutive-occurrences* command does not work. We recommend that you use the **ip sla monitor** *operation-number* command to reconfigure the ICMP echo operation and use the **ip sla monitor reaction-configuration** *operation-number* **threshold-type consecutive** *consecutive-occurrences* command to reconfigure proactive threshold monitoring.

SNMP Version 1 BGP4-MIB Limitations

You may notice incorrect BGP trap OID output when using the SNMP version 1 BGP4-MIB that is available for download at ftp://ftp.cisco.com/pub/mibs/v1/BGP4-MIB-V1SMI.my. When a router sends out BGP traps (notifications) about state changes on an SNMP version 1 monitored BGP peer, the enterprise OID is incorrectly displayed as .1.3.6.1.2.1.15 (bgp) instead of .1.3.6.1.2.1.15.7 (bgpTraps). The problem is not due to any error with Cisco IOS software. This problem occurs because the BGP4-MIB does not follow RFC 1908 rules regarding version 1 and version 2 trap compliance. This MIB is controlled by IANA under the guidance of the IETF, and work is currently in progress by the IETF to replace this MIB with a new version that represents the current state of the BGP protocol. In the meantime, we recommend that you use the SNMP version 2 BGP4-MIB or the CISCO-BGP4-MIB to avoid an incorrect trap OID.

Important Notes

The following information applies to all releases of Cisco IOS Release 12.4.

Important Notes for Cisco IOS Release 12.4(17)

The following information applies to Cisco IOS Release 12.4(17).

SNMP Trap Generation

Simple Network Management Protocol (SNMP) traps will be generated automatically when a Secure Shell (SSH) session terminates if the traps have been enabled and SNMP debugging has been turned on.

Important Notes for Cisco IOS Release 12.4(8)

The following information applies to Cisco IOS Release 12.4(8).

Japan ISR Profiled Release

Cisco IOS Release 12.4(8) is hardened by Japan Broadband WAN service emulated NSITE Next Generation Branch End-to-End System Test. Cisco IOS Release 12.4(8) and following 12.4 maintenance releases are classified as “Japan ISR Profiled Release.”

The release has integrated major software defects captured by the testing activities and the service requests reported to Japan TAC.

Important Notes for Cisco IOS Release 12.4

The following information applies to all releases of Cisco IOS Release 12.4.

CSCeg52210 for Cisco CME

Effective with Cisco IOS Releases 12.3(11)T7 and 12.4, the **mwi sip-server** command was replaced with the **mwi-server** command in SIP user-agent configuration mode and the **mwi reg-e164** command in telephony-service configuration mode.

For detailed information about this command, see the *Cisco Unified Communications Manager Express Command Reference* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_cr.html.

CSCeg52210 for Cisco SRST

Effective with Cisco IOS Releases 12.3(11)T7 and 12.4, the **mwi sip-server** command was replaced with the **mwi-server** command in SIP user-agent configuration mode and the **mwi reg-e164** command in call-manager-fallback configuration mode.

For detailed information about this command, see the *Cisco SRST and SIP SRST Command Reference* at http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html.

CSCei24868 for New Cisco IP Phones Supported with Cisco SRST

The following Cisco IP phones are now supported with Cisco Survivable Remote Site Telephony (SRST) systems:

- Cisco IP Phone 7941G and Cisco IP Phone 7941G-GE
- Cisco IP Phone 7961G and Cisco IP Phone 7961G-GE

No additional SRST configuration is required for these phones. The **show ephone** command has been enhanced to display the configuration and status of the new Cisco IP Phones.

CSCei36482 for Cisco ERM

Effective with Cisco IOS Release 12.4(5), output of the **show resource user iosprocess brief** command shows all resource owners (ROs) and their usage by resource user (RU) for all RUs.

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml

Field Notices and Software-Related Tools and Information

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. You can find Field Notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

Visit the Software Center/Download Software page on Cisco.com to subscribe to Cisco software notitications, locate MIBs, access the Software Advisor, and find other Cisco software-related information and tools. Access the Software Center/Download Software page at http://www.cisco.com/cisco/web/download/index.html, or by logging into Cisco.com and selecting **Support > Download Software**.

Caveats for Cisco IOS Release 12.4

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

For information on caveats in Cisco IOS Release 12.4, see the *Caveats for Cisco IOS Release 12.4* document, which lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.4 and is located on Cisco.com.

Note If you have an account on 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 **Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.4 > Troubleshooting > Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page*

  http://www.cisco.com/en/US/products/hw/routers/ps214/products_tech_note09186a008012fb88.shtml

- *Troubleshooting Bus Error Exceptions*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml

- *Why Does My Router Lose Its Configuration During Reboot?*

  http://www.cisco.com/en/US/products/hw/routers/ps233/products_tech_note09186a00800a65a5.shtml

- *Troubleshooting Router Hangs*

  http://www.cisco.com/en/US/products/hw/routers/ps359/products_tech_note09186a0080106fd7.shtml

- *Troubleshooting Memory Problems - SYS-2-MALLOCFAIL*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6f3a.shtml

- *Troubleshooting High CPU Utilization on Cisco Routers*

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a00800a70f2.shtml

- *Troubleshooting Router Crashes*

  http://www.cisco.com/en/US/products/hw/iad/ps397/products_tech_note09186a00800b4447.shtml

- *Using CAR During DOS Attacks*

  http://www.cisco.com/en/US/customer/products/sw/iosswrel/ps1835/products_tech_note09186a00800fb50a.shtml