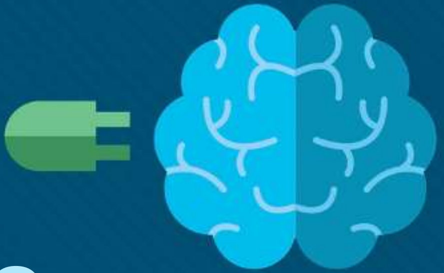
Module 4: Secure Device Access



Networking Security v1.0
(NETSEC)

Module Objectives

Module Title: Secure Device Access

Module Objective: Configure secure administrative devices.

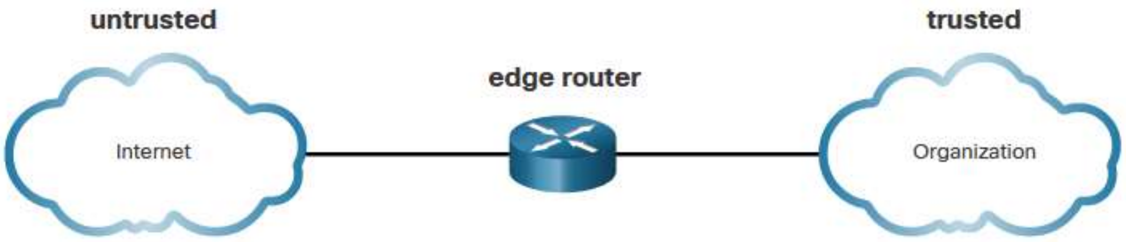
Topic Title	Topic Objective
Securing the Edge Router	Explain how to secure a network perimeter.
Configure Secure Administrative Access	Use the correct commands to configure passwords on a Cisco IOS device.
Configure Enhanced Security for Virtual Logins	Use the correct commands to configure enhanced security for virtual logins.
Configure SSH	Configure an SSH daemon for secure remote management.

4.1 Secure the Edge Router

Secure the Network Infrastructure

Securing the network infrastructure is critical to overall network security. The network infrastructure includes routers, switches, servers, endpoints, and other devices. Routers are a primary target for attacks because these devices direct traffic into, out of, and between networks.

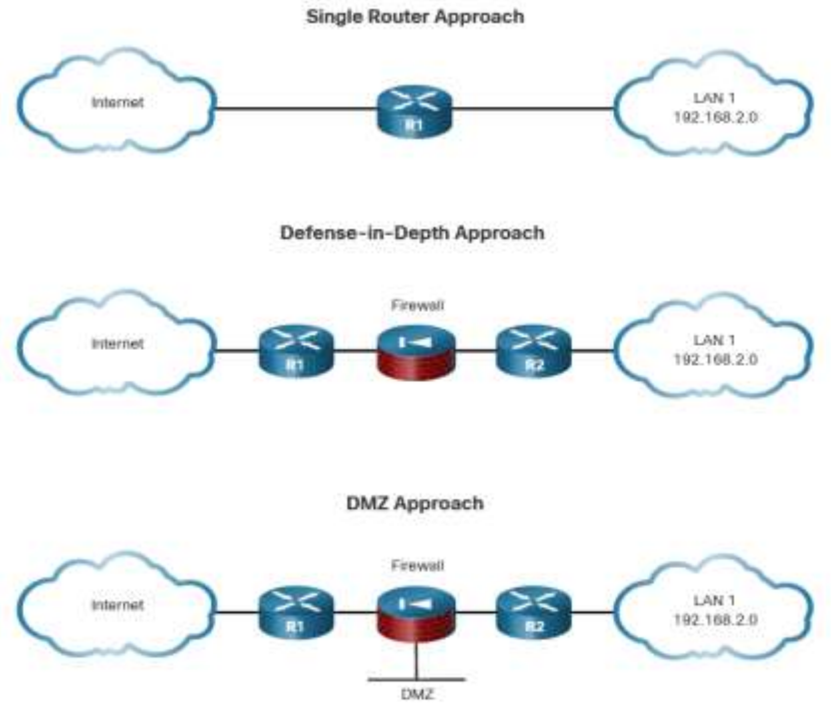
The edge router shown in the figure is the last router between the internal network and an untrusted network, such as the internet. All an organization’s internet traffic goes through an edge router, which often functions as the first and last line of defense for a network.



Secure the Edge Router

Edge Router Security Approaches

- **Single Router** - A single router connects the protected network or internal local area network (LAN), to the internet. All security policies are configured on this device.
- **Defense-in-Depth** – This uses multiple layers of security prior to traffic entering the protected LAN. There are three primary layers of defense: the edge router, the firewall, and an internal router that connects to the protected LAN.
- **DMZ** - The DMZ can be used for servers that must be accessible from the internet or another external network. The DMZ can be set up between two routers, with an internal router connecting to the protected network and an external router connecting to the unprotected network.



Three Areas of Router Security

Three areas of router security must be maintained:

- **Physical** - Place the router and physical devices that connect to it in a secure locked room that is accessible only to authorized personnel. Install an uninterruptible power supply (UPS) or diesel backup power generator.
- **Operating System** - Configure the router with the maximum amount of memory possible. The availability of memory can help mitigate DoS attacks. Use the latest, stable version of the operating system that meets the feature specifications of the router or network device. Keep a secure copy of router operating system images and router configuration files as backups.
- **Router Hardening** - Ensure that only authorized personnel have access and that their level of access is controlled. Disable unused ports and interfaces. Disable unnecessary services. A router has services that are enabled by default. Some of these services can be used by an attacker to gather information about the router and the network.

Secure the Edge Router

Secure Administrative Access

Securing administrative access is important. If an unauthorized person gains administrative access to a router, that person could alter routing parameters, disable routing functions, or discover and gain access to other systems within the network. Several tasks are involved in securing administrative access to an infrastructure device:

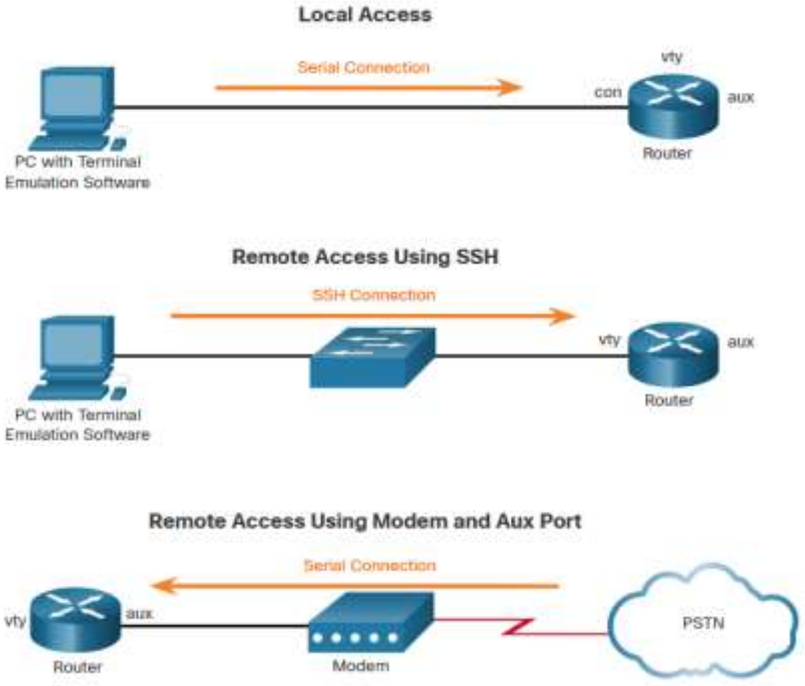
- Restrict device accessibility
- Log and account for all access
- Authenticate access
- Authorize actions
- Present legal notification
- Ensure the confidentiality of data

Secure the Edge Router

Secure Local and Remote Access

A router can be accessed for administrative purposes locally or remotely:

- **Local access** - The administrator must have physical access to the router and use a console cable to connect to the console port. Local access is typically used for initial configuration of the device.
- **Remote access** - Although the aux port option is available, the most common remote access method involves allowing Telnet, SSH, HTTP, HTTPS, or SNMP connections to the router from a computer. The computer can be on the local network or a remote network.



4.2 Configure Secure Administrative Access

Configure Secure Administrative Access

Passwords

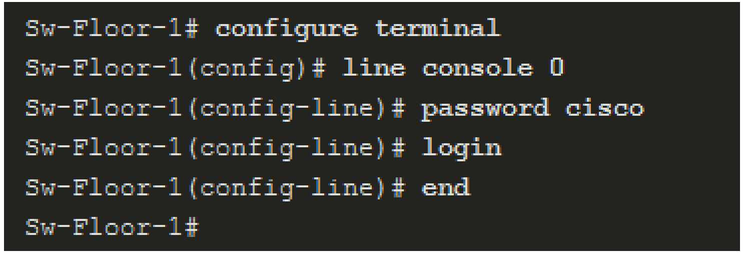
The table shows examples of strong and weak passwords.

Weak Password	Why it is Weak
secret	Simple dictionary password
smith	Maiden name of mother
toyota	Make of a car
bob1967	Name and birthday of the user
Blueleaf23	Simple words and numbers

Strong Password	Why it is Strong
b67n42d39c	Combines alphanumeric characters
12^h u4@1p7	Combines alphanumeric characters, symbols, and includes a space

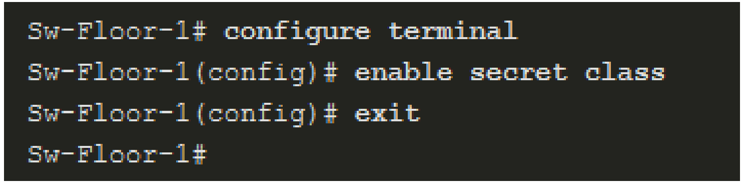
Configure Passwords

To secure user EXEC mode access, enter line console configuration mode using the **line console 0** global configuration command. Specify the user EXEC mode password using the **password** *password* command. Enable user EXEC access using the **login** command.



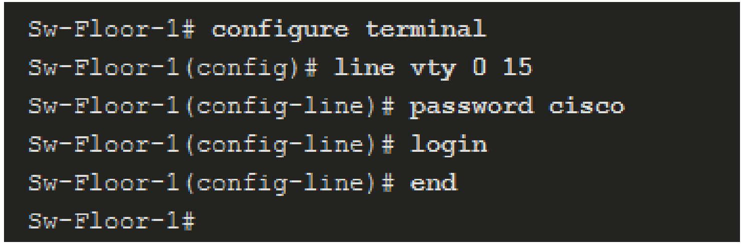
```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

To have administrator access to all IOS commands including configuring a device, you must gain privileged EXEC mode access. To secure privileged EXEC access, use the **enable secret** *password* global config command.



```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

To secure vty lines, enter line vty mode using the **line vty 0 15** global config command. Specify the vty password using the **password** *password* command. Enable vty access using the **login** command.



```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

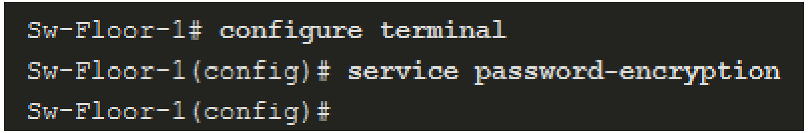
Configure Secure Administrative Access

Encrypt Passwords

Strong passwords are only useful if they are secret. There are several steps that can be taken to help ensure that passwords remain secret on a Cisco router and switch including these:

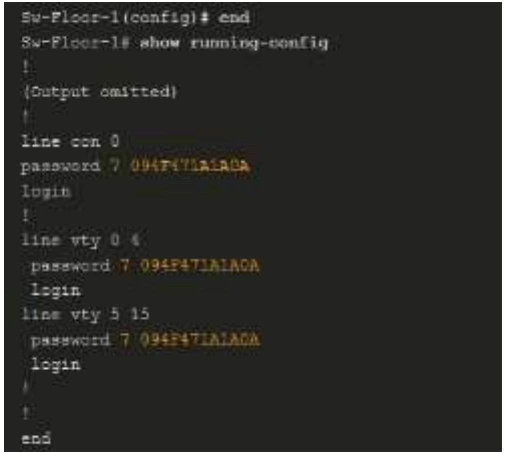
- Encrypting all plaintext passwords
- Setting a minimum acceptable password length
- Deterring brute-force password guessing attacks
- Disabling an inactive privileged EXEC mode access after a specified amount of time.

To encrypt all plaintext passwords, use the **service password-encryption** global config command.



```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)#
```

Use the **show running-config** command to verify that passwords are now encrypted.



```
Sw-Floor-1(config)# end
Sw-Floor-1# show running-config
!
(Output omitted)
!
line con 0
password 7 094F471A1A0A
login
!
line vty 0 4
 password 7 094F471A1A0A
 login
line vty 5 15
 password 7 094F471A1A0A
 login
!
!
end
```

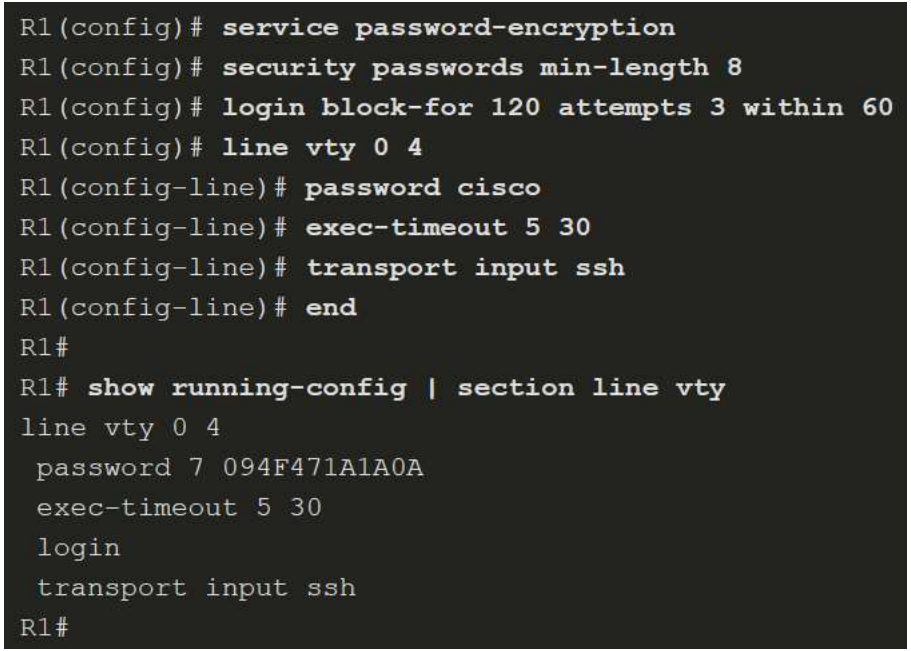
Configure Secure Administrative Access

Additional Password Security

As shown in the sample configuration, the **service password-encryption** global configuration command prevents unauthorized individuals from viewing plaintext passwords in the configuration file.

To ensure that all configured passwords are a minimum of a specified length, use the **security passwords min-length** *length* command in global configuration mode.

Threat actors may use password cracking software to conduct a brute-force attack on a network device. This attack continuously attempts to guess the valid passwords until one works. Use the **login block-for** *seconds* **attempts** *number* **within** *seconds* global configuration command to deter this type of attack.

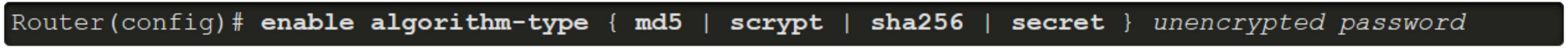


```
R1(config)# service password-encryption
R1(config)# security passwords min-length 8
R1(config)# login block-for 120 attempts 3 within 60
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# exec-timeout 5 30
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
R1# show running-config | section line vty
line vty 0 4
 password 7 094F471A1A0A
 exec-timeout 5 30
 login
 transport input ssh
R1#
```

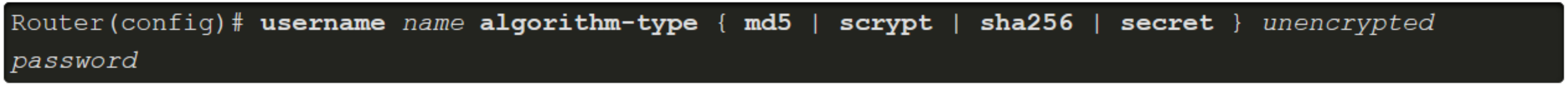
Secret Password Algorithms

MD5 hashes are no longer considered secure because attackers can reconstruct valid certificates. This can allow attackers to spoof any website. The enable secret password uses an MD5 hash by default. It is now recommended that you configure all secret passwords using either type 8 or type 9 passwords. Type 8 and type 9 were introduced in Cisco IOS 15.3(3)M. Type 8 and type 9 use SHA encryption.

To enter an unencrypted password, use the **enable algorithm-type** command syntax:



```
Router(config)# enable algorithm-type { md5 | scrypt | sha256 | secret } unencrypted password
```



```
Router(config)# username name algorithm-type { md5 | scrypt | sha256 | secret } unencrypted
password
```

Algorithm Keyword	Description
md5	Type 5; selects the message digest algorithm 5 (MD5) as the hashing algorithm.
scrypt	Type 9; selects scrypt as the hashing algorithm.
sha256	Type 8: selects Password-Based Key Derivation Function 2 (PBKDF2) with Secure Hash Algorithm, 256-bits (SHA-256) as the hashing algorithm.

4.3 Configure Enhanced Security for Virtual Logins

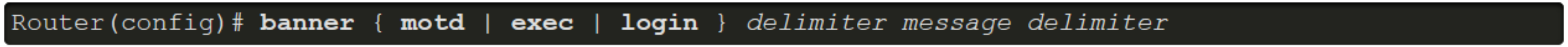
Configure Enhanced Security for Virtual Logins

Enhance the Login Process

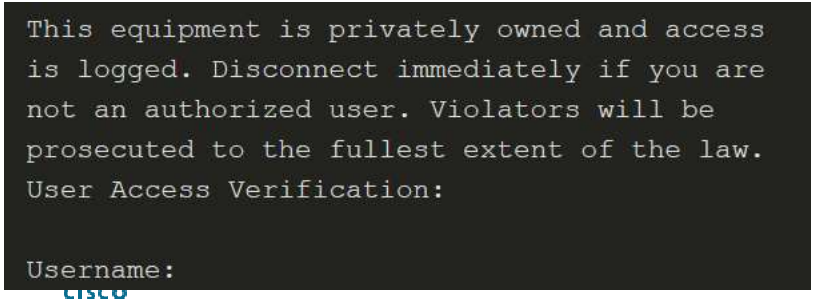
Login blocking is enabling a detection profile that lets you configure a network device to react to repeated failed login attempts by refusing further connection requests.

Access control lists (ACLs) can be used to permit legitimate connections from addresses of known system administrators.

Use the **banner** global configuration mode command to specify appropriate messages. Banners protect the organization from a legal perspective.



```
Router(config)# banner { motd | exec | login } delimiter message delimiter
```



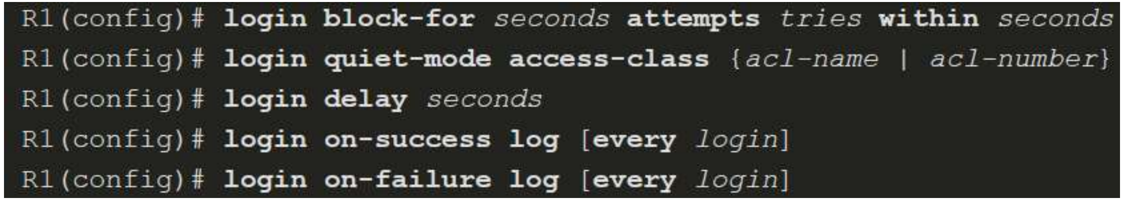
```
This equipment is privately owned and access
is logged. Disconnect immediately if you are
not an authorized user. Violators will be
prosecuted to the fullest extent of the law.
User Access Verification:

Username:
```

Configure Enhanced Security for Virtual Logins

Configure Login Enhancement Features

The **login block-for** command can defend against DoS attacks by disabling logins after a specified number of failed login attempts. The **login quiet-mode** command maps to an ACL that identifies the permitted hosts. The **login delay** command specifies the number of seconds the user must wait between unsuccessful login attempts. The **login on-success** and **login on-failure** commands log successful and unsuccessful login attempts.



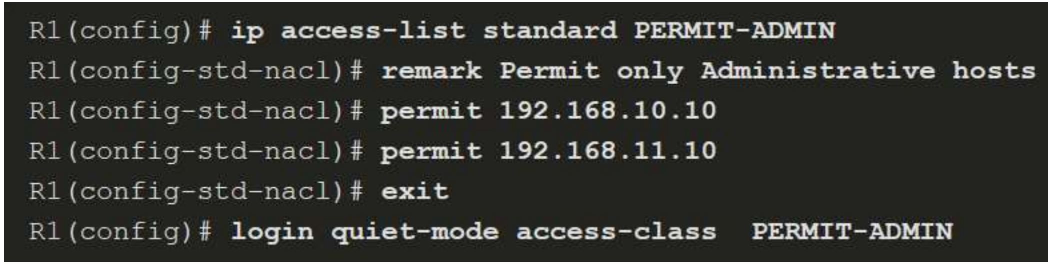
```
R1(config)# login block-for seconds attempts tries within seconds
R1(config)# login quiet-mode access-class {acl-name | acl-number}
R1(config)# login delay seconds
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
```

Configure Enhanced Security for Virtual Logins

Enable Login Enhancements

To help a Cisco IOS device provide DoS detection, use the **login block-for** command, which must be issued before any other login command. The **login block-for** command monitors login device activity and operates in two modes:

- **Normal mode** - Also called watch mode, the router keeps count of the number of failed login attempts within an identified amount of time.
- **Quiet mode** – Also called the quiet period. If the number of failed logins exceeds the configured threshold, all login attempts using Telnet, SSH, and HTTP are denied for the time specified in the **login block-for** command.

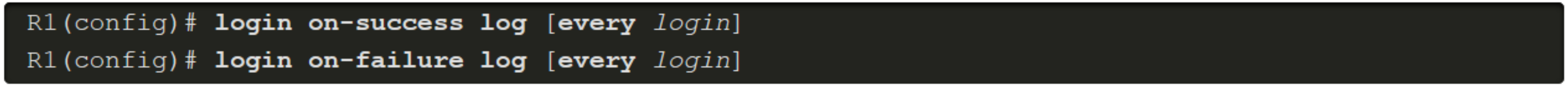


```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class  PERMIT-ADMIN
```

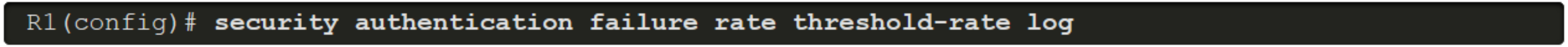
Configure Enhanced Security for Virtual Logins

Log Failed Attempts

There are three commands that can be configured to help an administrator detect a password attack. Each lets a device to generate syslog messages for failed or successful login attempts. The first two commands, **login on-success log** and **login on-failure log**, generate syslog messages for successful and unsuccessful login attempts. An alternative to the **login on-failure log** command is the **security authentication failure rate** command can be configured to generate a log message when the login failure rate is exceeded.



```
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
```



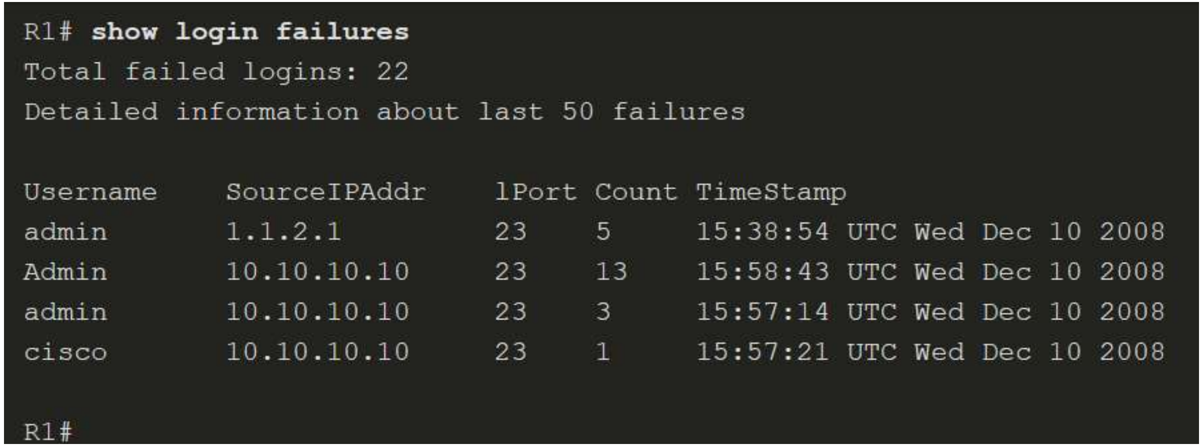
```
R1(config)# security authentication failure rate threshold-rate log
```

Configure Enhanced Security for Virtual Logins

Log Failed Attempts (Cont.)

Use the **show login** command to verify the **login block-for** command settings and current mode.

The **show login failures** command displays additional information regarding the failed attempts, such as the IP address from which the failed login attempts originated.



```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures

Username    SourceIPAddr    lPort Count TimeStamp
admin       1.1.2.1         23    5     15:38:54 UTC Wed Dec 10 2008
Admin       10.10.10.10     23    13    15:58:43 UTC Wed Dec 10 2008
admin       10.10.10.10     23    3     15:57:14 UTC Wed Dec 10 2008
cisco       10.10.10.10     23    1     15:57:21 UTC Wed Dec 10 2008

R1#
```

4.4 Configure SSH

Configure SSH

Enable SSH

Configure a Cisco device to support SSH using the following six steps:

Step 1. Configure a unique device hostname.

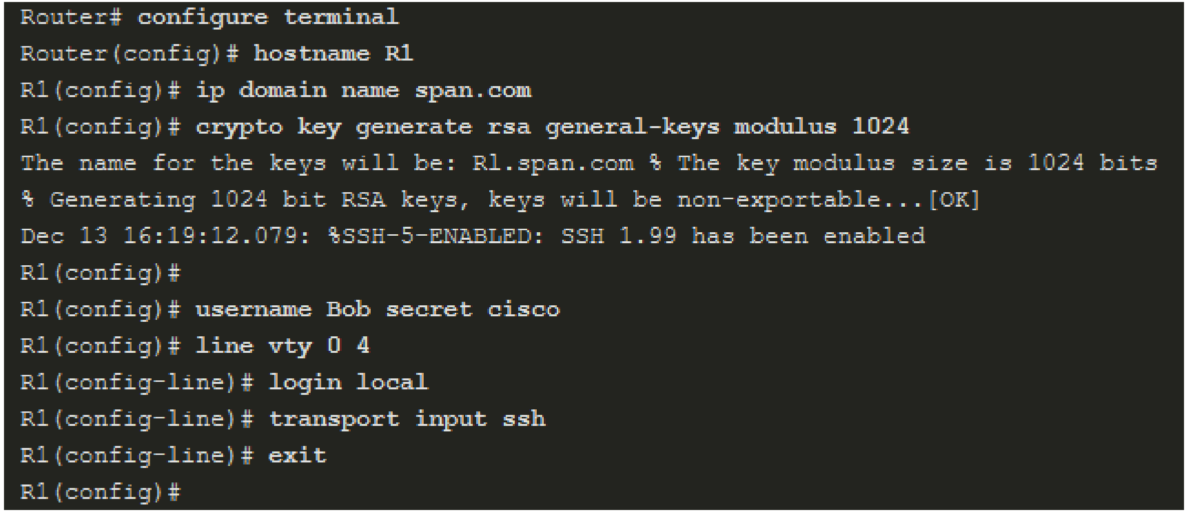
Step 2. Configure the IP domain name.

Step 3. Generate a key to encrypt SSH traffic.

Step 4. Verify or create a local database entry.

Step 5. Authenticate against the local database.

Step 6. Enable vty inbound SSH sessions.

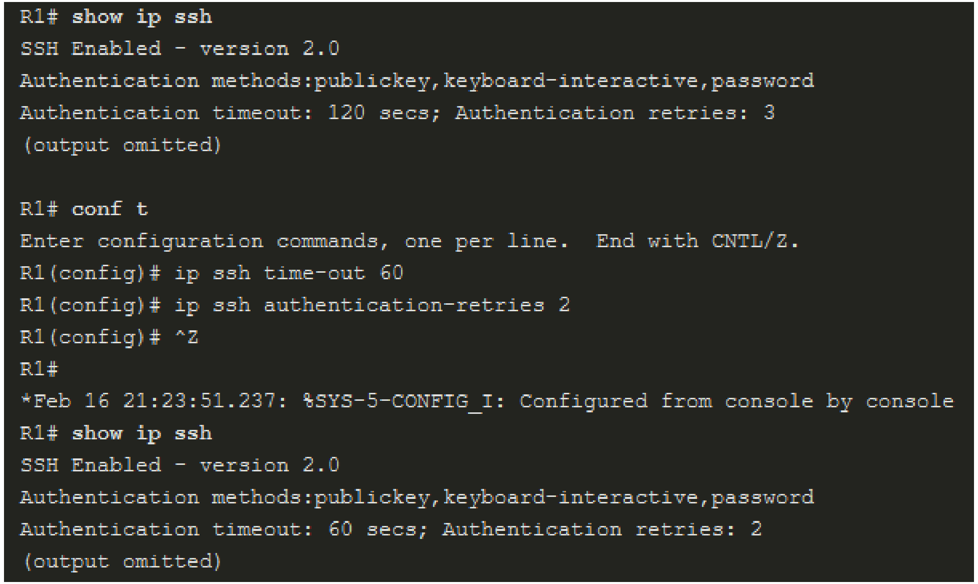


```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
R1(config)#
```

Configure SSH

Enhance SSH Login Security

To verify the optional SSH command settings, use the **show ip ssh** command. Use the **ip ssh time-out** *seconds* global configuration mode command to modify the default 120-second timeout interval. This configures the number of seconds that SSH can use to authenticate a user. By default, a user logging in has three attempts to enter the correct password before being disconnected. To configure a different number of consecutive SSH retries, use the **ip ssh authentication-retries** *integer* global configuration mode command.



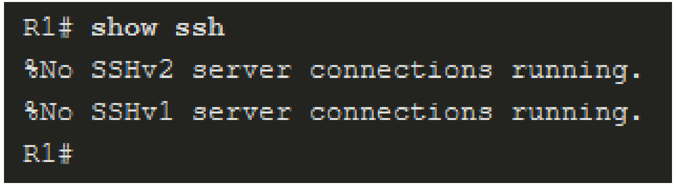
```
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 120 secs; Authentication retries: 3
(output omitted)

R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
*Feb 16 21:23:51.237: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 60 secs; Authentication retries: 2
(output omitted)
```

Connect a Router to an SSH-Enabled Router

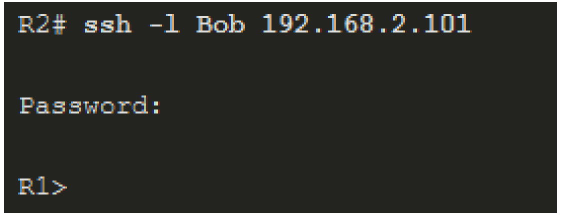
To verify the status of the client connections, use the **show ssh** command. There are two different ways to connect to an SSH-enabled router. By default, when SSH is enabled, a Cisco router can act as an SSH server or SSH client. As a server, a router can accept SSH client connections. As a client, a router can connect via SSH to another SSH-enabled router.

Check SSH Status



```
R1# show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
R1#
```

Connect from R2
To R1

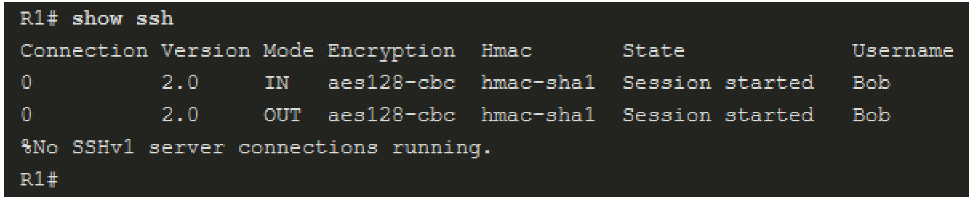


```
R2# ssh -l Bob 192.168.2.101

Password:

R1>
```

View SSH Connections



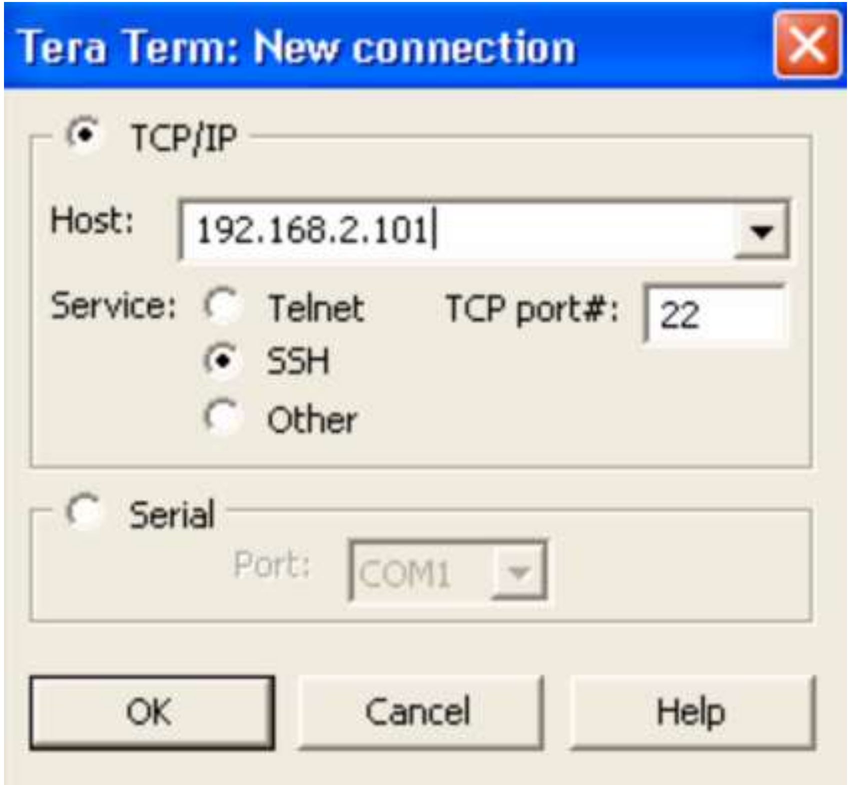
```
R1# show ssh
Connection Version Mode Encryption  Hmac       State           Username
0          2.0     IN   aes128-cbc  hmac-sha1  Session started  Bob
0          2.0     OUT  aes128-cbc  hmac-sha1  Session started  Bob
%No SSHv1 server connections running.
R1#
```

Configure SSH

Connect a Host to an SSH-Enabled Router

Connect using an SSH client (e.g., PuTTY, OpenSSH, TeraTerm) running on a host.

Generally, the SSH client initiates an SSH connection to the router. The router SSH service prompts for the correct username and password combination. After the login is verified, the router can be managed as if the administrator was using a standard Telnet session.



● TCP/IP

Host: 192.168.2.101

Service: ○ Telnet ● SSH ○ Other

TCP port#: 22

○ Serial

Port: COM1

Lab - Configure Secure Administrative Access

In this lab, you will complete the following objectives:

- Part 1: Configure Basic Device Settings
- Part 2: Configure and Encrypt Passwords on Routers R1 and R3
- Part 3: Configure Enhanced Username Password Security on Routers R1 and R3
- Part 4: Configure the SSH Server on Routers R1 and R3

Packet Tracer - Configure Secure Passwords and SSH

The network administrator has asked you to prepare RTA and SW1 for deployment. Before they can be connected to the network, security measures must be enabled.

Lab - Configure Network Devices with SSH

In this lab, you will complete the following objectives:

- Part 1: Configure Basic Device Settings
- Part 2: Configure the Router for SSH Access
- Part 3: Configure the Switch for SSH Access
- Part 4: SSH from the CLI on the Switch

4.5 Secure Device Access Summary

Secure Device Access Summary

What Did I Learn in this Module?

- The edge router is the last router between the internal network and an untrusted network, such as the internet.
- The three approaches to this are the single router approach, defense-in-depth approach, and the DMZ approach.
- There are three primary layers of defense: the edge router, the firewall, and an internal router that connects to the protected LAN.
- The DMZ can be set up between two routers, with an internal router connecting to the protected network and an external router connecting to the unprotected network.
- The three areas of router security that must be maintained are physical security, operating system security, and router hardening.
- A router can be accessed for administrative purposes locally or remotely.
- To encrypt all plaintext passwords, use the **service password-encryption** global config command.
- The Cisco IOS login enhancements provide more security by slowing down attacks, such as dictionary attacks and DoS attacks.

What Did I Learn in this Module? (cont.)

- Login enhancements include login block-for, login quiet-mode, login delay, login on-success, login on-failure, and ip ssh time-out commands.
- It is possible to configure a Cisco device to support SSH using the following six steps: configure a unique device hostname, configure the IP domain name, generate a key to encrypt SSH traffic, verify or create a local database entry, authenticate against the local database, and enable vty inbound SSH sessions.

Secure Device Access Summary

New Terms and Commands

- edge router
- trusted and untrusted networks
- Defense-in-Depth
- demilitarized zone (DMZ) network
- local access
- remote access
- **line console 0**
- **password**
- **enable secret**
- **line vty 0 15**
- **login**
- **service password-encryption**
- **show running-config**
- **banner** { **motd** | **exec** | **login** } *delimiter message delimiter*
- **login block-for** *seconds* **attempts** *tries* **within** *seconds*
- **login quiet-mode access-class** {*acl-name* | *acl-number*}
- **login delay** *seconds*
- **login on-success log** [**every** *login*]
- **login on-failure log** [**every** *login*]
- normal and quiet modes
- **security authentication failure rate**
- **hostname** *name*
- **ip domain name name**
- **crypto key generate rsa general-keys modulus** *value*
- **username** *name* **secret** *password*
- **login local**
- **transport input ssh**
- **show ip ssh**
- **ip ssh time-out** *seconds*
- **ip ssh authentication retries** *integer*

Secure Device Access Summary

New Terms and Commands

- **show ssh**
- **ssh -l** *username* {*ip address* | *hostname*}
- PuTTY, OpenSSH, and TeraTerm