

Use Format Conventions for Technical Tips and Other Content

Contents

[Introduction](#)

[General Conventions](#)

[Text](#)

[Alert Messages and Icons](#)

[Cisco IOS® Software Commands](#)

[Configuration Examples](#)

[IP Addresses](#)

[IP Address Reference](#)

[Comments in Code Blocks](#)

[Related Information](#)

Introduction

This document describes the formats for text, image, and command conventions used in Cisco technical tips and content.

General Conventions

The general conventions must be followed for:

- Text
- Alerts and Icons
- Cisco IOS® Software Commands
- Configuration Examples
- IP Addresses (Please use caution here.)
- Comments in Code Blocks

Text

- Bold indicates text the user must enter or select, such as menu items, buttons, and commands.
- Italics indicate emphasis.
- The forward angle bracket (>) indicates the progression of menu choices the user must select in a graphical user interface (GUI), such as File > Print.
- Output examples from Cisco devices are displayed in Courier font; for example (commands are in bold, do not use color other than black):

```
3524x1# show running-config  
Building configuration...
```

Current configuration:

```
!  
version 12.0  
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!
```

- System error messages from Cisco devices are displayed in Courier font; for example:
- A router restarted with the reload command displays the `System returned to ROM by reload` message.


Alert Messages and Icons

Note: Means reader take note. Notes contain helpful suggestions or references to material not covered in the document. It is recommended that you read any Note within the article.

Tip: Means this information can help you solve a problem. The tips information cannot be a suggested way to troubleshoot information or even an action, but could be useful information. Tips are optional reading.

Caution: Means reader be careful. In this situation, your action could result in equipment damage or loss of data. You must read Caution statements.

Warning: Warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry. You must be familiar with standard practices for accident prevention. To see translated versions of the warning, refer to the Regulatory Compliance and Safety document that accompanied your device. You must read Warning statements.

The exit icon  shows that you are about to exit the Cisco website. This image appears at the end of a link to websites external to Cisco.com and opens in a separate browser window. Cisco is not responsible for the content of other websites.

Cisco IOS[®] Software Commands

The next conventions for Cisco IOS commands are also used in the command reference guides. For more information about conventions in Cisco IOS documentation, refer to the [Cisco Technical Content Style Guide](#) .

- Vertical bars (|) separate alternative, mutually exclusive arguments. Example: `req-qos {best-effort | controlled-load | guaranteed-delay}`
- Square brackets ([]) indicate optional elements. Example: `[no] ip route-cache [cbus]`
- Braces ({ }) indicate a required choice. Example: `access-list number [{permit | deny}]`
- Braces within square brackets ([{ }]) indicate required choices within optional elements.

- Angle brackets (< >) indicate arguments in contexts that do not allow italics, and in examples indicate character strings a user enters that do not appear on the screen (for example, a password).
- Bold indicates commands and keywords.
- Italics indicate user variables.

Configuration Examples

Generic router names, hostnames, usernames, passwords, and IP addresses are used in configuration examples. These must be replaced with the names, passwords, and addresses appropriate for your company.

Caution: Do not use username **cisco** or password **cisco** in your configurations. To use **cisco** as a password or username, or to use any trivial password, is a security risk. Also note, it is not recommended that you include **Cisco** in the article title.

- Router names: RouterX, nasX, and so on.
- Phone numbers: 555nnnn

IP Addresses

Caution: IP addresses conform to [RFC 1918](#) definitions of private network addresses. See image below. There has been a recent breach due to a client IP address exposed in a **Cisco.com** article. Use judgment and caution when you include an IP address anywhere in your article. Check your images for IP addresses that could be in violation of this.

Three blocks of IP addresses are reserved by the Internet Assigned Numbers Authority (IANA) for private Internets:

- Range: 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- Range: 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- Range: 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

IP Address Reference

IPv4 Addresses Reserved for Public Documentation

IPv4 Unicast Addresses

[RFC 5737](#), *IPv4 Address Blocks Reserved for Documentation*, references previous RFCs (including [RFC 1918](#), *Address Allocation for Private Internets*, and [RFC 3330](#), *Special-Use IPv4 Addresses*) and assigns the following IPv4 address blocks for use in technical content and examples of code:

Address Block	Host Starting Address	Host Ending Address	Broadcast Address	Subnet Mask
192.0.2.0/24	192.0.2.1	192.0.2.254	192.0.2.255	255.255.255.0
198.51.100.0/24	198.51.100.1	198.51.100.254	198.51.100.255	255.255.255.0
203.0.113.0/24	203.0.113.1	203.0.113.254	203.0.113.255	255.255.255.0

IPv4 Addresses Reserved by Cisco

Cisco has acquired three blocks of IPv4 addresses that are reserved for documentation. These addresses allow writers to show complex network configurations. Each block includes a subnet. If you use the following IPv4 addresses in documentation, you must also include the subnet mask:

Address Block	Host Starting Address	Host Ending Address	Broadcast Address	Subnet Mask
209.165.200.224/27	209.165.200.225	209.165.200.254	209.165.200.255	255.255.255.224
209.165.201.0/27	209.165.201.1	209.165.201.30	209.165.201.31	255.255.255.224
209.165.202.128/27	209.165.202.129	209.165.202.158	209.165.202.159	255.255.255.224

Private IPv4 Addresses

[RFC 1918](#) provides a group of IPv4 addresses that are never assigned publicly and are not routed through the public internet, as listed in the following table. The same pool of addresses can be used within any private network (a network that does not communicate with the internet or with other private networks, or communicates only through gateways that translate the address).

Address Block	Host Starting Address	Host Ending Address	Broadcast Address	Subnet Mask
10.0.0.0/8	10.0.0.1	10.255.255.254	10.255.255.255	255.0.0.0
172.16.0.0/12	172.16.0.1	172.31.255.254	172.31.255.255	255.240.0.0
192.168.0.0/16	192.168.0.1	192.168.255.254	192.168.255.255	255.255.0.0

Note: Automatic Private IP Addressing (APIPA) uses addresses that range from 169.254.0.0 through 169.254.255.255. Although these addresses are safe, their use in Cisco documentation is not recommended.

IP Addresses Reserved for Public Documentation

Comments in Code Blocks

Often comments are included in the configuration examples. Comments are italicized. They must be shown as black text only; colors are unacceptable except when they appear in a screen shot. They provide more information about the configuration output and commands used. Configuration comments appear similar to:

```
!--- Define IPsec traffic of interest.
!--- This line covers traffic between the LAN segment behind two PIXes.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind PIX 515. access-
list 101 permit ip 172.18.124.0 255.255.255.0 10.99.99.0 255.255.255.0
```

Note: It is recommended that you shorten codeblock examples so that no slider appears at the end of the example.

Related Information

- [RFC 1918](#)
- [Cisco Technical Content Style Guide](#)
- [Cisco Technical Support & Downloads](#)