

Verwenden von Formatkonventionen für technische Tipps und andere Inhalte

Inhalt

[Einleitung](#)

[Allgemeine Konventionen](#)

[Text](#)

[Warnmeldungen und Symbole](#)

[Cisco IOS® Software-Befehle](#)

[Konfigurationsbeispiele](#)

[IP-Adressen](#)

[IP-Adressreferenz](#)

[Kommentare in Codeblöcken](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Formate für Text, Bild und Befehlskonventionen beschrieben, die in den technischen Tipps und Inhalten von Cisco verwendet werden.

Allgemeine Konventionen

Die allgemeinen Konventionen müssen eingehalten werden für:

- Text
- Warnungen und Symbole
- Cisco IOS® Software-Befehle
- Konfigurationsbeispiele
- IP-Adressen (Vorsicht!)
- Kommentare in Codeblöcken

Text

- Fett steht für Text, den der Benutzer eingeben oder auswählen muss, z. B. Menüelemente, Schaltflächen und Befehle.
- Kursiv gedruckt bedeutet Hervorhebung.
- Die spitze Klammer (>) gibt den Verlauf der Menüoptionen an, die der Benutzer in einer grafischen Benutzeroberfläche (GUI) auswählen muss, z. B. Datei > Drucken.
- Ausgabebeispiele von Cisco Geräten werden in der Courier-Schriftart angezeigt; z. B. (Befehle sind fett formatiert, verwenden Sie keine andere Farbe als Schwarz):

Building configuration...

Current configuration:

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

- Systemfehlermeldungen von Cisco Geräten werden in der Courier-Schriftart angezeigt.
Beispiel:
- Ein Router, der mit dem Befehl reload neu gestartet wurde, zeigt die Meldung an, dass das System durch Neuladen zum ROM zurückgeleitet wurde.

Warnmeldungen und Symbole

Hinweis: Bedeutet, dass der Leser dies zur Kenntnis nehmen muss. Hinweise enthalten nützliche Vorschläge oder Verweise auf Material, das nicht in diesem Dokument behandelt wird. Es wird empfohlen, dass Sie alle Notizen in diesem Artikel lesen.

Tipp: Bedeutet, dass diese Informationen Ihnen bei der Lösung eines Problems helfen können. Die Tipps können keine empfohlene Methode zur Fehlerbehebung von Informationen oder einer Aktion sein, sondern können nützliche Informationen sein. Tipps sind optionales Lesen.

Vorsicht: Das bedeutet, dass der Leser vorsichtig sein muss. In dieser Situation kann Ihre Aktion zu Schäden an den Geräten oder zu Datenverlust führen. Sie müssen die Anweisungen zur Vorsicht lesen.

Warnung: Warnung bedeutet Gefahr. Sie befinden sich in einer Situation, die zu körperlichen Verletzungen führen könnte. Bevor Sie an einem Gerät arbeiten, müssen Sie sich der Gefahren bewusst sein, die mit elektrischen Schaltkreisen verbunden sind. Sie müssen mit den gängigen Verfahren zur Unfallverhütung vertraut sein. Übersetzte Versionen der Warnung finden Sie im Dokument Regulatory Compliance and Safety (Gesetzliche Auflagen und Sicherheit), das Ihrem Gerät beiliegt. Sie müssen Warnhinweise lesen.

Das Symbol zum Beenden  zeigt, dass Sie kurz davor sind, die Cisco Website zu verlassen. Dieses Bild wird am Ende eines Links zu externen Websites von Cisco.com angezeigt und in einem separaten Browserfenster geöffnet. Cisco übernimmt keine Verantwortung für den Inhalt anderer Websites.

Cisco IOS[®] Softwarebefehle

Die nächsten Konventionen für Cisco IOS-Befehle werden auch in den Befehlsreferenzen verwendet. Weitere Informationen zu Konventionen in der Cisco IOS-Dokumentation finden Sie im [Cisco Technical Content Style Guide](#) .

- Vertikale Balken (|) separate alternative, sich gegenseitig ausschließende Argumente.
Beispiel: req-qos {Best Effort | Kontrollierte Last | Garantierte Verzögerung}
- Eckige Klammern ([]) weisen auf optionale Elemente hin. Beispiel: [no] ip route-cache [cbus]
- Geschweifte Klammern ({ }) weisen auf eine erforderliche Auswahl hin. Beispiel:
Zugriffslistennummer [{permit | deny}]
- Geschweifte Klammern in eckigen Klammern ([{ }]) weisen auf erforderliche Optionen innerhalb optionaler Elemente hin.
- Winkelklammern (< >) weisen auf Argumente in Kontexten hin, die keine Kursivschrift zulassen, und in Beispielen auf Zeichenfolgen, die ein Benutzer eingibt und die nicht auf dem Bildschirm angezeigt werden (z. B. ein Kennwort).
- Fett steht für Befehle und Schlüsselwörter.
- Kursiv: Benutzervariablen

Konfigurationsbeispiele

In Konfigurationsbeispielen werden allgemeine Routername, Hostnamen, Benutzernamen, Kennwörter und IP-Adressen verwendet. Diese müssen durch die für Ihr Unternehmen geeigneten Namen, Kennwörter und Adressen ersetzt werden.

Vorsicht: Verwenden Sie in Ihren Konfigurationen nicht den Benutzernamen **cisco** oder das Kennwort **cisco**. Die Verwendung von **cisco** als Passwort oder Benutzername oder die Verwendung trivialer Passwörter stellt ein Sicherheitsrisiko dar. Beachten Sie außerdem, dass Sie **Cisco** nicht in den Artikeltitel aufnehmen sollten.

- Routername: RouterX, nasX usw.
- Telefonnummern: 555nnnn

IP-Adressen

Achtung: IP-Adressen entsprechen [RFC 1918](#)-Definitionen privater Netzwerkadressen. Siehe Bild unten. Kürzlich gab es eine Sicherheitsverletzung aufgrund einer Client-IP-Adresse, die in einem Artikel auf **Cisco.com** angegeben wurde. Gehen Sie vorsichtig vor, wenn Sie in Ihrem Artikel eine IP-Adresse angeben. Überprüfen Sie Ihre Images auf IP-Adressen, die dies verletzen könnten.

Die Internet Assigned Numbers Authority (IANA) reserviert drei Blöcke mit IP-Adressen für das private Internet:

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

IP-Adressreferenz

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.

Für öffentliche Dokumentation reservierte IP-Adressen

Kommentare in Codeblöcken

In den Konfigurationsbeispielen sind häufig Kommentare enthalten. Kommentare sind kursiv formatiert. Sie dürfen nur als schwarzer Text angezeigt werden; Farben sind unzulässig, außer wenn sie in einem Screenshot angezeigt werden. Sie liefern weitere Informationen über die Konfigurationsausgabe und die verwendeten Befehle. Die Konfigurationskommentare sehen ähnlich aus:

```
!--- 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
```

Hinweis: Es wird empfohlen, Codeblock-Beispiele zu kürzen, sodass am Ende des Beispiels kein Schieberegler angezeigt wird.

Zugehörige Informationen

- [RFC 1918](#)
- [Stilvorgaben für technische Inhalte von Cisco](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.