Cisco Systems
Networking Academy

Cisco.com

Network Security 2

Module 7 – Secure Network Architecture and Management

CCNA CISCO CERTIFIED

Högskolan Halmstad

Learning Objectives

- 7.1 Layer 2 Security Best Practices
- 7.2 SDM Security Audit
- 7.3 Router Management Center (MC)
- 7.4 Simple Network Management Protocol (SNMP)

Module 7 – Secure Network Architecture and Management

7.1 Layer 2 Security Best Practices

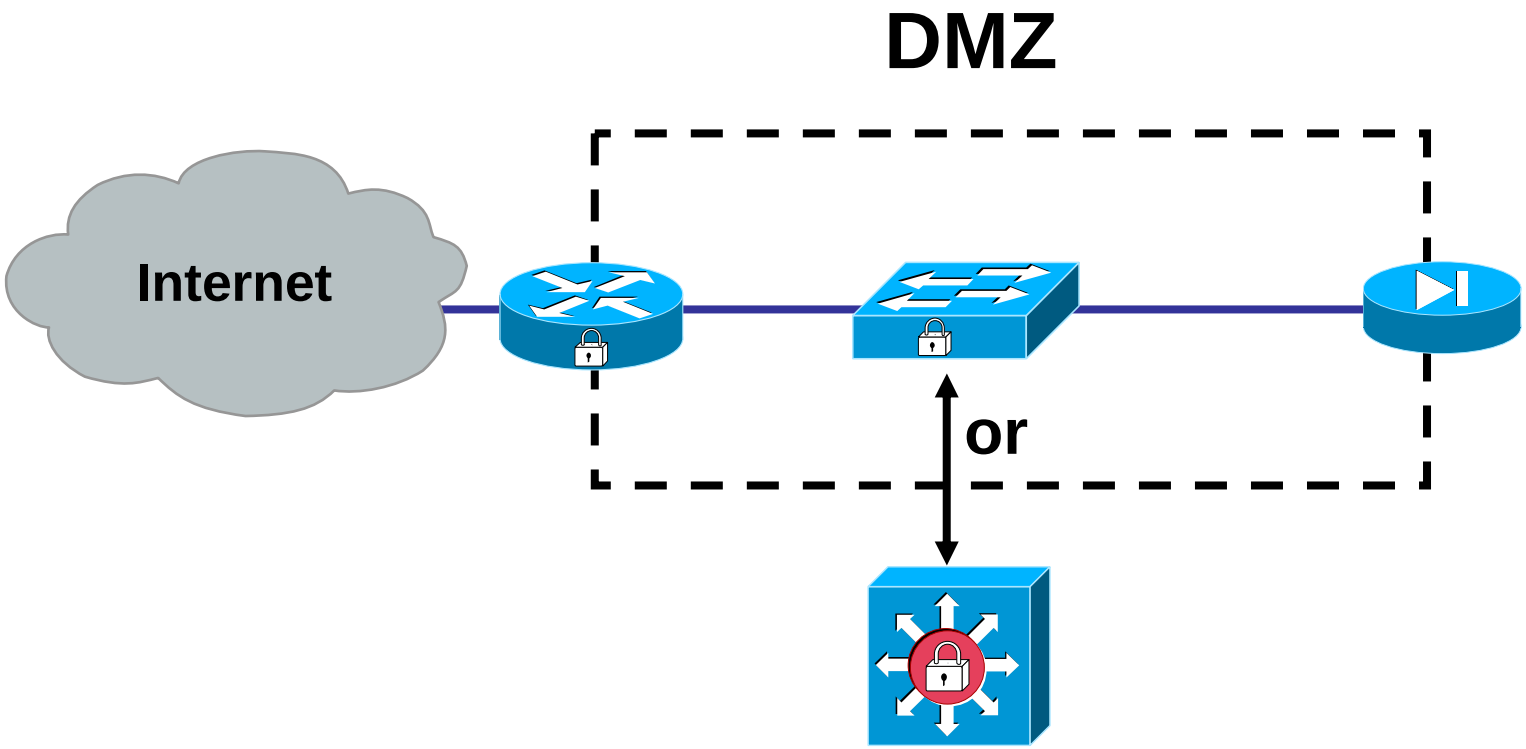
Factors Affecting Layer 2 Mitigation Techniques

- The number of security zones in the network design
- The number of user groups in the network design
- The number of switch devices in the design

Typical Cases

Case #	Security Zones	Number of User Groups	Number of Switch Devices
1	Single	Single	Single
2	Single	Single	Multiple
3	Single	Multiple	Single
4	Single	Multiple	Multiple
5	Multiple	Single	Single
6	Multiple	Single	Multiple
7	Multiple	Multiple	Single
8	Multiple	Multiple	Multiple

Single Security Zone, One User Group, One Physical Switch



Commands to mitigate MAC Spoofing (Cisco IOS)


```
switch(config-if)#
```

```
switchport port-security maximum value
```

- **Sets the maximum number of secure MAC addresses for the interface**

```
switch(config-if)#
```

```
switchport port-security violation {protect | restrict | shutdown}
```

- **Sets the violation mode and the action to be taken**

```
switch(config-if)#
```

```
arp timeout seconds
```

- **Configures the timeout, in seconds that an entry remains in the ARP cache**

Commands to mitigate MAC Spoofing (Catalyst OS)

Cisco.com

```
switch>
set port security mod/port enable [mac_addr]
```

- **Enable port security**

```
switch>
set port security mod/port mac_addr
```

- **Enable port security for specific MAC Address**

```
switch>
set port security mod/port violation {shutdown|restrict}
```

- **Set actions on violation**

Configuring DHCP Snooping(Cisco IOS)


```
switch(config)#
ip dhcp snooping
```

- **Enable DHCP snooping globally**

```
switch(config)#
ip dhcp snooping vlan vlan_id{,vlan_id}
```

- **Enable DHCP snooping on VLANs**

```
switch(config-if)#
ip dhcp snooping trust
```

- **Configure the interface as trusted or untrusted.**

Configuring DHCP Snooping(Cisco IOS)


```
switch(config-if)#
```

```
ip dhcp snooping limit rate rate
```

- **Configure the number of DHCP packets per second (pps) that an interface can receive**

Dynamic ARP Inspection


```
switch(config)#
```

```
ip arp inspection vlan vlan_id{,vlan_id}
```

- **Enable ARP inspection per vlan**

```
switch(config)#
```

```
ip arp inspection validate [src-mac] [dst-mac] [ip]
```

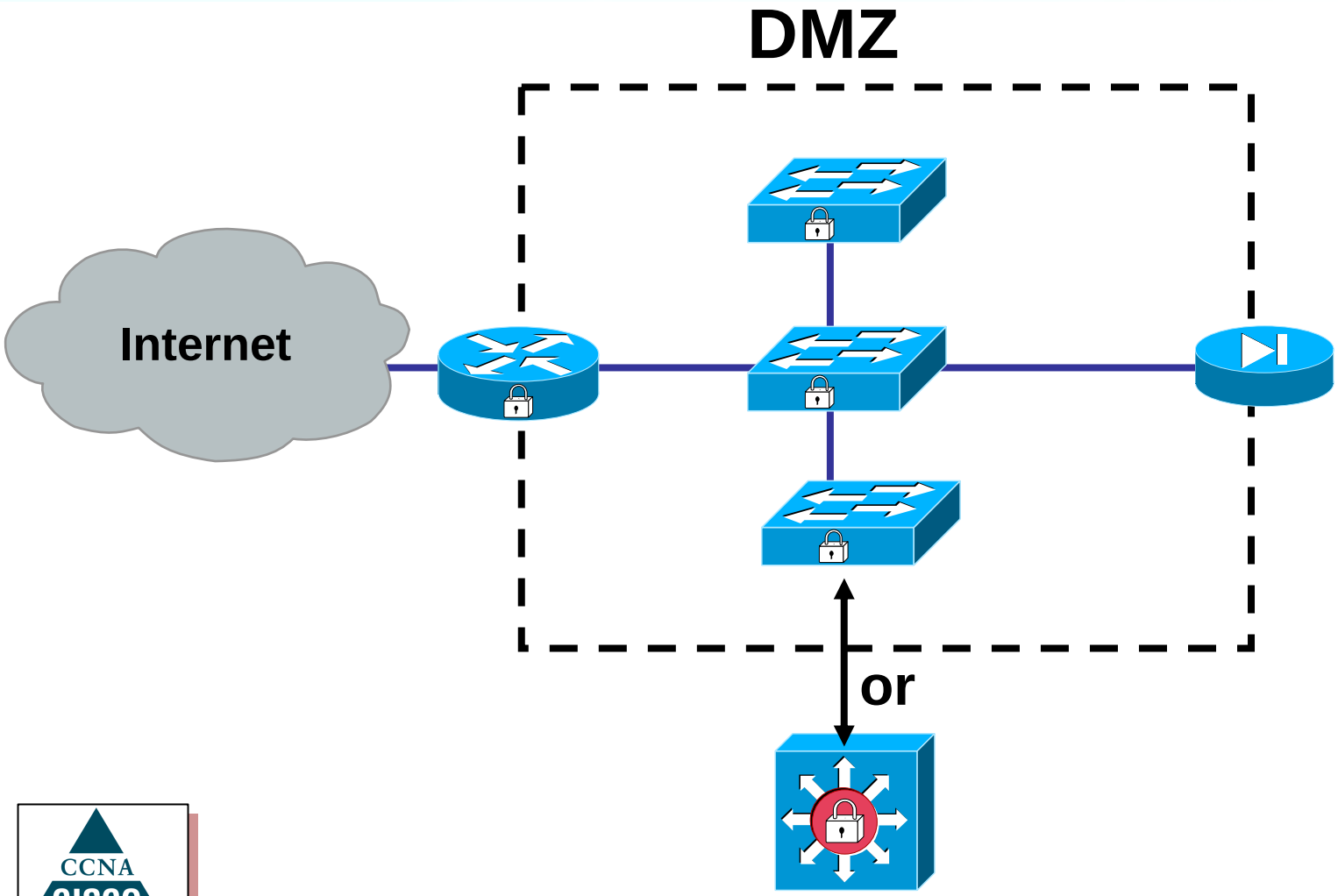
- **Perform specific checks for ARP inspection**

```
switch(config-if)#
```

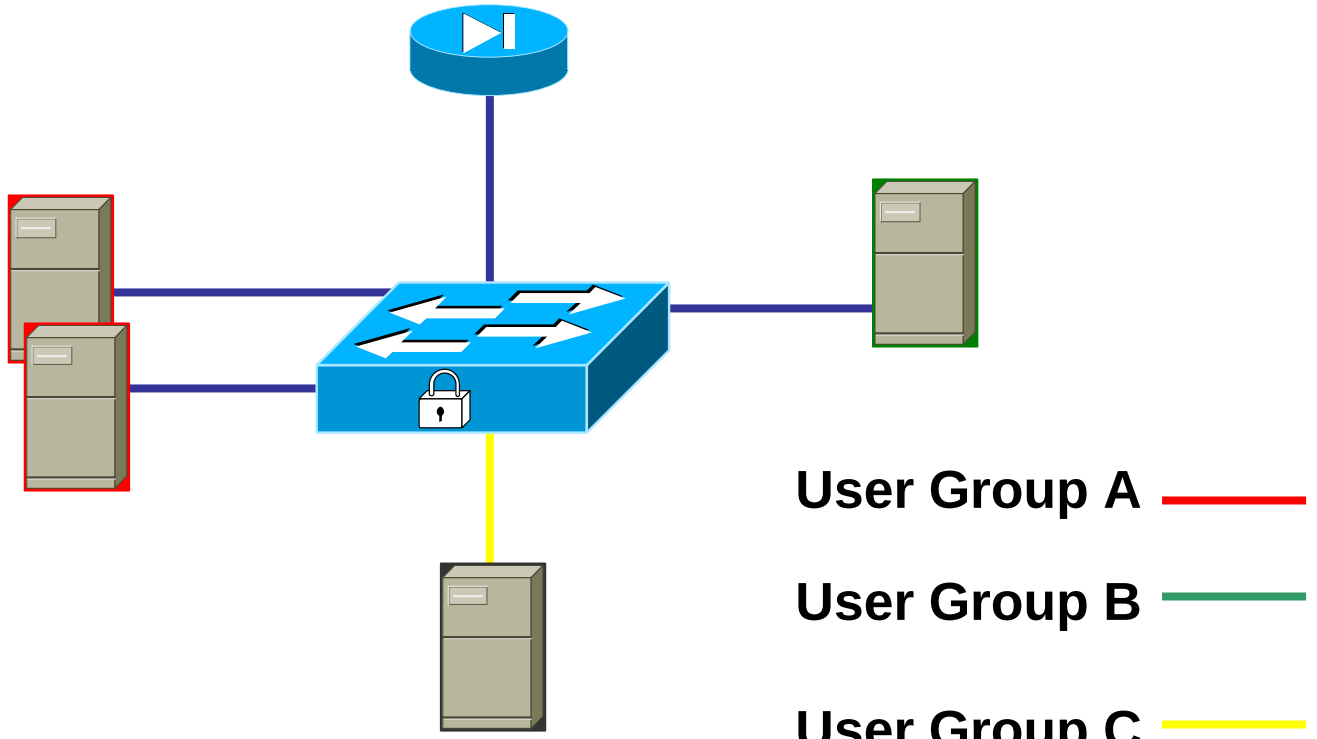
```
ip arp inspection trust
```

- **Set a per-port configurable trust state**

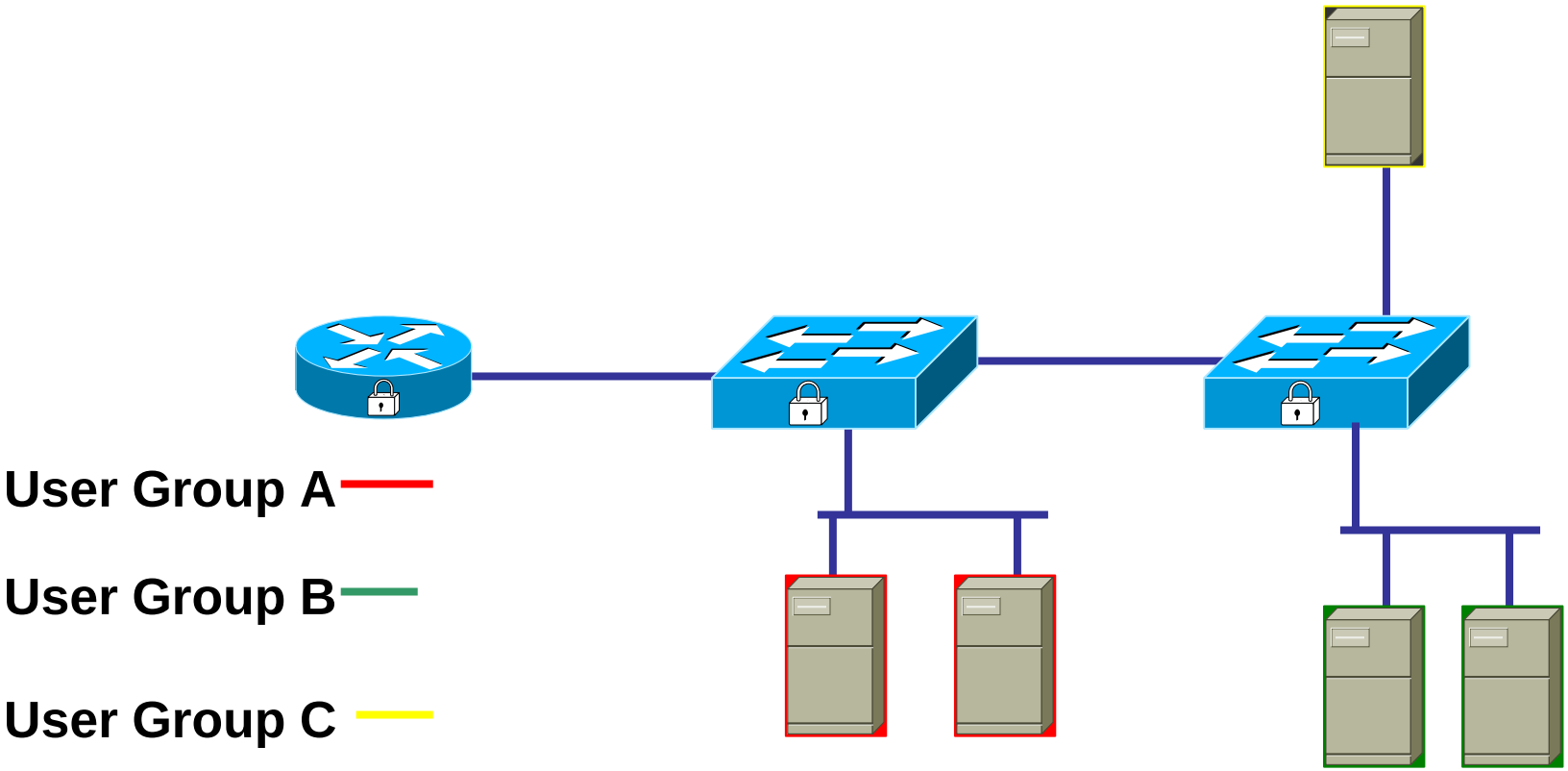
Single Security Zone, One User Group, Multiple Physical Switches



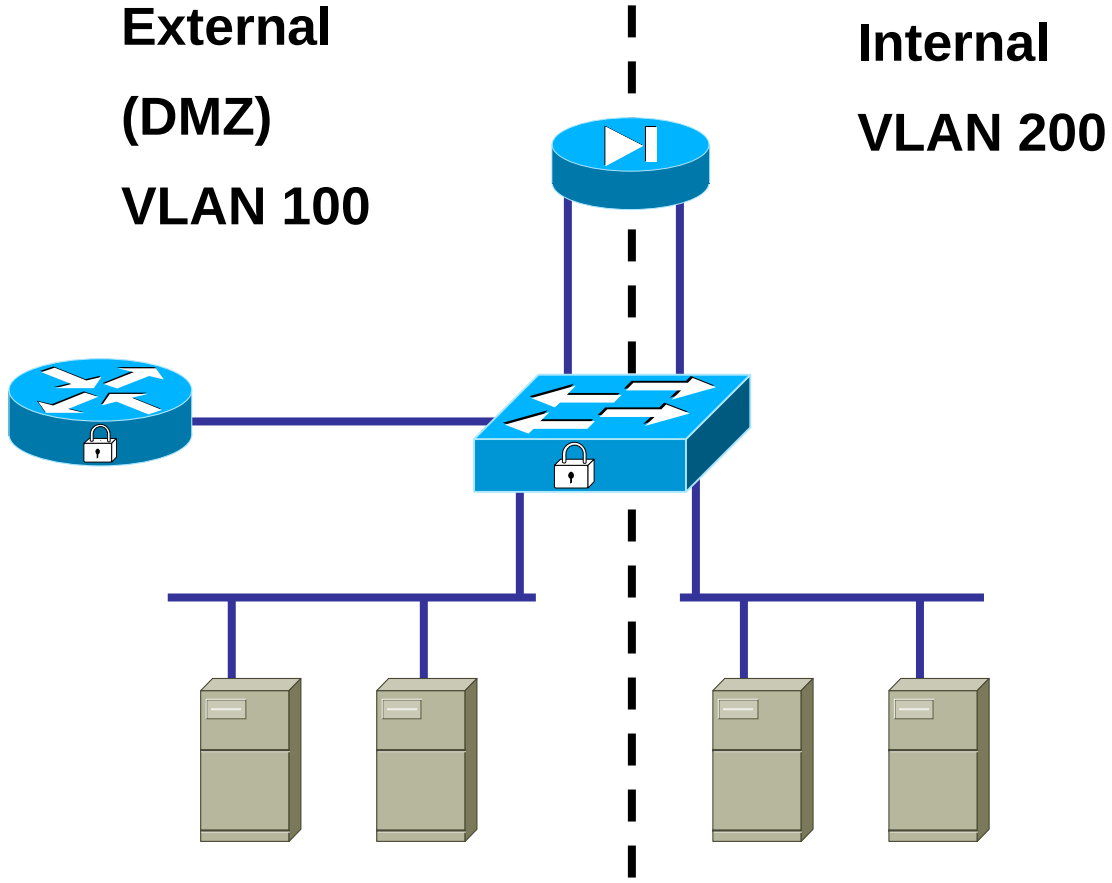
Single Security Zone, Multiple User Groups, Single Physical Switch



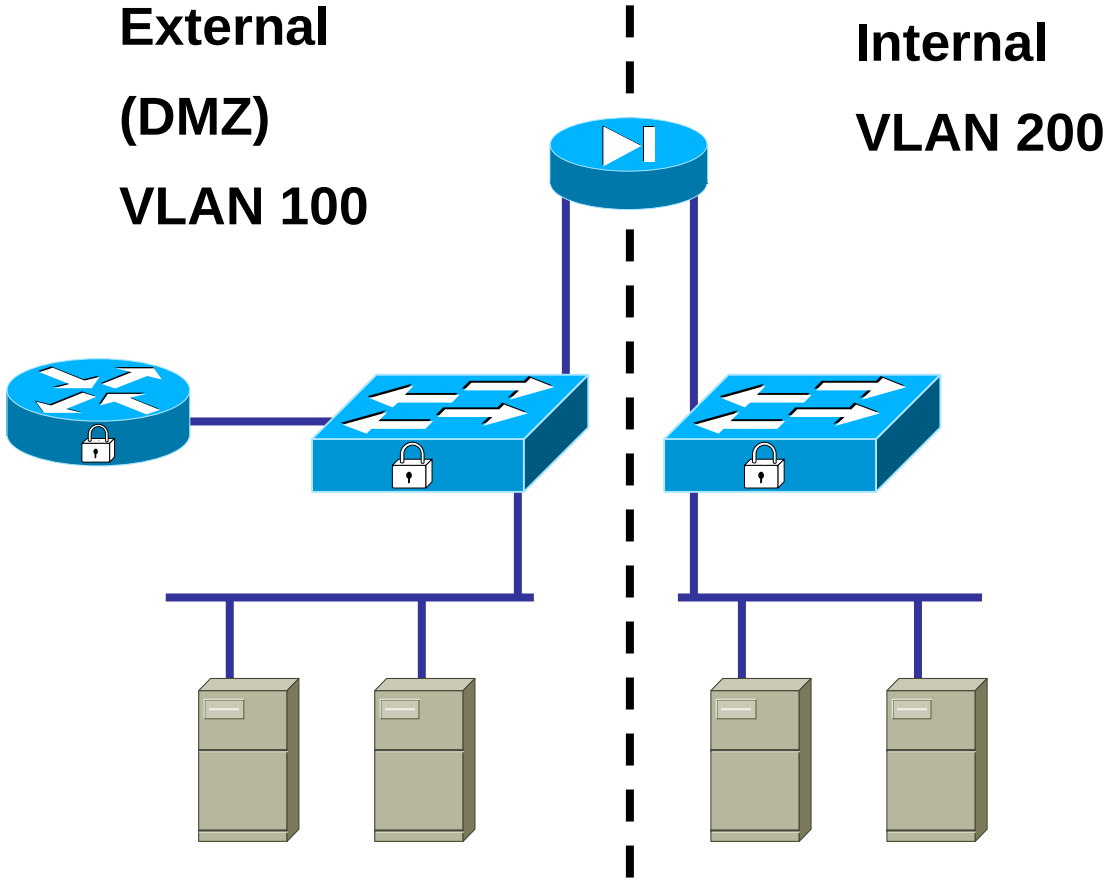
Single Security Zone, Multiple User Groups, Multiple Physical Switches



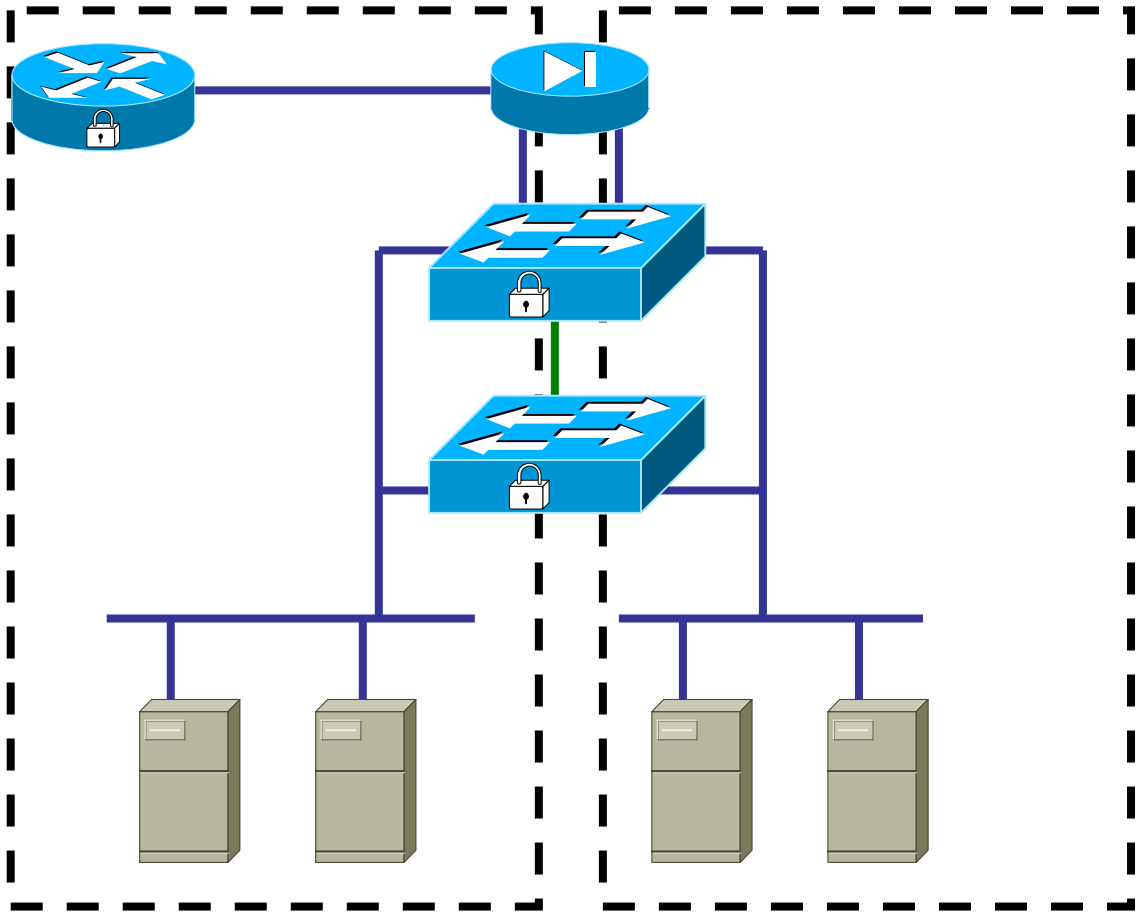
Multiple Security Zone, One User Group, Single Physical Switch



Multiple Switch Network Separation



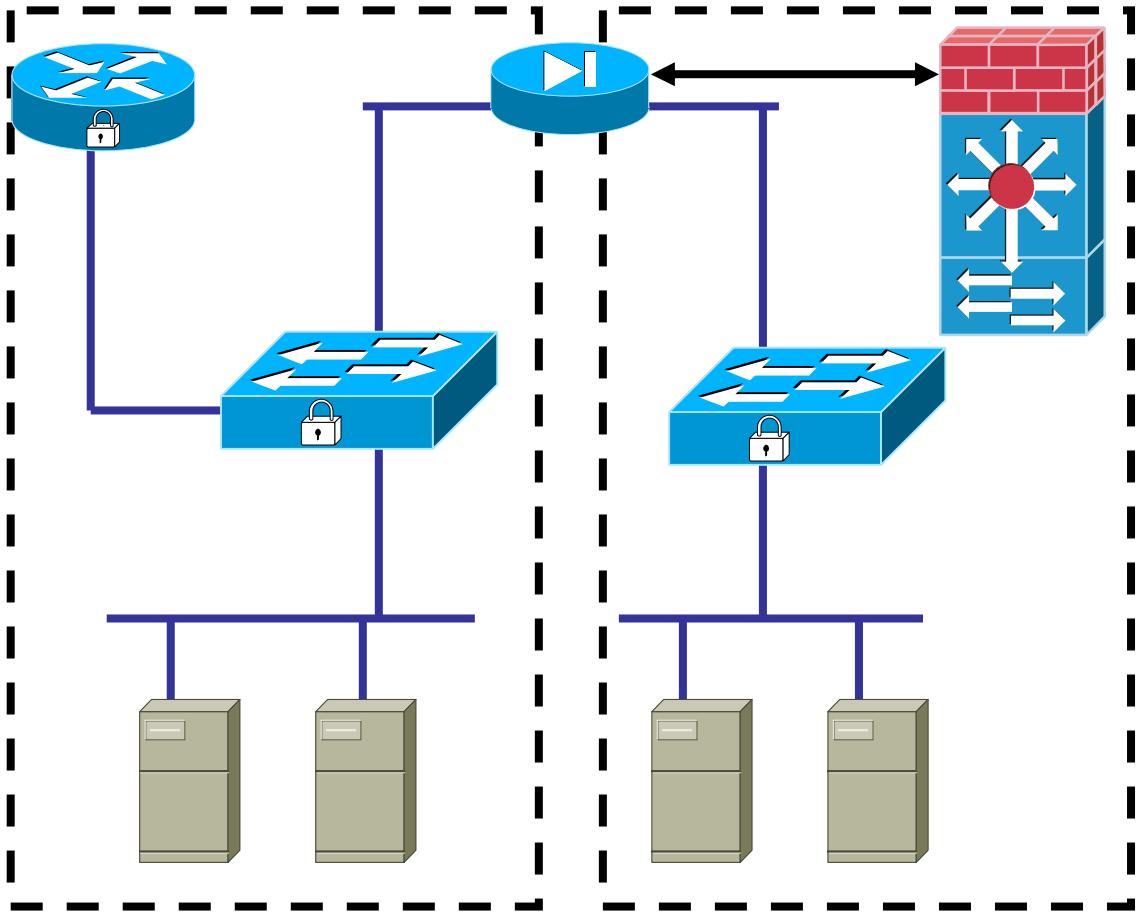
Multiple Security Zones, One User Group, Multiple Physical Switches



Security Zone 1

Security Zone 2

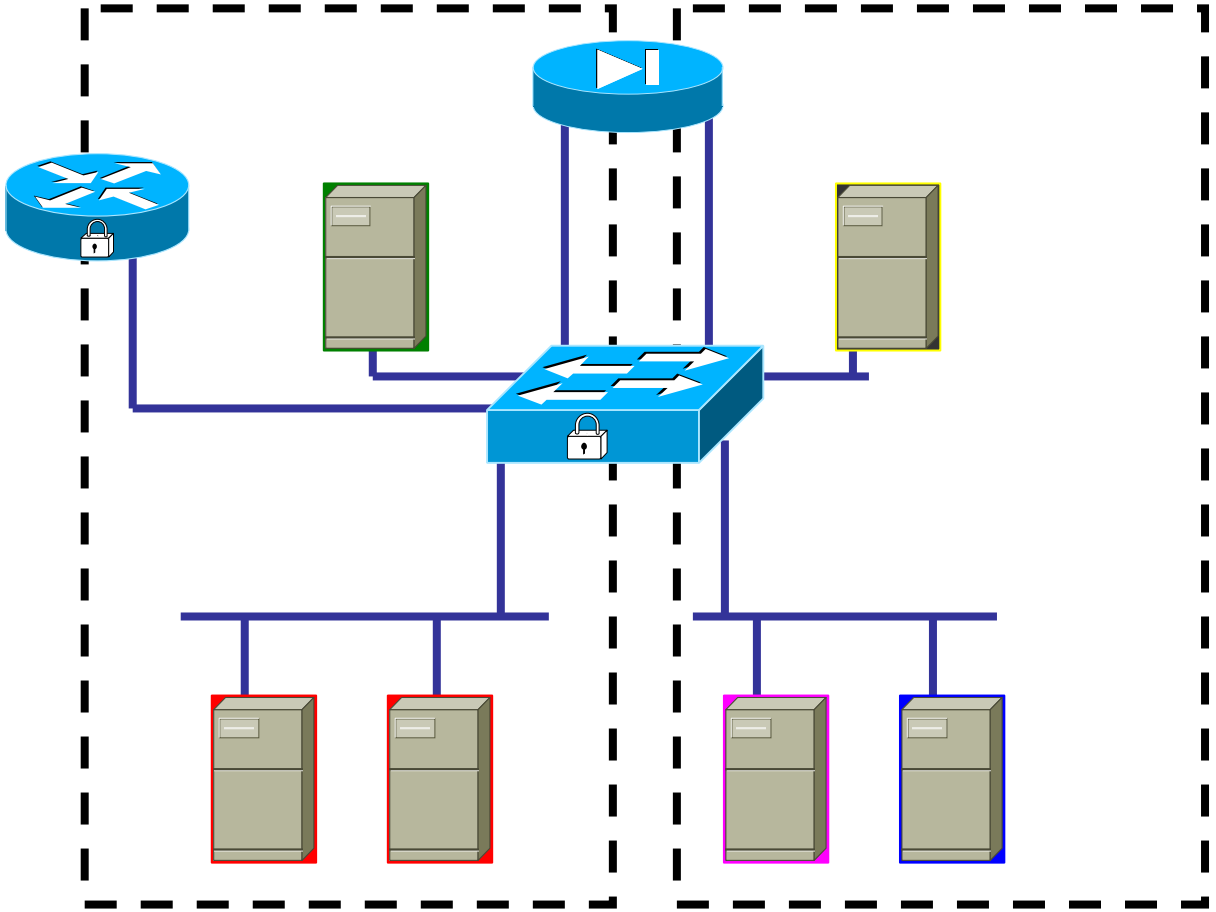
Alternative Design for Multiple Security Zones, One User Group, Multiple Switches



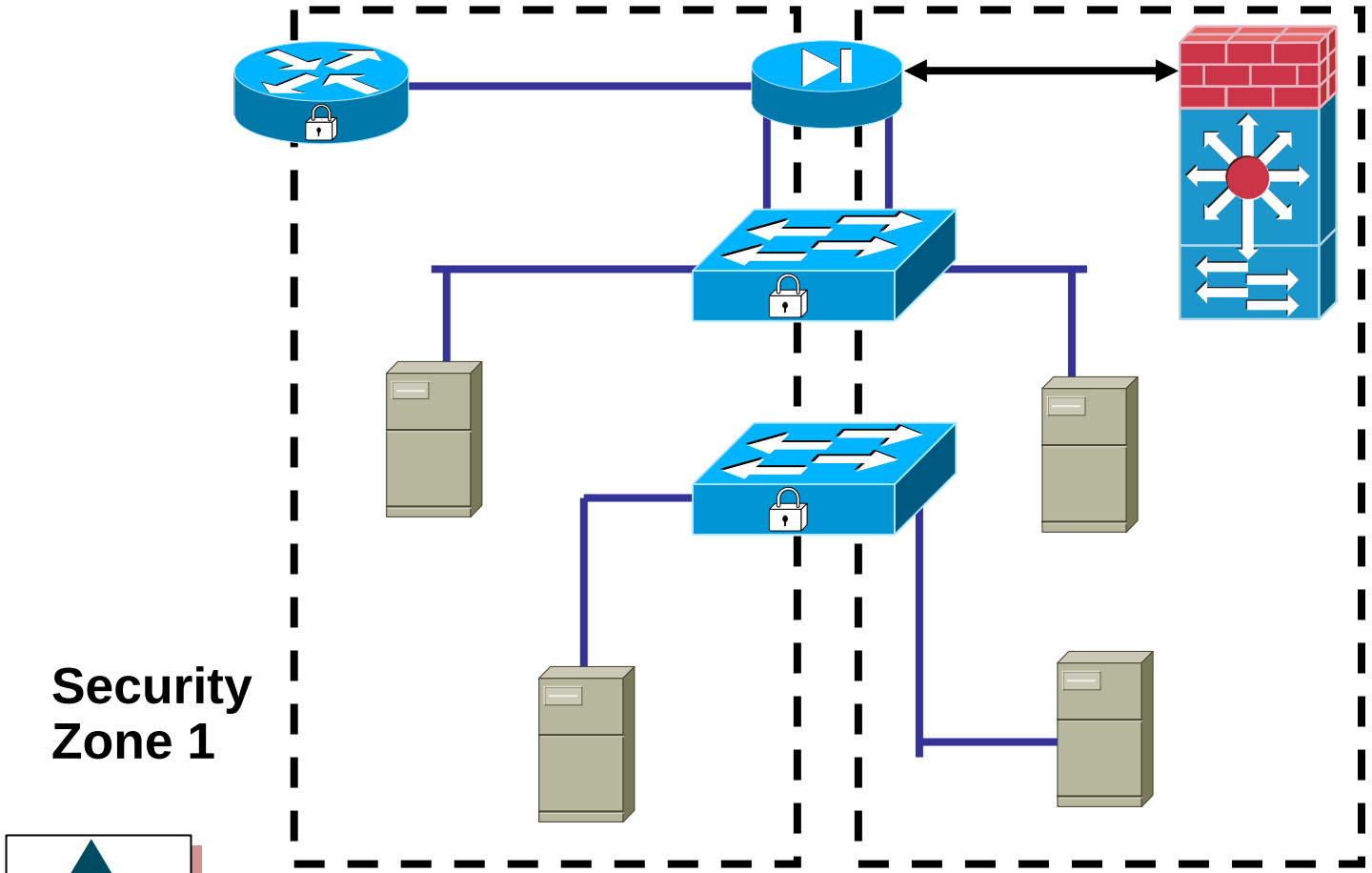
Security Zone 1

Security Zone 2

Multiple Security Zones, Multiple User Groups, Single Physical Switch



Multiple Security Zones, Multiple User Groups, Multiple Physical Switches



Cisco Systems
Networking Academy

Cisco.com

Module 7 – Secure Network Architecture and Management

7.2 SDM Security Audit

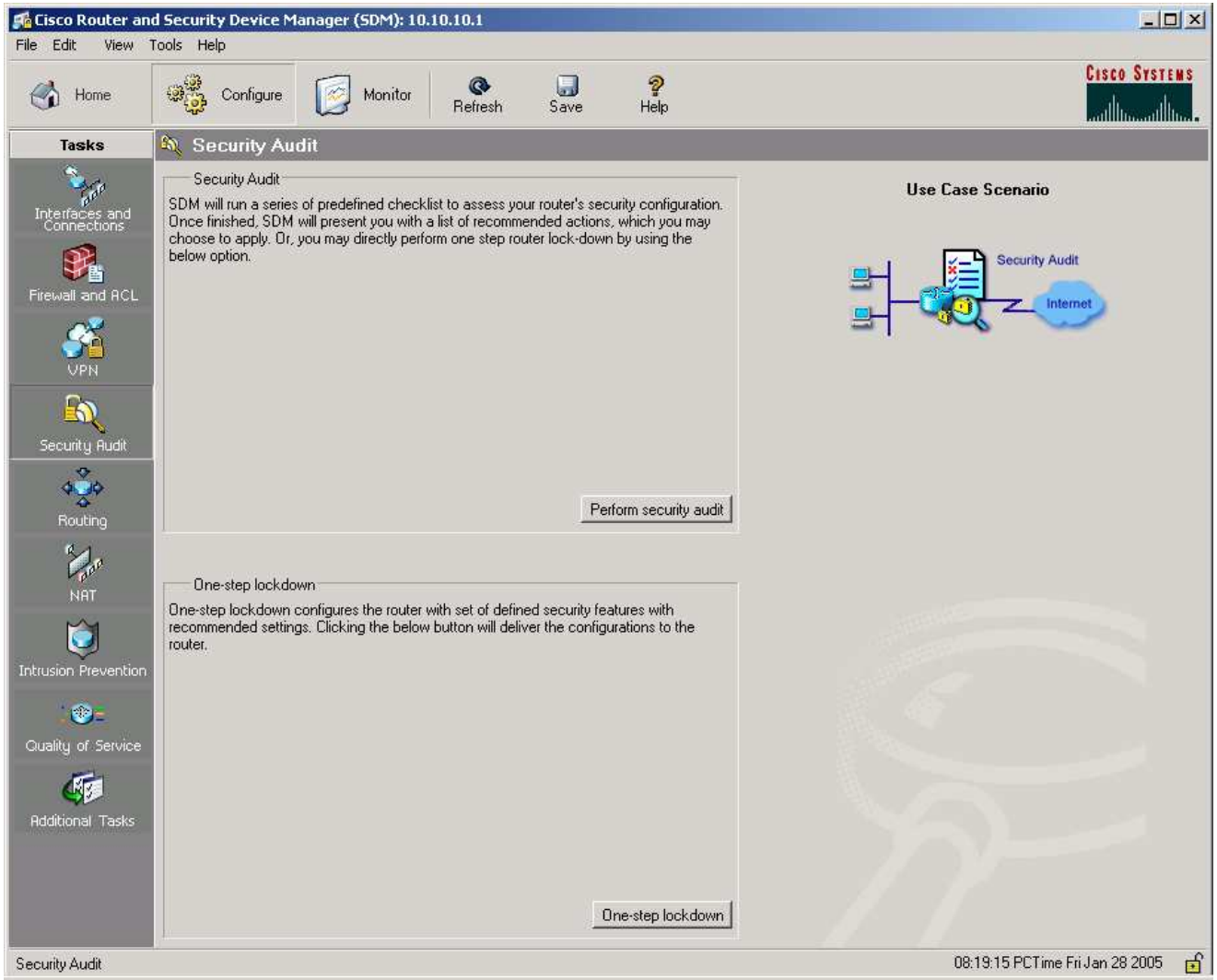
CCNA CISCO CERTIFIED™

Högskolan Halmstad

Security Audit Overview

- Compares router configuration against a predefined checklist of ICSA and TAC approved best practices.
- Examples of the audit include, but are not limited to, the following:
  - Shut down unneeded servers on the router, such as BOOTP, finger, and tcp/udp small-servers.
  - Shut down unneeded services on the router, such as CDP, ip source-route, and ip classless.
  - Apply firewall to outside interfaces.
  - Disable SNMP or enable with hard-to-guess community strings.
  - Shut down unused interfaces, no ip proxy-arp.
  - Force passwords for console and vty lines.
  - Force an enable secret password.
  - Enforce the use of access lists.

Security Audit Main Window



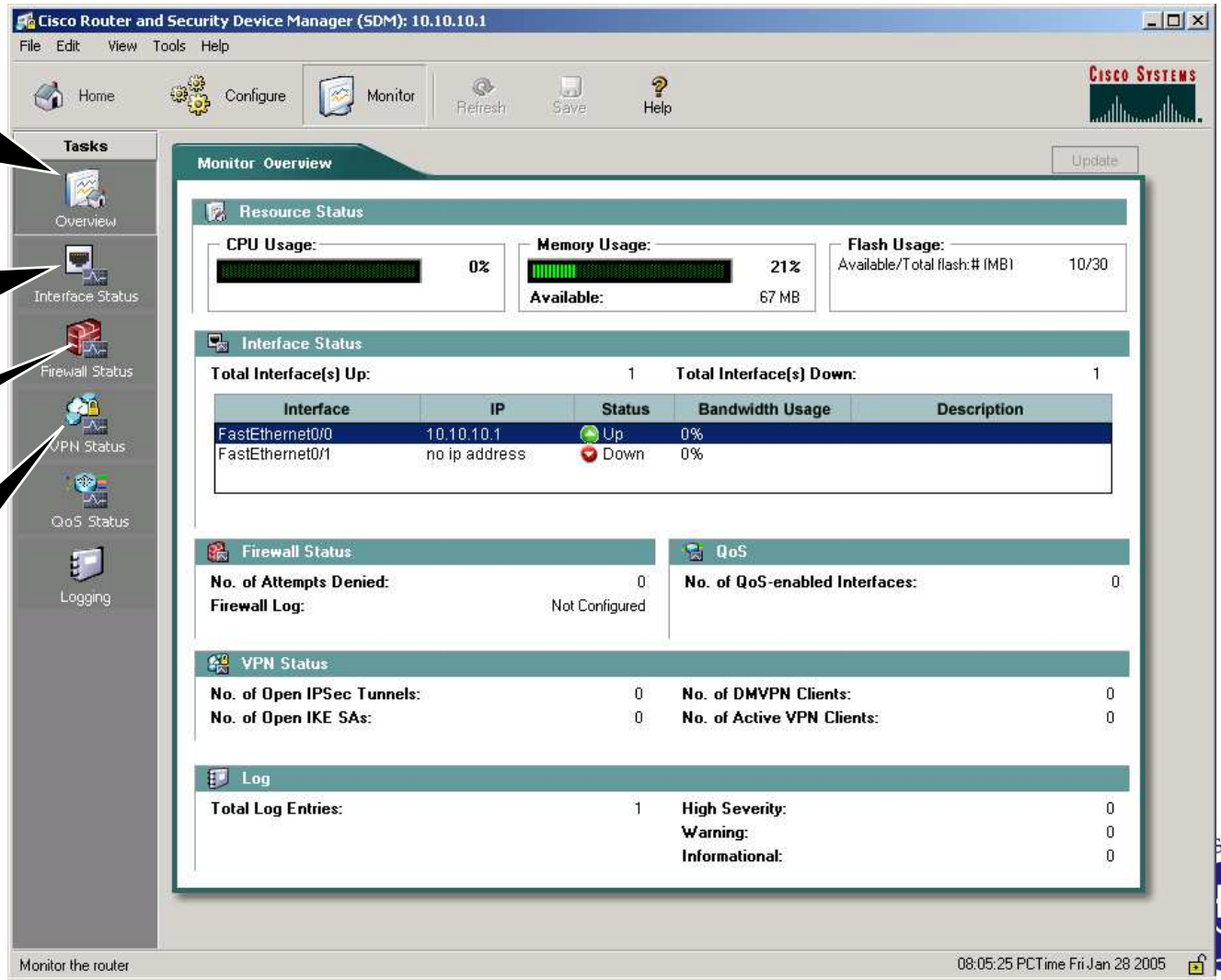
Monitor Mode

Overview

Interface Stats

Firewall Stats

VPN Stats



Cisco Systems
Networking Academy

Cisco.com

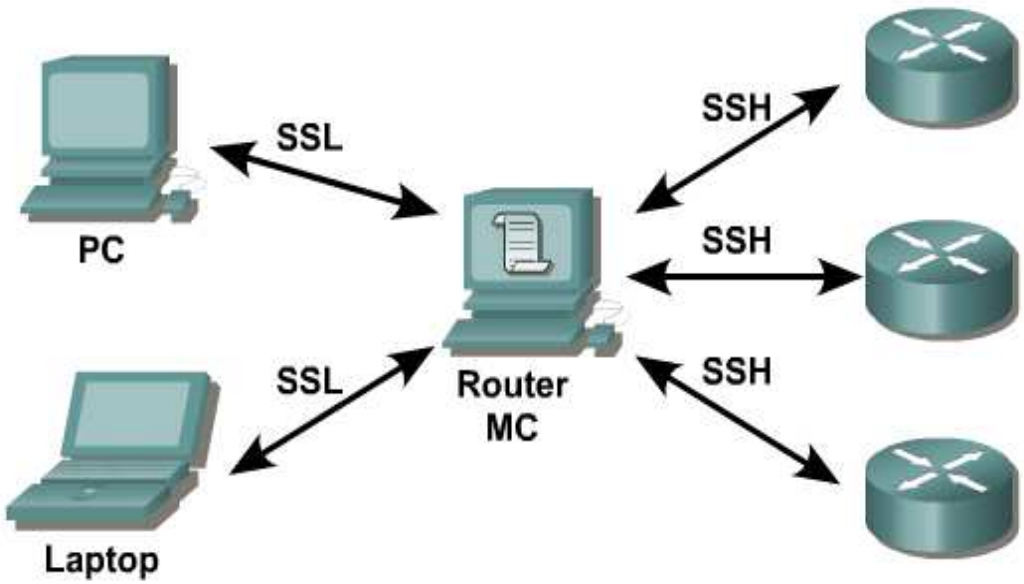
Module 7 – Secure Network Architecture and Management

7.3 Router Management Center (MC)

CCNA CISCO CERTIFIED

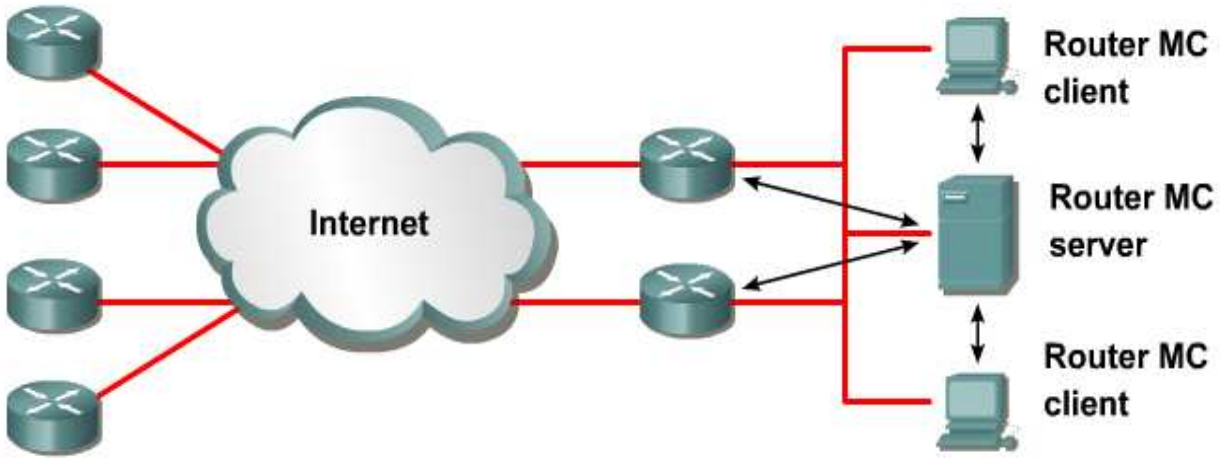
Högskolan Halmstad

The Router Management Center (MC)



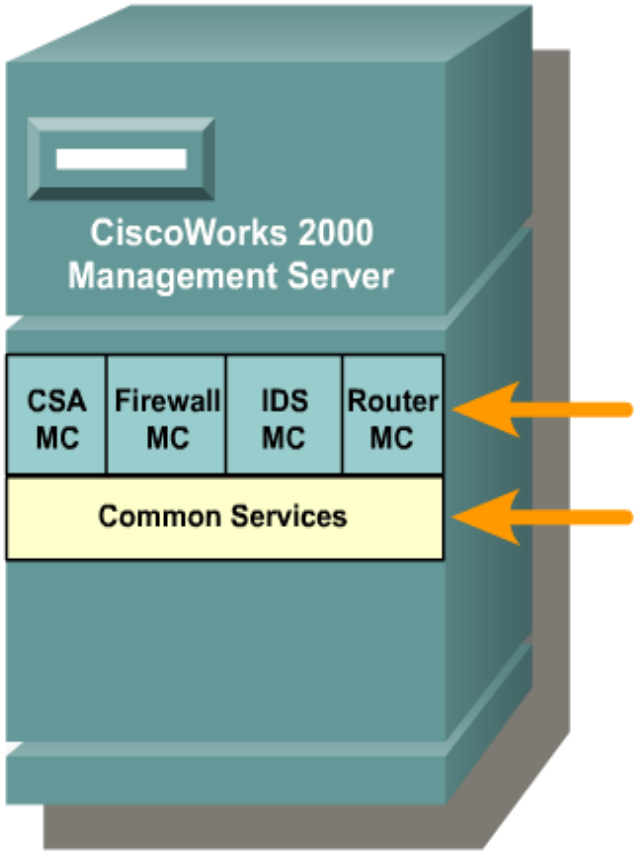
Router MC is a web-based application designed for large-scale management of VPN and firewall configurations on Cisco routers.

What is the Router MC?



Router MC is a web-based application designed for large-scale management of VPN and firewall configurations on Cisco routers.

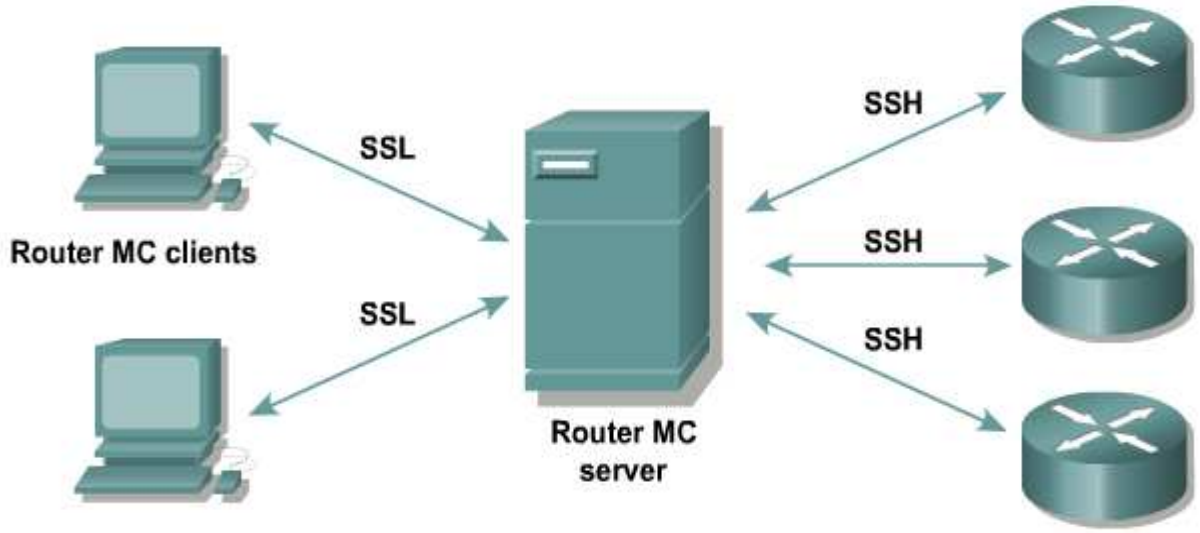
Router MC Components



Web-based applications for configuring and managing multiple devices such as PIX Firewalls, routers, IDS Sensors, HIDS, and so on

Common set of management services that are shared by multiple network management application

Configure Routers for SSH



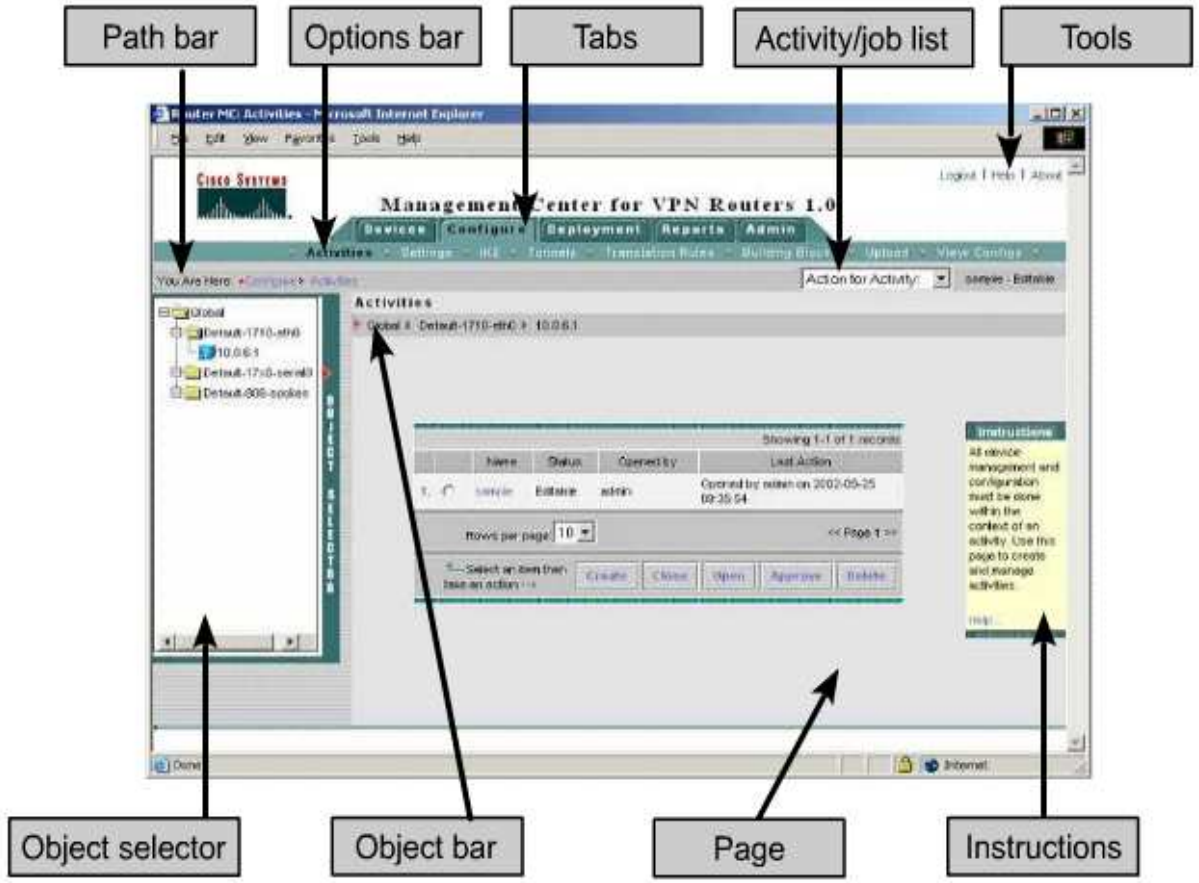

```
Router(config)# hostname Austin
Austin(config)# ip domain-name cisco.com
Austin(config)# crypto key generate rsa usage-keys modulus 1024
Austin(config)# ip ssh time-out 60
Austin(config)# ip ssh authentication 2
```

CCNA CISCO CERTIFIED

HÖGSKOLAN HALMSTAD

Using the Router MC

The Router MC User Interface



Cisco Systems
Networking Academy

Cisco.com

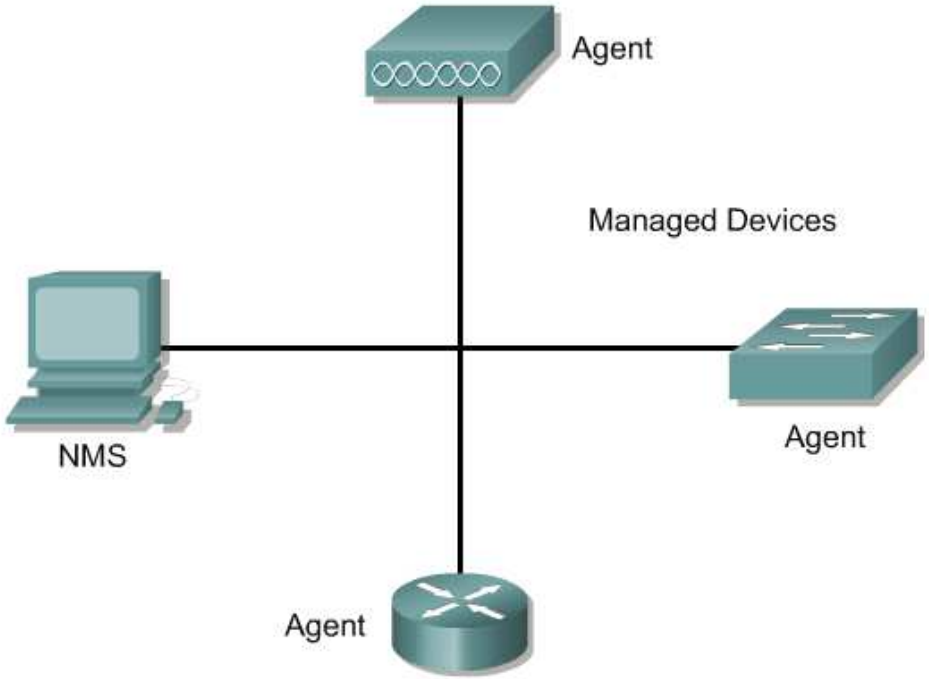
Module 7 – Secure Network Architecture and Management

7.4 Simple Network Management Protocol (SNMP)

CCNA CISCO CERTIFIED™

Högskolan Halmstad

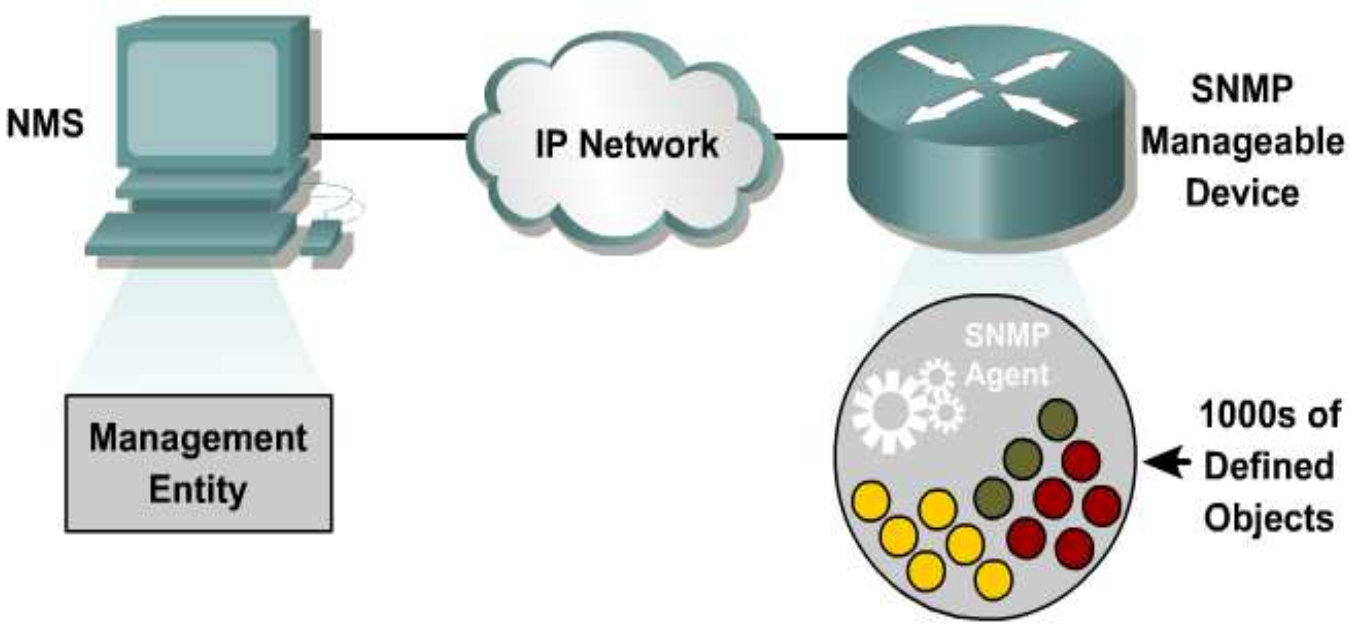
SNMP Introduction



An SNMP managed network consists of three key components:

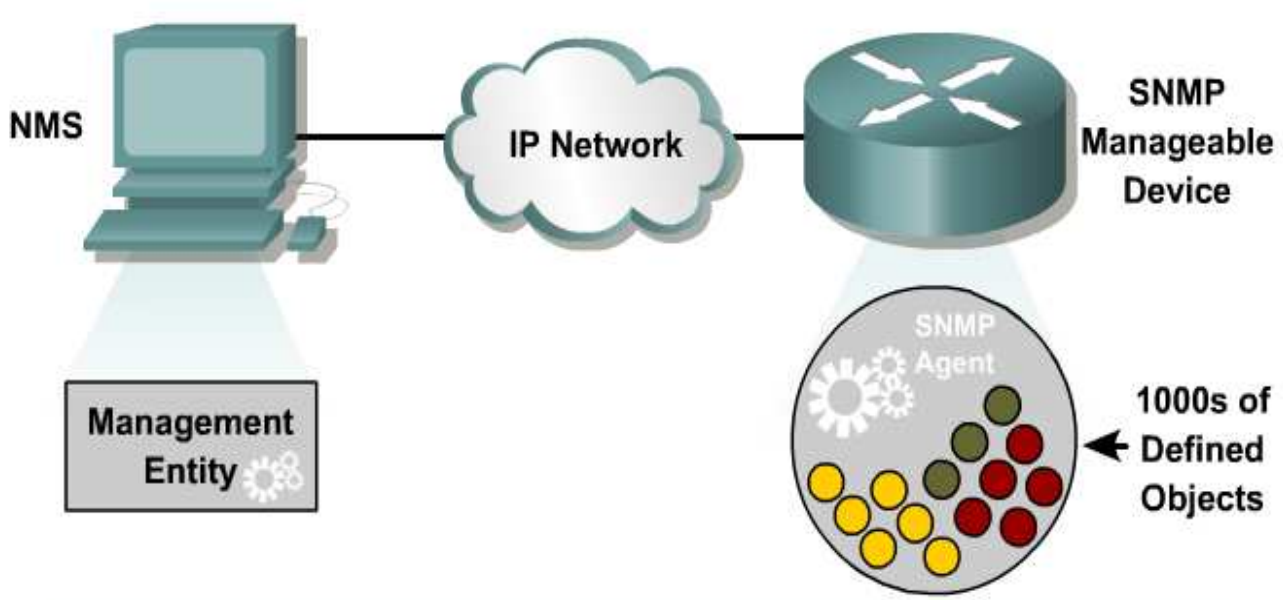
- **Managed Devices**
- **Agents**
- **Network management systems (NMSs)**

SNMP Agent



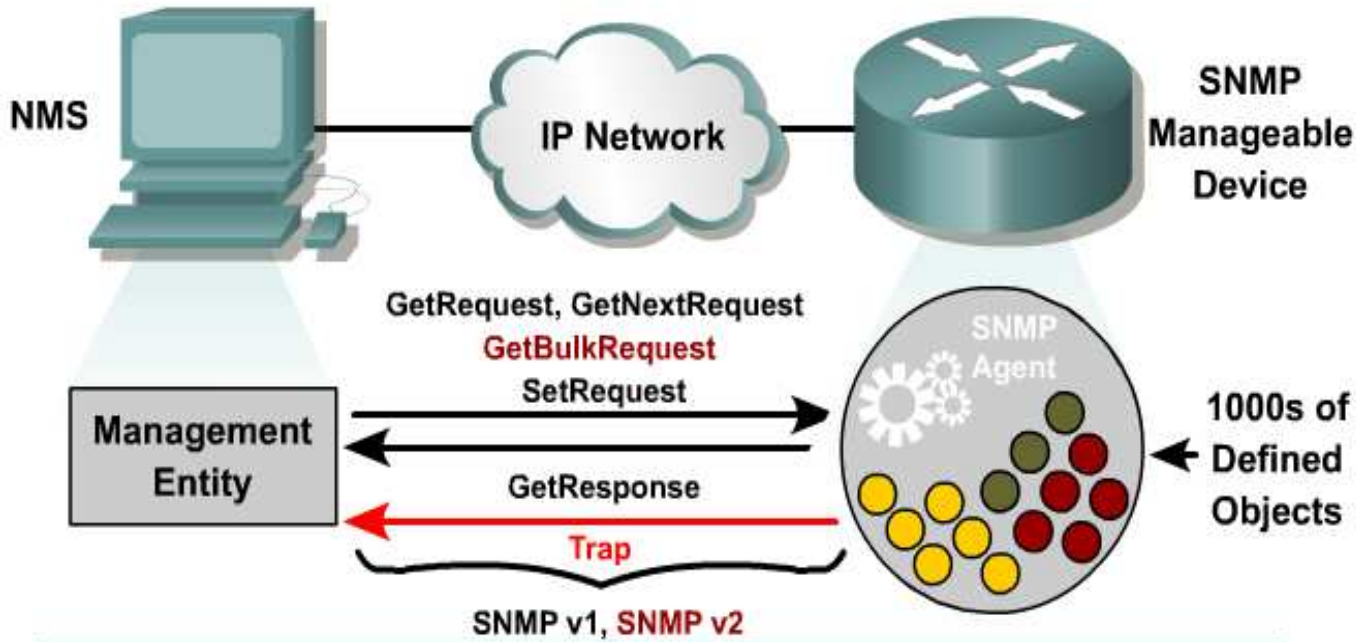
- Information storehouse
- Information structured as per Structure of Management Information (SMI) standards
- Object definitions provided in many Management Information Bases (MIBs)

SNMP Management Entity



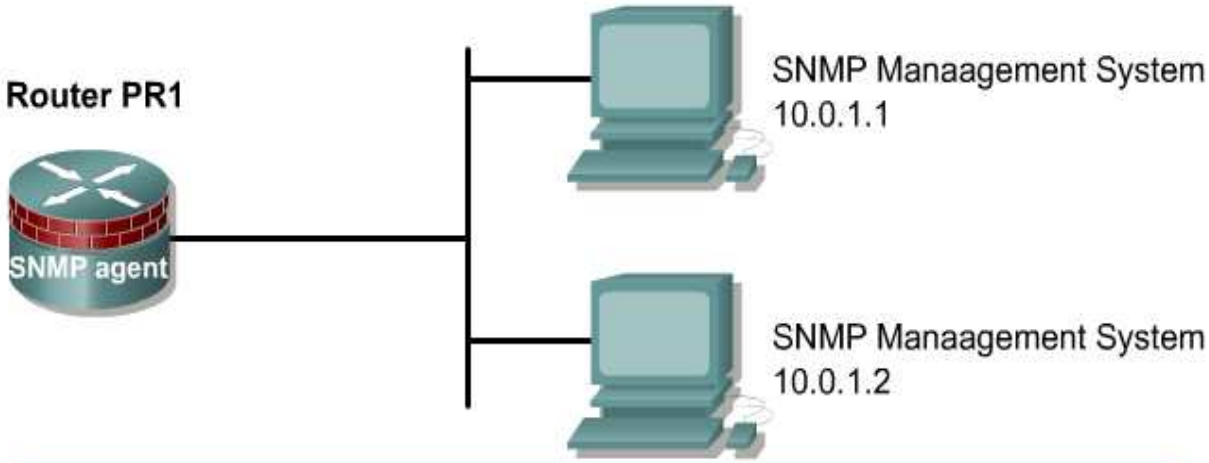
- Management entity collects data by generating requests. This causes in-band traffic coexisting with production traffic.
- Management entity receives notifications of network alarms or events. This can be forwarded to the manager through email, or SMS.
- Management entity runs applications to analyze or interpret management data.

SNMP Device Management



- GetRequests used to read the value of object
- SetRequests used to modify the value of object
- Traps provide asynchronous event notification

Securing SNMP Access



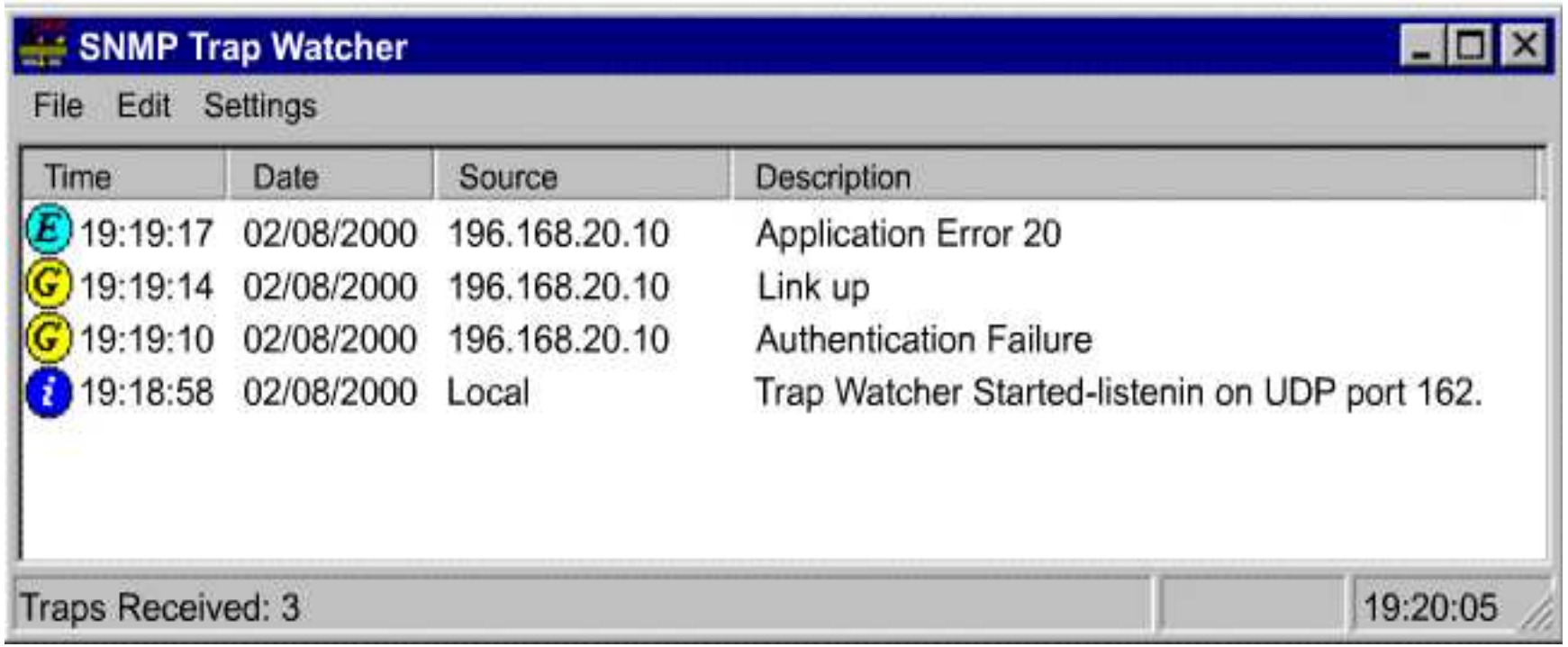
Mode	Command	Description
router (config)#	**snmp-server community *string* [ro | rw] [*number*]**	

```
PR1(config)# snmp-server community readSNMP ro
```

```
PR1(config)# snmp-server community ReadWritesnmp rw
```

```
PR1(config)# access-list 10 permit 10.0.1.1
PR1(config)# access-list 10 permit 10.0.1.2
PR1(config)# snmp-server community RWSNMP rw 10
```

SNMP Trap Watcher



Configure SNMP Engine

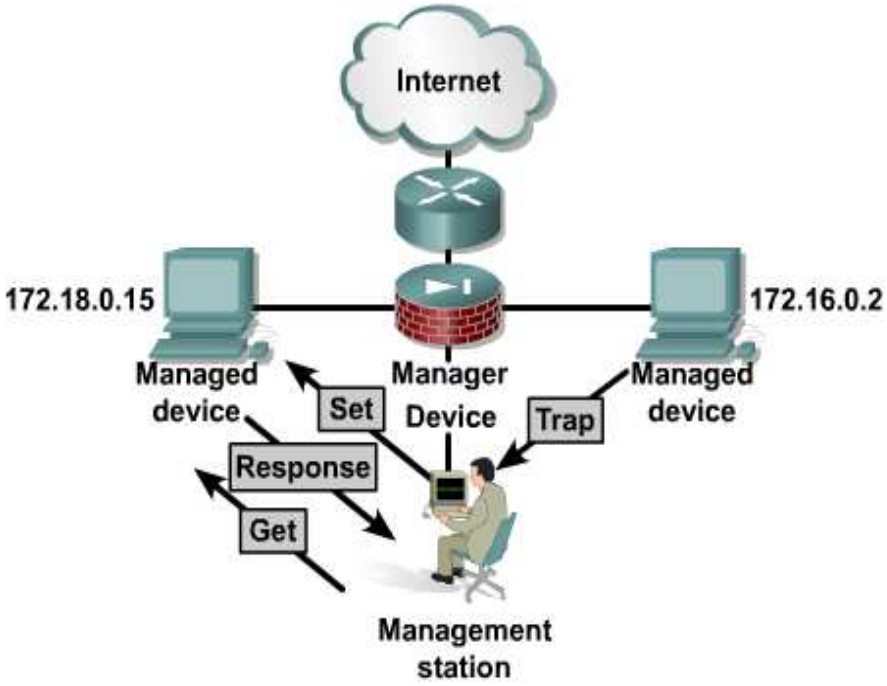
Mode	Command	Description
`router (config)#`	**`snmp-server engineID [local`** ***`engineid-string`*** **`] | [remote`** ***`ip-address`*** **`udp-port`** ***`port-number engineid-string`*** **`]`**	To configure a name for either the local or remote SNMP engine on the router, use the **`snmp-server engineID`** global configuration command. Use the no form of this command to remove a specified SNMP group.

Syntax	Description
`local`	(Optional) Specifies the local copy of SNMP on the router.
`engineid-string`	(Optional) The name of a copy of SNMP.
`remote`	(Optional) Specifies the remote copy of SNMP on the router.
`ip-address`	Optional) The IP address of the device that contains the remote copy of SNMP.
`udp-port`	(Optional) Specifies a UDP port of the host to use.
`port`	(Optional) The socket number on the remote device that contains the remote copy of SNMP. The default is 161.

CCNA CISCO CERTIFIED™

HÖGSKOLAN HALMSTAD

SNMP and the PIX Security Appliance



The network administrator is able to manage and monitor network devices from the management station using the SNMP protocol.