Release Notes for the SOHO 70 Series Routers and the Cisco 800 Series Routers for Cisco IOS Release 12.2(4)YH

May 28, 2002

These release notes for the SOHO 70 Series Routers and Cisco 800 Series Routers describe the enhancements provided in Cisco IOS Release 12.2(4)YH. These release notes are updated as needed. Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* located on Cisco.com and the Documentation CD.

For a list of the software caveats that apply to Release 12.2(4)YH, see the "Caveats" section on page 7 and *Caveats for Cisco IOS Release 12.2 T.* The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD.

Contents

These release notes discuss the following topics:

CISCO SYSTEMS

System Requirements

This section describes the system requirements for Release 12.2(4)YH and includes the following sections:

Memory Requirements

Table 1 and Table 2 provide the memory recommendations for the Cisco IOS feature sets supported by Cisco IOS Release 12.2(4)YH on the SOHO 70 Series Routers and Cisco 800 Series Routers.

Table 1 Recommended Memory for the SOHO 70 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory	Runs from
SOHO 71 Routers	Cisco SOHO 70 Series IOS IP FW	IP FW	soho71-oy6-mz	8 MB	16 MB	RAM

Table 2 Recommended Memory for the Cisco 800 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory	Runs from
Cisco 806 Routers	Cisco 806 Series IOS IP/FW Plus	IP/FW Plus	c806-o3sy6-mz	8 MB	32 MB	
	Cisco 806 Series IOS IP Plus	IP Plus	c806-sy6-mz	8 MB	16 MB	RAM

Hardware Supported

Cisco IOS Release 12.2(4)YH supports the following Cisco routers:

- SOHO 71 routers
- Cisco 806 Routers

For detailed descriptions of new hardware features and which features are supported on each router, see the "New and Changed Information" section on page 4. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to SOHO 70 Series Routers and Cisco 800 Series Routers, which are available on Cisco.com and the Documentation CD at the following location: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/index.htm

This URL is subject to change without notice. If it changes, point your web browser to Cisco.com, and click the following path:
Cisco Product Documentation: **Access Servers and Access Routers**: **Fixed Configuration Access Routers**: **<platform_name>**

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco router, log in to the router and enter the **show version** EXEC command. The following sample displays command output from a Cisco 806 router running Release 12.2(4)YH:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) C806 Software (C806-Y6-MZ), Version 12.2(4)YH, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Synched to technology version 12.2(5.4)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see Software Installation and Upgrade Procedures located at: http://www.cisco.com/warp/public/130/upgrade_index.shtml.

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 12.2(4)YH supports the same feature sets as Releases 12.2 T, but Release 12.2(4)YH can include new features supported by the SOHO 70 Series Routers and Cisco 800 Series Routers. Table 3 and Table 4 list the features and feature sets supported in Cisco IOS Release 12.2(4)YH.

The tables use the following conventions:

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

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

Table 3   Feature List by Feature Set for the SOHO 71 Routers

Features	In	Feature Sets	
		IP	IP/FW
Security			
Firewall			
Authentication Proxy		No	No
CBAC Audit Trails and Alerts		No	No
Port to Application Mapping		No	No
TACACS+	12.2(4)YH	No	Yes

Table 4   Feature List by Feature Set for the Cisco 806 Series Routers

Features	In	Feature Set		
		IP/FW	IP Plus	IP
Security				
Firewall				
Authentication Proxy	12.2(4)YH	Yes	No	No
CBAC Audit Trails and Alerts	12.2(4)YH	Yes	No	No
Port to Application Mapping	12.2(4)YH	Yes	No	No
TACACS+		No	No	No

New and Changed Information

The following sections list the new hardware and software features supported by Release 12.2(4)YH for the SOHO 70 Series Routers and the Cisco 800 Series Routers.

New Features in Release 12.2(4)YH

The following sections list the new software features supported by Cisco IOS Release 12.2(4)YH for the SOHO 70 Series routers and the Cisco 800 Series routers.

Firewall Features

Cisco IOS release 12.2(4)YH supports the following firewall features: authentication proxy, port to application mapping, and Context-based Access Control (CBAC) audit trails and alerts.

Authentication Proxy

The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access was associated with a user's IP address, or a single security policy had to be applied to an entire user group

or subnet. Now, users can be identified and authorized on the basis of their per-user policy, and access privileges tailored on an individual basis are possible, as opposed to general policy applied across multiple users.

With the authentication proxy feature, users can log into the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS, or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

The authentication proxy is compatible with other Cisco IOS security features such as Network Address Translation (NAT), Context-based Access Control (CBAC), IP Security (IPSec) encryption, and VPN client software.

For instructions on configuring authentication proxy, refer to the *Cisco IOS Security Configuration Guide*, Release 12.2. You can view this document at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c

Port to Application Mapping

Port to Application Mapping (PAM) is a feature of the Cisco IOS Firewall feature set. 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.

Using the port information, PAM establishes a table of default port-to-application mapping information at the firewall. The information in the PAM table enables Context-based Access Control (CBAC) supported services to run on nonstandard ports. Previously, CBAC was limited to inspecting traffic using only the well-known or registered ports associated with an application. Now, PAM allows network administrators to customize network access control for specific applications and services.

PAM also supports host or subnet specific port mapping, which allows you to apply PAM to a single host or subnet using standard access control lists (ACLs). Host or subnet specific port mapping is done using standard ACLs.

For instructions on configuring PAM, refer to the *Cisco IOS Security Configuration Guide*, Release 12.2. You can view PAM configuration instructions at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfpam.htm#xtocid2

CBAC Audit Trails and Alerts

Context-based access control (CBAC) is a security feature that enables the router to filter TCP and UDP packets based on application-layer protocol session information and generate real-time alerts and audit trails. Without CBAC, filtering can only be performed based on network layer and transport layer information. Enhanced audit trail features use SYSLOG to track all network transactions; recording time stamps, source host, destination host, ports used, and the total number of transmitted bytes, for advanced, session-based reporting. Real-time alerts send SYSLOG error messages to central management consoles upon detecting suspicious activity. Using CBAC inspection rules, you can configure alerts and audit trail information on a per-application protocol basis. For example, if you want to generate audit trail information for HTTP traffic, you can specify that in the CBAC rule covering HTTP inspection.

For instructions on configuring CBAC audit trails and alerts, refer to the *Cisco IOS Security Configuration Guide*, Release 12.2. You can view CBAC configuration instructions at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfcbac.htm

TACACS+

SOHO 71 routers support the Terminal Access Controller Access Control System Plus (TACACS+) protocol through Telnet. TACACS+ is a Cisco proprietary authentication protocol that provides remote access authentication and related network security services, such as event logging. User passwords are administered in a central database rather than in individual routers. TACACS+ also provides support for separate modular authentication, authorization, and accounting (AAA) facilities that are configured at individual routers.

Refer to the *Cisco 806 Software Configuration Guide* for more information on TACACS+. A configuration overview is provided at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/806/806swcg/routconf.htm

New Software Features in Release 12.2 T

For information regarding the features supported in Cisco IOS Release 12.2 T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on Cisco.com and the Documentation CD-ROM:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm

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

Service & Support: **Technical Documents**: **Release 12.2** (from the **Cisco IOS Software** drop-down list)

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(4)YH that can apply to SOHO 70 and Cisco 800 series routers. (Also, see the .)

Changing IP Addresses When Using the Cisco Easy VPN Client Feature

In Cisco 800 series routers, the Ethernet 0 LAN interface defaults to the primary IP address of 10.10.10.0 in a private network. If you need to change this IP address to match the local network configuration, you can use the command **ip address** or the Cisco Router Web Setup (CRWS) web interface.

Using the CRWS interface to change the IP address preserves the existing IP address as the primary address of the interface and assigns the new IP address as the secondary address on the interface. This CRWS interface functionality maintains (does not break) the existing connection between the PC web browser and the Cisco 800 series router and thereby does not interfere with normal router operations for most configurations.

Because of this behavior, the Cisco Easy VPN client feature assumes that if a secondary IP address exists on the Ethernet 0 interface, the secondary address should be used as the IP address for the inside interface for the NAT/PAT configuration. If no secondary address exists, the primary IP address will be used for the inside interface address, as is normally done on other platforms. If this behavior is not desired, use the **ip address** CLI command instead of the CRWS web interface to change the interface address.

Caveats

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

Caveats in Cisco IOS Releases 12.2 and 12.2 T are also in Cisco IOS Release 12.2(4)YH. For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*. For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*. These two documents list severity 1 and 2 caveats and are located on Cisco.com and the Documentation CD-ROM.

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

Caveats for Release 12.2(4)YH

This section describes possibly unexpected behavior by Release 12.2(4)YH. Only severity 1 through 3 caveats are included.

Miscellaneous

CSCin08536

The 806uut is unable to resolve the domain name and the router probe timeout occurs for a DNS operation.

CSCin08623

The router timeout is lost after a reload if the timeout value is set to a value greater than 60,000 ms and the frequency parameter is set to 300 seconds. Although the timeout setting works in the running configuration, when the configuration is saved and the router is reloaded, the timeout is set to 30,000 ms and the following error message appears.

```
%Illegal Value:  Cannot set Timeout to be greater than Frequency
```

CSCin08626

When a Cisco router listens for TFTP Protocol in a non-standard port using a PAM configuration and with nat overload configured, the TFTP transfer fails.

CSCin08629

The default value for the object rttMonEchoAdminCache variable cannot be read using SNMP.

CSCin09365

Due to a timing issue, even when an interface is up, the DHCP process is not activated and DHCP functionality is disabled on that interface. To work around this problem, again enter the command **no shut** on the WAN (Ethernet1) interface.

CSCin09643

The nat translation functionality does not work for IPSec traffic on a 806uut.

CSCin09771

Valid RTT probes can not be determined from querying the MIB object rttMonApplSupportedRttTypesValid.

CSCin10161

The router returns a value of 0 instead of the default value of 1 for the TCP MIB object rttMonEchoAdminPktDataRequestSize.

Related Documentation

The following sections describe the documentation available for the SOHO 70 and Cisco 800 series 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 and the Cisco IOS release notes, which are available online on Cisco.com and the Documentation CD-ROM.

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

- Release-Specific Documents
- Platform-Specific Documents
- Obtaining Documentation and Technical Assistance

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Release 12.2(4)YH. They are located on Cisco.com and the Documentation CD-ROM (under the heading **Service & Support**):

- To reach the *Release Notes for the Cisco 800 Series Routers for Cisco IOS Release 12.2(4)YH*, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cisco 800 Series Routers**: **Cisco 800 Series - Release Notes for Release 12.2(4)YH**

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

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

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

  Technical Documents: **Product Bulletins**

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

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

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

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents are available for the SOHO 70 and Cisco 800 series routers on Cisco.com and the Documentation CD-ROM.

SOHO 70 and Cisco 800 Series Routers

Documentation specific to the SOHO 70 Series Routers and Cisco 800 Series Routers is available on Cisco.com and the Documentation CD at the following location:

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

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

Cisco Product Documentation: **Access Servers and Access Routers**: **Fixed Configuration Access Routers**: **Cisco 1700 Series Routers**: **<platform_name>**

Software Configuration

The document *Cisco Router Web Setup User Guide* is available for the SOHO 70 and Cisco 800 series routers at the following location:

http://www.cisco.com/univercd/cc/td/doc/clckstrt/crws/ugcrws30.htm

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

Technical Documents: **Router Configuration Tools**: **Cisco Router Web Setup**

Obtaining Documentation and Technical Assistance

The *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* contains the latest descriptions and locations of the following sources for obtaining documentation and technical assistance from Cisco Systems. See the section "Release-Specific Documents" for the location of the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T*.

Additional sources of documentation and technical assistance are listed below:

- World Wide Web, Cisco.com—Cisco Systems website: http://www.cisco.com.

- Documentation CD—Cisco documentation and additional literature are available in a CD package, which ships with your product.

- Ordering documentation—Methods for ordering documentation include Networking Products MarketPlace, the online Subscription Store, and calling a local account representative using the Cisco corporate headquarters or North America phone numbers.

- Documentation feedback—When using the World Wide Web, you can submit technical comments electronically. You can also send e-mail, mail in the response card that is behind the front cover of many documents, or send correspondence to Cisco Systems. We appreciate your comments.

- Technical Assistance Center (TAC)—The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract. You can contact the TAC using Cisco.com or by phone. Toll-free numbers are available for many countries.