



# Release Notes for the Cisco 1841 Series and 2801 Series Routers for Cisco IOS Release 12.3(14)YT

---

August 8, 2007  
Cisco IOS Release 12.3(14)YT1  
OL-8340-2 Second Release

These release notes describe new features and significant software components for the Cisco 1841 and Cisco 2801 routers that support Cisco IOS Release 12.3 (14)YT1. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. **Use these release notes with the [Cross-Platform Release Notes for Cisco IOS Release 12.3 T for Cisco IOS Release 12.3 T](#) located on [Cisco.com](#).**

For a list of the software caveats that apply to Release 12.3(14)YT1, refer to the [Caveats](#) section below, and to the online [Caveats for Cisco IOS Release 12.3 T](#) document. The caveats document is updated for every 12.3 T maintenance release and is located on [Cisco.com](#).

## Contents

- [System Requirements, page 2](#)
- [New and Changed Information, page 4](#)
- [Caveats, page 10](#)
- [Additional References, page 15](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 16](#)



# System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(14)YT1.

## Memory Requirements

[Table 1](#) lists the memory requirements for Cisco IOS Release 12.3(14)YT1.

**Table 1** *Memory Requirements*

Platform	Software Product Description	Feature Set	Image	Flash	DRAM
Cisco 1841	Cisco 1841 Advanced IP Services	Cisco 1841 Advanced IP Services	c1841-advipservicesk9-mz	32MB	128MB
Cisco 1841	Cisco 1841 Advanced Enterprise Services	Cisco 181X Advanced Enterprise Services	c1841-adventerprisek9-mz	32MB	128MB
Cisco 2801	Cisco 2801 Advanced IP Services	Cisco 2801 Advanced IP Services	c2801-advipservicesk9-mz	32MB	128MB
Cisco 2801	Cisco 2801 Advanced Enterprise Services	Cisco 2801 Advanced Enterprise Services	c2801-adventerprisek9-mz	32MB	128MB

## Hardware Supported

Cisco IOS Release 12.3(14)YT1 supports the following routers:

- Cisco 1841 router
- Cisco 2801 router

## Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco router, log in to the router and enter the **show version** command:

```
Router> show version
Cisco IOS Software, 2801 Software (C2801-ADVENTERPRISEK9-M), Version 12.3(14)YT1, RELEASE SOFTWARE (fc1)
Synched to version 12.4(1.7)
```

## Upgrading to a New Software Release

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

## Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Release 12.3(8)YT1 supports the same feature sets as Release 12.3(14)YT.

[Table 2](#) list the features and feature sets supported in Cisco IOS Release 12.3(14)YT1.

**Table 2** Feature Set Table

Platforms					
	<b>Basic MPLS Forwarding and Signaling</b>	<b>Label Distribution Protocol (LDP)</b>	<b>Resource Reservation Protocol (RSVP)</b>	<b>L-LSP</b>	<b>Congestion Management</b>
1841	Yes	Yes	Yes	No	Yes
2801	Yes	Yes	Yes	No	Yes
	<b>Congestion Avoidance</b>	<b>Packet Marking, Policing and Shaping</b>	<b>MPLS Traffic Engineering</b>	<b>TE-RSVP</b>	<b>Guaranteed Bandwidth Traffic Engineering Tunnels (GB-TE)</b>
1841	Yes	Yes	Yes	Yes	Yes
2801	Yes	Yes	Yes	Yes	Yes
	<b>MPLS DiffServ-Aware Traffic Engineering (DS-TE)</b>	<b>ISIS-TE</b>	<b>MPLS-VPN</b>	<b>Guaranteed Bandwidth VPN.</b>	<b>Interprovider VPN</b>
1841	Yes	Yes	Yes	Yes	Yes
2801	Yes	Yes	Yes	Yes	Yes
	<b>BGP Attributes</b>	<b>MPLS VPN Support for EIGRP (PE/CE)</b>	<b>VRF Aware IPsec</b>	<b>Per-VRF AAA</b>	<b>DHCP Relay VRF Aware</b>
1841	Yes	No	No	No	No
2801	Yes	No	No	No	No
	<b>NAT for MPLS VPNs (VRF-aware NAT)</b>	<b>On Demand Address Pools (ODAP)</b>	<b>NAT for MPLS VPNs (VRF-aware NAT)</b>	<b>Carrier Supporting Carrier (CsC) VPN</b>	<b>Ethernet over MPLS</b>
1841	No	No	No	Yes	No
2801	No	No	No	Yes	No
	<b>Frame Relay over MPLS</b>	<b>HDLC/PPP over MPLS</b>	<b>ATM AAL5 over MPLS</b>	<b>Any-to-Any Connectivity over MPLS</b>	<b>Fast Reroute</b>
1841	No	No	No	No	No

**Table 2**      **Feature Set Table (continued)**

Platforms					
2801	No	No	No	No	No
	<b>LSP Preemption</b>	<b>Backup LSPs</b>	<b>MPLS Management</b>		
1841	Yes	No	No		
2801	Yes	No	No		

## New and Changed Information

Cisco IOS Release 12.3(14)YT1 contains the features listed in this section.

### New Hardware Features in Cisco IOS Release 12.3(14)YT1

There are no new hardware features in this release.

### New Hardware Features in Cisco IOS Release 12.3(14)YT1

There are no new hardware features in this release.

### New Software Features in Cisco IOS Release 12.3(14)YT

The Cisco IOS Release 12.3(14)YT1 supports the same software features that are supported in the Cisco IOS Release 12.3(14)YT.

### New Software Features in Cisco IOS Release 12.3(14)YT

Cisco IOS Software Release 12.3(14)YT supports Advanced IP services, including the features described in this section.

#### Basic MPLS Forwarding and Signaling

This feature allows service providers to manually provision their MPLS networks, potentially increasing security and determinism throughout the network. The feature is similar in high-level concept to Static IP Routes currently available in IOS. Functions include the following:

- Label Switching (Swap). Label Stacking: Must support a label stack five deep, to enable technologies such as MPLS VPN, MPLS Traffic Engineering, and Fast Reroute.
- MPLS Explicit Null Label
- MPLS Implicit Null Label
- Penultimate Hop Popping
- Label Merging
- LSP Stitching: Provides a mechanism to connect two different LSPs, each in different traffic engineering domains, into a functionally single end-to-end LSP

## Label Distribution Protocol (LDP)

This feature adheres to IETF standard draft-ietf-mpls-ldp-1.0.txt and “Extensions to RSVP for LSP Tunnels” (draft-ietf-mpls-rsvp-lsp-tunnel-08.txt). Includes the following capabilities:

- Downstream unsolicited label advertisement is supported, along with transport of LDP LSPs over an RSVP-TE tunnel/LSP
- Interoperable, standards-based dynamic LSP setup and teardown between MPLS-enabled devices from Cisco and third-party vendors.
- Best-effort path selection
- Backwards-compatibility with TDP-based core networks, allowing interoperability with Cisco routers running TDP while allowing use of LDP only on edge OSR routers

## Resource Reservation Protocol (RSVP)

RSVP supports strict and loose explicit routes and bandwidth reservation. It provides explicitly created, source-routed path creation and teardown for guaranteed bandwidth reservation between two nodes end-to-end. The MPLS label specifies the CoS, while the EXP bits in the MPLS header signify the drop precedence within the service class, including IP ToS Mapping to LSPs. Multi-VC Mode L-LSP for ATM Deluxe on FlexWAN and on Blacktail. E-LSP. IP or Ethernet packets define the CoS and map the CoS into the EXP bits of an MPLS header. This value is then used to select priority queues, scheduling and drop thresholds, including IP ToS Mapping to MPLS EXP Bits, IP DSCP Mapping to MPLS EXP Bits, 802.1p Mapping to MPLS EXP Bits, and ACLs. This feature also includes mechanisms for traffic classification and security and is used to classify traffic for QoS application, and to permit/deny traffic access into an MPLS network.

## Congestion Management

Congestion management provides fair queue servicing of variable ToS, DSCP or 802.1p values, as expressed in the MPLS EXP bits of the header, strict priority queues, and class-based scheduling and link bandwidth guarantees. Classification is based on relative ToS, DSCP or 802.1p values, as expressed in the MPLS EXP bits of the header.

## Congestion Avoidance

Congestion avoidance includes selective congestion control on a hop-by-hop basis, using a weighted average queue depth to determine drop probability. Drop thresholds are based on relative ToS, DSCP or 802.1p values, as expressed in the MPLS EXP bits of the header.

## Packet Marking, Policing and Shaping

Packet Marking, Policing, and shaping is used to classify and limit traffic according to pre-defined traffic policies, on ingress and egress from an interface. It supports class of service for RSVP in adherence to IETF draft standards “Extensions to RSVP-TE and CR-LDP for support of Diff-Serv-aware MPLS Traffic Engineering” (draft-ietf-mpls-diff-te-ext-01.txt) and “Requirements for support of Diff-Serv-aware MPLS Traffic Engineering” (draft-ietf-mpls-diff-te-reqts-00.txt).

## MPLS Traffic Engineering

This capability adheres to IETF RFC 2702, “Requirements for Traffic Engineering Over MPLS.” It supports RSVP-initiated Traffic Engineered Tunnels - Routing with Resource Reservation (RRR), OSPF-TE Single Area, ISIS-TE Single Area.

### Guaranteed Bandwidth Traffic Engineering Tunnels (GB-TE)

GB-TE extends MPLS Traffic Engineering capabilities to provide additional constraint-based routing and admission control functionality. GB-TE builds upon traditional TE by introducing the concept of an additional class of service for specifically guaranteed bandwidth, enabling delivery of QoS services for customers that rely upon signaled QoS instead of provisioned QoS. This enables service providers to provide firm bandwidth commitments without fear of accidental over provisioning as a premium QoS service. Extends OSPF and ISIS to advertise available GB-TE bandwidth, in addition to available regular TE bandwidth.

## TE-RSVP

RSVP was developed to fit in the existing and enduring IP QoS model defined by various working groups in the IETF. RSVP defines a small number of QoS parameters that are mapped to the underlying data link layers. Supporting the IP QoS model is important for two reasons: First, the relative simplicity of the IP QoS model enables it to be supported over all existing Layer 2 technologies. Second, given that IP-based services will provide the majority of future revenue for service providers, interoperability at the boundary of IP and MPLS networks is of paramount importance. Using RSVP in MPLS networks provides a QoS model designed to run over a variety of technologies and optimized to support IP applications, both of which are necessary to build a consistent, workable, end-to-end IP QoS service.

## MPLS DiffServ-Aware Traffic Engineering (DS-TE)

DS-TE is an enhancement to MPLS TE that introduces the concept of class types to TE. Each participating link advertises the amount of available bandwidth of each class type on that link. When the constraint-based-routing process is executed for a new tunnel, a bandwidth constraint of a particular class type can be defined as one of the criteria to be used for the path selection. The admission control process carried using RSVP at each hop is performed against the available bandwidth of the specific class type.

## MPLS-VPN

MPLS VPN support includes Layer 3 VPN according to IETF RFC 2547 and RFC 2547bis (draft-rosen-rfc2547bis-02.txt), PE-PE IBGP Routing, PE-CE Routing, MPLS VPN Support for EBGp, MPLS VPN Support for Static Routes, MPLS VPN Support for OSPF, and MPLS VPN Support for RIPv2.

## Guaranteed Bandwidth VPN

Guaranteed bandwidth is a mechanism to extend the concept of basic MPLS VPNs by creating point-to-point services with tightly defined and controlled quality of service. This includes Fast VRF Convergence, VRF Route Limiting, BGP Site of Origin, BGP Hub and Spoke, CLI Command to Enter VRF Descriptions, VRF-specific Static ARP Entries, Multiple FIB Tables (MFIB), and 802.1Q VLAN-to-VRF Mapping.

## Interprovider VPN

Interprovider VPN is a mechanism for placing two or more MPLS PE devices into the same VPN, though each PE node might reside in different Autonomous Systems (AS) with an EBGp connection between the two ASs.

## BGP Attributes

It is possible to test BGP operation with specific attributes configured and passed. Attributes include Site of Origin (SOO) and Hub and Spoke

## MPLS VPN Support for EIGRP (PE/CE)

The MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) feature provides the network operator with the capability to transparently connect EIGRP customer networks through an MPLS-enabled service provider Border Gateway Protocol (BGP) network. EIGRP routes are redistributed as internal routes through BGP across a Virtual Private Network (VPN). This feature is configured only on PE routers within the service provider BGP network. Customer networks can connect to each other through a MPLS VPN, which is configured within a service provider backbone (BGP network). The MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) feature, when used within an MPLS-enabled service provider backbone, allows several EIGRP sites to connect seamlessly. EIGRP routes are converted to BGP routes and transported through the service provider backbone with the use of multiprotocol (mBGP) extended community attributes. The integration is transparent to the EIGRP sites, which appear as a single EIGRP network.

## VRF Aware IPsec

Network-based IPsec VPNs are an integrated solution for allowing remote access to the MPLS network. VRF-aware IPsec allows service providers and enterprise customers to setup per-VRF IKE/IPsec profiles and key matches. This enables any-to-any IPsec connectivity through a single global address. VRF-aware IPsec extends the scalability of the remote access solution.

## Per-VRF AAA

Using the Per VRF AAA feature, Internet Service Providers (ISPs) can partition authentication, authorization, and accounting (AAA) services based on Virtual Route Forwarding (VRF).

## DHCP Relay VRF Aware

In some environments, a relay agent resides in a network element that also has access to one or more MPLS VPNs. A DHCP server that wants to offer service to DHCP clients on those different VPNs needs to know the VPN in which each client resides. The network element that contains the relay agent typically knows about the VPN association of the DHCP client and includes this information in the relay agent information option. The DHCP Relay-MPLS VPN support feature allows the relay agent to forward this necessary VPN-related information to the DHCP server using the following three sub-options of the DHCP relay agent information option: VPN identifier; Subnet selection; and Server identifier override.

## On Demand Address Pools (ODAP)

ODAP automates the expansion of IP address pools for VPNs, enabling service providers to more effectively manage IP address spaces across multiple VPNs. With NAT and ODAP for MPLS VPNs, service providers can ensure their enterprise customers that the integrity of existing enterprise addressing schemes will be maintained once managed inside the service provider network, and that they will have access to the same robust functionality as in the enterprise environment.

## NAT for MPLS VPNs (VRF-aware NAT)

NAT for MPLS VPNs creates unique translations per VPN, allowing access to shared services even though IP addresses overlap. Benefits include increased SP revenues with outsourcing of NAT services; efficient shared services delivery; simpler central management of resources; reduced network complexity and costs for the enterprise.

## Carrier Supporting Carrier (CsC) VPN

CsC VPNs are a mechanism for supporting the concept of hierarchical VPNs, by defining two new VPN layers for service provider networks: backbone carriers and customer carriers. In this architecture, the backbone carrier uses a VPN to carry all of the traffic of its customer carrier, which in turn is free to provision its own VPNs within the higher-level VPN to support its own customers.

## Ethernet over MPLS

Ethernet over MPLS complies with IETF Draft Standards “Transport of Layer 2 Frames Over MPLS” (draft-martini-l2circuit-trans-mpls-05.txt) and “Encapsulation Methods for Transport of Layer 2 Frames Over MPLS” (draft-martini-l2circuit-encap-mpls-01.txt).

## Frame Relay over MPLS

Frame relay over MPLS complies with IETF Draft Standards “Transport of Layer 2 Frames Over MPLS” (draft-martini-l2circuit-trans-mpls-05.txt) and “Encapsulation Methods for Transport of Layer 2 Frames Over MPLS” (draft-martini-l2circuit-encap-mpls-01.txt).

## HDLC/PPP over MPLS

HDLC/PPP over MPLS complies with IETF Draft Standards “Transport of Layer 2 Frames Over MPLS” (draft-martini-l2circuit-trans-mpls-05.txt) and “Encapsulation Methods for Transport of Layer 2 Frames Over MPLS” (draft-martini-l2circuit-encap-mpls-01.txt).

## ATM AAL5 over MPLS

ATM AAL5 over MPLS complies with IETF Draft Standards “Transport of Layer 2 Frames Over MPLS” (draft-martini-l2circuit-trans-mpls-05.txt) and “Encapsulation Methods for Transport of Layer 2 Frames Over MPLS” (draft-martini-l2circuit-encap-mpls-01.txt).

## Any-to-Any Connectivity over MPLS

Any-to-any connectivity over MPLS provides arbitrary Layer 2 VPN connectivity between dissimilar endpoints enabling them to connect to Frame Relay endpoints over MPLS.

## Fast Reroute

Fast reroute provides 50 ms link restoration, link-level protection, and node-level protection.

## LSP Preemption

High priority LSPs can preempt low priority LSPs using route bumping.

## Backup LSPs

Backup features include hot standby that is established upon failure, LSP load balancing, and LSP bundling.

## MPLS Management

CLI Commands are provided to clear all LSP statistics, or to clear only the statistics of a particular LSP. Support is also provided for the following:

- MPLS LSR MIB using SMI v2
- MPLS Traffic Engineering MIB
- MPLS VPN MIB
- MPLS FEC-To-NHLFE (FTN) MIB using SMI v2
- ICMP Extensions to MPLS (MPLS Ping)
- MPLS VPN-aware Ping MIB (CISCO-PING-MIB.my)
- MPLS Traceroute
- MPLS Traffic Matrix Statistics
- MPLS VPN Traffic Statistics
- MPLS provisioning in the Cisco VPN Solution Center (VPNSC) software provisioning tool

# Caveats

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

## Resolved Caveats - Cisco IOS Release 12.3(14)YT1

- CSCsb24007

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

## Resolved Caveats - Cisco IOS Release 12.3(14)YT

- CSCeh60551

Symptoms: Certain malformed client certificates may cause an AP running 12.3.2.JA2 or 12.3.4.JA to crash when EAP-TLS is used.

Workaround: Issue a new client certificate.

- CSCei61732

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

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

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

- CSCeg51272

Symptoms: A router may reload while executing the **show ip nbar protocol-discovery** command.

Conditions: NBAR protocol-discovery is enabled on the Virtual-Template interface.

Workaround: There is no workaround.

- CSCeh61857  
Symptom: Unable to configure anything under non-dot11 subinterface, including IP address.  
Workaround: None before code change.
- CSCeh92096  
Bridge MIB not Populated.
- CSCei13397  
Symptom: Traceback messages are seen during bootup.  
Conditions: Diffie-Hellman group 2 or 5 is configured for IPSec.  
Workaround: There is no workaround.
- CSCei16040  
VendorType and ParentRelPos of ENTITY-MIB displays incorrect values.
- CSCsb43655  
Symptoms: Some incoming packets that are larger than 1400 bytes are incorrectly counted as "input errors" on an ATM interface. An ATM error debug reports an "ATM0: AAL5 rx errors (status = 0C100000)" message, which suggests congestion occurs while cells pass through the ATM interface.  
Workaround: There is no workaround.

- CSCei21607  
Symptom: A Cisco router configured for IP NAT may send "ALIGN-3-SPURIOUS: Spurious memory access" to the log.  
Workaround: There is no workaround.
- CSCeh35823  
Symptoms: When a router detects "invalid identity" failures while decrypting IPsec packets, a memory leak occurs for the packet memory associated with the failed packets.  
Conditions: This symptom is observed only when an "invalid identity" error occurs, which is an uncommon error that indicates that the originating router does not send packets according to what was originally negotiated. However, if there is another error that causes a "bad" decryption, the packet could be invalid and may also cause the symptom to occur.  
Workaround: There is no workaround.
- CSCeh46867  
Unmatched SSID probe request response causes TX stuck.
- CSCei27330  
Symptoms: A router that is configured for Dynamic Multipoint VPN (DMVPN) may frequently generate the following error message:  
%SYS-2-BADSHARE: Bad refcount in datagram\_done.  
Conditions: This symptom is observed on the Cisco 871 and Cisco 1800 series routers that function as a DMVPN spoke.  
Workaround: There is no workaround.
- CSCej04384  
Symptom: The adsl line can not be trained.  
Condition: Huawei DSLAM with ADSLoISDN, UR2.  
Workaround: There is no workaround.
- CSCin96534  
Symptoms: Cisco180x and 181x series routers will crash on enabling dot1x.  
Conditions: The crash is seen only when enabling dot1x on onboard FE interface, not on the switchports.  
Workaround: There is no workaround.
- CSCsa87733  
Symptoms: Only the first syslog server defined on a system receives syslog messages.  
Conditions: More than one syslog server is defined on a router, and when "logging source-interface xxxxx" command is in place.

Workaround: For those logging hosts impacted (in other words, if message counts are not changing), enter “no logging source-interface xxxxx” if possible. Next, re-enter “logging a.b.c.d,” and type the CLI command for each configured host. For example, re-enter the following two lines in “config term” mode; in this case:

```
“logging source interface FastEthernet1/0”
```

```
“logging 192.168.104.234”
```

```
“logging 192.168.104.103”
```

The list of hosts are found by entering “show run | include logging.”

- CSCsb13034

IPv6 multicast traffic do not get fast-switched.

- CSCsb47557

Symptom: DHCP fails with following message: “DHCP: Scan: bad FQDN option len 3.”

Conditions: The Option 81 response returned from the DHCP Server has no domain-name.

Workaround: Include a domain-name in the Option 81 response from the DHCP Server.

- CSCsb56224

Symptom: The last character of AT commands from router AUX line (line 1) is displayed only after first "RETURN" character. After second "RETURN" character AT command is executed by analog modem. This behaviour is causing problems with chat scripts and sending AT commands to analog modem (impossible to dialout using chat scripts). It's possible to send AT commands to modem using reverse telnet (AUX port) - after each command, we have to double hit "enter" key. Even entering command characters (like AT) letter A is echoed after pressing T, T is echoed after next character and so on.

Conditions: This problem is observed on a Cisco 871 series and Cisco 851 series routers.

Workaround: There is no workaround.

- CSCsb70282

The Cisco 1812 ISR router is not wireless capable; however, WLCCP port 2887 is open even though it should be closed.

- CSCsb3506

Support for CNS Inventory Agent registries on 18xx platforms for IE2100.

- CSCei30235

EAP User-name field length restricted to 64 bytes.

## Resolved Caveats - Cisco IOS Release 12.3(14)YT

- CSCef63944

Alignment/spurious errors occur while testing IPsec-realtime DNS.

- CSCec25511

Carbon: Bad getbuffer traceback on alpha WDS unit.

- CSCeh24429

Router crashes due to corrupted redzone after FE-FE performance test.

- CSCeh51374  
Loss of range with latest image.
- CSCeh59258  
Router crashes during bootup with broadband image and aircard.
- CSCeh61315  
Remove 1C20 FPGA support.
- CSCeh65303  
Cannot add max vlans to the database.
- CSCeh69802  
TX side of G radio fluctuates during stress/performance testing.
- CSCeh72067  
Shared/static wep function broken in latest.
- CSCeh72284  
Illegal config register values are allowed when NSPR is configured CSCeh73210 station-role root is missing from Dot11Radio0 interface.
- CSCeh75459  
FPGA ver1.3.
- CSCeh76767  
PSP client may stuck in dead lock, keep associated, but no traffic.
- CSCeh80343.  
Show dot11 associations doesn't populate all fields for 7920 clients.
- CSCeh80746  
See ASSERTION FAILED: when trying to associate more than 25 clients.
- CSCeh80843  
Can configure aes-ccm encryption mode, clients will be disassociated.
- CSCeh80851  
Remove ipv6 commands under dot11 interface.
- CSCeh83208  
Router crashes with Airlink during client LEAP authentication.
- CSCeh86927  
FW broken on dot11 with VLAN.
- CSCei05357  
Router crashes while configuring dot1x system-auth-control.
- CSCei12608  
Do not drop the packets with any of ATM cell with CLP=1.
- CSCei12639  
Some of ATM info msg should be printed when atm\_event\_debug is ON.

- CSCin90771  
Airlink IF-MIB - ifInUcastPkts Counter32 value getting decreasing.
- CSCin91153  
FTP failure with NVI - LAN host to LAN server.

## Additional References

The following sections describe the documentation available for the Cisco 1841 and Cisco 2801 routers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents. Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com in pdf or html form.

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

- [Release-Specific Documents, page 15](#)
- [Platform-Specific Documents, page 15](#)

## Release-Specific Documents

The following documents are specific to Release 12.3 and apply to Cisco IOS Release 12.3(14)YT. They are located on [Cisco.com](#):

- [Cross-Platform Release Notes for Cisco IOS Release 12.3](#)T
- [Field Notices: http://www.cisco.com/warp/public/tech\\_tips/index/fn.html](http://www.cisco.com/warp/public/tech_tips/index/fn.html).
- [Caveats for Cisco IOS Release 12.3](#) and [Caveats for Cisco IOS Release 12.3T](#)

## Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 1841 and Cisco 2801 routers are available on [Cisco.com](#) at the following location:

[http://www.cisco.com/en/US/products/hw/routers/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/routers/tsd_products_support_category_home.html)

## Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.3 and Cisco IOS Release 12.3(14)YT, and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only.

## Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image. Cisco Feature Navigator is available 24 hours a day, 7 days a week.

To use Cisco Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Cisco Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

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

## Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents.

### Documentation Modules

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

Select your release and click the command references, configuration guides, or any other Cisco IOS documentation you need

## Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feed-back, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

---

Use this document in conjunction with the documents listed in the “Additional References” section.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007, Cisco Systems, Inc. All rights reserved

