SchoolNetwerk annotaties

Secure Shell (SSH) configuration on a switch and router in Packet Tracer

SSH config Switch (L2):
0. SVI aanmaken in VLAN99: interface VLAN99, IP Address 192.168.99.10 255.255.255.0, no shutdown (elke Switch heeft uniek IP in 192.168.99.0/24)
ip default-gateway 192.168.99.1
1. Hostname Switch-0de
2. ip domain name SchoolNetwerk
3. crypto key generate rsa
(name key == Switch-0de.SchoolNetwerk)
Bits in modulus [512]: 1024
4. Enable secret Class
5. username NetAdmin password Cisco
6. ip ssh version 2
7. line vty 0 4
transport input ssh
login local

Vanaf NetAdmin:

ssh -l NetAdmin 192.168.99.10 (aangemaakte SVI)

password == Cisco.

SSH config MLS (L2&3):
1. Hostname MLS
2. ip domain name SchoolNetwerk
3. crypto key generate rsa
(name key == MLS.SchoolNetwerk)
Bits in modulus [512]: 1024
4. Enable secret Class
5. username NetAdmin password Cisco
6. ip ssh version 2
7. line vty 0 4
transport input ssh
login local

Vanaf NetAdmin:

ssh -l NetAdmin 192.168.99.1 (bestaande SVI)

password == Cisco.

SSH config Router:
1. Hostname Router_SchoolNetwerk
2. ip domain name SchoolNetwerk
3. crypto key generate rsa
(name key == Router_SchoolNetwerk.SchoolNetwerk)
Bits in modulus [512]: 1024
4. Enable secret Class
5. username NetAdmin password Cisco
6. ip ssh version 2
7. line vty 0 4
transport input ssh
login local

Vanaf NetAdmin:

ssh -l NetAdmin 172.16.0.2

password == Cisco.

Interface Fa0/0 naar DHCP (ISP):
Interface Fa0/0
ip address dhcp

Static-NAT Router SchoolNetwerk

1. Extern IP adres Webserver: 209.209.209.5 (excluded bij DHCP!)

ISP:
2. Static route toevoegen op ISP naar 209.209.209.5/32
Router_SchoolNetwerk

3. Static NAT configureren:
ip nat inside source static 192.168.40.10 209.209.209.5

int fa0/1
ip nat inside (is al geconfigureerd bij PAT)

int fa0/0
ip nat outside (is al geconfigureerd bij PAT)

Bij NACL Firewall regel toevoegen:
5 permit tcp any host 209.209.209.5 eq 80
6 permit tcp any host 209.209.209.5 eq 443

PAT op Router SchoolNetwerk:

access-list 1 permit 192.168.0.0 0.0.255.255

ip nat inside source list 1 interface fa0/0 overload

interface fa0/1
ip nat inside

interface fa0/0
ip nat outside

ACL (Firewall) op Router SchoolNetwerk:

ip access-list extended Firewall
10 permit tcp any any established
20 permit icmp any any echo-reply
25 permit udp any any 68
30 deny ip any any (implicit deny)

interface Fa0/0
ip access-group Firewall in
ip address DHCP

DHCP voor VLANs 10, 20 en 30 op MLS

1. Service dhcp

2. IP DHCP Pool Docenten
network 192.168.10.0 255.255.255.0
domain-name Docenten
default-router 192.168.10.1
dns-server 192.168.40.10

3. IP DHCP Pool Leerlingen
network 192.168.20.0 255.255.255.0
domain-name Leerlingen
default-router 192.168.20.1
dns-server 192.168.40.10

4. IP DHCP Pool Gasten
network 192.168.30.0 255.255.255.0
domain-name Gasten
default-router 192.168.30.1
dns-server 192.168.40.10

NACL MLS:

ip access-list extended Docenten
2 permit tcp any any established
5 permit icmp any any echo-reply
10 deny ip 192.168.10.0 0.0.0.255 192.168.99.0 0.0.0.255
20 permit ip any any

interface vlan 10
ip access-group Docenten in

ip access-list extended Leerlingen
2 permit tcp any any established
5 permit icmp any any echo-reply
7 permit ip 192.168.20.0 0.0.0.255 host 192.168.40.10
10 deny ip 192.168.20.0 0.0.0.255 192.168.0.0 0.0.255.255
20 permit ip any any

interface vlan 20
ip access-group Leerlingen in

ip access-list extended Gasten
2 permit tcp any any established
5 permit icmp any any echo-reply
7 permit ip 192.168.30.0 0.0.0.255 host 192.168.40.10
10 deny ip 192.168.30.0 0.0.0.255 192.168.0.0 0.0.255.255
20 permit ip any any

interface vlan 30
ip access-group Gasten in

Inter VLAN Routing MLS:
ip routing
interface vlan 10
ip address 192.168.10.1 255.255.255.0
no shutdown
idem voor vlan 20, 30 en 99.

Statische route naar: (met EI!)
1. 172.16.0.0/30
2. 192.168.0.0/16
3. 209.209.209.5/32

Welcome to this tutorial! Here, we'll have an overview of Secure Shell (SSH) protocol, then see how to configure it on a **switch** and a **router** in Packet Tracer.

An overview of SSH

Secure Shell, just like Telnet, enables a user to access a remote device and manage it remotely. However, with SSH, all data transmitted over a network (including usernames and passwords) is **encrypted and secure** from eavesdropping.

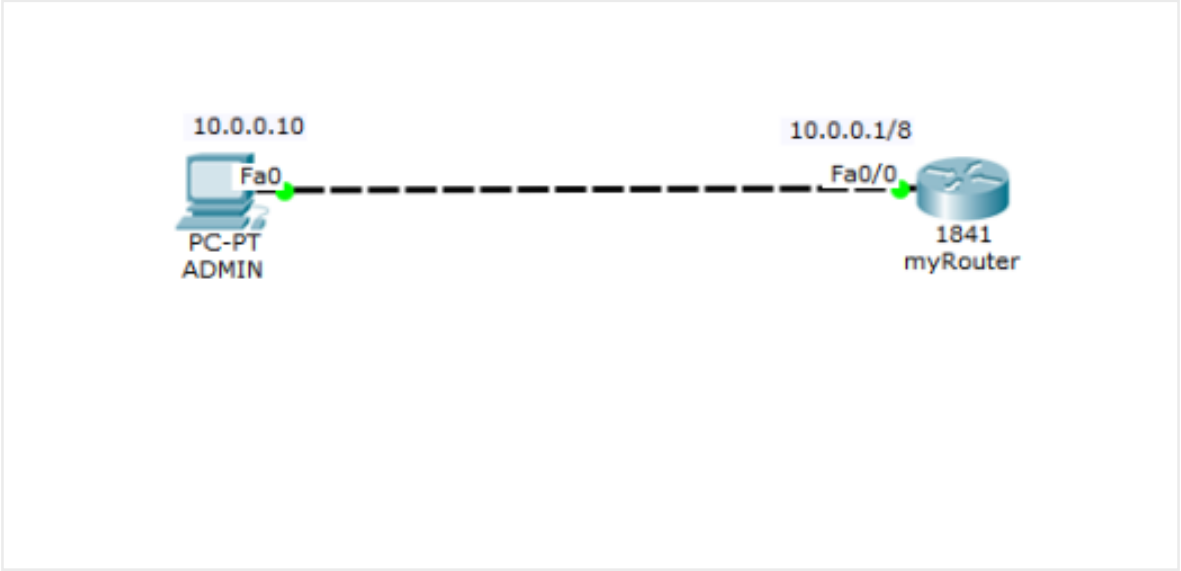
SSH is a **client-server** protocol, with a SSH client and a SSH server. The client machine (such as a PC) establishes a connection to a SSH server running on a remote device (such as a router). Once the connection has been established, a network admin can execute commands on the remote device.

Configuring SSH on a router in Packet Tracer

For this tutorial, we'll configure SSH on the router so that you as the admin can access and manage it remotely using an SSH client on the admin PC.

And now on to it:

First build the network topology.



Then do these basic IP configurations on the PC and the router:

Router

Router(config)#int fa0/0
Router(config-if)#ip add 10.0.0.1 255.0.0.0
Router(config-if)#no shut
Router(config)#exit

PC : **IP address** 10.0.0.10 **Subnet mask** 255.0.0.0 **Default gateway** 10.0.0.1

Now, to set up SSH on the router, you'll need to:

1. Set Router's **hostname**

Router(config)#hostname myRouter

2. Set **domain name**

myRouter(config)#ip domain name admin

Both the *hostname* and *domain name* will be used in the process of **generating encryption keys.**

3. Now generate **encryption keys** for securing the session using the command *crypto key generate rsa*.

myRouter(config)#crypto key generate rsa

The name for the keys will be: myRouter.admin
Choose the size of the key modulus in the range of 360 to 2048 for your

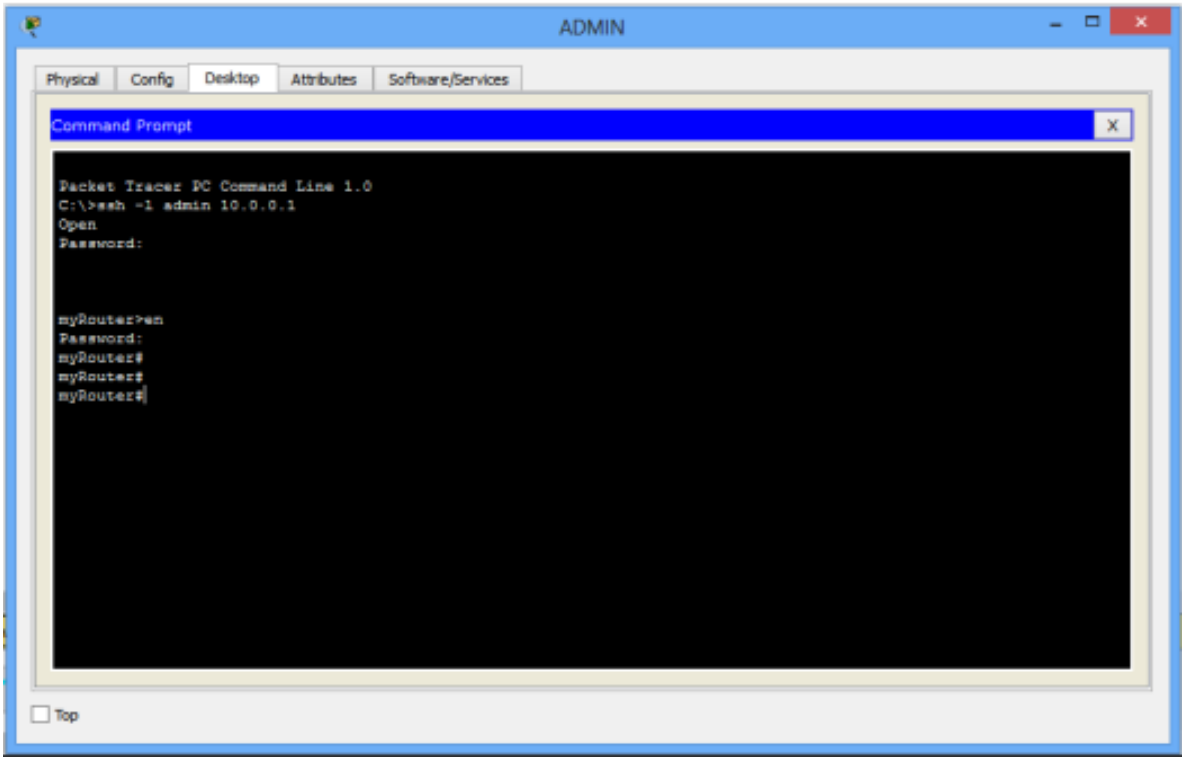
General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
4. Set an **enable password .**
myRouter(config)# enable password admin

Note that this password is not for use with SSH; its only for use in accessing the privileged executive mode of the router after you are able to access its CLI remotely via SSH .
5.Set **username** and **password** for local login.
myRouter(config)#username admin password admin
The password will have to be provided before you can access the CLI of the router when using SSH.
6.Specify the **SSH version** to use.
myRouter(config)#ip ssh version 2
7.Now connect to **VTY** lines of the Router and configure the SSH protocol.
myRouter(config)#line vty 0 15
myRouter(config-line)#transport input ssh
myRouter(config-line)#login local
That's all for configuration. Move on to see if you can access the router remotely from the PC.
8. On the command prompt of the **PC**, open a SSH session to the remote router by typing the command: *ssh -l admin 10.0.0.1*
a*dmin* is the **username** set in step 5.
9. Provide the **login password** which you set in step 5 and press enter.
You're now probably in the CLI of the router. Provide the **enable password** (the one you set in step 4) to access the privileged executive mode.

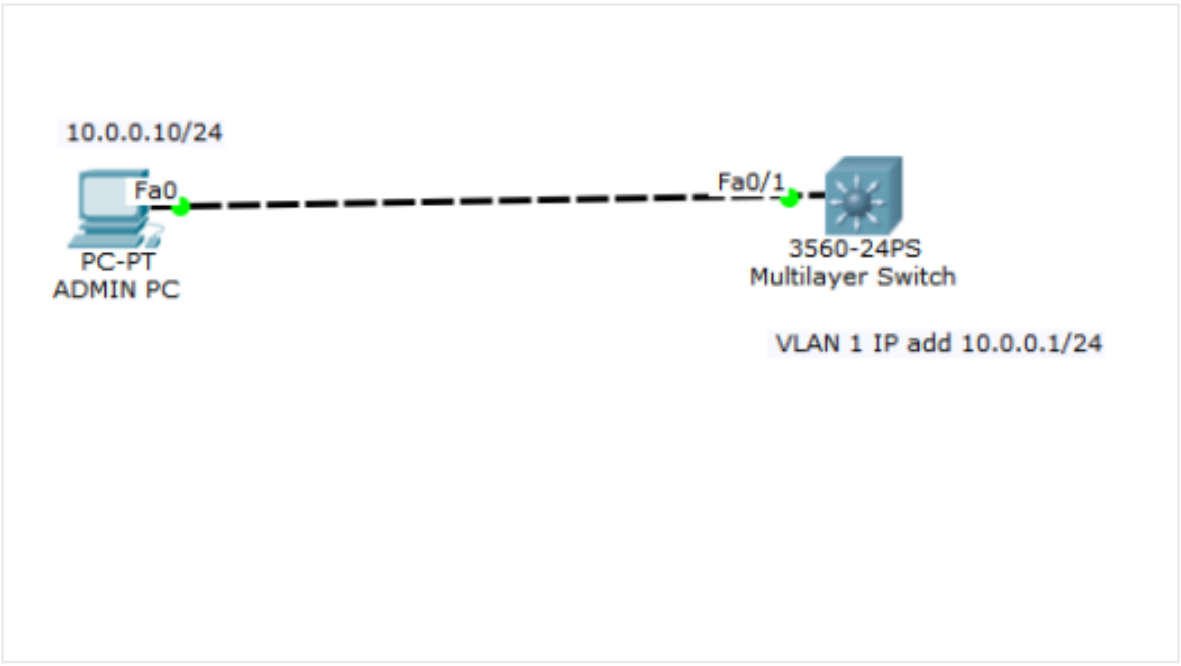


You can proceed and do configurations on the Router.You're now managing the router remotely from the PC.
That's it!
At this point, let's move on and configure SSH on a **switch**.

SSH configuration on a Switch

Here, we'll configure SSH on a multi-layer switch. The commands remain almost the same as for the router; only that in a switch, we'll use the IP address of its **VLAN interface** to access it from the PC.
So then, let's move on.

1. Begin by creating the network topology.



Then configure basic IP addressing on the PC and the switch. On the switch, we'll assign an IP address to a VLAN interface, just as we've said.

Switch

Switch(config)#int vlan 1
Switch(config-if)#ip add 10.0.0.1 255.0.0.0
Switch(config-if)#no shut

Give the **ADMIN PC** IP address 10.0.0.10 /8

Now, to configure SSH on the multilayer switch, here are the steps.

1.Configure **hostname**

Switch(config)#hostname SW1

2. Configure IP **domain name**

SW1(config)#ip domain name admin

Both the host name and domain name will be used in the process of generating encryption keys.

3. Now generate **encryption keys** for securing the session.

SW1(config)#crypto key generate rsa

The name for the keys will be: SW1.admin

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

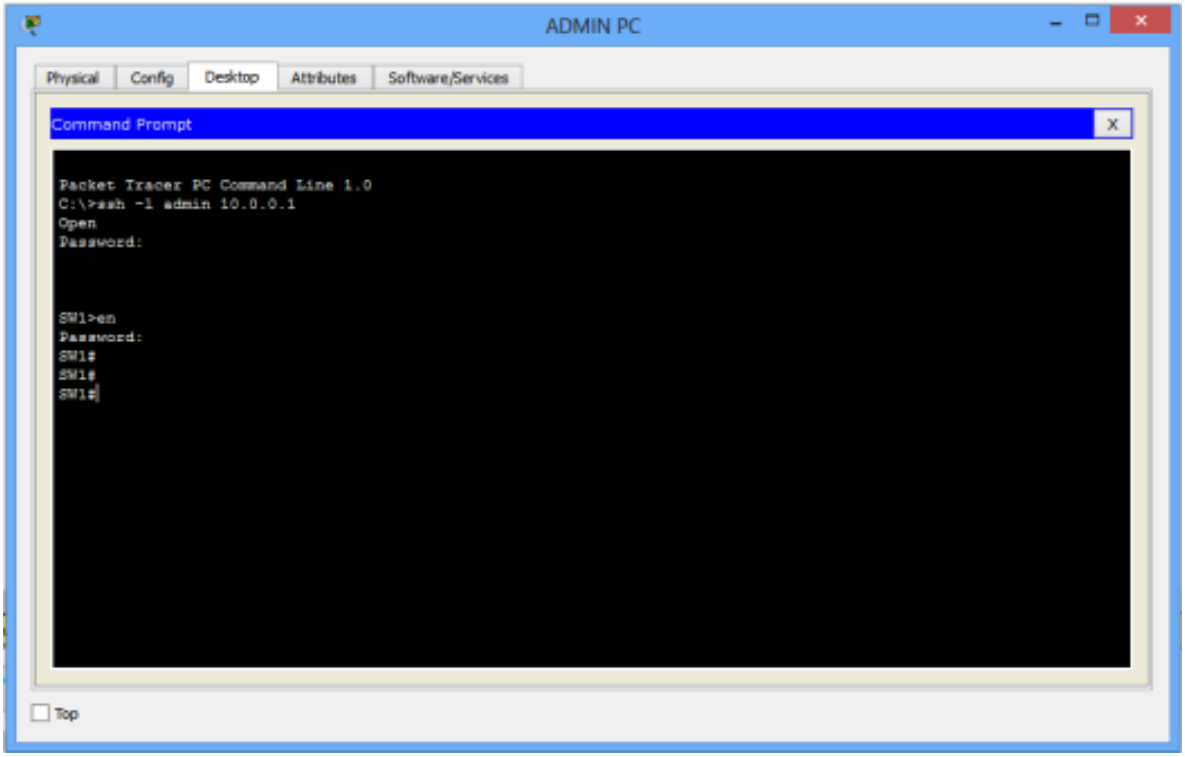
How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

4.Set an **enable password.**

SW1(config)#enable password admin

Again, note that enable password is not necessarily used in configuring SSH; it will allow the admin to access the **privileged executive mode** of the switch once a remote connection to the switch via SSH is established.
5. Set **username** and **password** for local login.
SW1(config)#username admin password admin
6. Specify the **SSH version** to use.
SW1(config)#ip ssh version 2
7. Now connect to the **VTY** lines of the switch and configure SSH on the lines.
SW1(config)#line vty 0 15
SW1(config-line)#transport input ssh
SW1(config-line)#login local
That's all for SSH configuration on the switch. Move on and try to access the switch remotely from the PC.
So then:
8. On the command prompt of the **Admin PC**, open a SSH session to the switch using the command **ssh -l admin 10.0.0.1**
Note that: *admin* is the username defined in step 5 while **10.0.0.1** is the IP address of the VLAN interface of then switch.
command prompt



CDP-LLDP

Zoals al eerder gecommuniceerd via teams, zou je het volgende aan de LE SchoolNetwerk willen toevoegen?

Bij 1.3 Product Informatie toevoegen: Fase 8: Een back-up verbinding realiseren voor alle laag 2 switches.

Bij 2.9 Fase 8 – Back-up toevoegen:

Bij Aanleiding toevoegen: Verder moet er een back-up verbinding gerealiseerd worden voor alle laag 2 switches.

Bij Doel toevoegen: en het robuuster maken van het switched netwerk door het toepassen van redundante verbindingen tussen de laag 2 access switches, waardoor single-point-of-failure uit dit deel van het netwerk wordt weggehaald.

Bij Uit te voeren werkzaamheden toevoegen:

Zoek in je bronnen op wat Spanning Tree is en hoe je Per-VLAN Spanning Tree (PVST) configureert.
Verbind de switches van de 1^{ste} en de 2^{de} verdieping rechtstreeks met de MLS en gebruik hiervoor alleen Gbps Ethernet trunk poorten.
Configureer de MLS uit de distributie laag als Root switch voor alle VLAN's die in gebruik zijn en zorg ervoor dat de verbindingen tussen de access switches in back-up mode staan. Deze worden ingeschakeld als een verbinding tussen een access switch en de MLS uitvalt.

Bij Beroepsproduct toevoegen:

Rechtstreekse Gbps Ethernet verbindingen toegevoegd op de access switches naar de MLS.
MLS is Root switch voor alle VLAN's die in gebruik zijn.
De verbindingen tussen de laag 2 access switches staan standaard in back-up mode.

Link Layer Discovery Protocol (LLDP) is also vulnerable to reconnaissance attacks. Configure **no lldp run** to disable LLDP globally. To disable LLDP on the interface, configure **no lldp transmit** and **no lldp receive**.

The show cdp neighbors Command

There are several other IOS commands that are useful. The Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol that runs at the data link layer. Because CDP operates at the data link layer, two or more Cisco network devices, such as routers that support different network layer protocols, can learn about each other even if Layer 3 connectivity has not been established. When a Cisco device boots, CDP starts by default. CDP automatically discovers neighboring Cisco devices running CDP, regardless of which Layer 3 protocol or suites are running. CDP exchanges hardware and software device information with its directly connected CDP neighbors.
CDP provides the following information about each CDP neighbor device:

- **Device identifiers** - The configured host name of a switch, router, or other device
- **Address list** - Up to one network layer address for each protocol supported
- **Port identifier** - The name of the local and remote port in the form of an ASCII character string, such as FastEthernet 0/0
- **Capabilities list** - For example, whether a specific device is a Layer 2 switch or a Layer 3 switch
- **Platform** - The hardware platform of the device--for example, a Cisco 1841 series router.

Refer to the topology and the **show cdp neighbor** command output.
router R3 is connected via interface G0/0/1 to switch S3 at port F0/5 which is connected to switch S4

G0/0/1 F0/5 R3 S3
S4

R3# 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
S3 Gig 0/0/1 122 S I WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#

The output displays that the R3 GigabitEthernet 0/0/1 interface is connected to the FastEthernet 0/5 interface of S3, which is a Cisco Catalyst 2960+ switch. Notice that R3 has not gathered information about S4. This is because CDP can only discover directly connected Cisco devices. S4 is not directly connected to R3 and therefore is not listed in the output.
The **show cdp neighbors detail** command reveals the IP address of a neighboring device, as shown in the output. CDP will reveal the IP address of the neighbor regardless of whether or not you can ping that neighbor. This command is very helpful when two Cisco routers cannot route across their shared data link. The **show cdp neighbors detail** command will help determine if one of the CDP neighbors has an IP configuration error.
As helpful as CDP is, it can also be a security risk because it can provide useful network infrastructure information to threat actors. For example, by default many IOS versions send CDP advertisements out all enabled ports. However, best practices suggest that CDP should be enabled only on interfaces that are

connecting to other infrastructure Cisco devices. CDP advertisements should be disabled on user-facing ports.
Because some IOS versions send out CDP advertisements by default, it is important to know how to disable CDP. To disable CDP globally, use the global configuration command **no cdp run**. To disable CDP on an interface, use the interface command **no cdp enable**.