UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Chapter 2: Securing Network Devices (Cisco IOS routers)

CCNA Security v2.0 / Network Security v1.0

Chap 2 / Modules 4, 5, 6

Bezpečnosť informačných sietí – KIS FRI UNIZA
Aktualizované v rámci projektu KEGA 026TUKE-4/2021.

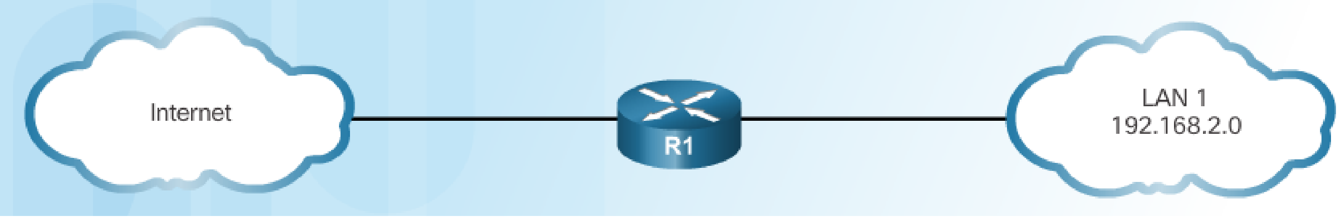
Securing Device Access

- Upon completion of this section, you should be able to:
  - Explain how to secure a network perimeter.
  - Configure secure administrative access to Cisco routers.
  - Configure enhanced security for virtual logins.
  - Configure an SSH daemon for secure remote management.

Securing the Edge Router

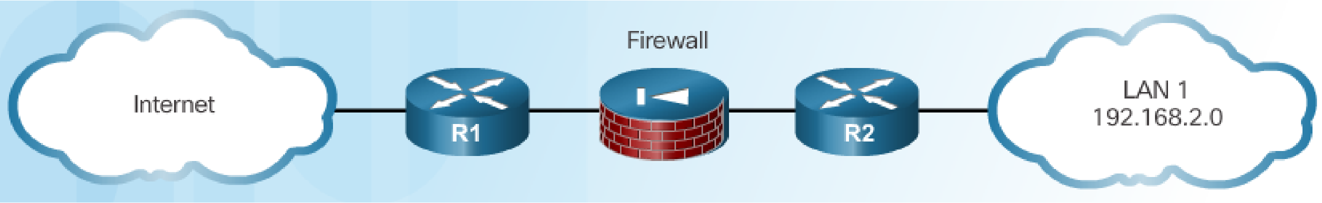
Edge Router – Approaches (lines of defense)

Single Router Approach



- Suitable for simple topologies
  - SOHO
  - Uses ISR

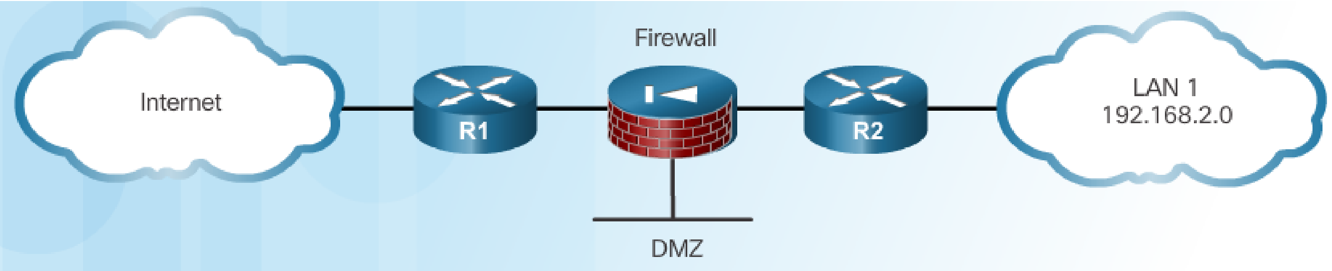
Defense in Depth Approach



- More layers of security = more layers of defense
- Edge router = screening router
  - First line of defense, Initial filtering
- Firewall
  - by.def. deny connection from outside, allows only from inside
- Internal router

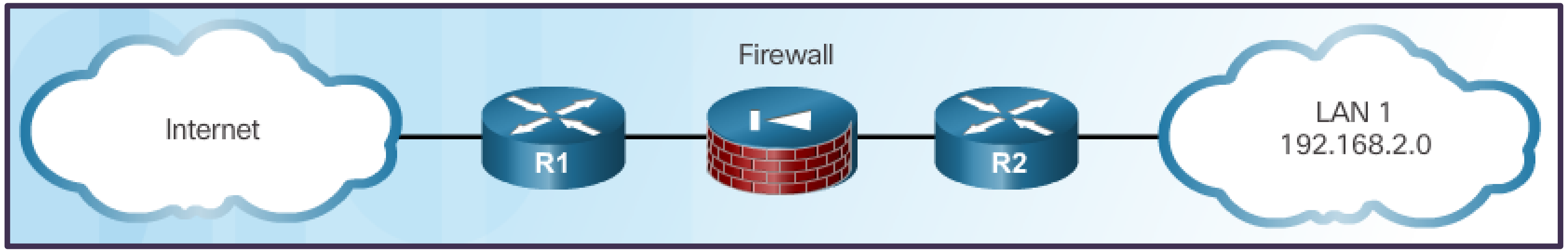
  Final filtering
- Boxes: Routers, Firewalls or IPSs, web/mail security appliances

DMZ Approach



- Variation of the defense in depth approach
- Includes DMZ zone
  - For example, for servers
  - Network segment or port of a router/fw

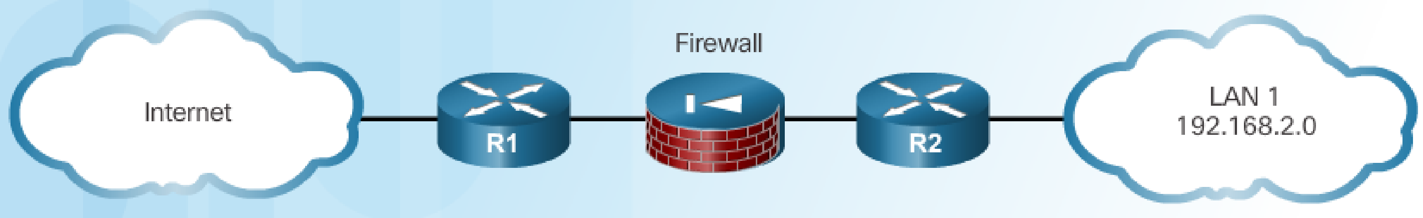
Defense-in-Depth Approach



- More layers of security = more layers of defense
- Edge router = screening router (next presentation)
  - First line of defense, Initial filtering => passes only one must go in
- Firewall
  - Additional filtering
  - By.def. deny all connections from outside, allows only from inside
    - Other functions (user auth, VPN GW, filtering, in depth control)
- Internal router
  - Final filtering
- Boxes:
  - Routers, Firewalls or IPSs,
  - + other appliances (web/mail security appliances)

Securing the Network Infrastructure

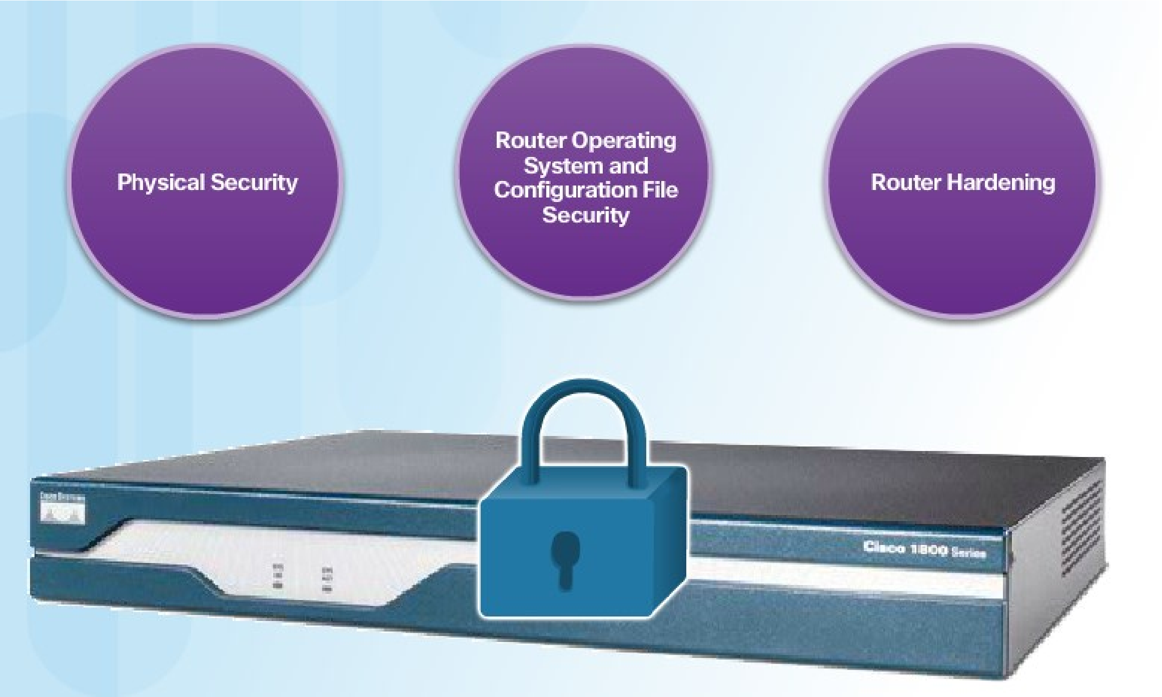
- Net infrastructure:
  - Routers, switches, AP, servers, endpoints
- All nets usually connected through an **Edge router**
- Edge router
  - Critical entity
    - All traffic goes through
  - Help to secure perimeter and improve security
- Critical to overall security
  - Secure routers!



```
R1#erase startup-config
R1#reload in 5
Proceed with reload?
[confirm]
R1#
***
*** -- SHUTDOWN in 0:05:00 --
***
R1#
```

Three Areas of Router Security

- **Physical security**
  - Physical security of the router
    - Things like a secured room with:
      - Authorized access, protection for electrostatic or magnetic interference,
      - fire suppression, temperature and humidity controls
      - Outage protection
        - UPS, diesel backup generator
- **Router hardening**
  - Secure processes and turn off all unused services
    - Secure administrative control
    - Disable unused ports and interfaces
    - Disable unnecessary services
    - Logging
    - ...
- **Operating system security**
  - Manage devices
    - Patching
      - Uses latest IOSs
    - Backuping
      - Keep a secure copy of IOSs and configs



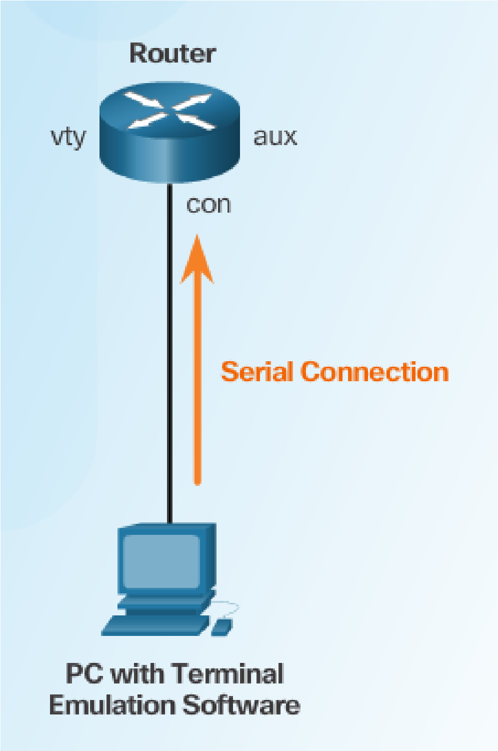
Router hardening - Secure Administrative Access

- One of first steps – extremely important
- Tasks:
  - **Present legal notification**
    - Banners with useful info
  - **Restrict device accessibility**
    - Limit accessible ports, restrict communicators, restrict methods of access
  - **Authenticate access**
    - Grant the access only to authenticated personnel
    - Limit failed login attempts and setup login and session timers

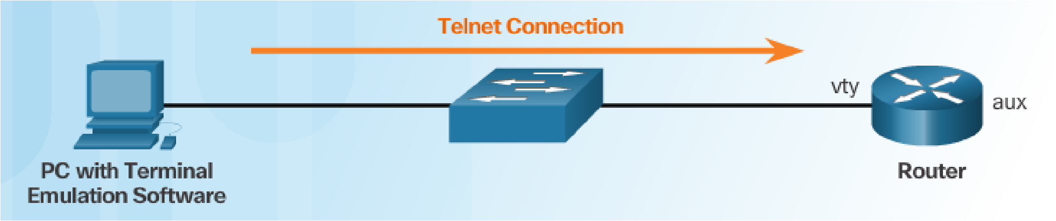
- **Authorize actions =>** assigning administrative roles
  - Assign commands per user/group/service
- **Log and account for all access**
  - Record required logs (who, when and what he did) => logging/monitoring
- **Ensure the confidentiality of data**
  - Protect locally stored data
  - Protect data on the transport (against sniffing, mitm)

Secure Local and Remote Access

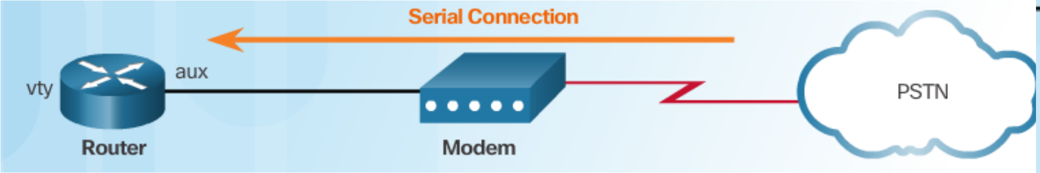
Local Access



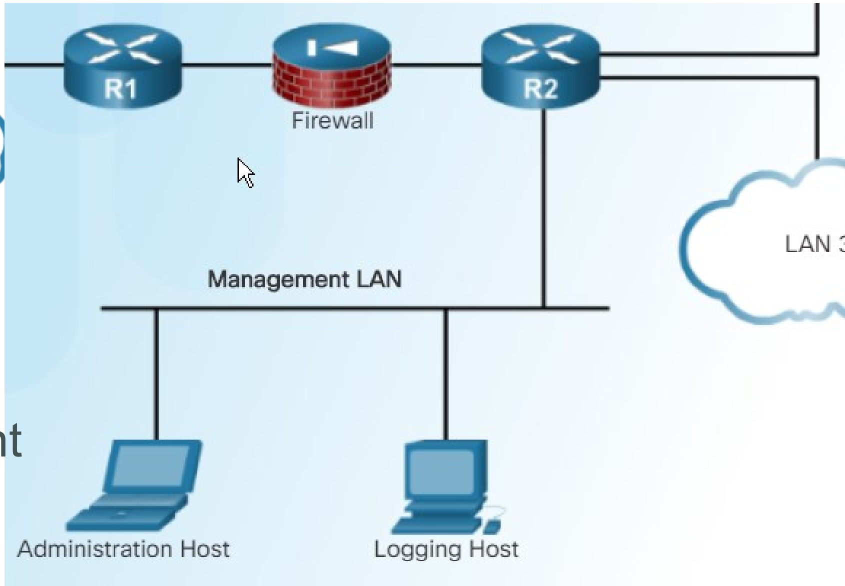
Remote Access Using Telnet



Remote Access Using Modem and Aux Port



Dedicated management network



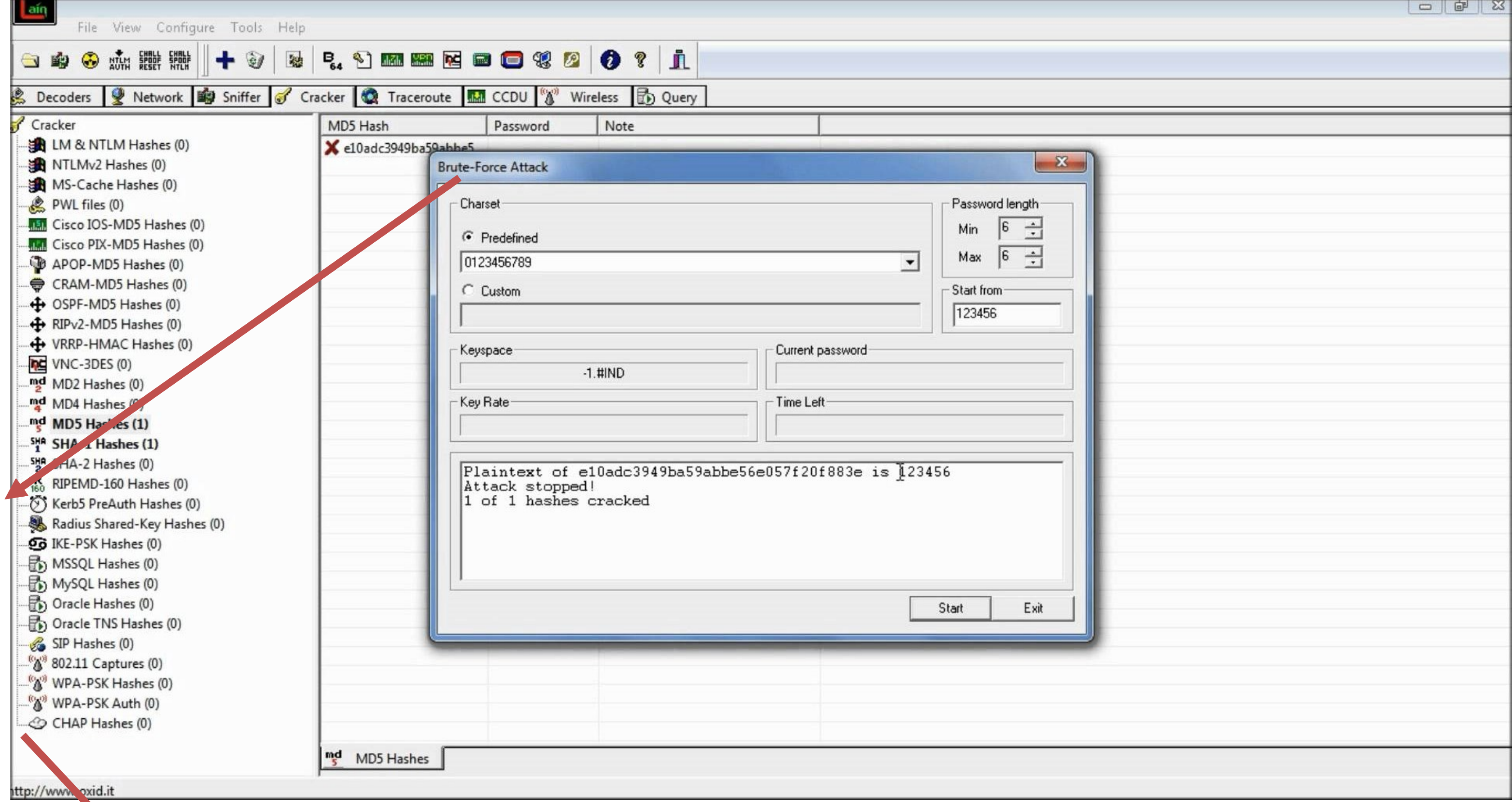
- Secure console and aux
- Try to avoid remote access, but if required
  - use a secure version of remote access protocols (ssh, https)
  - create a dedicated management network (Out of Band - OOB)
  - configure packet filtering
  - use VPN

Configuring Secure Administrative Access

Strong Passwords

Guidelines:

- Use a password length of 10 or more characters.
- Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces.
- Avoid passwords based on easily identifiable pieces of information.
- Deliberately misspell a password (Smith = Smyth = 5mYth).
- Change passwords often
    - ☺
- Use passphrasses
    - Several words
- Do not write passwords down and leave them in obvious places.



MD5 Hash: e10adc3949ba59abbe5

Charset: ● Predefined 0123456789

Password length: Min 6 Max 6

Start from: 123456

Keyspace: -1.#IND

```
Plaintext of e10adc3949ba59abbe56e057f20f883e is 123456
Attack stopped!
1 of 1 hashes cracked
```

Weak Password	Why it is Weak	Strong Password	Why it is Strong
secret	Simple dictionary password	b67n42d39c	Combines alphanumeric characters
smith	Mother's maiden name	12^h u4@1p7	Combines alphanumeric characters, symbols, and includes a space
toyota	Make of car		
bob1967	Name and birthday of user		
Blueleaf23	Simple words and numbers		

Increasing Access Security

- Set minimum password length

```
Router(config)# security passwords min-length ?
  <0-16>  Minimum length of all user/enable passwords
```

- Restrict number of failed login attempts

```
Router(config)# security authentication failure ?
  rate  Authentication failure threshold rate
```

- Turn on password encryption

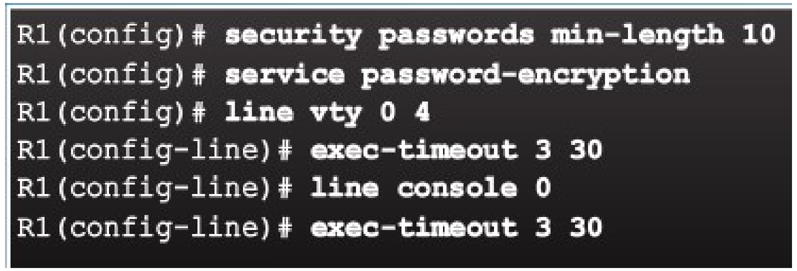
```
Router(config)# service password-encryption
```

- Turn off EXEC mode for some line (will deny the line)

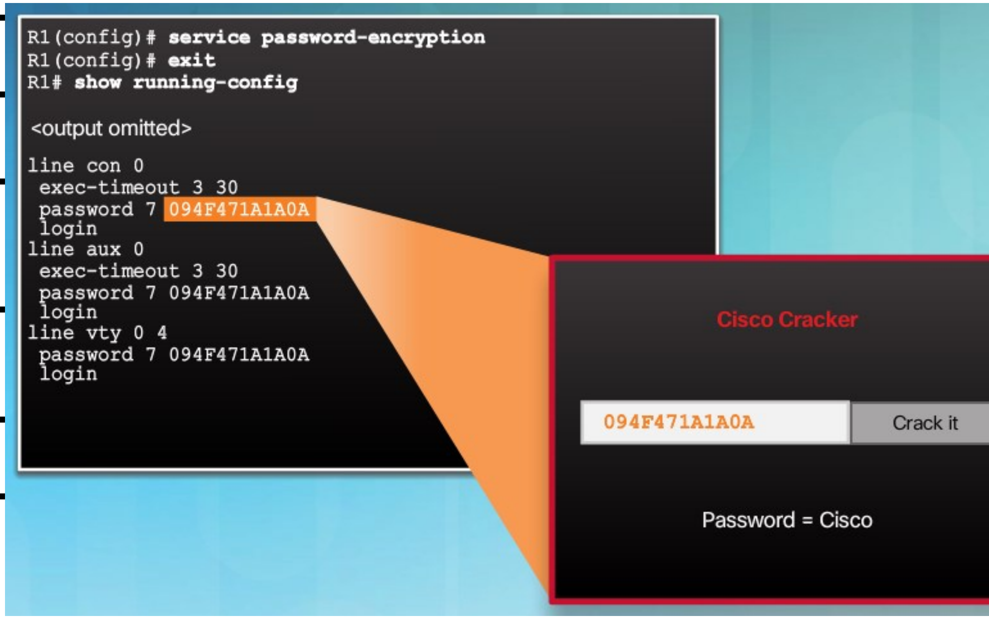
```
Router(config)# line aux 0
Router(config-line)# no exec
```

- Setup session inactivity timeout (def 10 min)

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



```
R1(config)# security passwords min-length 10
R1(config)# service password-encryption
R1(config)# line vty 0 4
R1(config-line)# exec-timeout 3 30
R1(config-line)# line console 0
R1(config-line)# exec-timeout 3 30
```



```
R1(config)# service password-encryption
R1(config)# exit
R1# show running-config

<output omitted>

line con 0
 exec-timeout 3 30
 password 7 094F471A1A0A
 login
line aux 0
 exec-timeout 3 30
 password 7 094F471A1A0A
 login
line vty 0 4
 password 7 094F471A1A0A
 login
```

Cisco Cracker

094F471A1A0A

Password = Cisco

Secret Password Algorithms

- Older versions of IOSs uses the Message Digest 5 (MD5) hash algorithm
  - No longer considered as secure
  - Online cracking tool example: https://www.md5online.org/
  - Note: The *enable secret password* command uses MD5 by default

```
R1(config)# enable secret cisco12345
R1(config)# exit
R1# show run
...OUTPUT OMITTED...
enable secret 5 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

    - If 4 = SHA256
    - if 5 = MD5

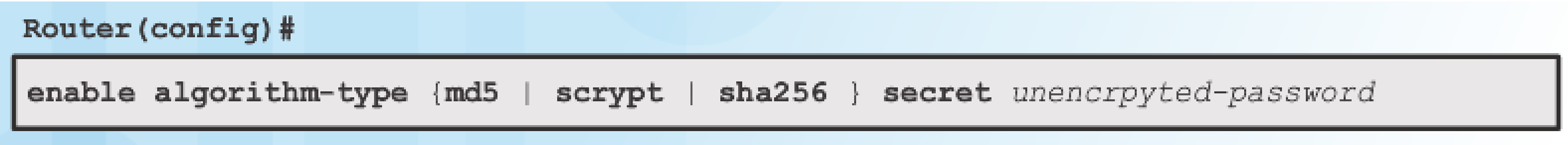
- Newer IOSs since IOS 15.3(3)M provides **new encryption algorithms** - Type 8 and 9
  - 9 is more secure

```
R1(config)#enable secret ?
  0      Specifies an UNENCRYPTED password will follow
  5      Specifies a MD5 HASHED secret will follow
  8      Specifies a PBKDF2 HASHED secret will follow
  9      Specifies a SCRYPT HASHED secret will follow
  LINE   The UNENCRYPTED (cleartext) 'enable' secret
  level  Set exec level password
```

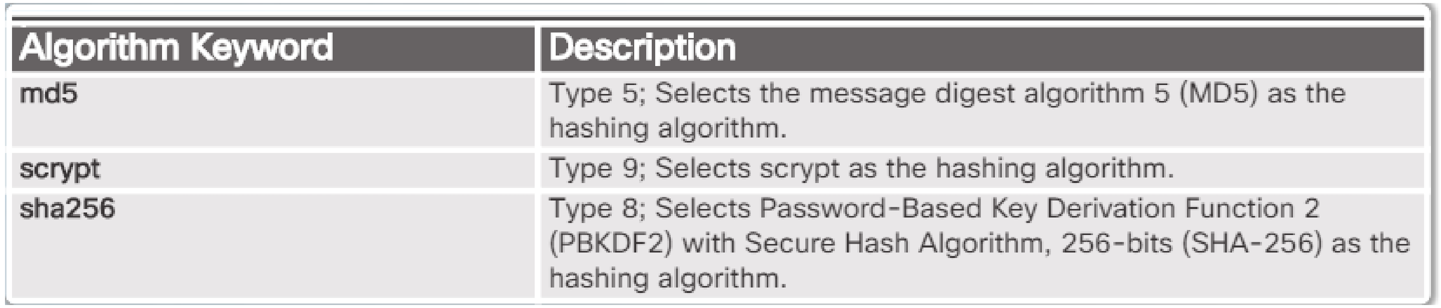
Secret Password Algorithms

Guidelines:

- Configure all secret passwords using type 8 or type 9 passwords
- Use the enable algorithm-type command syntax to enter an unencrypted password
  - Otherwise, using the *enable secret 9* command requires as the input the *HASH*

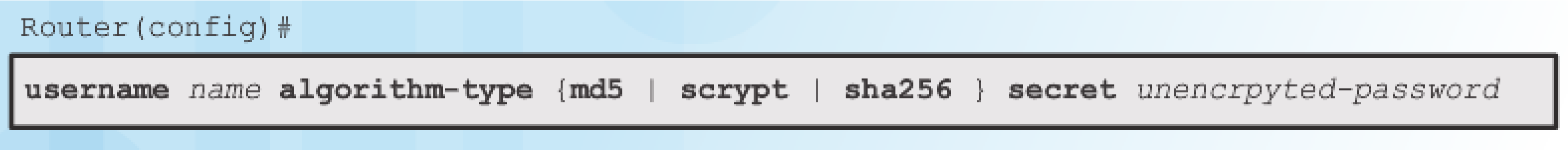


```
Router(config)#
enable algorithm-type {md5 | scrypt | sha256 } secret unencrpyted-password
```



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.

- Use the username name ***algorithm-type command*** to specify type 9 encryption



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

Configuring Secure Administrative Access

Securing Line Access

- Securing the console, vty and aux lines
  - Using shared pass, no encryption – not recommended

```
Router(config)# line console 0 | vty 0 15 | aux
! Pozor, ulozene v konfigu ako plain text
Router(config-line)# login PASSWORD
! Zapni jeho šifrovanie
Router(config)# service password-encryption
```

  - Using the local DB – recommended for the course
    - Create an user

```
Router(config)# username Palo algorithm-type scrypt secret cisco12345
```

    - Setup the authentication against a local DB

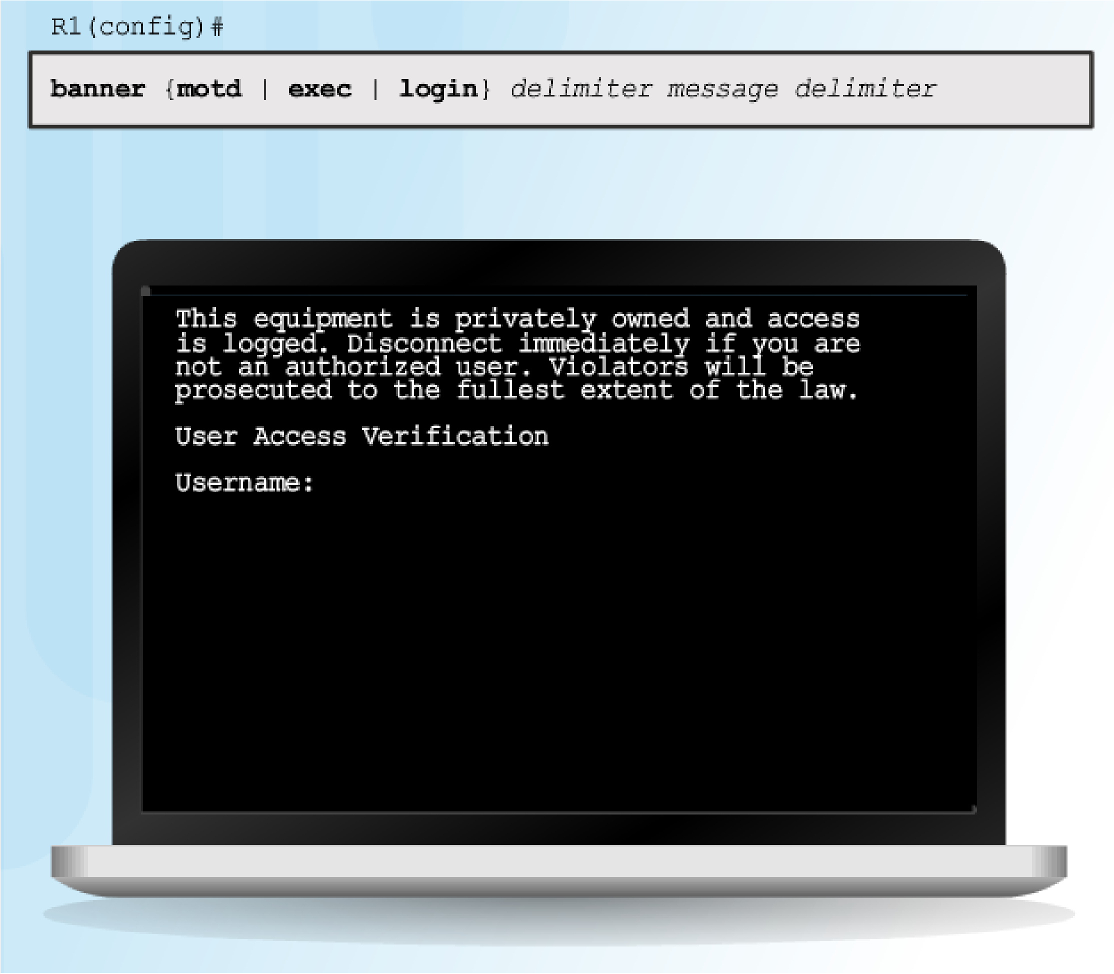
```
Router(config)# line console 0 | aux
Router(config-line)# login local
Router(config-line)# line vty 0 15
Router(config-line)# login local
Router(config-line)# transport input ssh
```

Configuring Enhanced Security for Virtual Logins

Enhancing the Login Process

Virtual login security enhancements:

- Generate system-logging messages for login detection
  - Use appropriate words ("welcome" is not a good example)
- Implement delays between successive login attempts
- Enable login shutdown if DoS attacks are suspected
  - Allows to react on repeated attempts



```
R1(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:
```

Configuring Login Enhancement Features

- Increases the security of virtual login connections
- Cmd defenses against **DOS/trial attacks**

```
R1(config)# login block-for SECONDS attempts FAIL_ATTEMPTS within SECONDS
```

- Cmd maps logins to ACL, that identifies the permitted hosts

```
R1(config)# login quite-mode access-class {ACL-NAME | ACLL-NUMBER}
```

- Cmd specifies the wait interval between unsuccessful login attempts

```
R1(config)# login delay SECONDS
```

- Cmds specify, that login have to be logged

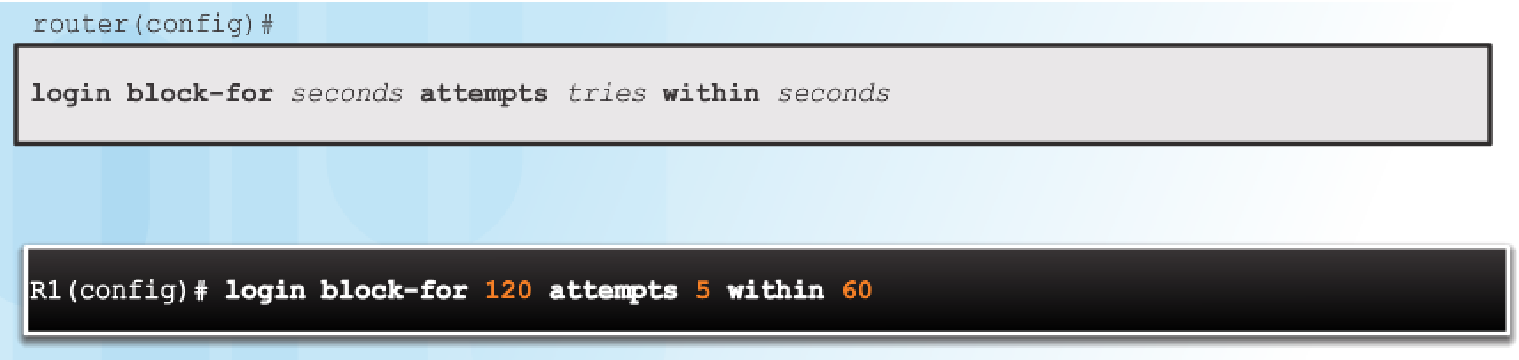
```
R1(config)# login on-success log {every LOGIN_ATTEMPT}
R1(config)# login on-failure log {every LOGIN_ATTEMPT}
```

- Notes:
  - Does not apply for console
  - Local DB has to be used

Enable Login Enhancements

- Cmd *login block-for* must be configured first
  - Otherwise, other login features are disabled
  - Uses 1sec interval
- Login block-for operates in two modes
  - Normal mode
    - i.e. watch mode
      - keeps count of the number of failed login attempts within an identified amount of time
  - Quiet mode
    - If the number of failed logins exceeds => all logins (including valid logins) are not permitted!!
    - The behavior need to be overwritten

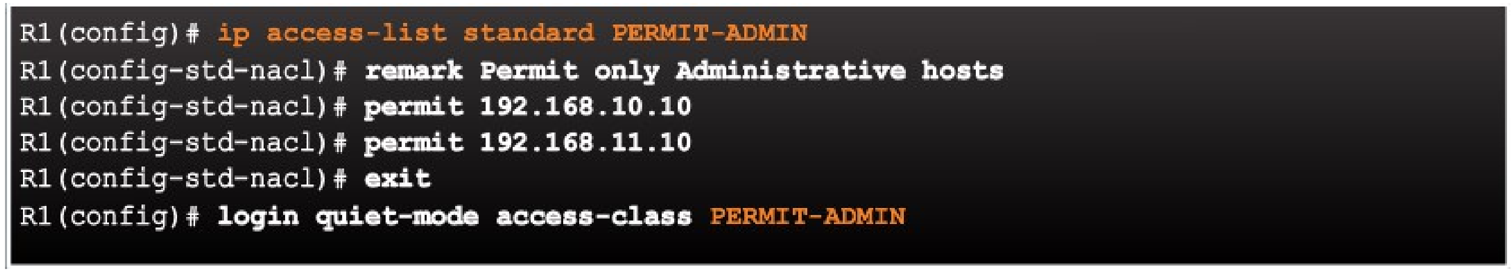
Command Syntax: `login block-for`



```
router(config)#

login block-for seconds attempts tries within seconds
```

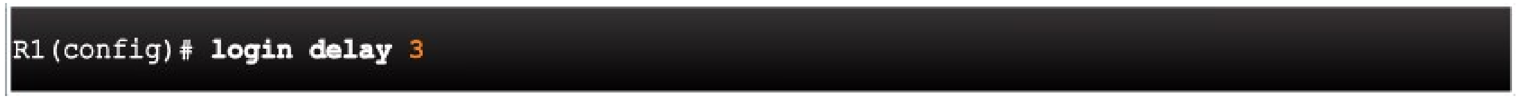
```
R1(config)# login block-for 120 attempts 5 within 60
```

Example: `login quiet-mode access-class`



```
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
```

Example: `login delay`

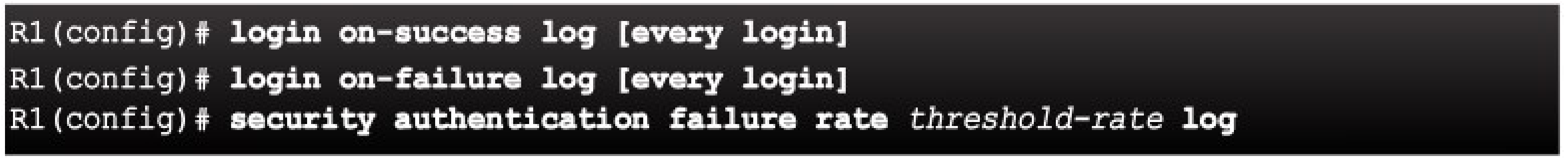


```
R1(config)# login delay 3
```

Logging Failed Attempts

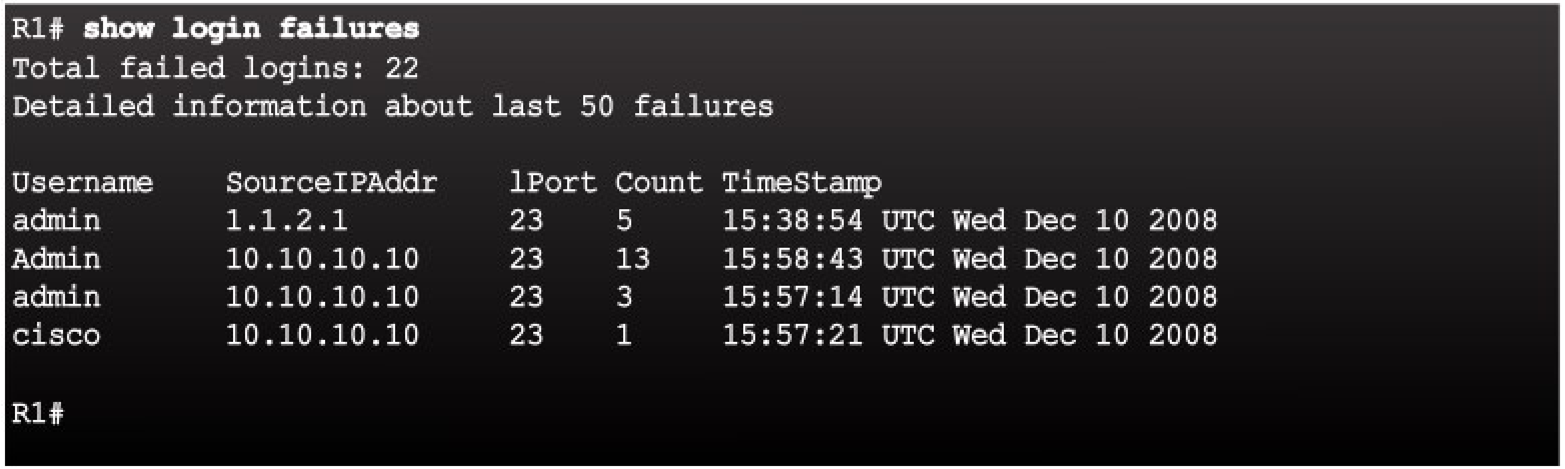
- Both cmds generates syslog messages
  - By default on each attempt
  - Parameter LOGIN may specify the number
- **`security authentication failure rate`**
  - is an alternative to cmd login on-failure

Generate Login Syslog Messages



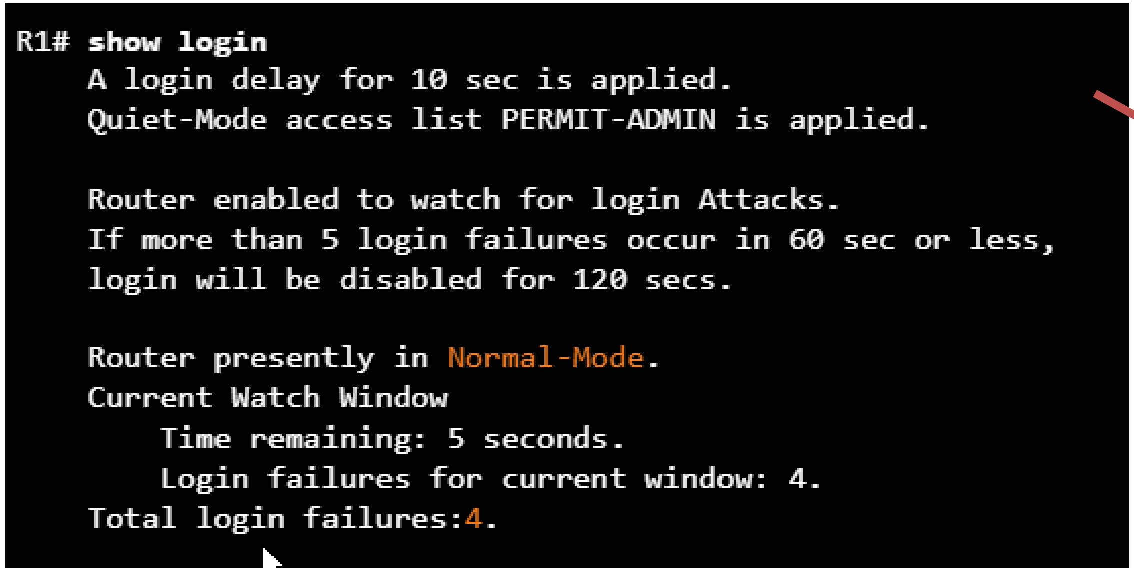
```
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
R1(config)# security authentication failure rate threshold-rate log
```

Example: **`show login failures`**

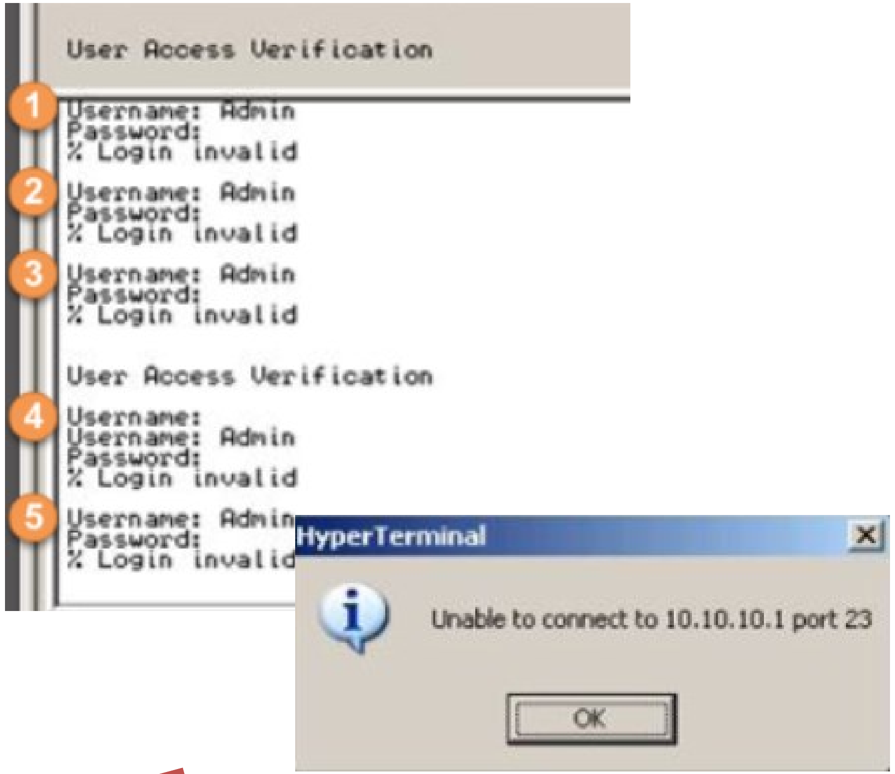


```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures

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#
```

Logging Failed Attempts - Login configuration status

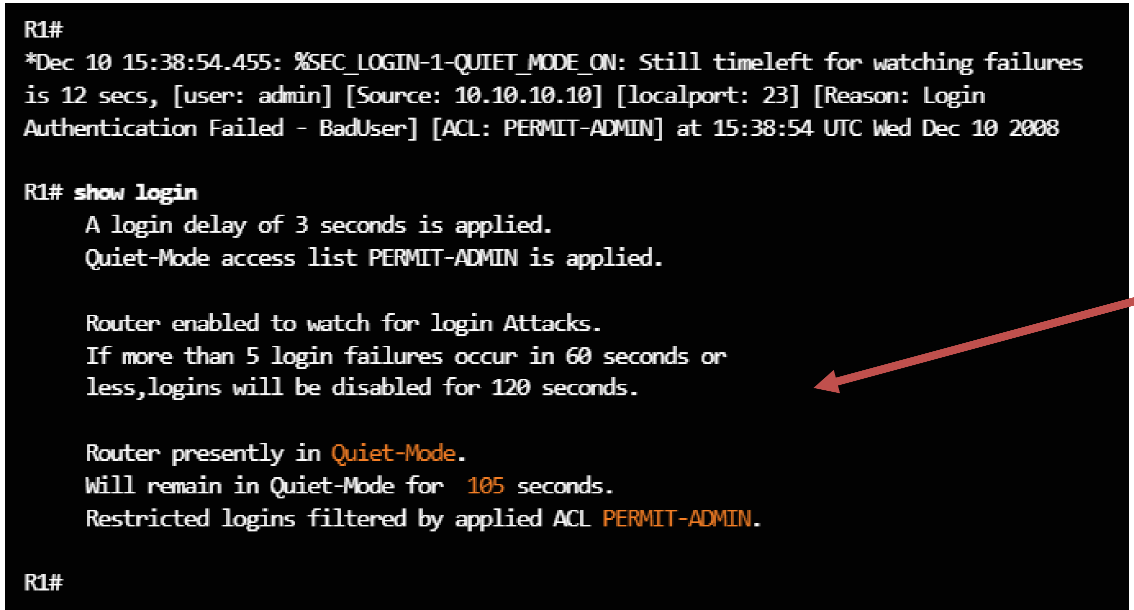


```
R1# show login
    A login delay for 10 sec is applied.
    Quiet-Mode access list PERMIT-ADMIN is applied.

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

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

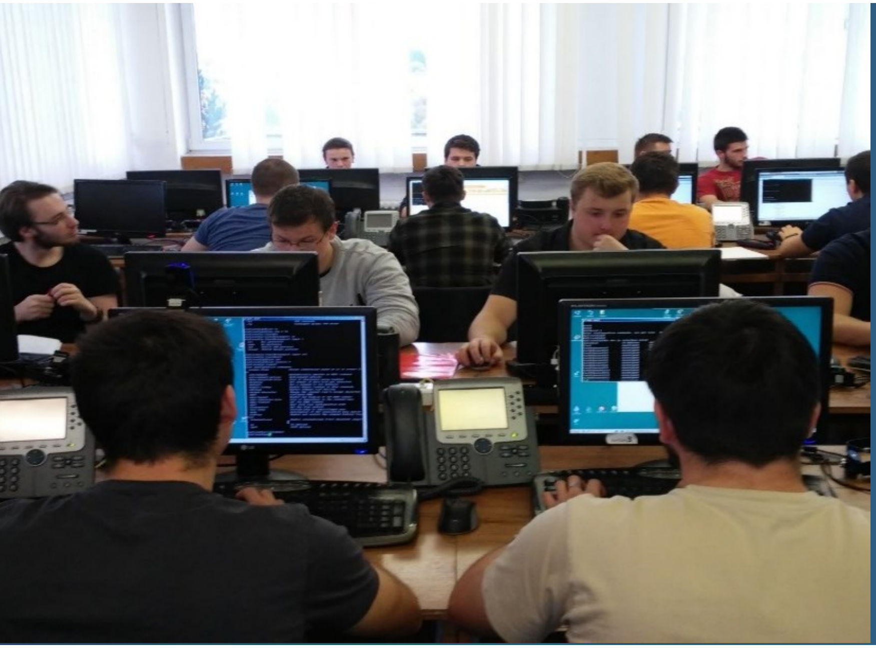


```
User Access Verification

Username: Admin
Password:
% Login invalid

Username: Admin
Password:
% Login invalid

Username: Admin
Password:
% Login invalid

User Access Verification

Username:
Username: Admin
Password:
% Login invalid

Username: Admin
Password:
% Login invalid
```

Unable to connect to 10.10.10.1 port 23

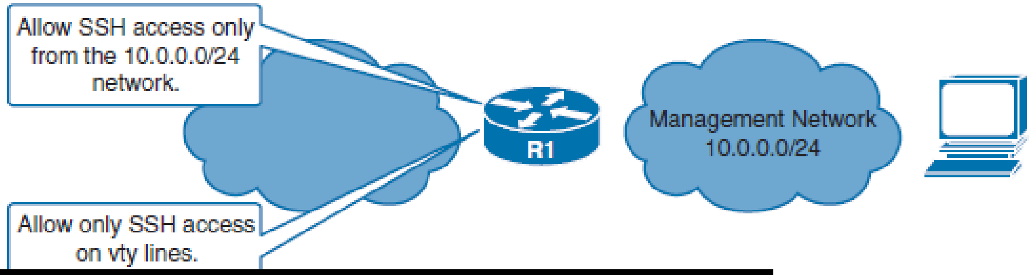


```
R1#
*Dec 10 15:38:54.455: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failures
is 12 secs, [user: admin] [Source: 10.10.10.10] [localport: 23] [Reason: Login
Authentication Failed - BadUser] [ACL: PERMIT-ADMIN] at 15:38:54 UTC Wed Dec 10 2008

R1# show login
    A login delay of 3 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#
```



Configuring SSH

Configuring SSH v2


Allow SSH access only from the 10.0.0.0/24 network.

Allow only SSH access on vty lines.

```
R1(config)#username palo algorithm-type scrypt secret HESLO
R1(config)#ip domain-name kis.fri.uniza.sk
R1(config)#crypto key generate rsa modulus 2048
The name for the keys will be: R1.kis.fri.uniza.sk

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 5 seconds)

*Sep  7 15:28:25.167: %SSH-5-ENABLED: SSH 1.99 has been enabled

R1(config)# ip ssh version 2
R1(config)# ip access-list standard PERMIT-SSH
R1(config-std-nacl)# remark Permit SSH from my management LAN
R1(config-std-nacl)# permit 10.0.0.0 0.0.0.255
R1(config-std-nacl)# deny any log
R1(config-std-nacl)#exit
Router(config)# line vty 0 15
Router(config-line)# login local
Router(config-line)# transport input ssh
Router(config-line)# access-class PERMIT-SSH in
```

Modifying the SSH Configuration

- Modify default ssh timeout
  - Def. is 120s.

```
Router(config)# ip ssh time-out SECONDS
```

- Modify ssh retries

```
Router(config)# ip ssh authenticatios-retries NUM
```

Show / remove SSH keys

```
R1# show crypto key mypubkey rsa
% Key pair was generated at: 15:28:25 UTC Sep 7 2018
Key name: R1.kis.fri.uniza.sk
Key type: RSA KEYS
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
  00C010D7 CFE29D09 CC1DC9F1 7D9F99A5 D061704A 83A05081 E87A9B2E 097117E9
  B18C74E2 D467150C CAF204F8 89B8370B EB0F59F9 0C66E35E A5F9BA66 CDFC7FA4
  DC900718 89DD96F8 A4740C2A 2FB1B887 5282C093 94C21722 77702482 6F2E823D
  391C0CCB 36243007 63D91297 EE86B7D7 313A9D59 07E1A9FF C0C15060 CB7490ED
  1685B4E3 5AB8C365 CB6BA3FF 773E9871 55720C8A 7D89596C 77755CD9 EAA0624B
  5CA0CB4E 866D9E1B E717EB0A E2BEB66C C9B6DB16 C03AFC16 95BDDD64 CEEE41BF
  FF6506ED 02C99CB5 823DE60D EEC1BF33 2BA68134 AD19B491 01EDCC3B EE504BAE
  31F59FFE D42C3049 24D514CE F12C9B8A B8D6F5F3 AA13C351 1E9F4A5A E024674A
  AF020301 0001
% Key pair was generated at: 15:28:25 UTC Sep 7 2018
Key name: R1.kis.fri.uniza.sk.server
Key type: RSA KEYS
Temporary key
 Usage: Encryption Key
```

```
!removing keys
R1(config)# crypto key zeroize rsa
% All keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
R1(config)#
*Sep  7 15:36:04.607: %SSH-5-DISABLED: SSH 2.0 has been disabled
```

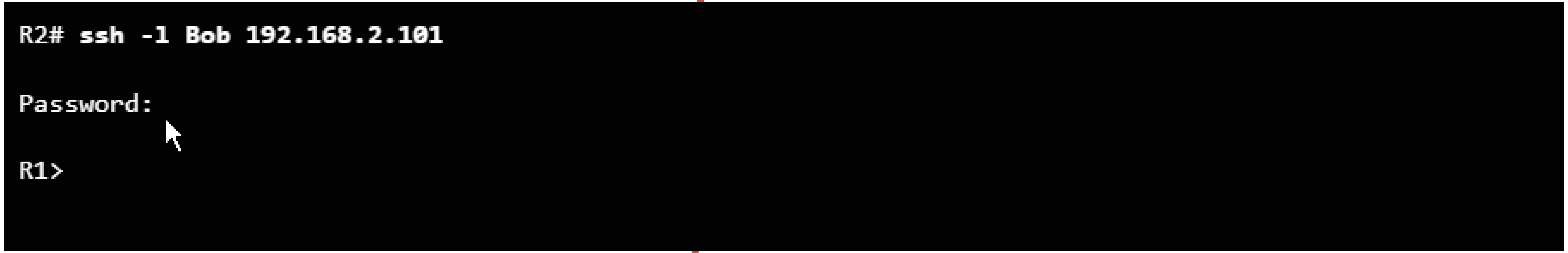
Verification of ssh service and SSH sessions

```
! Show the protocol version of running ssh service
R1# sh ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDAENfP4p0JzB3J8X2fmaXQYXBKg6BQgeh6my4JcRfp
sYx04tRnFQzK8gT4ibg3C+sPWfkMZuNepfm6Zs38f6TckAcYid2W+KR0DCovsbiHUoLAk5TCFyJ3cCSC
by6CPTkcDMs2JDAHY9kSl+6Gt9cxOp1ZB+Gp/8DBUGDLdJDtFoW041q4w2XLa6P/dz6YcVVyDIp9iVls
d3Vc2eqgYktcoMtOhm2eG+cX6wrivrZsybbbFsA6/BaVvd1kzu5Bv/9lBu0CyZy1gj3mDe7BvzMrpoE0
rRm0kQHtzDvuUEuuMfWf/tQsMEkk1RTO8SybirjW9fOqE8NRHp9KWuAkZ0qv
```

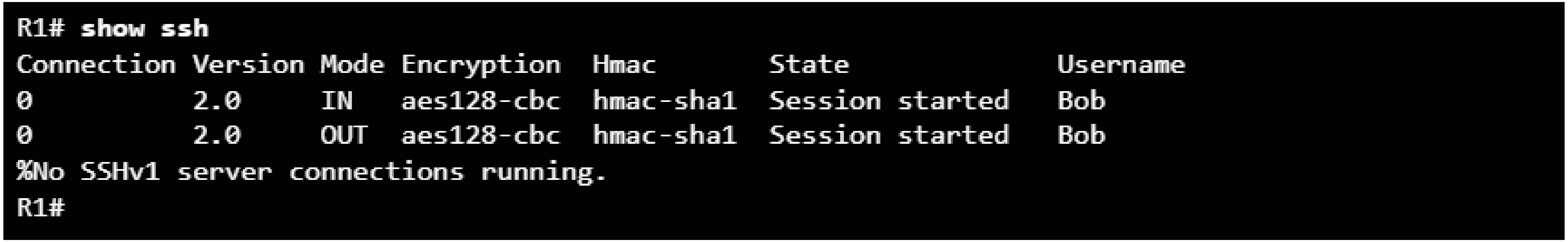
```
! Show present ssh sessions
R1# sh ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
```

Verify ssh sessions

```
R1(config)#do sh ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
```



```
R2# ssh -l Bob 192.168.2.101

Password:

R1>
```



```
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#
```

Assigning Administrative Roles

Configuring Privilege Levels

- Privilege levels: Determines who should be allowed to connect to the device and what should be able to do with
  - Cisco has two types

ROLE BASED CLI - access commands:

- views, and assigned users
- Commands per user-role

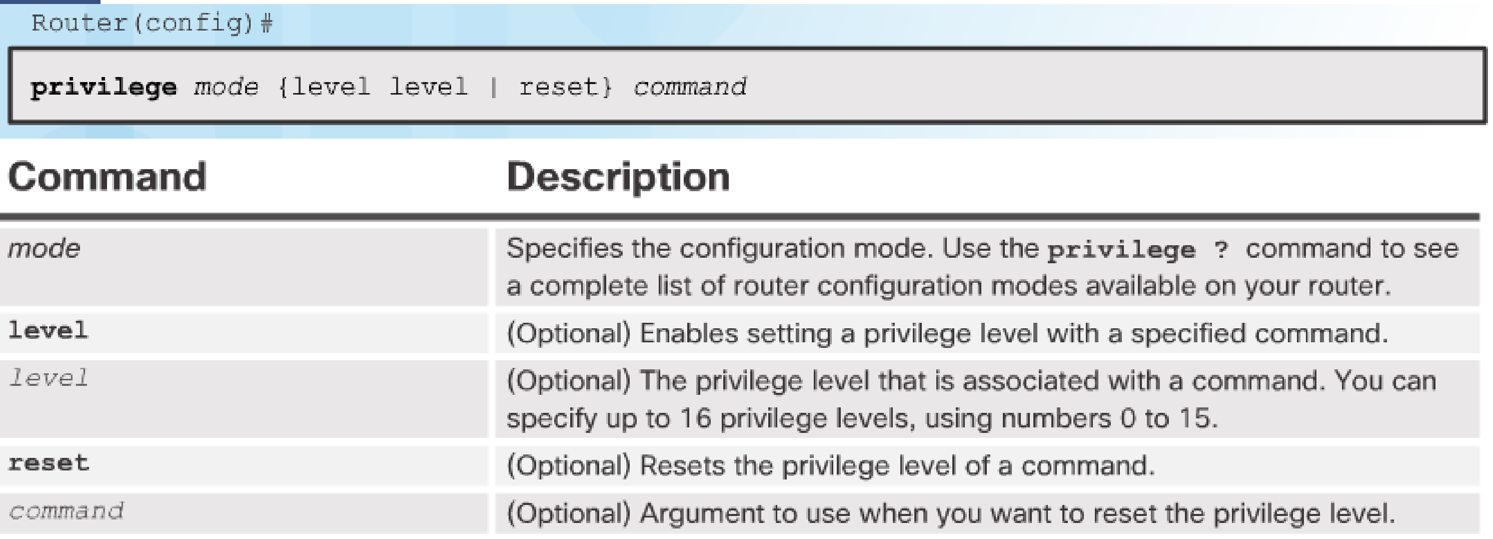
* **PRIVILEGE levels:**

* assign certain commands to certain privilege levels, then assign those levels to a user.

- Level 0: Predefined for user-level access privileges.
- Level 1: Default level for login with the router prompt.
- Level 2-14: May be customized for user-level privileges.
- Level 15: Reserved for the enable mode privileges

- **User EXEC mode (privilege level 1)**
  - Lowest EXEC mode user privileges
  - Only user-level command available at the router> prompt
- **Privileged EXEC mode (privilege level 15)**
  - All enable-level commands at the router# prompt

Privilege Level Syntax



```
Router(config)#

privilege mode {level level | reset} command
```

Command	Description
mode	Specifies the configuration mode. Use the **privilege ?** command to see a complete list of router configuration modes available on your router.
level	(Optional) Enables setting a privilege level with a specified command.
level	(Optional) The privilege level that is associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15.
reset	(Optional) Resets the privilege level of a command.
command	(Optional) Argument to use when you want to reset the privilege level.

Configuring and Assigning Privilege Levels

- Configure a privilege level with specific commands

```
Router(config)# privilege exec level LEVEL [COMMAND]
```

- Example

```
! Level 5 and SUPPORT user configuration
! Add the ping cmd to the level 5
R1(config)# privilege exec level 5 ping
! 1) Assign a pass for accessing level 5 - one method
R1(config)# enable algorithm-type scrypt secret level 5 cisco5
! Or 2) Create an user and assign him to the level 5 with a password - second method
R1(config)# username SUPPORT privilege 5 algorithm-type scrypt secret cisco5

! Level 10 and JR-ADMIN user configuration
R1(config)# privilege exec level 10 reload
R1(config)# enable algorithm-type scrypt secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 algorithm-type scrypt secret cisco10

! Level 15 and ADMIN user configuration
R1(config)# enable algorithm-type scrypt secret level 15 cisco123
R1(config)# username ADMIN privilege 15 algorithm-type scrypt secret cisco123
```

Check

```
R1#enable ?
  <0-15>  Enable level
  view    Set into the existing view
  <cr>

R1>enable 5
Password: <cisco5>
R1#show privilege
Current privilege level is 5
R1#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

R1#reload
Translating "reload"

% Bad IP address or host name
Translating "reload"

% Unknown command or computer name, or unable to find computer address

R1#conf t
      ^
% Invalid input detected at '^' marker.


R1#enable 10
R1#reload

System configuration has been modified. Save? [yes/no]:yes
```

Limitations of Privilege Levels

- No access control to specific interfaces, ports, logical interfaces, and slots on a router
- Commands available at lower privilege levels are always executable at higher privilege levels
- Commands specifically set at higher privilege levels are not available for lower privilege users
- Assigning a command with multiple keywords allows access to all commands that use those
  - For example allowing the access to **show ip route** allows the user access to all **show** and **show ip** commands.

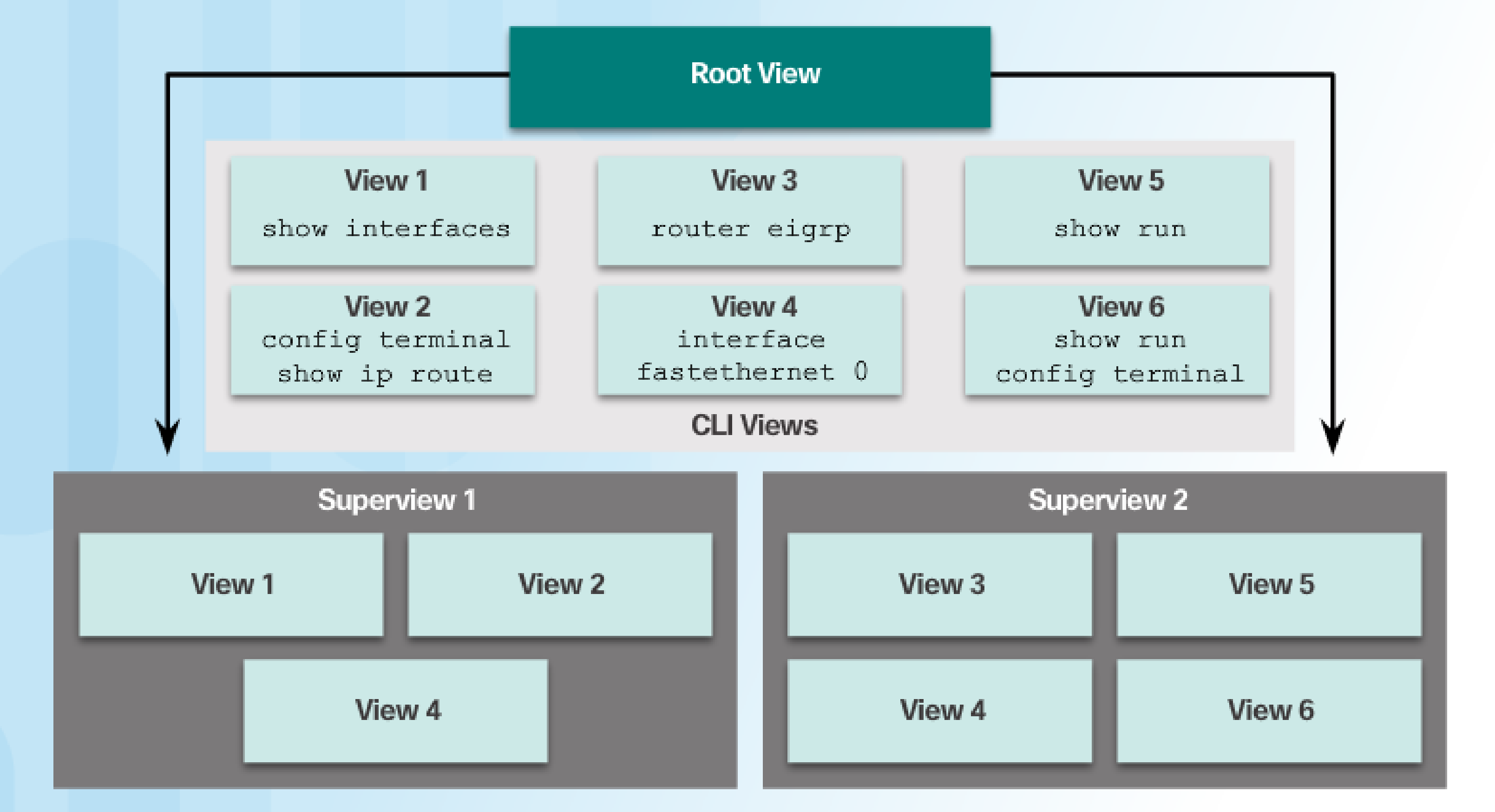
Configuring Role-Based CLI

Role-Based CLI Access

- Role-Based CLI
  - Provides more flexibility as privilege levels
  - Introduced in 12.3(11)T
  - Uses different views for different users
    - That allow add and control which commands are available to specific roles
    - For example:
      - Other set of commands for the Security operator
      - And other set of commands for WAN engineer
    - ***Note**: Number of views and superviews is limited up to 15*
  - That enhance
    - Security
      - Defines sets of cmds for an user
      - Allows control the access to specific port/slot/interface
    - Availability
      - Disallows to execute commands that are not assigned
    - Operational Efficiency
      - Users see assigned commands only

Role-Based Views

- Provides three types of view:
  - **Root view**
    - The same privileges as a user with level 15 privileges
    - Added/removed/configured only by a root
  - **CLI views**
    - Specific set of commands
    - No hierarchy, no higher/lower orders
    - No inherit cmds
    - the same commands can be used in multiple views
    - Single CLI view ma be shared with several SuperView
  - **Superviews**
    - Consists of one or more CLI views
    - Allows assign to users/groups more CLI views at once
    - Does not contain cmds directly
    - User with a superview may access all cmds of all assigned CLI views
    - Each superview has a password
    - Deleting a superview does not delete the associated CLI view



Superviews contain Views but not commands. Two Superviews can use the same View. For example, both Superview 1 and Superview 2 can have CLI View 4 placed inside.

Configuring Role-Based CLI Views

- Step 1: enable AAA and enter into a root view

```
! Enabling aaa-new-model is required
Router(config)# aaa new-model
Router(config)# exit
Router# enable [view [VIEW-NAME]]
```

  - view: without *VIEW-NAME* enters into a root view, which enable to configure a CLI view
  - *view-name:* optional, enter/exit a specific CLI view; switch between CLI views

- Step 2: create a view

```
Router(config)# parser view VIEW-NAME
Router(config-view)#
```

- Step 3: Assign a secret password for a view; mandatory

```
Router(config-view)# secret ENCR-PASS
```

- Step 4: assigns commands to a view

```
Router(config-view)# commands PARSER MODE {include | include-exclusive | exclude}  [all]
   [interface INT-NAME | COMMAND]
```

- Step 5: exit

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

Example

```
R1(config)# aaa new-model
R1(config)# exit

R1# enable view
Password: <priv-level-15-pass / enable secret>

R1# conf t

! Create a CLI view
R1(config)# parser view SHOWVIEW
! Secure access
R1(config-view)# secret cisco
! Add commands
R1(config-view)# commands exec include show version
R1(config-view)# commands exec include show interfaces
R1(config-view)# commands exec include show ip interface
brief
R1(config-view)# commands exec include show parser view
R1(config-view)# exit

R1(config)# parser 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)# secret cisco10
R1(config-view)# commands exec include reload
R1(config-view)# exit
```

```
! Verify
R1# sh parser view all
No view is active ! Currently in Privilege Level
Context

! View must be active
R1# enable view SHOWVIEW
Password: cisco

R1# show parser view
Current view is 'SHOWVIEW'

R1# sh parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
-------(*) represent superview-------

R1# show ?
…
  interfaces   Interface status and configuration
  ip           IP information
  parser       Display parser information
  version      System hardware and software status

R1# show run | begin view
parser view SHOWVIEW
 secret 5 $1$C3gn$NTq088ymZY4VlfwvpmiuZ.
 commands exec include all show
…
! Delete view
No parser view SHOWVIEW
```

Configuring Role-Based CLI Superviews

- Step 1: enable AAA and enter into a root view

```
! Enabling aaa-new-model is required
Router(config)# aaa new-model
Router(config)# exit
Router# enable [view [VIEW-NAME]]
```

- Step 2: create a view

```
Router(config)# parser view VIEW-NAME superview
Router(config-view)#
```

- Step 3: Assign a secret password for a superview; mandatory

```
Router(config-view)# secret ENCR-PASS
```

- Step 4: adds a CLI view to a superview;

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

  - multiple allowed, must exist

- Step 5: exit a superview

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

- Access a view/superview

```
Router(config)# enable view VIEW-NAME
```

```
! Delete view
Router(config)# no parser view VIEW-NAME
```

Example

```
R1(config)# aaa new-model
R1(config)# exit
R1# enable view
Password: <priv-level-15-pass>

R1# conf t

R1(config)# parser view USER superview
R1(config-view)# secret cisco
R1(config-view)# view SHOWVIEW
R1(config-view)# exit


R1(config)# parser view SUPPORT superview
R1(config-view)# secret cisco1
R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# exit

R1(config)# parser view JR-ADMIN superview
R1(config-view)# secret cisco2
R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# view REBOOTVIEW
R1(config-view)# end
```

Verification

```
R1# sh parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 REBOOT
 VERIFYVIEW
 REBOTVIEW
 TEMP
 USER *

 SUPPORT *

 JR-ADMIN *

-------(*) represent superview-------

R1# show run | begin view

parser view SHOWVIEW
 secret 5 $1$C3gn$NTq088ymZY4VlfwvpmiuZ.
 commands exec include show
…
```

```
R1# show parser view
Current view is 'root'

R1#enable view JR-ADMIN
Password:

R1#sh parser view
Current view is 'JR-ADMIN`
R1# ?
Exec commands:
  do-exec   Mode-independent "do-exec" prefix support
  enable    Turn on privileged commands
  exit      Exit from the EXEC
  ping      Send echo messages
  reload    Halt and perform a cold restart
  show      Show running system information
R1#show ?
  bootflash:  display information about bootflash: file
system
  disk0:      display information about disk0: file system
  disk1:      display information about disk1: file system
  flash:      display information about flash: file system
  parser      Display parser information
  slot0:      display information about slot0: file system
  slot1:      display information about slot1: file system
```

Assigning a view

```
! Start aaa new model authorization
aaa authorization exec default local

! Assign view to an user
username NAME view VIEW-NAME algorithm-type scrypt secret SECRET-PASS
```

Monitoring and Managing Devices

Use the Cisco IOS resilient configuration feature to secure the Cisco IOS image and configuration files.

- Compare in-band and out-of band management access.
- Configure syslog to log system events.
- Configure secure SNMPv3 access using ACL
- Configure NTP to enable accurate timestamping between all devices.

Securing Cisco IOS Image and Configuration Files

Boot secure

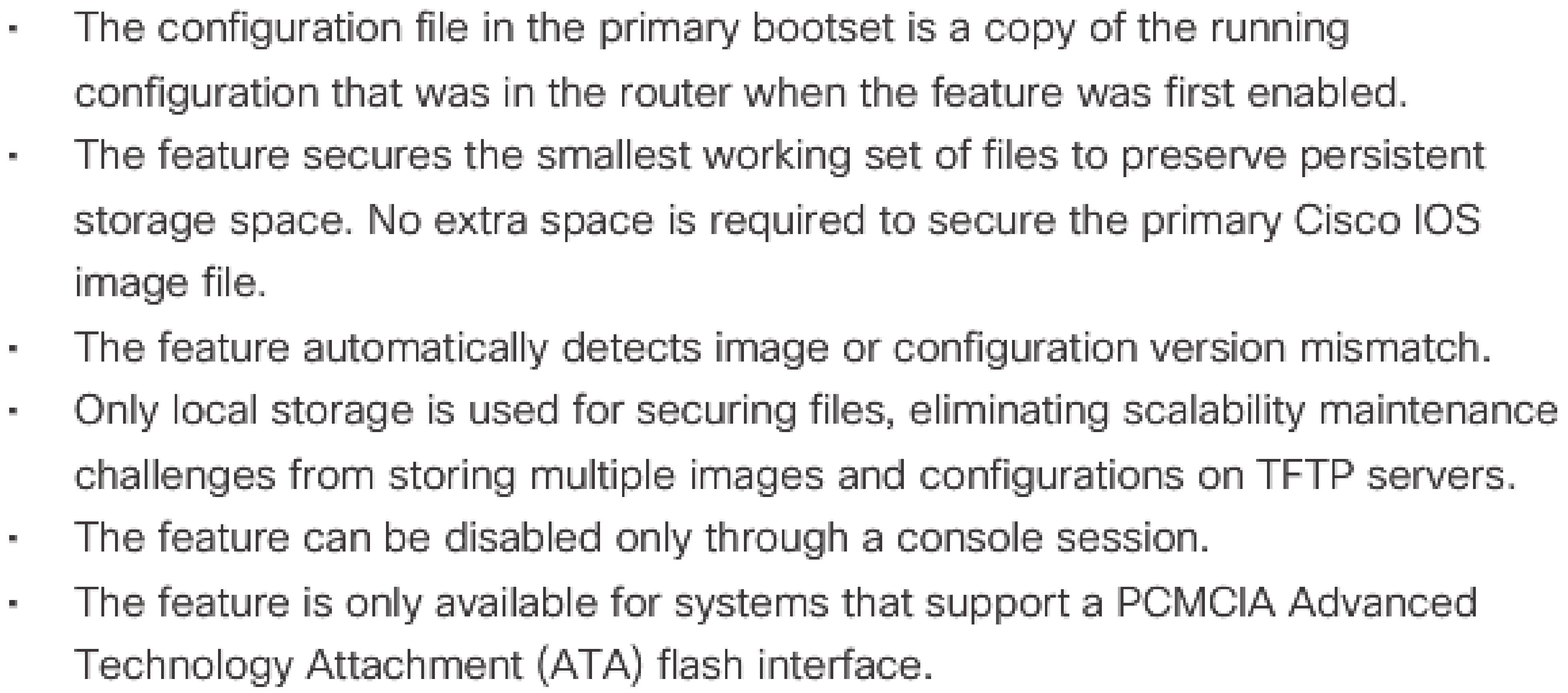
Config secure

Backup files using SCP

Cisco IOS Resilient Configuration

- Available from 12.3(8)T IOS
- Allows for faster recovery in the case of flash reformats or NVRAM erases
  - Allows to make secure IOS and config backups into hidden files stored on flash
  - These files are not directly accessible using IOS commands
    - Cannot be deleted using format or erase commands
    - They allows to make an IOS file and config recovery
    - The support of Resilient configuration can not be deactivated remotely
    - Usually supported on routers

Cisco IOS Resilient Configuration Facts



- The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.
- The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file.
- The feature automatically detects image or configuration version mismatch.
- Only local storage is used for securing files, eliminating scalability maintenance challenges from storing multiple images and configurations on TFTP servers.
- The feature can be disabled only through a console session.
- The feature is only available for systems that support a PCMCIA Advanced Technology Attachment (ATA) flash interface.

IOS Resilient Configuration

- Enable Cisco IOS image resilience and secure the IOS image

```
Router(config)# secure boot-image
```

- Disable the feature

```
Router(config)# no secure boot-image
```

- Backup actual config (must be used repeatedly after each config change):

```
Router(config)# secure boot-config
```

- Verify the archive: list infos

```
Router# show secure [bootset]
```

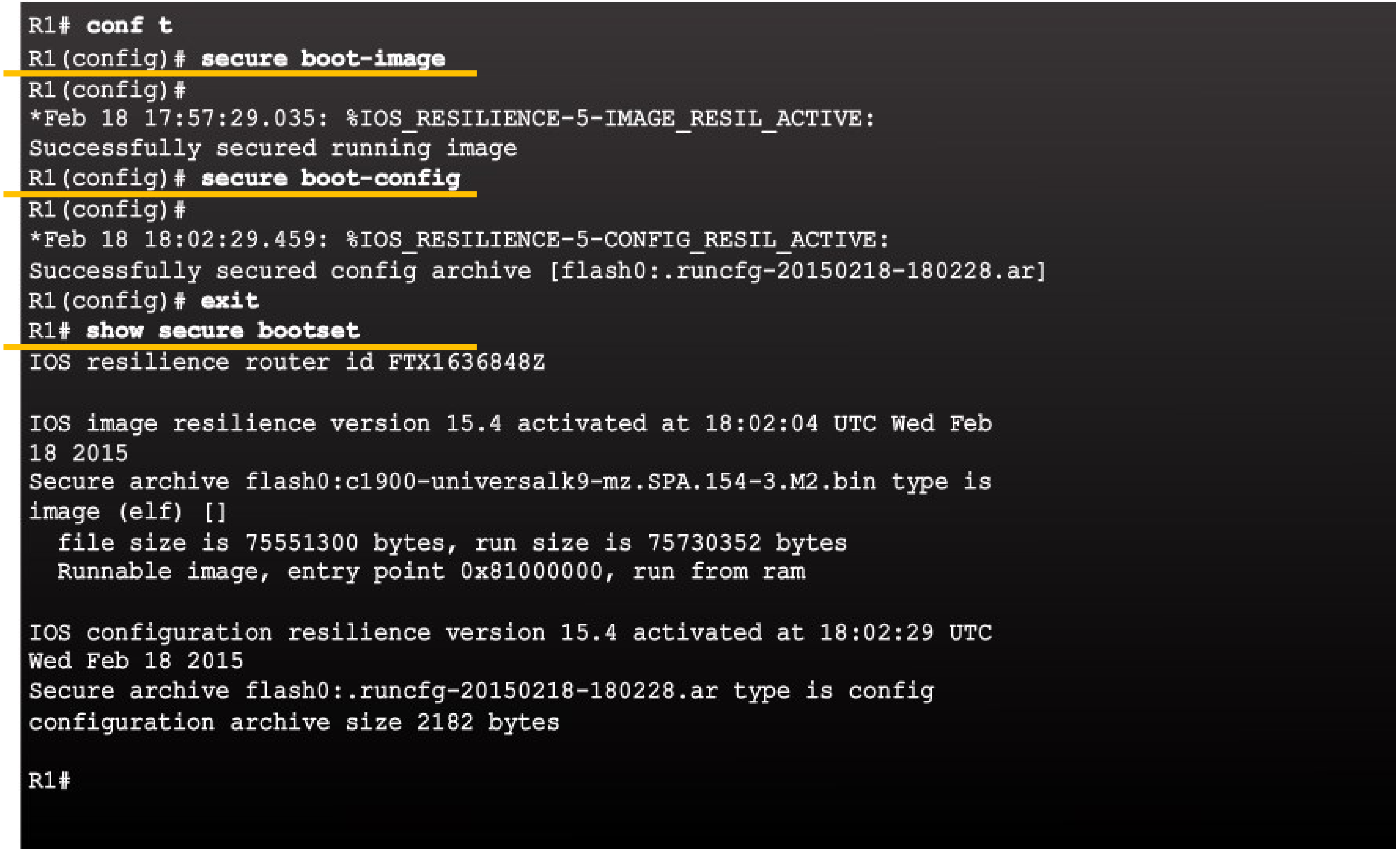
- **IOS recovery** – inside of the ROMMON using

```
rommon 1 > no secure boot-image
```

- **Config recovery** using cmd:

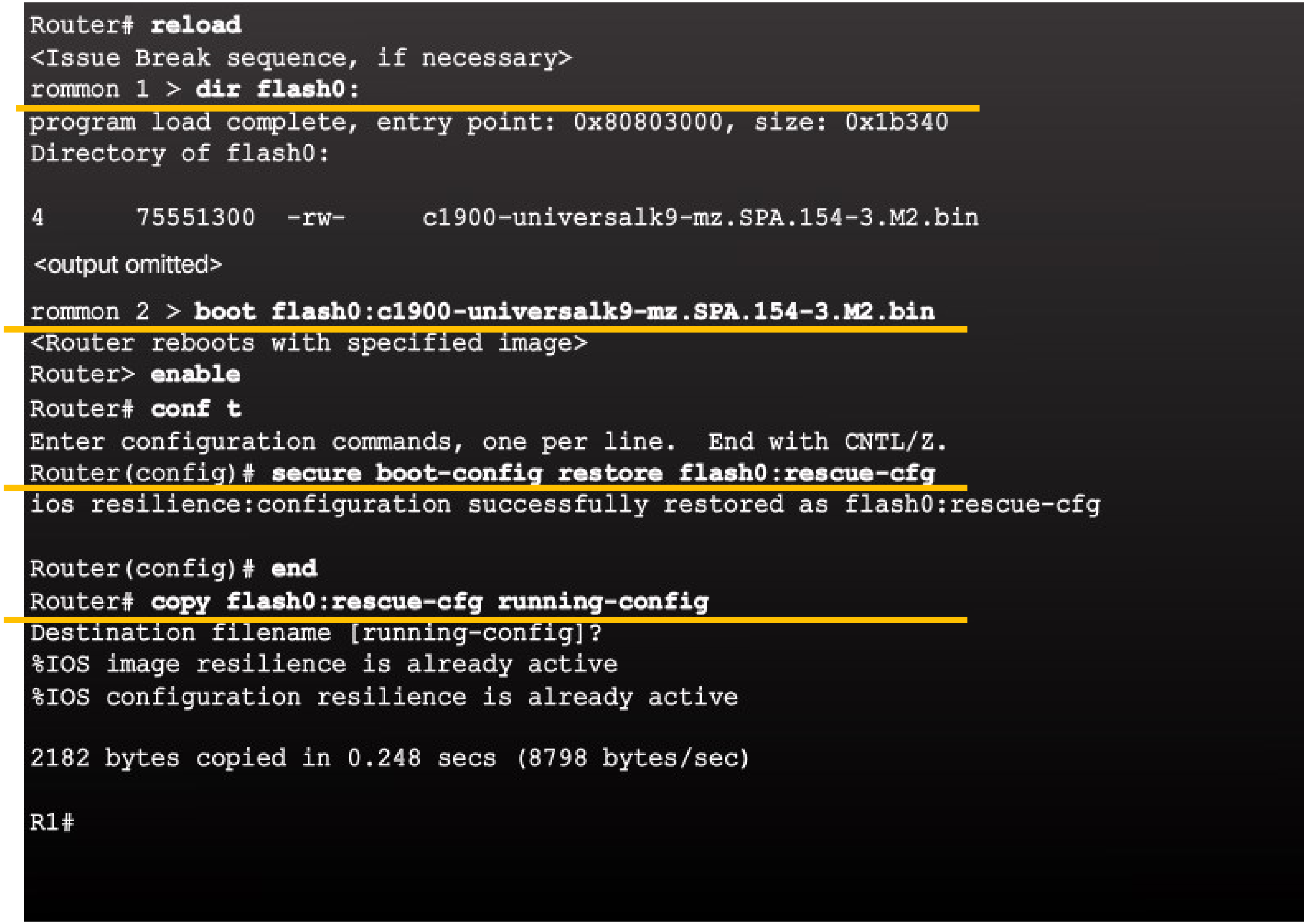
```
Router(config)# secure boot-config restore CIEĽOVÝ-SÚBOR
```

Enabling the IOS Image Resilience Feature



```
R1# conf t
R1(config)# secure boot-image
R1(config)#
*Feb 18 17:57:29.035: %IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE:
Successfully secured running image
R1(config)# secure boot-config
R1(config)#
*Feb 18 18:02:29.459: %IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE:
Successfully secured config archive [flash0:.runcfg-20150218-180228.ar]
R1(config)# exit
R1# show secure bootset
IOS resilience router id FTX1636848Z

IOS image resilience version 15.4 activated at 18:02:04 UTC Wed Feb
18 2015
Secure archive flash0:c1900-universalk9-mz.SPA.154-3.M2.bin type is
image (elf) []
  file size is 75551300 bytes, run size is 75730352 bytes
  Runnable image, entry point 0x81000000, run from ram

IOS configuration resilience version 15.4 activated at 18:02:29 UTC
Wed Feb 18 2015
Secure archive flash0:.runcfg-20150218-180228.ar type is config
configuration archive size 2182 bytes

R1#
```

Restore the Primary Bootset Image - example



```
Router# reload
<Issue Break sequence, if necessary>
rommon 1 > dir flash0:
program load complete, entry point: 0x80803000, size: 0x1b340
Directory of flash0:

4      75551300  -rw-     c1900-universalk9-mz.SPA.154-3.M2.bin

<output omitted>

rommon 2 > boot flash0:c1900-universalk9-mz.SPA.154-3.M2.bin
<Router reboots with specified image>
Router> enable
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# secure boot-config restore flash0:rescue-cfg
ios resilience:configuration successfully restored as flash0:rescue-cfg

Router(config)# end
Router# copy flash0:rescue-cfg running-config
Destination filename [running-config]?
%IOS image resilience is already active
%IOS configuration resilience is already active

2182 bytes copied in 0.248 secs (8798 bytes/sec)

R1#
```

Backup files using the Secure Copy (SCP)

- The Secure Copy (SCP) feature provides a secure and authenticated method for copying router configuration or router image files.

Enabling SCP on a Router

- **Step 1.** Use the `username name [ privilege level ] { secret password }` command for local authentication or configure TACACS+ or RADIUS.
- **Step 2.** Enable SSH. Configure a domain name using the `ip domain-name` and generating the crypto keys using the `crypto key generate rsa general key` global configuration commands.
- **Step 3.** AAA with the `aaa new-model` global configuration mode command.
- **Step 4.** Use the `aaa authentication login { default | list-name } method1 [ method2 ...]` command to define a named list of authentication methods.
- **Step 5.** Use the `aaa authorization { network | exec | commands level } { default | listname } method1... [ method4 ]` command to configure command authorization.
- **Step 6.** Enable SCP server-side functionality with the **ip scp server enable** command.

SCP - Example

```
R1(config)# username admin privilege 15 algorithm-type scrypt secret admin
R1(config)# ip domain name kis.lab.sk
R1(config)# crypto key generate rsa general-keys modulus 1024
R1(config)# aaa new-model
R1(config)# aaa authentication login default local
R1(config)# aaa authorization exec default local none
R1(config)# ip scp server enable
```

```
! Copy/download running-config from PC using SCP
pscp -scp -l admin -pw admin admin@1.1.1.2:system://running-config R1.cfg
R1.cfg                    | 2 kB |   2.9 kB/s | ETA: 00:00:00 | 100%

! Copy startup
pscp -scp -l admin -pw admin admin@1.1.1.2:nvram://startup-config R1.cfg
R1.cfg                    | 2 kB |   2.8 kB/s | ETA: 00:00:00 | 100%
```

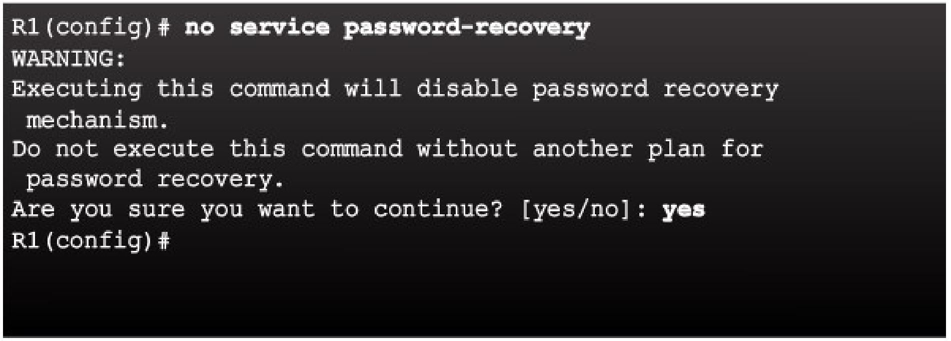
```
! Copy/upload from router to SCP server
R1# copy system:running-config scp:
Address or name of remote host []? 10.1.1.1
Destination username [R1]? admin
Destination filename [r1-confg]?
Writing r1-confg
Password: <admin>
!
1381 bytes copied in 5.596 secs (161 bytes/s)
```

Recovering a Router Password

1. Connect to the console port.
2. Record the configuration register setting (**show version)**.
3. Power cycle the router.
4. Issue the break sequence
   - press and keep Ctrl +Break key
   - Putty (if previous does not work) => right click on the header of putty / Special Commands / Break.
5. Change the default configuration register
   - CLI> **confreg 0x2142**
6. Reboot the router.
   - CLI> reset
7. Press Ctrl-C to skip the initial setup procedure.
8. Put the router into privileged EXEC mode.
9. Copy the startup configuration to the running configuration.
10. Verify the configuration.
11. Change the enable secret password.
12. Enable all interfaces.
13. Change the config-register with the *config-register configuration_register_setting*.
14. Save the configuration changes

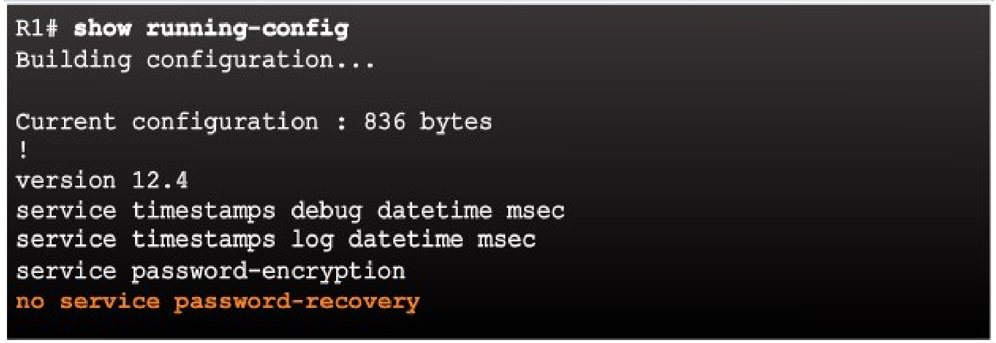
Mitigation of Password Recovery attack

- **Attack:** Attacker with a physical access and using password recovery procedure may gain control of a box
- **Mitigation**: Disable password recovery service
  - Command is hidden, must by applied as is written

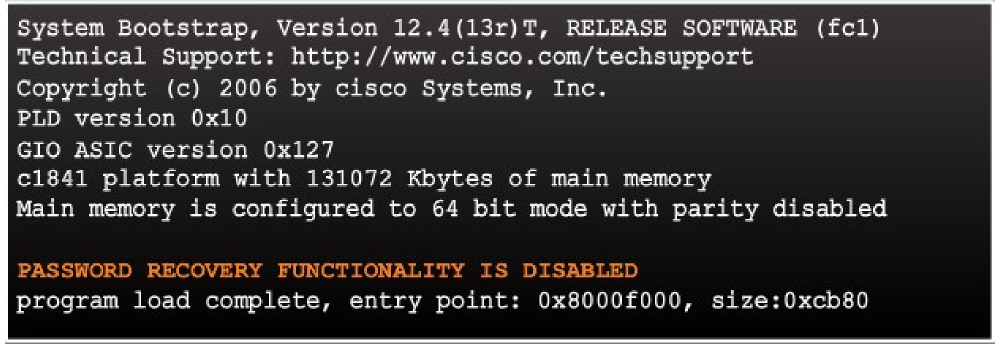


```
R1(config)# no service password-recovery
WARNING:
Executing this command will disable password recovery
 mechanism.
Do not execute this command without another plan for
 password recovery.
Are you sure you want to continue? [yes/no]: yes
R1(config)#
```

- Verification:
- **Show run** **boot proces**



```
R1# show running-config
Building configuration...

Current configuration : 836 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service password-recovery
```



```
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x8000f000, size:0xcb80
```

  - `no service password-recovery`
    - Needed to initiate and confirm the break sequence within five seconds after the image decompresses
    - router boots empty with the factory default configuration

Caution !!!!

- *If the router flash memory does not contain a valid Cisco IOS image because of corruption or deletion, the ROMmon xmodem command cannot be used to load a new flash image. To repair the router, an administrator must obtain a new Cisco IOS image on a flash SIMM or on a PCMCIA card. However, if an administrator has access to ROMmon they can restore an IOS file to flash memory using a TFTP server.*
- *Refer to Cisco.com for more information regarding backup flash images.*

Further reading (…in case of interest)

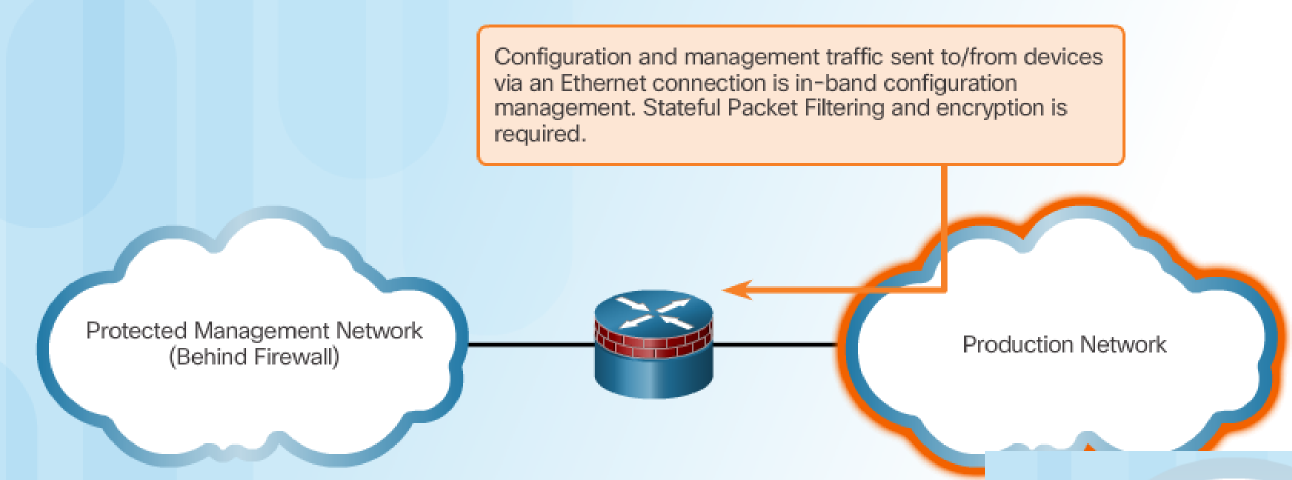
- User Security Configuration Guide, Cisco IOS Release 15MT
  - Views, privilege levels
    - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-mt/sec-usr-cfg-15-mt-book/sec-role-base-cli.html
  - Login Enhancements-Login Block
    - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-mt/sec-usr-cfg-15-mt-book/sec-login-enhance.html
  - Resilient config
    - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-mt/sec-usr-cfg-15-mt-book/sec-resil-config.html

Secure Management and Reporting

Determining the Type of Management Access

- Management (and monitoring) is an essential requirements for working on secured network
  - it suppose bidirectional informational flows between managing and managed devices
- Realization of management/monitoring access can take two ways
  - **In-Band**
    - Using regular data communication paths
    - Less secure, therefore need to be enhanced using the encryption (encrypted VPN, SSH/SSL)
    - Recommended for smaller networks
  - **Out-of-Band (OOB)**
    - Use of dedicated and secured management network
      - separate from production data traffic
      - highly secured, segmented (for example vlan separation)
      - disallow direct communication with other hosts
    - Terminal servers are connected directly to devices console
    - Preferred way for large enterprise networks

Determining the Type of Management Access



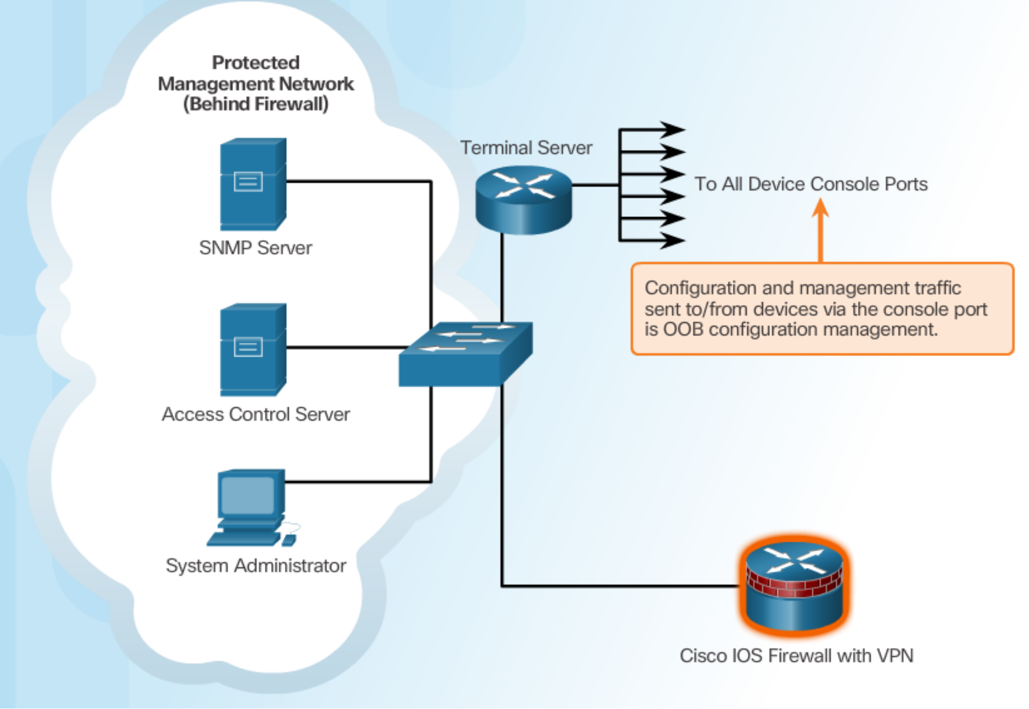
Configuration and management traffic sent to/from devices via an Ethernet connection is in-band configuration management. Stateful Packet Filtering and encryption is required.

In-Band Management:

- Apply only to devices that need to be managed or monitored
- Use IPsec, SSH, or SSL when possible
- Decide whether the management channel need to be open at all time

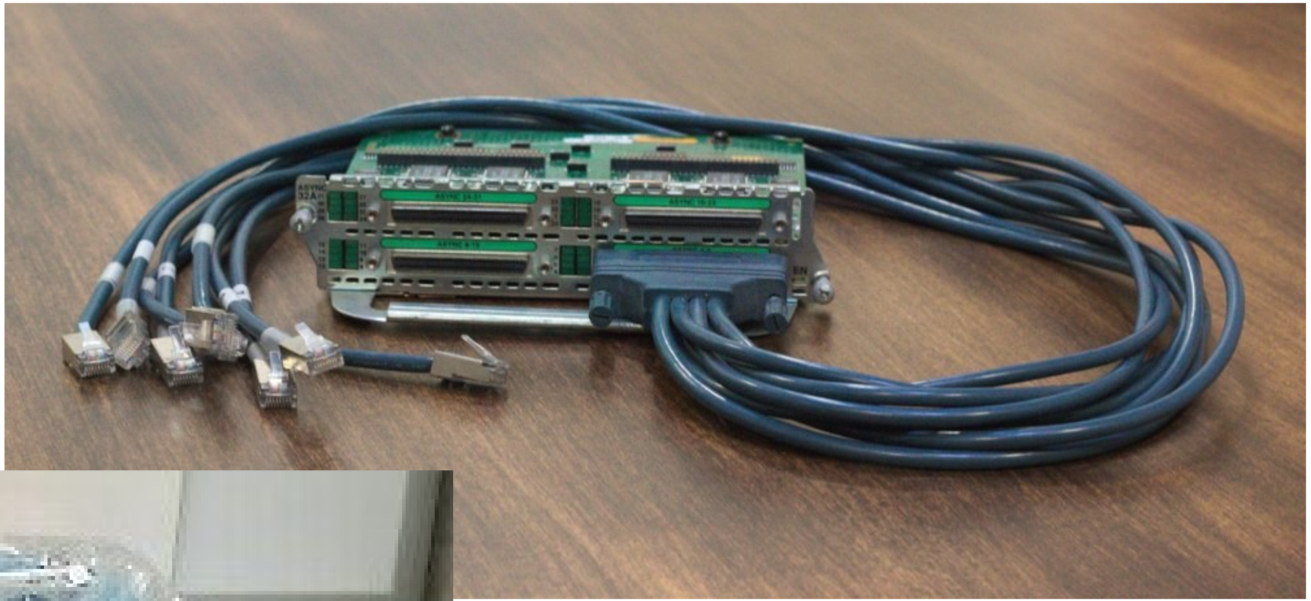
Out-of-Band (OOB) Management:

- Provide highest level of security
- Mitigate the risk of passing management protocols over the production network



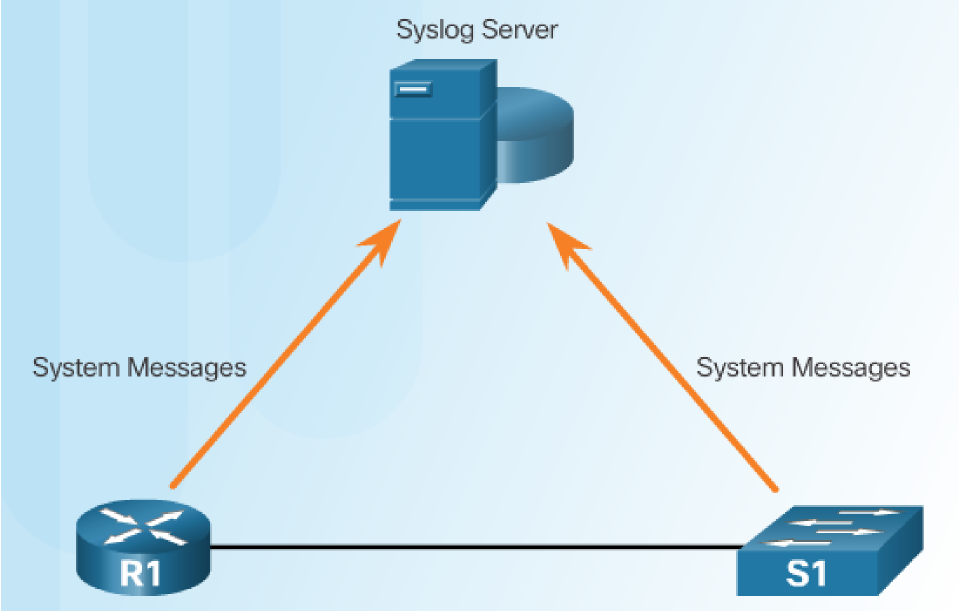
Configuration and management traffic sent to/from devices via the console port is OOB configuration management.

Cisco “octopus” RAS/console server

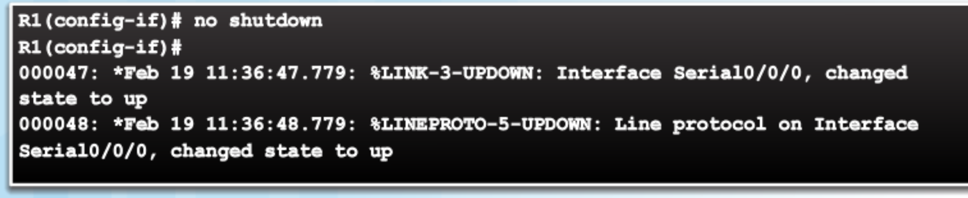


Using Syslog for Network Security

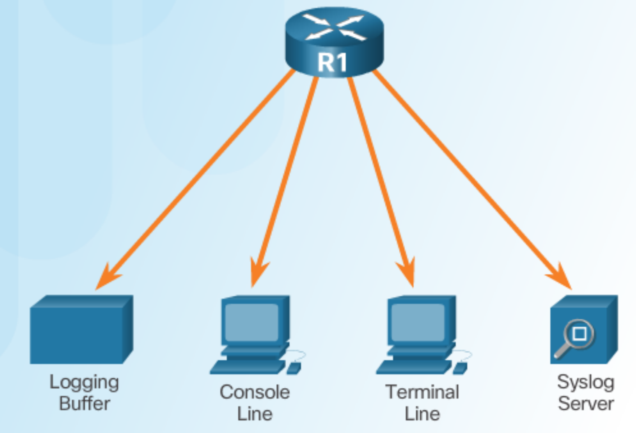
Introduction to Syslog



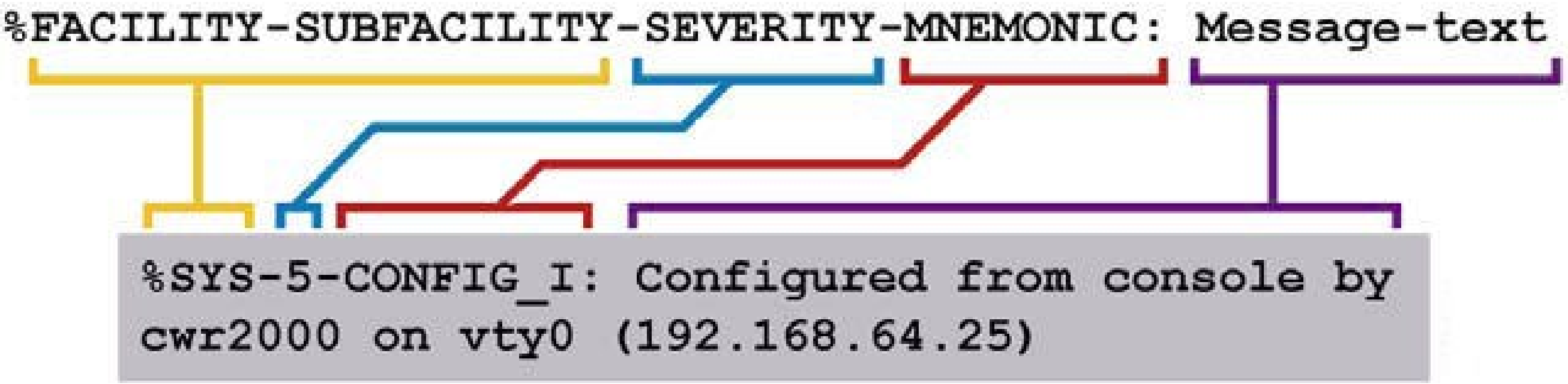
- **Sys**tem Message **Log**ging
  - Universally supported system
- Client / server model
  - Syslog client (agent)
    - Allows monitored devices report system error and notification messages
  - Syslog server
    - Collect, parse and interprets log messages
- Using port UDP 514
- Cisco support logging on:
  - Console (default), vty, buffer, syslog server



```
R1(config-if)# no shutdown
R1(config-if)#
000047: *Feb 19 11:36:47.779: %LINK-3-UPDOWN: Interface Serial0/0/0, changed
state to up
000048: *Feb 19 11:36:48.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
```



Cisco - Syslog message format



```
%FACILITY-SUBFACILITY-SEVERITY-MNEMONIC: Message-text
```

```
%SYS-5-CONFIG_I: Configured from console by
cwr2000 on vty0 (192.168.64.25)
```

- Systémová správa začína so znakom percento (%)
- **Facility**
  - Dve alebo viac písmen identifikujúci hw zariadenie, protocol, alebo sw modul
- **Severity**
  - Kód od 0-7, ktorá indikuje úroveň závažnosti
- **Mnemonic**
  - Kód jednoznačne identifikujúci správu
- **Message-text**
  - Text popisujúci daný stav. Môže obsahovať detailnejší popis danej udalosti, zahŕňajúci portové číslo, terminal, meno používateľa apod

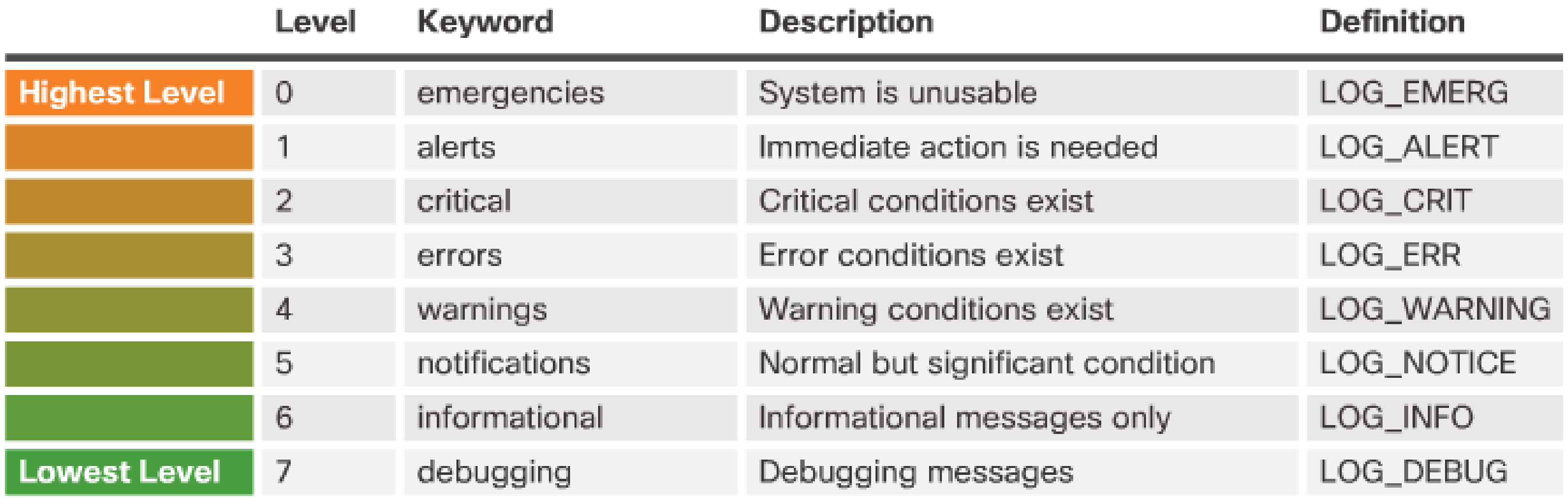
Syslog Facilities

- Identifikuje službu, ktorá poslala hlášku na syslog.
- Využívané na identifikáciu a kategorizáciu hlásení
- Cisco IOS má aktuálne viac ako 500 „facilities“
- Najznámejšie:
    - IP
    - OSPF
    - SYS operating system
    - IP Security (IPsec)
    - Route Switch Processor (RSP)
    - Interface (IF)

Severity levels

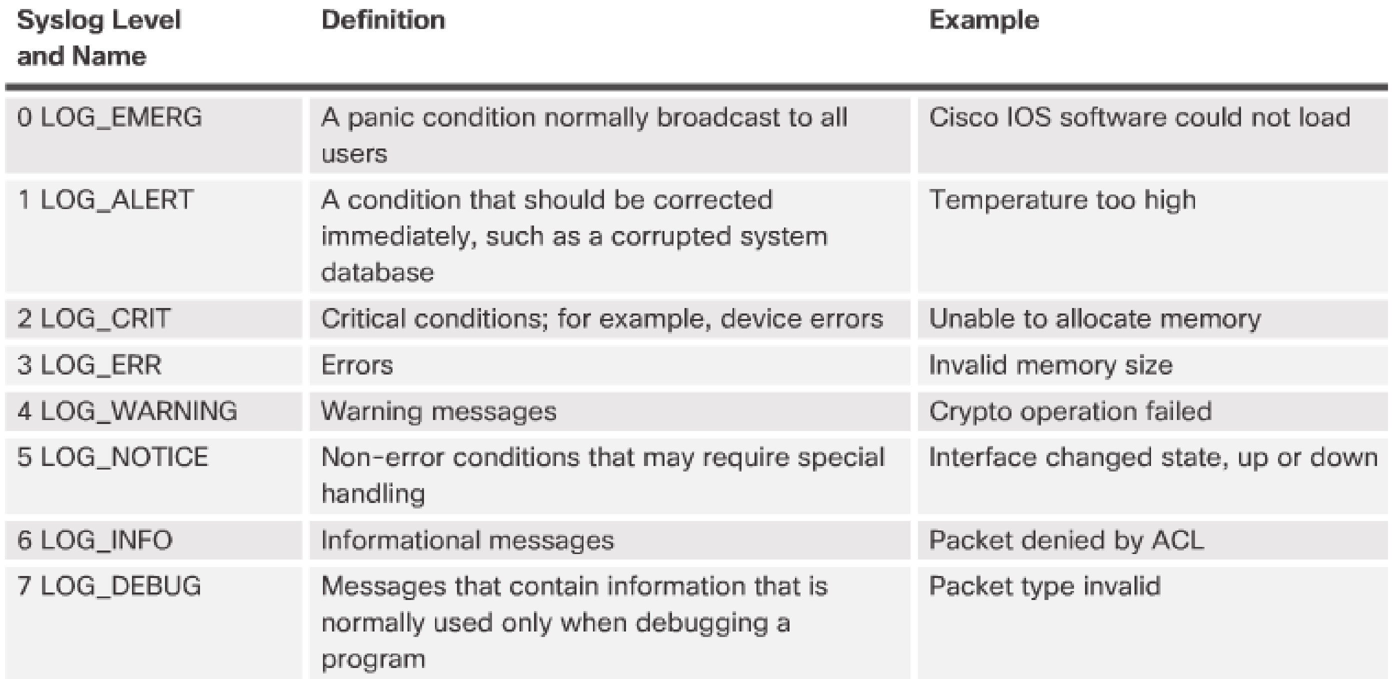
Security Levels

- Lower number higher importance



	Level	Keyword	Description	Definition
Highest Level	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	notifications	Normal but significant condition	LOG_NOTICE
	6	informational	Informational messages only	LOG_INFO
Lowest Level	7	debugging	Debugging messages	LOG_DEBUG

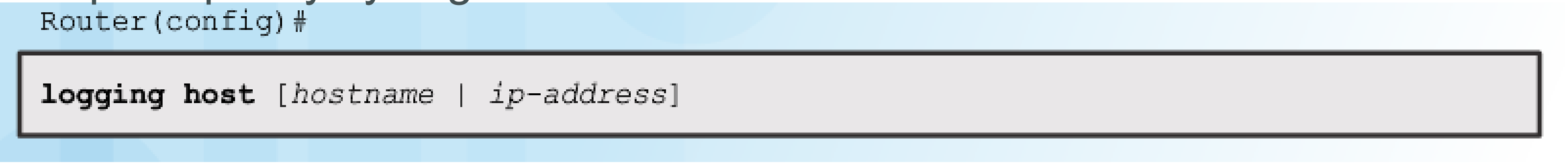
Example Severity Levels



Syslog 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, device errors	Unable to allocate memory
3 LOG_ERR	Errors	Invalid memory size
4 LOG_WARNING	Warning messages	Crypto operation failed
5 LOG_NOTICE	Non-error conditions that may require special handling	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 a program	Packet type invalid

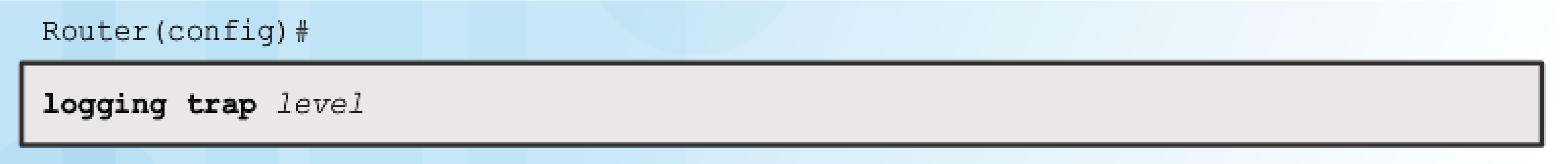
Configuring System Logging

Step 1: specify syslog server IP add/name



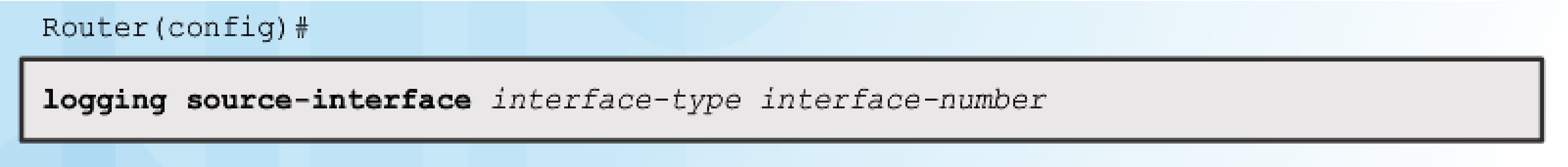
```
Router(config)#
logging host [hostname | ip-address]
```

Step 2 (optional): set severity level



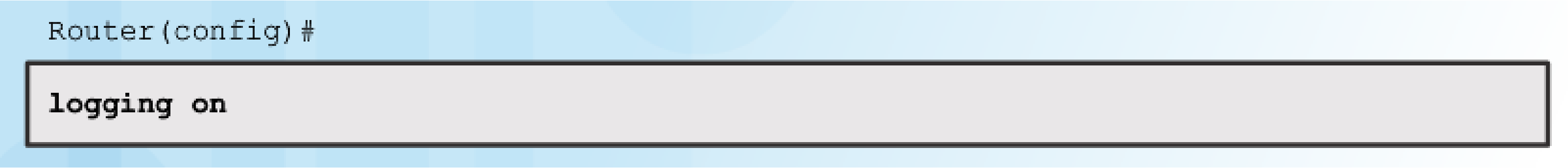
```
Router(config)#
logging trap level
```

Step 3: specify sending interface



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

Step 4



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

Time (especially correct) is important!!!!

```
! Pridaj casovu znacku pre debug spravy
Router(config)# service timestamps debug datetime msec localtime show-
timezone

! Pridaj casovu znacku pre log spravy
Router(config)# service timestamps log datetime msec localtime show-
timezone
```

debug	Indicates that the timestamp should be applied to debugging messages.
log	Indicates that the timestamp should be applied to system logging messages.
uptime	Time stamp with the time since the system was rebooted. The time stamp format for uptime is HHHH:MM:SS.
datetime	Time stamp with the date and time. The time stamp format for datetime is MMM DD HH:MM:SS.
msec	(Optional) Include milliseconds in the time stamp.
localtime	(Optional) Time stamp relative to the local time zone.
year	Include the year in the datetime format.
show-timezone	(Optional) Include the time zone name in the time stamp.

Expected correct time using NTP

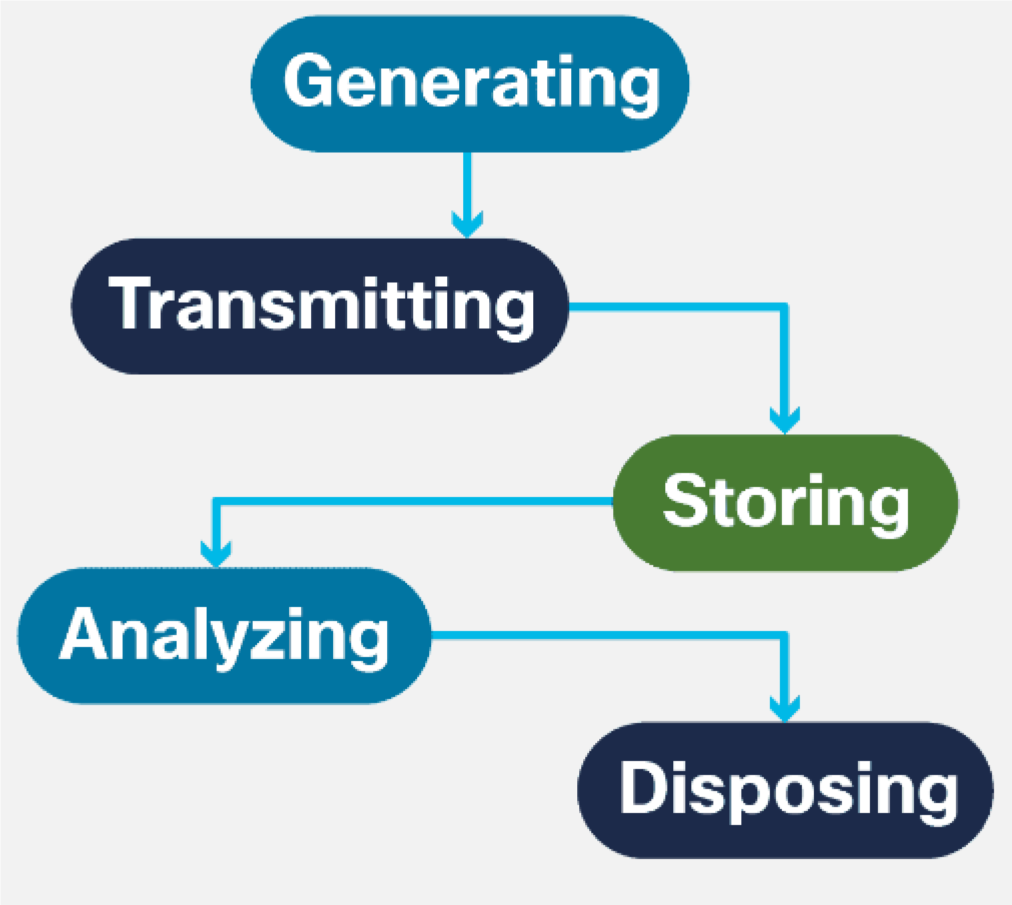
Using Syslog

- Command
  - **`show logging`**
- Use pipe (|) with a key word
  - **`include`** or **`begin`**

```
Switch# show logging | include LINK-3
2d20h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
2d20h: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
2d20h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Switch# show logging | begin %DUAL
2d22h: %DUAL-5-NBRCHANGE: EIGRP-IPv4:(10) 10: Neighbor 10.1.253.13
(FastEthernet0/11) is down: interface down
2d22h: %LINK-3-UPDOWN: Interface FastEthernet0/11, changed state to down
2d22h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to down
```

Logging – final words

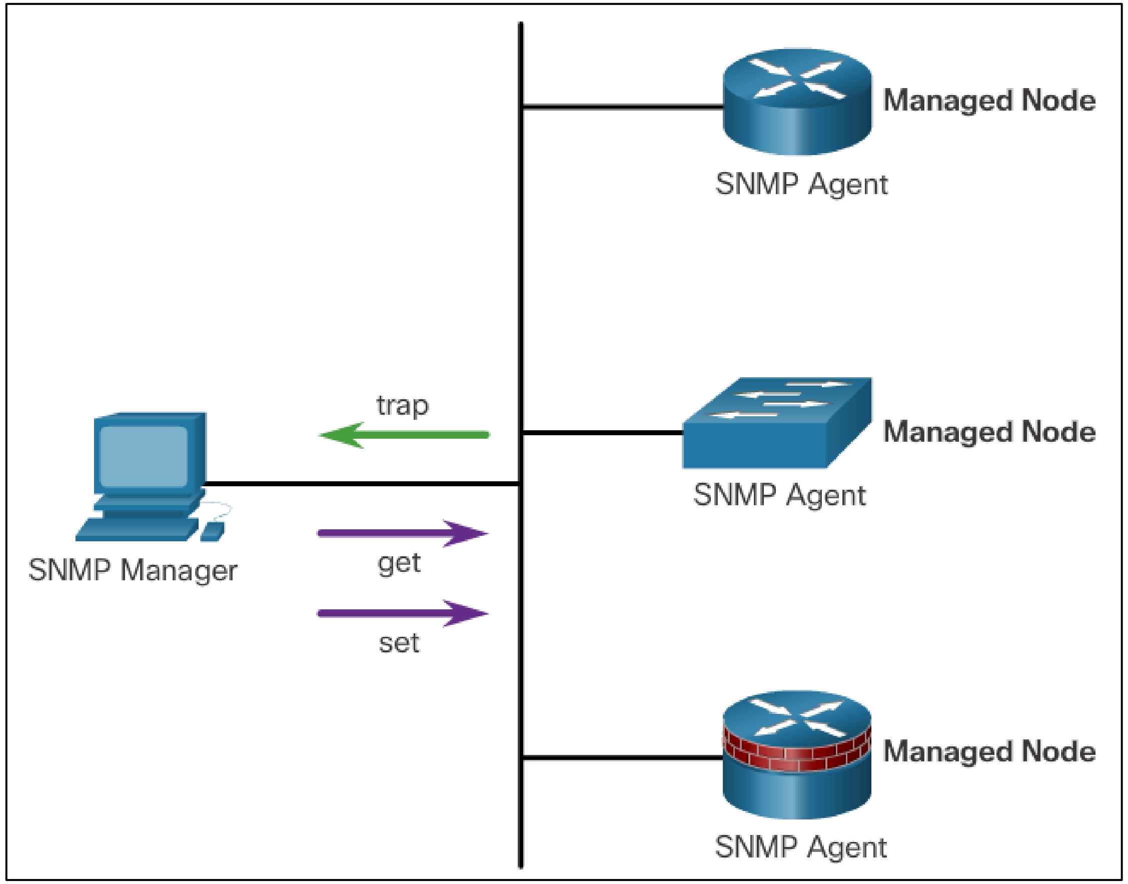
- A log => record of all events as they occur
- Accurate and complete logs => very important in cybersecurity
- A lot of log records => log management is required
  - Popular open source
    - Syslog server:
      - Syslog-ng
    - Syslog solutions:
      - Graylog (all-in-one)
      - Logstash (Elastic Stack)



Using SNMP for Network Security

Introduction to SNMP

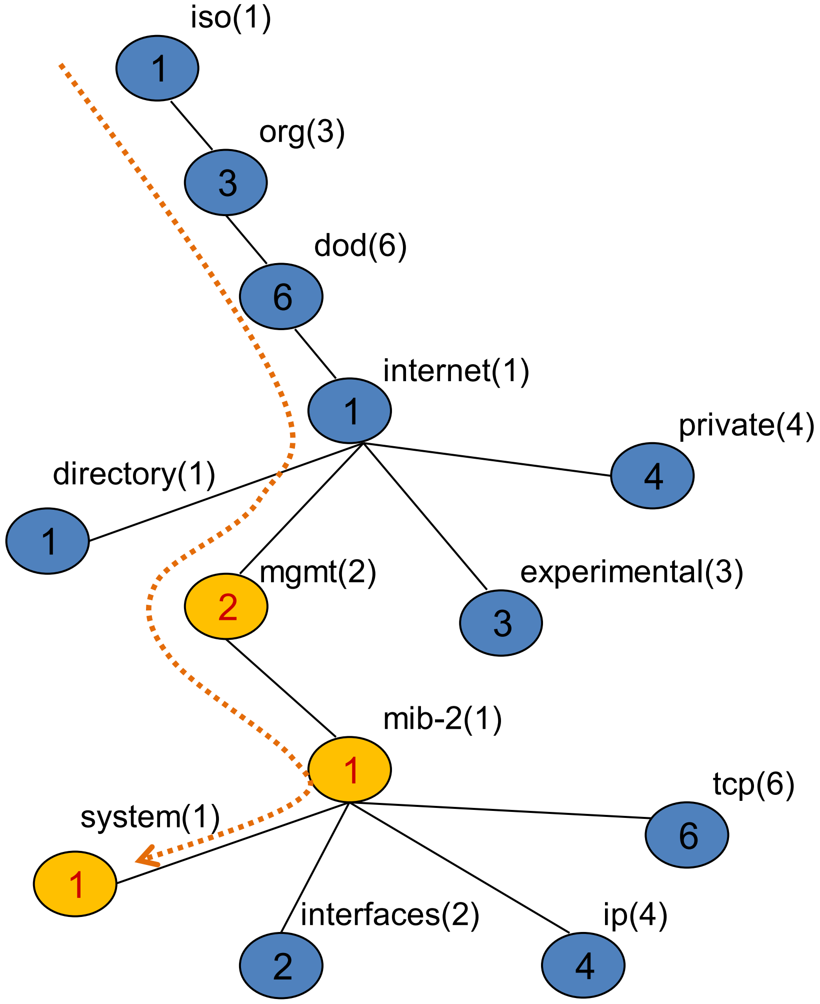
- De facto the only one standardized management protocol for IP
- Uses UDP
- Has three components
  - SNMP Manager (Network Management Application/Server)
    - Listen on UDP 162
  - SNMP Agents
    - Inside of managed device
    - Listen on UDP 161
  - MIB Database
    - DB of informational objects
- Modes of communication
  - Pull model
    - a manager asks or sets agents
  - Push model
    - Traps/notification from an agent onto a manager



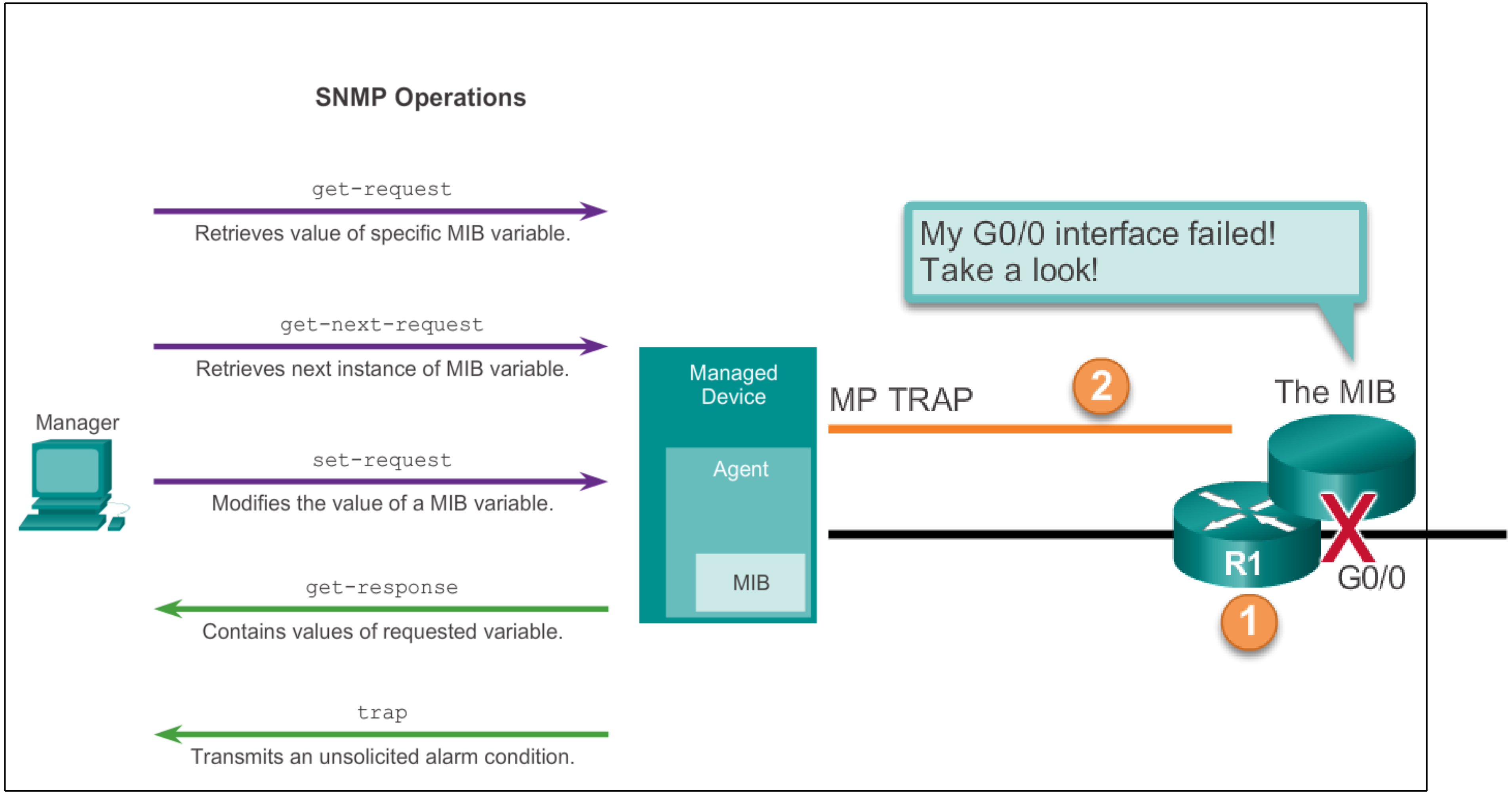
MIB – Management Information Base

- Objects store values
  - updated locally by SNMP agent
  - or remotely from manager using set messages
- Objects are identified by their OID (Object IDentifier)
  - OID forms a three structure
  - Nodes have both a numeric and a verbal name
  - Objects are addressed from the root of the tree
- Example: .1.3.6.1.2.1.1

iso(1) org(3) dod(6) internet(1)
mgmt(2)
mib-2 (1)
system (1)



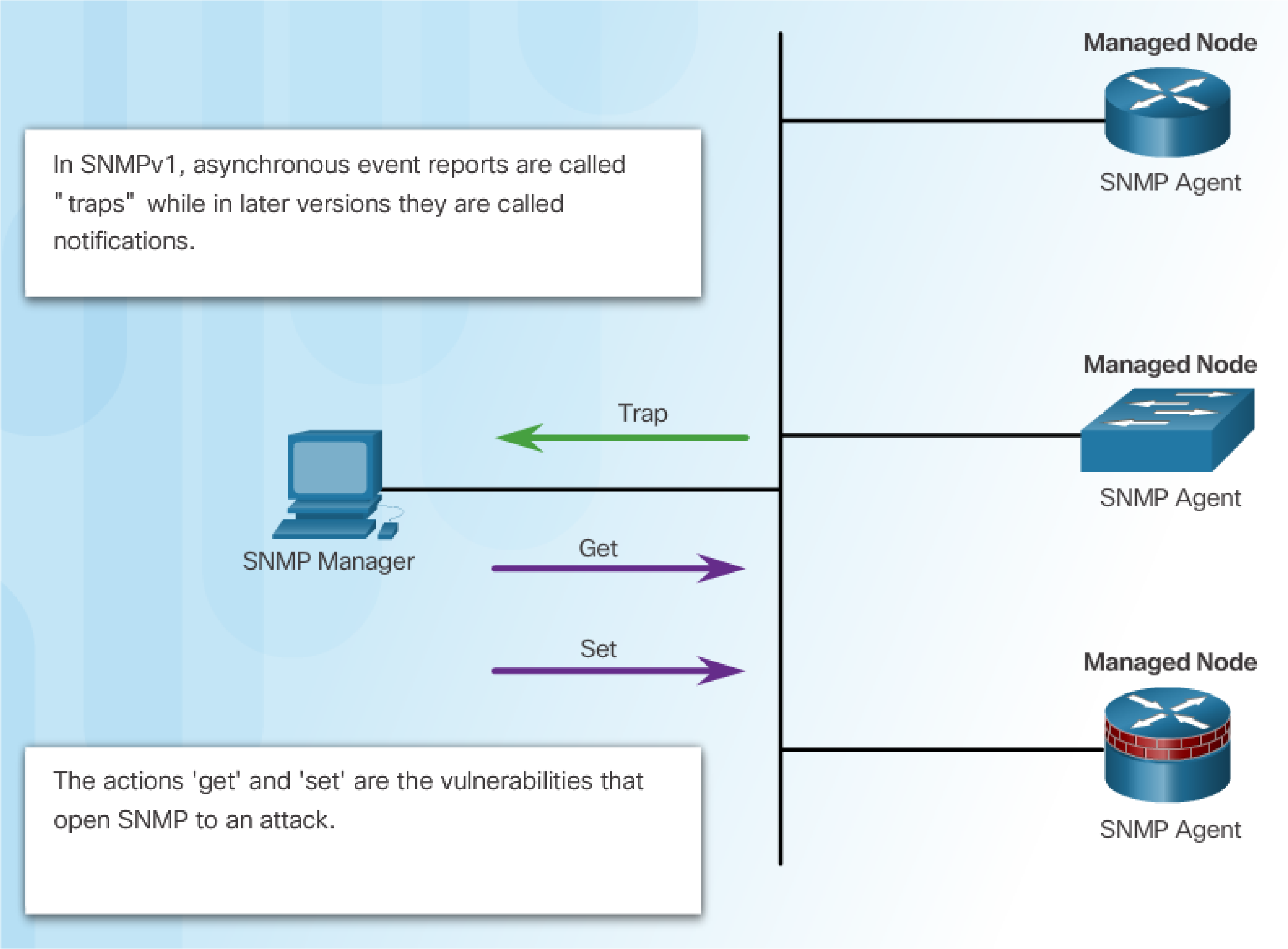
SNMP Operation


SNMP Operations
get-request
Retrieves value of specific MIB variable.
get-next-request
Retrieves next instance of MIB variable.
set-request
Modifies the value of a MIB variable.
get-response
Contains values of requested variable.
trap
Transmits an unsolicited alarm condition.
Manager
Managed Device
Agent
MIB
MP TRAP
2
My G0/0 interface failed! Take a look!
The MIB
R1
G0/0
1

Securing SNMPv1/v2/v2c - Community Strings

- There are two types of community strings:
  - **Read-only (ro)**
    - Provides access to the MIB variables, but does not allow these variables to be changed, only read.
    - Because security is so weak in version 2c, many organizations use SNMPv2c in read-only mode.
  - **Read-write (rw)**
    - Provides read and write access to all objects in the MIB.

SNMP Vulnerabilities

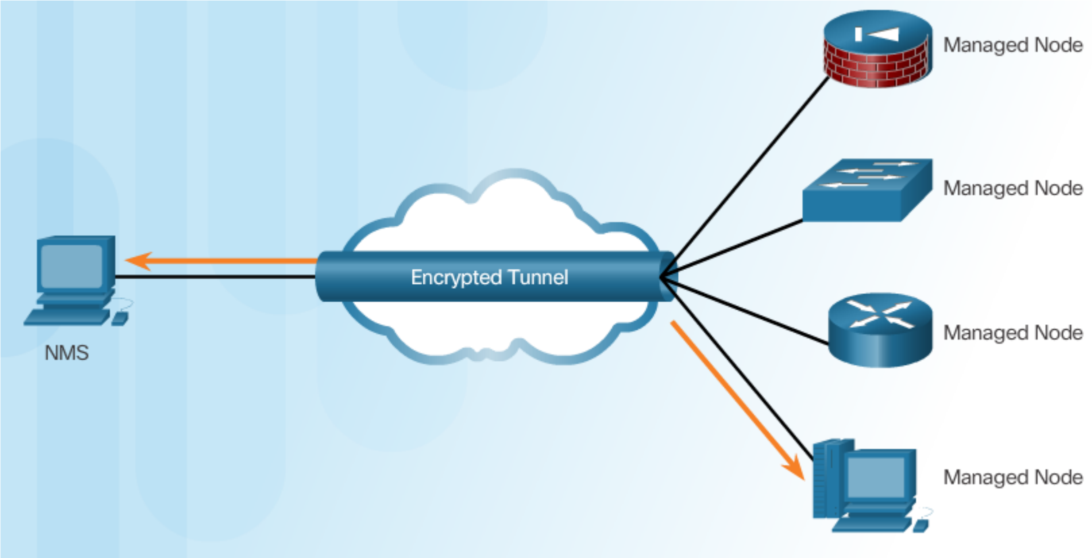


In SNMPv1, asynchronous event reports are called " traps" while in later versions they are called notifications.

The actions 'get' and 'set' are the vulnerabilities that open SNMP to an attack.

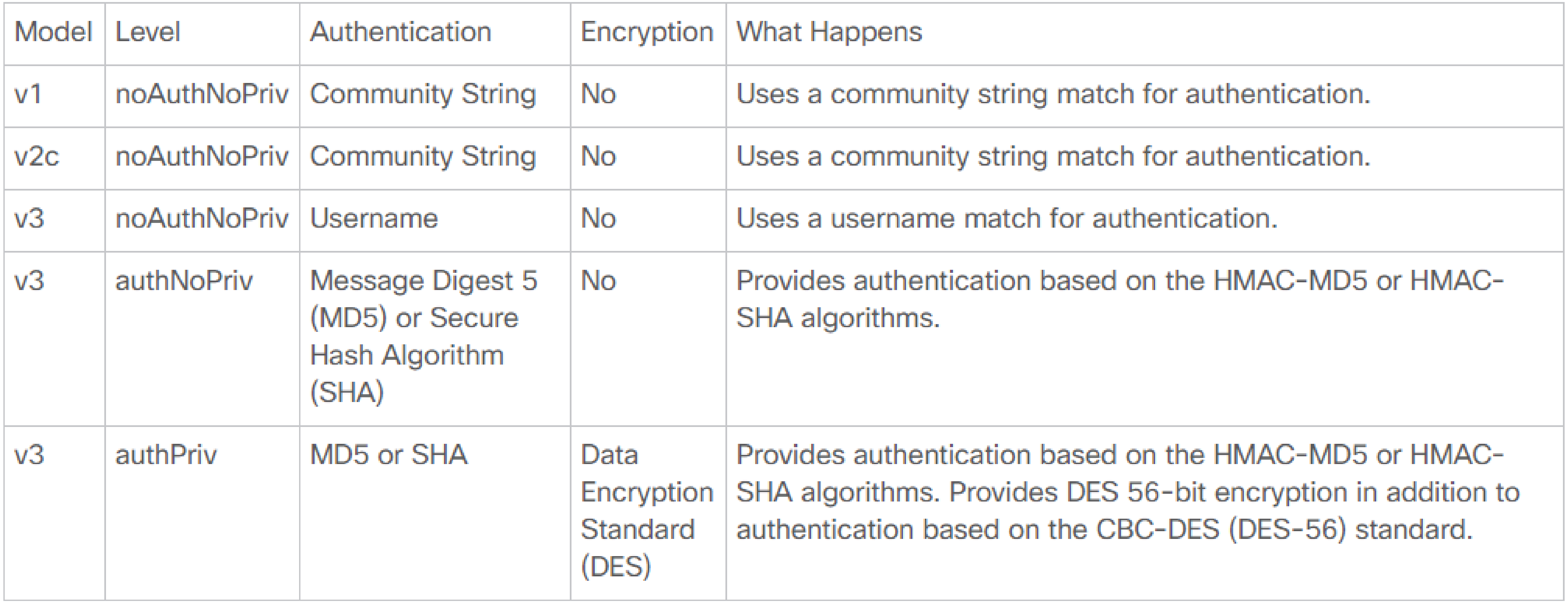
SNMPv3

- RFCs 3410 - 3415
- Adds a methodology to ensure the transmission of critical data between managed devices
  - Message integrity & authentication
  - Encryption
  - Access control
- SNMPv3 supports three levels of security
  - **noAuthNoPriv:**
    - Authentication is not required, encryption is not providedAuth
      - Uses clear-text community string Or username
  - **authNoPriv**
    - Support authentication using Hash-based Message Authentication Code with Message Digest 5 (HMAC-MD5) or Hash-based Message Authentication Code with Secure Hash Algorithm (HMAC-SHA).
    - Encryption is not provided
  - **authPriv**
    - Supports authentication and encryption using Cipher Block Chaining-Data Encryption Standard (CBC-DES)



- Transmissions from manager to agent may be authenticated to guarantee the identity of the sender and the integrity and timeliness of a message.
- SNMPv3 messages may be encrypted to ensure privacy.
- Agent may enforce access control to restrict each principal to certain actions on specific portions of data.

SNMP Versions



Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	Data Encryption Standard (DES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

Basic SNMPv2c/v3 configuration

```
! ziadne trapy
! Len Read Only pristup bez sifrovania
Router(config)# snmp-server community public
```

SNMPv3 configuration steps

- **Step 1.** Configure an ACL to limit who has SNMP access to the device.
- **Step 2.** Configure an SNMPv3 view using the **`snmp-server view`** *`view-name`* global configuration command.
- **Step 3.** Configure an SNMPv3 group using the **`snmp-server group`** *`group-name`* global configuration command.
- **Step 4.** Configure an SNMPv3 user using the **`snmp-server user`** *`username groupname`* global configuration command.
- **Step 5.** Configure an SNMPv3 trap receiver using the **`snmp-server host`** global configuration command.
- **Step 6.** Configure interface index persistence using the **`snmp-server ifindex persist`** global configuration command.

SNMP Groups (SNMPv3)

```
! ACL
R1(config)# ip access-list standard NMS-SERVERS
R1(config-std-nacl)# permit 172.16.99.0 0.0.0.255

! Views
R1(config)#snmp-server view NMS-LIMIT iso included
R1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.21 excluded
R1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.22 excluded

!SNMP groups
! Nastav snmpv3, uroven zabezpecenia priv (auth + sifrovanie) s
! Citanim a zapisom do MIBS podla views NMS-LIMIT,
! ak je pristup z IP podla ACL NMS-SERVERS
R1(config)# snmp-server group MOJA_GRUPA v3 priv read NMS-LIMIT write NMS-LIMIT access NMS-
SERVERS

! Pouzivatela student zarad do grupy, autentifikuje sa sha a heslom
! Sifruj aes 128bit a heslom
R1(config)# snmp-server user STUDENT MOJA_GRUPA v3 auth sha cisco123 priv aes 128 cisco123

! Nastav posielanie trap-ov o CPU cez SNMPv3 na IP adresu s heslom
R1(config)# snmp-server host 10.1.1.254 traps version 3 priv ADMIN cpu
R1(config)# snmp-server ifindex persist
```

Verification

```
! Zakladne info o konfiguracii snmp
R1# show snmp
Chassis: FDT11111111
2932 SNMP packets input
…
```

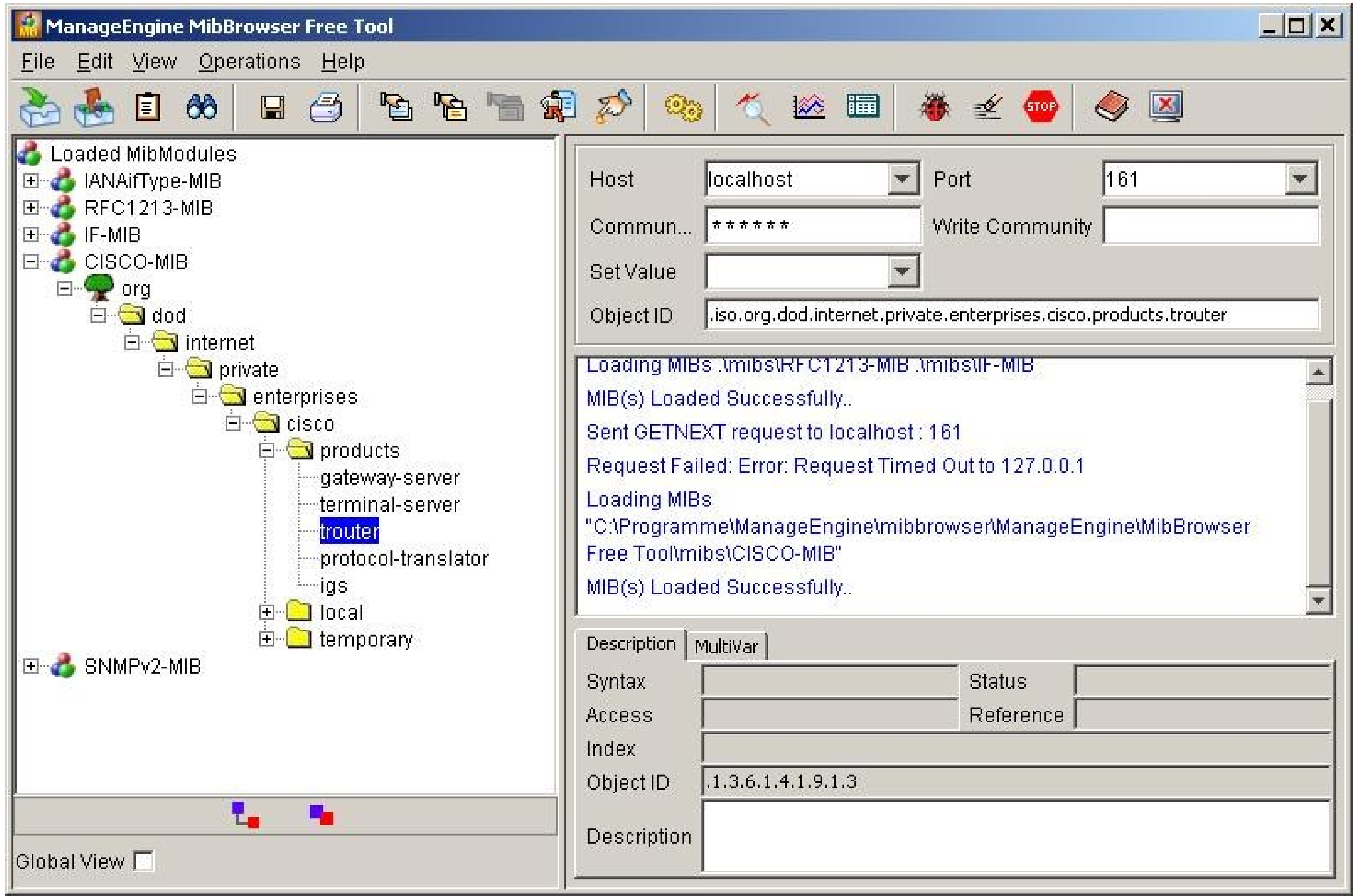
```
! Zakladne info o konfigurovanych views
R1# show snmp view
cac_view pimMIB - included read-only active
cac_view msdpMIB - included read-only active
….
```

```
! Zakladne info o konfiguracii grup
R1# show snmp group
…
Groupname: MOJA_GRUPA                         security model:v3 priv
contextname: <no context specified>           storage-type: nonvolatile
readview : NMS-LIMIT                          writeview: NMS-LIMIT
notifyview: <no notifyview specified>
row status: active      access-list: NMS-SERVERS
```

```
! Zakladne info o konfiguracii pouzivatelov
R1# show snmp user
…
User name: STUDENT
Engine ID: 800000090300CA010E240000
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: MOJA_GRUPA
```

Using GUI MIB browsers (walkers)

- Free SNMP MIB Browser Tools
  - http://www.manageengine.com/products/mibbrowser-free-tool/
- SnmpB
  - http://sourceforge.net/projects/snmpb/



Host: localhost
Port: 161
Commun...: ******
Write Community:
Set Value:
Object ID: .iso.org.dod.internet.private.enterprises.cisco.products.trouter

```
Loading MIBs .\mibs\RFC1213-MIB .\mibs\IF-MIB
MIB(s) Loaded Successfully..
Sent GETNEXT request to localhost : 161
Request Failed: Error: Request Timed Out to 127.0.0.1
Loading MIBs
"C:\Programme\ManageEngine\mibbrowser\ManageEngine\MibBrowser
Free Tool\mibs\CISCO-MIB"
MIB(s) Loaded Successfully..
```

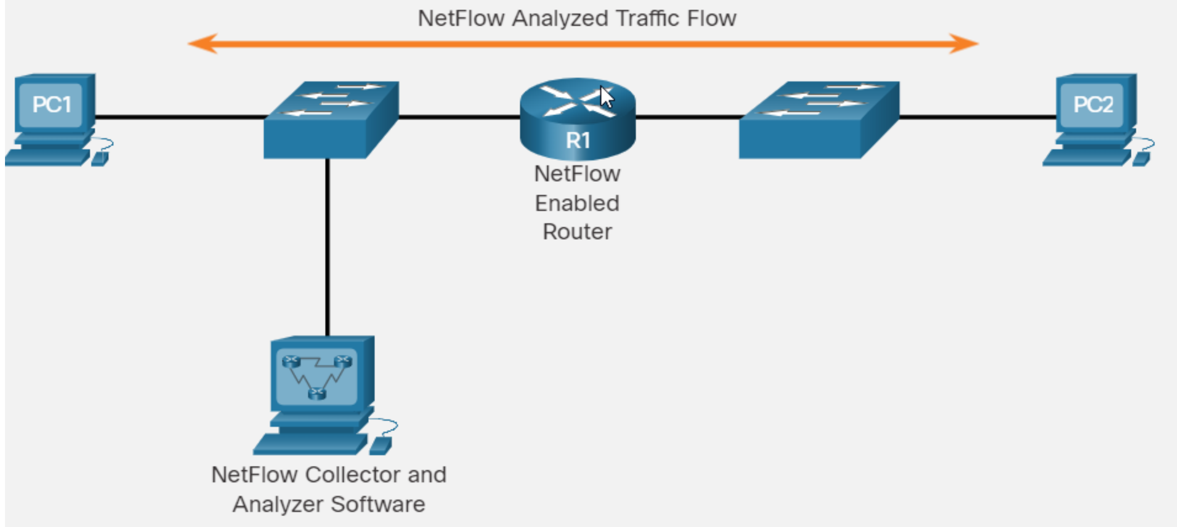
Syntax:
Status:
Access:
Reference:
Index:
Object ID: .1.3.6.1.4.1.9.1.3
Description:

Netflow / IPFlow

ToDo

Netflow / IPFlow

- Provides **statistics** on packets flowing through a network device
  - Netlow – Cisco proprietary
  - IPFIX - IETF standard, derived from NetFlow v9
  - L2-L7 info
- Flow =
  - Source IP address
  - Destination IP address
  - Source port number
  - Destination port number
  - Layer 3 protocol type
  - Type of Service (ToS) marking
  - Input logical interface



- Why?
  - BW monitoring, performance issue, threat/anomaly detection, prediction ….

Netflow

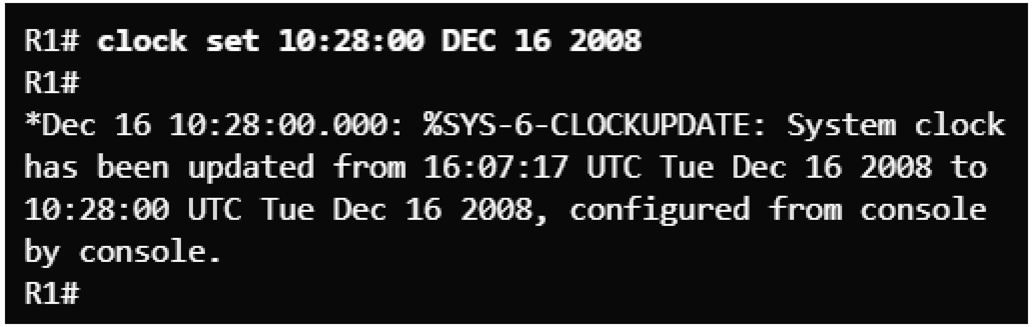
- Several protocol versions
  - Latest: NetFlow v9

- Entities
  - Netflow Cache
    - Keeps flow statistics
    - Needed to be exported otherwise rewritten
  - Netflow Exporter
  - Netflow Collector
    - Collects netflow exports
    - Example: Ntop-ng
  - Analysis application

Using network time – NTP protocol

Time

- Correct time is very important as many things depend on it
  - Logs, digital certificates validity, key-chains validity
- Time can be set:
  - Manually edit the date and time locally
    - Cmd **clock**

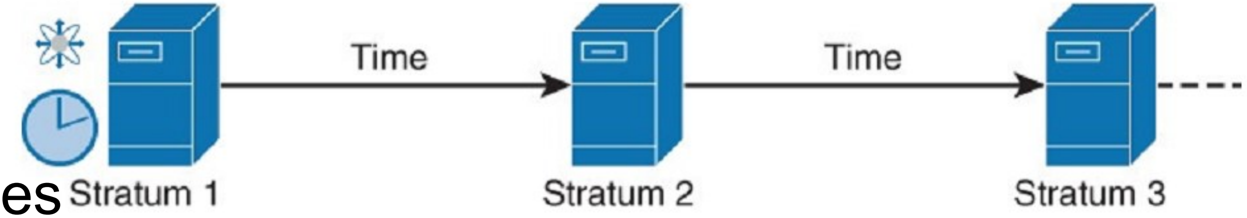


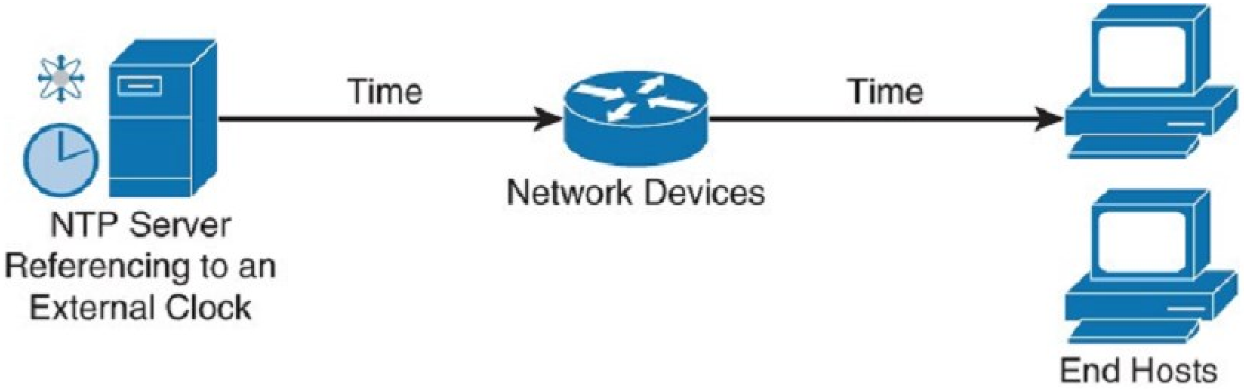
```
R1# clock set 10:28:00 DEC 16 2008
R1#
*Dec 16 10:28:00.000: %SYS-6-CLOCKUPDATE: System clock
has been updated from 16:07:17 UTC Tue Dec 16 2008 to
10:28:00 UTC Tue Dec 16 2008, configured from console
by console.
R1#
```

  - Configure the Network Time Protocol (NTP)
    - Better solution

NTP

- is an open protocol specified in RFC 5905 for network node time synchronization
  - Uses UDP/123
  - Built hierarchical system of time sources
  - Stratum 0 – Authoritative time source
  - Stratum number indicates how far the server is from the time source
    - Max. 15, 16 = unsynchronized
- Client/server architecture
  - Server
    - Private or public
  - Client
  - Peer
- Popular for amplified DDoS attacks



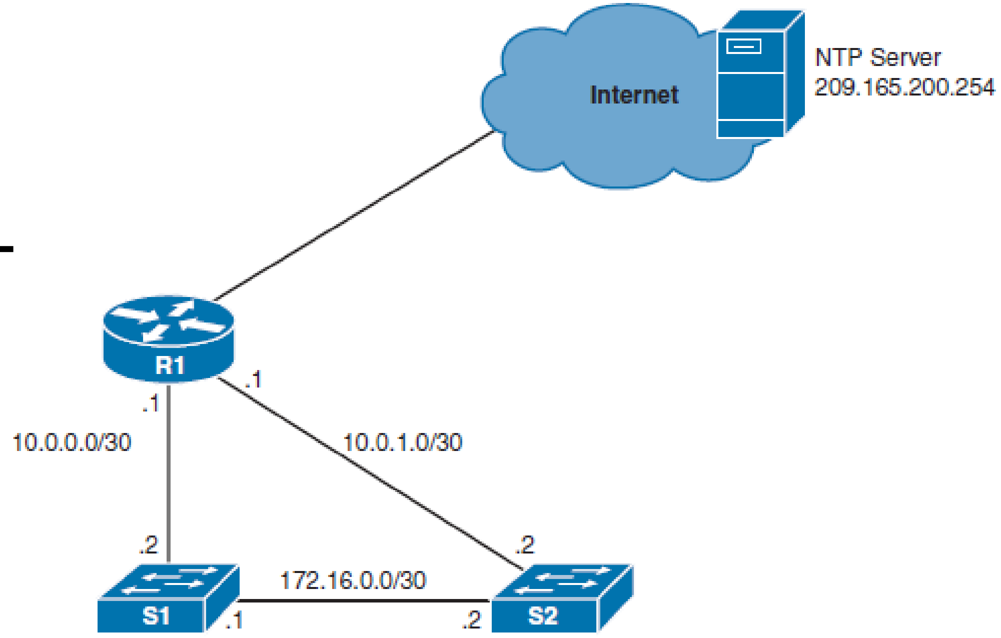


NTP config and verification example

```
! Set NTP servers, first one as preferred
ntp server 158.193.48.7 prefer
ntp server 158.193.152.2
!
! Setup timestamps for log and debug messages
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
! Setup time zone and summr/winter time
clock timezone CET 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
```

```
Router# show ntp status
Clock is synchronized, stratum 12, reference is 158.193.48.7
nominal freq is 119.2092 Hz, actual freq is 119.2078 Hz, precision is 2**18
reference time is D2054E5B.686C9787 (01:31:39.407 CEST Mon Aug 29 2011)
clock offset is -0.0317 msec, root delay is 2.15 msec
root dispersion is 12.08 msec, peer dispersion is 0.23 msec

Router# show ntp associations
      address         ref clock     st  when  poll reach  delay  offset    disp
*~158.193.48.7     127.127.1.0      11    37   512  377     2.2   -0.03     0.2
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

NTP Authentication (NTPv3)



```
! R1 – NTP server
ntp master 8
! heslo
ntp authentication-key 1 md5 HESLISKO
! Ze sa ma zdroj autentifikovat
ntp authenticate
! Ktory kluc pouzit
ntp trusted-key 1
!
Access-list 10 permit 10.0.0.0 0.0.255.255
ntp access-group serve-only 10
```

```
! S1 – NTP klient
ntp authentication-key 1 md5 HESLISKO
ntp authenticate
ntp trusted-key 1
ntp server 10.0.0.1 key 1
! ntp source INT
```

Note: authentication is used to verify time source, so client without authe still receive clock, but is not trustworthy

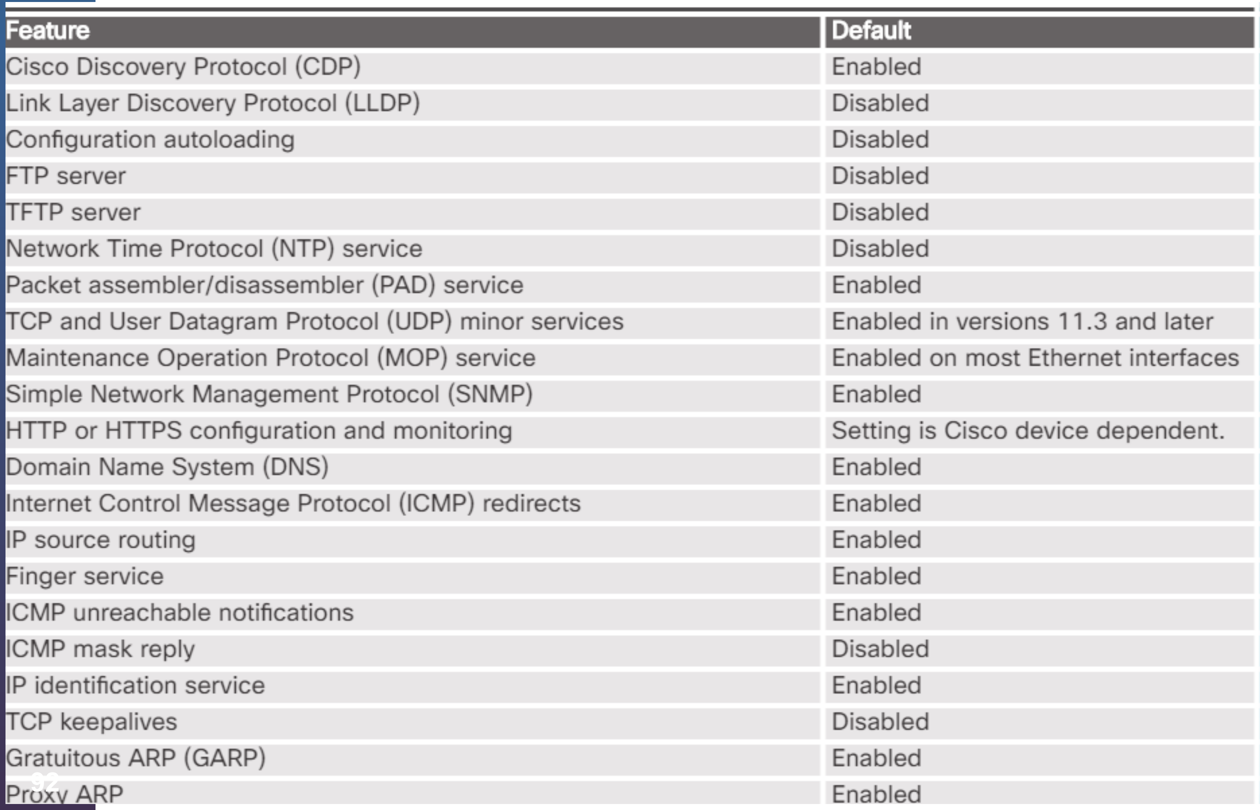
Using Automated Security Features

Upon completion of this section, you should be able to:

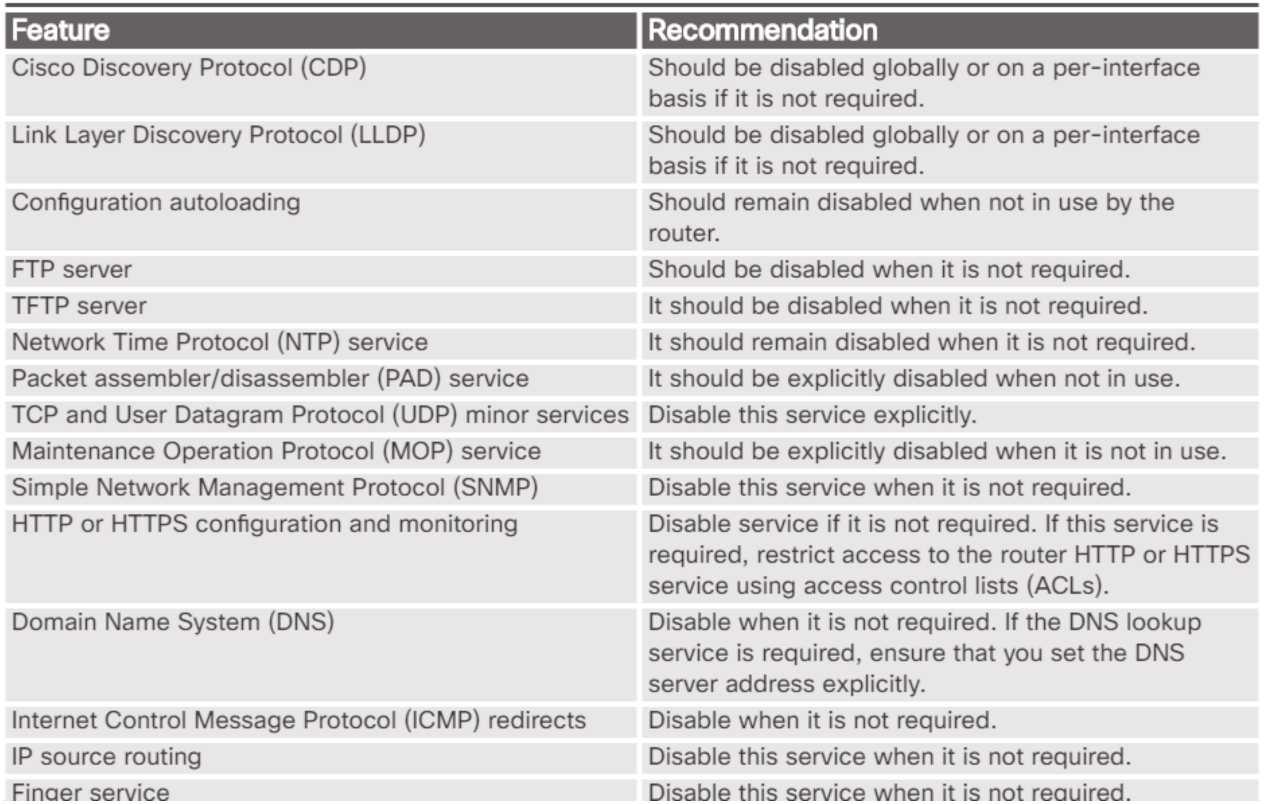
- Use security audit tools to determine IOS-based router vulnerabilities.
- Use AutoSecure to enable security on IOS-based routers.

Settings for Protocols and Services

- Cisco routers comes with many protocols and services enabled by default
  - For example CDP/LLDP on all interfaces
    - Can be used for gathering net info or overflow attacks
  - Many of these features that are unused should be disabled or restricted in their capabilities



Feature	Default
Cisco Discovery Protocol (CDP)	Enabled
Link Layer Discovery Protocol (LLDP)	Disabled
Configuration autoloading	Disabled
FTP server	Disabled
TFTP server	Disabled
Network Time Protocol (NTP) service	Disabled
Packet assembler/disassembler (PAD) service	Enabled
TCP and User Datagram Protocol (UDP) minor services	Enabled in versions 11.3 and later
Maintenance Operation Protocol (MOP) service	Enabled on most Ethernet interfaces
Simple Network Management Protocol (SNMP)	Enabled
HTTP or HTTPS configuration and monitoring	Setting is Cisco device dependent.
Domain Name System (DNS)	Enabled
Internet Control Message Protocol (ICMP) redirects	Enabled
IP source routing	Enabled
Finger service	Enabled
ICMP unreachable notifications	Enabled
ICMP mask reply	Disabled
IP identification service	Enabled
TCP keepalives	Disabled
Gratuitous ARP (GARP)	Enabled
Proxy ARP	Enabled



Feature	Recommendation
Cisco Discovery Protocol (CDP)	Should be disabled globally or on a per-interface basis if it is not required.
Link Layer Discovery Protocol (LLDP)	Should be disabled globally or on a per-interface basis if it is not required.
Configuration autoloading	Should remain disabled when not in use by the router.
FTP server	Should be disabled when it is not required.
TFTP server	It should be disabled when it is not required.
Network Time Protocol (NTP) service	It should remain disabled when it is not required.
Packet assembler/disassembler (PAD) service	It should be explicitly disabled when not in use.
TCP and User Datagram Protocol (UDP) minor services	Disable this service explicitly.
Maintenance Operation Protocol (MOP) service	It should be explicitly disabled when it is not in use.
Simple Network Management Protocol (SNMP)	Disable this service when it is not required.
HTTP or HTTPS configuration and monitoring	Disable service if it is not required. If this service is required, restrict access to the router HTTP or HTTPS service using access control lists (ACLs).
Domain Name System (DNS)	Disable when it is not required. If the DNS lookup service is required, ensure that you set the DNS server address explicitly.
Internet Control Message Protocol (ICMP) redirects	Disable when it is not required.
IP source routing	Disable this service when it is not required.
Finger service	Disable this service when it is not required.

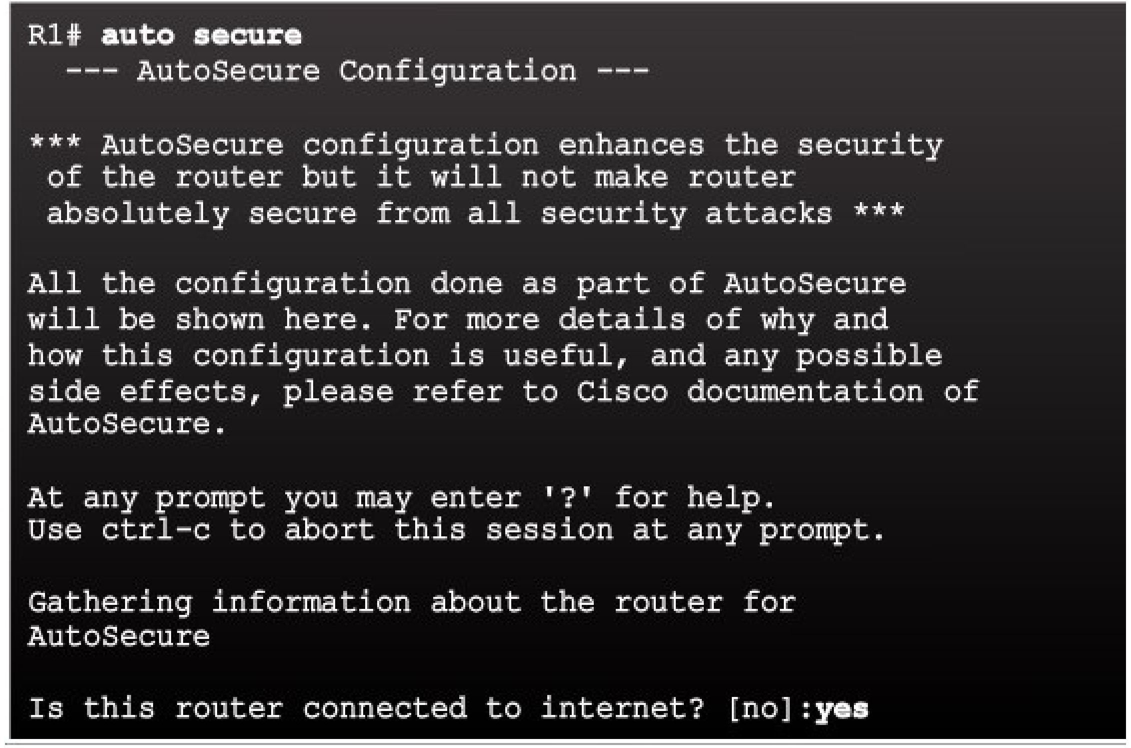
Settings for Protocols and Services

- Therefore, additional recommended practices to ensure a device is secure:
  - Disable unnecessary services and interfaces.
  - Disable and restrict commonly configured management services.
  - Disable probes and scans.
  - Ensure terminal access security.
  - Disable gratuitous and proxy ARPs
  - Disable IP-directed broadcasts.
- This could be realized
  - Manually
  - Using ***AutoSecure*** IOS command (feature)

AutoSecure

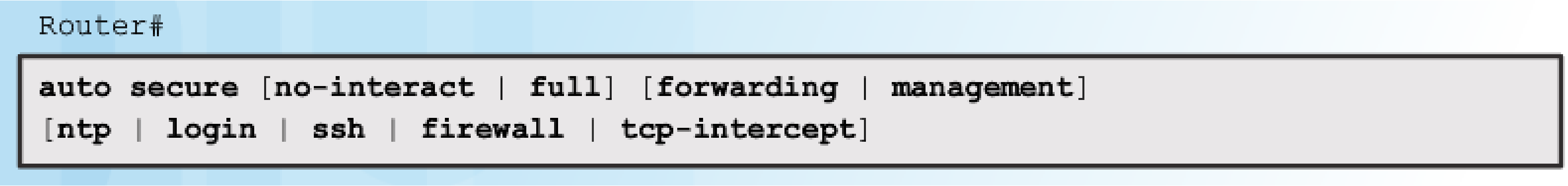
- Feature that can lock down or enable some management and forwarding functions
  - Management functions
    - Secure BOOTP, CDP, FTP, TFTP, PAD, UDP, and TCP small servers, MOP, ICMP (redirects, mask-replies), IP source routing, Finger, password encryption, TCP keepalives, gratuitous ARP, proxy ARP, and directed broadcast
    - Legal notification using a banner
    - Secure password and login functions
    - Secure NTP and others
    - …
  - Enabled Forwarding functions
    - Cisco Express Forwarding (CEF), Traffic filtering with ACLs, Cisco IOS firewall inspection for common protocols

- One started, it executes a script
  - Some steps are interactive, some not
- Useful to establish the baseline security setting of a new router

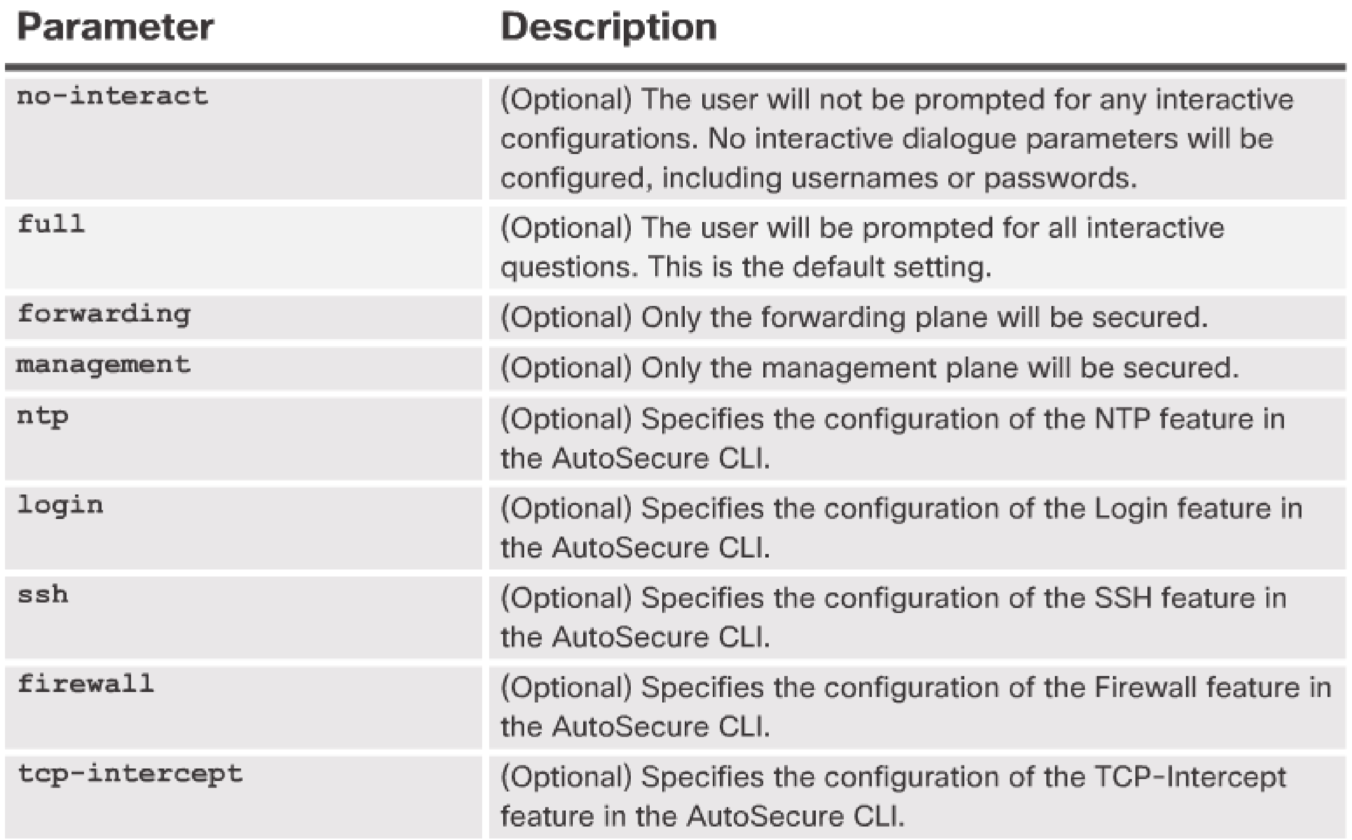


```
R1# auto secure
  --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security
 of the router but it will not make router
 absolutely secure from all security attacks ***

All the configuration done as part of AutoSecure
will be shown here. For more details of why and
how this configuration is useful, and any possible
side effects, please refer to Cisco documentation of
AutoSecure.

At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for
AutoSecure

Is this router connected to internet? [no]:yes
```

Using the Cisco AutoSecure Feature



```
Router#
auto secure [no-interact | full] [forwarding | management]
[ntp | login | ssh | firewall | tcp-intercept]
```



Parameter	Description
`no-interact`	(Optional) The user will not be prompted for any interactive configurations. No interactive dialogue parameters will be configured, including usernames or passwords.
`full`	(Optional) The user will be prompted for all interactive questions. This is the default setting.
`forwarding`	(Optional) Only the forwarding plane will be secured.
`management`	(Optional) Only the management plane will be secured.
`ntp`	(Optional) Specifies the configuration of the NTP feature in the AutoSecure CLI.
`login`	(Optional) Specifies the configuration of the Login feature in the AutoSecure CLI.
`ssh`	(Optional) Specifies the configuration of the SSH feature in the AutoSecure CLI.
`firewall`	(Optional) Specifies the configuration of the Firewall feature in the AutoSecure CLI.
`tcp-intercept`	(Optional) Specifies the configuration of the TCP-Intercept feature in the AutoSecure CLI.

Using the auto secure command

1. The auto secure command is entered
2. Wizard gathers information about the outside interfaces
3. AutoSecure secures the management plane by disabling unnecessary services
4. AutoSecure prompts for a banner
5. AutoSecure prompts for passwords and enables password and login features
6. Interfaces are secured
7. Forwarding plane is secured

Securing the Control Plane

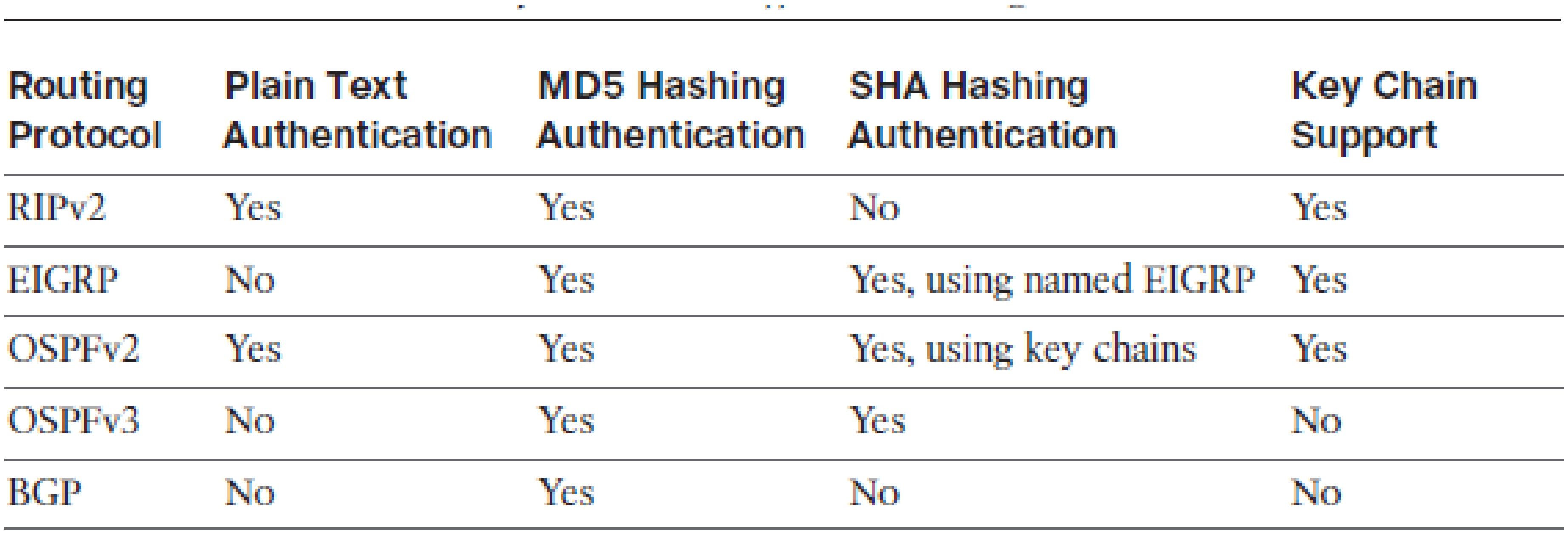
Upon completion of this section, you should be able to:

- Configure a routing protocol authentication.
- Explain the function of Control Plane Policing.

Routing Protocol Authentication

- One of attacks on routing protocols is the falsification of routing information
  - The attack focuses on the information transmitted in routing updates
- The aim / consequence of falsification of routing information is
  - Redirecting traffic into a routing loop (DoS)
  - Redirecting traffic for listening/monitoring
  - Redirecting traffic to drop packets
- Solution => Authentication of Neighbors or Updates
- There are two types of authentication
  - Plain-text authentication
  - Hashing Authentication (Pre-Shared Key - PSK)
- Note: packets are not encrypted !!!

Authentication and Routing protocols

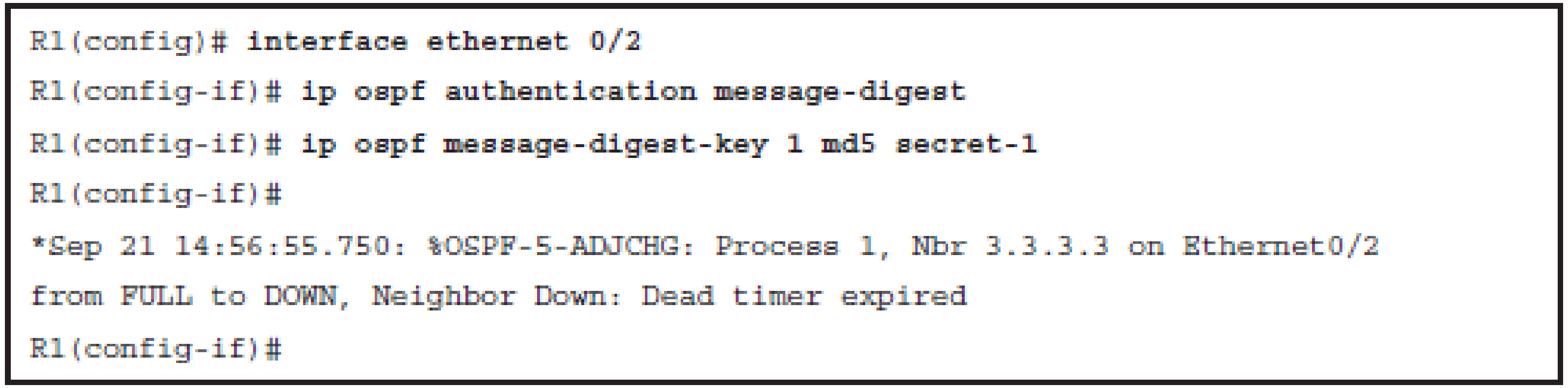


Routing Protocol	Plain Text Authentication	MD5 Hashing Authentication	SHA Hashing Authentication	Key Chain Support
RIPv2	Yes	Yes	No	Yes
EIGRP	No	Yes	Yes, using named EIGRP	Yes
OSPFv2	Yes	Yes	Yes, using key chains	Yes
OSPFv3	No	Yes	Yes	No
BGP	No	Yes	No	No

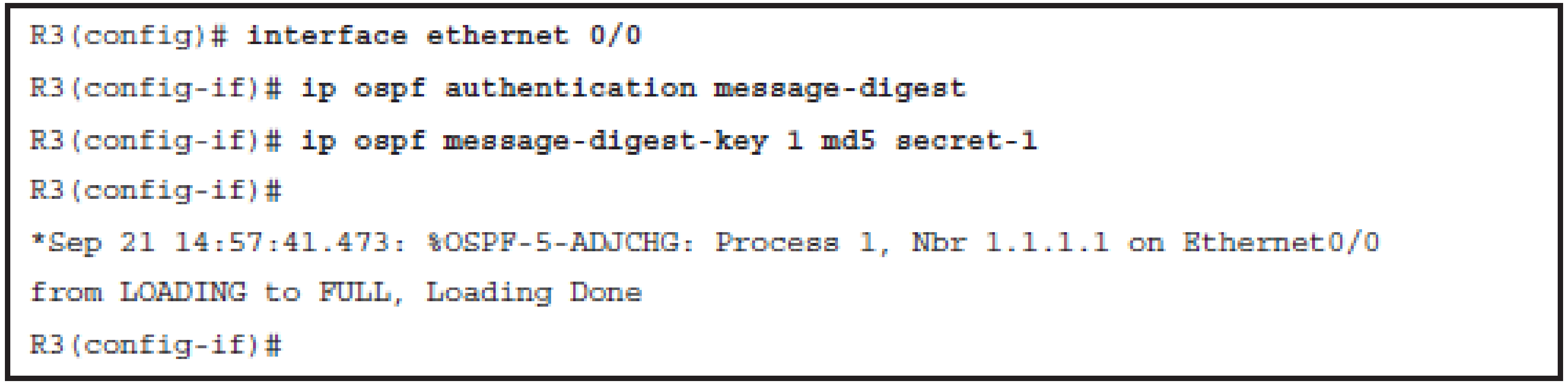
Autentifikácia v OSPF

- V default stave OSPF nepoužíva autentifikáciu
- OSPFv2 podporuje
  - **Null autentifikáciu (RFC 1583)**
  - **Plain-text autentifikáciu (RFC 1583)**
    - Nazývaná aj ako **simple password** autentifikácia
    - Najmenej bezpečná, jednoduchá autentifikácia heslom
    - Neodporúča sa pre produkčné prostredie
  - **MD5 autentifikáciu (RFC 2328)**
    - Jednoduchá a zabezpečená autentifikácia
    - Odporúča sa používať ak nie je dostupná SHA autentifikácia.
  - **HMAC-SHA autentifikáciu (RFC 7474)**
    - Nazývaná aj ako **kryptografická autentifikácia**
    - Dostupná v IOS 15.4(1)T.
    - Momentálne najlepšia forma zabezpečenia, používa key chains

OSPFv2 MD5 authentication - interface

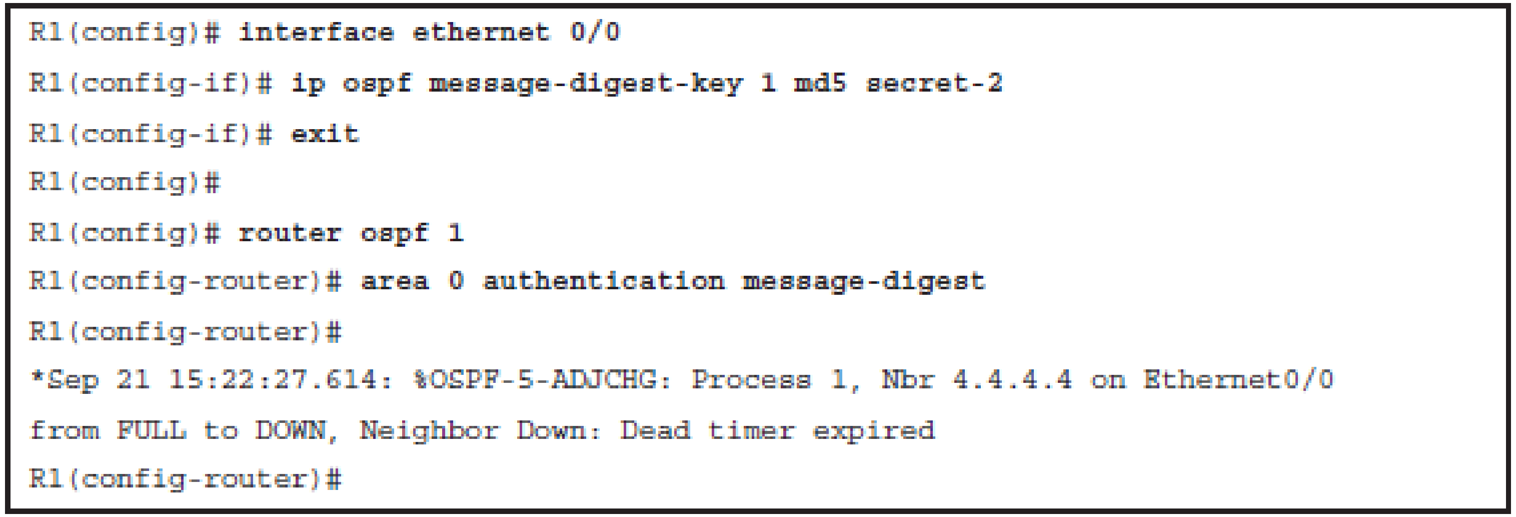


```
R1(config)# interface ethernet 0/2
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# ip ospf message-digest-key 1 md5 secret-1
R1(config-if)#
*Sep 21 14:56:55.750: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Ethernet0/2
from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
```

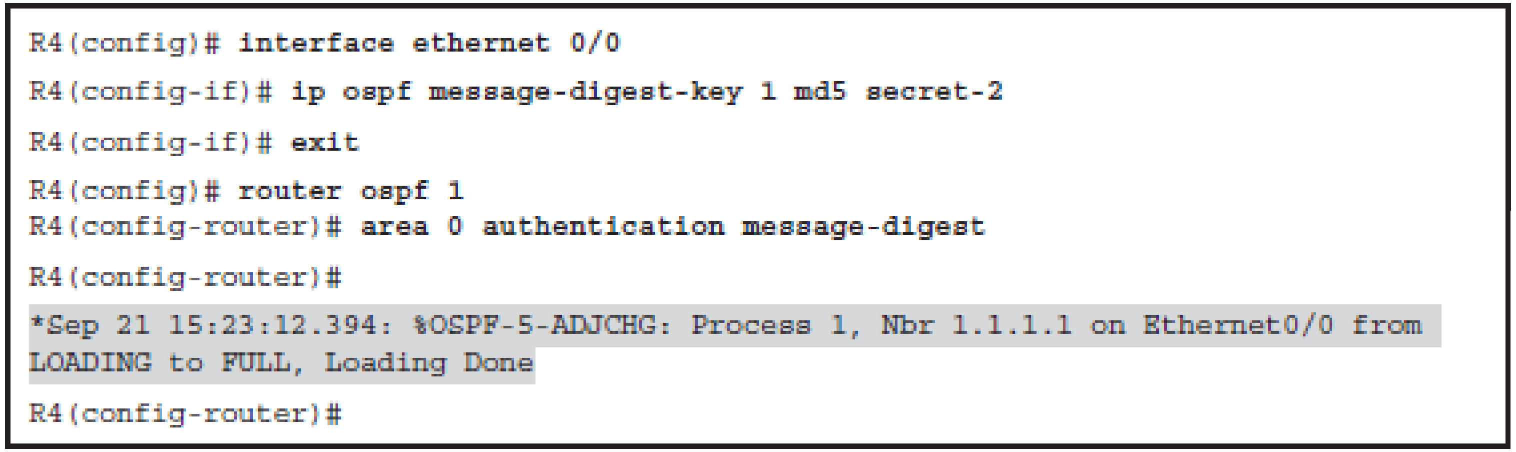


```
R3(config)# interface ethernet 0/0
R3(config-if)# ip ospf authentication message-digest
R3(config-if)# ip ospf message-digest-key 1 md5 secret-1
R3(config-if)#
*Sep 21 14:57:41.473: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Ethernet0/0
from LOADING to FULL, Loading Done
R3(config-if)#
```

OSPFv2 MD5 authentication - Area



```
R1(config)# interface ethernet 0/0
R1(config-if)# ip ospf message-digest-key 1 md5 secret-2
R1(config-if)# exit
R1(config)#
R1(config)# router ospf 1
R1(config-router)# area 0 authentication message-digest
R1(config-router)#
*Sep 21 15:22:27.614: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Ethernet0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-router)#
```



```
R4(config)# interface ethernet 0/0
R4(config-if)# ip ospf message-digest-key 1 md5 secret-2
R4(config-if)# exit
R4(config)# router ospf 1
R4(config-router)# area 0 authentication message-digest
R4(config-router)#
*Sep 21 15:23:12.394: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Ethernet0/0 from
LOADING to FULL, Loading Done
R4(config-router)#
```

```
!verification
show ip ospf interface interface_identifier
```

OSPFv2 – cryptographic authentication

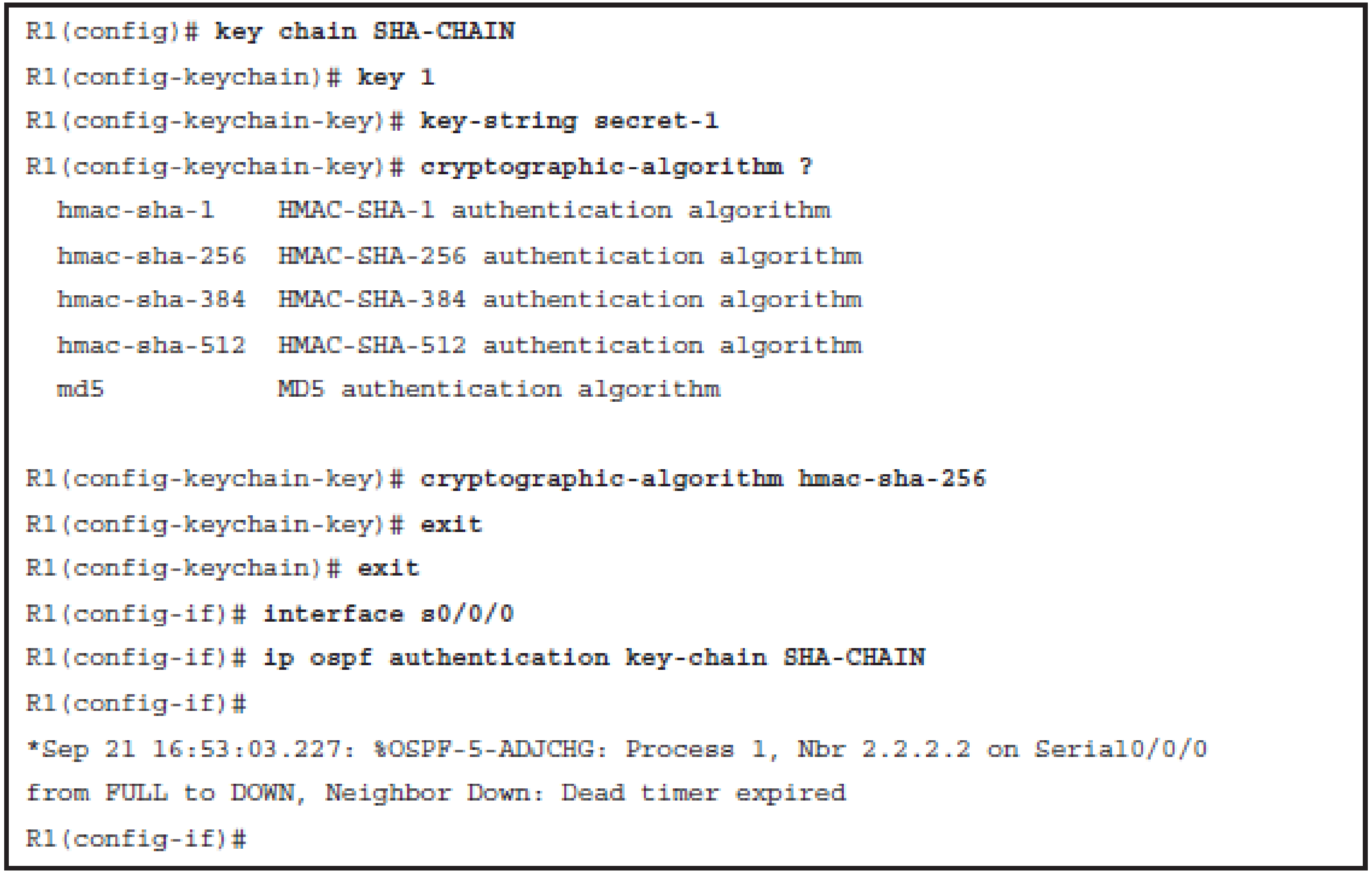
- **Step 1 -** Create a key-chain

```
key-chain  KEY-NAME
       key KEY-ID
             key-string HESLO
             cryptographic-algorithm ALGORITMUS
             ! Mozne pridat send/accept lifetime
```

- **Step 2.**
  - Bound the keychain with an interface

```
ip ospf authentication key-chain KEY-NAME
```

OSPFv2 cryptographic authentication - example

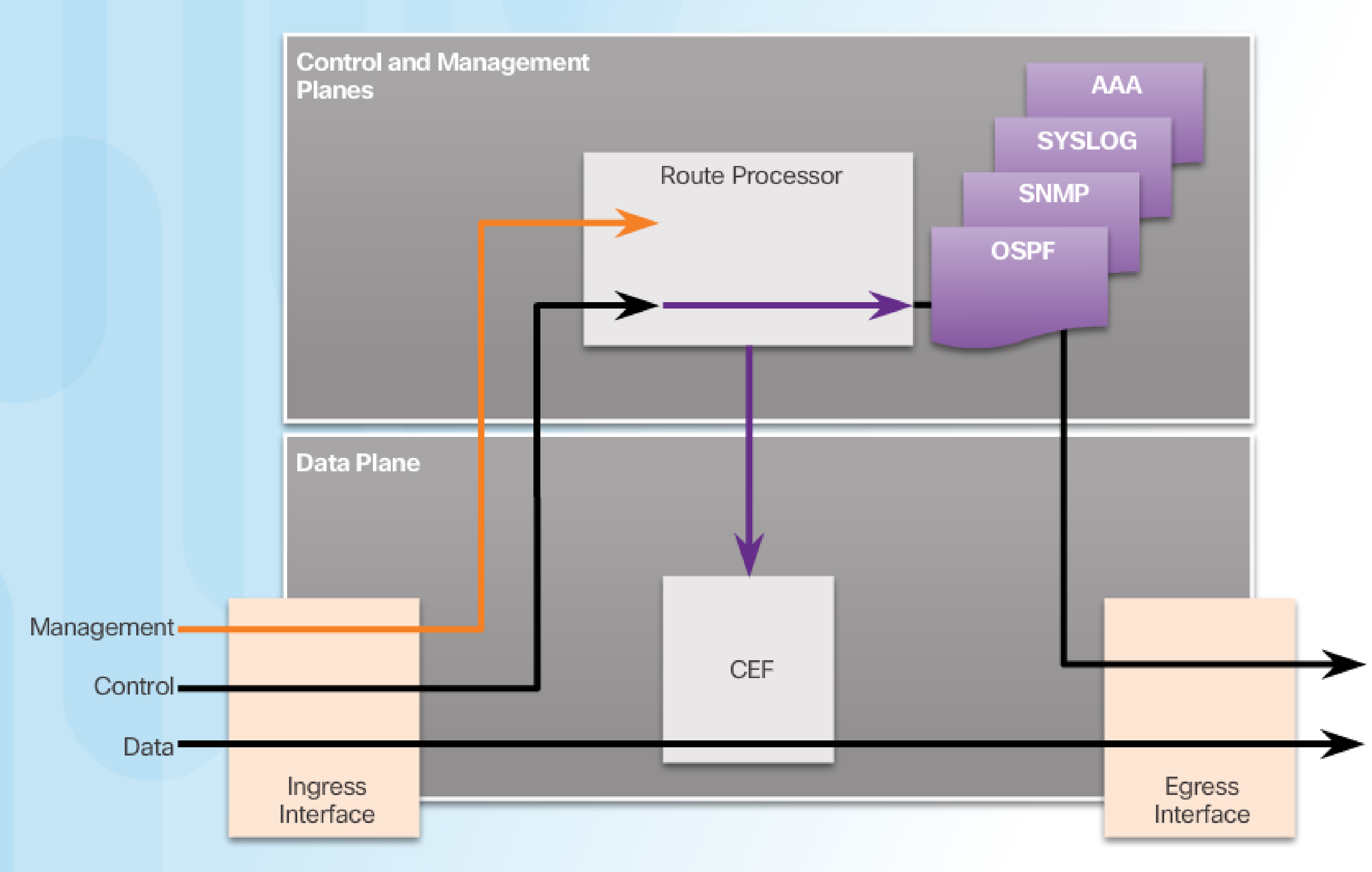


```
R1(config)# key chain SHA-CHAIN
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string secret-1
R1(config-keychain-key)# cryptographic-algorithm ?
  hmac-sha-1    HMAC-SHA-1 authentication algorithm
  hmac-sha-256  HMAC-SHA-256 authentication algorithm
  hmac-sha-384  HMAC-SHA-384 authentication algorithm
  hmac-sha-512  HMAC-SHA-512 authentication algorithm
  md5           MD5 authentication algorithm

R1(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config-if)# interface s0/0/0
R1(config-if)# ip ospf authentication key-chain SHA-CHAIN
R1(config-if)#
*Sep 21 16:53:03.227: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
```

Control Plane Policing - CoPP

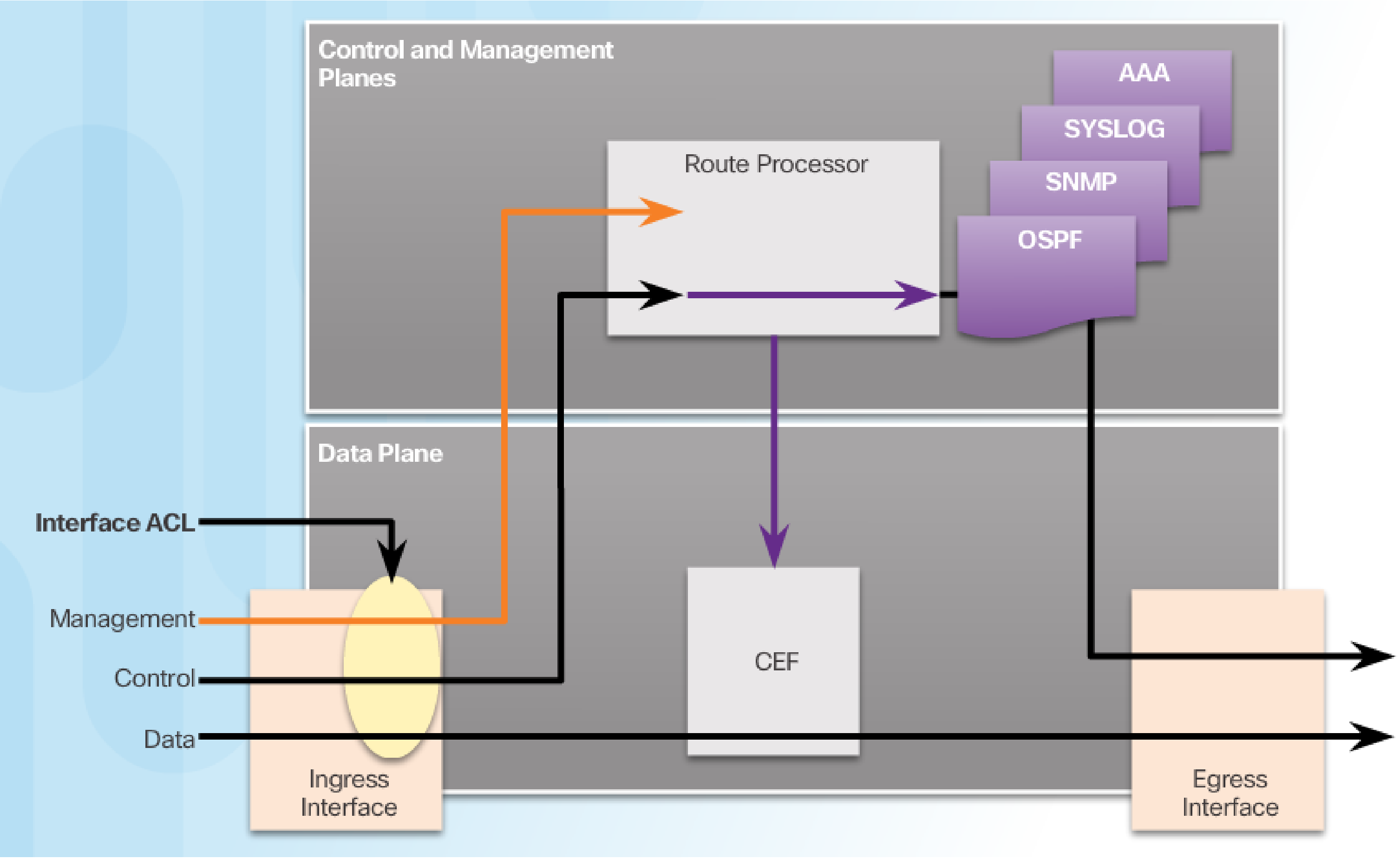
Network Device Operations

- Router architecture can be divided into three rows:
  - Management plane
    - Management
  - Control plane
    - Routing control and protocol functions
  - Data/forwarding plane
    - Packet forwarding



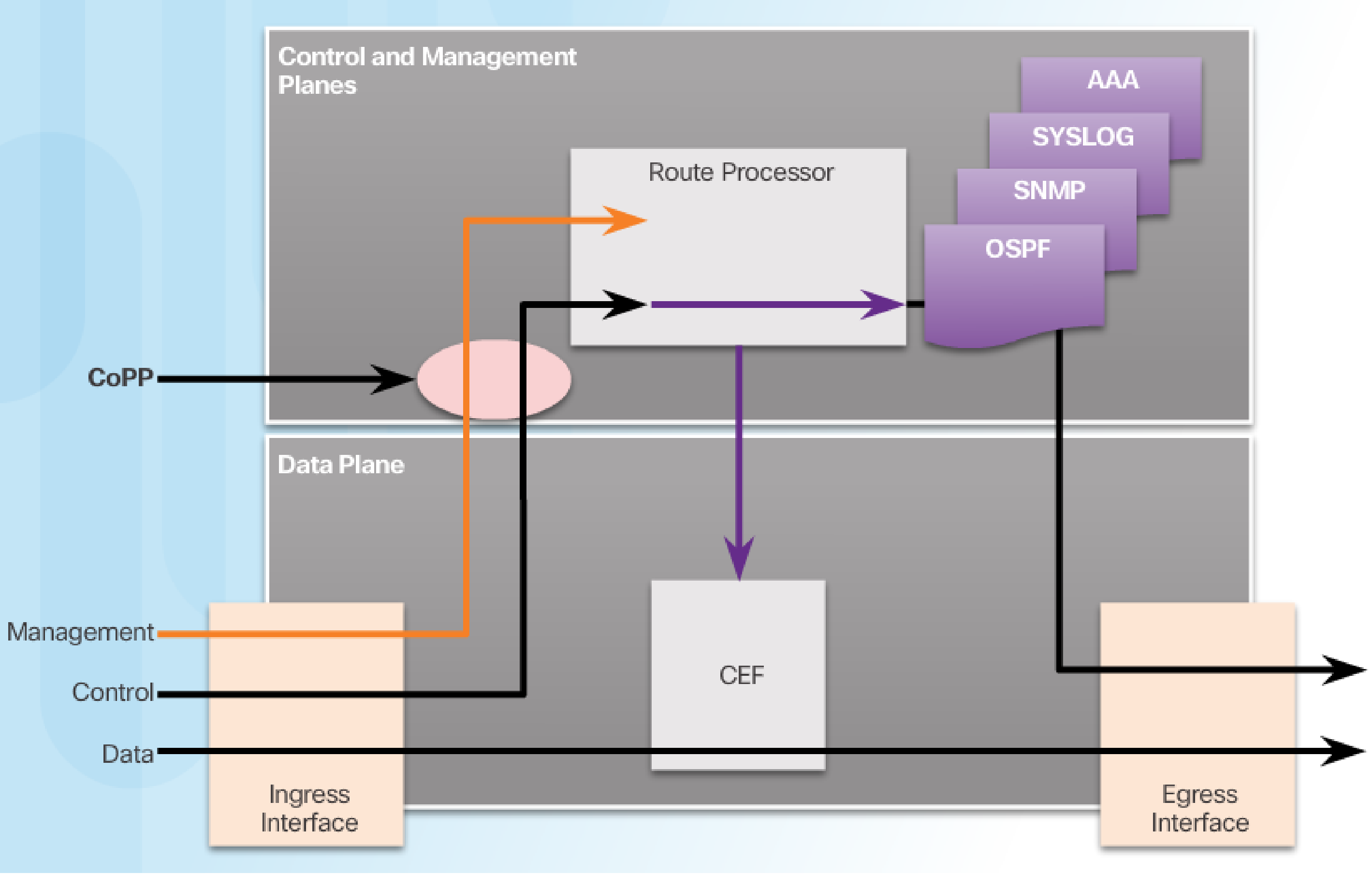
Control and Management Plane Vulnerabilities

- Router CPU usually
  - process Control plane and management plane functions
  - Not involved in packet forwarding (cef)
- However attack (malicious or not) on a control/management plane may consume CPU resources
  - Straight influence on control/mgmt. plane functions
  - Straight influence on forwarding
    - No routing info – no correct routing decisions
- **important is to protect the route processor !!!!**
  - For example using ACL
  - Or CoPP



Control Plane Policing - CoPP

- Cisco IOS feature that
  - allow to manage the flow of traffic that is “punted” to the route processor (not processed by CEF)
  - i.e. helps to protect against overwhelm of CPU resources



UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

KATEDRA INFORMAČNÝCH SIETÍ * FAKULTA RIADENIA A INFORMATIKY ŽU *

CISCO
Networking
Academy

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Aktualizované v rámci projektu KEGA 026TUKE-4/2021