



Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2(14)SU2

January 2, 2005

Text Part Number: OL-6724-01 B0

These release notes describe changes to the software for the Cisco 7000 family for Cisco IOS Release 12.2(14)SU2.

Contents

- [Introduction, page 2](#)
- [System Requirements, page 5](#)
- [New and Changed Information, page 8](#)
- [Caveats, page 8](#)
- [Sample Configuration, page 11](#)
- [Related Documentation, page 13](#)
- [Obtaining Documentation, page 13](#)
- [Documentation Feedback, page 14](#)
- [Cisco Product Security Overview, page 15](#)
- [Obtaining Technical Assistance, page 16](#)
- [Obtaining Additional Publications and Information, page 17](#)
- [Glossary, page 19](#)



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

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

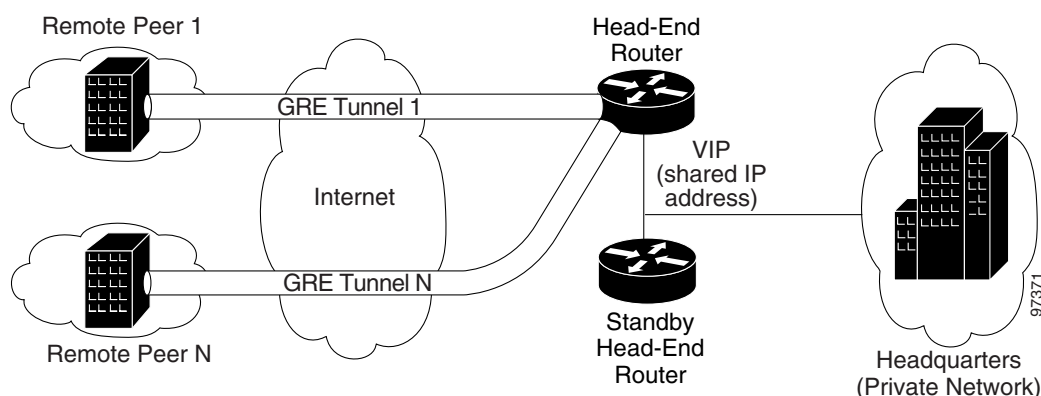
Introduction

Cisco IOS Software Release 12.2(14)SU2 features Stateful Failover of IPSec security associations (SAs) for site-to-site VPN (see [Figure 1](#)), storage of encrypted pre-shared keys in the configuration, Cisco 7200 NPE-G1 processor support, and VAM2 crypto card support (DES and 3DES only). Cisco IOS Software Release 12.2(14)SU2 is based on Cisco IOS Release 12.2(14)SU.

[Figure 1](#) shows a sample topology for site-to-site configuration of IPSec Stateful Failover with Generic Routing Encapsulation (GRE), a tunnel interface not tied to specific “passenger” or “transport” protocols.

GRE supports multicast traffic, critical for V3PN applications.

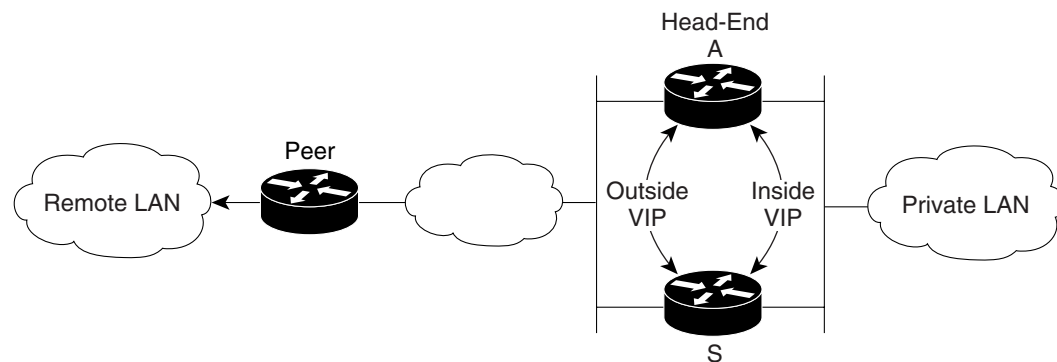
Figure 1 Site-to-Site VPN Configuration



There are four possible configurations for the Cisco 7200 series routers using Cisco IOS Release 12.2(14)SU2:

- non-GRE High Availability (HA) with a virtual IP (VIP), or redundancy groups, on the outside and a VIP on the inside (see [Figure 2](#))
- non-GRE HA with only VIPs on the outside. The route to the outside is provided by Reverse Route Injection (RRI) (see [Figure 3](#))
- GRE HA, with VIPs on the outside and inside interfaces (see [Figure 4](#))
- GRE HA, with only a VIP on the outside, using RRI to inject routes (see [Figure 5](#))

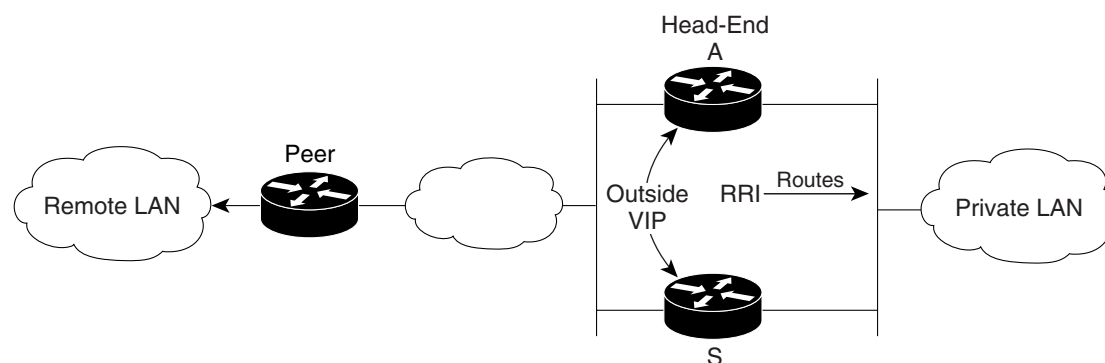
Figure 2 HSRP VIP on Inside and Outside



Inside VIP configured as default gateway for route from private LAN to remote LAN

114186

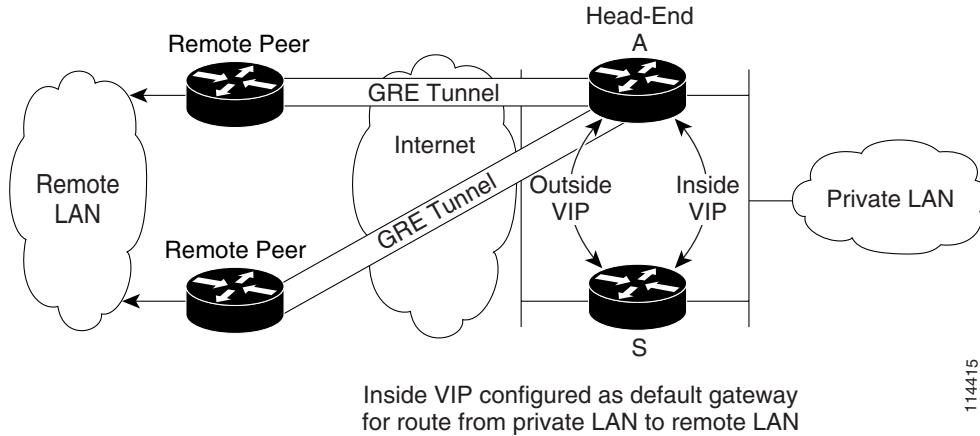
Figure 3 HSRP VIP on Outside, RRI Injected Routes on Inside



Reverse Route Injection (RRI) is configured on the head-end router when the tunnel is forming. RRI injects static routes to the remote network.

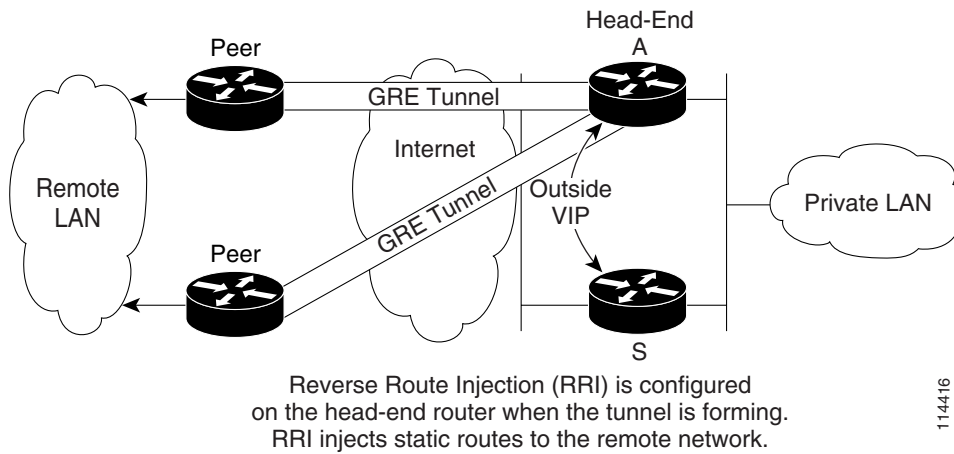
114187

Figure 4 GRE HA with VIPs on the Outside and Inside Faces



114415

Figure 5 GRE HA with Only a VIP on the Outside, Using RRI to Inject Routes



114416

Features

There are no new features in Cisco IOS Release 12.2(14)SU2. However, several caveats have been resolved.

[Table 1](#) provides a summary of the Cisco IOS Release 12.2(14)SU2 performance guidelines.



Note

Performance may vary depending on the actual features enabled, however these guidelines offer general guidelines for stable deployment. Contact Cisco TAC for guidelines outside of these parameters.

Table 1 Performance Guidelines

Feature	Description
Number of tunnels	<ul style="list-style-type: none"> 2000 tunnels [2000 IKE SA: 4000 IPSec SA] for Cisco 7200 with NPE-G1 or NPE400 with VAM/VAM2 500 tunnels for Cisco 7200 with NPE225 with VAM/VAM2
GRE	1000 GRE/IPSec tunnels

Limitations

The Cisco IOS Release 12.2(14)SU2 shares the same set of limitations as 12.2(14)SU, including the following:

- No EzVPN support for Stateful Failover
- Only single VAM/VAM2 support in the high availability (HA) configuration
- IPSec stateful solution is incompatible with old style IKE keepalives but is compatible with DPD (Note: DPD is not a requirement for IPSec stateful HA solution)
- No AES support in Cisco IOS Release 12.2(14)SU2
- No NAT-T features

System Requirements

This section includes the following topics:

- [Memory Requirements, page 6](#)
- [Hardware Supported, page 6](#)
- [Determining the Software Version, page 7](#)
- [Upgrading to a New Software Release, page 7](#)
- [Feature Set Tables, page 7](#)

Memory Requirements

Table 2 lists the software images and corresponding memory requirements for the Cisco 7200 series routers in Cisco IOS Release 12.2(14)SU2.


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>


Note

It is recommended that you upgrade your boot image with the c7200-kboot-mz boot helper image when using Cisco IOS Release 12.2(14)SU2.

Table 2 Software Images and Memory Recommendations for Cisco IOS Release 12.2(14)SU2

Platform	Feature Set	Image Name	Flash Memory Required	Minimum DRAM
Cisco 7200	Cisco IOS IP/FW/IDS/IPSec 3DES	c7200-ik9o3s-mz	64 MB	256 MB
	Cisco IOS IP Plus/IPSec 3DES	c7200-ik9s-mz	64 MB	256 MB
	Cisco IOS Enterprise/FW/IDS/IPSec 3DES	c7200-jk9o3s-mz	64 MB	256 MB
	Cisco IOS Enterprise/IPSec 3DES	c7200-jk9s-mz	64 MB	256 MB
	Cisco IOS Enterprise IPSec 3DES	c7200-kboot-mz	64 MB	256 MB

Hardware Supported

Cisco IOS Software Release 12.2(14)SU2 supports the Cisco 7200 series routers with NPE- 225, NPE-400, and NPE-G1 processors, as well as the VPN Acceleration Module (VAM) and VAM2 crypto cards (DES and 3DES only).


Note

Cisco IOS Software Release 12.2(14)SU2 supports only a single VAM/VAM2 in the HA configuration.

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/hwswwmatrix.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(14)SU2, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to *Software 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

This section includes the following topics:

- [New Hardware Features in Cisco IOS Release 12.2\(14\)SU2, page 8](#)
- [New Software Features in Cisco IOS Release 12.2\(14\)SU2, page 8](#)

New Hardware Features in Cisco IOS Release 12.2(14)SU2

There are no new hardware features supported on Cisco IOS Release 12.2(14)SU2.

New Software Features in Cisco IOS Release 12.2(14)SU2

There are no new software features introduced in Cisco IOS Release 12.2(14)SU2.

Caveats

This section lists the caveats for the Cisco IOS Release 12.2(14)SU2, by tracking number (DDTS #) and release number, and indicates whether the caveat has been corrected. An “O” indicates that the caveat is open in the release; a “C” indicates that the caveat is closed in the release, and an “R” indicates that the caveat is resolved in the release.



Note

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml

To become a registered cisco.com user, go to the following website:

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

Table 3 lists the caveats for the Cisco IOS Release 12.2(14)SU2.

Table 3 *Caveats for Cisco IOS Releases 12.2(14)SU2*

DDTS Number	Cisco IOS Software Release 12.2(14)SU2
•CSCeb56909	R
•CSCed15310	R
•CSCed40933	R
•CSCee67450	R
•CSCef46191	R
•CSCef75551	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\(14\)SU2, page 9](#)
- [Resolved and Closed Caveats—Cisco IOS Release 12.2\(14\)SU2, page 9](#)
- [Sample Configuration, page 11](#)

Open Caveats—Cisco IOS Release 12.2(14)SU2

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(14)SU2. All the caveats listed in this section are open in Cisco IOS Release 12.2(14)SU2. 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>

There are no open caveats in Cisco IOS Release 12.2(14)SU2.

Resolved and Closed Caveats—Cisco IOS Release 12.2(14)SU2

This section describes caveats that have been resolved by Cisco IOS Release 12.2(14)SU2.

- CSCeb56909

Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

More details can be found in the security advisory which is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>.

- CSCed15310

Symptoms: On Cisco 7200 routers with NPEs and NSE-1 processors, and on Cisco 7400 routers, a router may crash due to an L3 cache parity error.

Conditions: This symptom is seen in under unpredictable circumstances.

Workaround: The workaround is to disable the L3 cache.

- CSCed40933

Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

More details can be found in the security advisory, which is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>.

- CSCee67450

A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command 'bgp log-neighbor-changes' configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

If a malformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

Cisco has made free software available to address this problem.

For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>

- CSCef46191

A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

The Advisory is available at:

<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>

- CSCef75551

Symptoms: A Cisco 7200 router running IPSec with the TED (Tunnel End-point discovery) feature may crash due to a watchdog timeout.

Conditions: The crash is seen on the IKE responder under stress and scalability conditions when TED is configured.

Workaround: Do not use the TED feature; otherwise there is no known workaround.

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 the physical interface (not the tunnel). 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
  redundancy PRIVATE

!
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
```



Note

The 20.1.+1 addresses are the remote peers.

```
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
 ip unnumbered FastEthernet0/0.1
 tunnel source 172.1.1.100
 tunnel destination 20.1.1.1
!
interface Tunnel2
 ip unnumbered FastEthernet0/0.2
 tunnel source 172.1.2.100
 tunnel destination 20.1.2.1
!
!
```

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

```

interface FastEthernet0/0
 no ip address
 no shutdown
 duplex full
 speed 100
!
interface FastEthernet0/0.1
 encapsulation dot1Q 500
 ip address 172.1.1.6 255.255.255.0
 standby delay minimum 35 reload 60
 standby 1 ip 172.1.1.100
 standby timer 1 3
 standby 1 preempt
 standby 1 name GRE_1
 standby 1 track FastEthernet0/1
 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 35 reload 60
 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
 crypto map gre_2 ssp 100
!
!
interface FastEthernet0/1
 ip address 40.0.0.6 255.255.255.0

 duplex full
 speed 100
 standby delay minimum 35 reload 60
 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_2
 permit gre host 172.1.10.100 host 20.1.2.1

```

Related Documentation

Hardware Documents

Cisco 7200 series router hardware documentation is available on [cisco.com](http://www.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](http://www.cisco.com) at this URL:

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

Obtaining Documentation

Cisco documentation and additional literature are available on [Cisco.com](http://www.cisco.com). Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

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

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

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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



Tip

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support Website

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

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

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

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



Note

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

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

Glossary

Active—Active IPsec High Availability router

DPD—Dead Peer Detection. DPD allows two IPsec peers to determine if the other is still “alive” during the lifetime of a VPN connection.

EzVPN—Cisco Easy Virtual Private Networks (EzVPN) Client on Cisco IOS Software. The Cisco EzVPN client feature can be configured to create IPsec VPN tunnels between a supported router and another Cisco router that supports this form of IPsec encryption/decryption.

GRE—Generic Routing Encapsulation. Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

HSRP—Hot Standby Routing Protocol. HSRP provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

IKE—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPsec) that require keys. Before any IPsec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts or by a CA service.

IPsec—IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

SA—security association. An instance of security policy and keying material applied to a data flow. Both IKE and IPsec use SAs, although SAs are independent of one another. IPsec SAs are unidirectional and they are unique in each security protocol.

SSP—State Synchronization Protocol (SSP) is a protocol developed to transfer state information between the active and standby routers.

Standby—Standby IPsec High Availability router.

Stateful Failover—Feature that enables a backup (standby) router to automatically take over the primary (active) router’s tasks in the event of a active router failure with minimal or no loss of traffic. The remote peer sees no difference between the two routers since it is connected to a virtual end point (VEP), owned by either headend router that shares the same IPsec information.

V3PN—Voice and Video Enabled VPN (V3PN), integrates three core technologies: IP Telephony, Quality of Service (QoS), and IP Security (IPsec) VPN to guarantee the timely delivery of latency-sensitive applications such as voice and video.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0411R)

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