Release Notes for the Cisco 7200 Series for Cisco IOS Release 12.2(11)YX and 12.2(11)YX1

June 23, 2003

Text Part Number OL-3617-02

These release notes describe changes to the software for the Cisco 7200 series routers for Cisco IOS Release 12.2(11)YX and 12.2(11)YX1.

Contents

Introduction

Cisco IOS Software Release 12.1(11)YX1 features IPSec stateful failover, but with the addition of generic routing encapsulation (GRE), a tunnel interface not tied to specific “passenger” or “transport” protocols.

Tunneling protocols, such as GRE, encapsulate packets inside of a transport protocol. A tunnel interface creates a virtual point-to-point link between two routers at remote points over an IP internetwork. Each tunnel must be configured separately for each link.

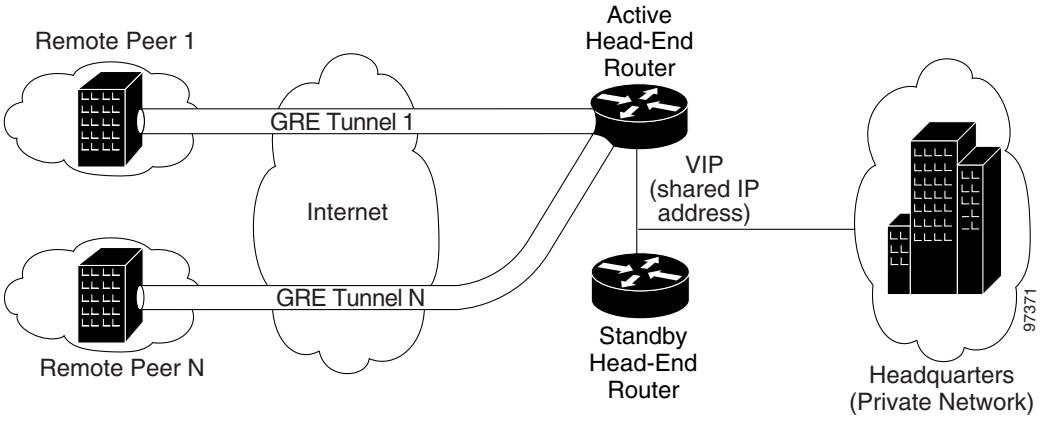
CISCO SYSTEMS

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

GRE supports multicast traffic, critical for V3PN applications.

Figure 1 shows a sample topology for site-to-site configuration of IPSec Stateful Failover with GRE.

Figure 1 Sample Topology for Site-to-Site



System Requirements

Memory Requirements

Table 1 lists the software images and corresponding memory requirements for the and Cisco 7200 series routers in Cisco IOS Release 12.2(11)YX and 12.2(11)YX1.

Note For a complete list of the minimum memory recommendations for the Cisco 7200 series of routers in Cisco IOS Release 12.2, go to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122/122feats.htm#55814

Table 1 Software Images and Memory Recommendations for Cisco IOS Release 12.2(11)YX and 12.2(11)YX1

Platform	Feature Set	Image Name	Flash Memory Required	DRAM
Cisco 7200	Cisco IOS IP/FW/IDS/IPSec 3DES	c7200-ik9o3s-mz	20 MB	128 MB
	Cisco IOS IP Plus/IPSec 3DES	c7200-ik9s-mz	20 MB	128 MB
	Cisco IOS Enterprise/FW/IDS/IPSec 3DES	c7200-jk9o3s-mz	20 MB	128 MB
	Cisco IOS Enterprise/IPSec 3DES	c7200-jk9s-mz	20 MB	128 MB

Hardware Supported

This release supports the Cisco 7200 series routers with NPE- 400, 300, 225, 200, and NSE-1 processors. The Cisco IOS Release 12.2(11)YX and 12.2(11)YX1 also support the VPN Acceleration Module (VAM).

Note Cisco IOS Release 12.2(11)YX and 12.2(11)YX1 do not support the NPE-G1 processor or the service adapter VPN acceleration module (SA-VAM2).

For additional information about supported hardware for these platforms, refer to the Hardware/Software Compatibility Matrix in the Cisco Software Advisor at the following URL:

http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Determining the Software Version

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

Note The following example shows output from the Cisco 7200 series router.

```
router> show version

Cisco Internetwork Operating System Software
IOS (tm) 7200 series Software c7200-jk9o3s-mz, Version 12.2(11)YX1, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to S*oftware Installation and Upgrade Procedures* located at the following URL:

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.

For a complete list of feature sets supported by the Cisco 7200 series routers in Release 12.2, go to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122/122reqs.htm#xtocid3

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

New and Changed Information

New Hardware Features in Cisco IOS Release 12.2(11)YX and 12.2(11)YX1

There are no new hardware features in Cisco IOS Release 12.2(11)YX or Cisco IOS Release 12.2(11)YX1.

New Software Features in Cisco IOS Release 12.2(11)YX1

The following software feature is new to Cisco IOS Release 12.2(11)YX1:

- IPSec High Availability with generic routing encapsulation (GRE)—Adds a tunnel interface for each GRE endpoint. Because tunnels are point-to-point links, you must configure a separate tunnel for each link.

New Software Features in Release 12.2(11)YX

The following software features are new in Cisco IOS Release 12.2(11)YX:

- IPSec High Availability—Enables VPN tunnels to fail over from an active unit to a standby unit without reinitiating the VPN tunnels, and without detection by remote devices.
- IKE Acceleration—Reduces VPN tunnel setup time. This feature is useful in network storm situations, when a large number of tunnels need to be set up simultaneously.
- Dead Peer Detection (DPD)—Tracks peer connectivity for failover purposes. When a peer connection is down, failover occurs. While similar to IKE Keepalive functions, it provides improved scalability and less peer tracking overhead.

Caveats

This section lists caveats for the Cisco IOS Release 12.2(11)YX and 12.2(11)YX1 by tracking number (DDTS #) and release number, and indicates whether the caveat has been corrected. An “O” indicates that the caveat is open in that release; a “C” indicates that the caveat is closed in that release, and an “R” indicates that the caveat is resolved in a later release.

Table 2 lists the caveats for the Cisco IOS Release 12.2(11)YX and 12.2(11)YX1.

Table 2 Release Caveats and Caveats Corrected Reference

	Cisco IOS Software Release 12.2(11)YX and 12.2(11)YX1
DDTS Number	**Corrected**
CSCdx71554	R
CSCdz36655	R
CSCdz44533	O
CSCdz49120	R
CSCdz50548	O
CSCdz63175	R
CSCea55900	R
CSCea86277	R
CSCea86336	R

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Software Center**: **Cisco IOS Software**: **Bug Toolkit**: **Bug Navigator II**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

The caveats section includes the following subsections:

- Open Caveats—Cisco IOS Release 12.2(11)YX1, page 5
- Resolved Caveats—Cisco IOS Release 12.2(11)YX1, page 6

Open Caveats—Cisco IOS Release 12.2(11)YX1

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(11)YX1. All the caveats listed in this section are open in Cisco IOS Release 12.2(11)YX1. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Note Many caveats that apply to Cisco IOS Release 12.2 also apply to Cisco IOS Release 12.2(11)S. For information on severity 1 and 2 caveats in Cisco IOS Release 12.2, see the *Caveats for Cisco IOS Release 12.2* document located on Cisco.com at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122/index.htm

- CSCdz44533

  Symptoms: In the event of a failure on the active device, Hot Standby Router Protocol (HSRP) does not report a change in state. Consequently, in the case of stateless failover, existing IPSec security associations (SAs) are not removed from the failed device. Also, where reverse route injection (RRI) is used with a static crypto map, routes on the failed device are not removed from the routing table.

  Conditions: The HSRP failure to report symptom is observed with stateless failover configurations; for example, when using the **redundancy** keyword to apply a crypto map to an interface. The RRI symptom is observed with both stateless and stateful failovers, when the **reverse-route** keyword is added to a static crypto map.

  Workaround: Do not use RRI, instead add static routes manually or use dynamic crypto maps. For stateless failover, enter the **clear crypto sa** command after a failover on the failed device.

- CSCdz50548

  Symptoms: If the redundancy name used in an Switch-to-Switch Protocol (SSP) configuration is more than 21 characters, the router crashes when booting. A long redundancy name causes a crash only when it is parsed as part of an SSP configuration.

  Conditions: This symptom is observed when using a very long HSRP redundancy name.

  Workaround: Use a redundancy name less than 21 characters.

Resolved Caveats—Cisco IOS Release 12.2(11)YX1

This section describes caveats that have been resolved by Cisco IOS Release 12.2(11)YX1.

- CSCdx71554

  Symptoms: Cisco IOS Software Release 12.2S supports generic routing encapsulation (GRE) in IPSec, which requires that the crypto map be applied to both the physical and tunnel interfaces on the router. At bootup, however, only the tunnel interface is activated:

```
int tunnel 0
crypto map fred ssp 1

int fa 0/1
crypto map fred ssp 1
```

  Conditions: When you remove the crypto map from both the physical and tunnel interfaces, a crash results:

```
crypto_ha_ipsec_notify_enable(ipaddrtype sadb_id, boolean enable)
{
    if(enable) {
        sspstatetype state;
            if(ipsec_ha_usage_counter == 0) {
            if(crypto_ha_ipsec_hook_ssp()) {
                ipsec_ha_usage_counter++;
            }
.......
```

  Workaround: None.

- CSCdz49120

  Symptoms: Reverse route injection works only after the initial injection.

  When the Unity Client (UC) connects to the UUT, reverse route injection results and a route for address 22.0.0.2 is set up on the UUT.

  Topology:

```
cat6503          35xx_switch              PC
     gig2/2 - gig0/1    fa0/1 -------- fe
  10.0.0.2                            10.0.0.5
```

  The 22.0.0.2 is in the private address pool used to give to the PC when it connects via UC.

```
     22.0.0.0/32 is subnetted, 1 subnets
S       22.0.0.2 [1/0] via 10.0.0.5
```

  Conditions: When you reload the UUT, and reinitiate the tunnel, the route is reinjected.

  Workaround: Add static route for 22.0.0.2, however, this workaround does not always work.

- CSCea55900

  Symptom: The active and standby route processors are in the high availability setup when the active route processor crashes with the traceback below.

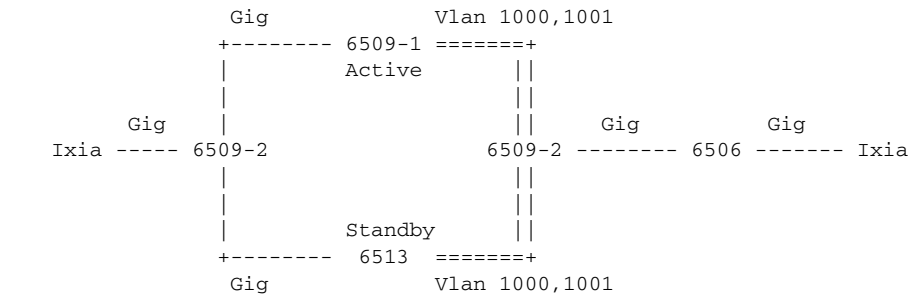
```
-Traceback=
      4130B310[crypto_ipsec_lock_peer+0x0]
      412FBD50[ha_clear_peer_sas+0x44]
```

  Conditions: In the following example 6513 is the active route processor and 6509-1 is the standby route processor. The crash occurred on the active route processor:

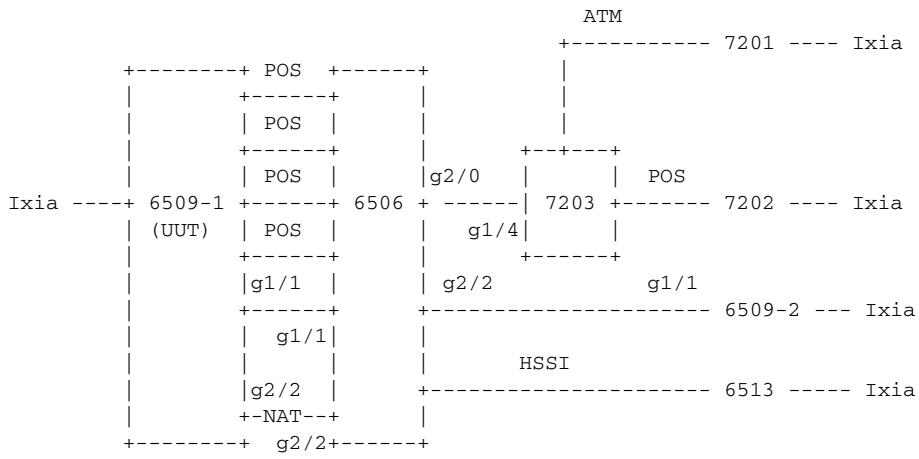
```
6513#show crypto eli
Hardware Encryption Layer :   ACTIVE
Number of crypto engines = 1 .

CryptoEngine-8 (slot-9) details.
Capability-IPSec : No-IPPCP, 3DES, NoAES, RSA

IKE-Session   :  1242 active, 10899 max, 0 failed
DH-Key        :     0 active,  9999 max, 0 failed
IPSec-Session :  3170 active, 21865 max, 0 failed
```

  Topologies:

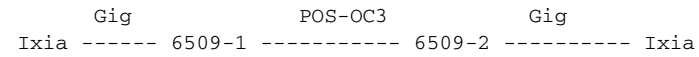
  HA:



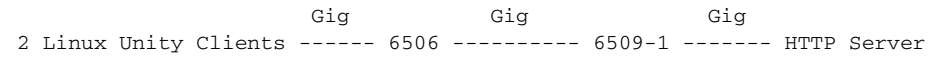
Non HA:



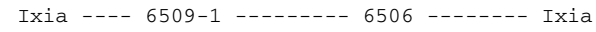
GRE:



HTTP Traffic:



IP Mutlicast Clear Traffic through security modules for Catalyst 6500:



Workaround: None.

- CSCea86277

  Symptom: As the active and standby routers boot up, the active router crashes immediately on initial SA setup with the remote router.

  Conditions: This symptom appears under the following conditions:

  1. The active and standby routers are loaded with the ddukes-special image.
  2. The routers are configured for high availability (HA) with GRE.
  3. All the routers are reloaded, and when the active router initially sets up SA with the remote, it crashes.

Queued messages:

```
Unexpected exception, CPU signal 23, PC = 0x60621440

$0 : 00000000, AT : 627F0000, v0 : 62B71028, v1 : 00000000
a0 : 629E1418, a1 : 000132E4, a2 : 627E9730, a3 : 000001F0
t0 : 00000020, t1 : 3400FF01, t2 : 3400C100, t3 : FFFF00FF
t4 : 60626830, t5 : 00001D98, t6 : 80000000, t7 : 00000000
s0 : 00000000, s1 : 00000000, s2 : 624B0000, s3 : 00000002
s4 : 62320000, s5 : 62320000, s6 : 00000001, s7 : 627E0000
t8 : 634C7D04, t9 : 00000000, k0 : 3040D001, k1 : 00000000
gp : 627F1368, sp : 63481990, s8 : 62320000, ra : 6061F794
EPC  : 60621440, ErrorEPC : FFFFFFFF, SREG     : 3400FF03
MDLO : 00000000, MDHI     : 00000000, BadVaddr : 00000014
Cause 00000024 (Code 0x9): Breakpoint exception

-Traceback= 60621440 6061F794 605FFF94 61876A58 618745C4 61934888 618750BC 61872
638 61872800 61840AD8
=== Flushing messages (09:20:11 EDT Fri Apr 25 2003) ===
```

Workaround: None.

- CSCdz36655

  Symptom: This symptom occurs when using enc 3des on ike and/or ipsec.

  ```
  crypto isakmp policy 10
  encryption 3des
  hash md5
  authentication pre-share
  group 2

  crypto ipsec transform-set t1 ah-sha-hmac esp-3des esp-sha-hmac comp-lzs
  ```

  Having the above configurations will not work when failing over from software to hardware crypto.

  Condition: If the active router is using software crypto, updating a hardware-equipped standby router will not create an ike sa, and the following error is displayed:

  ```
  Nov 19 11:14:53.748 EST: IPSECcard: an error coming back 0x000F
  Nov 19 11:14:53.748 EST: %CRYPTO_HA-3-IKEINSERTKEYFAIL: (VIP=172.16.1.10)ISAKMP SA
  entry key insertion on standby device failed for src=172.16.1.155, dst=172.16.1.10
  Nov 19 11:14:53.944 EST: IPSECcard: an error coming back 0x000F
  Nov 19 11:14:53.948 EST: IPSECcard: an error coming back 0x000F
  Nov 19 11:15:09.412 EST: IPSECcard: an error coming back 0x000F
  Nov 19 11:15:09.412 EST: IPSECcard: an error coming back 0x000F
  7140-16>
  ```

  If both the active and standby routers are using a VPN Accelerator Module (VAM), this error does not occur.

  Workaround: None.

- CSCdz63175

  Symptom: Phase one of stateful failover doesn't support clients.

  Condition: When high availability is enabled over GRE tunnels, each GRE tunnel should use "ip unnumber interface xxx" to setup its ip address.

  Workaround: Each GRE tunnel have its own ip address in addition to using ip unnumber.

- CSCea86336

  Symptom: The remote router receives ike new sa packet when the standby router comes up from reload. The remote router receive another ike new sa packet when the standby router is reloaded. This is a regression bug.

  Conditions:

  1. Load HA routers with ddukes-special April 24 image.
  2. Configure HA with GRE and wait for SA's and routes to settle.
  3. Reload the Standby router and as it comes up, the Remote will receive an NewSA IKE packet.

  Workaround: None.

Sample Configuration

The configuration for IPSec Stateful Failover builds on the standard Stateful Failover configuration, but with the addition of a tunnel interface for each GRE endpoint, as shown in Figure 1.

1. The crypto parameters on the Stateful Failover Pair must be the same for:
   - isakmp policy (encryption, authentication, hash, lifetime, group)
   - isakmp key (shared secret with remote peer)
   - ipsec security-association lifetimes
   - ipsec transform set
2. Crypto map has to be applied to BOTH the tunnel and physical interface. To get traffic to go to the Tunnel interface there should be a route to the Tunnel IP address from the crypto peer.
3. SSP group can be configured with up to 32 redundancy groups, (with 32 Virtual IP Addresses).
4. There must be an access-list for the gre traffic with the VIP as one of the endpoints.

Following is a sample configuration which uses multiple redundancy groups, and multiple GRE tunnels. Note that this isn't necessarily a realistic deployment, but was used in the lab to illustrate the failover of multiple redundancy groups with multiple GRE tunnels. Ethernet sub-interfaces were used to simulate multiple VIPs.

Note that the other redundant router would have the same configuration except that the physical IP addresses will be different, and the SSP remote address will be pointing to the physical IP address of the private interface of the SSP peer.

Head-end router:

```
ip cef
!
ssp group 100
 remote 40.0.0.5
 redundancy GRE_1
 redundancy GRE_2
```

Note 20.i.j.1 addresses are the remote peers

```
!
crypto isakmp policy 1
 encr 3des
```

```
 authentication pre-share
crypto isakmp key gre1 address 20.1.1.1
crypto isakmp key gre2 address 20.1.2.1
crypto isakmp ssp 100
!
!
crypto ipsec security-association lifetime kilobytes 536870912
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set HA_TRANSFORM esp-3des
!
crypto map gre_1 1 ipsec-isakmp
 set peer 20.1.1.1
 set transform-set HA_TRANSFORM
 match address gre_1
!
crypto map gre_2 1 ipsec-isakmp
 set peer 20.1.2.1
 set transform-set HA_TRANSFORM
 match address gre_2
!
!
call rsvp-sync
!
!
interface Tunnel1
 bandwidth 500
 ip unnumbered FastEthernet0/0.1
 tunnel source 172.1.1.100
 tunnel destination 20.1.1.1
 crypto map gre_1 ssp 100
 ip rsvp bandwidth
!
interface Tunnel2
 bandwidth 500
 ip unnumbered FastEthernet0/0.2
 tunnel source 172.1.2.100
 tunnel destination 20.1.2.1
 crypto map gre_2 ssp 100
 ip rsvp bandwidth
!
!
```

Note Sub-interfaces are used to simulate failover of multiple hsrp groups.

```
interface FastEthernet0/0
 no ip address
 shutdown
 duplex full
 speed 100
 standby delay minimum 200 reload 200
!
interface FastEthernet0/0.1
 encapsulation dot1Q 500
 ip address 172.1.1.6 255.255.255.0
 standby delay minimum 60 reload 120
 standby 1 ip 172.1.1.100
 standby 1 timers 1 3
 standby 1 preempt
 standby 1 name GRE_1
 standby 1 track FastEthernet0/1
 standby 1 track FastEthernet0/0
```

```
 crypto map gre_1 ssp 100
!
interface FastEthernet0/0.2
 encapsulation dot1Q 501
 ip address 172.1.2.6 255.255.255.0
 standby delay minimum 60 reload 120
 standby 2 ip 172.1.2.100
 standby 2 timers 1 3
 standby 2 preempt
 standby 2 name GRE_2
 standby 2 track FastEthernet0/1
 standby 2 track FastEthernet0/0
 crypto map gre_2 ssp 100
!
!
interface FastEthernet0/1
 ip address 40.0.0.6 255.255.255.0
 shutdown
 duplex full
 speed 100
 standby delay minimum 60 reload 120
 standby 255 ip 40.0.0.100
 standby 255 timers 1 3
 standby 255 preempt
 standby 255 name PRIVATE
 standby 255 track FastEthernet0/0
!
!
ip classless
ip route 10.0.1.1 255.255.255.255 Tunnel1
ip route 10.0.1.2 255.255.255.255 Tunnel2
ip route 20.1.1.0 255.255.255.0 172.1.1.4
ip route 20.1.2.0 255.255.255.0 172.1.2.4
ip route 40.0.1.0 255.255.255.0 40.0.0.13
ip route 40.0.2.0 255.255.255.0 40.0.0.13
ip route 40.0.3.0 255.255.255.0 40.0.0.13
ip route 40.0.4.0 255.255.255.0 40.0.0.13
ip route 40.0.5.0 255.255.255.0 40.0.0.13
ip route 223.255.254.254 255.255.255.255 40.0.0.1
no ip http server
!
```

Note Access-lists are needed to permit GRE traffic to flow.

```
ip access-list extended gre_1
 permit gre host 172.1.1.100 host 20.1.1.1
ip access-list extended gre_10
 permit gre host 172.1.10.100 host 20.1.10.1
```

Related Documentation

Hardware Documents

Cisco 7200 series router hardware documentation is available on cisco.com at this URL:

http://www.cisco.com/en/US/products/hw/routers/ps341/products_product_index09186a0080123f5a.html

Cisco IOS Software Documents

Cisco IOS Release 12.2 software documentation is available on cisco.com at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_tech_note09186a00800941da.shtml

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

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

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

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

  http://www.ciscopress.com

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

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

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

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

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

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

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

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

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