https://www.ciscopress.com/articles/article.asp?p=2420613

Overview

For Cisco (and many other vendors), new commands are introduced at each progressive level of system verification. This article looks at five essential commands used to verify a network switch's status and operation:

- ping
- traceroute
- telnet
- ssh
- show cdp neighbors

ping

Available on almost all operating system platforms, including Cisco IOS, the ping command is used to verify the reachability of a targeted device. It does this by sending an Internet Control Message Protocol (ICMP) echo message to the target; if the target receives the message (and is not configured to drop it), it responds to the initial sender with an ICMP echo-reply message. In a perfect world, with no firewalls, and all devices configured to respond to these messages, the ping command would work perfectly. However, many devices (or devices en route, like firewalls) are purposely configured to ignore ICMP echo messages automatically, in order to hide their existence and avoid being targeted by attackers. In these cases, engineers must decide whether the unsuccessful ping is a real problem or a purposeful part of a network's design.

TIP

As a general rule, don't worry about devices that are outside your organization's control.

Cisco IOS also has an extended version of the ping command that allows for more complex command configurations. For example, an engineer has the ability to control the source IP used (which makes sense when being run from a router configured with multiple IP addresses), the size of the messages being sent, and the content of the messages, among other options.

traceroute

The traceroute command is typically used along with the ping command to further determine the reachability of a destination. traceroute works a bit differently from ping; instead of simply sending a message to the destination directly, it aims to find the path from the source to the target destination. It does this by using either ICMP echo messages on Windows or the User Datagram Protocol (UDP) probe messages on Linux and Cisco IOS. It figures out the path by taking advantage of the IP Time to Live (TTL) field.

It's important to understand what the TTL field does. In normal circumstances, the TTL is used as a loop-prevention mechanism; it works by being set to a number which is then decremented at every respective IP "'hop." If the TTL reaches a device and is decremented to 0, the packet is dropped and an ICMP "destination unreachable" message is sent back to the source device. When used by the traceroute command, the TTL finds each of the hops in the path between the source and the destination:

1. Initially the source sends an ICMP or UDP message to the destination with a TTL of 1.
2. When the packet reaches the first hop, the TTL is decremented to 0; the device drops the packet and sends back an ICMP "destination unreachable" message.
3. To find the second hop, the TTL is set to 2, for the third hop it's set to 3, and so on; typically three packets are sent for each step toward the destination (three with a TTL set to 1, three with a TTL set to 2, and so on).
4. These ICMP "destination unreachable" messages are received by the running traceroute command and interpreted into a readable output showing the path toward the destination.

As with the ping command, many organizations block the ICMP echo messages and some of the UDP messages; and the output should be read with this fact in mind.

The traceroute command on Cisco IOS is extended in the same way as the ping command variant that allows for extended command configurations. The options offered by traceroute mirror most of the options available in an extended ping.

telnet

The telnet command has been around for a long time, allowing users to manage devices via a command-line interface. Its very simple operation provides an unsecured Transmission Control Protocol (TCP) session between the source and destination. Characters entered on the source are immediately relayed to the destination, providing an experience on Cisco IOS (and Linux) that is the same as if the user were directly connected into the device locally.

CAUTION

A key term to take from this description is *unsecured*, the username and login information are sent between the source and destination in clear text.

The telnet command uses TCP port 23.

ssh

The ssh (secure shell) command works similarly to the telnet command but creates a secure communications channel between source and destination. This means that the username and password are *not* sent in clear text and are protected (at least to some level) from anyone listening in on the conversation.

The ssh command uses TCP port 22.

show cdp neighbors

The show cdp neighbors command is used on a Cisco IOS device to view neighboring devices discovered by the Cisco Discovery Protocol (CDP). CDP is a Cisco proprietary protocol used for Layer 2 discovery; it has the ability to discover all other supporting CDP devices on a shared segment. (It doesn't work *across* Layer 3 devices.) The following example shows some typical output of this command:

```
R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R2               Fas 0/0           172           R    7206VXR   Fas 0/0
R1#
```

In this example, we learn that the remote device (R2) is connected via R1's FastEthernet0/0 interface and is connected to R2's FastEthernet0/0 interface, and R2 is a Cisco 7206VXR router. This information is very helpful when mapping out unfamiliar networks. It can also be used to help ensure that a device is connected to the correct remote device(s) on the correct interface; as engineers often must configure devices remotely, this command is useful when installing new equipment, to ensure that physical interfaces are connected to the appropriate networks.

Keep in mind that CDP is a proprietary protocol and will not work to discover most other non-Cisco devices; this command is enabled by default on Cisco devices. A standards-based alternative to CDP is the Link Layer Discovery Protocol (LLDP)—IEEE 802.1AB, which is supported by many other vendors, but is *not* enabled by default on Cisco devices.

Summary

This article covers some of the most important basic commands you will need to know in order to verify status and current operational state of a network switch. You are likely to use these commands often. Engineers at every level must know these commands and be familiar with how they work.

NOTE

Be sure to check out my previous article "Nine Switch Commands Every Cisco Network Engineer Needs to Know."

Nine Switch Commands Every Cisco Network Engineer Needs to Know

Overview

To be considered experts, network engineers need experience with a wide variety of commands used with network technology. At the Cisco Certified Network Associate (CCNA) level, Cisco has indicated a number of commands that should be known initially for Cisco network switches. This article covers these commands, explaining what they do and how they alter the behavior and/or use of a Cisco switch.

hostname

Syntax: hostname *hostname*

One of the most basic network commands, hostname configures the hostname used for a device. This hostname identifies the device to other locally connected devices for protocols such as the Cisco Discovery Protocol (CDP), which helps in the identification of devices attached directly to the network. Although it is not case-sensitive, the hostname must follow certain rules: It must begin with a letter and end in a letter or digit, and interior characters must be letters, digits, or hyphens (-).

ip default-gateway

Syntax: ip default-gateway *gateway*

The ip default-gateway command configures the default gateway for a switch when IP routing is *not* enabled (with the ip routing global configuration command), which is typical when lower-level Layer 2 switches are being configured. The easiest way to determine whether IP routing has been enabled is to run the show ip route command. When IP routing has not been enabled, the output will look similar to the following example:

```
SW1#show ip route
Default gateway is 10.10.10.1


Host            Gateway         Last Use    Total Uses  Interface
ICMP redirect cache is empty
SW1#
```

When IP routing is enabled, the output looks similar to the output displayed on a router:

```
SW1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
     D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
     N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
     E1 - OSPF external type 1, E2 - OSPF external type 2
     i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
     ia - IS-IS inter area, * - candidate default, U - per-user static route
     o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
     + - replicated route, % - next hop override

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.10.0/24 is directly connected, Vlan1
L       10.10.10.10/32 is directly connected, Vlan1
SW1#
```

NOTE

The configuration entered with the ip default-gateway command has no effect when IP routing is enabled.

username

Syntax: username *username* {password | secret} *password*

The username command configures a username and associates a password with it. Using the password or secret version of this command is a matter of security:

- The password version of this command will do one of two things with the configured *password*:
  - Place the password into the configuration in plaintext (if the service password-encryption command is not enabled).
  - Put the password through a Cisco-proprietary encryption algorithm before placing it into the configuration. (Note that this encryption is easily reversed.)
- The secret version of this command will create an MD5 hash with the configured *password* and then place it into the configuration. This reconfigured password is much harder to crack than the encrypted version created with the *password* version of this command.

This username/password can be used for a number of different features, including Telnet and SSH.

enable

Syntax: enable {password | secret} *password*

The enable command configures the password that will be used to access a switch's privileged configuration mode. Because all configuration of a Cisco IOS switch requires privileged configuration mode, keeping this password private is very important. As with the username command, this command has two options: password and secret. The differences between these two options are the same as those for the username command in the preceding section. The enable secret version of the command should be used in all production environments.

Console and Terminal Login Commands

Five commands are used to configure login via the control and virtual terminal (VTY) lines of a switch:

- password
- login
- exec-timeout
- service password-encryption
- copy running-config startup-config

The following sections describe these individual commands.

password

Syntax: password *password*

When entered in line-configuration mode (console or terminal), the password command is used to configure the password that will be used to access a switch from that specific line, depending on the line mode (console or terminal). However, the password configured with this command is used only if the login command is used (which is the default).

login

Syntax: login [local]

The login command is used to enable password checking on an interface. If this command is used without any parameters, the system will check the password entered with the login against the one entered with the password command discussed in the preceding section. If used with the local parameter, both username and password will be prompted, and the entries will then be checked against the local username database that was created with the username command discussed previously.

exec-timeout

Syntax: exec-timeout *minutes* [*seconds*]

The exec-timeout command is used to configure the amount of time that can pass before a device considers the connection idle and disconnects. By default, timeout is set to 10 minutes. This timeout can be disabled with the no exec-timeout command. (This command is a shortcut and actually enters the exec-timeout 0 0 command into the configuration.)

service password-encryption

Syntax: service password-encryption

The service password-encryption command is used to enable the encryption of configured passwords on a device. The passwords referenced with this command are the ones configured with a command's *password* parameter, such as username *password* and enable *password*. The passwords encrypted with this command are not highly encrypted and can be broken relatively easily. By and large this command is deprecated, as most network engineers will use the secret version of the appropriate commands; however, even weak protection is better than nothing.

copy running-config startup-config

Syntax: copy running-config startup-config

The copy running-config startup-config command (popularly shortened to copy run start) is one of the most fundamental commands learned by new Cisco network engineers. It copies the active configuration (running-config) on a device to non-volatile memory (NVRAM) (startup-config), which maintains a configuration across a reload. Without this command, a configuration can be lost when a device is reloaded or powered off. The copy command can also be extended to save configuration and IOS images to and from a local device, as well as to and from different locations on the local device.

Summary

Network engineers must learn many Cisco OS commands in the process of becoming a CCNA (and beyond), and understanding these basic management commands is where the process starts. Without the knowledge of how to access devices, the complex commands are useless. You must understand when learning these concepts that they are intended to be stacked on top of each other. Lack of knowledge of a few base concepts undermines learning other, more advanced concepts that build on top of those basics.