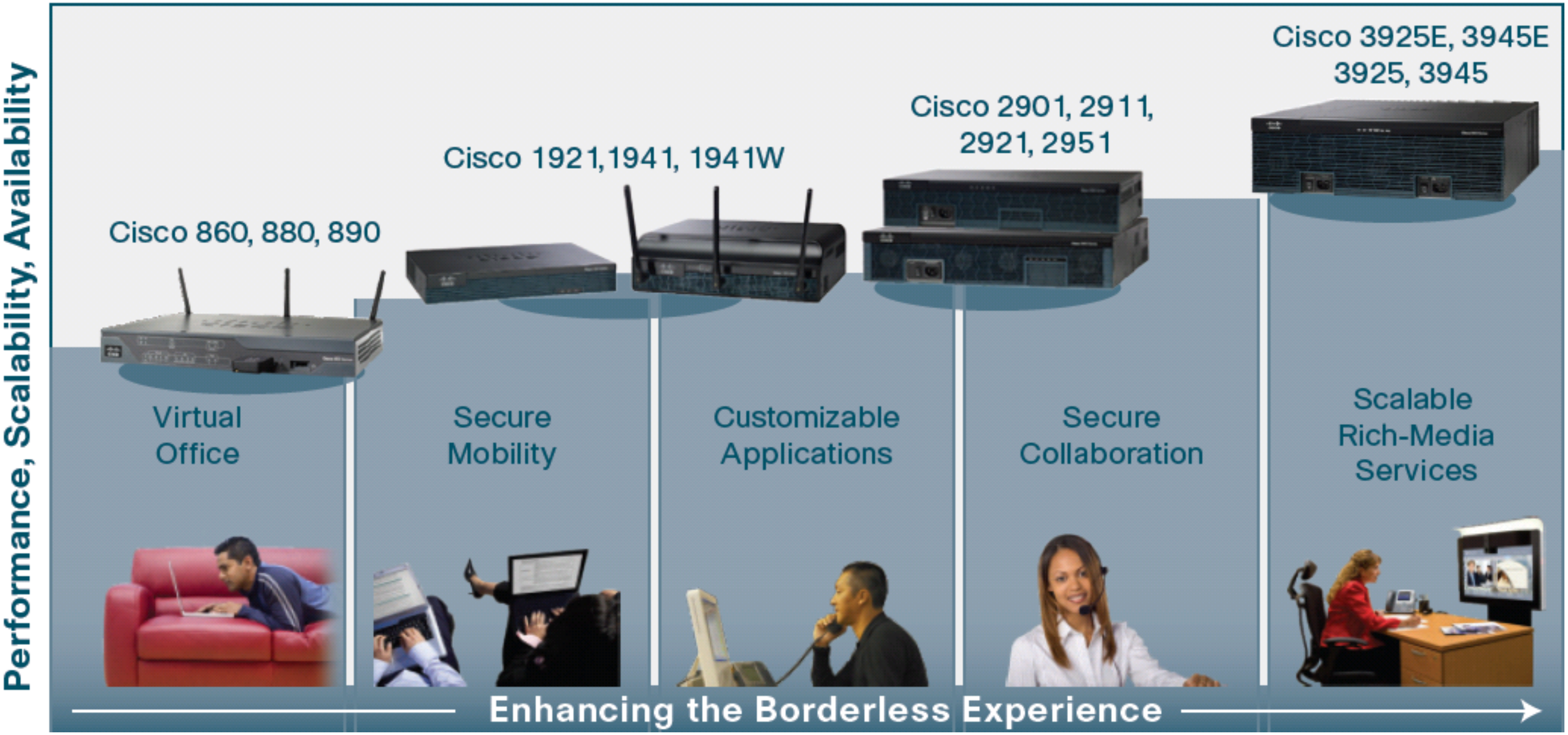
Securing Network Devices

Cisco Integrated Services Routers G2

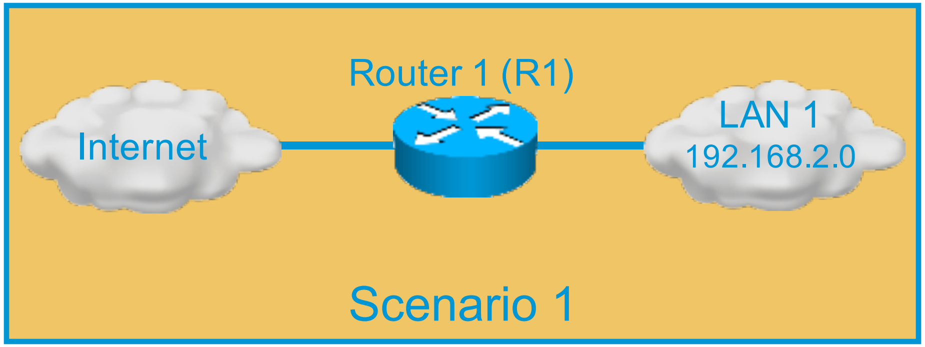
- Cisco has a new Series of 2nd Generation Routers.
- G2 ISRs have integrated Gigabit Ethernet interfaces.


Performance, Scalability, Availability
Cisco 860, 880, 890
Cisco 1921,1941, 1941W
Cisco 2901, 2911, 2921, 2951
Cisco 3925E, 3945E 3925, 3945
Virtual Office
Secure Mobility
Customizable Applications
Secure Collaboration
Scalable Rich-Media Services
Enhancing the Borderless Experience

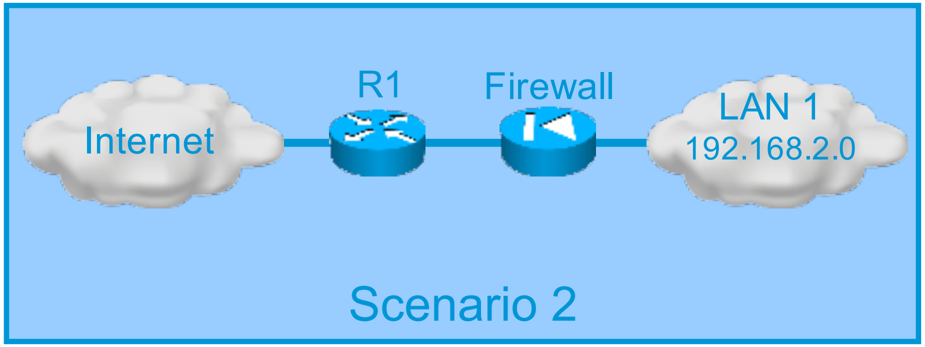
http://www.cisco.com/en/US/products/ps10906/Products_Sub_Category_Home.html#

Enforcing Perimeter Security Policy

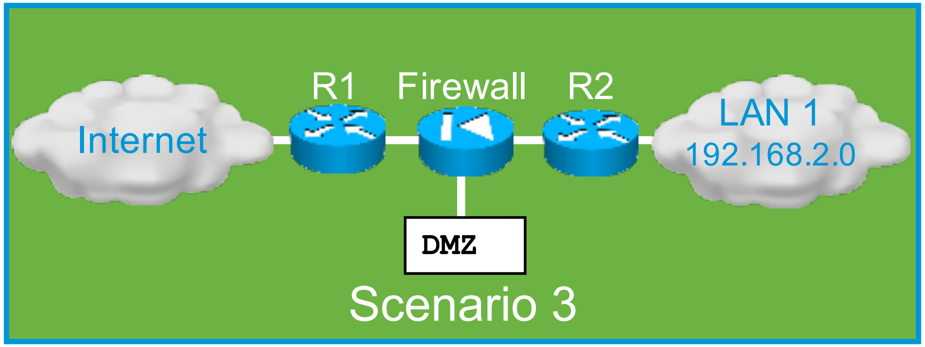
- Routers are used to secure the network perimeter.
- Scenario 1:
  - The router protects the LAN.



- Scenario 2:
  - The router screens traffic before a firewall (PIX/ASA).



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



Three Areas of Router Security

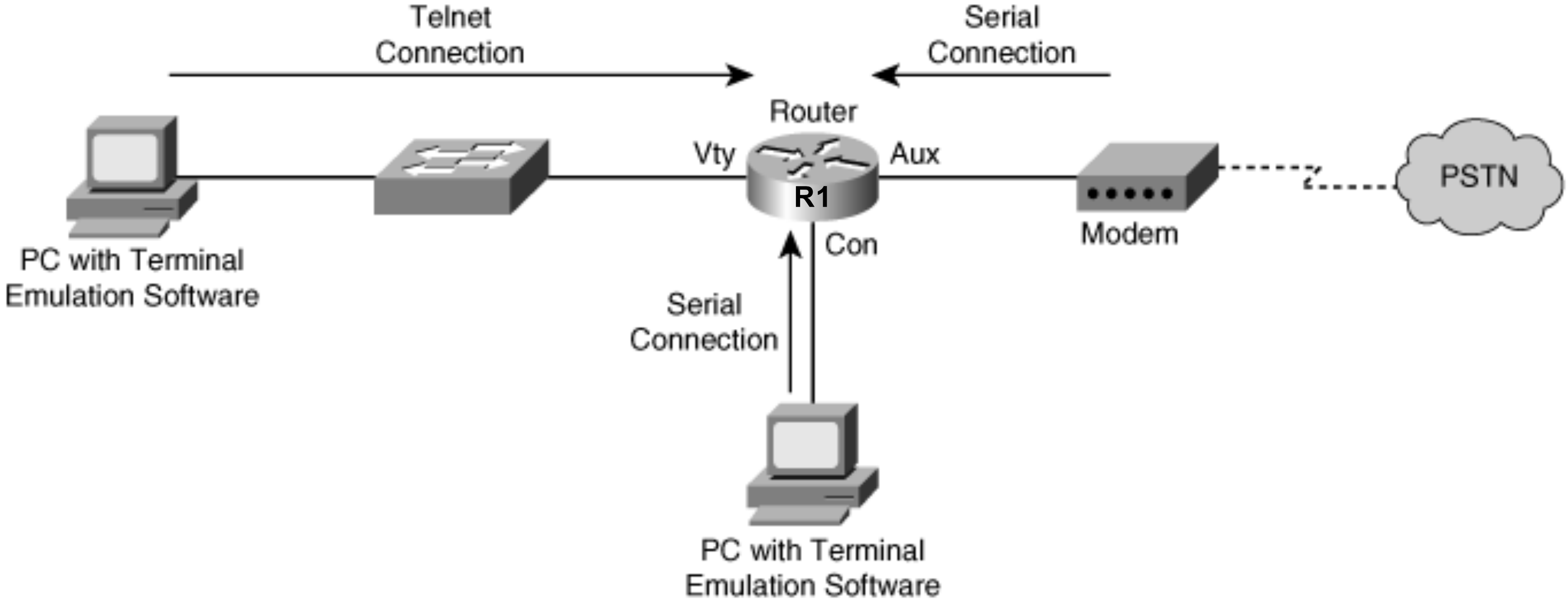
- Physical security
  - Secure infrastructure equipment in a locked room that:
    - Is accessible only to authorized personnel.
    - Is free of electrostatic or magnetic interference.
    - Has fire suppression.
    - Has controls for temperature and humidity.
  - Install an uninterruptible power supply (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

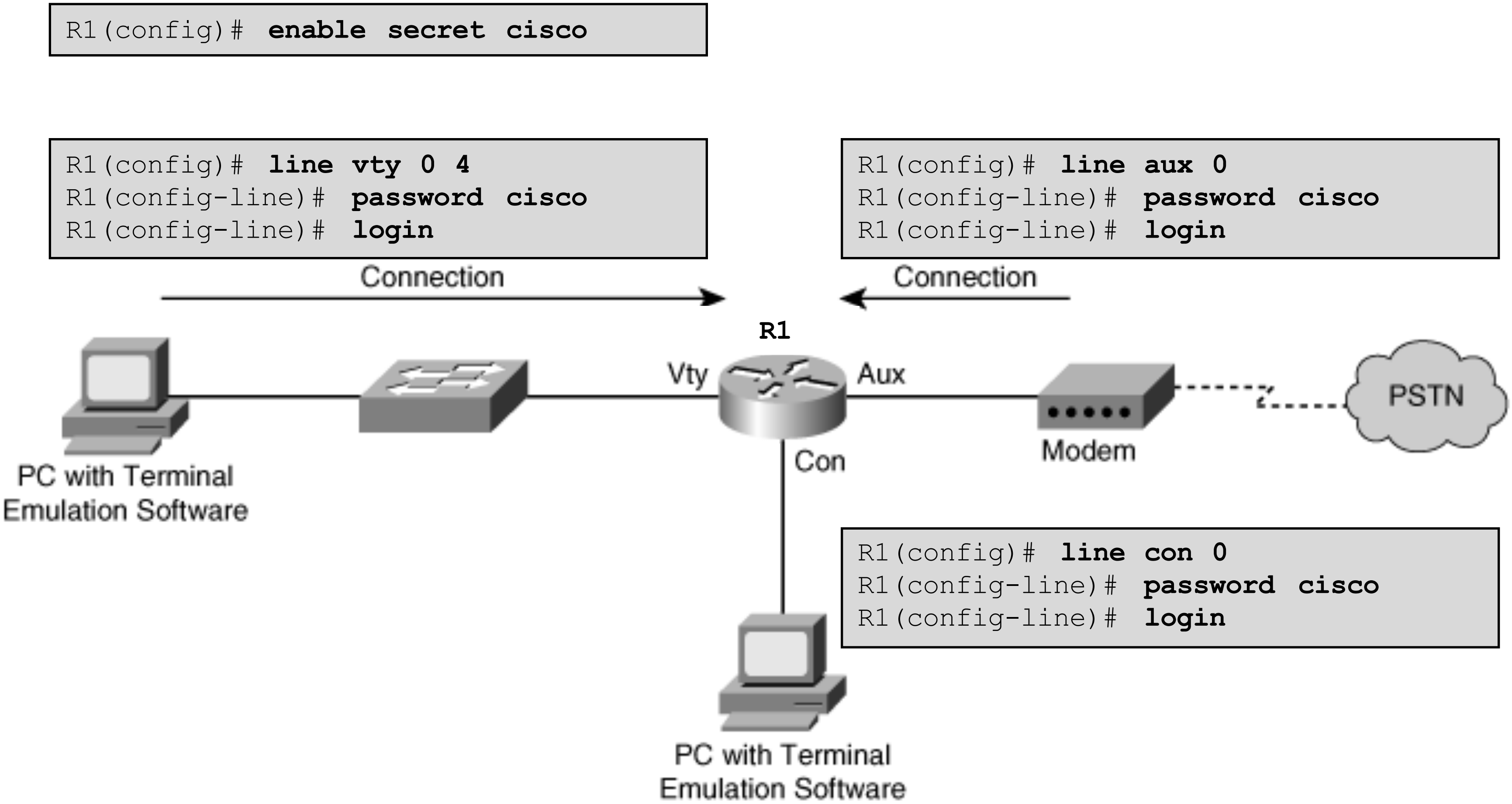
- Restrict device accessibility
  - Limit the accessible ports, restrict the permitted communicators, and restrict the permitted methods of access.
- Log and account for all access
  - For auditing purposes, record anyone who accesses a device, including what occurs and when.
- Authenticate access
  - 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.



```
R1(config)# enable secret cisco
```

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

```
R1(config)# line aux 0
R1(config-line)# password cisco
R1(config-line)# login
```

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

Connection
Connection
R1
Vty
Aux
Con
Modem
PSTN
PC with Terminal Emulation Software
PC with Terminal Emulation Software

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: **`security passwords min-length`**.
  - Disable unattended connections: **`exec-timeout`**.
  - Encrypt config file passwords: **`service password-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 in an “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 after 3 minutes and 30 seconds:

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

  - To disable the exec process on the line:

```
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

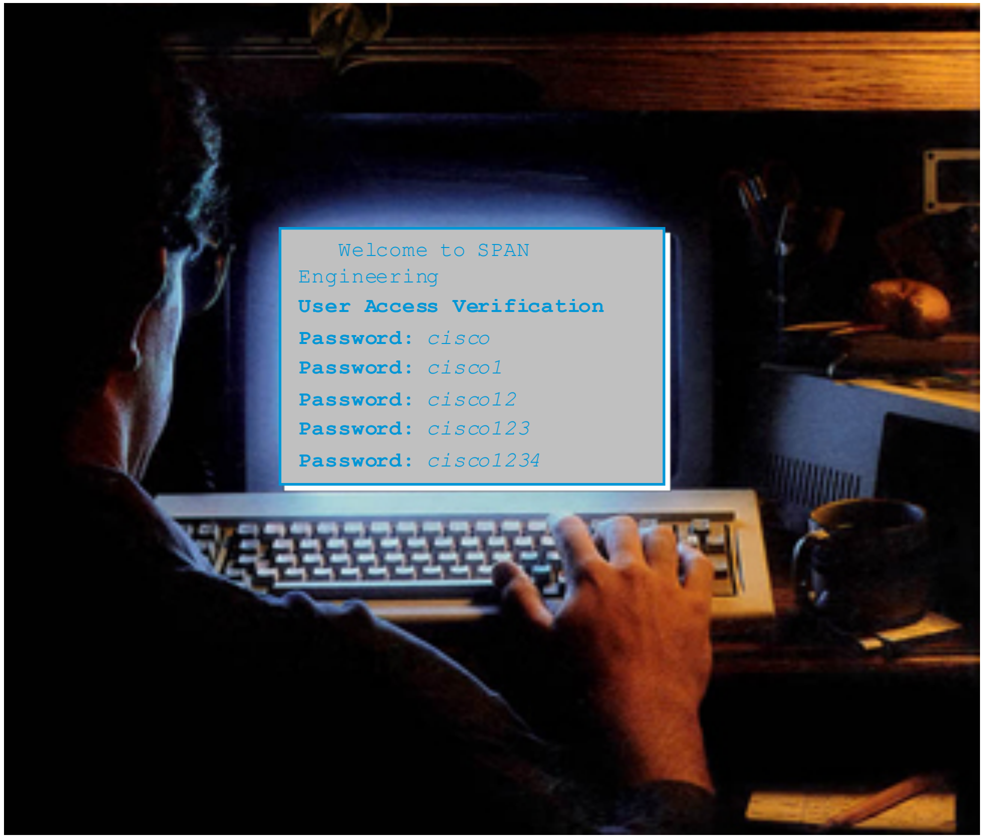
```
R1# conf t
R1(config)# username JR-ADMIN password letmein
% Password too short - must be at least 10 characters. Password configuration
failed
R1(config)# username JR-ADMIN password cisco12345
R1(config)# username ADMIN secret cisco54321
R1(config)# line con 0
R1(config-line)# login local
```

```
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.



```
   Welcome to SPAN
Engineering
User Access Verification
Password: cisco
Password: cisco1
Password: cisco12
Password: cisco123
Password: cisco1234
```

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 Mode

```
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

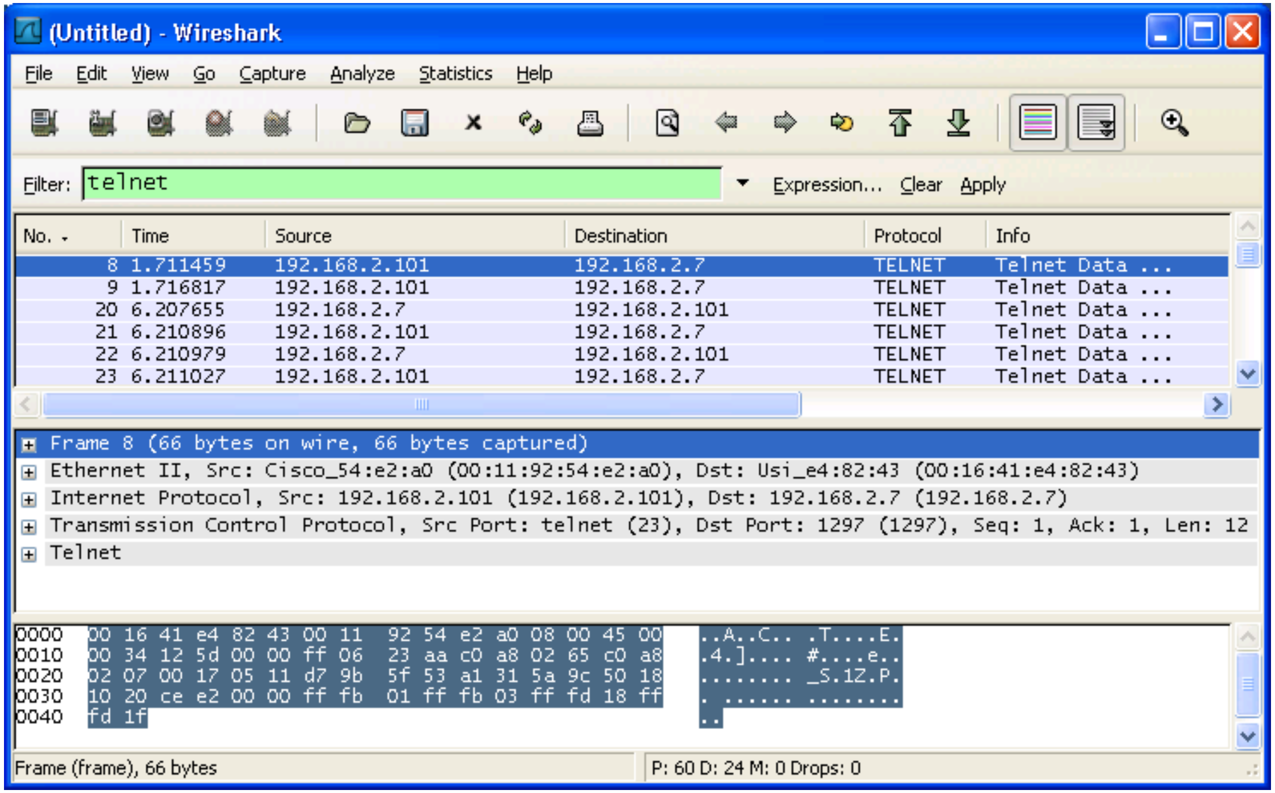
- If an enable mode password is NOT set for the router, privileged-EXEC mode can NOT be accessed using Telnet.
- Always use the **`enable secret`** *`password`* command to set the enable password.
  - Never use the **`enable password`** command!

Protecting vty Line Access #3

- Telnet access should be limited only to specified administrative hosts using ACLs:
  - Allows Telnet access from specific hosts only.
  - Implicitly or explicitly blocks access from untrusted hosts.
  - Tie the ACL to the vty lines using the **`access-class`** command.
- For example:

```
R1(config)#  access-list  30 permit 10.0.1.1  0.0.0.0
R1(config)#  line vty 0 4
R1(config-line)#  access-class  30 in
```

Sniffing a Telnet Password


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: telnet

No.	Time	Source	Destination	Protocol	Info
8	1.711459	192.168.2.101	192.168.2.7	TELNET	Telnet Data ...
9	1.716817	192.168.2.101	192.168.2.7	TELNET	Telnet Data ...
20	6.207655	192.168.2.7	192.168.2.101	TELNET	Telnet Data ...
21	6.210896	192.168.2.101	192.168.2.7	TELNET	Telnet Data ...
22	6.210979	192.168.2.7	192.168.2.101	TELNET	Telnet Data ...
23	6.211027	192.168.2.101	192.168.2.7	TELNET	Telnet Data ...

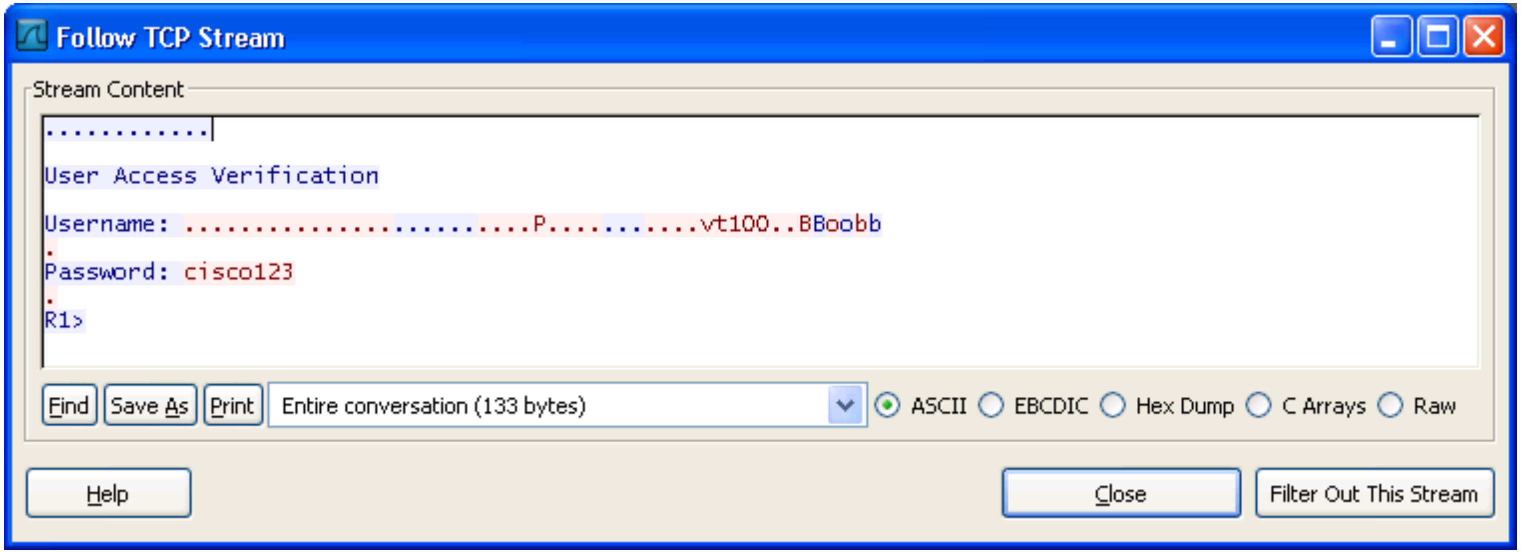
```
⊞ Frame 8 (66 bytes on wire, 66 bytes captured)
⊞ Ethernet II, Src: Cisco_54:e2:a0 (00:11:92:54:e2:a0), Dst: Usi_e4:82:43 (00:16:41:e4:82:43)
⊞ Internet Protocol, Src: 192.168.2.101 (192.168.2.101), Dst: 192.168.2.7 (192.168.2.7)
⊞ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1297 (1297), Seq: 1, Ack: 1, Len: 12
⊞ Telnet
```

```
0000  00 16 41 e4 82 43 00 11  92 54 e2 a0 08 00 45 00   ..A..C.. .T....E.
0010  00 34 12 5d 00 00 ff 06  23 aa c0 a8 02 65 c0 a8   .4.].... #....e..
0020  02 07 00 17 05 11 d7 9b  5f 53 a1 31 5a 9c 50 18   ........ _S.1Z.P.
0030  10 20 ce e2 00 00 ff fb  01 ff fb 03 ff fd 18 ff   . ...... ........
0040  fd 1f                                              ..
```

Frame (frame), 66 bytes | P: 60 D: 24 M: 0 Drops: 0

- An attacker is capturing packets using Wireshark on a local subnet.
- The attacker is interested in TCP Telnet streams and notices that the administrator’s IP address (192.168.2.7) has initiated a Telnet session to a device.

Follow the TCP Stream

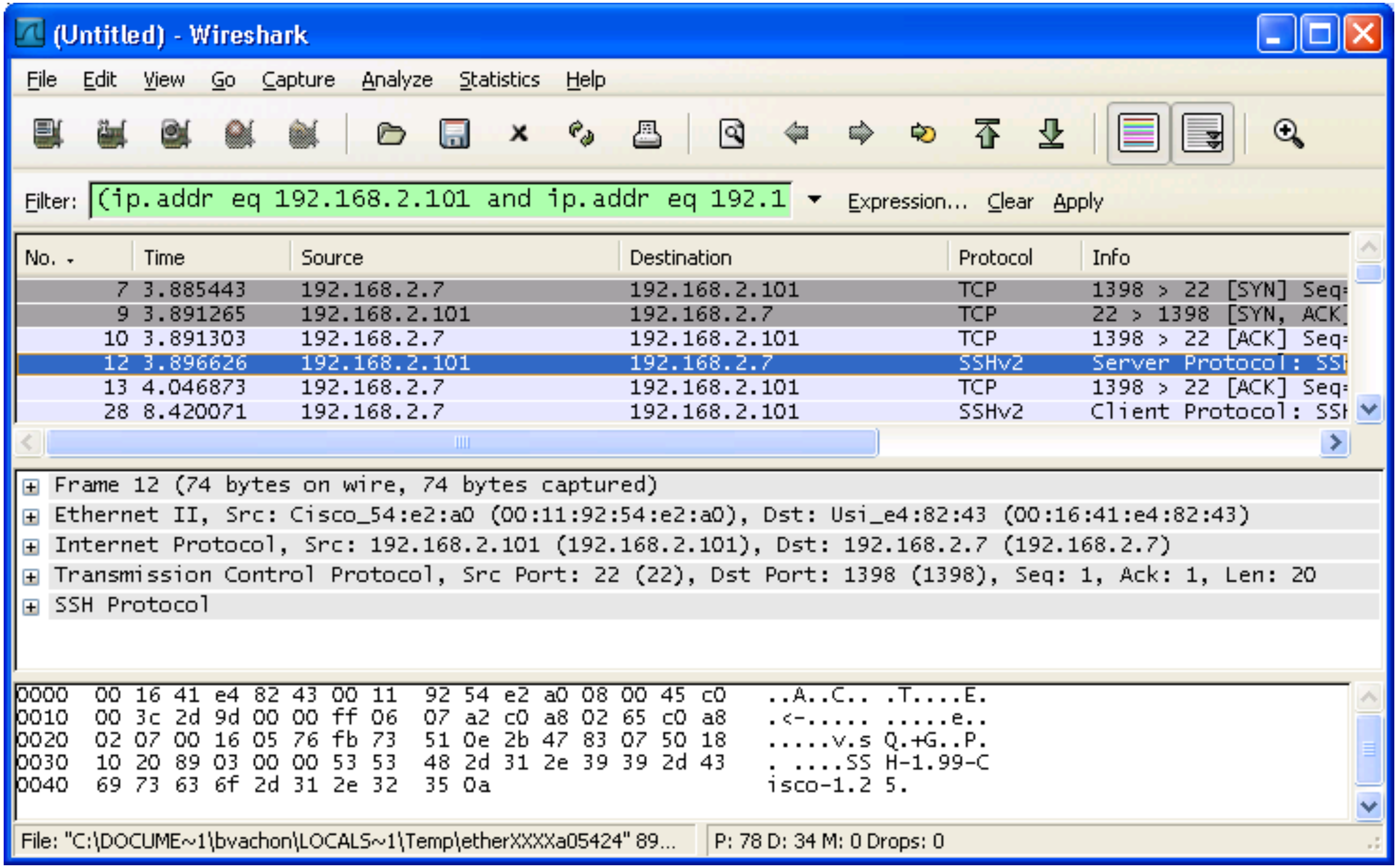


```
............

User Access Verification

Username: ..........................P...........vt100..BBoobb
.
Password: cisco123
.
R1>
```

Find
Save As
Print
Entire conversation (133 bytes)
● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw
Help
Close
Filter Out This Stream

- By following the TCP Telnet stream, the attacker has captured the administrator’s username (Bob) and password (cisco123).

Configure SSH



(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help

Filter: (ip.addr eq 192.168.2.101 and ip.addr eq 192.1

Expression... Clear Apply

```
No. .    Time        Source           Destination      Protocol  Info
      7 3.885443    192.168.2.7      192.168.2.101    TCP       1398 > 22 [SYN] Seq=
      9 3.891265    192.168.2.101    192.168.2.7      TCP       22 > 1398 [SYN, ACK]
     10 3.891303    192.168.2.7      192.168.2.101    TCP       1398 > 22 [ACK] Seq=
     12 3.896626    192.168.2.101    192.168.2.7      SSHv2     Server Protocol: SSH
     13 4.046873    192.168.2.7      192.168.2.101    TCP       1398 > 22 [ACK] Seq=
     28 8.420071    192.168.2.7      192.168.2.101    SSHv2     Client Protocol: SSH
```

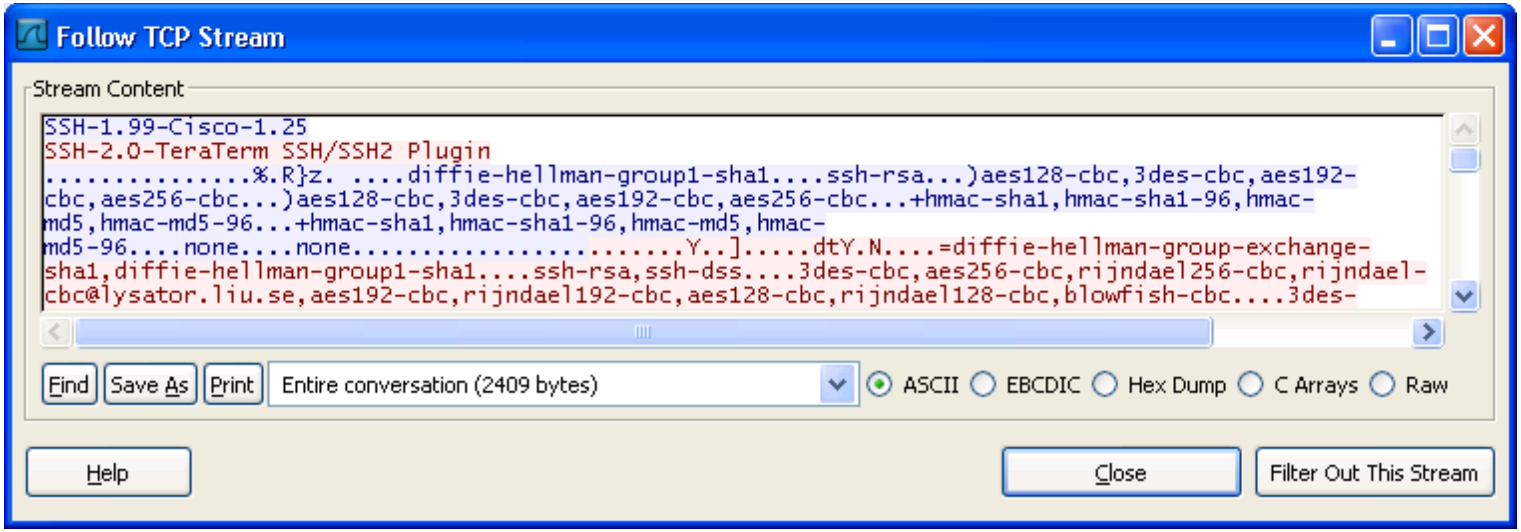
```
⊞ Frame 12 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Cisco_54:e2:a0 (00:11:92:54:e2:a0), Dst: Usi_e4:82:43 (00:16:41:e4:82:43)
⊞ Internet Protocol, Src: 192.168.2.101 (192.168.2.101), Dst: 192.168.2.7 (192.168.2.7)
⊞ Transmission Control Protocol, Src Port: 22 (22), Dst Port: 1398 (1398), Seq: 1, Ack: 1, Len: 20
⊞ SSH Protocol
```

```
0000  00 16 41 e4 82 43 00 11  92 54 e2 a0 08 00 45 c0   ..A..C.. .T....E.
0010  00 3c 2d 9d 00 00 ff 06  07 a2 c0 a8 02 65 c0 a8   .<-..... .....e..
0020  02 07 00 16 05 76 fb 73  51 0e 2b 47 83 07 50 18   .....v.s Q.+G..P.
0030  10 20 89 03 00 00 53 53  48 2d 31 2e 39 39 2d 43   . ....SS H-1.99-C
0040  69 73 63 6f 2d 31 2e 32  35 0a                     isco-1.2 5.
```

File: "C:\DOCUME~1\bvachon\LOCALS~1\Temp\etherXXXXa05424" 89... P: 78 D: 34 M: 0 Drops: 0

- When the administrator uses SSH, the attacker no longer sees Telnet packets and must instead filter by the administrator’s IP address.

Follow the TCP Stream



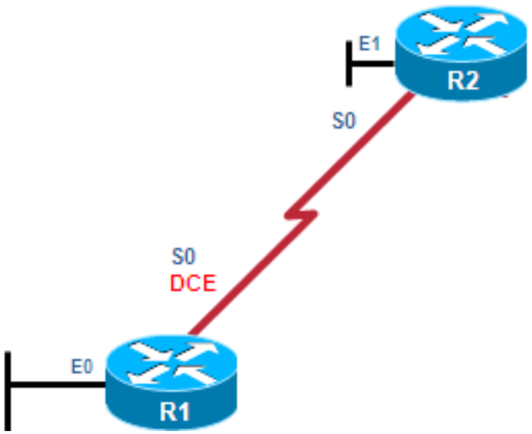
```
SSH-1.99-Cisco-1.25
SSH-2.0-TeraTerm SSH/SSH2 Plugin
...............%.R}z.  ....diffie-hellman-group1-sha1....ssh-rsa...)aes128-cbc,3des-cbc,aes192-
cbc,aes256-cbc...)aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc...+hmac-sha1,hmac-sha1-96,hmac-
md5,hmac-md5-96...+hmac-sha1,hmac-sha1-96,hmac-md5,hmac-
md5-96....none....none.......................Y..].....dtY.N....=diffie-hellman-group-exchange-
sha1,diffie-hellman-group1-sha1....ssh-rsa,ssh-dss....3des-cbc,aes256-cbc,rijndael256-cbc,rijndael-
cbc@lysator.liu.se,aes192-cbc,rijndael192-cbc,aes128-cbc,rijndael128-cbc,blowfish-cbc....3des-
```

Entire conversation (2409 bytes)

● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw

- When following the stream of data, the attacker only sees TCP and SSH packets which reveal useless encrypted information.

Configuring SSH



- Step 1: Configure the IP domain name.
- Step 2: Generate one-way secret RSA keys.
- Step 3: Create a local database username entry.
- Step 4: Enable VTY inbound SSH sessions.

```
R1# conf t
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]

R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
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
```

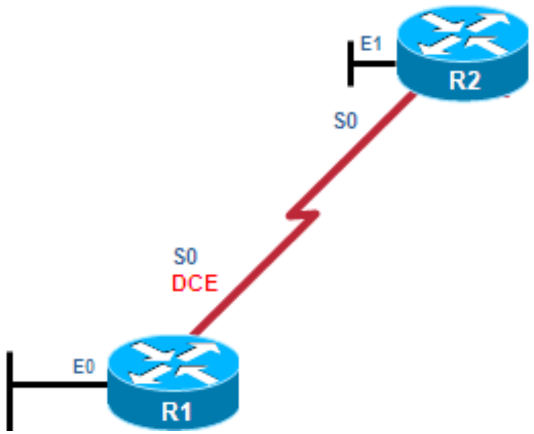
Optional SSH Features

- Optionally, SSH commands can be used to configure the following:
  - SSH version
  - Number of authentication retries
  - SSH timeout period

Optional SSH Features

- **SSH Versions:**
  - Cisco IOS Release 12.1(1)T and later supports SSHv1.
  - Cisco IOS Release 12.3(4)T and later supports both SSHv1 and SSHv2 (compatibility mode).
  - To change versions, use the **`ip ssh version {1 | 2}`** global command.
- **Number of authentication retries:**
  - By default, a user logging in has 3 attempts before being disconnected.
  - To configure a different number of consecutive SSH retries, use the **`ip ssh authentication-retries`** *`integer`* command in global configuration mode.
- **SSH Timeouts:**
  - The default time interval that the router will wait for an SSH client to respond during SSH negotiation phase is 120 seconds.
  - Change the time using **`ip ssh time-out`** *`seconds`*.

Optional SSH Commands



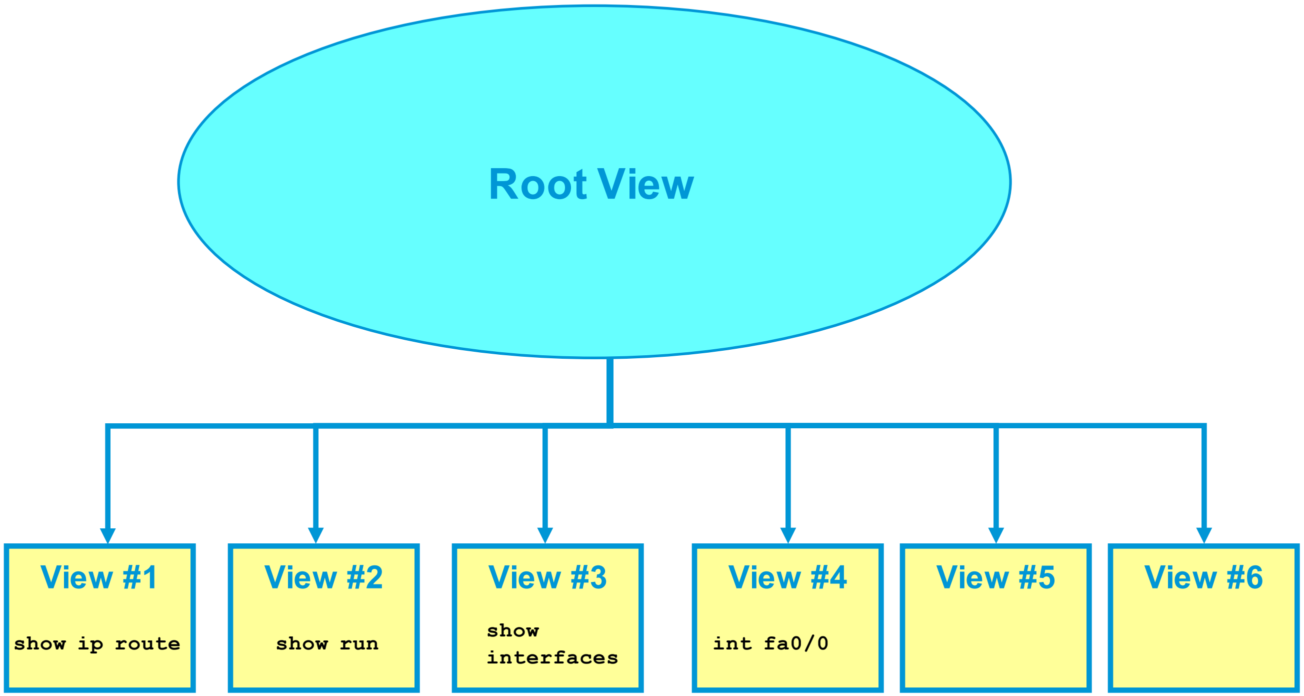
```
R1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R1#
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ssh version 2
R1(config)# ip ssh authentication-retries 2
R1(config)# ip ssh time-out 60
R1(config)# ^Z
R1#
R1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 2
R1#
```

Role-Based CLI Overview

- Privilege levels and enable mode passwords do not provide the necessary level of detail needed when working with Cisco IOS routers and switches.
- The Role-Based CLI Access feature allows the administrator to define “views”.
  - Views are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration mode commands.
  - Views restrict user access to Cisco IOS CLI and configuration information; that is, a view can define what commands are accepted and what configuration information is visible.

Root View

- Root View is required to defines Views and Superviews.
- Views contain commands.
- A command can appear in more than one view.



Role-Based CLI Overview

- Root view is the highest administrative view.
  - Creating and modifying a view or ‘superview’ is possible only from root view.
  - The difference between root view and privilege Level 15 is that only a root view user can create or modify views and superviews.
- Role-Based CLI views require AAA new-model:
  - This is necessary even with local view authentication.
- A maximum of 15 CLI views can exist in addition to the root view.

Getting Started with Role-Based CLI

- Before a view is entered or created, AAA must be enabled via the **`aaa new-model`** command.
- Next, use the **`enable`** command with the **`view`** parameter to enter the root view.
  - E.g., **`enable view`**
  - Optionally you can also use **`enable view root`**.
- Use the privilege 15 password (**`enable secret`**), if prompted for authentication (if authentication is configured).

Getting Started with Role-Based CLI

- Enter a privilege level or a CLI view.
- Use **enable** command with the **view** parameter to enter the root view.
- Root view requires privilege Level 15 authentication.

```
Router#
enable [privilege-level] [view [view-name]]
```

- The **aaa-new model** command must be entered.

```
R1(config)# aaa new-model
R1(config)# exit
R1# enable view
Password:
R1#
%PARSER-6-VIEW_SWITCH: successfully set to view 'root'
```

`enable` Parameters

```
Router#
enable [privilege-level] [view [view-name]]
```

Parameter	Description
privilege-level	(Optional) Sets the privilege level at which to log in.
view	(Optional) Enters root view, which enables users to configure CLI views. This keyword is required if you want to configure a CLI view.
view-name	(Optional) Enters or exits a specified CLI view. This keyword can be used to switch from one CLI view to another CLI view.

Configuring CLI Views

- Creates a view and enters view configuration mode.

```
Router(config)#
```

```
parser view view-name
```

- Sets a password to protect access to the view.
- Adds commands or interfaces to a view.

```
Router(config-view)#
```

```
password encrypted-password

commands parser-mode {include | include-exclusive | exclude} [all] [interface
interface-name | command]
```

- Example config setting a password and adding commands to the view named MONITOR-VIEW.

```
R1(config)# parser view MONITOR-VIEW
R1(config-view)# password cisco
R1(config-view)# commands exec include show version
```

commands Parameters

```
Router(config-view)#
```

```
commands parser-mode {include | include-exclusive | exclude} [all] [interface
interface-name | command]
```

Parameter	Description
parser-mode	Specifies the mode in which the specified command exists (e.g. exec mode).
include	Adds a command or an interface to the view and allows the same command or interface to be added to an additional view.
include-exclusive	Adds a command or an interface to the view and excludes the same command or interface from being added to all other views.
exclude	Excludes a command or an interface from the view; that is, users cannot access a command or an interface.
all	(Optional) Specifies a "wildcard" that allows every command in a specified configuration mode that begins with the same keyword or every subinterface for a specified interface to be part of the view.
interface *interface-name*	(Optional) Specifies an interface that is added to the view.
command	(Optional) Specifies a command that is added to the view.

Role-Based CLI Configuration Example

- The CLI view FIRST is created and configured to include the commands **show version**, **configure terminal**, and all commands starting with **show ip**.

```
R1(config)# aaa new-model
R1(config)# exit
R1# enable view
%PARSER-6-VIEW_SWITCH:  successfully set to view ‘root’.
R1# configure terminal
R1(config)# parser view FIRST
%PARSER-6-VIEW_CREATED:view ‘FIRST’ successfully created.
R1(config-view)#  secret firstpass
R1(config-view)#  command exec include show version
R1(config-view)#  command exec include configure terminal
R1(config-view)#  command exec include all show ip
R1(config-view)#  exit
```

Role-Based CLI Configuration Example

- Next, the administrator will verify the configuration by entering and viewing the available commands.
  - When a user enters the CLI view, an indication message appears.
  - Apart from the commands **enable** and **exit** that are available in all views, the only two commands that are visible in the CLI view are **configure** and **show**.

```
R1> enable view FIRST
Password:
%PARSER-6-VIEW_SWITCH:successfully set to view ‘FIRST'.
R1# ?
Exec commands:
configure               Enter configuration mode
enable                  Turn on privileged commands
exit                    Exit from the EXEC
show                    Show running system information
```

Role-Based CLI Configuration Example

- To further verify the view configuration, the administrator looks at the available options of the **show** command.
  - The available options include **parser**, which is always available, and the configured keywords **ip** and **version**.

```
R1# show ?
ip                    IP information
parser                Display parser information
version               System hardware and software status
```

Role-Based CLI Configuration Example

- Next, the user verifies that all sub-options of the **`show ip`** command are available in the view.

```
R1# show ip ?
access-lists                List IP access lists
accounting                  The active IP accounting database
aliases                     IP alias table
arp                         IP ARP table
as-path-access-list         List AS path access lists
bgp                         BGP information
cache                       IP fast-switching route cache
casa                        Display casa information
cef                         Cisco Express Forwarding
community-list              List community-list
dfp                         DFP information
dhcp                        Show items in the DHCP database drp
--More--
```

Another Sample Config

```
R1(config)# parser view SHOWVIEW
*Mar  1 09:54:54.873: %PARSER-6-VIEW_CREATED:  view ‘SHOWVIEW' successfully
created.
R1(config-view)# secret cisco
R1(config-view)# commands exec include show version
R1(config-view)# exit
R1(config)# parser view VERIFYVIEW
*Mar  1 09:55:24.813: %PARSER-6-VIEW_CREATED:  view ‘VERIFYVIEW' successfully
created.
R1(config-view)# commands exec include ping
% Password not set for the view VERIFYVIEW
R1(config-view)# secret cisco5
R1(config-view)# commands exec include ping
R1(config-view)# exit
R1(config)# parser view REBOOTVIEW
R1(config-view)#
*Mar  1 09:55:52.297: %PARSER-6-VIEW_CREATED:  view ‘REBOOTVIEW' successfully
created.
R1(config-view)# secret cisco10
R1(config-view)# commands exec include reload
R1(config-view)# exit
```

Display Views

```
R1# show running-config

<Output omitted>

parser view SHOWVIEW
 secret 5 $1$GL2J$8njLecwTaLAc0UuWo1/Fv0
 commands exec include show version
 commands exec include show
!
parser view VERIFYVIEW
 secret 5 $1$d08J$1zOYSI4WainGxkn0Hu7lP1
 commands exec include ping
!
parser view REBOOTVIEW
 secret 5 $1$L7lZ$1Jtn5IhP43fVE7SVoF1pt.
 commands exec include reload
!
```

Role-Based CLI Monitoring

- When monitoring role-based CLI, use the command **`show parser view`** to display information about the view that the user is currently in.
  - The **`all`** keyword displays information for all configured views.
  - The **`all`** keyword is available only to root users.
  - However, the keyword can be configured by a user in root view to be available for users in any CLI view.
- To display debug messages for all views, use the **`debug parser view`** command in privileged EXEC mode.

Verify All Views

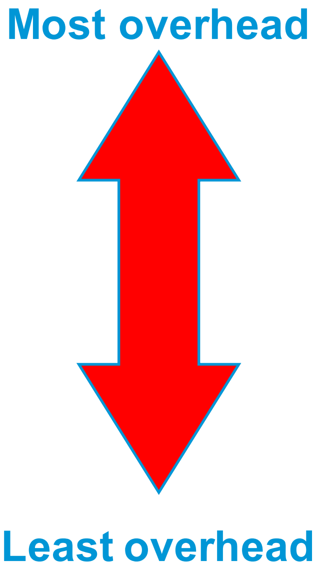
```
R1# show parser view
No view is active ! Currently in Privilege Level Context
R1#
R1# enable view
Password:
*Mar  1 10:38:56.233: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
R1#
R1# show parser view
Current view is 'root'
R1#
R1# show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
 SUPPORT *
 USER *
 JR-ADMIN *
 ADMIN *
-------(*) represent superview-------
R1#
```

Implementing Log Messaging for Security

- Routers should be configured to send log messages to one or more of these:
  - Console
  - Terminal lines
  - Memory buffer
  - Syslog Server

Logging Destinations

- Be aware that the logging destination used affects system overhead.
  - Logging to the **console**.
  - Logging to **VTY**.
  - Logging to a **Syslog Server**.
  - Logging to an internal **buffer**.

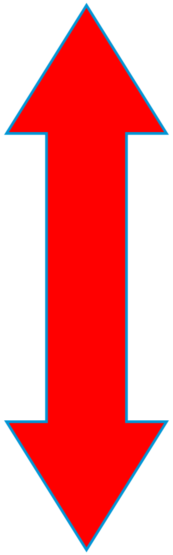


Two Components of Syslog Systems

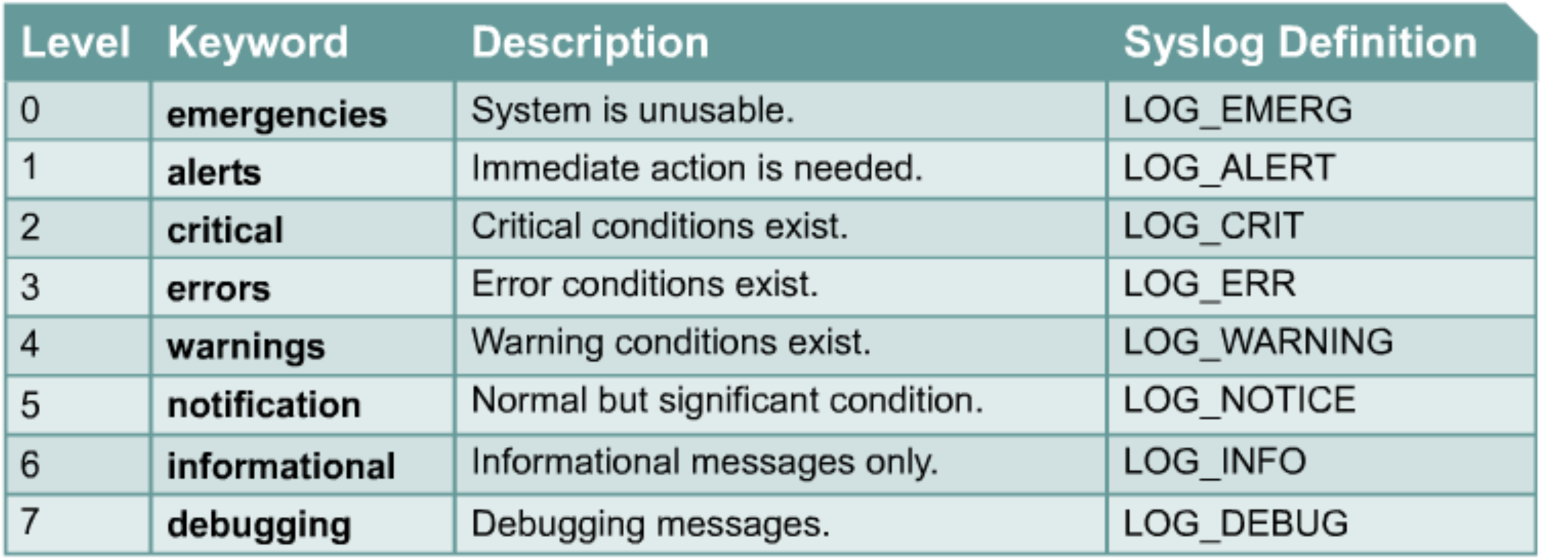
- Syslog server:
  - A host that accepts and processes log messages from one or more syslog clients.
- Syslog client:
  - A host that generates log messages and forwards them to a syslog server.
  - Routers, switches, PIXs, ASAs, APs, servers, …

Syslog Error Message Levels

Highest Level



Lowest Level



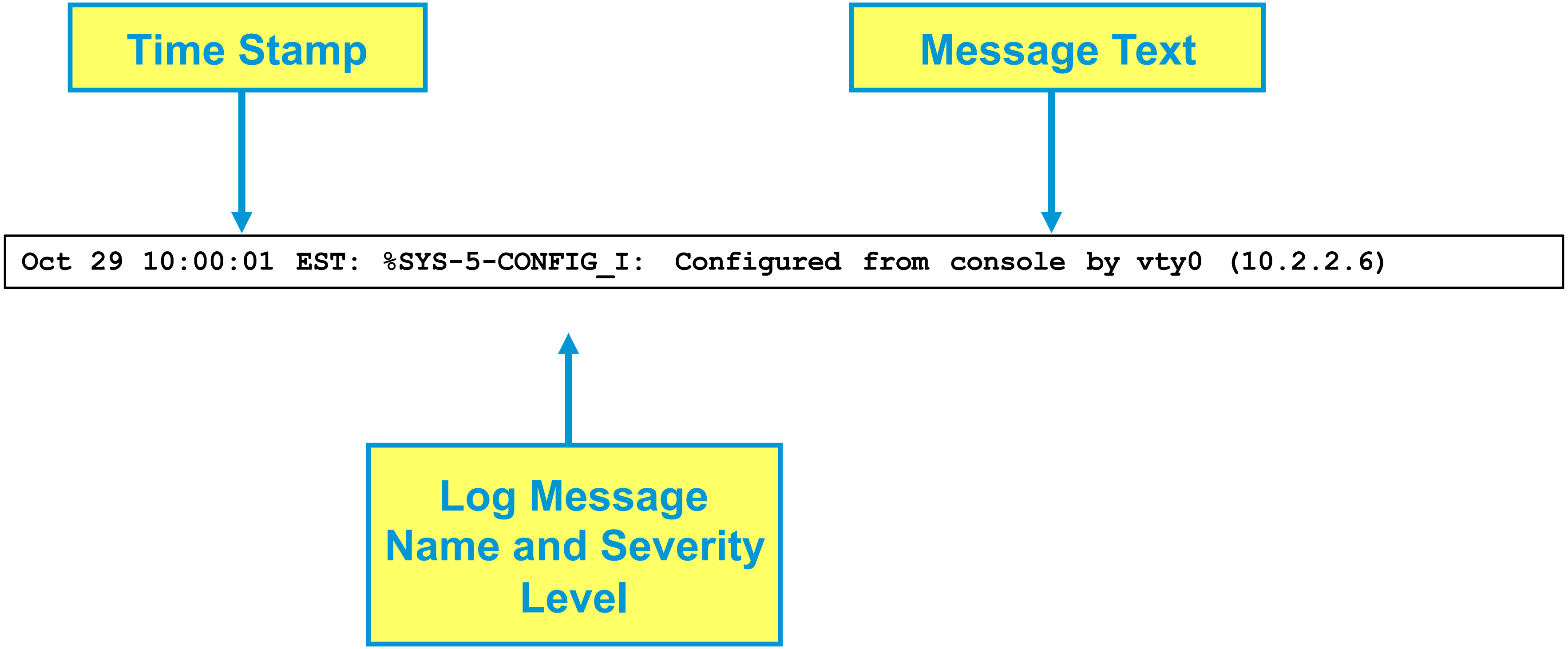
Level	Keyword	Description	Syslog Definition
0	**emergencies**	System is unusable.	LOG_EMERG
1	**alerts**	Immediate action is needed.	LOG_ALERT
2	**critical**	Critical conditions exist.	LOG_CRIT
3	**errors**	Error conditions exist.	LOG_ERR
4	**warnings**	Warning conditions exist.	LOG_WARNING
5	**notification**	Normal but significant condition.	LOG_NOTICE
6	**informational**	Informational messages only.	LOG_INFO
7	**debugging**	Debugging messages.	LOG_DEBUG

- By default, Severity level 7 (debugging) messages are sent to the router's console port (line con0).
- Note: Level varies by platform and IOS release.

Cisco Log Severity Levels

Level and Name	Definition	Example
0 LOG_EMERG	A panic condition normally broadcast to all users	Cisco IOS software could not load
1 LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database	Temperature too high
2 LOG_CRIT	Critical conditions; for example, hard device errors	Unable to allocate memory
3 LOG_ERR	Errors	Invalid memory size
4 LOG_WARNING	Warning messages	Crypto operation failed
5 LOG_NOTICE	Conditions that are not error conditions but should possibly be addressed	Interface changed state, up or down
6 LOG_INFO	Informational messages	Packet denied by ACL
7 LOG_DEBUG	Messages that contain information that is normally used only when debugging	Packet type invalid

Log Message Format



Time Stamp

Message Text

```
Oct 29 10:00:01 EST: %SYS-5-CONFIG_I:  Configured from console by vty0 (10.2.2.6)
```

Log Message Name and Severity Level

Note: The log message name is not the same as a severity level name.

Configuring Syslog Step 1

1. Set the destination logging host.
   - You can specify the IP address or the DNS name.

```
Router(config)#
logging host [host-name | ip-address]
```

Parameter	Description
host-name	The name of the host you want to use as a syslog server
ip-address	The IP address of the host you want to use as a syslog server

Configuring Syslog Step 2

2. (Optional) Set the log severity (trap) level.

```
Router(config)#
```

```
logging trap level
```

Parameter	Description
level	Limits the logging of messages to the syslog servers to a specified level. You can enter the level number (0 to 7) or level name.

Configuring Syslog Step 3

3. (Optional) Set the source interface.
   - Specifies that syslog packets contain the IP or IPv6 address of a particular interface, regardless of which interface the packet uses to exit the router.

```
Router(config)#
logging source-interface interface-type interface-number
```

Parameter	Description
interface-type	The interface type (for example, FastEthernet)
interface-number	The interface number (for example, 0/1)

Configuring Syslog Step 4

4. Enable logging

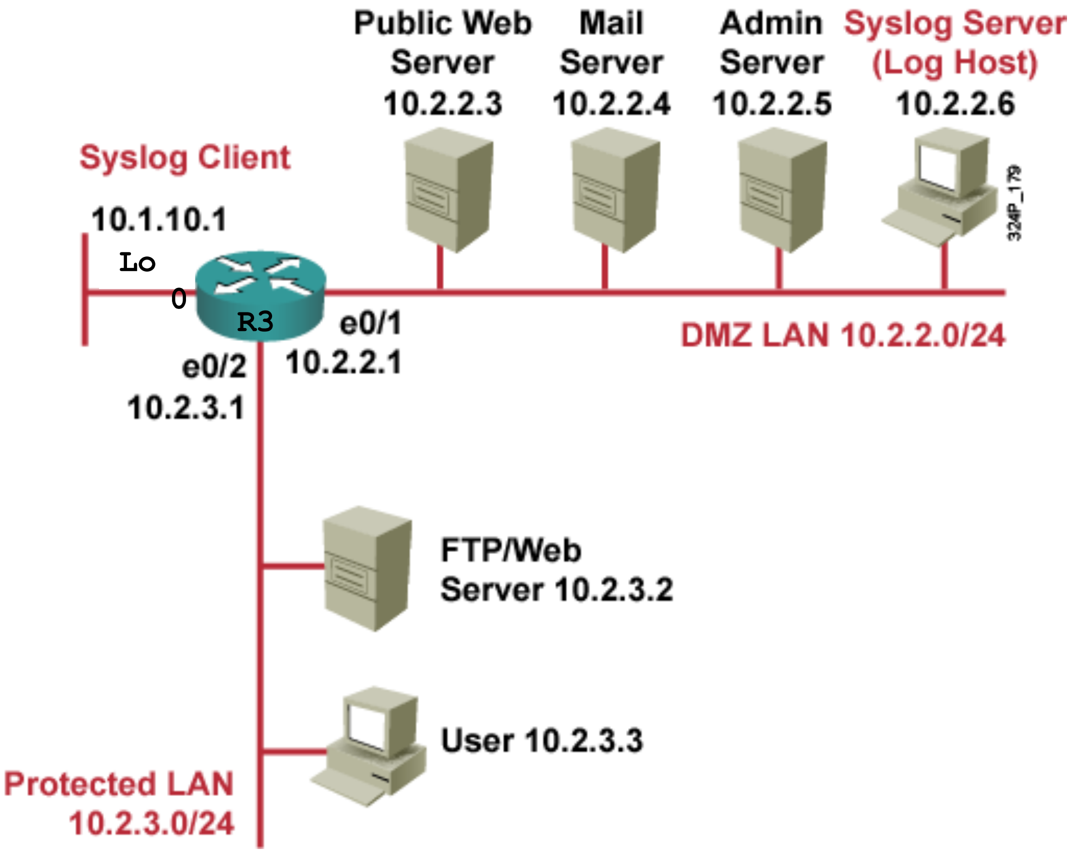
   – You can enable or disable logging individually:

     - **`[no] logging buffered`**
     - **`[no] logging monitor`**

   – However, if the **`no logging`** on command is configured, no messages will be sent to these destinations.

```
Router(config)#
logging on
```

Syslog Implementation Example



```
R3(config)# logging 10.2.2.6
R3(config)# logging trap informational
R3(config)# logging source-interface loopback 0
R3(config)# logging on
```

System Clock

- The heart of the router time service is the software-based system clock.
  - This clock keeps track of time from the moment the system starts.
- The system clock can be set from a number of sources and can be used to distribute the current time through various mechanisms to other systems.
  - When a router with a system calendar is initialized or rebooted, the system clock is set based on the time in the internal battery-powered system calendar.
- The system clock can then be set:
  - Manually using the **`set clock`** privileged EXEC command.
  - Automatically using the Network Time Protocol (NTP).
- NTP is an Internet protocol used to synchronize the clocks of network connected devices to some time reference.
  - NTP is an Internet standard protocol currently at v3 and specified in RFC 1305.

NTP

- NTP is designed to time-synchronize a network.
  - NTP runs over UDP.
- An NTP network usually obtains the time from an authoritative time source, such as a radio clock or an atomic clock.
  - NTP then distributes this time across the network.
  - NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within 1 mSec of one another.
- Cisco devices support specifications for NTP v3 (RFC 1305).
  - NTP v4 is under development but NTP v3 is the Internet standard.
- NTP services are enabled on all interfaces by default.
  - To disable NTP on a specific interface, use the **`ntp disable`** command in the interface configuration mode.

Configuring an NTP Master and Client

- To configure a router as the authoritative time source, use the **`ntp master`** command in global configuration mode.
- To configure a router as an NTP client, either:
  - Create an association to a server using the **`ntp server`** command.
  - Configure the router to listen to NTP broadcast packets using the **`ntp broadcast client`** command.

Identifying the NTP Server

- Although the router can be configured with either a peer or a server association, NTP clients are typically configured with a server association (meaning that only this system will synchronize to the other system, and not vice versa).
- To allow the software clock to be synchronized by an NTP time server, use the **ntp server** command in global configuration mode.

```
Router(config)#
```

```
ntp server {ip-address | hostname} [version number] [key keyid] [source interface]
[prefer]
```