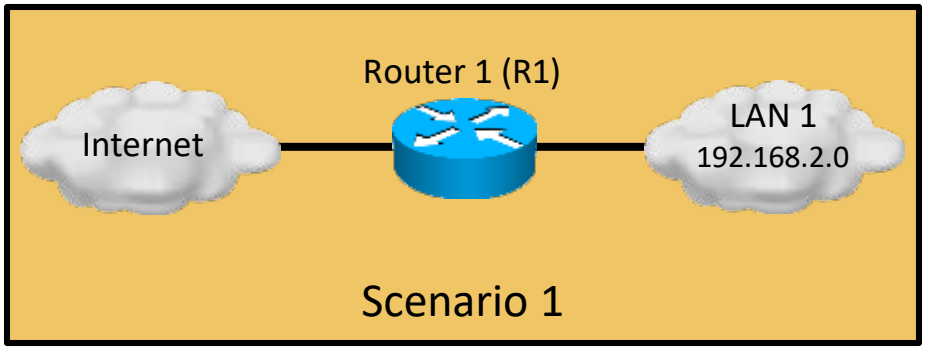
CIS 4080
Network Security

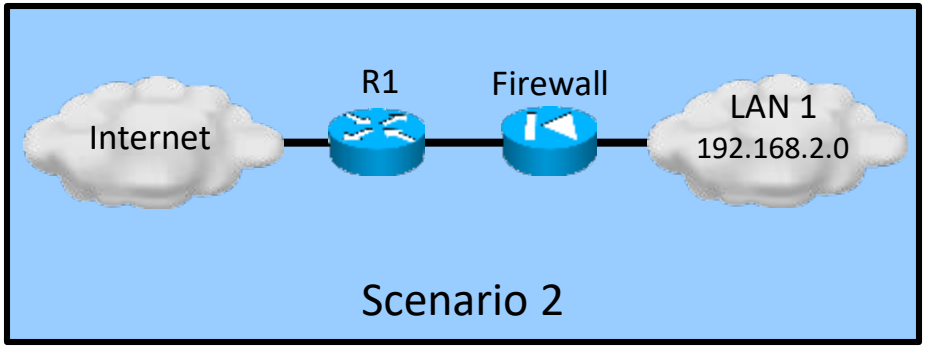
Securing Network Devices, Part 1

Enforcing Perimeter Security Policy

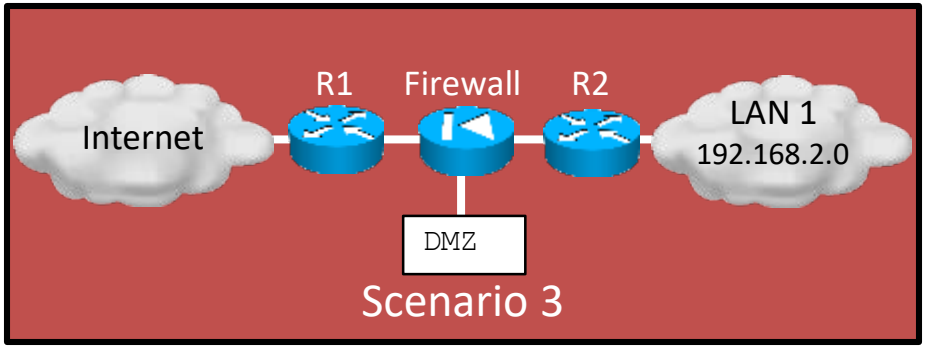
- Routers are used to secure the network perimeter.
- Scenario 1:
  - The router protects the LAN.



- Scenario 2:
  - The router screens traffic before a firewall (e.g., Cisco's Adaptive Security Appliance (ASA)).



- Scenario 3:
  - The zone directly connected to the firewall is called a DMZ (demilitarized zone).
  - Internet-accessible servers are located in the DMZ.



Three Areas of Router Security

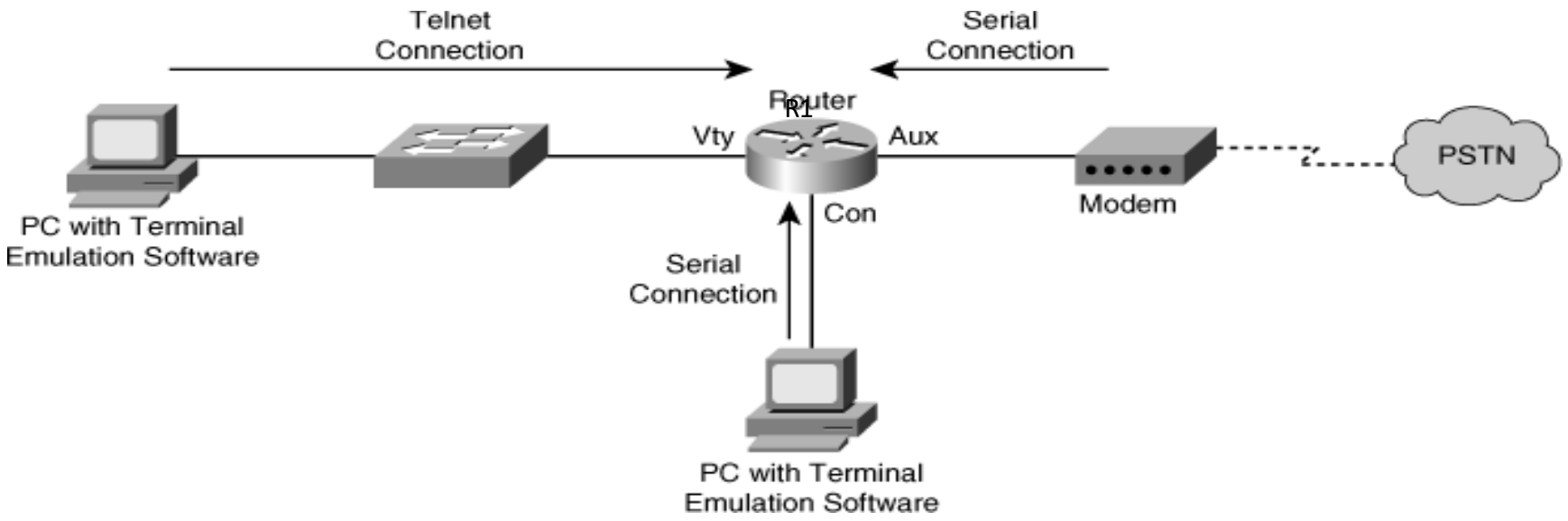
- Physical security
  - Secure infrastructure equipment in a locked room that:
    - Is accessible only to authorized personnel.
    - Is free of electrostatic or magnetic interference.
    - Has fire suppression.
    - Has controls for temperature and humidity.
  - Install an uninterruptible power supply (UPS) and keep spare components available to reduce the possibility of a DoS attack from power loss to the building.

Three Areas of Router Security

- Operating system
  - Configure the router with the maximum amount of memory possible.
    - Helps protect it from some DoS attacks.
  - Use the latest stable version of the operating system that meets the feature requirements of the network.
  - Keep a secure copy of the router operating system image and router configuration file as a backup.

Three Areas of Router Security

- Router hardening
  - Secure administrative control to ensure that only authorized personnel have access and that their level of access is controlled.
  - Disable unused ports and interfaces to reduce the number of ways a device can be accessed.
  - Disable unnecessary services that can be used by an attacker to gather information or for exploitation.



Secure Administrative Access

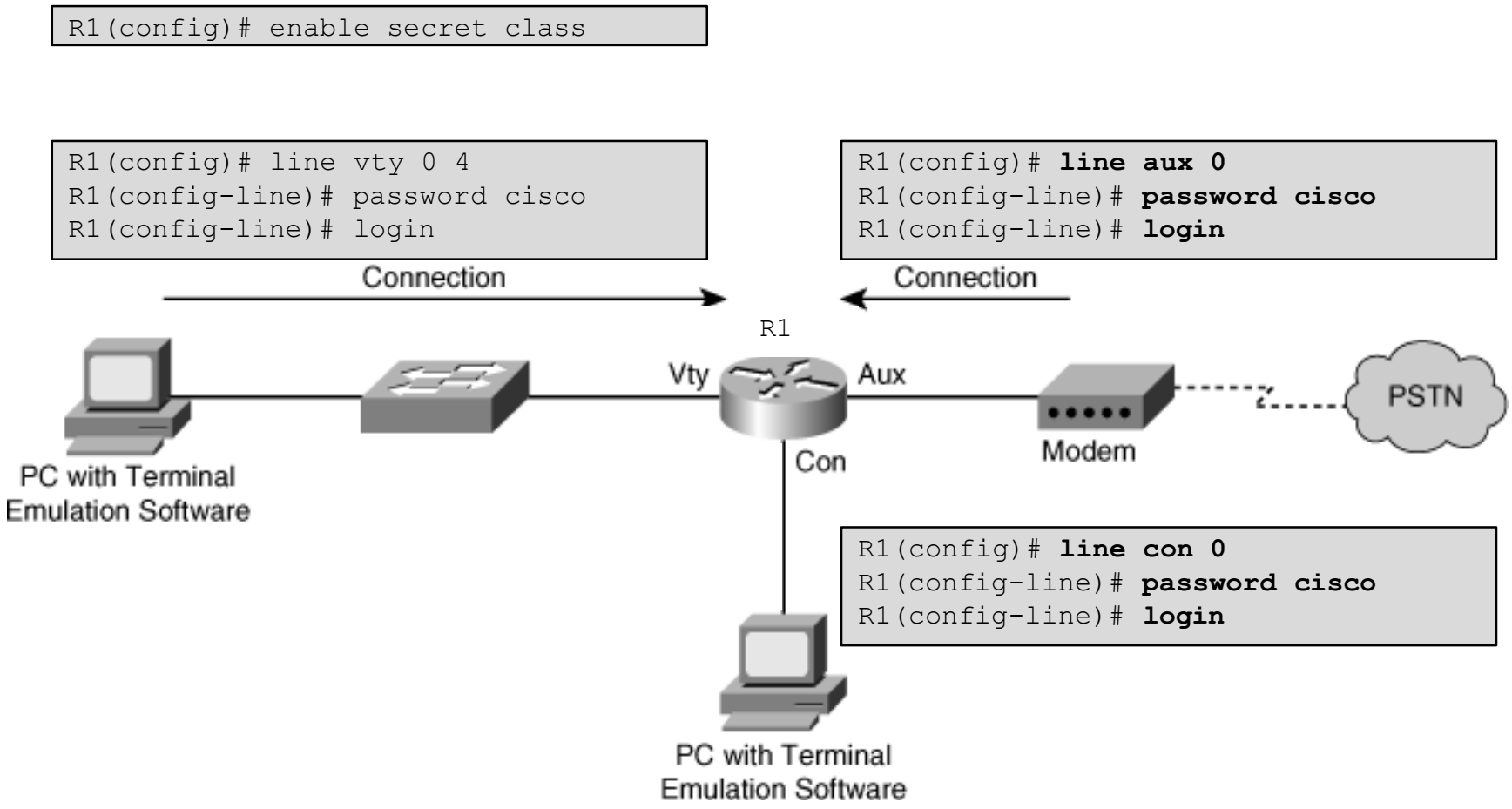
- Restrict device accessibility
  - Limit the accessible ports, restrict the permitted communicators, and restrict the permitted methods of access.
- Log and account for all access
  - For auditing purposes, record anyone who accesses a device, including what occurs and when.
- Authenticate access
  - Ensure that access is granted only to authenticated users, groups, and services.
  - Limit the number of failed login attempts and the time between logins.

Secure Administrative Access

- Authorize actions
  - Restrict the actions and views permitted by any particular user, group, or service.
- Present Legal Notification
  - Display a legal notice, developed in conjunction with company legal counsel, for interactive sessions.
- Ensure the confidentiality of data
  - Protect locally stored sensitive data from viewing and copying.
  - Consider the vulnerability of data in transit over a communication channel to sniffing, session hijacking, and man-in-the-middle (MITM) attacks.

Cisco Router Passwords

- All routers need a locally configured password for privileged access and other access.



Cisco Router Passwords

- To steal passwords, attackers:
  - Shoulder surf.
  - Guess passwords based on the user's personal information.
  - Sniff TFTP packets containing plaintext configuration files.
  - Use readily available brute force attack tools such as L0phtCrack or Cain & Abel.
- Strong passwords are the primary defense against unauthorized access to a router!

Strong Passwords

- Passwords should NOT use dictionary words
  - Dictionary words are vulnerable to dictionary attacks.
- Passwords may include the following:
  - Any alphanumeric character.
  - A mix of uppercase and lowercase characters.
  - Symbols and spaces.
  - A combination of letters, numbers, and symbols.

Note:

  - Password-leading spaces are ignored, but all spaces after the first character are NOT ignored.

Strong Passwords

- Change passwords frequently.
  - Implement a policy defining when and how often the passwords must be changed.
  - Limits the window of opportunity for a hacker to crack a password.
  - Limits the window of exposure after a password has been cracked.
- Local rules can make passwords even safer.

Passphrases

- One well known method of creating strong passwords is to use **passphrases.**
  - Basically a sentence / phrase that serves as a more secure password.
  - Use a sentence, quote from a book, or song lyric that you can easily remember as the basis of the strong password or pass phrase.
- For example:
  - “My favorite spy is James Bond 007.” = MfsiJB007
  - “It was the best of times, it was the worst of times.” = Iwtbotiwtwot
  - “Fly me to the moon. And let me play among the stars.” = FmttmAlmpats

Password Protection Guidelines

- Use a password length of 10 or more characters. The longer, the better.
- Make passwords complex by including a mix of UPPERCASE and lowercase letters, numbers, symbols, and spaces.
- Avoid passwords based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, such as birthdates, ID numbers, ancestor names, or other easily identifiable pieces of information.
- Deliberately misspell a password.
  - For example, Smith = Smyth = 5mYth or Security = 5ecur1ty.
- Change passwords often so if a password is unknowingly compromised, the window of opportunity for the attacker to use the password is limited.
- Do not write passwords down and leave them in obvious places such as on the desk or monitor.

Cisco Router Passwords

- To increase the security of passwords, the following Cisco IOS commands should be utilized:
  - Enforce minimum password length:
    `(config)# security passwords min-length`.
  - Disable unattended connections:
    `(config-line)# exec-timeout`.
  - Encrypt config file passwords:
    `(config)# service password-encryption`.
  - The last feature only obscures the password from view by shoulder surfers. It is not a serious encryption.

Enforce Minimum Password Lengths

- Make passwords lengthy.
  - IOS 12.3 and later passwords can be 0 to 16 characters in length.
  - The best practice is to have a minimum of 10 characters.
- To enforce the minimum length use the global command:
  - **`security passwords min-length`** *`length`*
- The command affects all “new” router passwords.
  - Existing router passwords are unaffected.
- Any attempt to create a new password that is less than the specified length fails and results a “Password too short” error message.

Disable Unattended Connections

- By default, an administrative interface stays active and logged in for 10 minutes after the last session activity.
  - After that, the interface times out and logs out of the session.
- The timer can be adjusted using the **`exec-timeout`** command in line configuration mode for each of the line types that are used.
  - **`exec-timeout`** *`minutes seconds`*

Note:

- **`exec-timeout 0 0`** means that there will be no timeout and the session will stay active for an unlimited time.
  - Great for Labs …
  - Bad in production networks!
  - Never set the value to 0!

Disable Unattended Connections

- Default time is 10 minutes.
- Terminates an unattended connection (console or vty).
- Provides additional level of security if an administrator walks away from an active console session.

```
Router(config-line)#
exec-timeout minutes [seconds]
```

– To terminate an unattended console connection:

```
Sudbury(config)# line console 0
Sudbury(config-line)# exec-timeout 3 30
```

– To disable the configured timeout:

```
Sudbury(config)# line aux 0
Sudbury(config-line)# no exec-timeout
```

Encrypt All Passwords

- Encrypt all passwords in the router configuration file.

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

```
R1(config)# service password-encryption
R1(config)# exit
R1# show running-config
enable password 7 06020026144A061E
!
line con 0
 password 7 094F471A1A0A
login
!
line aux 0
 password 7 01100F175804575D72
 login
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 login
```

Securing Local Database Passwords

- Secure the local database passwords.
  - Traditional user configuration with plaintext password.

```
username name password {[0] password | 7 hidden-password}
```

  - Use MD5 hashing for strong password protection.
  - More secure than the type 7 encryption.

```
username name secret {[0] password | encrypted-secret}
```

Securing Local Database Passwords

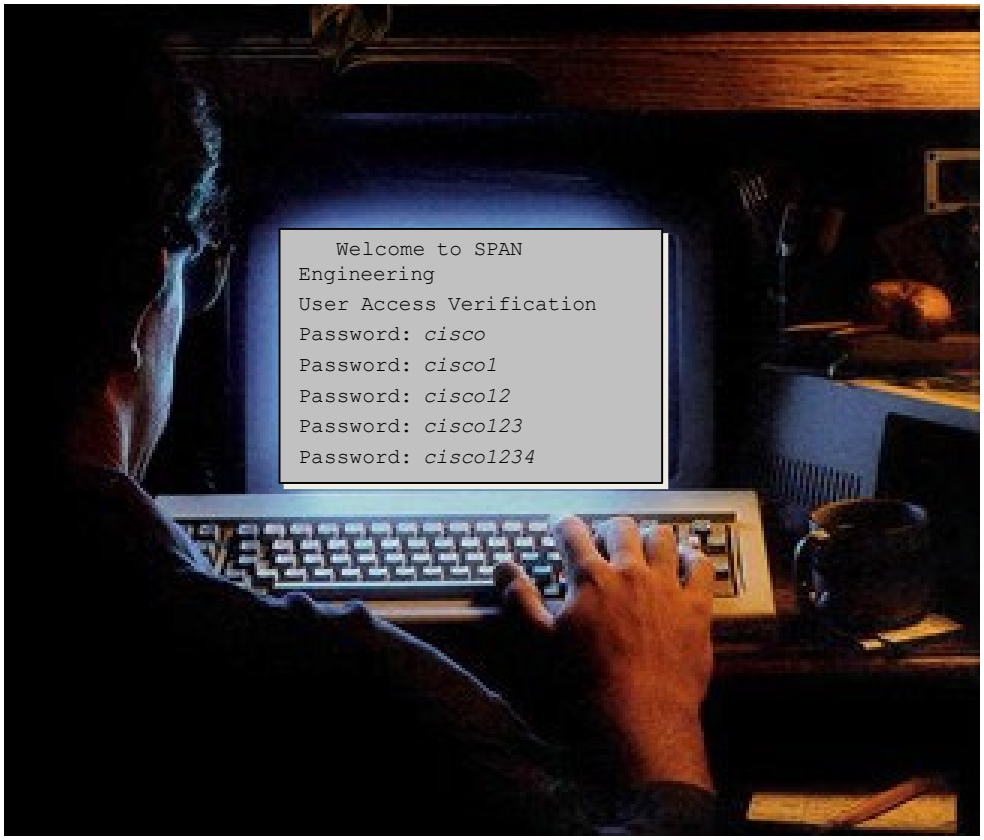
```
R1# configure terminal
R1(config)# username JR-ADMIN password letmein
% Password too short - must be at least 10 characters. Password configuration
failed
R1(config)# username JR-ADMIN password cisco12345
R1(config)# username ADMIN secret cisco54321
R1(config)# line con 0
R1(config-line)# login local
```

```
R1# show run | include username
username JR-ADMIN password 7 060506324F41584B564347
username ADMIN secret 5 $1$G3oQ$hEvsd5iz76WJuSJvtzs8I0
R1#
```

```
R1 con0 is now available

Press RETURN to get started.

User Access Verification

Username: ADMIN
Password:
R1>
```

Secure Virtual Logins

- To improve security for virtual login connections, the login process should be configured with specific parameters:
  - Implement delays between successive login attempts.
  - Enable login shutdown if DoS attacks are suspected.
  - Generate system logging messages for login detection.



Disable Login for Excessive Attempts

```
R1# configure terminal
R1(config)# username ADMIN secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config)# exit
R1(config)# login block-for 120 attempts 5 within 60
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
R1(config)# login delay 10
R1(config)# login on-success log
R1(config)# login on-failure log
R1(config)# exit
```

- In this sample config, if more than 5 login failures occur within 60 seconds, then all logins will be disabled for 120 seconds.
  - This command must be issued before any other login command can be used.
  - The command also helps provide DoS detection and prevention.
- The PERMIT-ADMIN commands exempt administrative stations from the disabled login.
  - If not configured, all login requests will be denied during the Quiet-Mode.

Verify Login Security

```
R1# show login
     A login delay of 10 seconds is applied.
     Quiet-Mode access list PERMIT-ADMIN is applied.

     Router enabled to watch for login Attacks.
     If more than 5 login failures occur in 60 seconds or less,
     logins will be disabled for 120 seconds.

     Router presently in Normal-Mode.
     Current Watch Window
         Time remaining: 5 seconds.
         Login failures for current window: 4.
     Total login failures: 4.
```

- In this example, the **`login block-for`** command was configured to block login hosts for 120 seconds if more than 5 login requests fail within 60 seconds.

Verify Login Security When in Quiet

```
R1#
*Dec 10 15:38:54.455: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching
failures is 12 secs, [user: admin] [Source: 10.10.10.10] [localport: 23] [Reason:
Login Authentication Failed - BadUser] [ACL: PERMIT-ADMIN] at 15:38:54 UTC Wed
Dec 10 2008

R1# show login
     A login delay of 10 seconds is applied.
     Quiet-Mode access list PERMIT-ADMIN is applied.

     Router enabled to watch for login Attacks.
     If more than 5 login failures occur in 60 seconds or less,
     logins will be disabled for 120 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 105 seconds.
     Restricted logins filtered by applied ACL PERMIT-ADMIN.

R1#
```

- In this example, a 6th failed attempt at logging has occurred.
  - A log message is initiated at the console stating that the router is in Quiet-Mode.
  - All login attempts made using Telnet, SSH, and HTTP are denied except as specified by the PERMIT-ADMIN ACL.

Verify Login Security When in Quiet Mode

```
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 2011
Admin           10.10.10.10     23    13    15:58:43 UTC Wed Dec 10 2011
admin           10.10.10.10     23    3     15:57:14 UTC Wed Dec 10 2011
cisco           10.10.10.10     23    1     15:57:21 UTC Wed Dec 10 2011

R1#
```

- In this example, the command identifies the number of failures, usernames tried, and offending IP addresses with a timestamp added to each unsuccessful attempt.

Provide Legal Notification

- Banner messages should be used to warn would-be intruders that they are not welcome on your network.
- Banners are important, especially from a legal perspective.
  - Intruders have been known to win court cases because they did not encounter appropriate warning messages.
  - Choosing what to place in banner messages is extremely important and should be reviewed by legal counsel before being implemented.
  - Never use the word “welcome” or any other familiar or similar greeting that may be misconstrued as an invitation to use the network.

Configuring Banner Messages

- Specify what is “proper use” of the system.
- Specify that the system is being monitored.
- Specify that privacy should not be expected when using this system.
- Do not use the word “welcome.”
- Have legal department review the content of the message.

```
Router(config)#
banner {exec | incoming | login | motd | slip-ppp} d message d
```

Protecting vty Line Access #1

- By default, Cisco routers do NOT have any line- level passwords configured for vty lines.
  - Passwords must be configured for all of the vty lines on the router.
  - Remember that more vty lines can be added to the router.
- If password checking is enabled (i.e., the **`login`** command), a vty password must also be configured before attempting to access the router using Telnet.
  - If a vty password is NOT configured and password checking is enabled for vty, an error message similar to the following will be produced:

```
Telnet 10.0.1.2
Trying 10.0.1.2 ….. open
Password required, but none set
[Connection to 10.0.1.2 closed by foreign host]
```

Protecting vty Line Access #2

- If an enable mode password is NOT set for the router, privileged-EXEC mode can NOT be accessed using Telnet.
- Always use the **`enable secret`** *`password`* command to set the enable password.
  - Never use the **`enable password`** command!