Svičevi

Svičevi

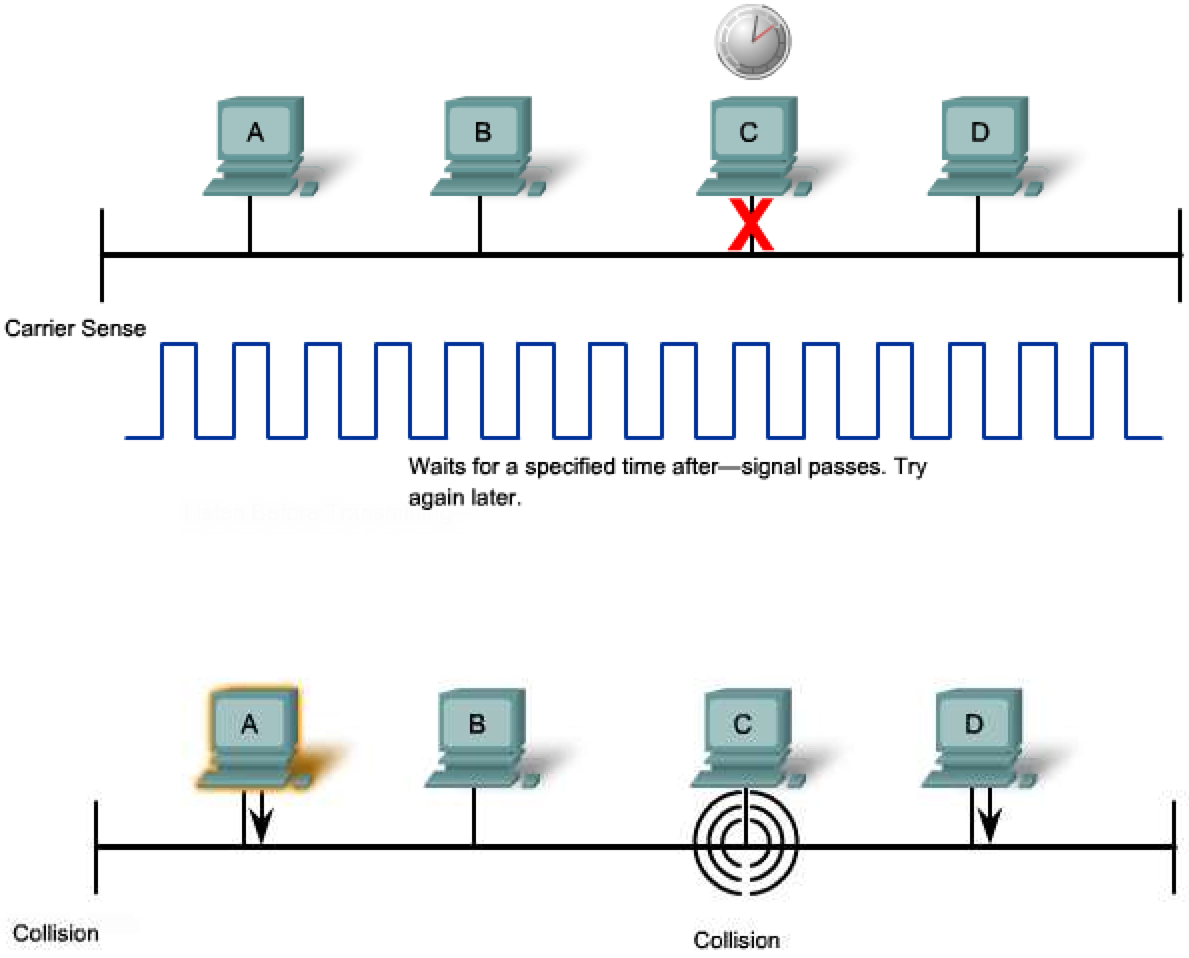
- Ethernet i prosleđivanje frejmova
- Navigacija kroz komandni interfejs upravljivih svičeva i osnovna podešavanja
- Pristup i zaštita od neovlašćenog pristupa
- Primeri tipičnih napada
- Bezbednost na nivou svič-porta

- Literatura: *CCNA Exploration LAN Switching and Wireless*, kompletno poglavlje 2

Ethernet i prosleđivanje frejmova

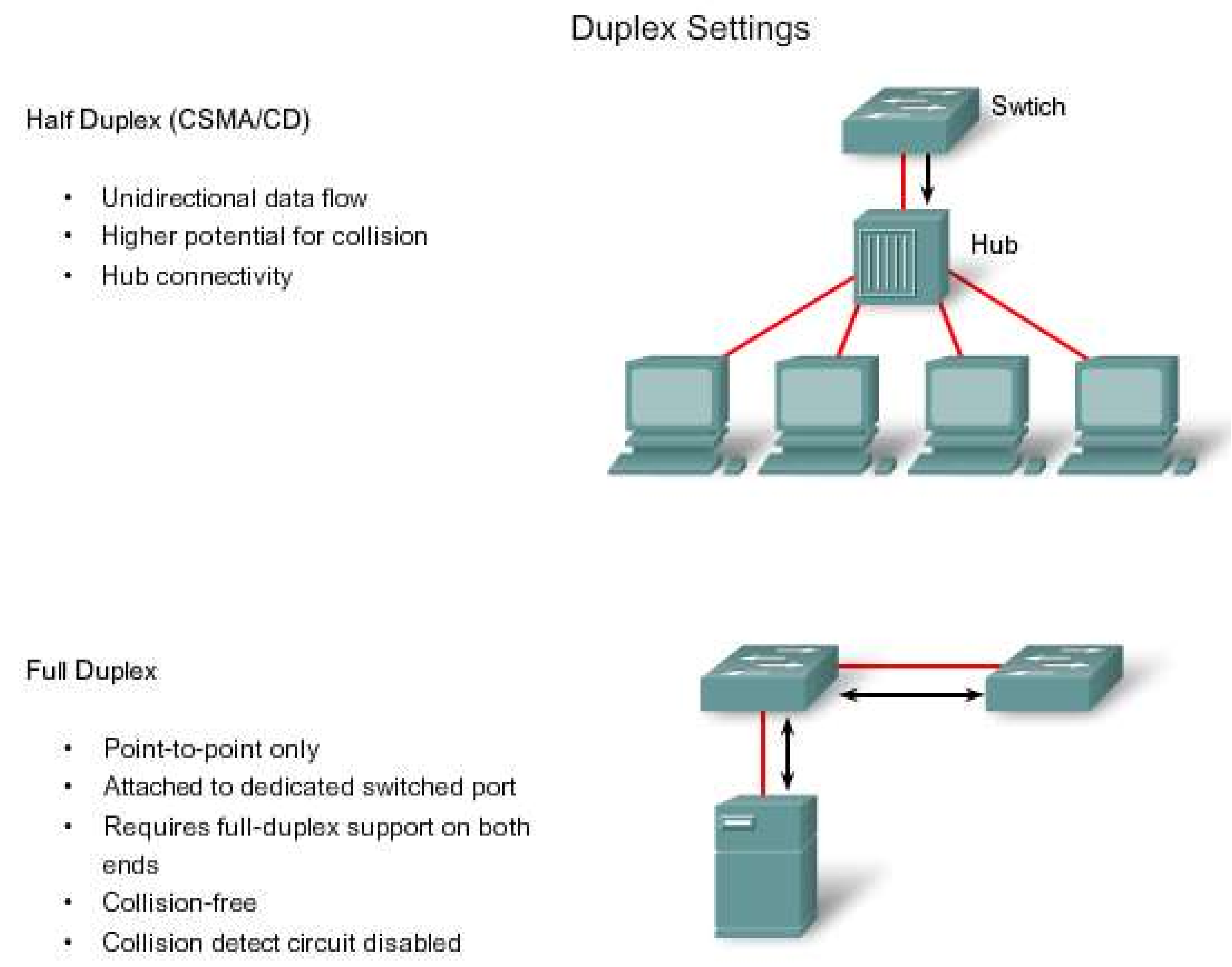
CSMA/CD

Carrier Sense Multiple Access Collision Detection (CSMA/CD)



Waits for a specified time after—signal passes. Try again later.

Half- i Full-duplex mod



Duplex Settings

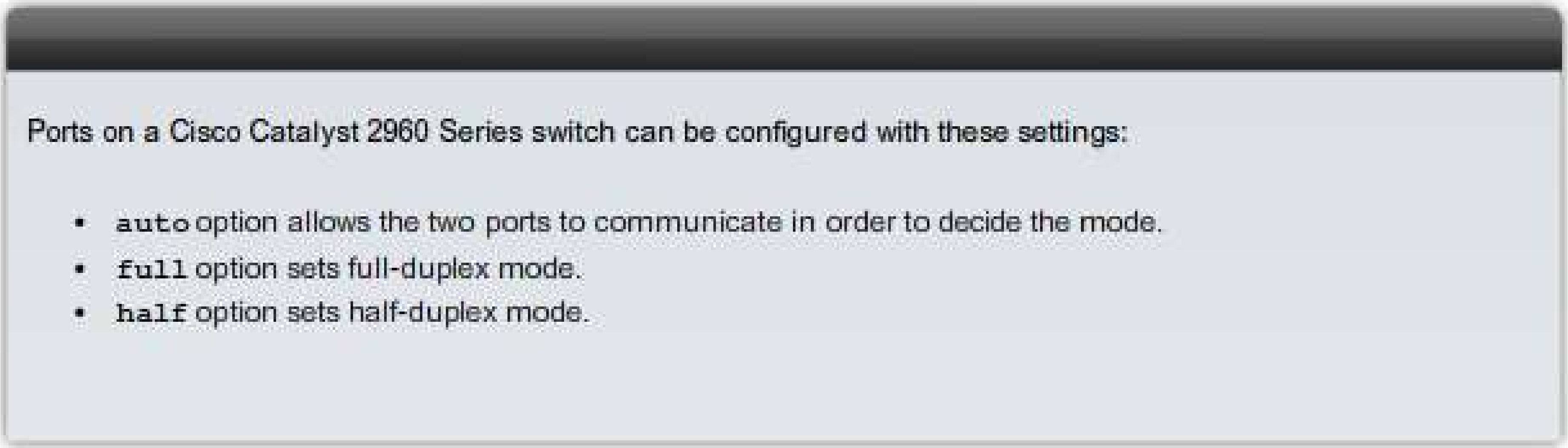
Half Duplex (CSMA/CD)

- Unidirectional data flow
- Higher potential for collision
- Hub connectivity

Full Duplex

- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision-free
- Collision detect circuit disabled

Podešavanje duplex-moda na sviču



Ports on a Cisco Catalyst 2960 Series switch can be configured with these settings:

- `auto` option allows the two ports to communicate in order to decide the mode.
- `full` option sets full-duplex mode.
- `half` option sets half-duplex mode.

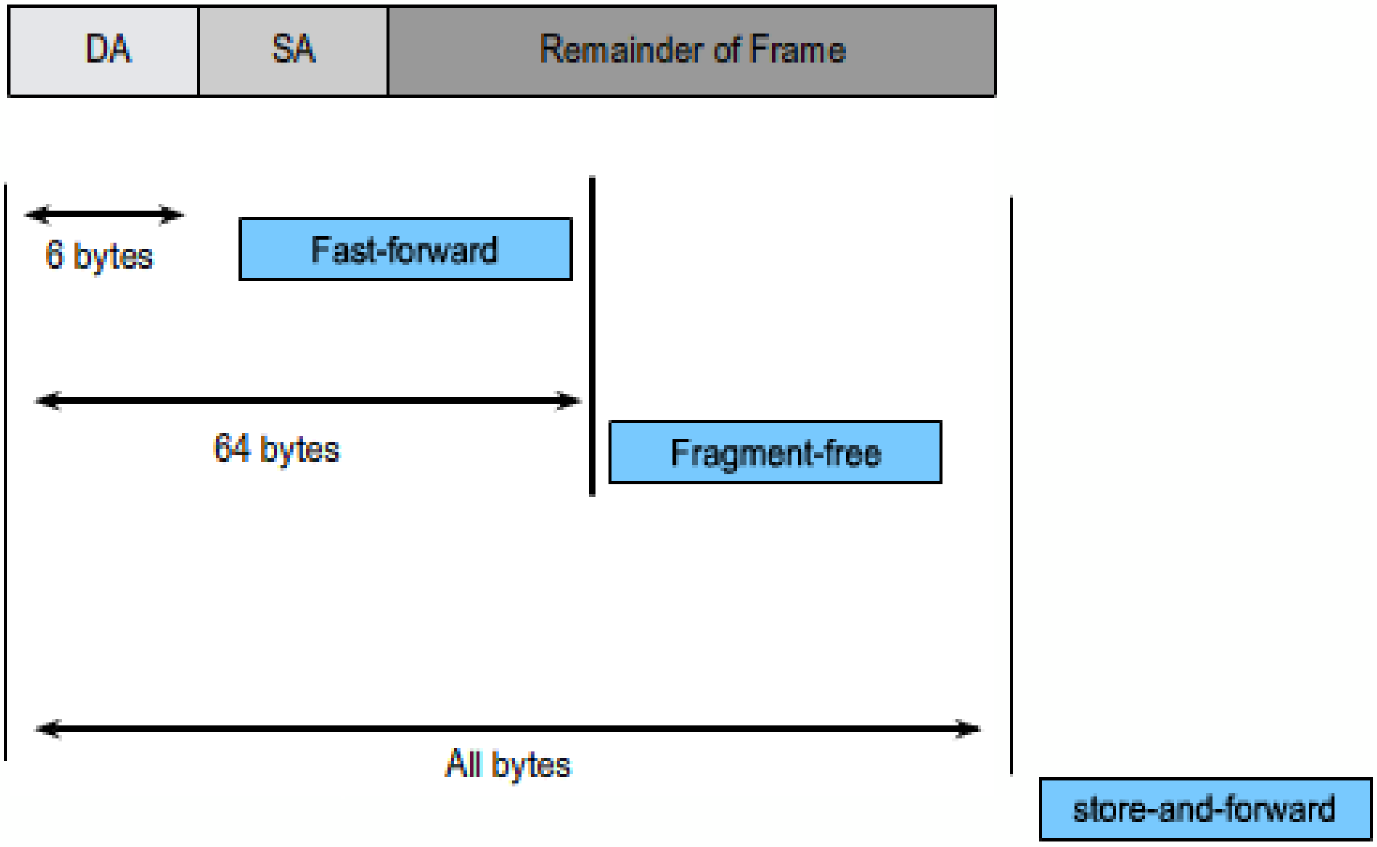
Tehnike za prosleđivanje frejmova

- Store-and-forward
  - Ceo frejm se pamti u bafer prilikom dolaska frejma, računa se CRC, pa tek ako je CRC u redu, onda se prosleđuje frejm. Prednost: ne opterećuje drugi kolizioni domen ako je do bilo kakve greške. Mana: veća latencija.
- Cut-through
  - Svič počinje da šalje frejm čim dobije odredišnu MAC adresu i proveri MAC tabelu. Prednost: manja latencija. Mana: Mogućnost prosleđivanja neispravnih frejmova.
- Fragment free
  - Kompromis: Baferuju se samo prva 64 bajta. Na ovaj način se ne proverava sve, a sprečava prosleđivanje u slučaju nastanka kolizije.

A store-and-forward switch receives the entire frame, computes the CRC, and checks the frame length. If the CRC and frame length are valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.

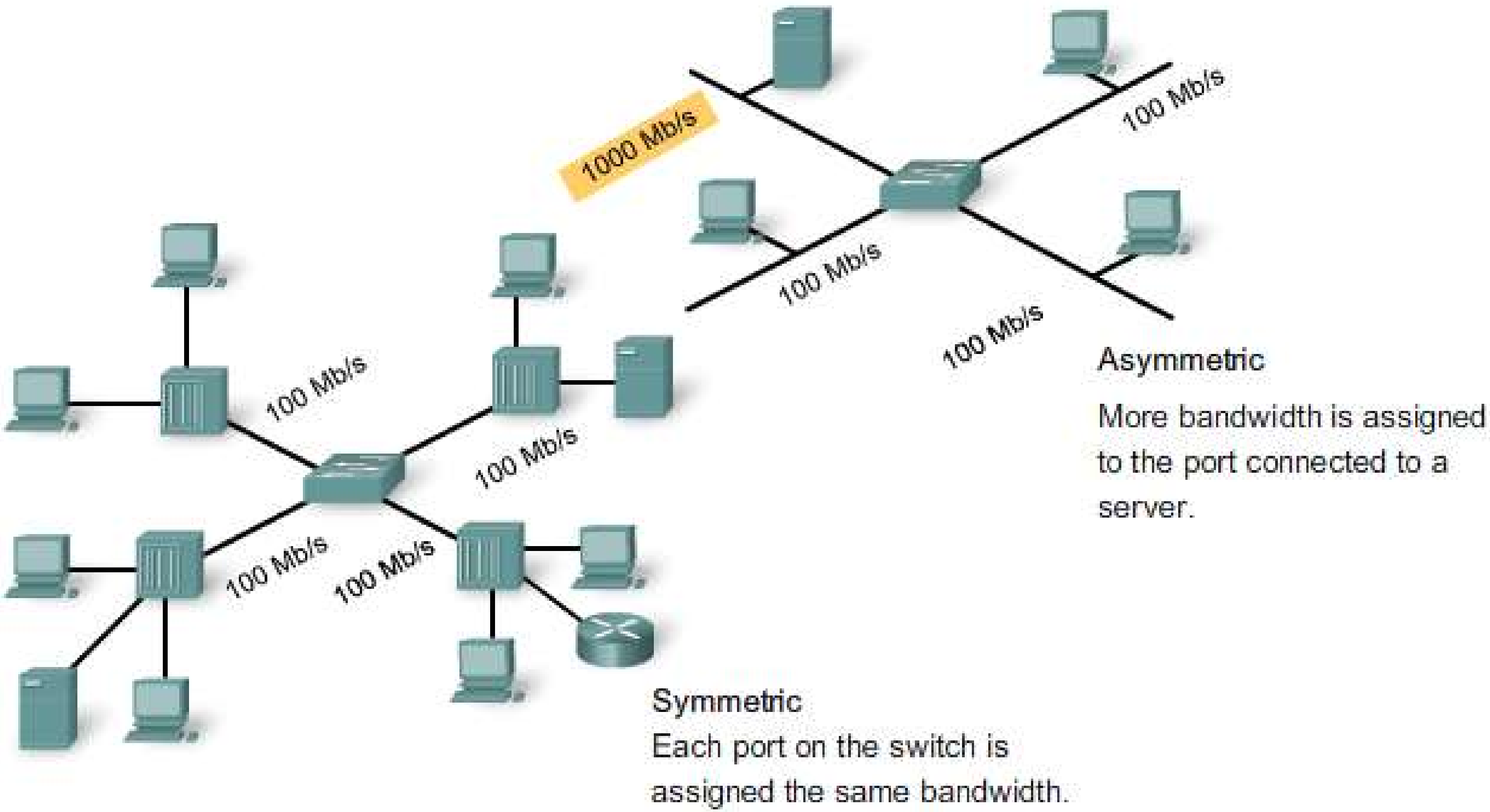
A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

Tehnike za prosleđivanje frejmova



Simetrični i asimetrični svičevi

Symmetric and Asymmetric Switching



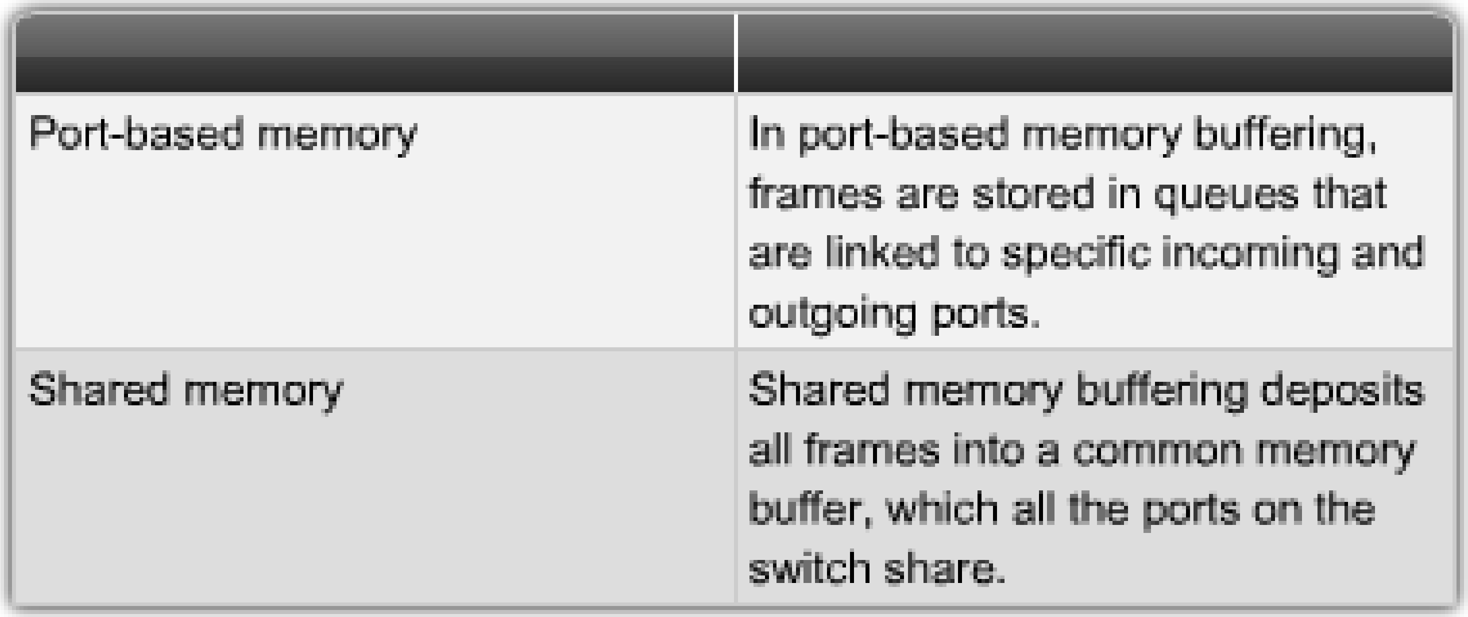
Asymmetric

More bandwidth is assigned to the port connected to a server.

Symmetric

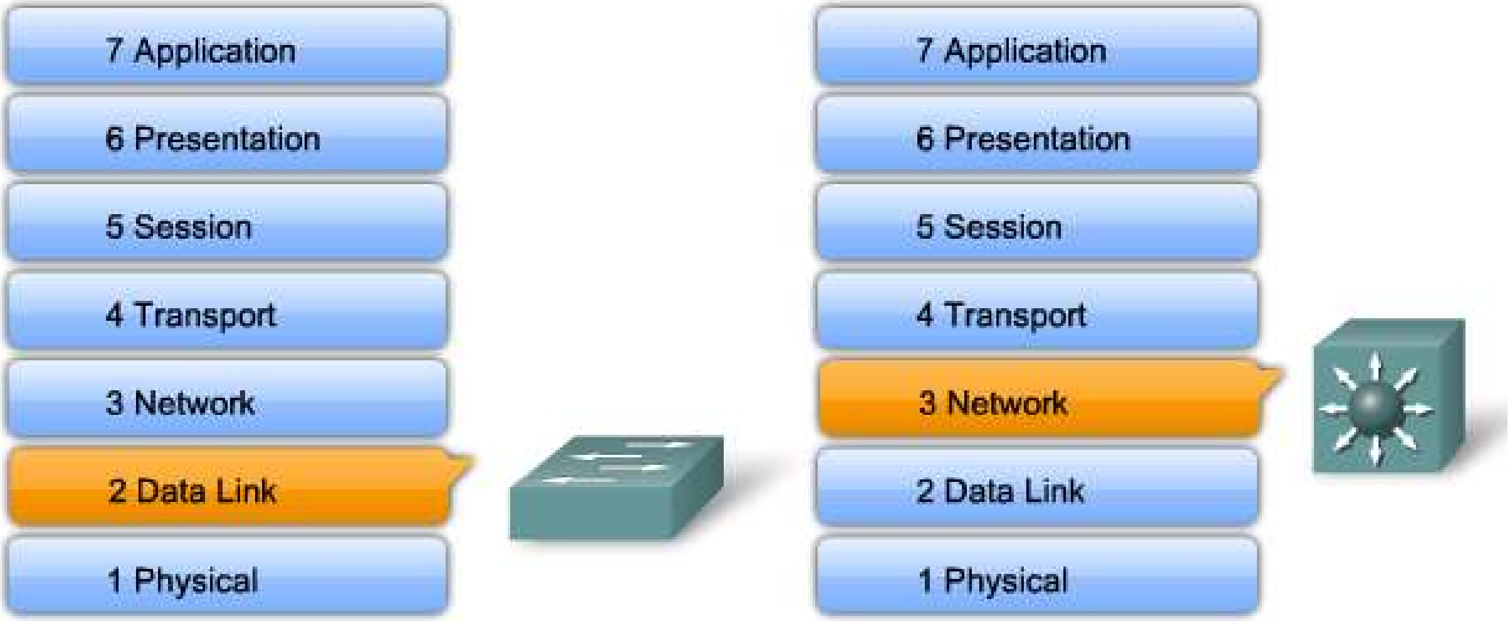
Each port on the switch is assigned the same bandwidth.

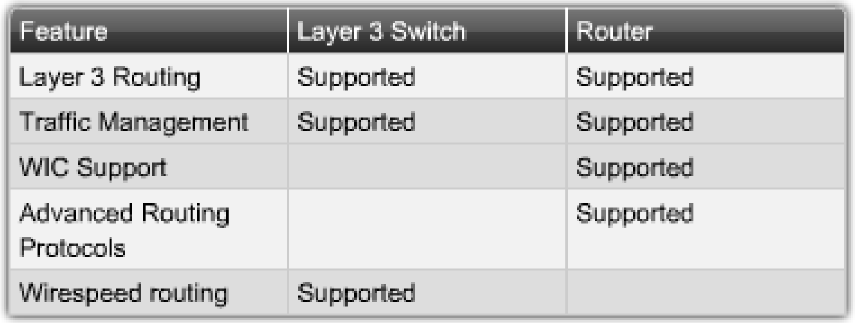
Tehnike baferovanja



Port-based memory	In port-based memory buffering, frames are stored in queues that are linked to specific incoming and outgoing ports.
Shared memory	Shared memory buffering deposits all frames into a common memory buffer, which all the ports on the switch share.

L2 i L3svičevi

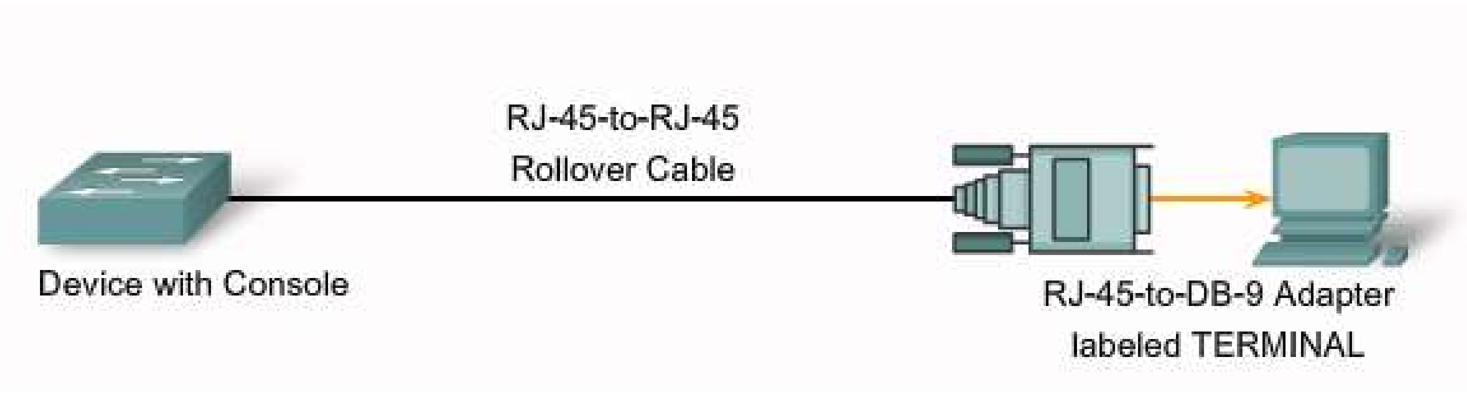


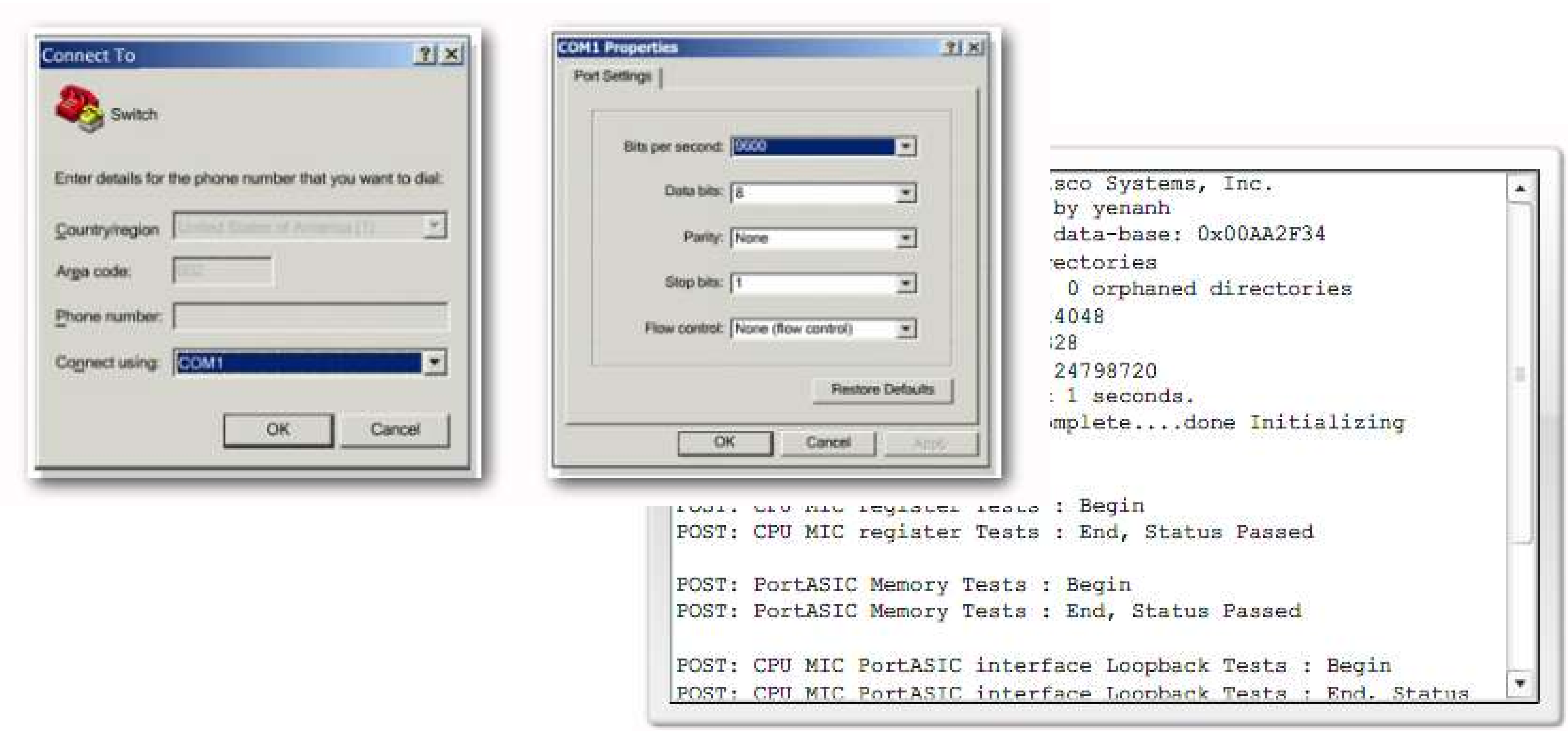


Feature	Layer 3 Switch	Router
Layer 3 Routing	Supported	Supported
Traffic Management	Supported	Supported
WIC Support		Supported
Advanced Routing Protocols		Supported
Wirespeed routing	Supported	

Navigacija kroz komandni interfejs upravljivih Cisco svičeva i osnovna podešavanja

Povezivanje konzole uređaja (sviča)





Switch

Enter details for the phone number that you want to dial:

Country/region: United States of America (1)

Area code:

Phone number:

Connect using: COM1

Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None (flow control)

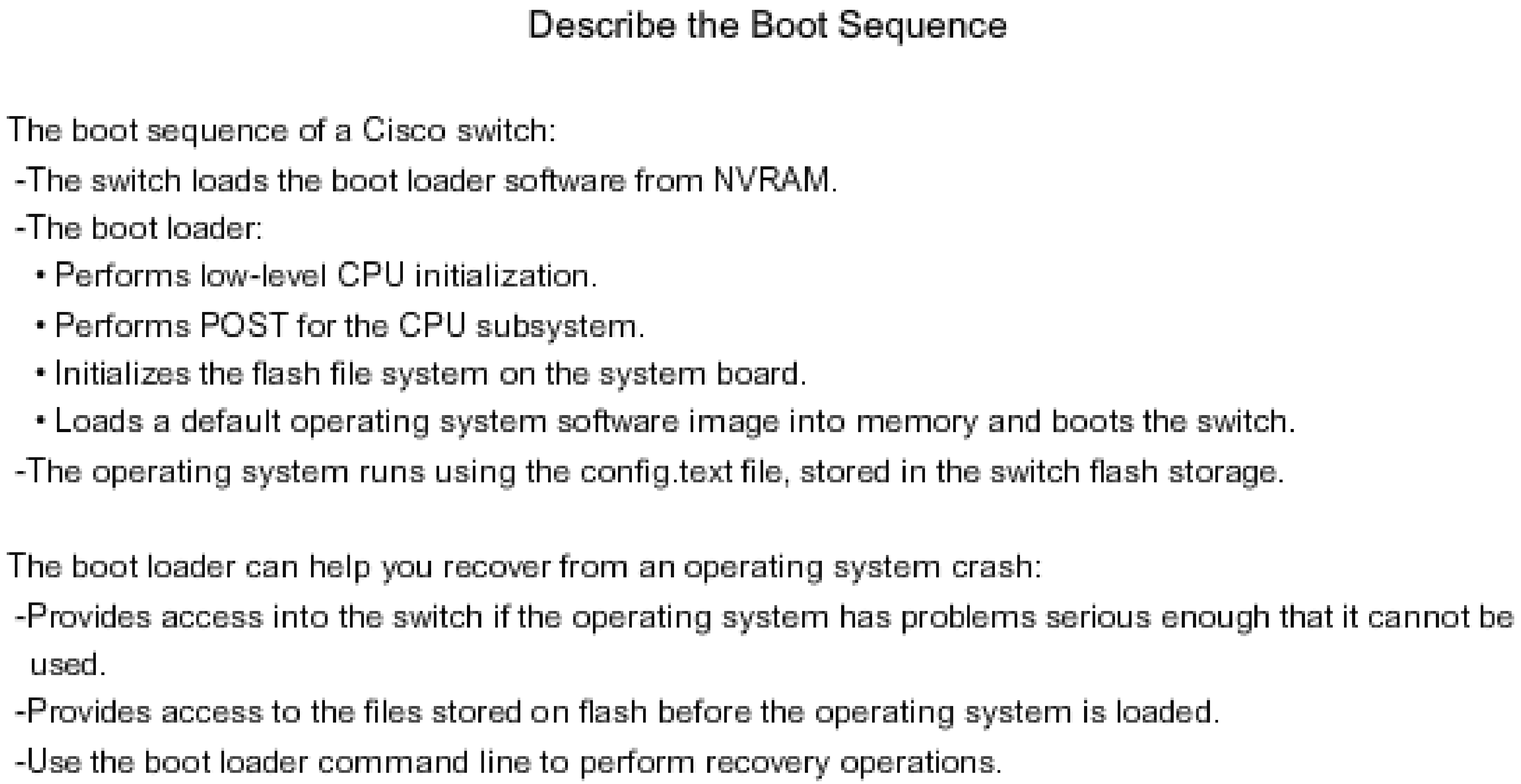
```
sco Systems, Inc.
by yenanh
data-base: 0x00AA2F34
ectories
 0 orphaned directories
4048
28
24798720
 1 seconds.
mplete....done Initializing

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed

POST: CPU MIC PortASIC interface Loopback Tests : Begin
POST: CPU MIC PortASIC interface Loopback Tests : End, Status
```

Boot sekvenca sviča



Describe the Boot Sequence

The boot sequence of a Cisco switch:

-The switch loads the boot loader software from NVRAM.

-The boot loader:

- Performs low-level CPU initialization.
- Performs POST for the CPU subsystem.
- Initializes the flash file system on the system board.
- Loads a default operating system software image into memory and boots the switch.

-The operating system runs using the config.text file, stored in the switch flash storage.

The boot loader can help you recover from an operating system crash:

-Provides access into the switch if the operating system has problems serious enough that it cannot be used.

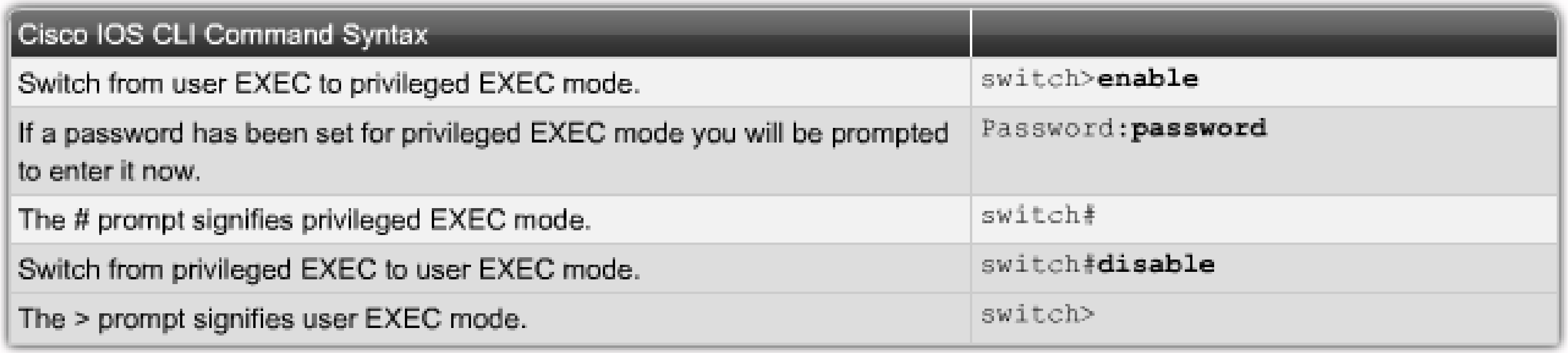
-Provides access to the files stored on flash before the operating system is loaded.

-Use the boot loader command line to perform recovery operations.

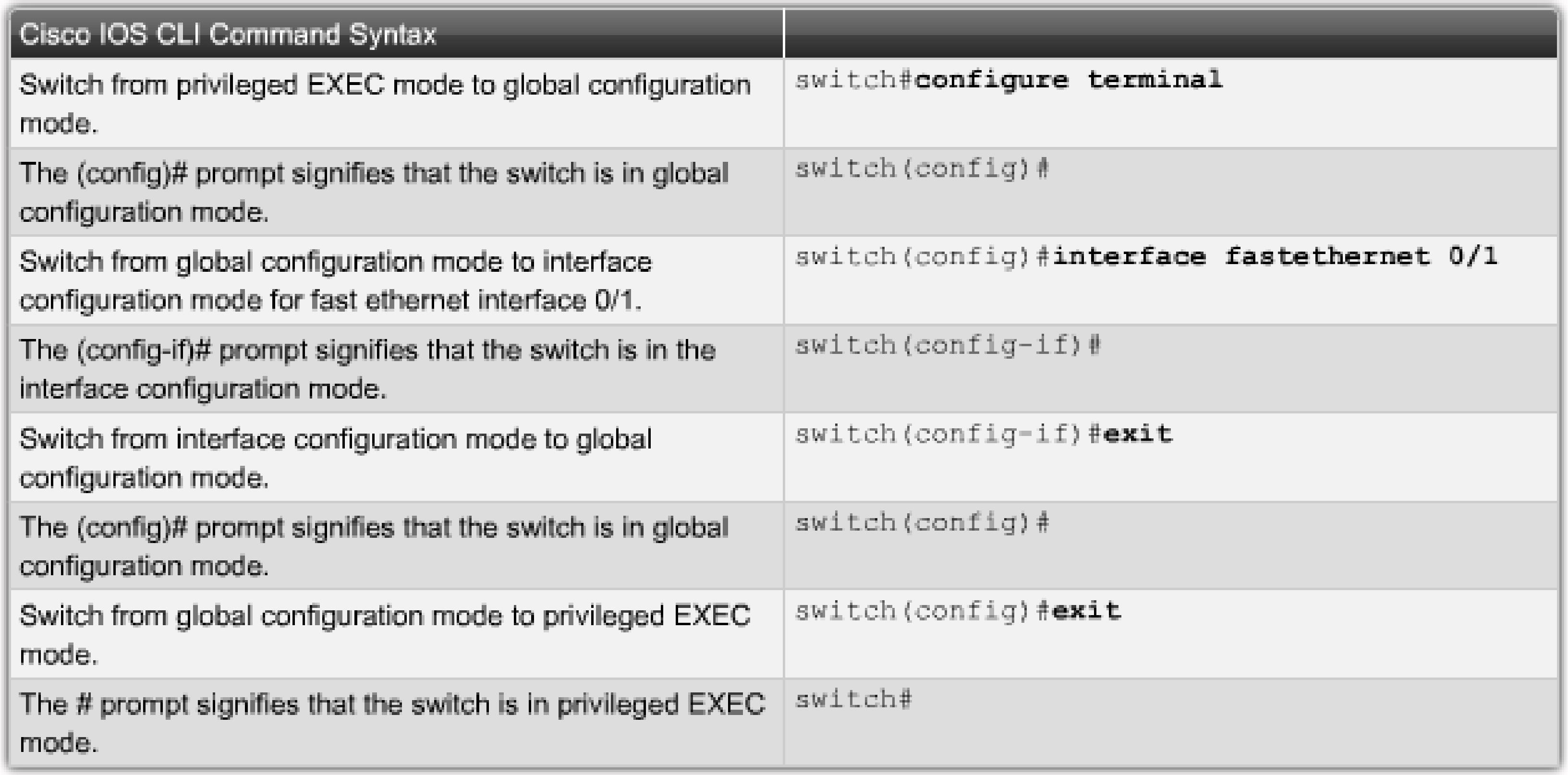
Komandni modovi

- Korisnički
  - Switch>
- Privilegovani
  - Switch#
- Mod za konfiguraciju uređaja
  - Switch(config)#
- Mod za podešavanje interfejsa
  - Switch(config-if)#
- Dodatni pod-modovi
  - ...

Kretanje kroz komandne modove

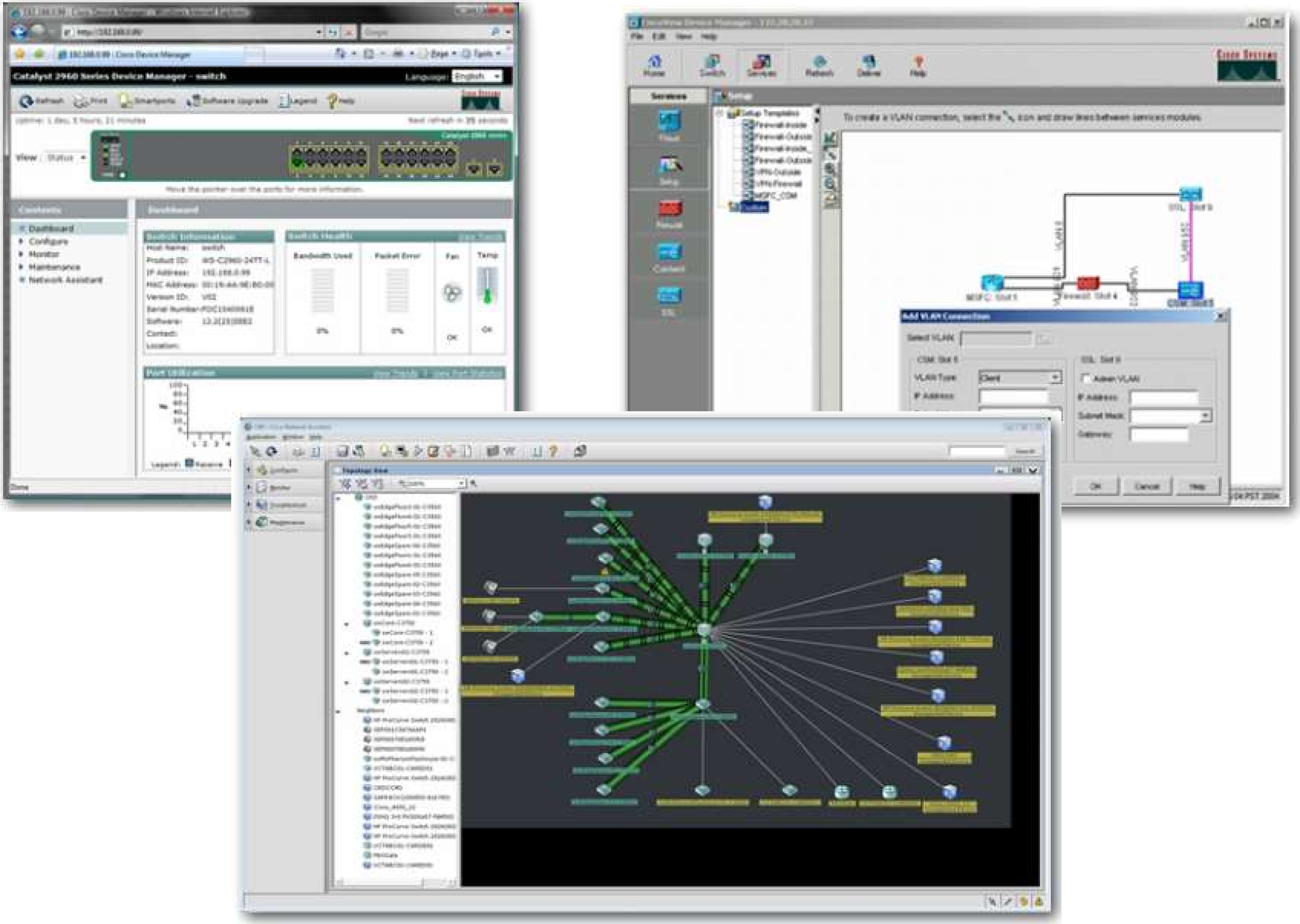


Cisco IOS CLI Command Syntax	
Switch from user EXEC to privileged EXEC mode.	switch>**enable**
If a password has been set for privileged EXEC mode you will be prompted to enter it now.	Password:**password**
The # prompt signifies privileged EXEC mode.	switch#
Switch from privileged EXEC to user EXEC mode.	switch#**disable**
The > prompt signifies user EXEC mode.	switch>

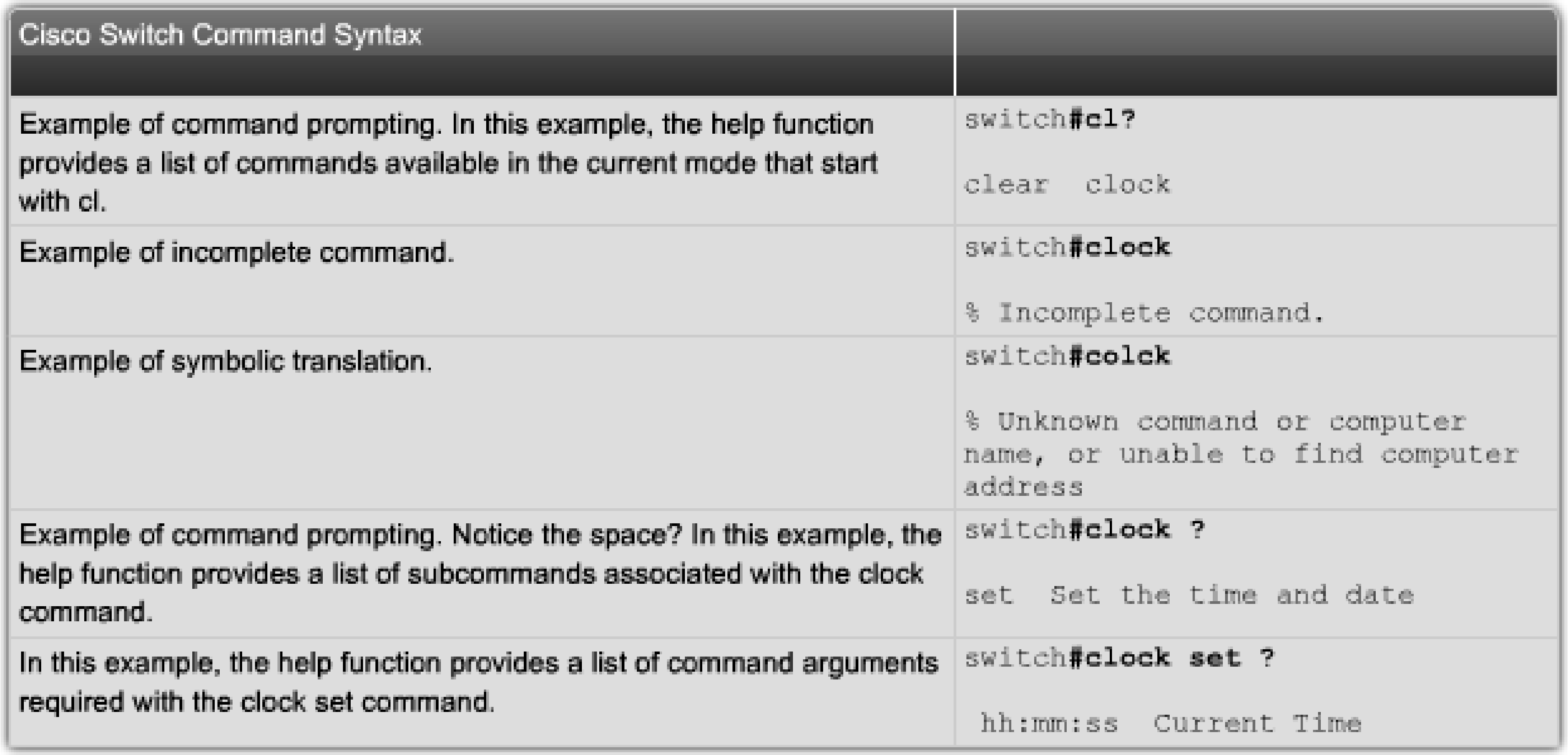


Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	switch#**configure terminal**
The (config)# prompt signifies that the switch is in global configuration mode.	switch(config)#
Switch from global configuration mode to interface configuration mode for fast ethernet interface 0/1.	switch(config)#**interface fastethernet 0/1**
The (config-if)# prompt signifies that the switch is in the interface configuration mode.	switch(config-if)#
Switch from interface configuration mode to global configuration mode.	switch(config-if)#**exit**
The (config)# prompt signifies that the switch is in global configuration mode.	switch(config)#
Switch from global configuration mode to privileged EXEC mode.	switch(config)#**exit**
The # prompt signifies that the switch is in privileged EXEC mode.	switch#

Dodatne mogućnosti za konfiguraciju



Kontekst-senzitivni help



Cisco Switch Command Syntax	

Example of command prompting. In this example, the help function provides a list of commands available in the current mode that start with cl.	`switch#cl?`
	
	`clear  clock`

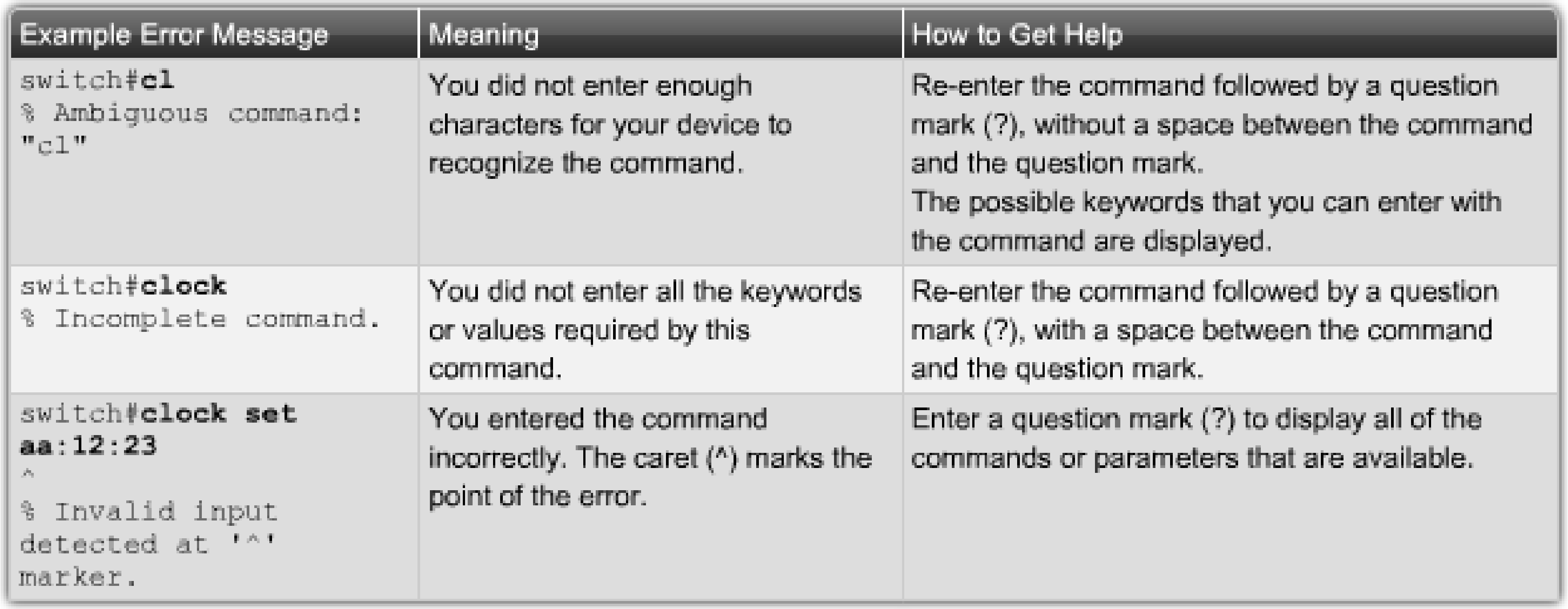
Example of incomplete command.	`switch#clock`
	
	`% Incomplete command.`

Example of symbolic translation.	`switch#colck`
	
	`% Unknown command or computer name, or unable to find computer address`

Example of command prompting. Notice the space? In this example, the help function provides a list of subcommands associated with the clock command.	`switch#clock ?`
	
	`set  Set the time and date`

In this example, the help function provides a list of command arguments required with the clock set command.	`switch#clock set ?`
	
	`hh:mm:ss  Current Time`

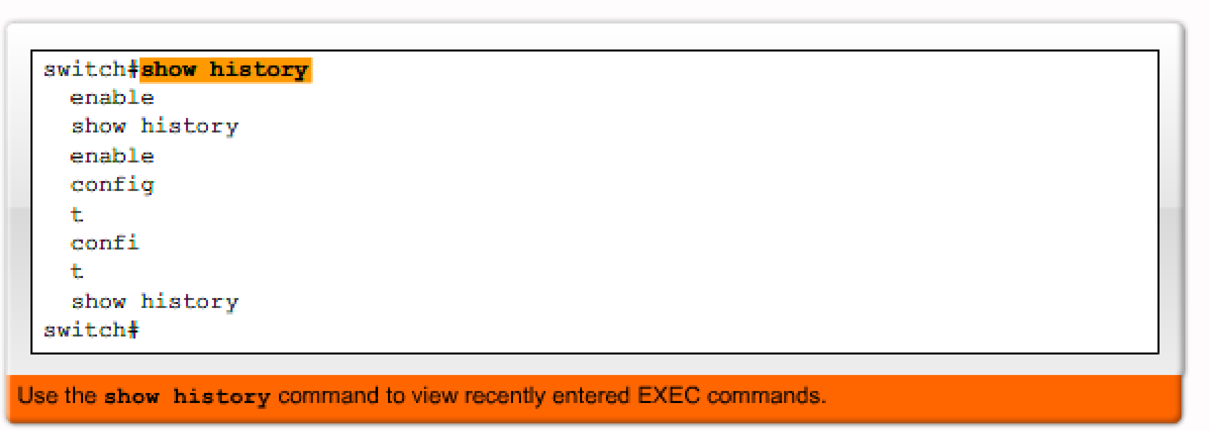
Poruke o greškama



Example Error Message	Meaning	How to Get Help
switch#**cl** % Ambiguous command: "cl"	You did not enter enough characters for your device to recognize the command.	Re-enter the command followed by a question mark (?), without a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
switch#**clock** % Incomplete command.	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (?), with a space between the command and the question mark.
switch#**clock set** **aa:12:23** ^ % Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands or parameters that are available.

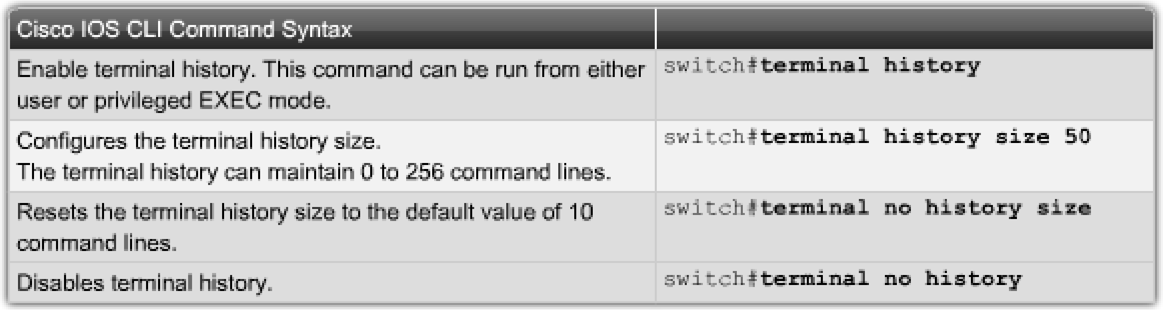
Prethodno unošene naredbe

- Strelicama gore-dole može se dobiti neka od prethodno unešenih naredbi, da bi se “ubrzalo” unošenje, ako je potrebno ponoviti naredbu, ili nešto modifikovati
- Sadržaj bafera se može prikazati, a može mu se i promeniti veličina



```
switch#show history
  enable
  show history
  enable
  config
  t
  confi
  t
  show history
switch#
```

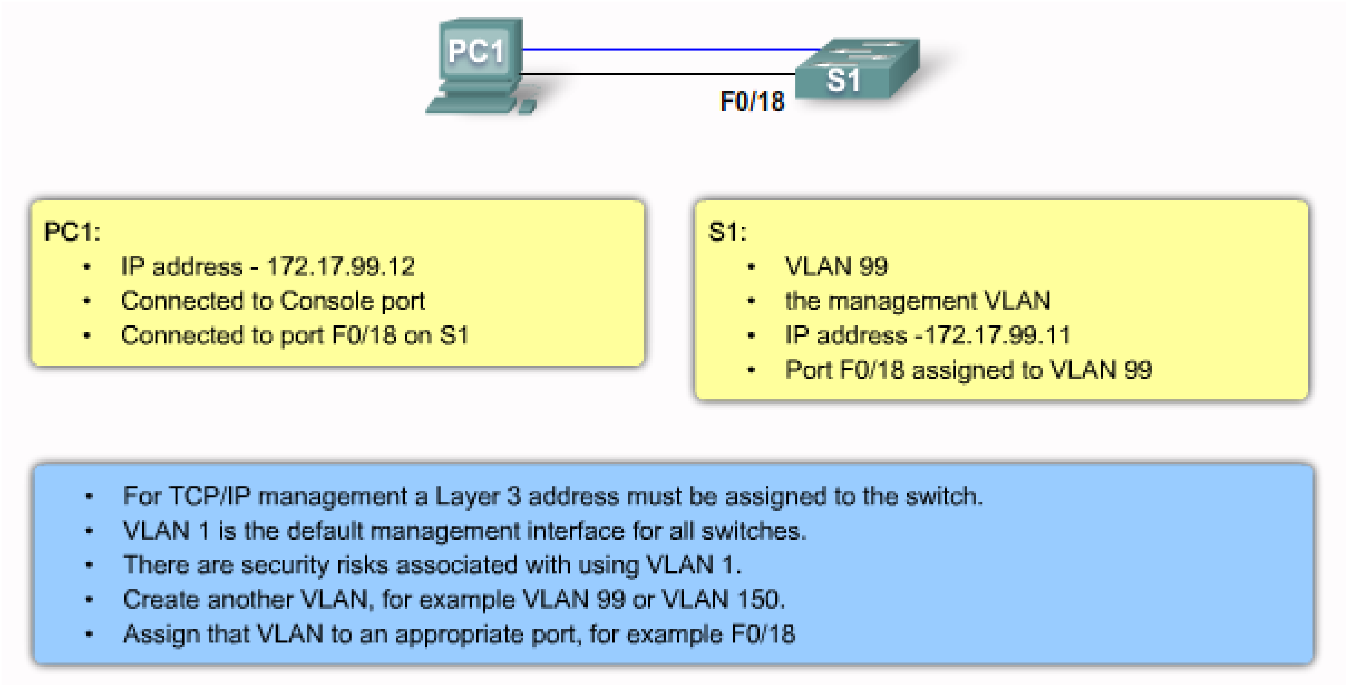
Use the **show history** command to view recently entered EXEC commands.



Cisco IOS CLI Command Syntax	
Enable terminal history. This command can be run from either user or privileged EXEC mode.	switch#**terminal history**
Configures the terminal history size. The terminal history can maintain 0 to 256 command lines.	switch#**terminal history size 50**
Resets the terminal history size to the default value of 10 command lines.	switch#**terminal no history size**
Disables terminal history.	switch#**terminal no history**

Osnovno podešavanje – IP adresa

- IP adresa se na sviču koristi da bi se omogućio pristup komandnom interfejcu (CLI) preko TCP/IP protokola sa udaljene lokacije
- Protokol koji se u tom slučaju koristi je *telnet* protokol aplikativnog nivoa na TCP portu 23

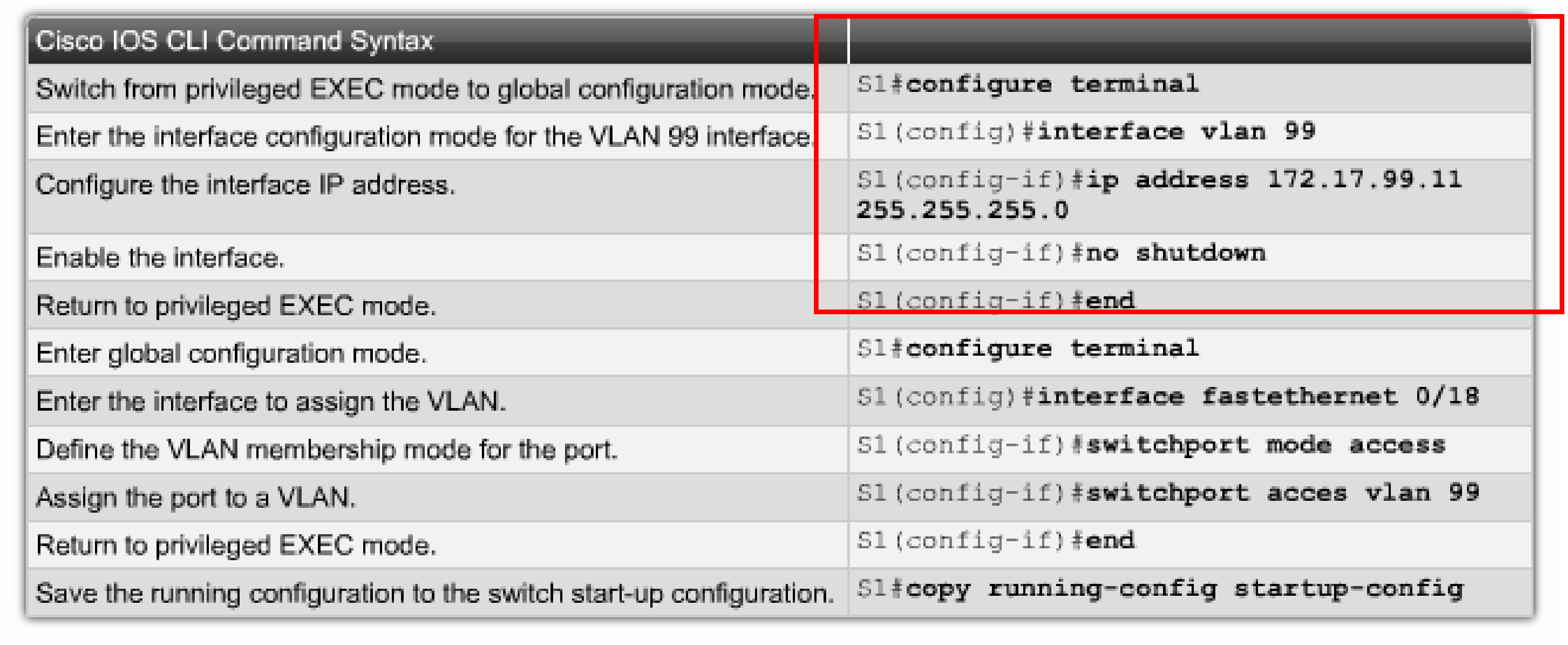


PC1:
- IP address - 172.17.99.12
- Connected to Console port
- Connected to port F0/18 on S1

S1:
- VLAN 99
- the management VLAN
- IP address -172.17.99.11
- Port F0/18 assigned to VLAN 99

- For TCP/IP management a Layer 3 address must be assigned to the switch.
- VLAN 1 is the default management interface for all switches.
- There are security risks associated with using VLAN 1.
- Create another VLAN, for example VLAN 99 or VLAN 150.
- Assign that VLAN to an appropriate port, for example F0/18

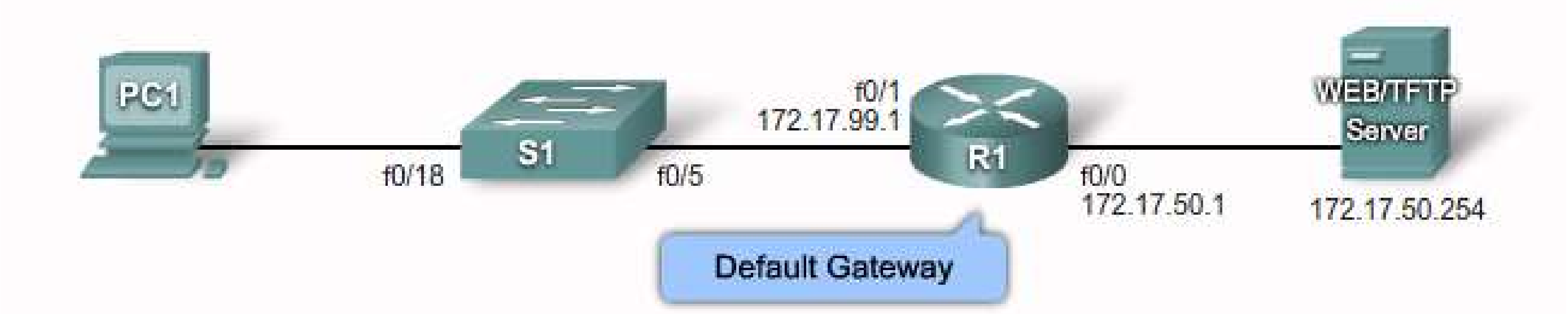
Osnovno podešavanje – IP adresa

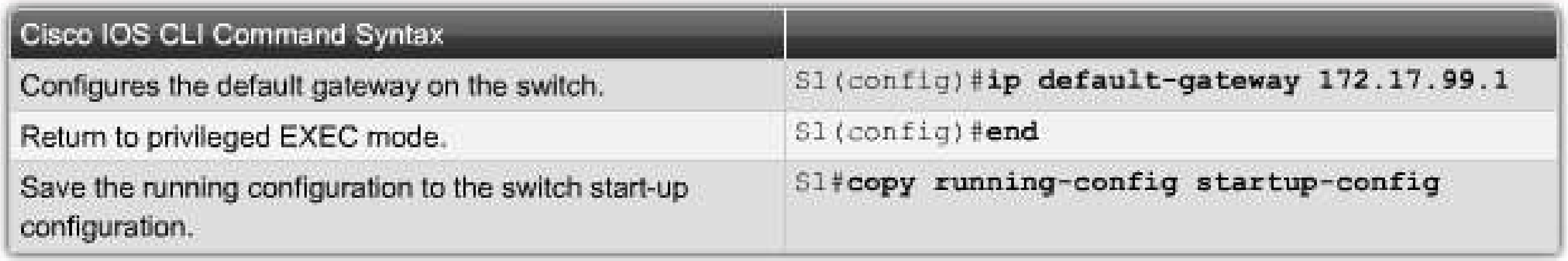


Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#**configure terminal**
Enter the interface configuration mode for the VLAN 99 interface.	S1(config)#**interface vlan 99**
Configure the interface IP address.	S1(config-if)#**ip address 172.17.99.11 255.255.255.0**
Enable the interface.	S1(config-if)#**no shutdown**
Return to privileged EXEC mode.	S1(config-if)#**end**
Enter global configuration mode.	S1#**configure terminal**
Enter the interface to assign the VLAN.	S1(config)#**interface fastethernet 0/18**
Define the VLAN membership mode for the port.	S1(config-if)#**switchport mode access**
Assign the port to a VLAN.	S1(config-if)#**switchport acces vlan 99**
Return to privileged EXEC mode.	S1(config-if)#**end**
Save the running configuration to the switch start-up configuration.	S1#**copy running-config startup-config**

Osnovno podešavanje – gateway

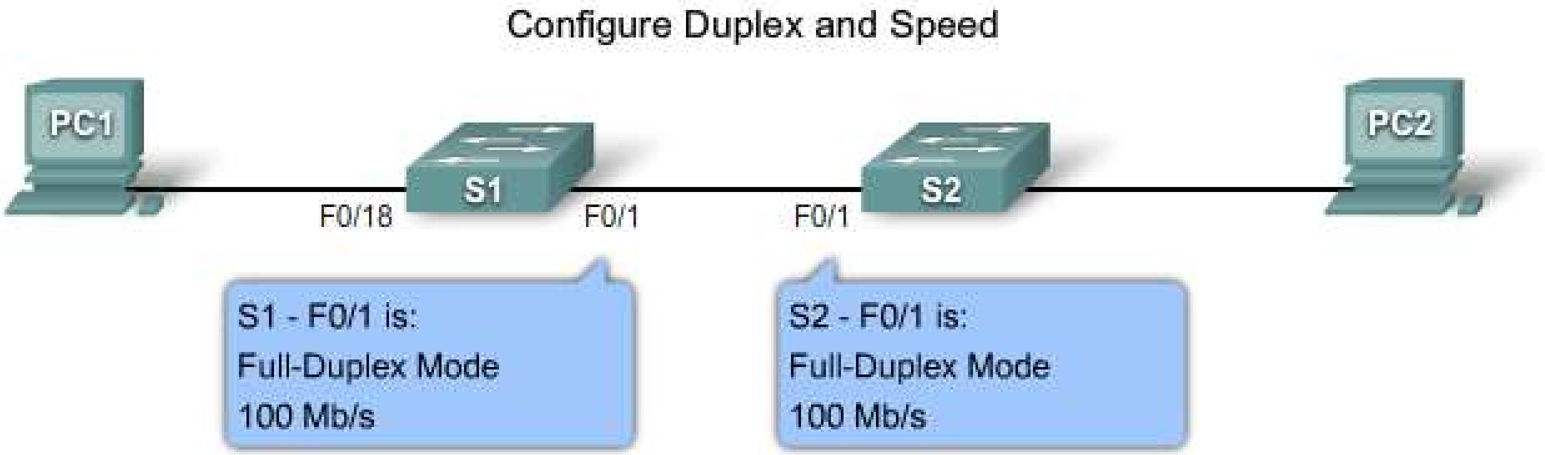
- Uloga gateway-a na sviču je ista kao i kod “običnog” računara: pristup udaljenim mrežama.





Cisco IOS CLI Command Syntax	
Configures the default gateway on the switch.	`S1(config)#ip default-gateway 172.17.99.1`
Return to privileged EXEC mode.	`S1(config)#end`
Save the running configuration to the switch start-up configuration.	`S1#copy running-config startup-config`

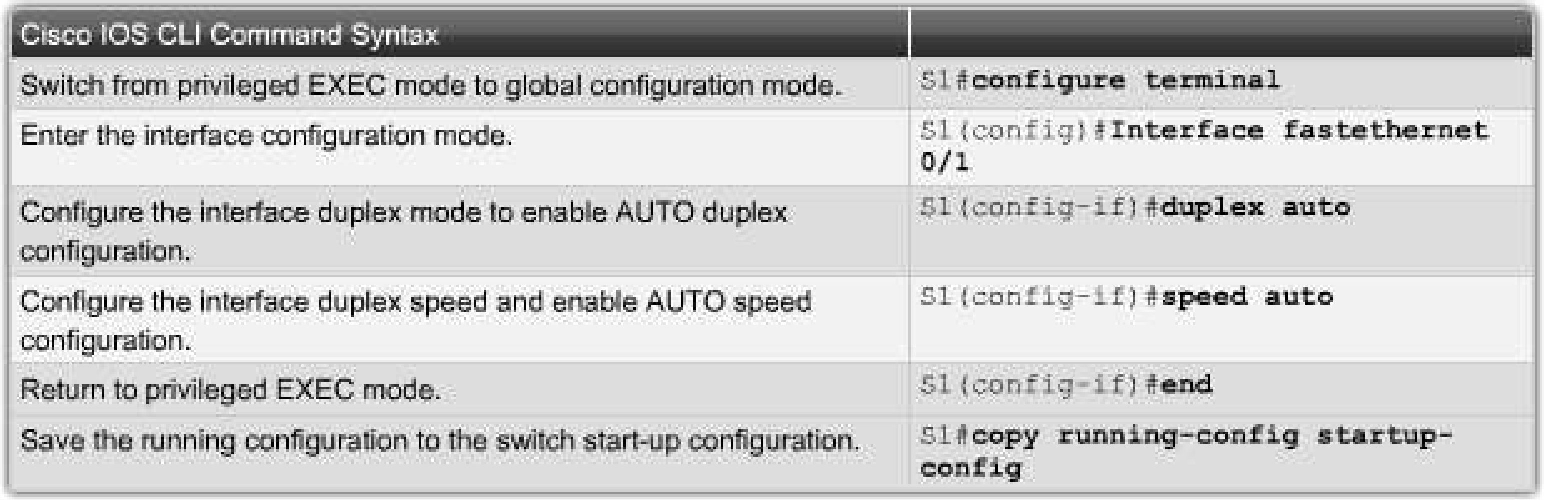
Konfiguracija dupleksa i brzine



Configure Duplex and Speed

S1 - F0/1 is:
Full-Duplex Mode
100 Mb/s

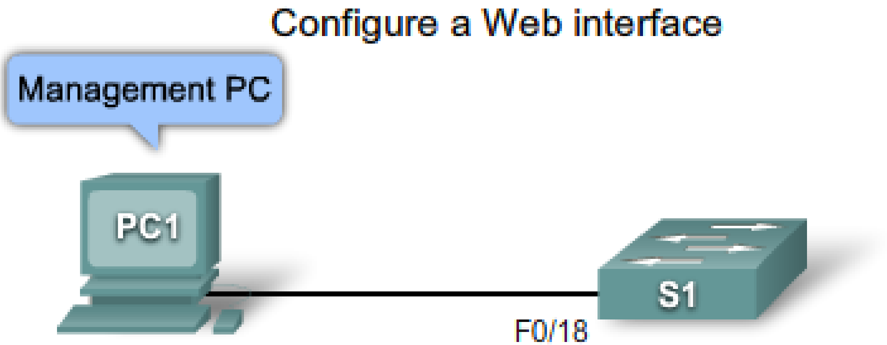
S2 - F0/1 is:
Full-Duplex Mode
100 Mb/s

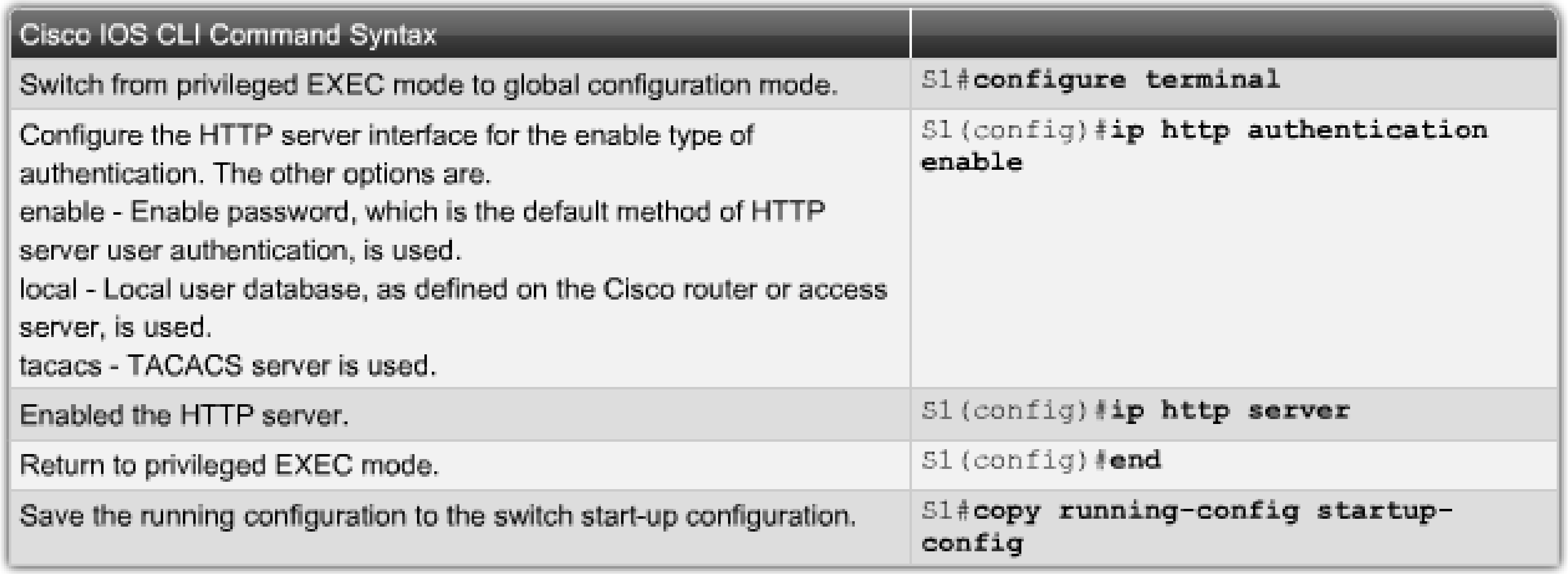


Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#configure terminal`
Enter the interface configuration mode.	`S1(config)#Interface fastethernet 0/1`
Configure the interface duplex mode to enable AUTO duplex configuration.	`S1(config-if)#duplex auto`
Configure the interface duplex speed and enable AUTO speed configuration.	`S1(config-if)#speed auto`
Return to privileged EXEC mode.	`S1(config-if)#end`
Save the running configuration to the switch start-up configuration.	`S1#copy running-config startup-config`

Omogućavanje pristupa preko web-a

- Na sviču se može pokrenuti veb server


Configure a Web interface



Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#configure terminal`
Configure the HTTP server interface for the enable type of authentication. The other options are. enable - Enable password, which is the default method of HTTP server user authentication, is used. local - Local user database, as defined on the Cisco router or access server, is used. tacacs - TACACS server is used.	`S1(config)#ip http authentication enable`
Enabled the HTTP server.	`S1(config)#ip http server`
Return to privileged EXEC mode.	`S1(config)#end`
Save the running configuration to the switch start-up configuration.	`S1#copy running-config startup-config`

MAC-address tabela

Prikaz sadržaja

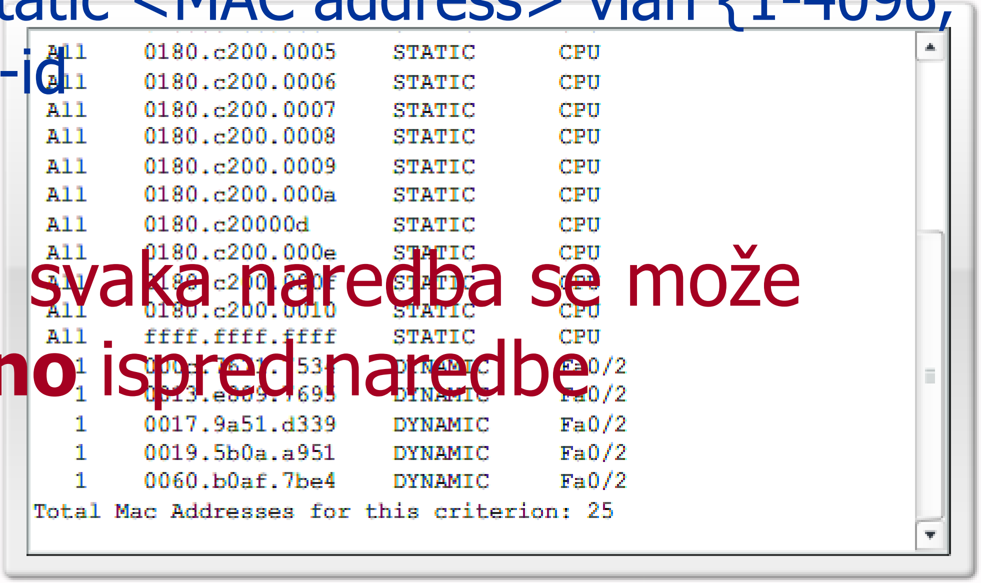
- switch#show mac-address-table

Statičko dodavanje zapisa

- mac-address-table static <MAC address> vlan {1-4096, ALL} interface *interface-id*

Brisanje zapisa

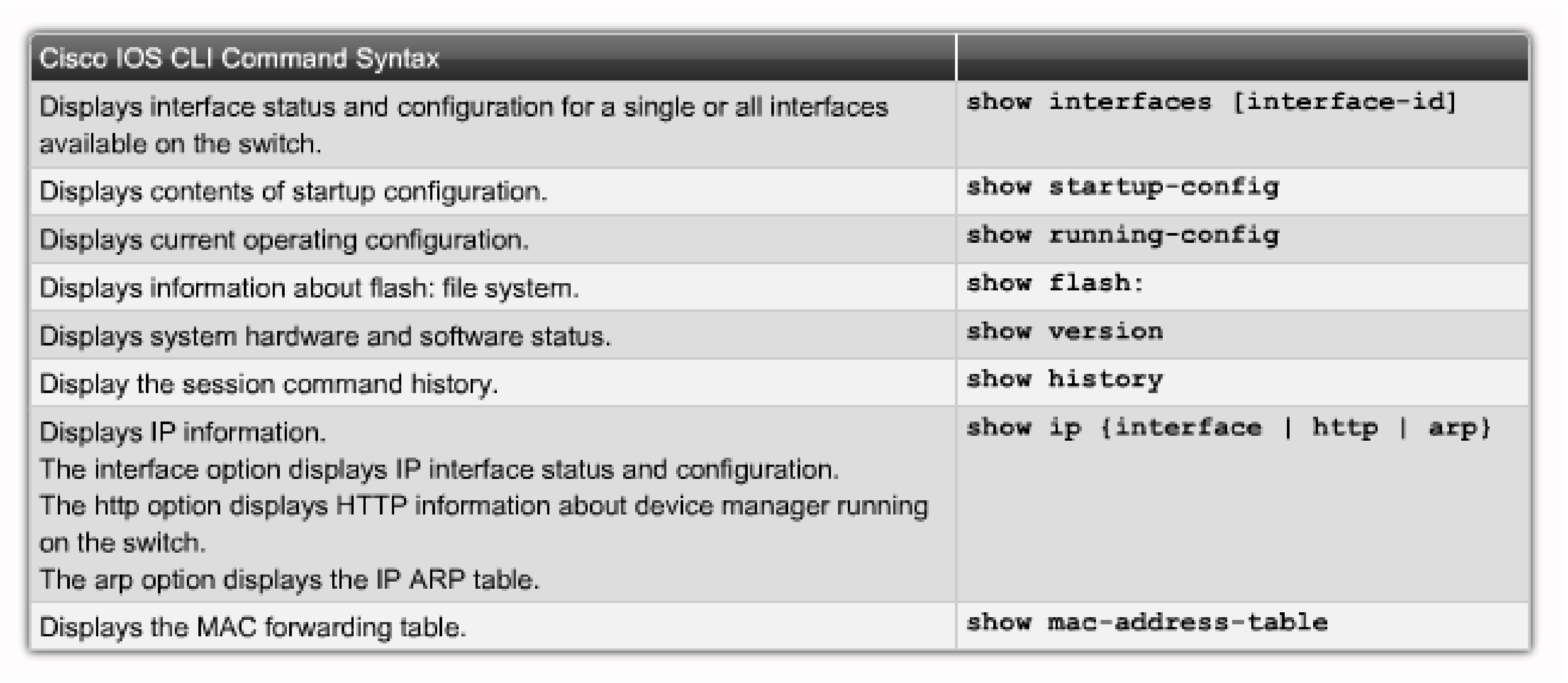
- no mac-address-table static <MAC address> vlan {1-4096, ALL} interface interface-id



```
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c20000d      STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    [illegible]       DYNAMIC     Fa0/2
   1    [illegible]       DYNAMIC     Fa0/2
   1    0017.9a51.d339    DYNAMIC     Fa0/2
   1    0019.5b0a.a951    DYNAMIC     Fa0/2
   1    0060.b0af.7be4    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 25
```

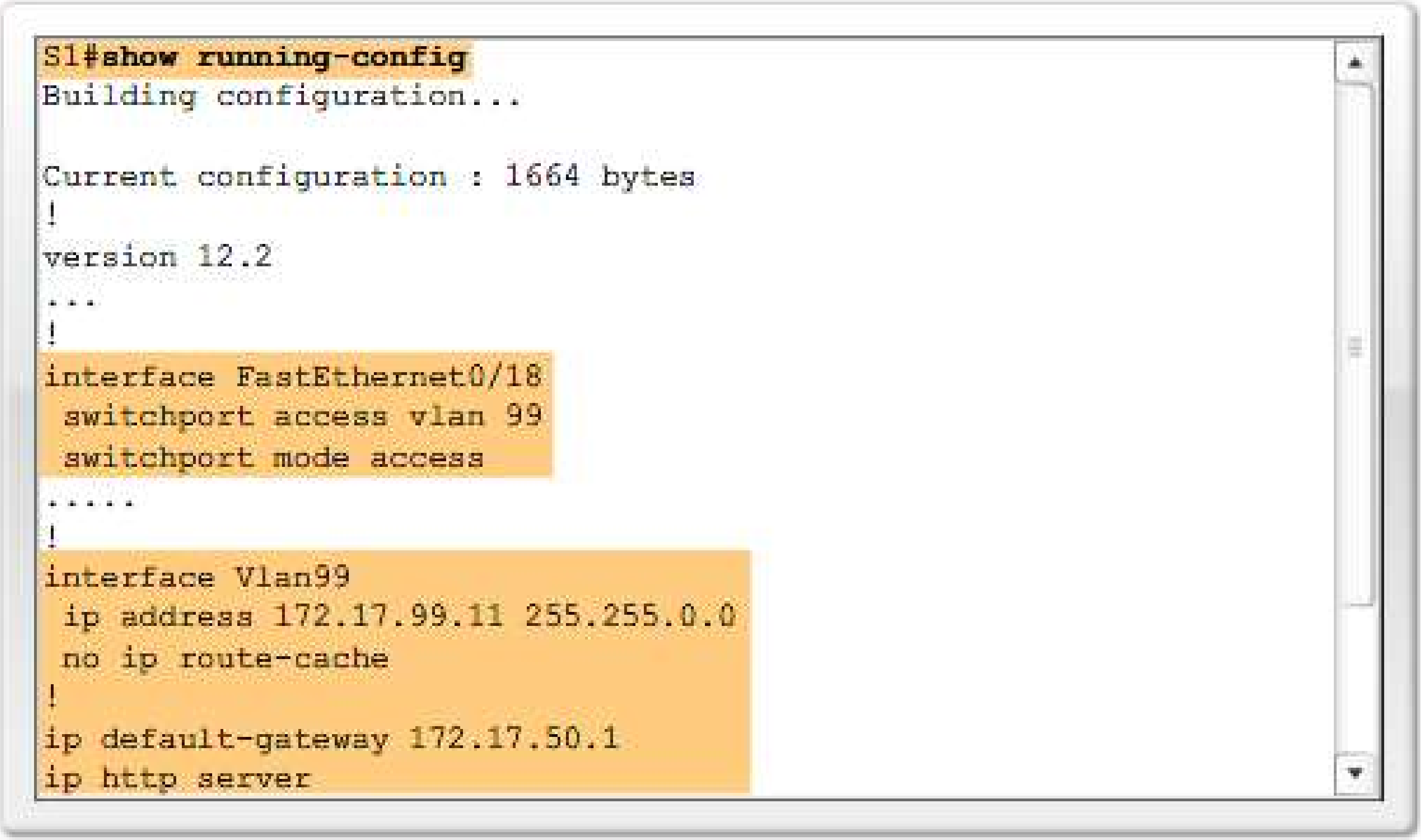
Generalna napomena: svaka naredba se može poništiti dodavanjem **no** ispred naredbe

Provera konfiguracije i statusa



Cisco IOS CLI Command Syntax	
Displays interface status and configuration for a single or all interfaces available on the switch.	`show interfaces [interface-id]`
Displays contents of startup configuration.	`show startup-config`
Displays current operating configuration.	`show running-config`
Displays information about flash: file system.	`show flash:`
Displays system hardware and software status.	`show version`
Display the session command history.	`show history`
Displays IP information. The interface option displays IP interface status and configuration. The http option displays HTTP information about device manager running on the switch. The arp option displays the IP ARP table.	`show ip {interface | http | arp}`
Displays the MAC forwarding table.	`show mac-address-table`

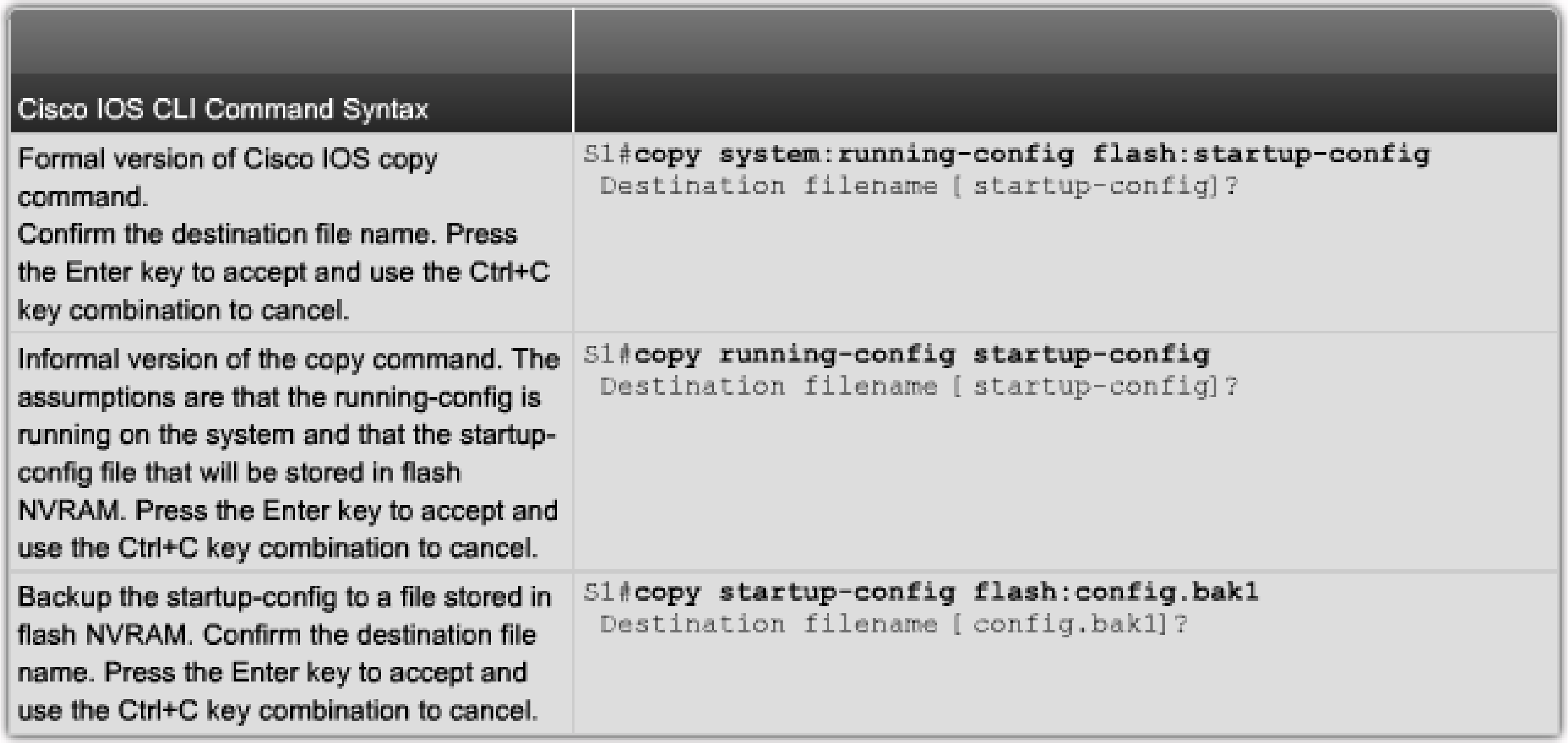
“Running “ konfiguracija



```
S1#show running-config
Building configuration...

Current configuration : 1664 bytes
!
version 12.2
...
!
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
.....
!
interface Vlan99
 ip address 172.17.99.11 255.255.0.0
 no ip route-cache
!
ip default-gateway 172.17.50.1
ip http server
```

Snimanje, učitavanje i bekap konfiguracije

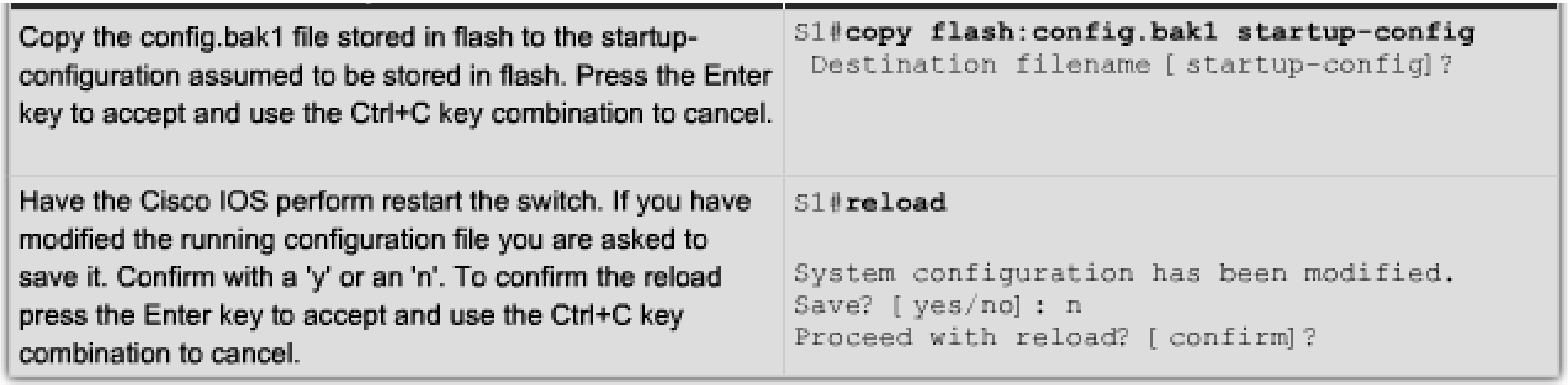


Cisco IOS CLI Command Syntax	

Formal version of Cisco IOS copy command.
Confirm the destination file name. Press the Enter key to accept and use the Ctrl+C key combination to cancel.
	`S1#copy system:running-config flash:startup-config`
	`Destination filename [startup-config]?`

Informal version of the copy command. The assumptions are that the running-config is running on the system and that the startup-config file that will be stored in flash NVRAM. Press the Enter key to accept and use the Ctrl+C key combination to cancel.	`S1#copy running-config startup-config`
	`Destination filename [startup-config]?`

Backup the startup-config to a file stored in flash NVRAM. Confirm the destination file name. Press the Enter key to accept and use the Ctrl+C key combination to cancel.	`S1#copy startup-config flash:config.bak1`
	`Destination filename [config.bak1]?`



Copy the config.bak1 file stored in flash to the startup-configuration assumed to be stored in flash. Press the Enter key to accept and use the Ctrl+C key combination to cancel.	`S1#copy flash:config.bak1 startup-config`
	`Destination filename [startup-config]?`

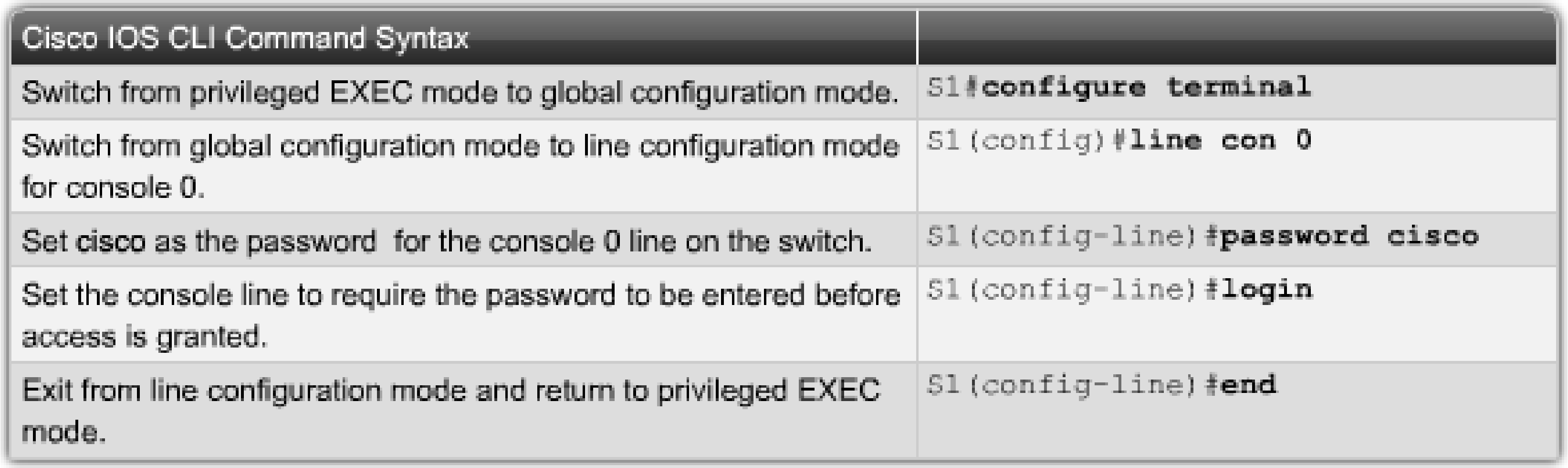
Have the Cisco IOS perform restart the switch. If you have modified the running configuration file you are asked to save it. Confirm with a 'y' or an 'n'. To confirm the reload press the Enter key to accept and use the Ctrl+C key combination to cancel.	`S1#reload`
	
	`System configuration has been modified.`
	`Save? [yes/no]: n`
	`Proceed with reload? [confirm]?`

Pristup i zaštita od neovlašćenog pristupa

Zaštita od neovlašćenog pristupa

✱ Zaštita pristupa preko konzole

- Ovaj tip zaštite nije apsolutna zaštita, jer postoje tzv. password-recovery procedure pomoću kojih je moguće preko konzole za veoma kratko vreme ukloniti ovaj vid zaštite
- Uređaje, ukoliko je neophodno, treba držati zaključane u rek ormanu

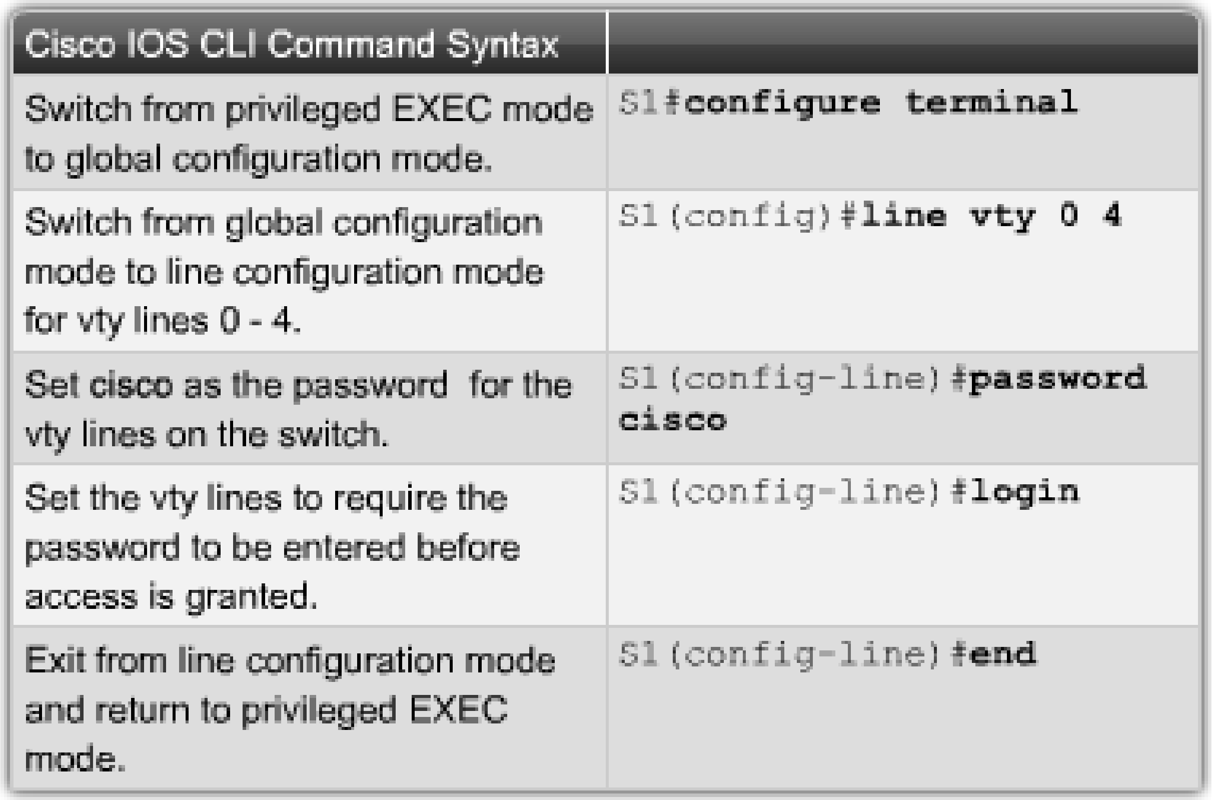


Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#**configure terminal**
Switch from global configuration mode to line configuration mode for console 0.	S1(config)#**line con 0**
Set cisco as the password for the console 0 line on the switch.	S1(config-line)#**password cisco**
Set the console line to require the password to be entered before access is granted.	S1(config-line)#**login**
Exit from line configuration mode and return to privileged EXEC mode.	S1(config-line)#**end**

Zaštita od neovlašćenog pristupa

Zaštita pristupa preko telneta

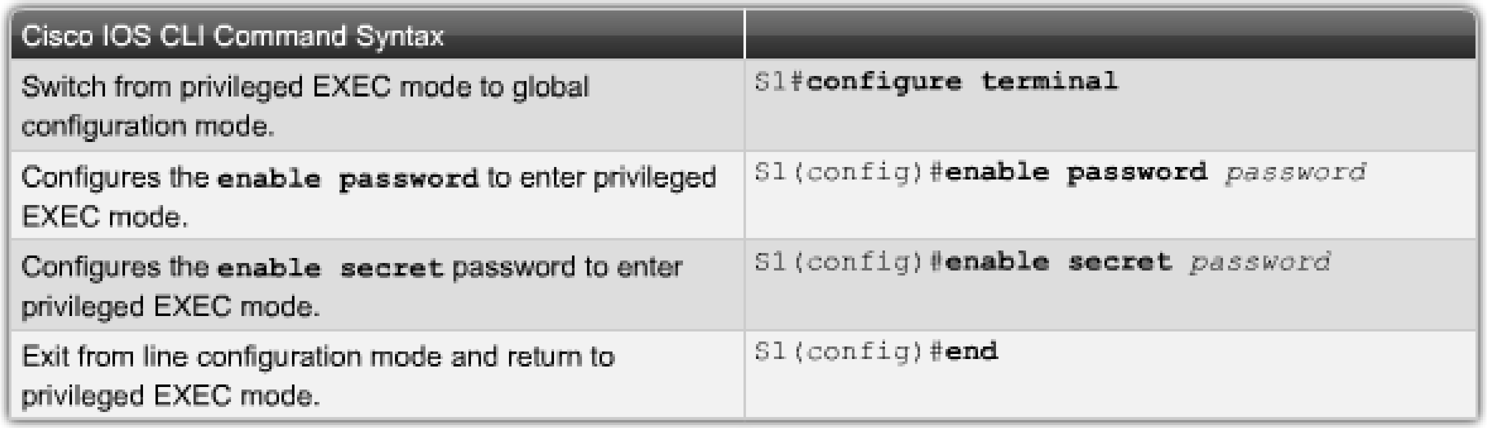
- Ovakav pristup se naziva i pristup preko vty linija (Virtual Terminal Line)
- Na ovaj način se zapravo aktivira telnet server na uređaju



Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#configure terminal`
Switch from global configuration mode to line configuration mode for vty lines 0 - 4.	`S1(config)#line vty 0 4`
Set cisco as the password for the vty lines on the switch.	`S1(config-line)#password cisco`
Set the vty lines to require the password to be entered before access is granted.	`S1(config-line)#login`
Exit from line configuration mode and return to privileged EXEC mode.	`S1(config-line)#end`

Zaštita pristupa privilegovanom modu

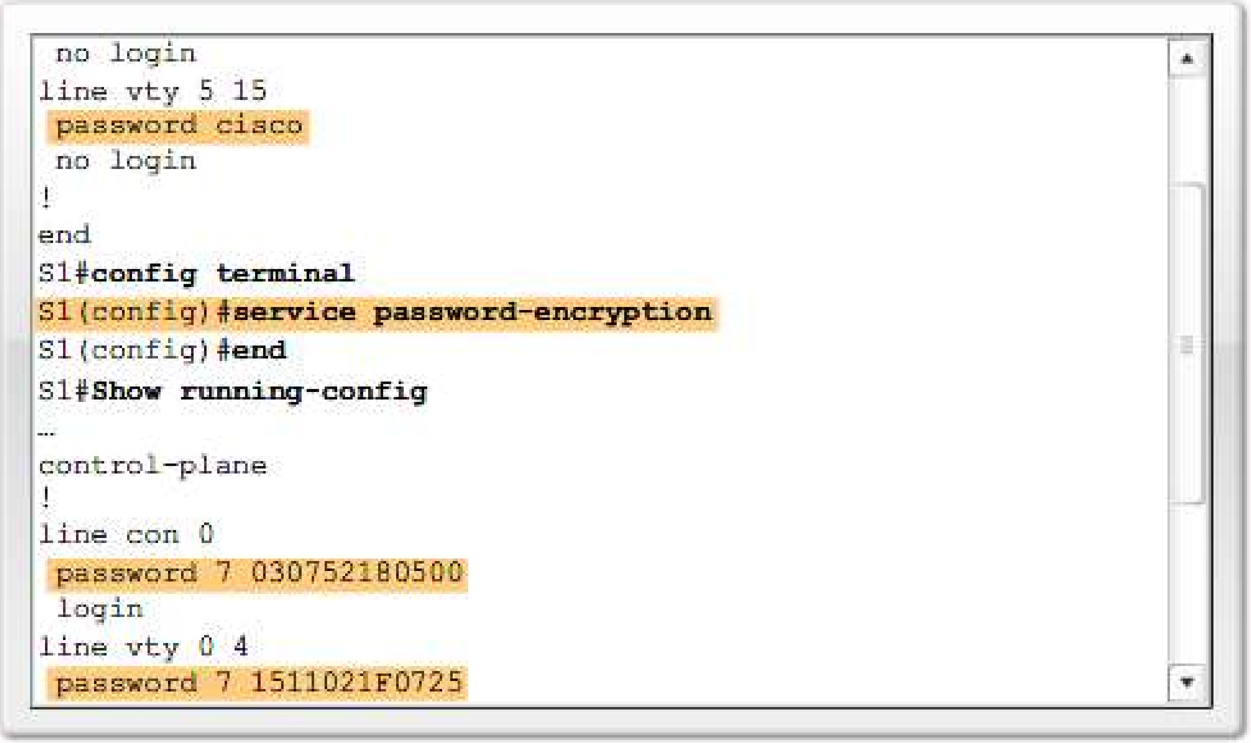
- Naredba za prelazak u privilegovani mod je enable, pa je zato i naziv ove zaštite enable-password
  - Ovo je neophodno podesiti da bi uređaj dozvolio telnet na njega, inače prilikom pokušaja pristupa preko telneta, bez obzira što je podešena IP adresa i vty linije, javlja da nije podešena “enable” šifra.
- Za pristup preko telneta neophodno je podesiti:
  - IP adresu
  - VTY linije
  - Enable-password



Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#`**`configure terminal`**
Configures the **`enable password`** to enter privileged EXEC mode.	`S1(config)#`**`enable password`** *`password`*
Configures the **`enable secret`** password to enter privileged EXEC mode.	`S1(config)#`**`enable secret`** *`password`*
Exit from line configuration mode and return to privileged EXEC mode.	`S1(config)#`**`end`**

Zabrana prikaza šifri u izvornom obliku

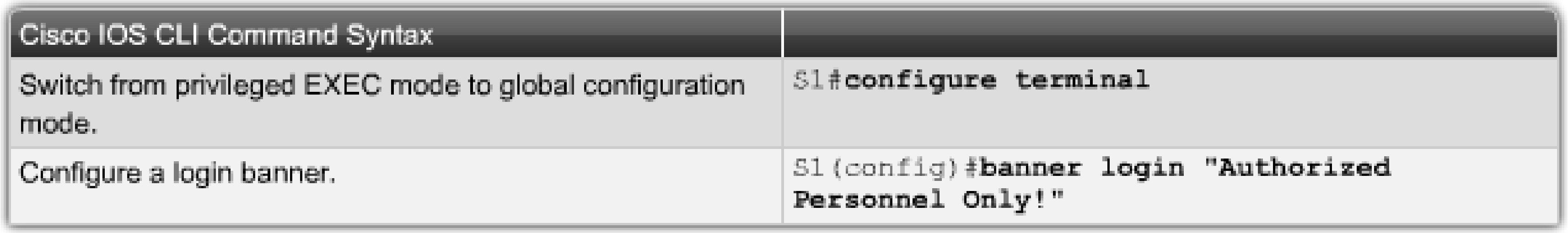
- U konfiguraciji su šifre zapamćene u izvornom obliku i prilikom prikaza konfiguracije show naredbom vidljive su na ekranu. Da bi se sakrila šifra samo u svrhu pristupa, portebno je uključiti servis koji je tome namenjen, a koji vrši šifriranje karaktera koji se nalaze iza ključne reči password u prikazu.
  - Switch(conf)#service password-encription



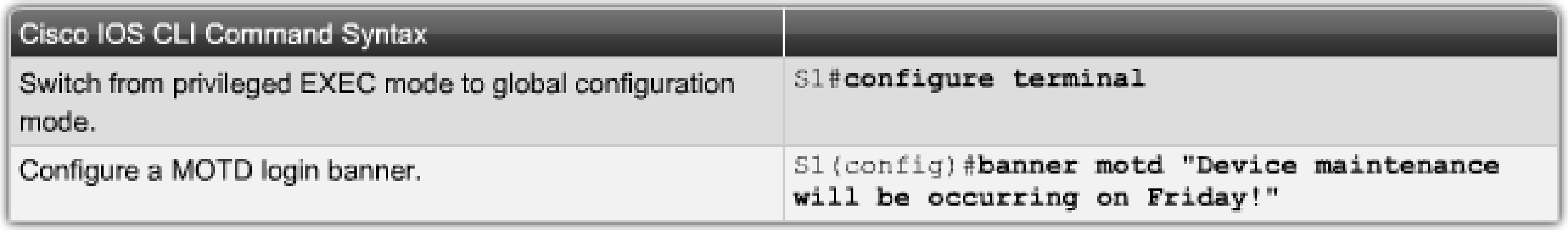
```
 no login
line vty 5 15
 password cisco
 no login
!
end
S1#config terminal
S1(config)#service password-encryption
S1(config)#end
S1#Show running-config
…
control-plane
!
line con 0
 password 7 030752180500
 login
line vty 0 4
 password 7 1511021F0725
```

Baner i poruka dana

- Baner i poruka dana (Message-Of-The-Day - MOTD) predstavljaju tekstove koji se prikazuju korisniku pre nego što uređaj potraži podatke za logovanje korisnika.

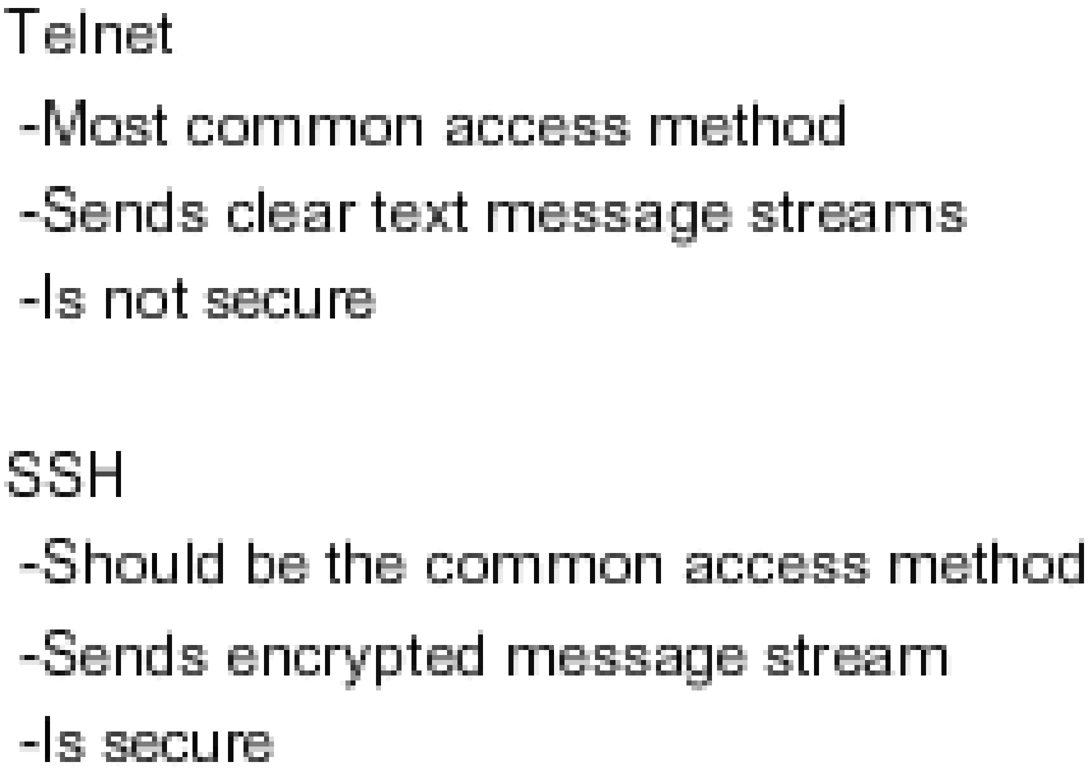


Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#`**`configure terminal`**
Configure a login banner.	`S1(config)#`**`banner login "Authorized Personnel Only!"`**



Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#`**`configure terminal`**
Configure a MOTD login banner.	`S1(config)#`**`banner motd "Device maintenance will be occurring on Friday!"`**

Telnet i SSH



Telnet

-Most common access method

-Sends clear text message streams

-Is not secure

SSH

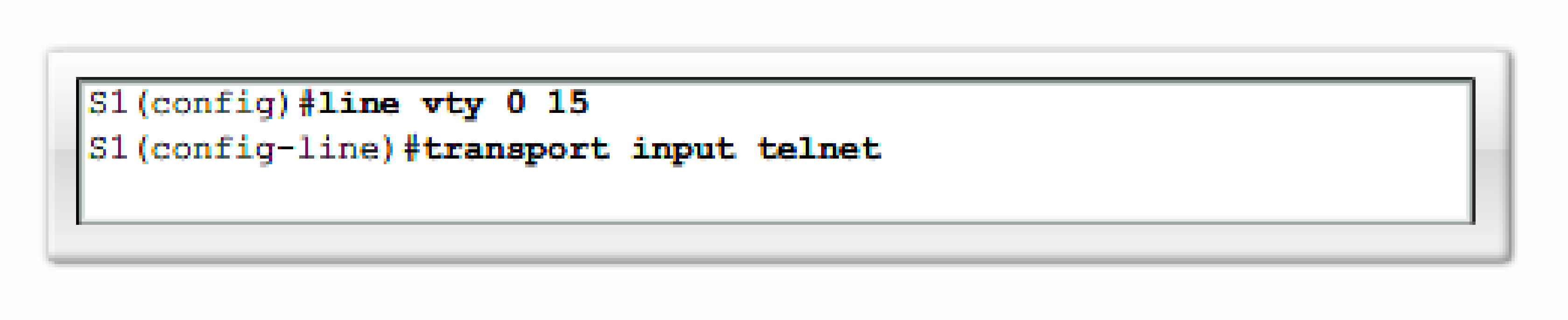
-Should be the common access method

-Sends encrypted message stream

-Is secure

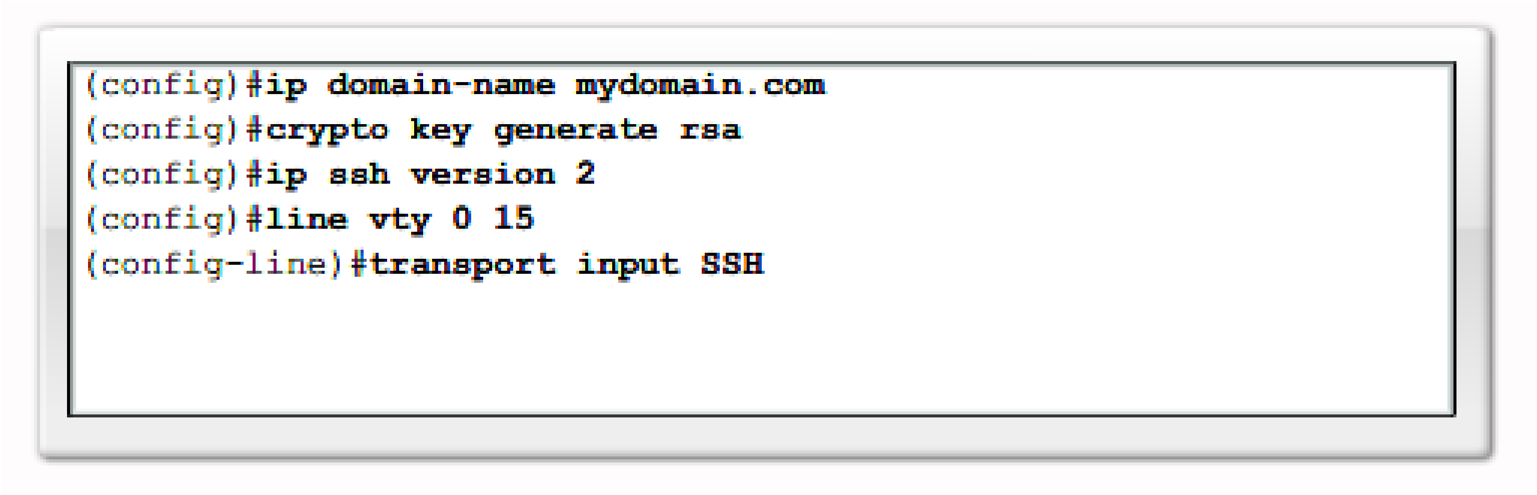
Telnet i SSH

- Telnet je podrazumevani način, a može se eksplicitno naglasiti:



```
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
```

- SSH:

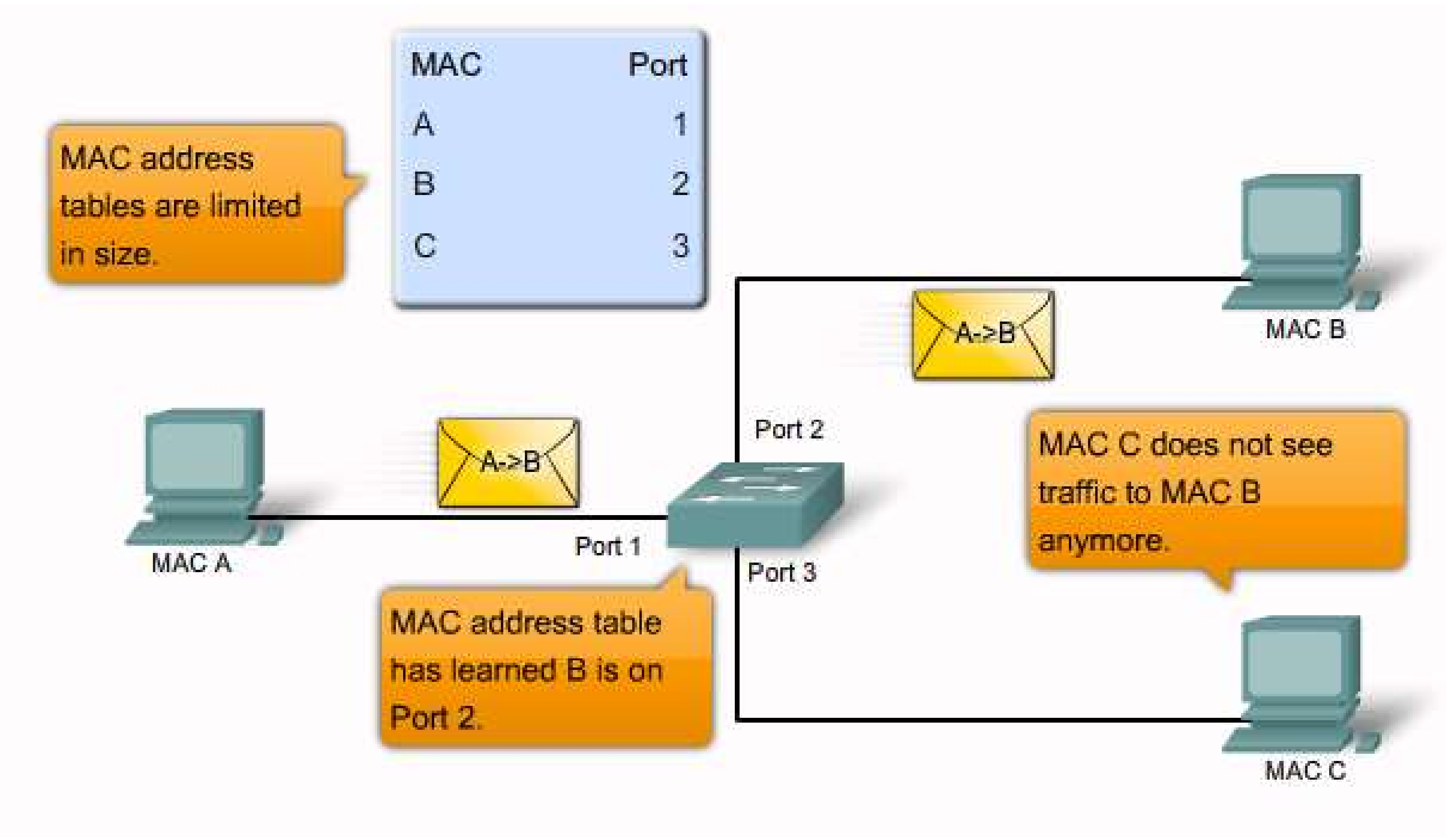


```
(config)#ip domain-name mydomain.com
(config)#crypto key generate rsa
(config)#ip ssh version 2
(config)#line vty 0 15
(config-line)#transport input SSH
```

Primeri tipičnih napada

MAC spoofing

- MAC address floding



MAC	Port
A	1
B	2
C	3

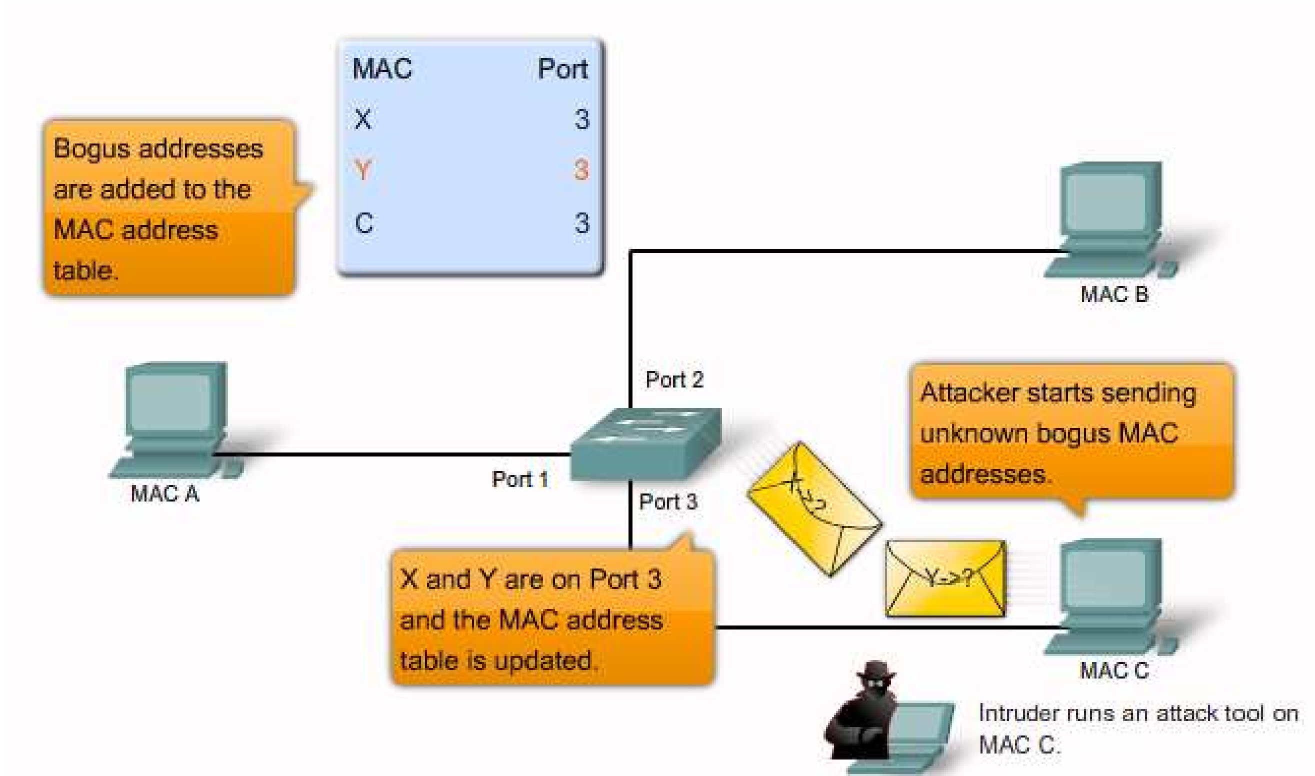
MAC address tables are limited in size.

MAC address table has learned B is on Port 2.

MAC C does not see traffic to MAC B anymore.

MAC spoofing

- Napadač može:
  - Poslati lažni frejm sa proizvoljnom MAC adresom u source polju (ako zna MAC) - spoofing
  - Može poslati veliki broj frejmova sa "random" izvorišnim adresama i "preplaviti", t.j. napuniti memoriju za MAC
- Razlog...



MAC	Port
X	3
Y	3
C	3

Bogus addresses are added to the MAC address table.

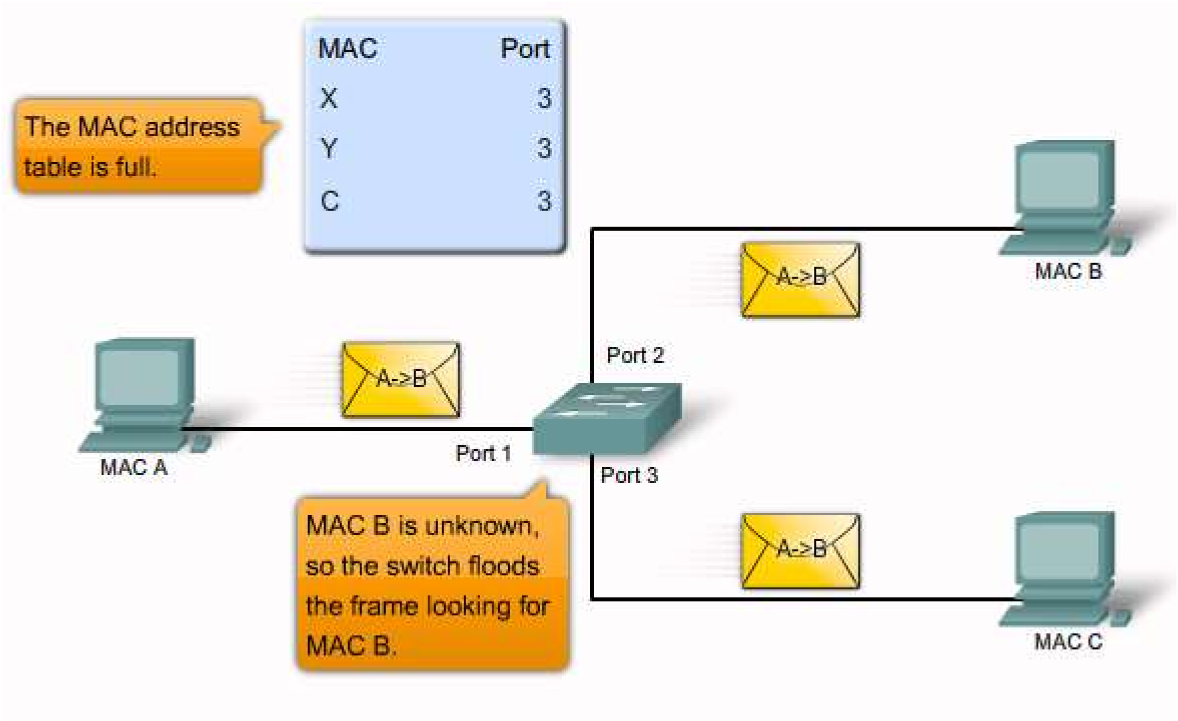
Attacker starts sending unknown bogus MAC addresses.

X and Y are on Port 3 and the MAC address table is updated.

Intruder runs an attack tool on MAC C.

Poplava MAC adresama

- Napadač može:
  - Poslati lažni frejm sa proizvoljnom MAC adresom u source polju (ako zna MAC)
  - Može poslati veliki broj frejmova sa "random" izvorišnim adresama i "preplaviti", t.j. napuniti memoriju za MAC
- Razlog...



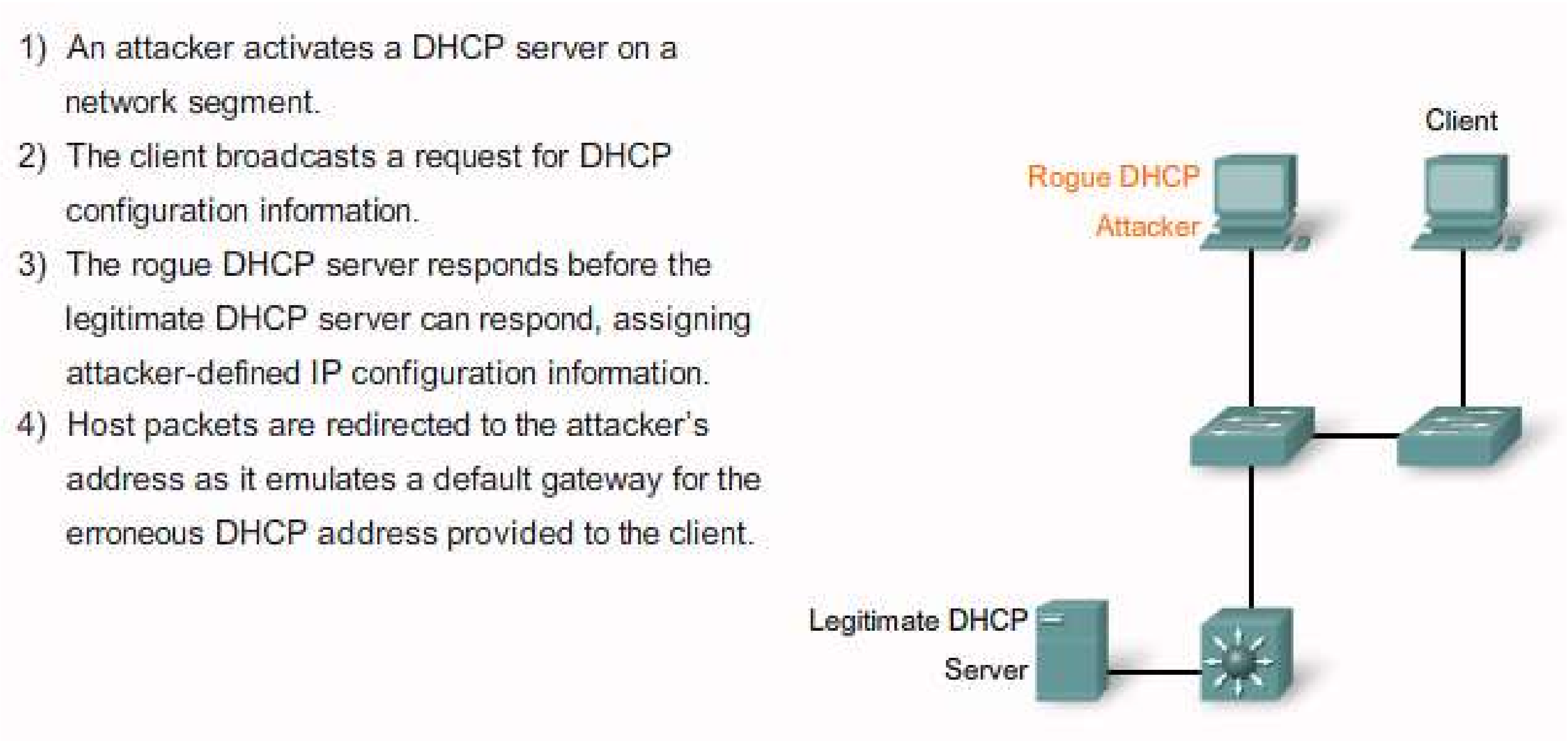
MAC	Port
X	3
Y	3
C	3

The MAC address table is full.

MAC B is unknown, so the switch floods the frame looking for MAC B.

DHCP Spoofing napad

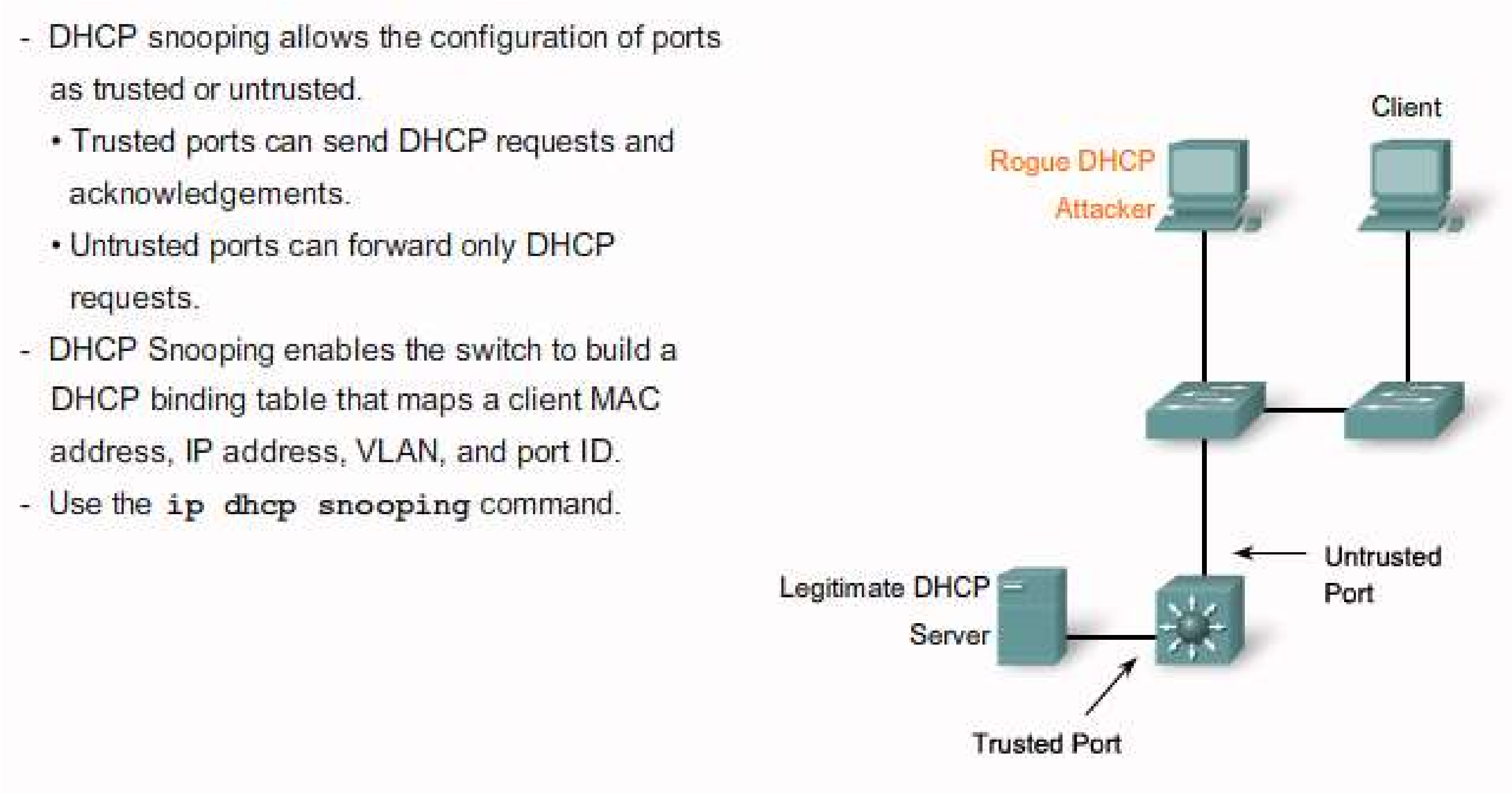
- Tehnika



1) An attacker activates a DHCP server on a network segment.
2) The client broadcasts a request for DHCP configuration information.
3) The rogue DHCP server responds before the legitimate DHCP server can respond, assigning attacker-defined IP configuration information.
4) Host packets are redirected to the attacker's address as it emulates a default gateway for the erroneous DHCP address provided to the client.

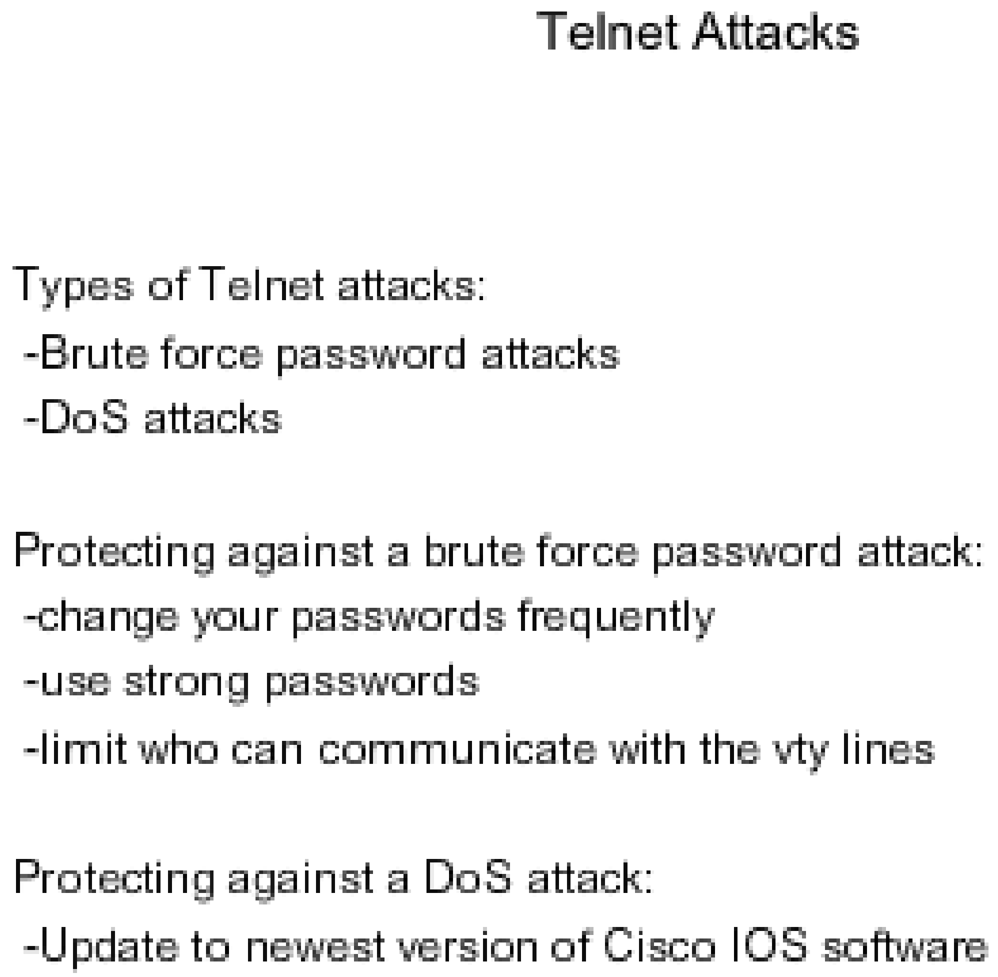
DHCP Spoofing napad

✱ Zaštita



- DHCP snooping allows the configuration of ports as trusted or untrusted.
  - Trusted ports can send DHCP requests and acknowledgements.
  - Untrusted ports can forward only DHCP requests.
- DHCP Snooping enables the switch to build a DHCP binding table that maps a client MAC address, IP address, VLAN, and port ID.
- Use the `ip dhcp snooping` command.

Telnet brute-force napadi



Telnet Attacks

Types of Telnet attacks:

- -Brute force password attacks
- -DoS attacks

Protecting against a brute force password attack:

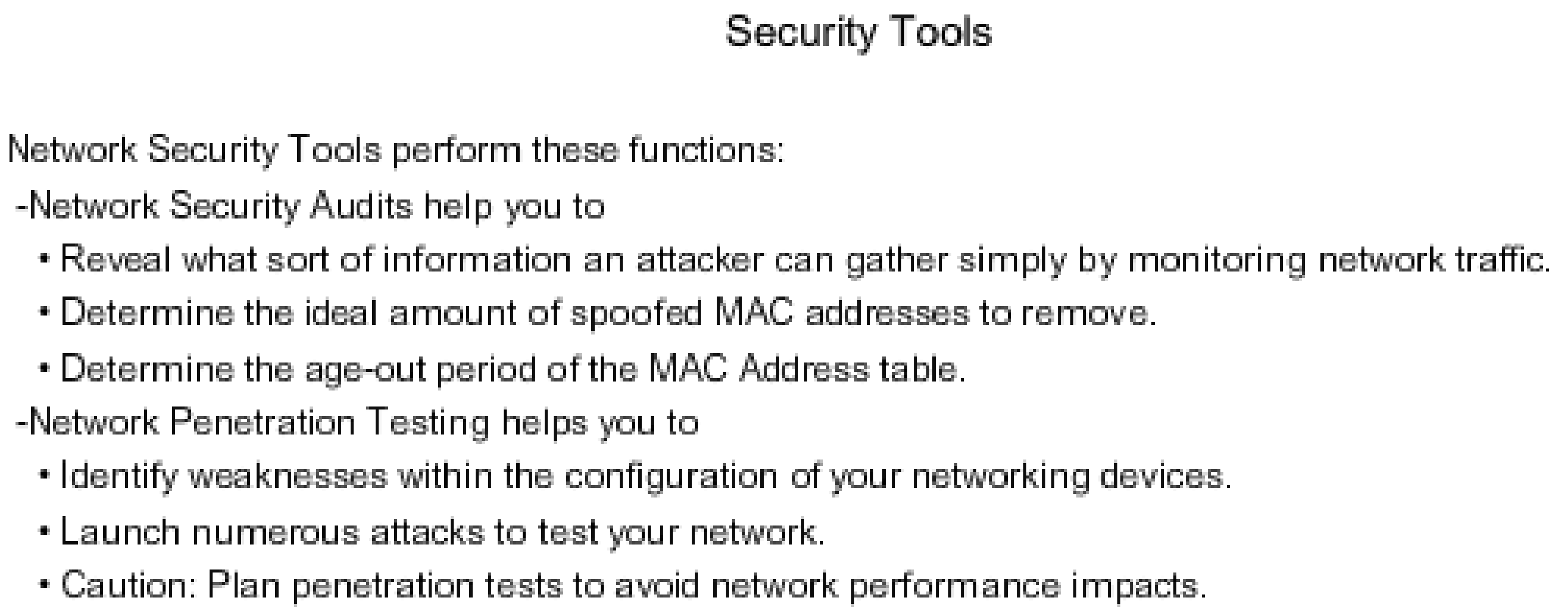
- -change your passwords frequently
- -use strong passwords
- -limit who can communicate with the vty lines

Protecting against a DoS attack:

- -Update to newest version of Cisco IOS software

Mere zaštite

- Pasivne mere
  - Revizija mreže (audit)
- Aktivne mere
  - Praćenjem mrežnog saobraćaja i otktivanje potencijalnih "upada" (penetration test)
  - IDS i IPS sistemi



Security Tools

Network Security Tools perform these functions:

-Network Security Audits help you to

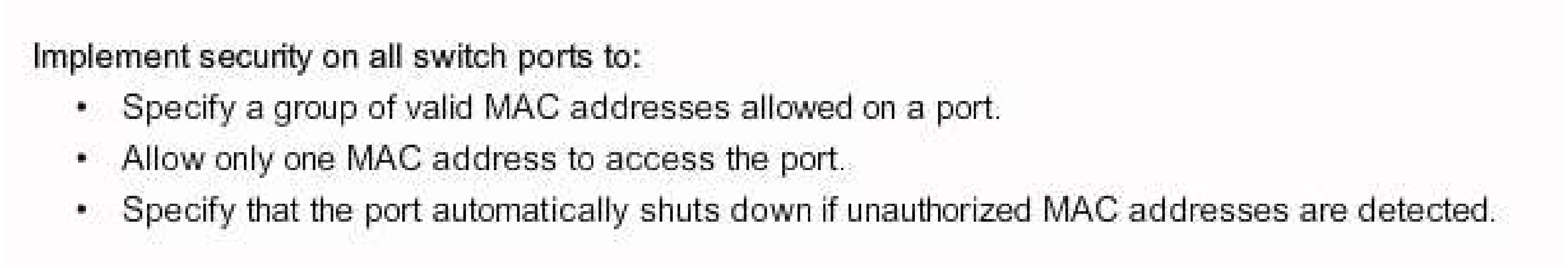
- Reveal what sort of information an attacker can gather simply by monitoring network traffic.
- Determine the ideal amount of spoofed MAC addresses to remove.
- Determine the age-out period of the MAC Address table.

-Network Penetration Testing helps you to

- Identify weaknesses within the configuration of your networking devices.
- Launch numerous attacks to test your network.
- Caution: Plan penetration tests to avoid network performance impacts.

Bezbednost na nivou svič-porta

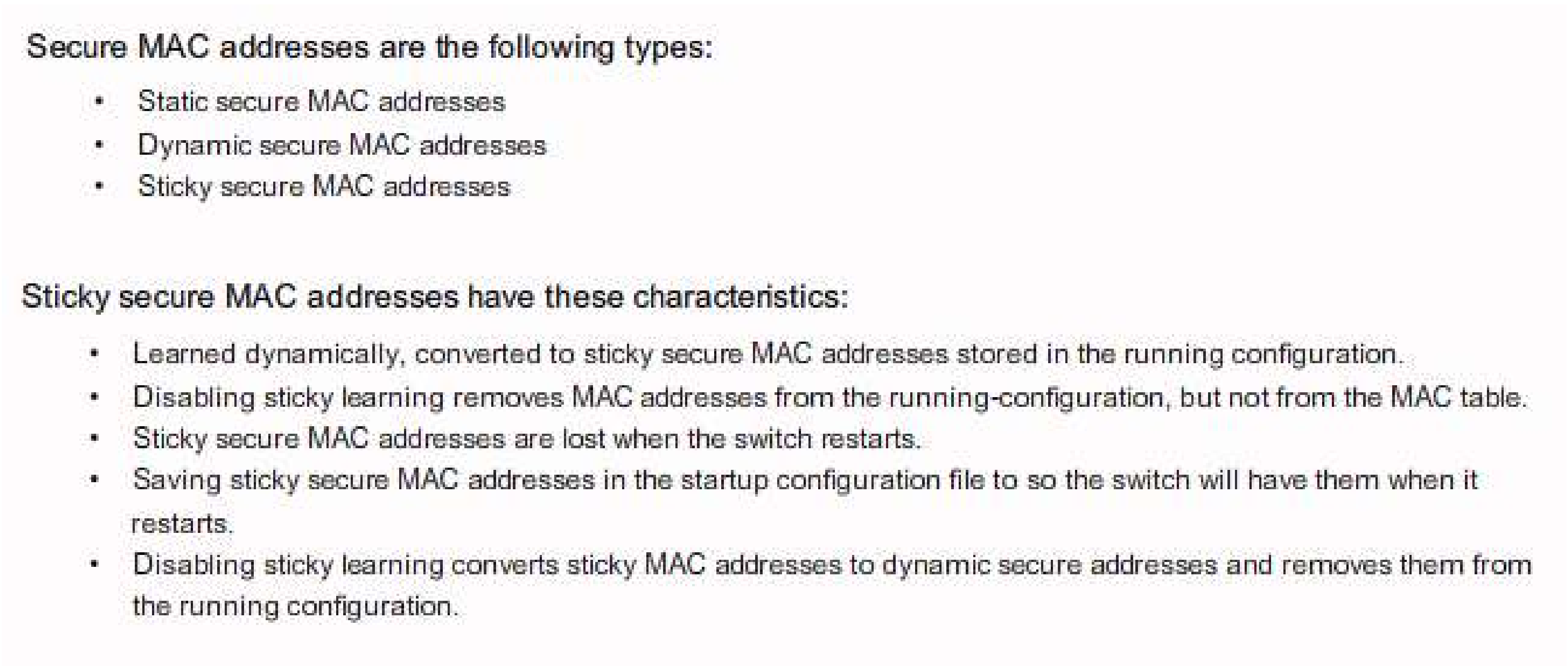
- Implementacija bezbednosti na nivou porta može izgledati ovako:



Implement security on all switch ports to:

- Specify a group of valid MAC addresses allowed on a port.
- Allow only one MAC address to access the port.
- Specify that the port automatically shuts down if unauthorized MAC addresses are detected.

Tipovi zaštite na nivou svič-porta



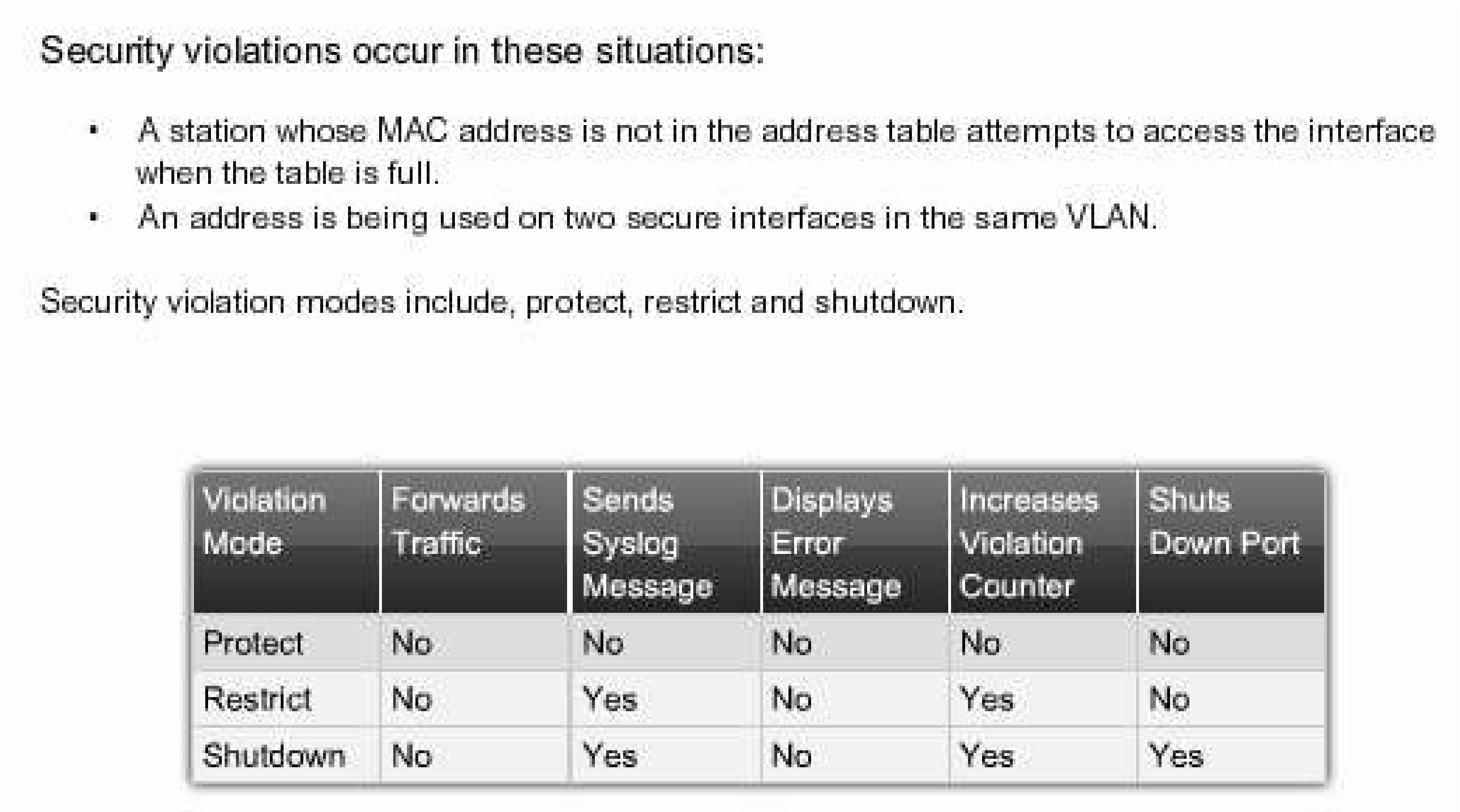
Secure MAC addresses are the following types:

- Static secure MAC addresses
- Dynamic secure MAC addresses
- Sticky secure MAC addresses

Sticky secure MAC addresses have these characteristics:

- Learned dynamically, converted to sticky secure MAC addresses stored in the running configuration.
- Disabling sticky learning removes MAC addresses from the running-configuration, but not from the MAC table.
- Sticky secure MAC addresses are lost when the switch restarts.
- Saving sticky secure MAC addresses in the startup configuration file to so the switch will have them when it restarts.
- Disabling sticky learning converts sticky MAC addresses to dynamic secure addresses and removes them from the running configuration.

Reakcija porta u slučaju neovlašćenog pristupa



Security violations occur in these situations:

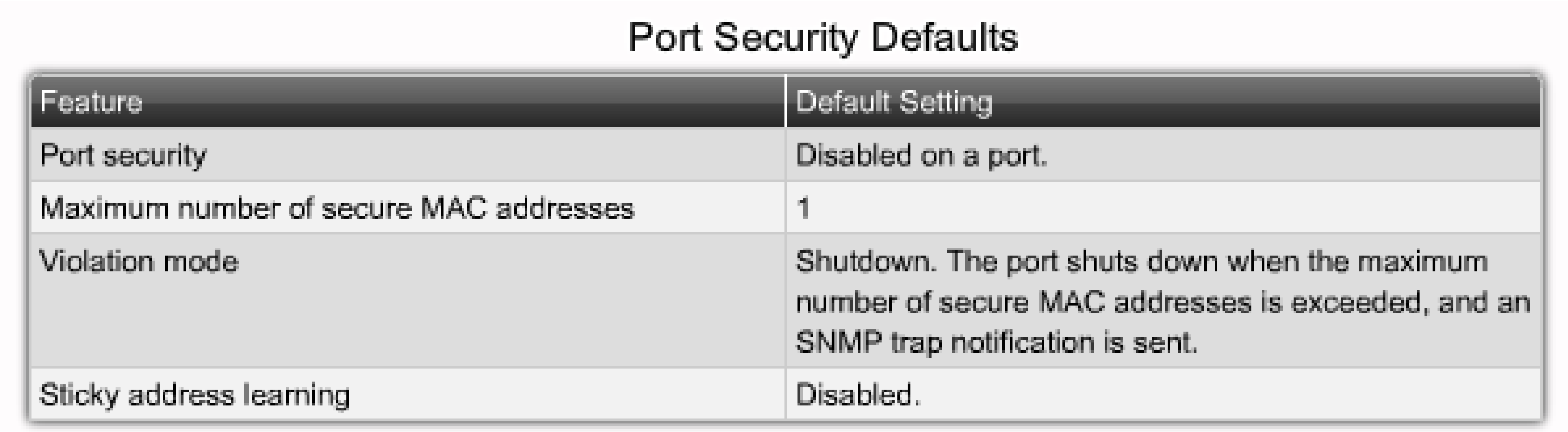
- A station whose MAC address is not in the address table attempts to access the interface when the table is full.
- An address is being used on two secure interfaces in the same VLAN.

Security violation modes include, protect, restrict and shutdown.

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	Yes	No	Yes	Yes

Podešavanje bezbednosti na nivou porta na Cisco sviču

- Podrazumevana (default) podešavanja



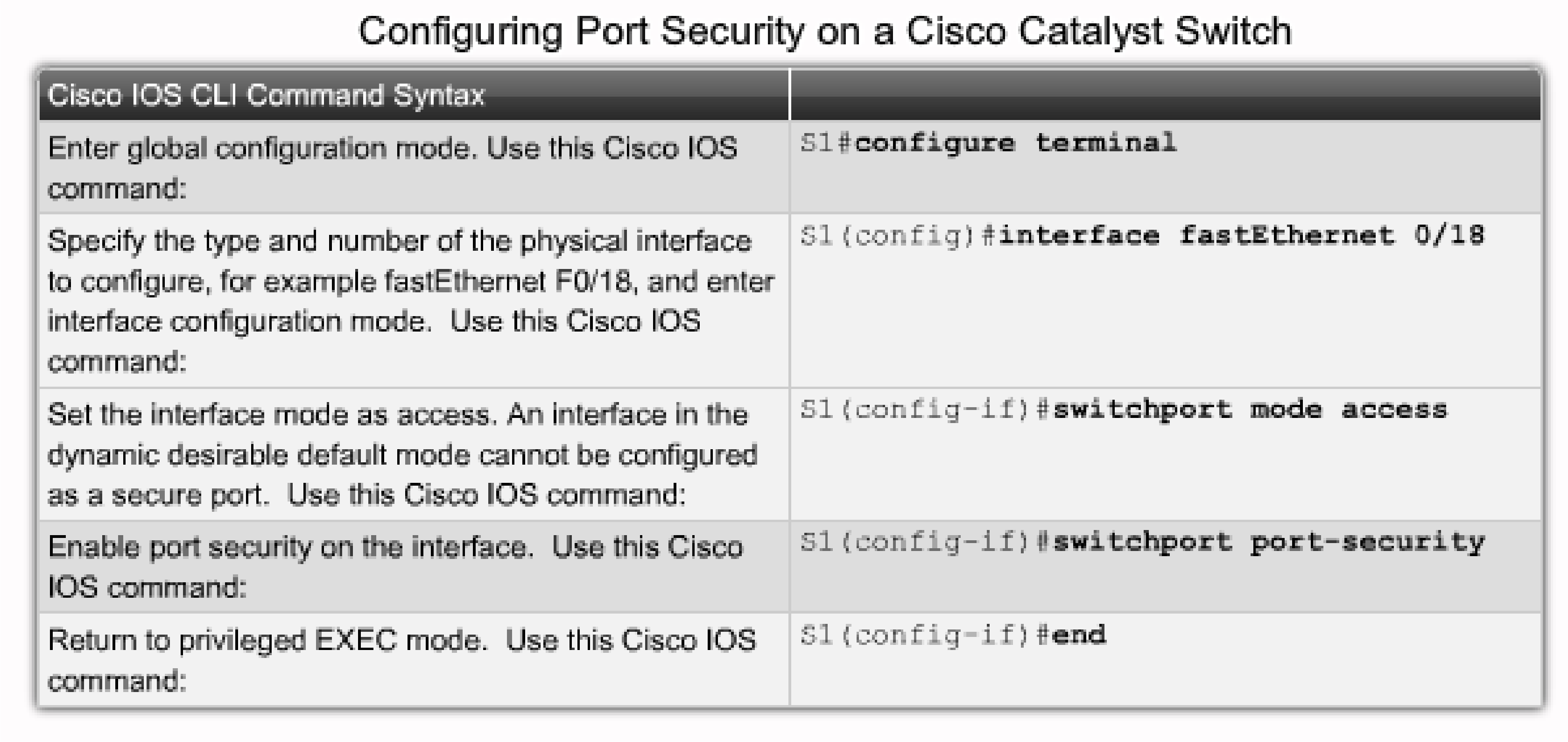
Port Security Defaults

Feature	Default Setting
Port security	Disabled on a port.
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

Podešavanje bezbednosti na nivou porta na Cisco sviču

Uključivanje zaštite

- Pored zadavanja parametara, zaštitu je neophodno aktivirati!

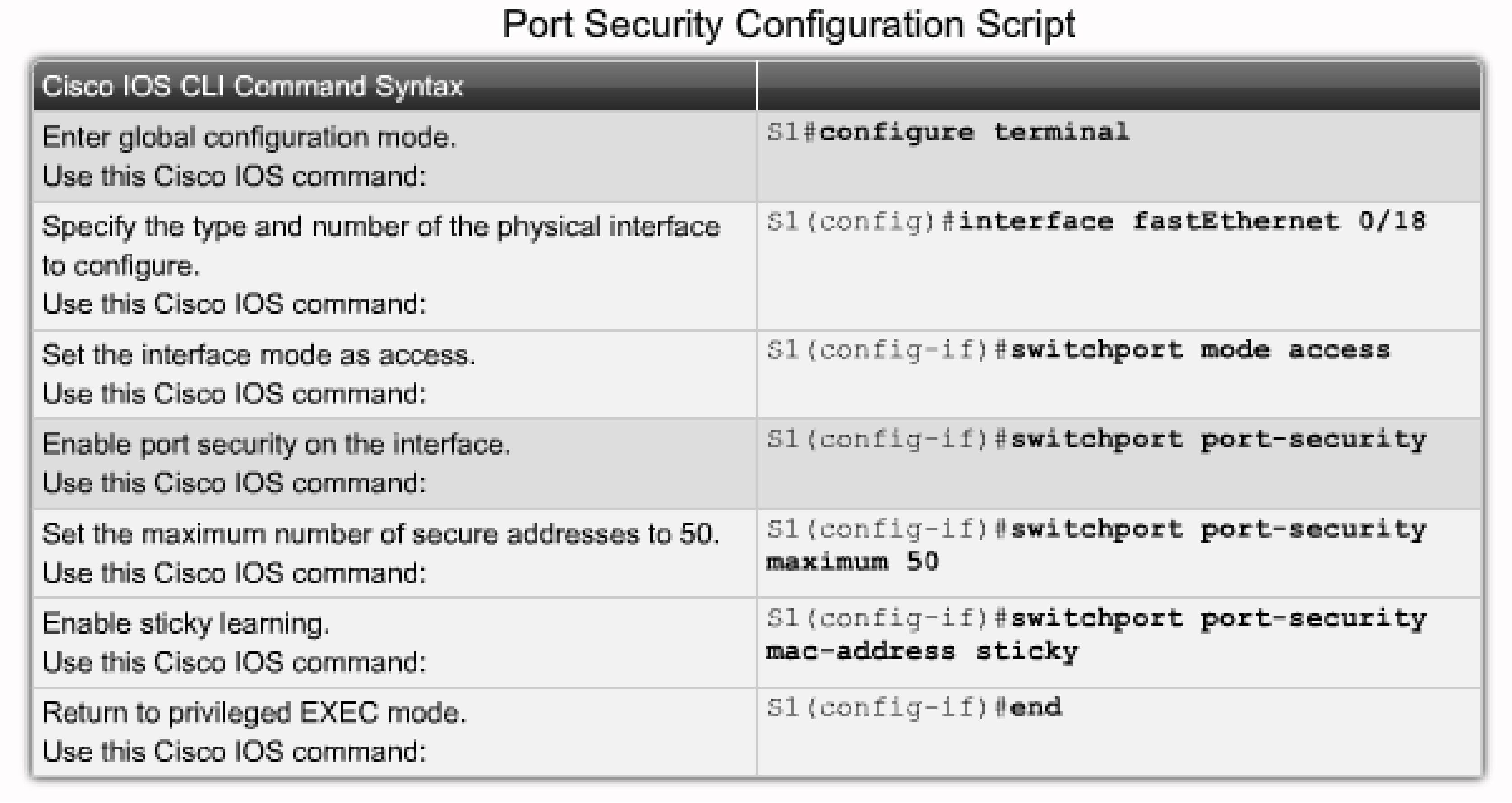


Configuring Port Security on a Cisco Catalyst Switch

Cisco IOS CLI Command Syntax	
Enter global configuration mode. Use this Cisco IOS command:	`S1#`**`configure terminal`**
Specify the type and number of the physical interface to configure, for example fastEthernet F0/18, and enter interface configuration mode. Use this Cisco IOS command:	`S1(config)#`**`interface fastEthernet 0/18`**
Set the interface mode as access. An interface in the dynamic desirable default mode cannot be configured as a secure port. Use this Cisco IOS command:	`S1(config-if)#`**`switchport mode access`**
Enable port security on the interface. Use this Cisco IOS command:	`S1(config-if)#`**`switchport port-security`**
Return to privileged EXEC mode. Use this Cisco IOS command:	`S1(config-if)#`**`end`**

Podešavanje bezbednosti na nivou porta na Cisco sviču

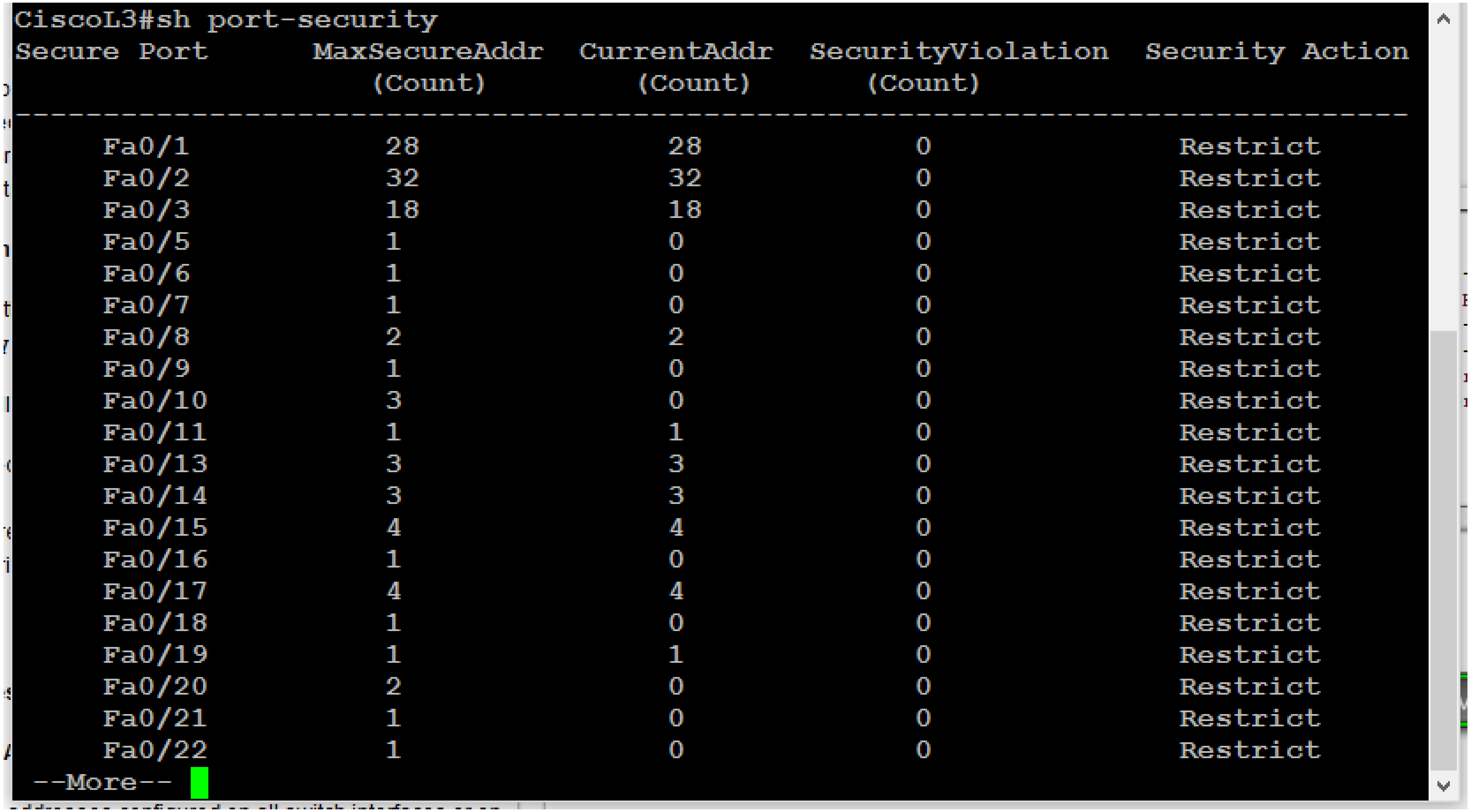
✱ Podešavanje "sticky" porta



Port Security Configuration Script

Cisco IOS CLI Command Syntax	
Enter global configuration mode. Use this Cisco IOS command:	`S1#configure terminal`
Specify the type and number of the physical interface to configure. Use this Cisco IOS command:	`S1(config)#interface fastEthernet 0/18`
Set the interface mode as access. Use this Cisco IOS command:	`S1(config-if)#switchport mode access`
Enable port security on the interface. Use this Cisco IOS command:	`S1(config-if)#switchport port-security`
Set the maximum number of secure addresses to 50. Use this Cisco IOS command:	`S1(config-if)#switchport port-security maximum 50`
Enable sticky learning. Use this Cisco IOS command:	`S1(config-if)#switchport port-security mac-address sticky`
Return to privileged EXEC mode. Use this Cisco IOS command:	`S1(config-if)#end`

Prikaz podešavanja portova



```
CiscoL3#sh port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)        (Count)        (Count)
-------------------------------------------------------------------------------
     Fa0/1             28             28             0              Restrict
     Fa0/2             32             32             0              Restrict
     Fa0/3             18             18             0              Restrict
     Fa0/5             1              0              0              Restrict
     Fa0/6             1              0              0              Restrict
     Fa0/7             1              0              0              Restrict
     Fa0/8             2              2              0              Restrict
     Fa0/9             1              0              0              Restrict
     Fa0/10            3              0              0              Restrict
     Fa0/11            1              1              0              Restrict
     Fa0/13            3              3              0              Restrict
     Fa0/14            3              3              0              Restrict
     Fa0/15            4              4              0              Restrict
     Fa0/16            1              0              0              Restrict
     Fa0/17            4              4              0              Restrict
     Fa0/18            1              0              0              Restrict
     Fa0/19            1              1              0              Restrict
     Fa0/20            2              0              0              Restrict
     Fa0/21            1              0              0              Restrict
     Fa0/22            1              0              0              Restrict
 --More--
```