



Securing Cisco Routers

Terms you'll need to understand:

- ✓ Types of threats
- ✓ Threat mitigation
- ✓ Console access
- ✓ VTY access
- ✓ Authentication methods
- ✓ Types of services
- ✓ Access control lists (ACLs)
- ✓ Threat mitigation using ACLs

Techniques you'll need to master:

- ✓ Securing console access
- ✓ Securing VTY access
- ✓ Securing passwords
- ✓ Securing Simple Network Management Protocol (SNMP)
- ✓ Disabling router services and interfaces
- ✓ Following rules for creating ACLs
- ✓ Configuring ACLs for threat mitigation

Introduction

In this chapter, you will learn about all the different ways you can secure a Cisco router from hackers and out-of-band threats. We discuss the different services you need to know when configuring a router.

We also delve into configuring access lists and the different access lists that are available to you as a network engineer that you can use to protect your network backbone.

Threat mitigation is an important aspect of network security, and as a security expert, it is your prime objective to ensure that you protect your network and mitigate threats that arise.

Assessing the Risk

The most important thing you need to understand is the risks involved in setting up networks via insecure installations. Insecure installation of network devices such as routers and switches would be classified as installs that can be attacked physically or via a configuration weakness.

Let us give you an example: Keeping your network devices under lock and key would prevent meditated physical attacks on the devices. It all depends on the type of environment you work in. Risk can be classified as low or high. High risk is associated with mission-critical devices, and these devices, in most cases, are your backbone routers and distribution layer switches.

Various Physical Threats and Mitigation

Physical threats have four parts:

- *Hardware threats*—All threats that are associated with physical damage to the routers and switches are classified as hardware threats. You can mitigate hardware threats by providing controlled access to the facilities. You limit access to only network-related personnel into the main distribution facility (MDF), intermediate distribution facility (IDF), and network operations center (NOC). You can provide security by ensuring that there is no access to the facility via the ceiling, raised floors, AC ducts, or windows. You can also mitigate hardware threats by using security cameras and by logging entry attempts.
- *Environmental threats*—Threats associated with climatic conditions are environmental threats. To mitigate environmental threats, you need to

ensure that there is adequate ventilation in the facility and that the temperature and humidity levels are maintained in accordance with the specifications defined in the equipment documentation. Once these parameters are in place, ensure that you have the ability to remotely manage and monitor temperature and humidity controls. Also make sure that the facility is free from electrostatic discharge (ESD) and magnetic interference.

- *Electrical threats*—Brown-outs, spikes, inadequate power supply, noise, and power loss are typical examples of electrical threats. We highly recommend that your mission-critical devices are hooked up to an uninterruptible power supply (UPS). A UPS provides line conditioning and protects your network devices against irregularities in your power-distribution system. Ensure that you have redundant power supplies in your network devices (if they support them) or some hot spares at the facility. This measure reduces the amount of downtime on your network. A generator can be an alternate source for power in case of a power outage if your environment is mission critical.
- *Maintenance threats*—Poor cabling, faulty labeling, and electronic devices without adequate ESD deterrents are classified as maintenance threats. Make sure that the equipment cabling is labeled properly and that a proper labeling convention is followed. This measure helps in tracing cables in the facility and aids in quick troubleshooting as well. Ensure that cables have smooth bends when you go around the corner. You want no kinks on the cable, so you can guarantee the smooth flow of data.

Securing the Network Using Cisco Routers

It is imperative that the networks be secured using some kind of security policy and parameters. The perimeter routers must be secured so that the corporate LAN resources are protected from the outside world.

Perimeter security comes in different forms. If you have a small network with only one router separating you from the rest of the world, it becomes imperative that the perimeter router be secured. This security helps you protect your internal resources.

Perimeter Router and PIX Firewall

Medium-size businesses can take security to the next level by deploying a firewall between the perimeter router and the internal network. The perimeter router provides support to the firewall by filtering out unnecessary traffic from coming into the network.

Perimeter Router Running the Firewall Feature Set

If you are a small- to medium-size network, you can use Cisco routers as a firewall as well. You have to load the firewall feature set on the router. Once the firewall feature set is installed on the router, you can then configure it to provide protection to your network using packet filtering.

You must understand that the firewall feature set does not provide the same level of protection as the PIX Firewall.

Perimeter Router, Firewall, and Internal Router

Large businesses use a three-tiered approach to network security. The perimeter routers provide preliminary protection to the PIX Firewall. The firewall then does the actual packet filtering, and finally, the internal router ensures that certain VLANs are protected from traffic coming into the corporate LANs.

Once the basics of securing networks are in place, how do we actually secure a Cisco router?

Securing Administrative Access to a Cisco Router

Configuring administrative access on the Cisco router is an important step toward network security. You can access all Cisco routers in various ways:

- Console
- VTY
- Aux

- SNMP
- HTTP

Connection Through the Console Port

To protect administrative access to the routers, you must protect the console port via a password policy. You can store passwords locally on the router or use some kind of remote administration using a CiscoSecure Access Control Server authentication, authorization, and accounting (AAA) server. You can store passwords locally on the router or use Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System + (TACACS+) for remote AAA using CSACS.

Password Policy

You should keep the following rules in mind when formulating a password policy:

- Acceptable password length must be between 1 and 25 characters. Blank passwords are not a part of a good security policy. The passwords should contain alphanumeric, uppercase, and lowercase characters.
- On Cisco equipment, the first character in the password cannot be a number.
- Leading spaces in the password are ignored; however, spaces after the first character are not ignored.
- Passwords must be changed often, and using the same passwords over again should be avoided. Be creative and generate unique passwords every time. Do not use obvious passwords such as your dog's name or your date of birth.

Securing Privilege EXEC Mode Using the `enable secret` Command

When you first power on the router, assuming that there is no prior configuration stored in the nonvolatile RAM (NVRAM), the router enters the Initial Configuration dialog box. The Initial Configuration dialog box is a menu system that assists you in applying basic configuration on the router. You can use Ctrl+Z to break out of the Initial Configuration dialog box.

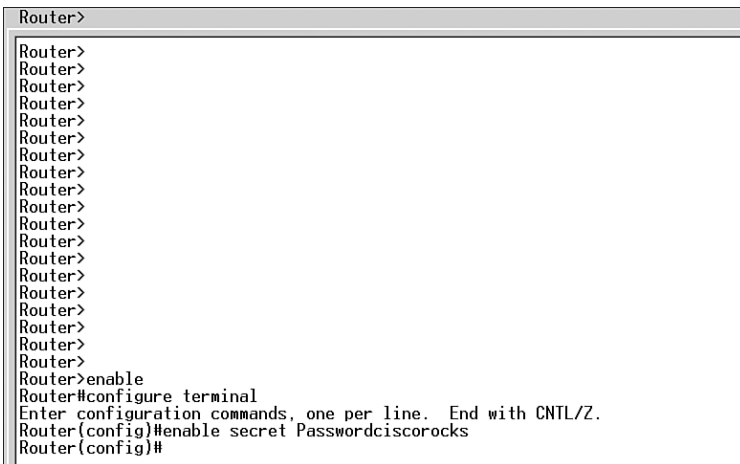
To make changes to the router configuration, you have to first enter privilege EXEC mode. By default, you do not need a password to access privilege EXEC mode. You can use the enable command to access the privilege EXEC mode of a router:

```
Router> enable  
Router#
```

Once you are in privilege EXEC mode, you can then secure privilege EXEC mode on the routers using the enable secret command in global configuration mode. The enable secret command encrypts the password to the privilege EXEC mode using the Message Digest 5 (MD5) hashing algorithm. It is a one-way hash. In other words, once you have a password using MD5, you cannot unhash it:

```
Router> enable  
Router# configure terminal  
Router(config)# enable secret Passwordciscorocks  
Router(config)#
```

Figure 3.1 shows how to configure an MD5 password on a router.



```
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>  
Router>enable  
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#enable secret Passwordciscorocks  
Router(config)#
```

Figure 3.1 Configuring the enable secret password on a router.

In the example, Passwordciscorocks is the password that will be used to access the privilege EXEC mode of this router.

Let us look at another example:

```
Router> enable  
Router# configure terminal  
Router(config)# enable secret Password cisco rocks  
Router(config)#
```

In this example, what is the password assigned to the privilege EXEC mode?

- cisco
- cisco rocks
- password cisco rocks
- Password cisco rocks
- I have no idea; please explain.

The password assigned to the privilege EXEC mode will be `Password cisco rocks` because all spaces after the first character are part of the password.

If you do a `show running-config` on the router, you will note that the `enable secret` is encrypted and the 5 after `enable secret` identifies that it is an MD5 hash.

Here is an example to illustrate this concept:

```
Router# show running-config

! Last configuration change at 14:34:43 MST Wed Jul 16 2003
! NVRAM config last updated at 14:34:44 MST Wed Jul 16 2003
!
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Router
!
enable secret 5 $1$oeJp$08vrQkQWGGsz5S5h.VqQe/
!
```

Figure 3.2 shows how the `enable secret` password appears in a **show running-config** command.

If you forget your `enable secret` password, the only way to access the router's privilege EXEC mode would be by doing a password recovery. Different Cisco routers have different ways of doing password recovery. You can get information on password recovery by doing a search on the keywords “password recovery” on <http://www.cisco.com>. Always use the `enable secret` command instead of the older `enable password` command; `enable password` uses a very weak encryption algorithm.

```
Router#
Router#
Router#
Router#show running-config
Building configuration...

Current configuration : 861 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable secret 5 $1$SAw6$jNqXNy8ZWhgj7i8eyKyTJ.
!
!
ip subnet-zero
!
!
ip audit notify log
ip audit po max-events 100
!
!
```

Figure 3.2 Displaying the **enable secret** password command output in a **show running-config** command.

Securing Console Access Using a Console Password

A Cisco router's console port is the most important port on the device. Password recovery on the router can only be done using the console port. This port can be used to access the ROMMON mode on the router as well. The console port allows a hard break signal that interrupts the boot sequence of the router. You can issue the break sequence on a router within 60 seconds of the reboot, and it gives complete access to the user issuing this command.

Cisco routers are vulnerable if you have physical access to the devices. However, if someone is trying to access the console port of the router remotely, you can apply an additional layer of security by prompting the user for a password.

Here is how you protect the console port on the router:

```
Router> enable
Router# configure terminal
Router(config)# line console 0
Router(config-line)# password Ciscorocks123
Router(config-line)# login
Router(config-line)# end
Router#
```

Figure 3.3 shows how to configure password protection on the console port of a router.


```

Press RETURN to get started.

Router>enable
Password:
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password Ciscorocks123
Router(config-line)#login
Router(config-line)#end
Router#
00:16:03: %SYS-5-CONFIG_I: Configured from console by console
Router#

```

Figure 3.3 Configuring a password on the console port of a router.

Remember, to assign a password to the console port of the router, you first have to access the global configuration mode of the router. Once in the global configuration mode, you access the console port by issuing the `line console 0` command. Remember, the console port is always 0 because there is only one console port on every Cisco device, and Cisco starts its numbering of the ports with 0:

```

Router> enable
Router# configure terminal
Router(config)# line console 0

```

Once in the line configuration mode, you issue the `password` command followed by the password. This password by default is not encrypted:

```

Router(config-line)# password Ciscorocks123

```

Once you issue the `password` command, you issue the `login` command. The `login` command tells the router to ask for the password when someone is typing to access the router using the console port:

```

Router(config-line)# login

```

When you do a `show running-config` on the router, you note that the password is not encrypted. This output is truncated to fit the page; however, you must note that the line console information is always at the bottom of the configuration:

```

Router# show running-config
!
line con 0
 login

```

```

password Cisco123
line aux 0
line vty 0 4
!
end

```

Securing VTY Access Using a Telnet Password

By default, all Cisco routers support up to five simultaneous Telnet sessions, and by default, no passwords are assigned to these Telnet or VTY lines. There is built-in security on the VTY lines that mandates the use of passwords to access the router via a Telnet session. If a Telnet session is initiated to a router that does not have a password assigned to the VTY lines, the following message appears on the screen:

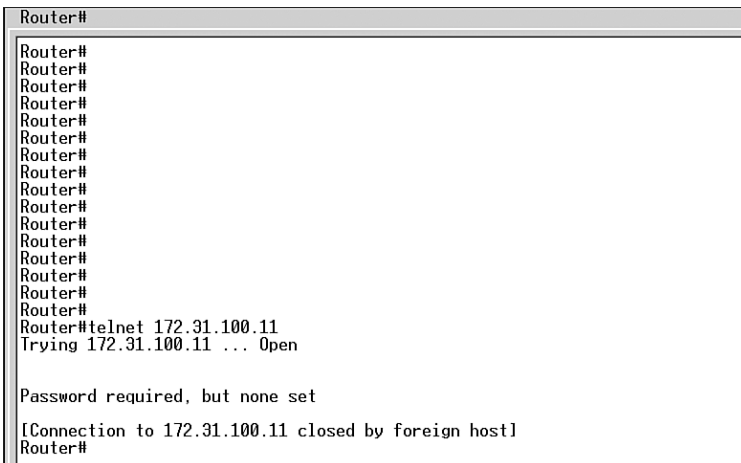
```

telnet 172.31.100.11

Trying...
Connected to 172.31.100.11
Escape character is '^]'.
Password required, but not set
Connection closed by remote host

```

Figure 3.4 shows how Telnet behaves when there is no password and login assigned to the VTY lines.



```

Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#telnet 172.31.100.11
Trying 172.31.100.11 ... Open

Password required, but none set

[Connection to 172.31.100.11 closed by foreign host]
Router#

```

Figure 3.4 Displaying the Telnet behavior when no password is assigned to the VTY lines.

Essentially, no Telnet sessions are allowed to the router. This measure is good security, but it disallows everyone to access the router, even the legitimate user. To remotely manage the routers using Telnet, it is imperative that you assign a password to the VTY lines.

Here is how you protect the Telnet lines on the router:

```
Router> enable
Router# configure terminal
Router(config)# line vty 0 4
Router(config-line)# password VtyLines123
Router(config-line)# login
Router(config-line)# end
Router#
```

In this example, the configuration logic is the same as that for the console port. The only difference is the following line:

```
Router(config)# line vty 0 4
```

This line can be interpreted as follows: As we said earlier, by default, Cisco routers allow up to five simultaneous Telnet sessions, and in the Cisco world, all counting begins with 0. Hence, 0 4 would give you five Telnet lines.

In the example, the password `VtyLines123` is assigned to all five VTY lines. You can assign separate passwords to each and every line. However, managing the passwords becomes an administrative nightmare.

You should consider a few guidelines when configuring VTY access to the router:

- If there is no password set on the router to access the privilege EXEC mode, you will not be able to access the privilege EXEC mode of the router via the Telnet session.
- Telnet transmits and receives all data in cleartext, even the passwords. To provide additional security in this aspect, you can use Secured Shell (SSH) or administer the router via an IPSec tunnel. You can provide additional security by using access lists to manage administrative access to the routers from specific IP addresses. Remember, Cisco routers work with SSH1 only.
- Make sure you have a password assigned to the VTY lines of the router; otherwise, no one will be able to access the router via Telnet.

Our recommendation: Do not use Telnet, use SSH instead. SSH encrypts all data flowing between you and the router, thus providing high-level security.



Cisco supports SSH1 only.

The aux port on the router is another way you can gain access to the router. You can protect the aux port on the router by assigning a password to it. Here is how you accomplish the task:

```
Router> enable
Router# configure terminal
Router(config)# line aux 0
Router(config-line)# password ProtectAux0
Router(config-line)# login
Router(config-line)# end
Router#
```

In this example, every time a user accesses the router via the aux port, he or she will be prompted for a password.

If you are not using the aux port on the router, you can disable it by issuing the following command:

```
Router(config)# line aux 0
Router(config-line)# no exec
```

Figure 3.5 shows how to disable the aux port if it is not being used.

```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#line aux 0
Router(config-line)#no exec
Router(config-line)#
```

Figure 3.5 Disabling the aux port.

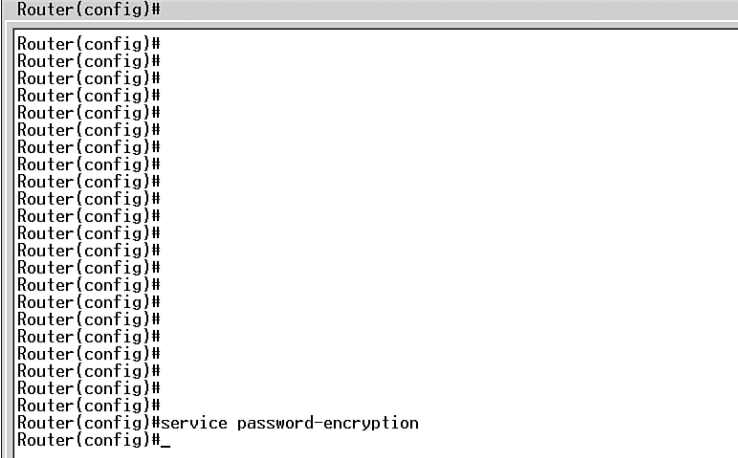
The `no exec` command disables all EXEC sessions to the router via that port. Do not issue this command on the console port of the router because it will disallow all exec sessions to the router's console port.

Encrypting All Passwords on the Router

By default, only the enable secret password is encrypted. To encrypt all other passwords configured on the router, issue the following command in global configuration mode:

```
Router(config)# service password-encryption
```

In Figure 3.6, the administrator is encrypting all the passwords except the enable secret password.



```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#service password-encryption
Router(config)#_
```

Figure 3.6 Configuring the `service password-encryption` command.

The `service password-encryption` command uses a Cisco proprietary Vigenere cipher to encrypt all other passwords on the router except the enable secret password (which uses MD5). The Vigenere cipher is easy to break, and if you do a `show running-config` on the router, it appears as follows:

```
line con 0
 password 7 110A1016141D
 logging synchronous
 login
 transport input none
```

Figure 3.7 shows the password parameters after configuring the `service password-encryption` command.

The number 7 after the keyword `password` indicates that the password has been encrypted using the Vigenere cipher. This command does not change the fact that the Vigenere cipher can be cracked. In fact, you can download the GETPASS utility, which will decrypt the Vigenere cipher for you.

This command sets the no activity timeout to 5 minutes. Setting a lower activity timeout automatically locks up the console once the timeout expires.



You can use the **exec-timeout** command to configure an activity timeout on the routers.

Configuring Access Levels on the Router

You can configure access levels on the routers so the junior administrators do not have complete access to the router. Cisco routers have 16 different privilege levels that you can configure. The 16 levels range from 0 to 15, where 15 is equal to full access. You can customize levels 2 to 15 to provide monitoring abilities to the secondary administrators. Here is a sample configuration for privilege levels on the router:

```
Central(config)#username junioradmin privilege 3 password 0 s3cUr!tY
.
.
.
Central(config)#privilege exec level 3 ping
Central(config)#privilege exec level 3 traceroute
Central(config)#privilege exec level 3 show ip route

Central(config-line)#line vty 0 4
Central(config-line)#password CisC0r0cK5
Central(config-line)#login local
```

Figure 3.9 displays the configuration of a privilege level for specific commands and applying local authentication to the VTY lines. Notice that in addition to the login local command a password is configured on the VTY lines. However, users will need to use the local router database to log in to the VTY lines because the login local command takes precedence over the password command.

Looking at this config, whenever junioradmin logs into the router, he or she is allowed only three commands: ping, traceroute, and show ip route. Using the privilege command, you can provide another layer of security to your network backbone.

```

Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#username junioradmin privilege 3 password s3cUr!tY
Router(config)#privilege exec level 3 ping
Router(config)#privilege exec level 3 traceroute
Router(config)#privilege exec level 3 show ip route
Router(config)#line vty 0 4
Router(config-line)#password CisC0r0cK5
Router(config-line)#login local
Router(config-line)#

```

Figure 3.9 Configuring Privilege Level and Local Authentication.

Configuring Routers with a Statutory Warning

It is imperative that you configure a statutory warning on all your networking devices that clearly states the repercussions of attempting to log on to an unauthorized system. You can achieve this by using various banner messages:

- ▶ `banner exec`—You can use this command to specify a message that appears when an EXEC process is initiated.
- ▶ `banner motd`—You can use this command to enable a message of the day for your admins and team.
- ▶ `banner login`—You can use this command to enable messages that appear before username and password prompts.

You can configure a few more banner messages on routers to ensure that you get the word out that unauthorized users will be prosecuted.

Just an FYI: Do not use such phrases as “*Welcome* to the ABC Network” because they can create a loophole that a hacker can use to avoid legal action. We highly recommend that you consult your legal department to come up with the correct verbiage.

Securing SNMP

SNMP is one of the most exploited protocols and can be used to gain administrative access to Cisco routers by establishing communication between a router's internal SNMP agent and management information base (MIB). SNMP uses community strings that act as the passwords to access the routers. Whenever you are setting up SNMP community strings, make sure you know which strings will have read-only access; which ones will have read-write access; and, most of all, which systems will be allowed SNMP access via ACLs.



SNMP version 3 supports MD5 and Secure Hash Algorithm 1 (SHA-1) authentication.

Securing Routers by Disabling Unused Router Services and Interfaces

On Cisco routers, a whole bunch of services come enabled by default. As a network security expert, your first order of operation would be to ensure that the unused services are disabled.

We now give you a rundown of a few services that you need know before entering into the security arena.

bootp

bootp is enabled by default, and if you are not using it, you should definitely disable it. You can use the `no ip bootp server` command in global configuration mode to disable bootp on your routers:

```
Central(config)# no ip bootp server
```

CDP

Cisco Discovery Protocol (CDP) is also enabled by default, and we highly recommend that you disable this service on the router globally. You can disable CDP globally by using the `no cdp run` command in global configuration

mode, or you can disable CDP on a per-interface basis by using the `no cdp enable` command in interface configuration mode:

```
Central(config)#no cdp run
Central(config-if)#no cdp enable
```



The **no cdp run** command disables CDP globally on the routers.

ip classless

The `ip classless` command is enabled on the Cisco routers by default in version 12.0 and higher. Disable `ip classless` if your network does not have a subnetted range of IP addresses. If you are subnetting a block of IP address allocated to you by the American Registry for Internet Numbers (ARIN), you should ensure that `ip classless` is enabled. You can learn more about ARIN by going to <http://www.arin.net>. It allows the router to advertise the subnetted addresses to its neighbors:

```
Central(config)#no ip classless
```

DNS

Domain Name System (DNS) lookup is enabled by default on Cisco routers, and if you are not implementing DNS lookup on your network, it is highly advisable to disable this feature globally by using the `no ip domain-lookup` command:

```
Central(config)#no ip domain-lookup
```

finger

The `finger` command is enabled by default and can be used to see what users are logged on to the network device. The `finger` command has been documented in RFC 742, and you should globally disable the `finger` command on network devices:

```
Central(config)#no ip finger
```



The **no service finger** command has been replaced by the **no ip finger** command.



Finger service can be disabled on the router in global configuration mode.

HTTP

Cisco routers can be accessed via a Web page, and unless you are implementing authentication proxy, we highly recommend that you turn off the HTTP service running on the router. You can use the `no ip http server` command to disable it.

If you want to implement HTTP-based management, we recommend that you implement HTTP authentication and limit the HTTP connections to the router using ACLs.

ip mask-reply

By default, the `ip mask-reply` command is disabled on all Cisco routers. The mask replies respond to Internet Control Message Protocol (ICMP) mask requests by sending out ICMP mask replies, and these mask replies contain important network information. If mask replies are enabled, make sure you disable them on the router by using the `no ip mask-reply` command in interface configuration mode:

```
Central(config-if)#no ip mask-reply
```

IP-Directed Broadcast

The IP-directed broadcast is another service that is commonly used in Smurf attacks. Smurf attacks send ICMP echo requests from a spoofed source address to a directed broadcast that cause all hosts to respond to the ping echo request, creating a lot of traffic on the network. By default on IOS version 12.0 and higher, `ip directed broadcast` is disabled, and if you are running any version lower than 12.0, it is imperative that you disable IP directed broadcasts on the router by issuing the following command in interface configuration mode:

```
Central(config-if)#no ip directed-broadcast
```



Smurf attacks send ICMP echo requests from a spoofed source address to a directed broadcast that cause all hosts to respond to the ping echo request, creating a lot of traffic on the network.

IP Source Routing

IP source routing allows the sender of an IP packet to control the route that packet will take to reach the destination endpoint. By default, IP source routing is disabled on the routers and should only be enabled if your network needs call for it. The following command disables IP source routing on the router globally:

```
Central(config)#no ip source-route
```



IP source routing allows the sender of an IP packet to control the route that packet will take to reach the destination endpoint.

IP Unreachable

IP unreachable messages can be used to map out the network topology, and they should be disabled on all interfaces. You can disable IP unreachables on all interfaces by issuing the following command in interface configuration mode:

```
Central(config-if)#no ip unreachablees
```



IP unreachablees should be disabled on all interfaces connected to insecure networks.

Small Servers

Cisco classifies echo, chargen, daytime, and discard as small services and recommends that these services be disabled on the router. By default, on versions 11.3 or higher, the small server service is disabled by default.

Cisco Access Lists

You can use ACLs to provide packet filtering at the router level. You can use ACLs extensively at a firewall to protect your internal network from the outside world. This section outlines the different types of ACLs that are available to you and the rules (we prefer the word *guidelines*) for creating ACLs. A wide variety of ACLs can be leveraged to provide additional layers of security on your network. We talk about a few types of access lists.



When building ACLs, note that there is an implicit **deny** statement at the end of the access list.

Standard

Standard ACLs filter traffic based on the network only, and they are not as granular as the extended ACLs. Standard IP access lists range from 1 to 99.

Extended

Extended access lists are more granular and can be used to provide filtering based upon source and destination IP addresses, TCP/UDP ports, and protocols. Extended access lists range from 100 to 199.

You can apply ACLs in two directions:

- *Inbound*—Inbound ACLs are subjected to all traffic coming into the router through an interface.
- *Outbound*—Outbound ACLs are subjected to all traffic leaving the router's interface.



ACLs are applied on the router at interface level and not at global level. ACLs are created at global level.

Starting with IOS version 12.0(6)S and higher, you can compile access lists on certain Cisco routers. This concept is called *Turbo ACLs*. Turbo ACL compiles the access list into lookup tables. Packet headers are used to access these lookup tables in small and fixed numbers of lookups. Note that this command was introduced with the high-end Cisco routers, namely the Cisco 7200 series.

Another way of securing Cisco routers is via context-based access control (CBAC). CBAC examines packets as they enter or leave the router's interfaces. This process also determines what application protocol to allow. CBAC was introduced in version 12.0T.

This configuration allows Telnet access to 30.120.11.1 from 10.0.0.1 hosts only by default, there is an implicit deny statement at the end.

IP Spoofing

Spoofing is a technique used to gain access to unauthorized networks or resources by sending a data stream to a host with an IP address that indicates that the message is coming from a trusted host.

As a golden rule, you should *never* allow any IP datagrams coming inbound to a protected network that contain the source address of any internal host or network. To mitigate IP spoofing on all inbound traffic, do the following:

1. You should deny all localhost addresses, which are the 127.0.0.0/8 class IP addresses.
2. You should also deny all reserved IP address spaces as described in RFC 1918. However, it is recommended that reserved IP addresses be blocked on interfaces connecting to the ISP's backbone.
3. Also deny all multicast address ranges from 224.0.0.0/4.
4. Most importantly, deny any addresses that have the same source address as the protected network.

When securing routers against outbound IP spoofing, make sure you do not allow outbound IP datagrams with source addresses other than the valid and legitimate IP addresses on the protected network.



You can use IP unicast reverse-path forwarding to verify that the packet is not spoofed. This feature is available to you from IOS version 12.0 and higher.

DoS SYN Attack Mitigation

A denial-of-service (DoS) TCP SYN attack is a dangerous type of attack that involves sending large amount of datagrams from a spoofed source to internal hosts. The SYN attack is a DoS attack. The attacked host needs an amount of memory and processor power for each half-open TCP session until it is overloaded and cannot respond to legitimate requests.

This attack opens hundreds of TCP session requests, and because the source IP address is spoofed, the end device starts opening embryonic sessions to that spoofed host. Bottom line: The TCP connections get saturated on the end device and no one can access the information on that device.

To overcome this issue, you can use the `TCP intercept` command. The `TCP intercept` command examines each inbound TCP connection attempt and ensures that the external source address is not spoofed but is actually reachable.



You can use the **TCP intercept** feature to protect the internal network from TCP SYN attacks.

Summary

In this chapter, we talked about the different ways you can provide additional security to your network by doing the following:

- ▶ Setting up encrypted passwords
- ▶ Turning off all unwanted services
- ▶ Configuring different access levels
- ▶ Using different access lists to filter all unwanted traffic out of your network and mitigate threats such as IP spoofing and DoS attacks on your network

Exam Prep Questions

Question 1

Which of the following passwords can be applied on a Cisco router?

- A. **enable secret 1cisco123**
- B. **enable secret password cisco**
- C. **enable secret c**
- D. **enable secret <space><space>ciscocisco**

Answers: B, C, D. Passwords on a Cisco router cannot start with a number, and they ignore the leading spaces after the keyword `secret`. You can have a password from 1 to 25 characters in length.

Question 2

Which of the following commands resulted in the output that is bolded:

```
line con 0
exec-timeout 0 0
password 7 104D000A061843595F50
logging synchronous
```

- A. **service password encryption**
- B. **service encryption password**
- C. **service password-encryption**
- D. **encryption-password**

Answer: C. The `service password-encryption` command uses the Cisco-proprietary Vigenere cipher to encrypt all the other passwords on the router except the `enable secret` password (which uses MD5). A, B, and D are incorrect because they have the wrong syntax.

Question 3

Which command can you use to ensure that all administrative interfaces stay active for a period of 5 minutes and 45 seconds only after the last session activity?

- A. **Central(config-line)#timeout 5 45**
- B. **Central(config-line)#exec-timeout 5 45**
- C. **Central(config)#exec-timeout 5 45**
- D. **Central#exec-timeout 5 45**

Answer: B. The `exec-timeout` in line configuration mode ensures that the administrative interface stays up for the specified duration after the last session activity. A is incorrect because the correct command is `exec-timeout` and not simply `timeout`. C and D are incorrect because you have to be in line configuration mode to execute the `exec-timeout` command.

Question 4

Which of the following commands on a Cisco router can you use to prevent a hacker from finding out which users are logged into the network device?

- A. **show cdp entry**
- B. **ip finger**
- C. **no ip finger**
- D. **no service finger**

Answers: C, D. You can use the `no ip finger` and `no service finger` commands to prevent a hacker from finding out which users are logged into the network device. The `no service finger` command is a legacy command and works just the same as `no ip finger`.

Question 5

You have just configured the following access list and would like only these hosts to have Telnet access to the Central router. Which of the following commands will you use to make sure this implementation works?

```
Central(config)#access-list 1 permit host 10.10.0.1  
Central(config)#access-list 1 permit host 10.10.0.2
```

- A. **ip access-group 1 in**
- B. **access-group 1 in**
- C. **ip access-class 1 in**
- D. **access-class 1 in**

Answer: D. You use the `access-class` command in line configuration mode in an inbound direction to ensure that only hosts 10.10.0.1 and 10.10.0.2 are allowed to Telnet to the router. By default, all access lists have an implicit `deny` in the end, and because of that rule, only two hosts will be allowed Telnet access to the Central router.

Need to Know More?



You can find more information about configuring network security with ACLs at http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a008007e8ed.html.



Look for the Security Recommendation Guide at <http://nsa1.www.conxion.com/cisco/download.htm>.



To learn more about improving security on Cisco routers, visit http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml.