



Frequently Asked Questions for Cisco Routers

[Home](#) > [Work With My Routers](#) > [Cisco Routers](#) > Frequently Asked Questions for Cisco Routers

Frequently Asked Questions for Cisco Routers

- [Introduction](#)
- [Requirements](#)
- [Frequently Asked Questions \(FAQ\)](#)

- [What are the different types of passwords available and how to configure them on Cisco routers?](#)
 - [How can I reset the passwords on a Cisco router?](#)
 - [How can I use Security Device Manager with my Cisco routers?](#)
 - [Can I manage the EtherSwitch service modules using the Cisco Router and Security Device Manager \(SDM\)?](#)
 - [What WAN optimization solutions do Cisco routers offer?](#)
 - [What are all the Communication services available on Cisco 2800 series and 3800 Series Routers?](#)
 - [What are all the IP Communication services available on Cisco 2800 series and 3800 series routers?](#)
 - [What are all the Security services available in Cisco Integrated Service Routers?](#)
 - [What is Cisco Configuration Professional \(CCP\)?](#)
 - [What is Cisco IOS Content Filtering?](#)
 - [What is Cisco IOS Intrusion Prevention System \(IPS\)?](#)
 - [What is Cisco IOS SSL VPN and what do I need to enable Cisco IOS SSL VPN on my Cisco router?](#)
 - [How does the licensing work for Cisco IOS SSL VPN?](#)
 - [Can I implement both IP Security \(IPsec\) and SSL VPN in my network?](#)
 - [What platforms does Cisco IOS SSL VPN support?](#)
- [Related Information](#)

Download PDF

 [Frequently Asked Questions for Cisco Routers](#)

Service Requests

- [Open a service request](#)
- [Update a service request](#)

Feedback

Please rate this site:

○ ++ ○ + ○ +/- ○ - ○ --

Suggestions for improvement:

If Cisco may contact you for more details or for future feedback opportunities, please enter your contact information:

Full Name:

Email:

Introduction

This document answers some of the frequently asked questions (FAQ) for Cisco Routers.

[Back to Top](#)

Requirements

There are no prerequisites for this document.

[Back to Top](#)

Frequently Asked Questions (FAQ)

What are the different types of passwords available and how to configure them on Cisco routers?

These are the different types of passwords:

- Telnet (VTY Line)
- Console Line
- Auxiliary Line
- Enable
- Enable Secret
- Local User Specific For configuring these passwords, refer to [Configure Different Types of Passwords on the Cisco Router](#).

How can I reset the passwords on a Cisco router?

For resetting the passwords on a Cisco router, refer to [Manually Reset the Password on a Cisco Router](#).

How can I use Security Device Manager with my Cisco routers?

To download and install Security Device Manager (SDM), refer to [Download and Install Security Device Manager](#). To use SDM for configuring Cisco router, refer to [Configure Your Router with Security Device Manager](#).

Can I manage the EtherSwitch service modules using the Cisco Router and Security Device Manager (SDM)?

SDM version 2.2 supports routers with the EtherSwitch service modules installed. SDM allows the administrator to configure the internal Gigabit Ethernet interface for the module, and launch the Switch Device Manager to configure the module itself.

What WAN optimization solutions do Cisco routers offer?

WAN optimization is the ability to improve the performance of business applications over WANs, and includes monitoring and diagnostics, traffic management, compression, and caching. Cisco has the broadest range of technologies and products to address both generic and application-specific WAN optimization challenges.

The Cisco WAN optimization solutions offer the industry's most integrated, yet flexible and cost-effective bandwidth management solutions. An integrated services solution in the branch router is the logical point of consolidation for WAN

optimization technologies, such as compression, caching, wide-area application services, quality of service (QoS), and access control, because it sits at the WAN/LAN interface where bottlenecks can efficiently be mitigated and critical network services (voice over IP [VoIP], security, QoS, and Multiprotocol Label Switching [MPLS]) need to be deployed. Cisco Layer 2 integrated compression, combined with a content engine object, and sequence caching module, provide WAN bandwidth management that improves application response time on congested links by reducing the amount of data sent across the WAN. Layer 2 compression provides many benefits over standalone compression appliances by providing a tightly integrated solution that interoperates with critical Cisco IOS Software features and services such as QoS, policy-based routing (PBR), network-based application recognition (NBAR), Network Address Translation (NAT), and access control lists (ACLs).

Cisco WAN optimization solutions are available in Cisco 2800 series and Cisco 3800 series routers.

What are all the Communication services available on Cisco 2800 series and 3800 Series Routers?

This table summarizes the primary Wireless services supported on the integrated services routers.

Features	Cisco 3800 series	Cisco 2800 series	Cisco 1841
WLAN Connectivity (Integrated Access Point)	Yes	Yes	Yes
Public WLAN Hotspot	Yes	Yes	Yes
Wireless Infrastructure Services	Yes	Yes (except 2801)	No
Wireless LAN Controller Functionality	Yes	Yes (except 2801)	No
PoE	Yes	Yes	No
Voice WLAN & Wired IP Telephony	Yes	Yes	No
Land Mobile Radio (LMR) over IP	Yes	Yes	No

What are all the IP Communication services available on Cisco 2800 series and 3800 series routers?

This list summarizes the primary IP Communication services available in Cisco 2800 series and 3800 series routers:

- Cisco CallManager voice gateway
- Cisco CallManager Express, Cisco Unity Express, Cisco SRST
- Cisco CallManager Ad Hoc Conferencing and Transcoding
- Digital T1, E1, BRI and analog FXS, FXO, E&M, CAMA, DID telephony interfaces
- MGCP, H.323, SIP call control protocols
- Voice, Video, VPN (V3PN)

What are all the Security services available in Cisco Integrated Service Routers?

This list summarizes the primary Security services available in Cisco 800 series, 1800 series, 2800 series and 3800 series routers:

Cisco VPN

- Group Encrypted Transport VPN
- Dynamic Multipoint VPN
- Easy VPN Remote & Server
- MPLS VPN
- Multi-VRF and MPLS Security Contexts
- Secure Provisioning & Digital Certificates
- Voice & Video Enabled VPN (V3PN)
- Virtual Tunnel Interface
- SSL VPN

Cisco IOS Firewall

- Application Firewall
- Transparent Firewall
- VRF-Aware Firewall
- Firewall for secure Unified communications

Cisco IOS Intrusion Prevention System (IPS)

- Inline IPS
- Transparent IPS
- Flexible Packet Matching

Cisco Network Foundation Protection (NFP)

- AutoSecure
- Control Plane Policing
- CPU / Memory Thresholding
- Network Based Application Recognition (NBAR)
- NetFlow
- Role based CLI access

- SSH v2
- SNMP v3

Cisco Network Admission Control (NAC)

Addition Security Features

- Authentication, Authorization & Accounting (AAA)
- Cisco IOS Certificate Server & Client
- Standard 802.1x support with integrated switching
- Cisco IOS Content Filtering

Secure Management

- Cisco Configuration Professional
- Enterprise Security Management
 - Cisco Security Manager
 - Cisco Security Monitoring, Analysis, and Response System (CS-MARS)
 - Cisco IP Solution Center (ISC)

What is Cisco Configuration Professional (CCP)?

Cisco Configuration Professional is a valuable, productivity-enhancing tool for network administrator, and channel partners deploying routers in medium-sized businesses and enterprise branch offices. Cisco Configuration Professional allows them to implement router, unified communications, security, and wireless network configurations with reduced cost and increased confidence and ease. Further, Cisco Configuration Professional configurations have been approved by the Cisco Technical Assistance Center (TAC). Cisco Configuration Professional also helps customers avoid potential network issues by proactively monitoring router performance statistics, system logs, and security logs in real time. Reduce Total Cost of Ownership By relying on best-practice configurations approved by the Cisco Technical Assistance Center (TAC), customers can:

1. Lower the total cost of ownership of Cisco routers
2. Reduce human errors
3. Simplify initial setup in voice deployments
4. Help ensure proper linkage between users, dialing plans, and voicemail settings.

Cisco Configuration Professional offers smart wizards and advanced configuration support for Cisco LAN and WAN interfaces, Network Address Translation (NAT), stateful and application firewall policy, IPS, IPsec VPN, QoS, and NAC policy features.

Cisco Configuration Professional assumes a general understanding of networking technologies and terms but assists individuals unfamiliar with the Cisco CLI.

For more information about the Cisco Configuration Professional, visit <http://www.cisco.com/go/ccp>.

What is Cisco IOS Content Filtering?

Unrestricted Internet use exposes organizations to needless risks such as inappropriate use of company resources, legal liability, and productivity losses. As internet threats get more complex, solutions that not only improve employee productivity but also prevent malware and malicious traffic, become increasingly essential. Part of the Cisco IOS Integrated Threat Control framework, this solution.

Cisco IOS Content Filtering helps your organization protect itself from known and new Internet threats, improve employee productivity, and enforce business policies for regulatory compliance.

Part of the Cisco IOS Integrated Threat Control framework, this solution:

- Monitors and regulates all Internet activities by blocking or restricting access to certain Websites
- Provides protection from malicious sites that are known to give out malware, adware, spyware, and phishing
- Is simple and easy to deploy, helping your organization better manage network resources

For more information on Cisco IOS Content Filtering, refer to [Cisco IOS Content Filtering](#).

What is Cisco IOS Intrusion Prevention System (IPS)?

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection feature that effectively mitigates a wide range of network attacks. A component of the Cisco IOS Integrated Threat Control framework and complemented by Cisco IOS Flexible Packet Matching feature, Cisco IOS IPS provides your network with the intelligence to accurately identify, classify, and stop or block malicious traffic in real time.

Benefits:

1. Increased network availability — Provides network wide, distributed protection from many attacks, exploits, worms, and viruses
2. Faster remediation — Pinpoints the source of network attacks faster and takes corrective actions closest to the attack
3. Deployment flexibility — Offers inline inspection of traffic through any combination of the router's LAN and WAN interfaces with field-customizable worm and attack signature sets and event actions that adjust automatically based on risk level
4. Comprehensive threat protection — Works with Cisco IOS Firewall, control-plane policing, and other Cisco IOS Software security features.

For more information on Cisco IOS Intrusion Prevention System, refer to [Cisco IOS Intrusion Prevention System](#).

For configuring Cisco IPS on your routers, refer to, [Configure IOS IPS on Your Router using SDM](#)

What is Cisco IOS SSL VPN and what do I need to enable Cisco IOS SSL VPN on my Cisco router?

Secure Sockets Layer (SSL)-based VPN is an emerging technology that provides remote-access connectivity from almost any Internet-enabled location using a Web browser and its native SSL encryption. SSL VPN provides the flexibility to support secure access for all users, regardless of the endpoint host from which they are establishing the connection. Cisco IOS SSL VPN does not require a VPN client to be preinstalled on the endpoint host.

The Cisco IOS SSL VPN comprehensive feature set is available with the Advanced Security and higher images starting with Cisco IOS Software Release 12.4(6)T (Base IP image doesn't include this functionality). All Cisco IOS SSL VPN features are included in a single, cost-effective license that would be purchased separately.

For configuring Cisco IOS SSL VPN on your router, refer to,

[Configure Clientless SSL VPN \(WebVPN\) on a Cisco Router with Security Device Manager](#)

[Configure Thin-Client SSL VPN \(WebVPN\) on a Cisco Router with Security Device Manager](#)

How does the licensing work for Cisco IOS SSL VPN?

The Cisco IOS SSL VPN licenses are cost-effective paper licenses. There's no software key to enable the feature hence, there is no support issue with using Cisco IOS SSL VPN once you have the Advanced Security or higher Cisco IOS image loaded on the Router. You can purchase the Feature license as a spare in packs of 10, 25 and 100 simultaneous users directly from Cisco.com configuration tool.

Can I implement both IP Security (IPsec) and SSL VPN in my network?

In many cases, IPsec and SSL VPN are complementary, because they solve different problems. This complementary approach allows a single device to address all remote-access user requirements. SSL allows you to secure clients independently, but remote sites with multiple PCs can use Cisco Easy VPN technology, taking advantage of IPsec.

What platforms does Cisco IOS SSL VPN support?

The Cisco IOS SSL VPN is supported on the Cisco 1800, 2800, and 3800 routers running Advanced security images of Cisco IOS Software Release 12.4(6)T.

[Back to Top](#)

Related Information

- [Router Support Page](#)
- [Site Survey](#)