Release Notes for the Cisco Network-Based IPSec VPN Solution Release 1.5

Contents

These release notes discuss the following topics:

- System Requirements, page 2
- Caveats, page 8
- Related Documentation, page 11
- Obtaining Documentation, page 14
- Obtaining Technical Assistance, page 15

Introduction

The Cisco Network-Based IPSec VPN Solution Release 1.5 is a network-based IP security (IPSec) Virtual Private Network (VPN) integrated solution that allows a service provider to offer scalable services to securely connect remote locations to a customer's corporate VPN network.

The Cisco network-based IPSec VPN solution Release 1.5 leverages the Cisco 7200 series router as an IPSec aggregator router or as an IPSec aggregator+provider edge (PE) router to integrate IPSec VPNs into MPLS-based VPNs or Layer 2 VPNs.

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

System Requirements

Hardware and Software Components

The key hardware components for Cisco network-based IPSec VPN solution Release 1.5 are the Cisco 7200 series routers with the Cisco 7200 Series Network Processing Engine (NPE) G1, Cisco 7200 Series Network Processing Engine (NPE) 400, the Integrated Services Adapter (ISA), and the VPN Acceleration Module (VAM).

The following Cisco platforms can be used as customer premises equipment at the remote locations for IPSec termination to the Cisco 7200 series router:

- Cisco PIX Firewall with EzVPN client
- Cisco VPN 3002 hardware client
- Cisco 800 series routers
- Cisco 1700 series routers
- Cisco 2600 series routers
- Cisco 3600 series routers
- Cisco 7200 series routers

See the Related Documentation section for more information on these routers. See Table 1 for information on solution components.

Table 1 Key Cisco Network-Based IPSec VPN Solution Components

Component Type	Hardware	Minimum Software Version Required	Minimum Flash Memory Required (MBs)	Minimum DRAM Memory Required (MBs)
Access concentrators	Cisco 7204	Cisco IOS Release 12.2(15)T	20	128
	Cisco 7206		20	128

Features

Table 2 lists the features for the Cisco network-based IPSec VPN solution Release 1.5.

Determining Software Versions

Cisco IOS Software

To determine the version of Cisco IOS software currently running, log in to the router and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number on the second output line:

```
Router> show version
```

Table 2 Cisco Network-Based IPSec VPN Solution Release 1.5—Supported Features

Feature	Supported Platform	Minimum Cisco IOS Version Required	Reference Documentation
MPLS Virtual Private Networks	Cisco 7200 series routers	Cisco IOS Release 12.0(5)T	MPLS Virtual Private Networks.
	Cisco 7500 series routers		
	Cisco 8540 series (MSR) routers		
	Cisco 8650 series (BPX) routers		
	Cisco 8800 series (MGX) routers		
	Cisco 3640 series routers		
	Cisco 7200 series routers		
	Cisco 7500 series routers		
Easy VPN Remote (Includes Client mode, Network Extension mode, and Xauth)	Cisco 806 router	Cisco IOS Release 12.2(4)YA	Cisco Easy VPN Remote Feature.
	Cisco 826 router		
	Cisco 827 router		
	Cisco 828 router		
	Cisco uBR905 router		
	Cisco uBR925 router		
	Cisco 1700 series routers		
Easy VPN Remote (Includes Manual Tunnel Control and Static NAT Interoperability)	Cisco 806 router	Cisco IOS Release 12.2(4)YJ	Cisco Easy VPN Remote Phase II.
	Cisco 826 router		
	Cisco 827 router		
	Cisco 828 router		
	Cisco uBR905 router		
	Cisco uBR925 router		
	Cisco 1700 series routers		

Table 2 Cisco Network-Based IPSec VPN Solution Release 1.5—Supported Features (continued)

Feature	Supported Platform	Minimum Cisco IOS Version Required	Reference Documentation
Easy VPN Server (Includes: Mode Configuration Version 6 Support, Xauth Version 6 Support, Internet Key Exchange, (IKE) Dead Peer Detection (DPD), Split Tunneling Control, Initial Contact, Group-Based Policy Control)	Cisco 800 series routers	Cisco IOS Release 12.2(8)T	Easy VPN Server.
	Cisco 1400 series routers		
	Cisco 1600 series routers		
	Cisco 1700 series routers		
	Cisco 2600 series routers		
	Cisco 3620 router		
	Cisco 3640 router		
	Cisco 3660 router		
	Cisco 7100 series routers		
	Cisco 7200 series routers		
	Cisco 7500 series routers		
	Cisco uBR905 router		
	Cisco uBR925 router		
IPSec VPN High Availability Enhancements [includes Hot Standby Router Protocol (HSRP) and Reverse Route Injection (RRI)]	Cisco 7100 series routers	Cisco IOS Release 12.1(9)E and Cisco IOS Release 12.2(8)T	IPSec VPN High Availability Enhancements.
	Cisco 7200VXR series routers		
Unicast Reverse Path Forwarding	Cisco 7000 series routers with Route Switch Processor (RSP)	Cisco IOS Release 11.1 CC	Unicast Reverse Path Forwarding.
	Cisco 7200 series routers		
	Cisco 7500 series routers		
	Cisco 12000 series routers		
Distinguished Name Based Crypto Maps	Cisco 1700 series routers	Cisco IOS Release 12.2(4)T	Distinguished Name Based Crypto Maps.
	Cisco 2600 series routers		
	Cisco 3620 routers		
	Cisco 3640 router		
	Cisco 3660 router		
	Cisco 7100 series routers		
	Cisco 7200 series		
	Cisco uBR905 Cable Access Router		
	Cisco uBR925 Cable Access Router		

Table 2 Cisco Network-Based IPSec VPN Solution Release 1.5—Supported Features (continued)

Feature	Supported Platform	Minimum Cisco IOS Version Required	Reference Documentation
VPN Acceleration Module (VAM)	Cisco 7100 series routers	Cisco IOS Release 12.2(13)T	VPN Acceleration Module.
	Cisco 7200 series routers with NPE 400, NPE 300, or NPE 225		
	Cisco 7401ASR Router		
Prefragmentation for IPSec	Cisco 1710 router	Cisco IOS Release 12.2(13)T	Pre-Fragmentation for IPSec VPNs.
	Cisco 1720 router		
	Cisco 1721 router		
	Cisco 1751 router		
	Cisco 1760 router		
	Cisco 2600 router		
	Cisco 2691 router		
	Cisco 3620 router		
	Cisco 3640 router		
	Cisco 3660 router		
	Cisco 3725 router		
	Cisco 3745 router		
	Cisco 7100 series routers		
	Cisco 7200 series routers		
	Cisco 7400 series routers		
IPSec NAT Transparency	For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.	Cisco IOS Release 12.2(13)T	IPSec NAT Transparency.
Per VRF AAA	For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.	Cisco IOS Release 12.2(13)T	Per VRF AAA.

Table 2 Cisco Network-Based IPSec VPN Solution Release 1.5—Supported Features (continued)

Feature	Supported Platform	Minimum Cisco IOS Version Required	Reference Documentation
IPSec Security Association Idle Timers	Cisco 1700 series access routers	Cisco IOS Release 12.2(15)T	IPSec Security Association Idle Timers.
	Cisco 2400 series integrated access devices		
	Cisco 2600 series multiservice platforms		
	Cisco 3600 series multiservice platforms		
	Cisco 3700 series multiservice access routers		
	Cisco 7100 series VPN routers		
	Cisco 7200 series routers		
	Cisco 7400 series routers,		
	Cisco 7500 series routers		
	Cisco 801-804 ISDN routers		
	Cisco 805 serial router		
	Cisco 806 broadband router		
	Cisco 811 router		
	Cisco 813 router		
	Cisco 820 router		
	Cisco 827 ADSL router		
	Cisco 828 G.SHDSL router		
	Cisco 8850 RPM		
	Cisco AS5350 universal gateway		
	Cisco 950		
	Cisco AS5400 series universal gateways		
	Cisco integrated communications system 7750		

Table 2 Cisco Network-Based IPSec VPN Solution Release 1.5—Supported Features (continued)

Feature	Supported Platform	Minimum Cisco IOS Version Required	Reference Documentation
IPSec Security Association Idle Timers (continued)	Cisco MC3810 series multiservice access concentrators		
	Cisco ubr7200		
	Cisco ubr900 series cable access routers		
IPSec VPN Accounting	Cisco 2610 through 2613 routers	Cisco IOS Release 12.2(15)T	IPSec VPN Accounting.
	Cisco 2620 through 2621 routers		
	Cisco 2650 through 2651 routers		
	Cisco 3620 router		
	Cisco 3640 router		
	Cisco 3660 router		
	Cisco 3725 router		
	Cisco 3745router		
	Cisco 7100 router		
	Cisco 7200 router		
	Cisco 7400 router		
	Cisco ubr7100 router		
	Cisco ubr7200 router		
VRF Aware IPSec	Cisco 1710 router	Cisco IOS Release 12.2(15)T	VRF-Aware IPSec.
	Cisco 1760 router		
	Cisco 2610 through 2613 routers		
	Cisco 2620 through 2621 routers		
	Cisco 2650 through 2651 routers		
	Cisco 3620 router		
	Cisco 3640 router		
	Cisco 3660 router		
	Cisco 7100 router		
	Cisco 7200 router		
	Cisco 7400 router		

Table 2 Cisco Network-Based IPSec VPN Solution Release 1.5—Supported Features (continued)

Feature	Supported Platform	Minimum Cisco IOS Version Required	Reference Documentation
IOS Server Load Balancing	Catalyst 6000 family switches with Supervisor Engine 1	Cisco IOS Release 12.1(13)E	IOS Server Load Balancing.
	Catalyst 6000 family switches with Supervisor Engine 2		
	Cisco 7100 series routers		
	Cisco 7200 series routers		

```
Cisco Internetwork Operating System Software
IOS (tm) 12.1 Software c5300-i-mz, Version 12.1(6), RELEASE SOFTWARE
```

Caveats

Open Caveats—Cisco Network-Based IPSec VPN Solution 1.5

Table 3 Open Caveats

Identifier	Description	Explanation/Workaround
CSCdz75630	Configuring IPSec to MPLS solution with the IP addresses on the interface facing the MPLS-PE and the pool addresses in the same subnet causes an ARP resolution problem in the VRF. This prevents traffic flow.	Add a static arp entry on the IPSec concentrator for the IP address on the MPLS-PE.
CSCdy73051	There are no VRF aware **show** commands to help troubleshoot problems.	New feature request.
CSCdy37971	The IPSec MIB stores extraneous data in the IKE peer table and returns the same extraneous data when SNMP get requests are issued.	None.
CSCdz13072	Fragmentation is not working for GRE IP to MPLS packets in the CEF path. This is because MPLS fragmentation is not supported into GRE tunnels.	Configure "tag mtu 65000" on both ends of the GRE tunnel.

Table 3 Open Caveats (continued)

Identifier	Description	Explanation/Workaround
CSCdz15390	Packets are not forwarded from IPSec to MPLS when software crypto is used on a router acting as an IPSec aggregator and an MPLS PE.	Use hardware encryption.
CSCea07470	In the site-to-site IPSec VPN Solution for Service Providers, when the CPE is performing fragmentation before encryption, there is no problem. But when the CPE is performing fragmentation after encryption, some packets are routed through the GRF interface of the concentrator.	None.

Resolved Caveats—Cisco Network-Based IPSec VPN Solution 1.5

Table 4 Resolved Caveats

Identifier	Description
CSCea15720	Previously, when trying to download configuration from the ftp server, the router failed. This caveat is resolved.
CSCdz43074	Pings greater then 1501 failed across an MPLS cloud. This caveat is resolved.
CSCea26264	Previously, the system was unable to disable NAT transparency. The **no crypto ipsec nat-transparency udp-encaps** command did not work. This caveat is resolved.
CSCea30557	Previously, you could not use UDP-NAT transparency between routers A and B, if router D (router that performs the NAT) had a crypto map enabled on its interface. This caveat is resolved.
CSCea20022	Previously, a Cisco 7200 router incorrectly used a local UDP port of 0 (instead of 500) when initiating an IKE rekey. This caveat is resolved.
CSCdy24844	Previously, the volume of crypto traffic (as inferred from the remaining volume lifetime of the IPSec SAs) was twice the correct value for inbound IPSec SAs. This means that the SAs expired two times faster than they should. This caveat is resolved.
CSCdz02826	Previously, in a Multiprotocol Label Switching (MPLS) environment, decoupling the crypto map from a physical interface for generic route encapsulation (GRE) tunnels sometimes did not function properly. This caveat is resolved.
CSCdx34698	Previously, Cisco Express Forwarding (CEF) per-destination load sharing did not work for IPSec+generic routing encapsulation (GRE). CEF on the Cisco 7200 shows per-packet load-balancing, but the packets were not load balanced on each tunnel. Removing IPSec and using simple GRE caused packets to be load-balanced on a per-packet basis. This caveat is resolved.
CSCdz46552	In Cisco IOS Release 12.2T, if a dynamic crypto map without an ACL existed, and if the user configured an access-list on the router, the existing remote-access VPN that was connected through that dynamic crypto map stopped working. This caveat is resolved.
CSCdy35419	If a fast Ethernet interface or subinterface was in a VRF, the **crypto map <name> redundancy <name>** command was not accepted as a valid command. This caveat is resolved.
CSCdx49948	Previously, RRI did not have an option to inject routes for public addresses or IPSec tunnel destination addresses into the routing table. This caveat is resolved.

Table 4 Resolved Caveats (continued)

Identifier	Description
CSCdv58874	Multiprotocol Label Switching (MPLS) failed to check for a crypto map on the outbound interface mapped to a VRF instance. This caveat is resolved.
CSCdw30566	CEF did not work with GRE; fast switching worked fine. With CEF on, packets were being process-switched. This caveat is resolved.
CSCdw30616	Previously, if you applied a crypto map using the same map tag to more than one interface, you could encounter a problem if the keyword redundancy was used on some maps and not on others. This caveat is resolved.
CSCdw67009	Previously, a Cisco router could experience a spurious memory condition and generate traceback messages when it attempted to establish an IPSec tunnel. This condition occurred when Cisco IOS Release 12.2(7.6)T1 was running with light traffic. This caveat is resolved.
CSCdw70494	Previously, CPU utilization on Cisco 7200 series router with multiple IPSec/GRE tunnels using Frame Relay encapsulation could reach 100 percent at about 22 Mbps of traffic for four tunnels. This caveat is resolved.
CSCdw82915	In Release 12.2(8)T of Cisco IOS, when you defined a VPN group for remote access clients (such as the Cisco VPN Client 3.X), this group profile information was global to the router. This means that any client initiating a VPN connection to the router could be authorized through the interface that the tunnel request was received on. This caveat is resolved.
CSCdx16321	On a Cisco 7206VXR router running Release 12.1(11b)E with GRE/IPSec tunnels and certain SNMP traps enabled, spurious memory accesses and alignment errors occurred with the following SNMP traps enabled: • snmp-server enable traps ipsec tunnel start • snmp-server enable traps ipsec tunnel stop This caveat is resolved.
CSCdx19963	A VPN unity client (Version 3.5) failed to establish an IPSec session to a Cisco IOS IPSec gateway running Cisco IOS Release 12.2(8.5)T or later if the group profile contained the Tunnel-Type or Tunnel-Medium-Type IETF tunnel attributes. This caveat is resolved.
CSCdx51540	The route to the client IP address which was installed through RRI in the VRF was removed when the IPSec security agreements were rekeyed. This induced connectivity loss for the client with the rest of the VPN network. This caveat is resolved.
CSCdx68629	CEF switching did not work with IPSec + Network Address Translator Traversal (NAT-T). This caveat is resolved.
CSCdv53287	With two VRFs on a Cisco 7200 router with IPSec, two unique routing tables work at a lower packets per second (PPS). Increasing PPS caused the router running 12.2.1 to drop packets. This caveat is resolved.
CSCdw63632	In Cisco IOS Release 12.2(8)T a wildcard mask value is appended to the **crypto isakmp key <key> address** command. This mask is automatically added for the case of the wildcard address so the command becomes **crypto isakmp key <key> address 0.0.0.0 0.0.0.0**. This caveat is resolved.
CSCdx35000	Easy VPN clients cannot connect to the router if the **crypto isakmp key** command is used with a 0.0.0.0 address and the no-xauth option. This caveat is resolved.
CSCdx77257	A security issue affected VPN routing/forwarding (VRF) VPN configurations for both site-to-site (preshare keys used with no-xauth) and remote-access (dynamic crypto). This caveat is resolved.
CSCdx95503	A user of one VPN could connect to another customer's Virtual Private Network (VPN) because Extended Authentication (Xauth) was a global procedure. This caveat is resolved.

Table 4 Resolved Caveats (continued)

Identifier	Description
CSCdx31123	ISA returned “Error isa_rx_error: 1204” for a packet that indicated a faulty ESP pad value when the packet was not faulty. This could result in a GRE keep-alive failure and, consequently, a failed GRE tunnel. This caveat is resolved.
CSCdx27415	Reverse route injection (RRI) tried to inject a route with an incorrect mask for the network behind an EZVPN client if the client used network extension mode. This caveat is resolved.

Related Documentation

The following sections show the related documentation available for the Cisco network-based IPSec VPN solution Release 1.5.

Platform-Specific Documents

Platform Release Notes

The platform release notes listed in the following sections are available for the Cisco network-based IPSec VPN solution Release 1.5:

Cisco 800 Series Router Release Notes

Fixed Configuration Access Routers

- Release Notes for Cisco 801-804 Routers

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/800/800rlnts/index.htm
- Release Notes for the Cisco 805 Router

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/805/805rlnts/index.htm
- Cisco 806 Router Release Notes

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/806/806rns/index.htm
- Release Notes for Cisco 811-813 Routers

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/811-813/800rn/index.htm
- *Release Notes for Cisco 826 and SOHO 76 Routers*

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/826/826rn.htm
- *Release Notes for Cisco 827 Routers*

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/827/827rlnts/index.htm
- *Cisco 828 Router*

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/828/828rlsnt.htm

Cisco 1700 Series Router Release Notes

Modular Access Routers

- Cisco 1700 Series Router Release Notes

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1700rlsn/index.htm

Cisco 1710 Routers

- *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(4)XM*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/1700/rn1700xm.htm
- *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(4)YA*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/1700/1700ya/rn1700ya.htm

Cisco 1720 Series Routers

- Cisco 1720 Series Router Release Notes

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1720/1720rlsn/index.htm

Cisco 1721 Access Router

- *Release Notes for Cisco 1721 Routers*

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1721/1721rn.htm

Cisco 1750 Series Routers

- Cisco 1750 Series Router Release Notes

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1750/1750rlsn/index.htm

Cisco 1751 Series Routers

- Cisco 1751 Router Release Notes

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1751/1751rlsn/index.htm

Cisco 1760 Series Routers

- Cisco 1760 Router Release Notes

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1760/1760rlsn/index.htm

Cisco 2600 Series Router Release Notes

Cisco 2600 Series Routers

- Cisco IOS Release Notes

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/rn2600/index.htm

Cisco 3600 Series Router Release Notes

Cisco 3600 Series Routers

- Cisco IOS Release Notes

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/rn/index.htm

Cisco IOS Software Release Notes and Documentation

- *Release Notes for Cisco IOS Release 11.2(11)P Feature Packs---7200 Series Routers*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/fp112rn/4837_02.htm
- *Release Notes for Cisco 7200 Series for Cisco IOS Release 11.3 AA*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/ios113p/7000fam/rn7200aa.htm

Cisco VPN 3002 Hardware Client

VPN 3002

- *Release Notes for Cisco VPN 3002 Hardware Client Release 3.5*
  http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/3_5/3002pdf.pdf
- *Release Notes for Cisco VPN 3002 Hardware Client Release 3.5.2*
  http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/3_5/3002_352.pdf
- *Release Notes for Cisco VPN 3002 Hardware Client Release 3.0*
  http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/3_0/3002rn.pdf

Platform Documentation

The following platform documents are available for the Managed IPSec CPE VPN Solution:

Cisco 800 Series Routers

Fixed Configuration Access Routers

- Cisco 801–804 Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/800/index.htm
- Cisco 805 Router
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/805/index.htm
- Cisco 806 Router
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/806/index.htm
- Cisco 811 and Cisco 813 Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/811-813/index.htm
- Cisco 826 Router
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/826/index.htm
- Cisco 827 Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/827/index.htm
- Cisco 828 and SOHO 78 Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/828/index.htm

Cisco 1700 Series Routers

Modular Access Routers

- Cisco 1700 Series Router
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/index.htm
- Cisco 1710 Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1710/index.htm
- Cisco 1720 Series Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1720/index.htm
- Cisco 1721 Access Router
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1721/index.htm
- Cisco 1750 Series Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1750/index.htm
- Cisco 1751 Series Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1751/index.htm
- Cisco 1760 Series Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1760/index.htm

Cisco 2600 Series Routers

- Cisco 2600 Series Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/index.htm

Cisco 3600 Series Routers

- Cisco 3600 Series Routers
  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/index.htm

Cisco 7200 Series Routers

- Cisco 7202
  http://www.cisco.com/univercd/cc/td/doc/product/core/7202/index.htm
- Cisco 7204
  http://www.cisco.com/univercd/cc/td/doc/product/core/7204/index.htm
- Cisco 7206
  http://www.cisco.com/univercd/cc/td/doc/product/core/7206/index.htm
- Cisco 7200 VXR
  http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/index.htm

Cisco VPN 3002 Hardware Client

VPN 3002

- VPN 3002 Hardware Client Release 3.5.2

http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/3_5/index.htm

- VPN 3002 Hardware Client Release 3.1

  http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/3_1_/index.htm

- VPN 3002 Hardware Client Release 3.0

  http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3002/3_0/index.htm

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 you call, 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, have your service agreement number and your product serial number available.

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.