PacketTracer + IOS

Computer Networks 101

ICTPro

Wistron InfoComm, April 2019, Brno

DEVICES

- Routers
  - C1841, C1941, C2620XM, C2621XM, C2811, C2901, C2911, C819
- Switches
  - Cat2950, Cat2950T, Cat2960, L3 3560
- Hubs
- Wireless
  - AP G/N/A, Linksys WRT300N
- Security
  - ASA5505
- End-devices
  - Destop, VoIP Phone, Phone, Tablet

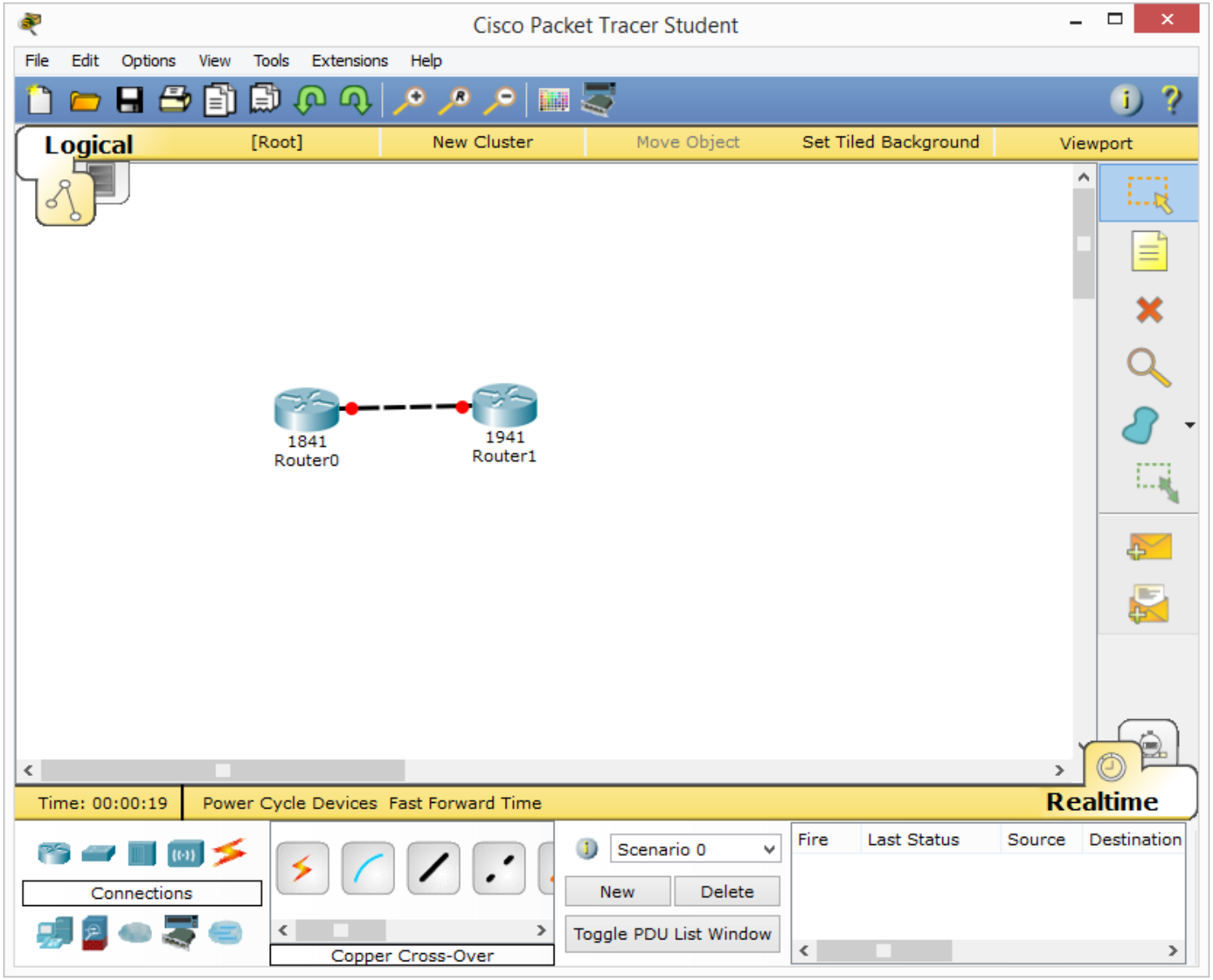
PROTOCOLS

Layer	Cisco Packet Tracer Supported Protocols
Application	FTP , SMTP, POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, ISR VOIP, SCCP config and calls ISR command support, Call Manager Express
Transport	TCP and UDP, TCP Nagle Algorithm & IP Fragmentation, RTP
Network	BGP, IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, RIPv1/v2/ng, Multi-Area OSPF, OSPFv3, EIGRP, EIGRPv6, Static Routing, Route Redistribution, Multilayer Switching, L3 QoS, NAT, CBAL, Zone-based policy firewall and Intrusion Protection System on the ISR, GRE VPN, IPSec VPN, HSRP, CEF
Network Access/ Interface	Ethernet (802.3), 802.11, HDLC, Frame Relay, PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.1q, PAgP, L2 QoS, SLARP, Simple WEP, WPA, EAP, VLANs, CSMA/CD, Etherchannel, DSL

IDE

PacketTracer

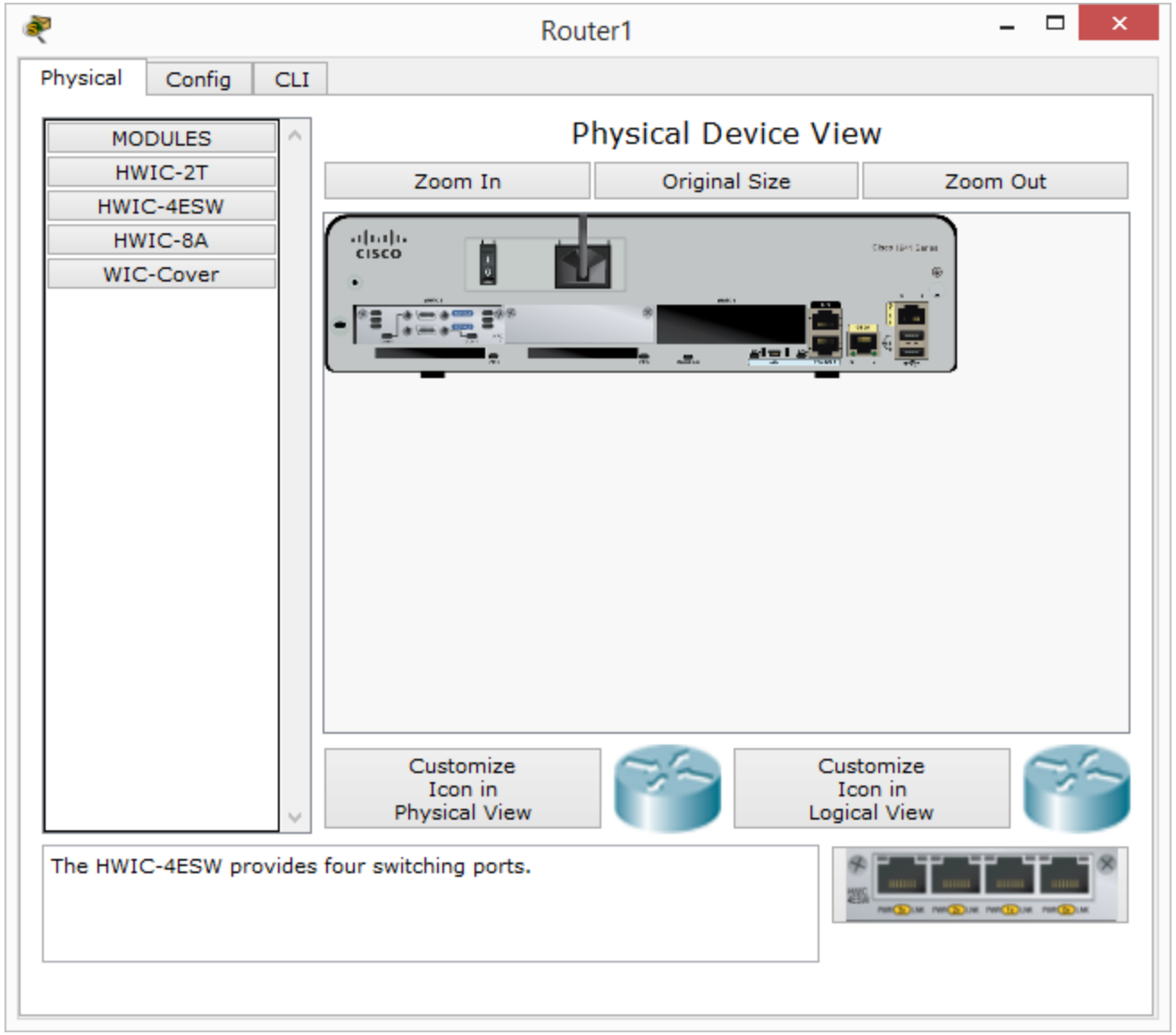
IOS



IDE: Device

PacketTracer

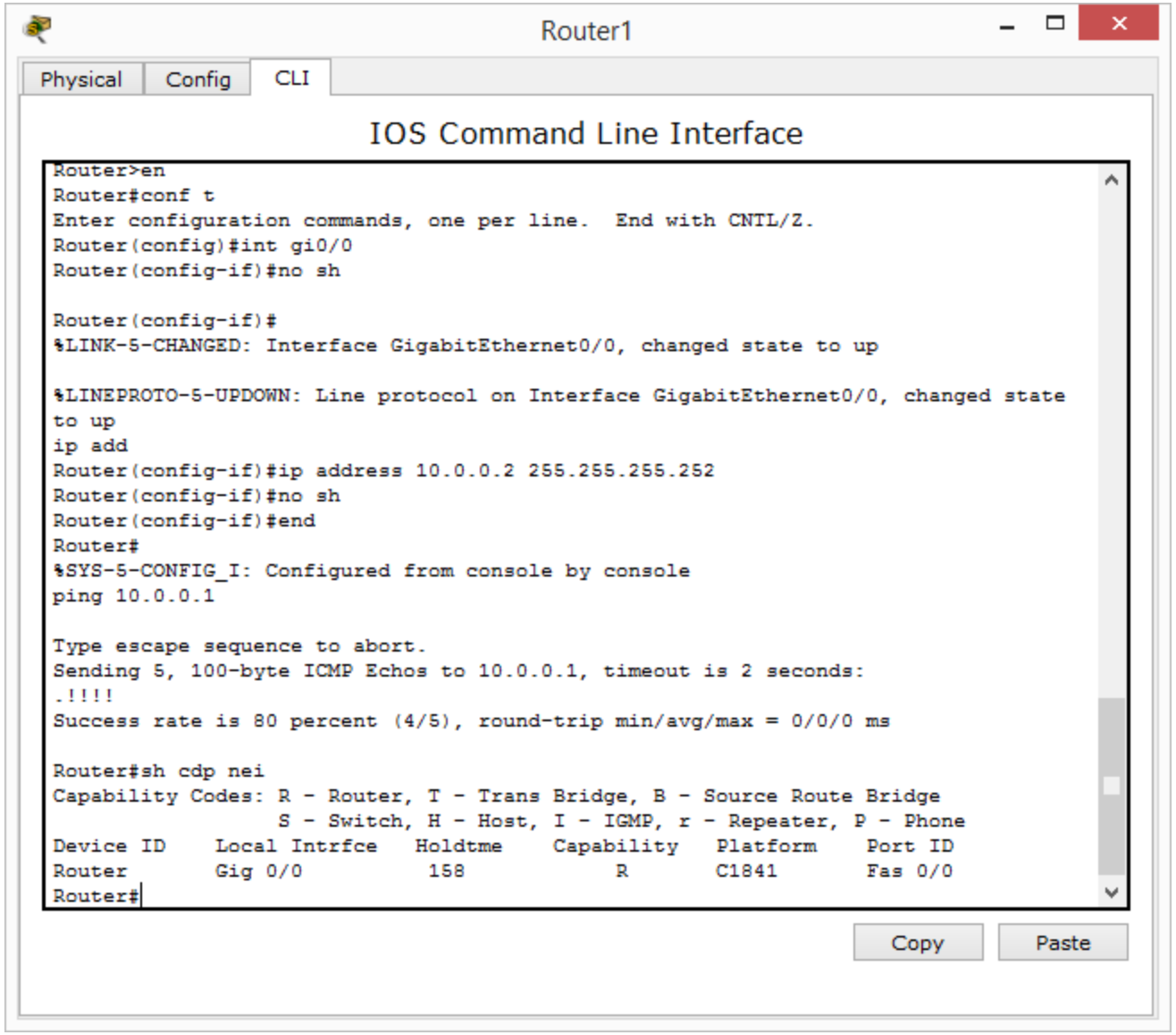
IOS



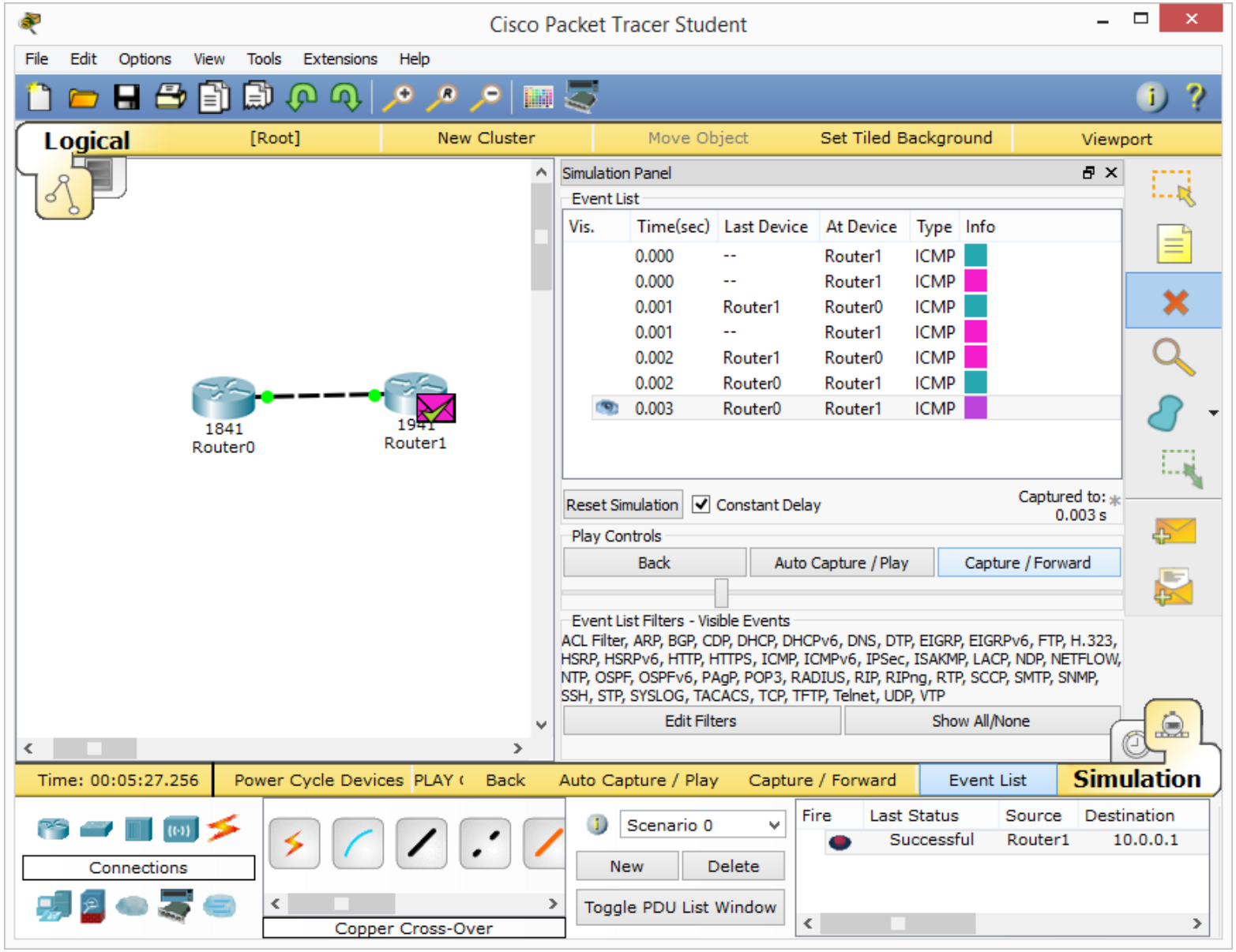
IDE: CLI Access

PacketTracer

IOS



IDE: Simulation Mode

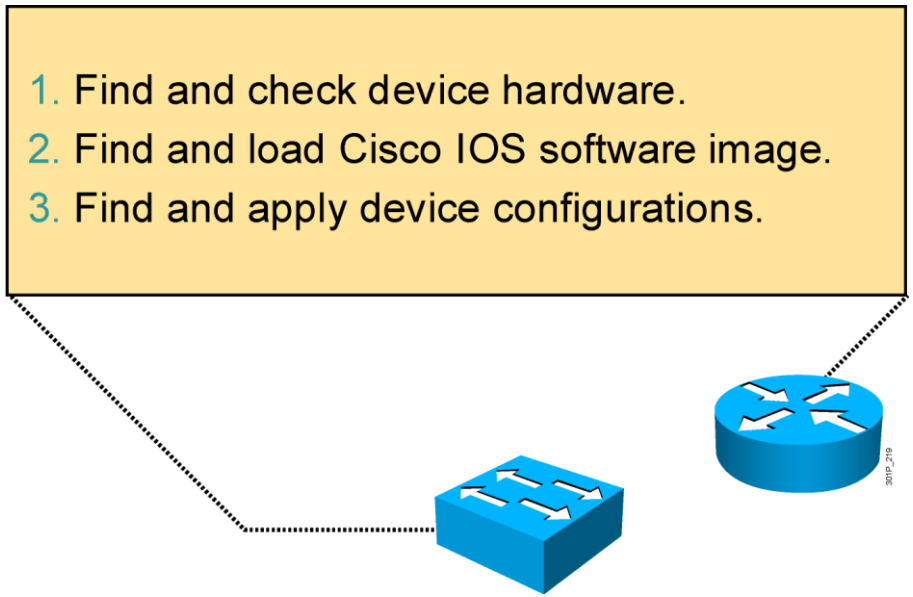


PacketTracer

IOS

FEATURES

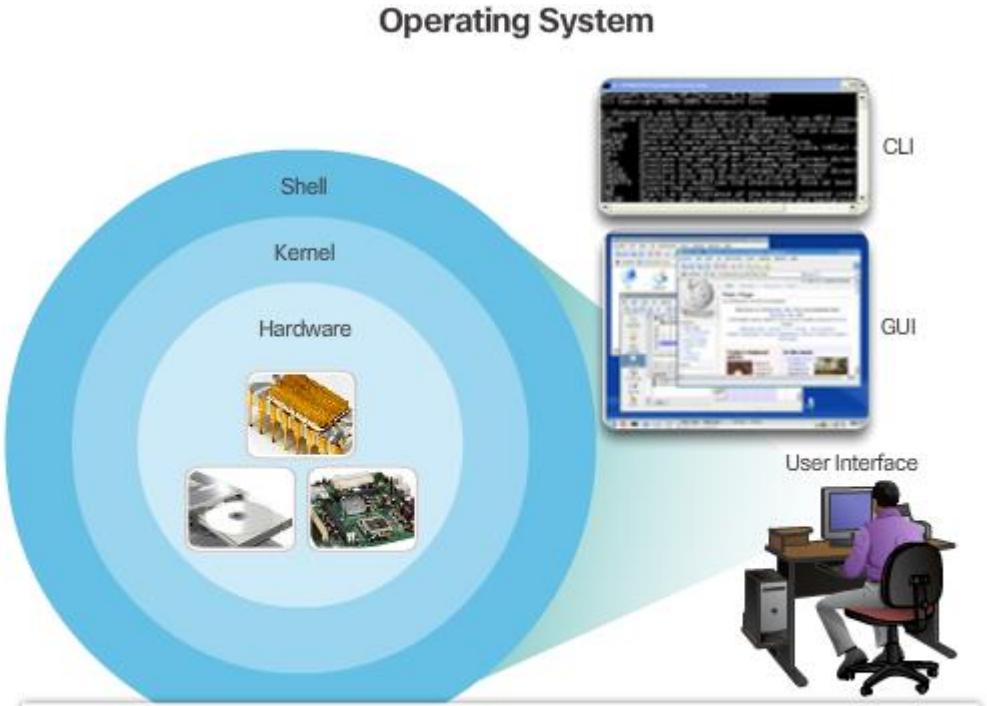
- Features to carry the chosen network protocols and functions
- Connectivity for high-speed traffic between devices
- Security to control access and prohibit unauthorized network use
- Scalability to add interfaces and capability as needed for network growth
- Reliability to ensure dependable access to networked resources



INTRODUCING

PacketTracer

IOS



Shell: The user interface that allows users to request specific tasks from the computer.
These requests can be made either through the CLI or GUI interfaces.

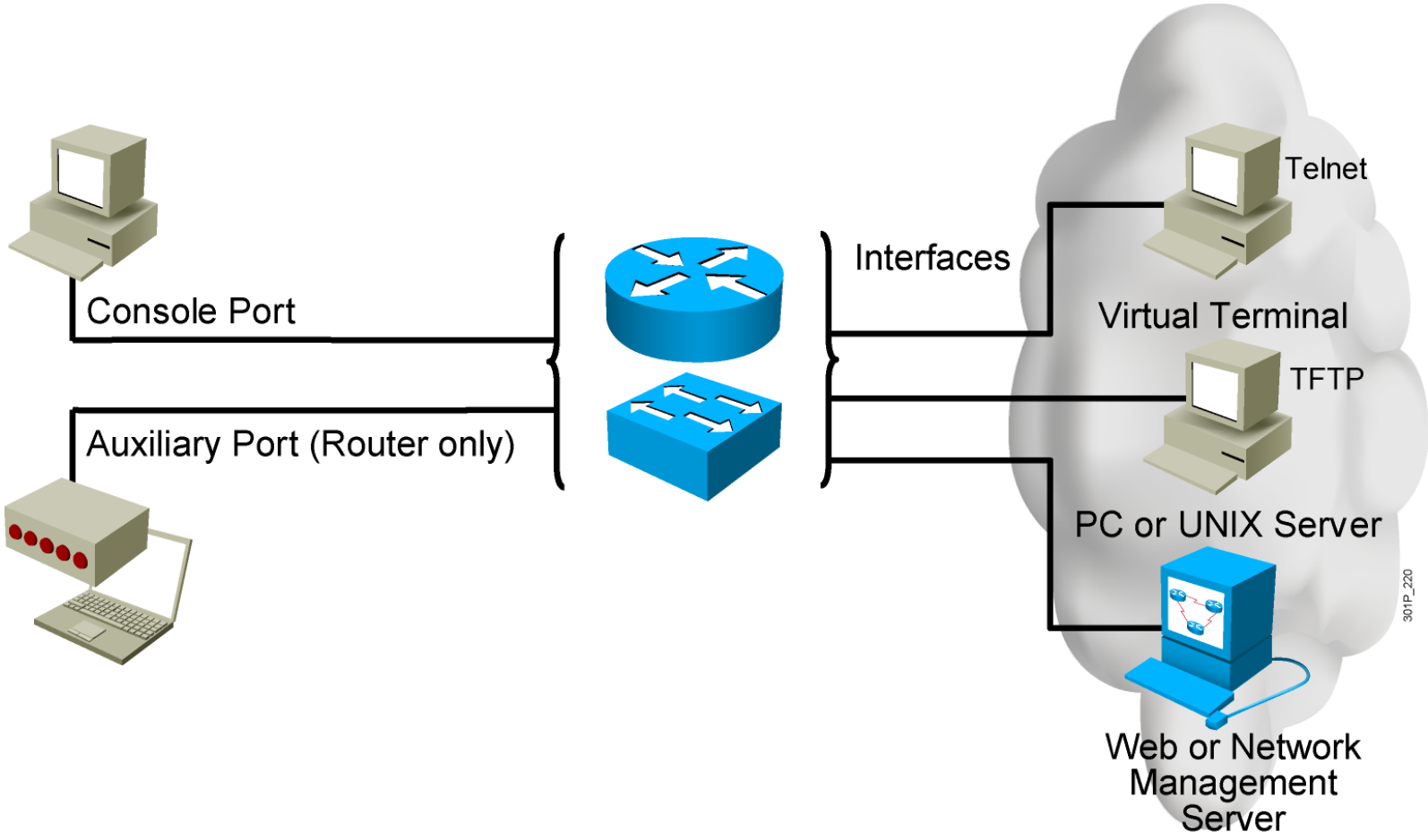
Kernel: Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.

Hardware: The physical part of a computer including underlying electronics.

CONFIGURATION SOURCES

PacketTracer

IOS



CLI

- Command Line Interface is used to enter commands
- Operations vary on different internetworking devices
- Users type or paste entries in the console command modes
- Command modes have distinctive prompts
- Enter key instructs device to parse and execute the command
- Two primary EXEC modes are user mode and privileged mode

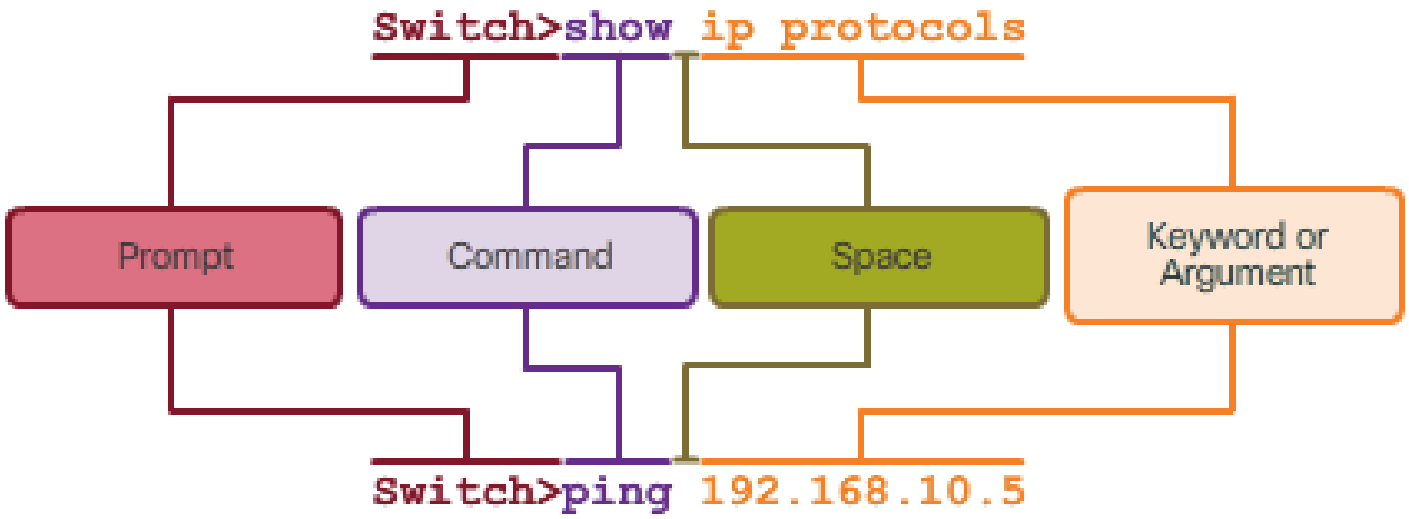
First Mode

User Mode
- Limited examination of switch or router
- Command prompt: hostname>

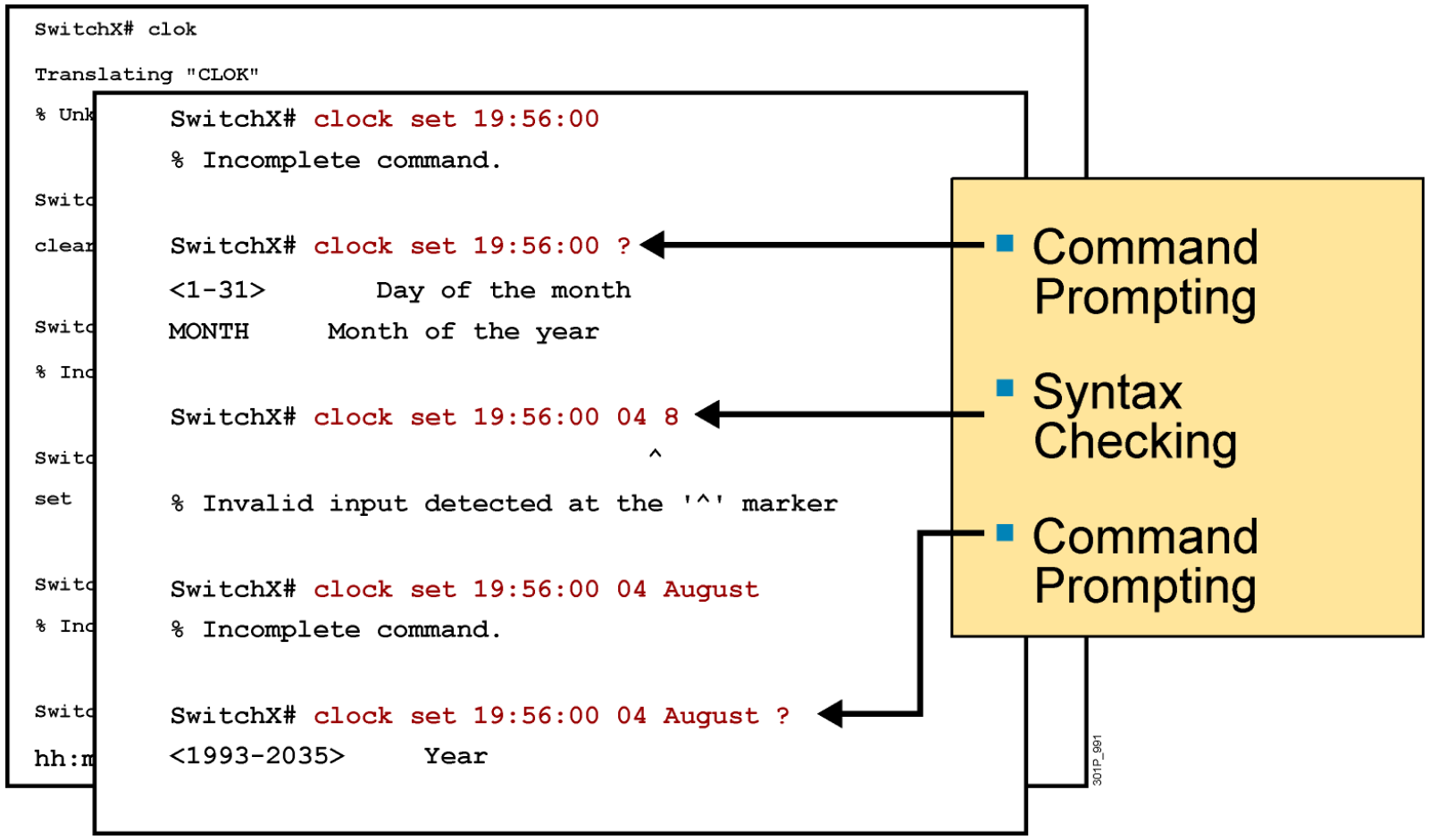
Second Mode (and Most Commonly Used)

Privileged (aka Enabled) Mode
- Detailed examination of switch or router
- Enables configuration and debugging
- Prerequisite for other configuration modes
- Command prompt: hostname#

COMMAND STRUCTURE



CONTEXT-SENSITIVE HELP



EDITING SHORTCUTS

```
SwitchX>$ value for customers, employees, and partners.
```

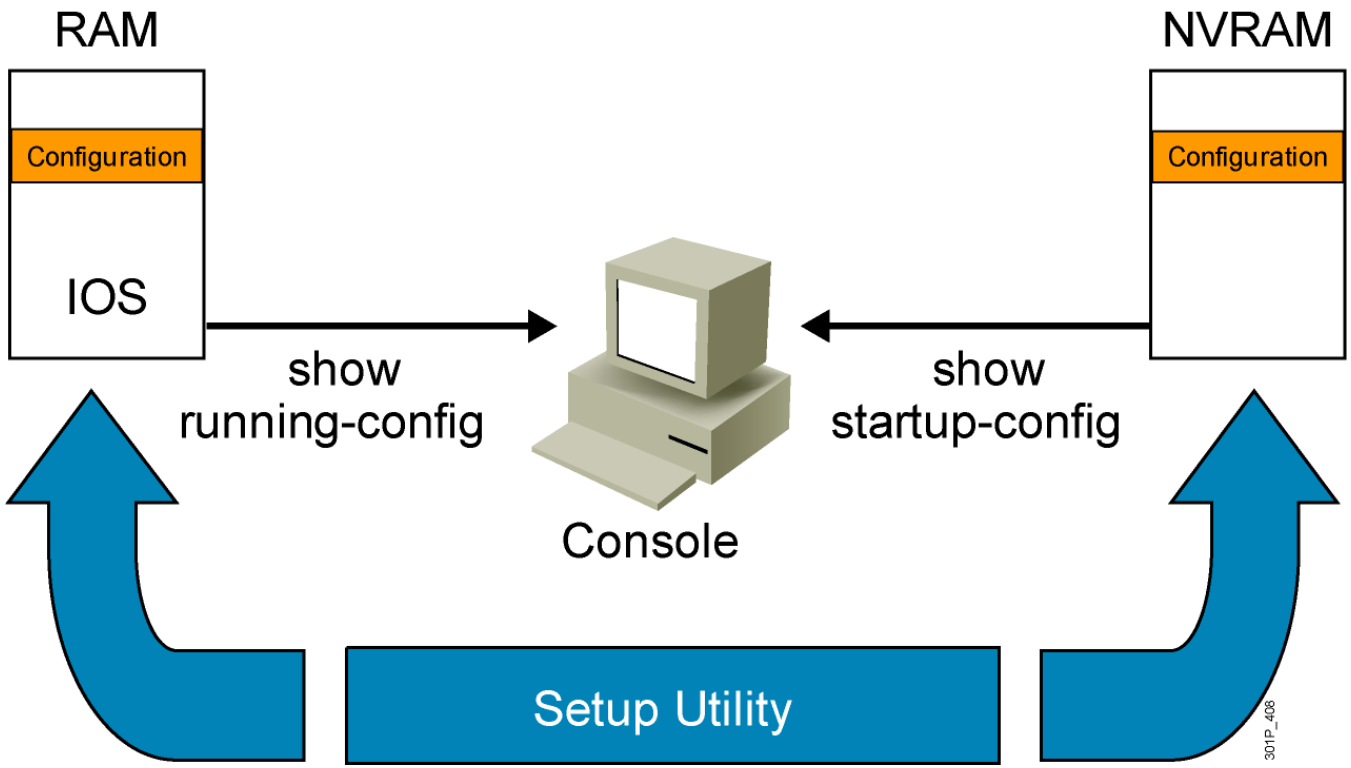
	(Automatic scrolling of long lines)
Ctrl-A	Move to the beginning of the command line.
Ctrl-E	Move to the end of the command line.
Esc-B	Move back one word.
Esc-F	Move forward one word.
Ctrl-B	Move back one character.
Ctrl-F	Move forward one character.
Ctrl-D	Delete a single character.

301P_980

Ctrl-P or Up Arrow	**Recalls last (previous) commands.**
Ctrl-N or Down Arrow	**Recalls more recent commands.**
`show history`	**Shows command buffer contents.**
`terminal history size` *lines*	**Sets session command buffer size.**

022P_249

CONFIGURATION



In RAM

```
SwitchX#show running-config
Building configuration...??
Current configuration:?
!?
version 12.0
!
 -- More --
```

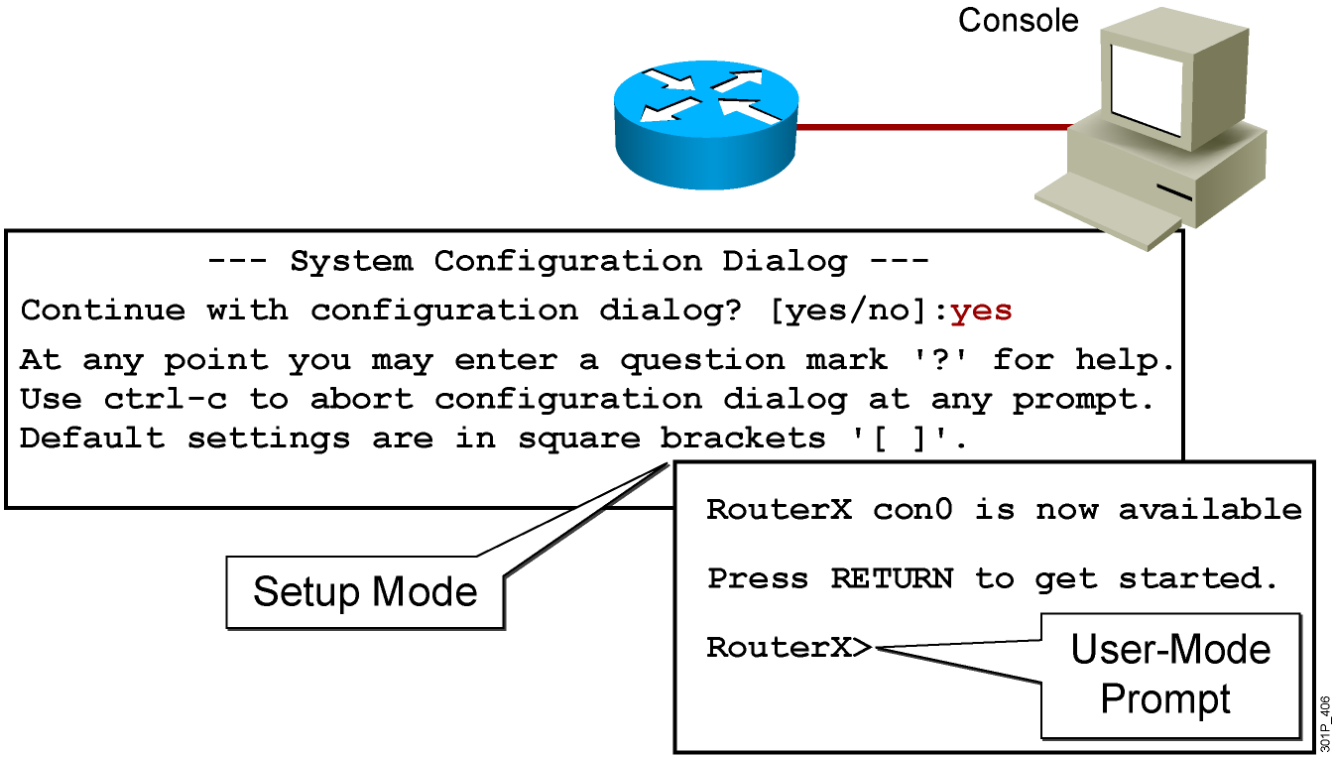
In NVRAM

```
SwitchX#show startup-config
Using 1359 out of 32762 bytes
!
version 12.0
!
 -- More --
```

301P_987

STARTING A DEVICE

- Unconfigured vs. configured device



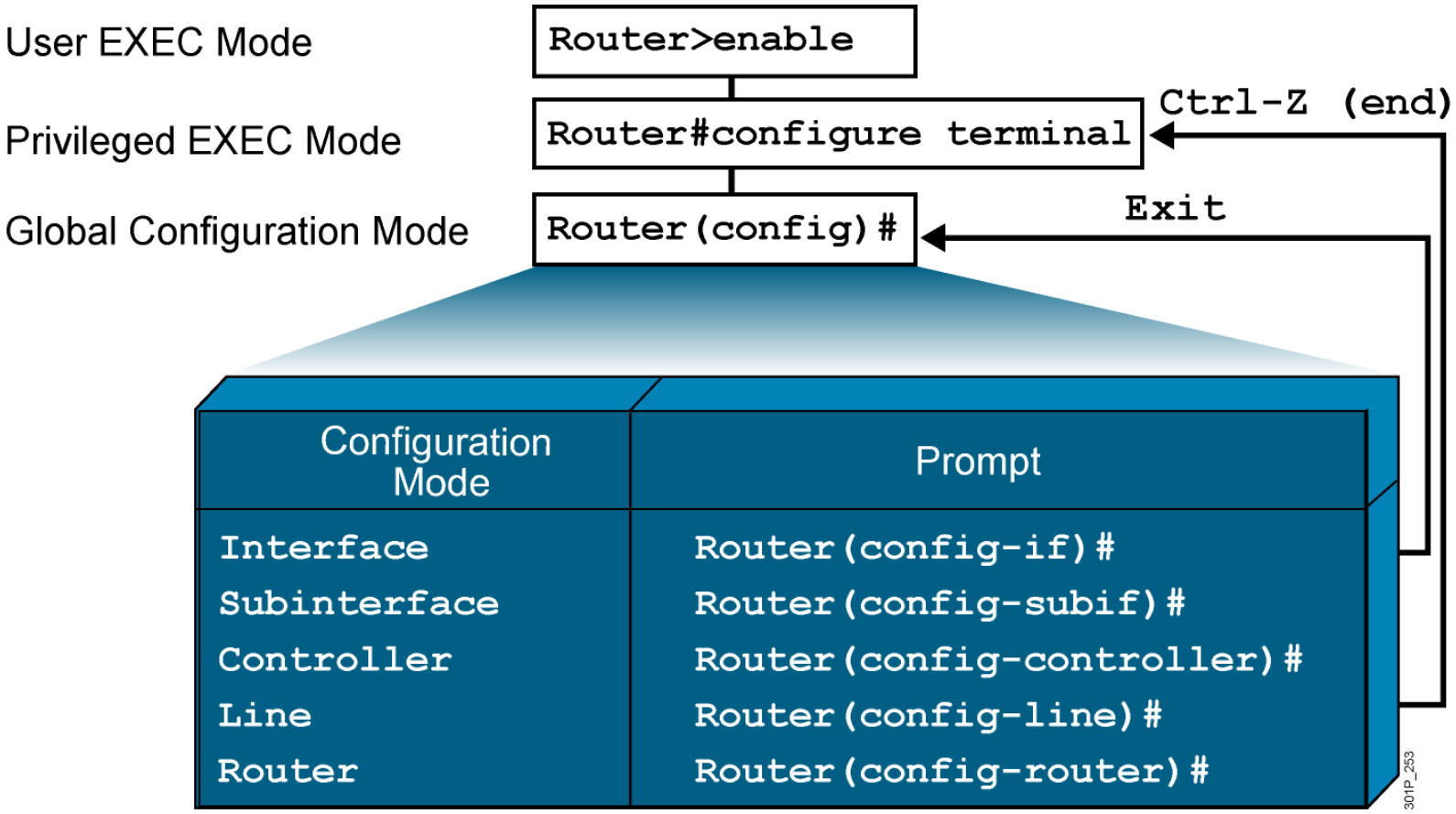
The show version Command

PacketTracer

IOS

```
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

RouterX uptime is 2 days, 21 hours, 15 minutes
System returned to ROM by power-on
System image file is "flash:c2800nm-advipservicesk9-mz.124-12.bin"


This product contains cryptographic features and is subject to United States and local country laws governing import,
export, transfer and use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are
responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable
laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 2811 (revision 53.50) with 249856K/12288K bytes of memory.
Processor board ID FTX1107A6BB
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

RouterX#
```

Overview of Router Modes



SAVING CONFIGURATIONS

- Copies the current configuration to NVRAM

```
RouterX#
RouterX# copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
RourterX#
```

CONFIGURING ROUTER IDENTIFICATION

PacketTracer

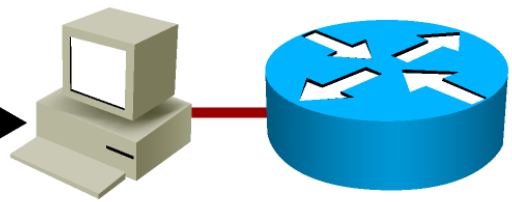
IOS

Router Name

```
Router(config)#hostname RouterX
RouterX(config)#
```

Message-of-the-Day Banner

```
RouterX(config)#banner motd  #
      Enter TEXT message. End with
      the character #. You have
      entered a secured system.
      Authorized access only! #
```



327P_131

CONSOLE-LINE COMMANDS


```
RouterX(config)#line console 0
RouterX(config-line)#exec-timeout 20 30
```

- Modifies console session timeout

```
RouterX(config)#line console 0
RouterX(config-line)#logging synchronous
```

- Redisplays interrupted console input

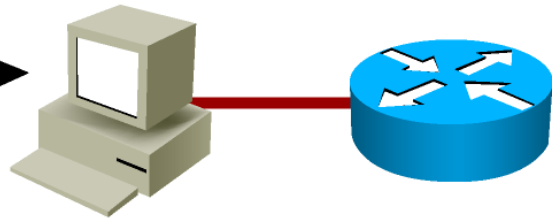
CONFIGURING A ROUTER PASSWORD

PacketTracer

IOS

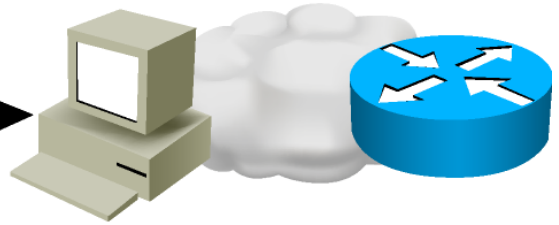
Console Password

```
RouterX(config)#line console 0
RouterX(config-line)#login
RouterX(config-line)#password cisco
```



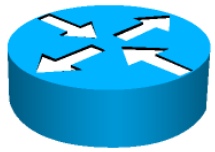
Virtual Terminal Password

```
RouterX(config)#line vty 0 4
RouterX(config-line)#login
RouterX(config-line)#password sanjose
```



Enable Password

```
RouterX(config)#enable password cisco
```



Secret Password

```
RouterX(config)#enable secret sanfran
```

Service Password-Encryption Commands

```
RouterX(config)#service password encryption
RouterX(config)#no service password-encryption
```

301P_984

CONFIGURING THE LOGIN BANNER

- Defines and enables a customized banner to be displayed before the username and password login prompts

```
RouterX# banner login " Access for authorized users only. Please enter your
username and password. "
```

Telnet vs. SSH Access

- Telnet
  - Most common access method
  - Insecure
- SSH
  - Encrypted
  - IP domain must be defined
  - key must be generated

```
!--- The username command create the username and password for the SSH session
username cisco password 0 cisco
ip domain-name mydomain.com
crypto key generate rsa
ip ssh version 2
line vty 0 4
  login local
  transport input ssh
```

CONFIGURING AN INTERFACE


```
RouterX(config)# interface type number
RouterX(config-if)#
```

- type includes serial, ethernet, token ring, fddi, hssi, loopback, dialer, null, async, atm, bri, tunnel, and so on
- number is used to identify individual interfaces

```
RouterX(config)# interface type slot/port
RouterX(config-if)#
```

- For modular routers, selects an interface

```
RouterX(config-if)# exit
```

- Quits from current interface configuration mode

CONFIGURING INTERFACE DESCRIPTION

```
RouterX(config-if)# description string
```

- *string is a c*omment or a description to help you remember what is attached to this interface.
- The maximum number of characters for the *string* argument is 238.

DISABLING OR ENABLING AN INTERFACE

PacketTracer

IOS

```
RouterX# configure terminal
RouterX(config)# interface serial 0
RouterX(config-if)# shutdown
%LINK-5-CHANGED: Interface Serial0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down
```

- Administratively turns off an interface

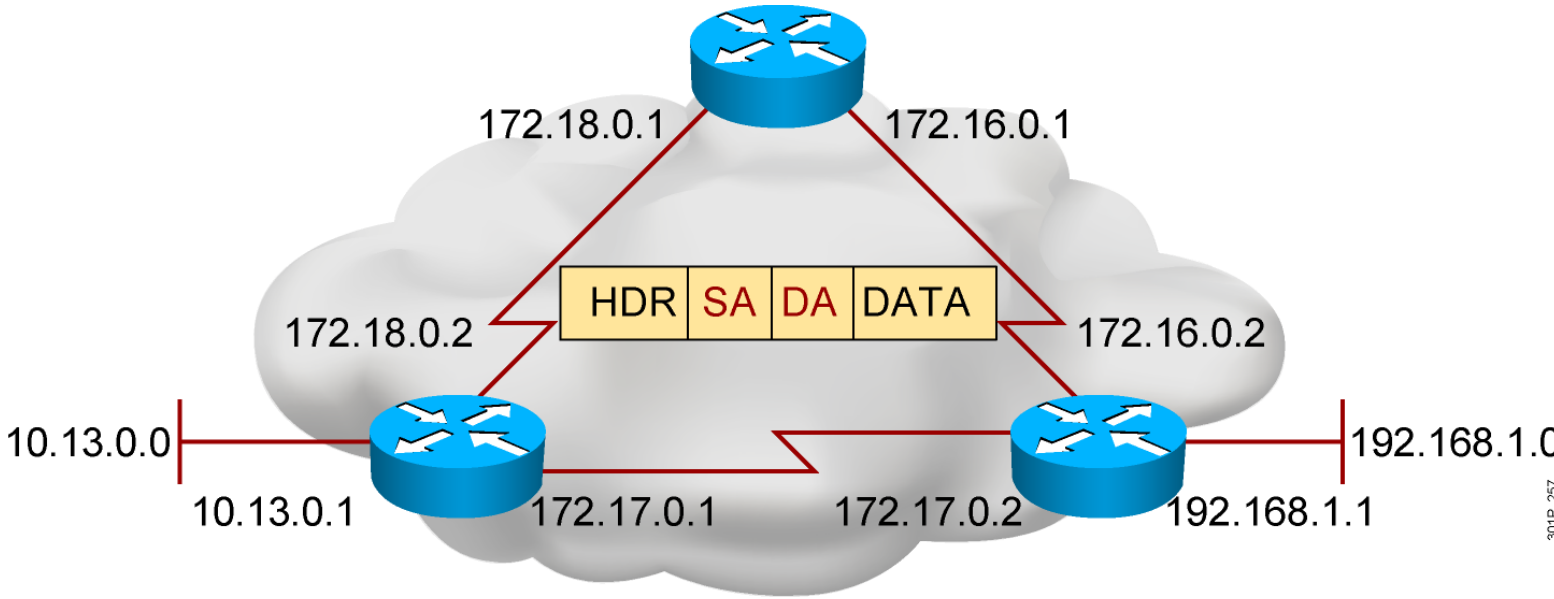
```
RouterX# configure terminal
RouterX(config)# interface serial 0
RouterX(config-if)# no shutdown
%LINK-3-UPDOWN:  Interface Serial0, changed state to up
%LINEPROTO-5-UPDOWN: Line Protocol on Interface Serial0, changed state to up
```

- Enables an interface that is administratively shut down

CONFIGURING IP ADDRESSES

PacketTracer

IOS




```
SwitchX(config)#interface identifier number
SwitchX(config-if)#ip address {ip address} {mask}
```

```
SwitchX(config)#interface gi0/0 1
SwitchX(config-if)#ip address 10.5.5.11 255.255.255.0
SwitchX(config-if)#no shutdown
```

SHOW INTERFACES COMMAND

PacketTracer

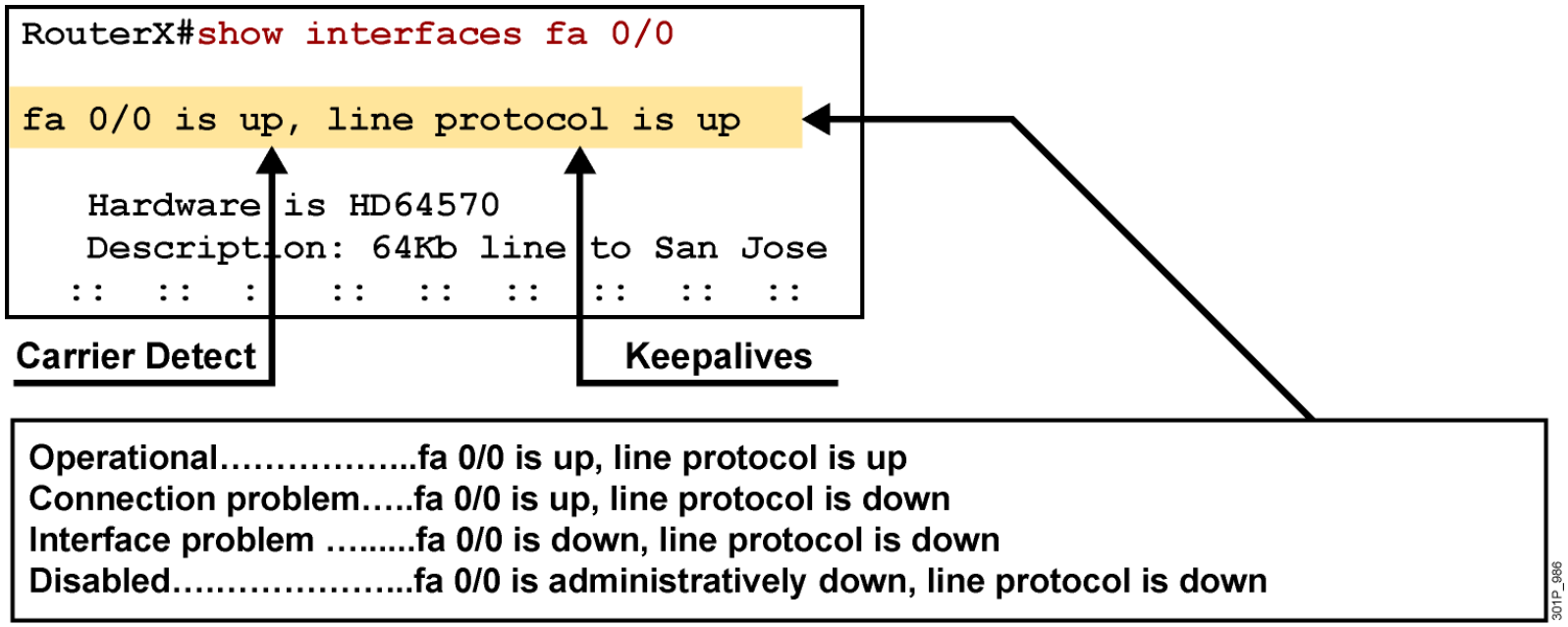
IOS

```
RouterX# show interfaces
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1e5d.ae2f (bia 00e0.1e5d.ae2f)
  Internet address is 10.1.1.11/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     81833 packets input, 27556491 bytes, 0 no buffer
     Received 42308 broadcasts, 0 runts, 0 giants, 0 throttles
     1 input errors, 0 CRC, 0 frame, 0 overrun, 1 ignored, 0 abort
     0 input packets with dribble condition detected
     55794 packets output, 3929696 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 4 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Interpreting the Interface Status

PacketTracer

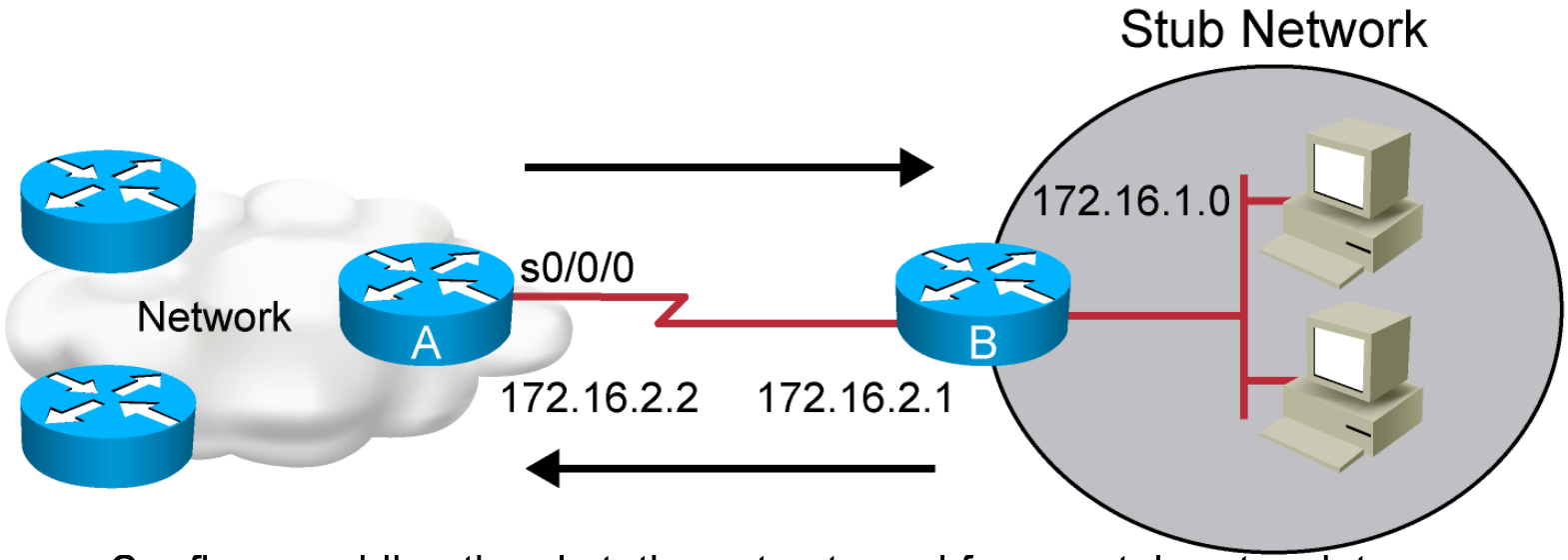
IOS



STATIC ROUTES

PacketTracer

IOS



Configure unidirectional static routes to and from a stub network to allow communications to occur.

STATIC ROUTE CONFIGURATION

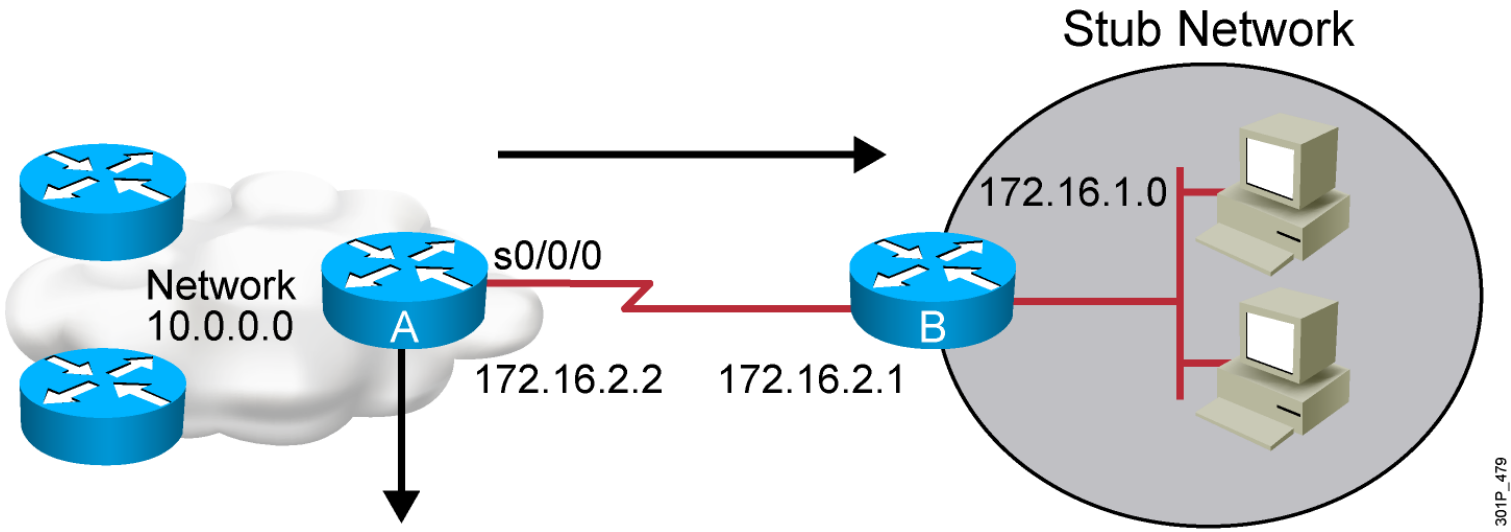
PacketTracer

IOS

```
RouterX(config)# ip route network  [mask]
{address | interface}[distance] [permanent]
```

- Defines a path to an IP destination network or subnet or host
- Address = IP address of the next hop router
- Interface = outbound interface of the local router

STATIC ROUTE EXAMPLE




```
RouterX(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

or

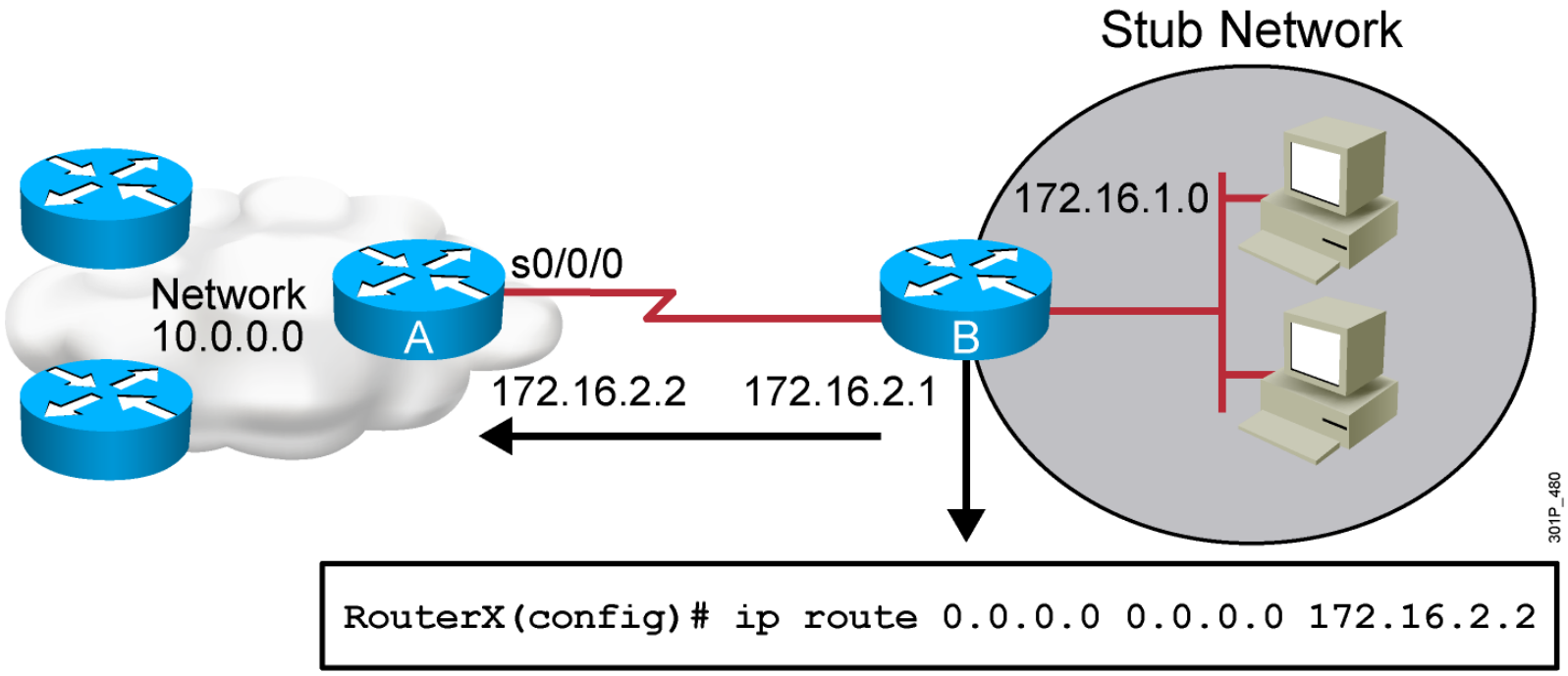
```
Router(config)# ip route 172.16.1.0 255.255.255.0 s0/0/0
```

- This is a unidirectional route. You must have a route configured in the opposite direction.

DEFAULT ROUTES

PacketTracer

IOS



- This route allows the stub network to reach all known networks beyond Router A.

VERIFYING ROUTE CONFIGURATION

PacketTracer

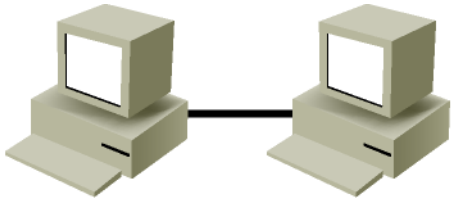
IOS

```
RouterX# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0
```

WAN Connection Bandwidth

PacketTracer

IOS



1 DS0 — DS0 = 64 kb/s

24 DS0s — DS1 or T1 = 1.544 Mb/s

672 DS0s — DS3 or T3 = 43.736 Mb/s

CONFIGURING A SERIAL INTERFACE

PacketTracer

IOS

Enter global configuration mode.

```
RouterX# configure terminal
RouterX(config)#
```

Specify interface.

```
RouterX(config)#interface serial 0/0/0
RouterX(config-if)#
```

Set clock rate (on DCE interfaces only).

```
RouterX(config-if)# clock rate 64000
RouterX(config-if)#
```

Set bandwidth (recommended).

```
RouterX(config-if)# bandwidth 64
RouterX(config-if)# exit
RouterX(config)# exit
RouterX#
```

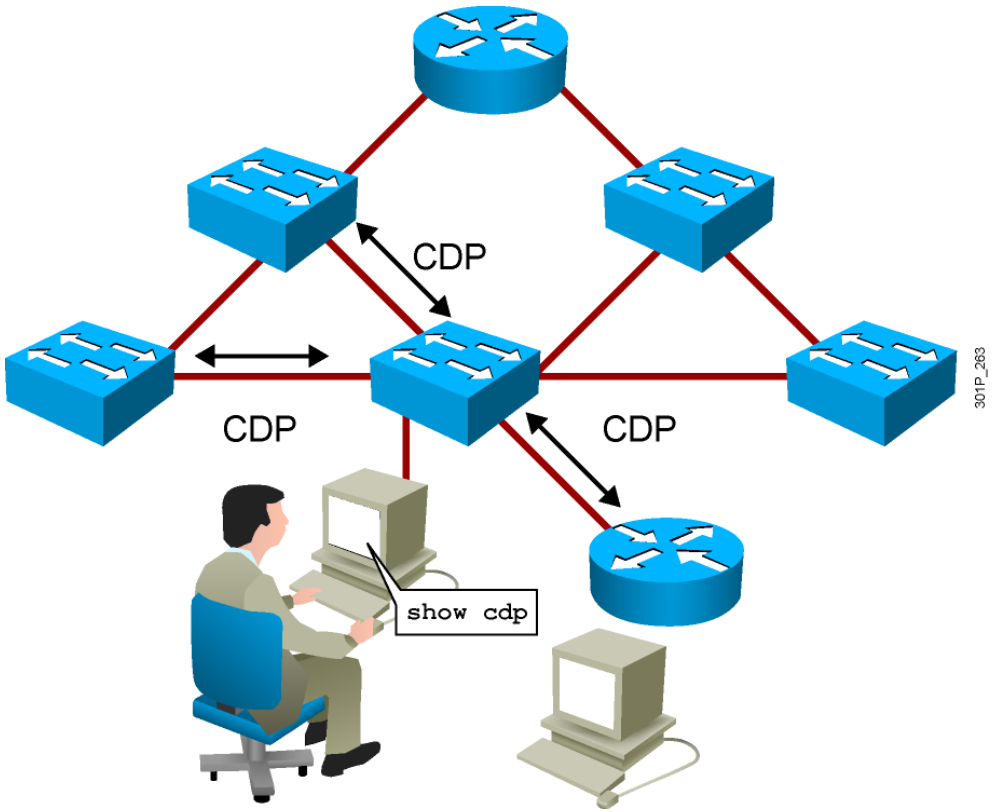
The show controller Command

- Shows the serial cable type

```
RouterX#show controller serial 0/0/0
HD unit 0, idb = 0x121C04, driver structure at 0x127078
buffer size 1524  HD unit 0, V.35 DTE cable
   .
   .
   .
```

CDP

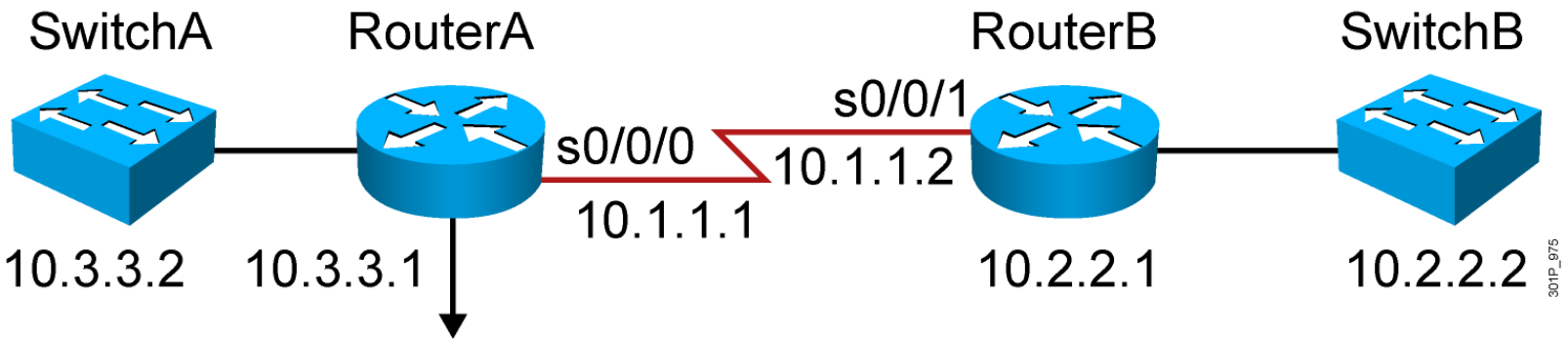
- Cisco Discovery Protocol runs on Cisco IOS devices.
- Summary information includes:
  - Device identifiers
  - Address list
  - Port identifier
  - Capabilities list
  - Platform



SHOW CDP NEIGHBORS COMMAND

PacketTracer

IOS

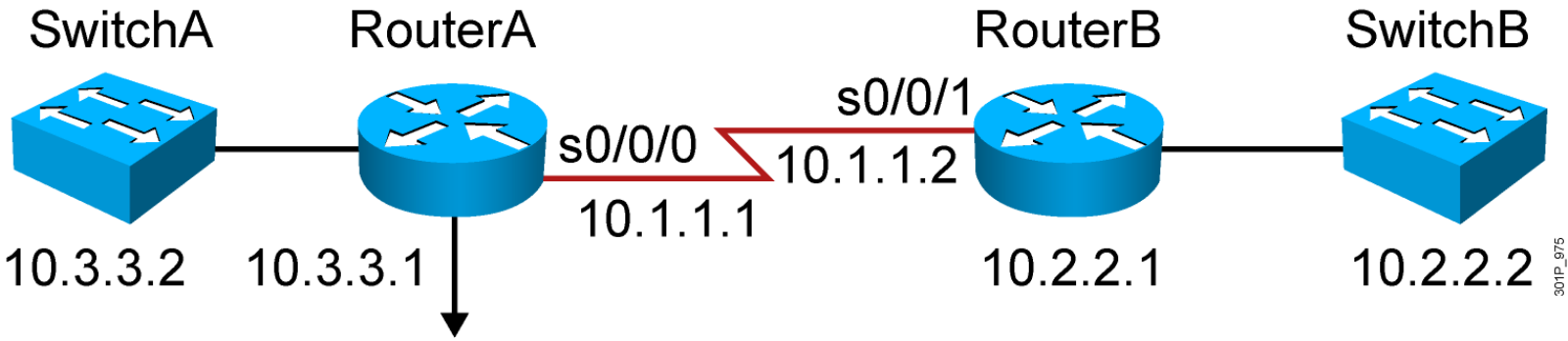



```
RouterA# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID    Local Intrfce    Holdtme    Capability  Platform  Port ID
SwitchA          fa0/0        122          S I       WS-C2960- fa0/2
RouterB          s0/0/0        177         R S I      2811      s0/0/1
```

THE SHOW CDP ENTRY COMMAND

PacketTracer

IOS




```
Device ID: RouterB
Entry address(es):
  IP address: 10.1.1.2
Platform: Cisco 2811,  Capabilities: Router Switch IGMP
Interface: Serial0/0/0,  Port ID (outgoing port): Serial0/0/1
Holdtime : 155 sec

Version :
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M),
Version 12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 12:02 by prod_rel_team
```

CONFIGURING A DHCPV4 SERVER

PacketTracer

IOS

A Cisco router running the Cisco IOS software can be configured to act as a DHCPv4 server. To set up DHCP:

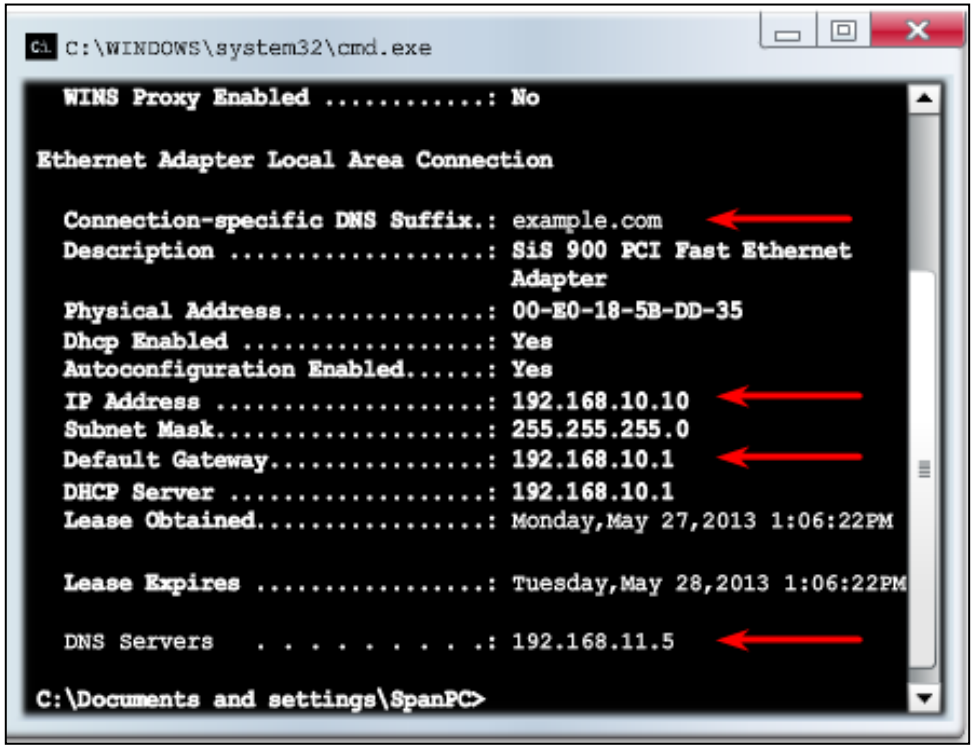
1. Exclude addresses from the pool.
2. Set up the DHCP pool name.
3. Define the range of addresses and subnet mask. Use the **`default-router`** command for the default gateway. Optional parameters that can be included in the *pool – dns server*, *domain-name*.

To disable DHCP, use the **no service dhcp** command.

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

VERIFYING A DHCPV4 SERVER

- Commands to verify DHCP:
  - `show running-config | section dhcp`
  - `show ip dhcp binding`
  - `show ip dhcp server statistics`
- On the PC, issue the **`ipconfig /all`** command.



DHCPv4 Relay

- Using an IP helper address enables a router to forward DHCPv4 broadcasts to the DHCPv4 server. Acting as a relay.

PacketTracer

IOS

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
<Output omitted>
```

CONFIGURING A DHCPV4 CLIENT

PacketTracer

IOS


```
SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
SOHO(config-if)#
*Jan 31 17:31:11.507: %DHCP-6-ADDRESS_ASSIGN: Interface
GigabitEthernet0/1 assigned DHCP address 209.165.201.12, mask
255.255.255.224, hostname SOHO
SOHO(config-if)# end
SOHO# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  <Output omitted>
```

ACL Operation

An inbound ACL filters packets coming into a specific interface and before they are routed to the outbound interface.

An outbound ACL filters packets after being routed, regardless of the inbound interface.

The last statement of an ACL is always an implicit deny. This statement is automatically inserted at the end of each ACL even though it is not physically present. The implicit deny blocks all traffic. Because of this implicit deny, an ACL that does not have at least one permit statement will block all traffic.

Types of Cisco IPv4 ACLs

Standard ACLs

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Standard ACLs filter IP packets based on the source address only.

Extended ACLs

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Extended ACLs filter IP packets based on several attributes, including the following:

- Source and destination IP addresses
- Source and destination TCP and UDP ports
- Protocol type/ Protocol number (example: IP, ICP, UDP, TCP, etc.)

PacketTracer

IOS

Wildcard Mask Examples

Example 1

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.0.	00000000.00000000.00000000.00000000
Result	192.168.1.1	11000000.10101000.00000001.00000001

Example 2

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	255.255.255.255	11111111.11111111.11111111.11111111
Result	0.0.0.0	00000000.00000000.00000000.00000000

Example 3

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.255	00000000.00000000.00000000.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000

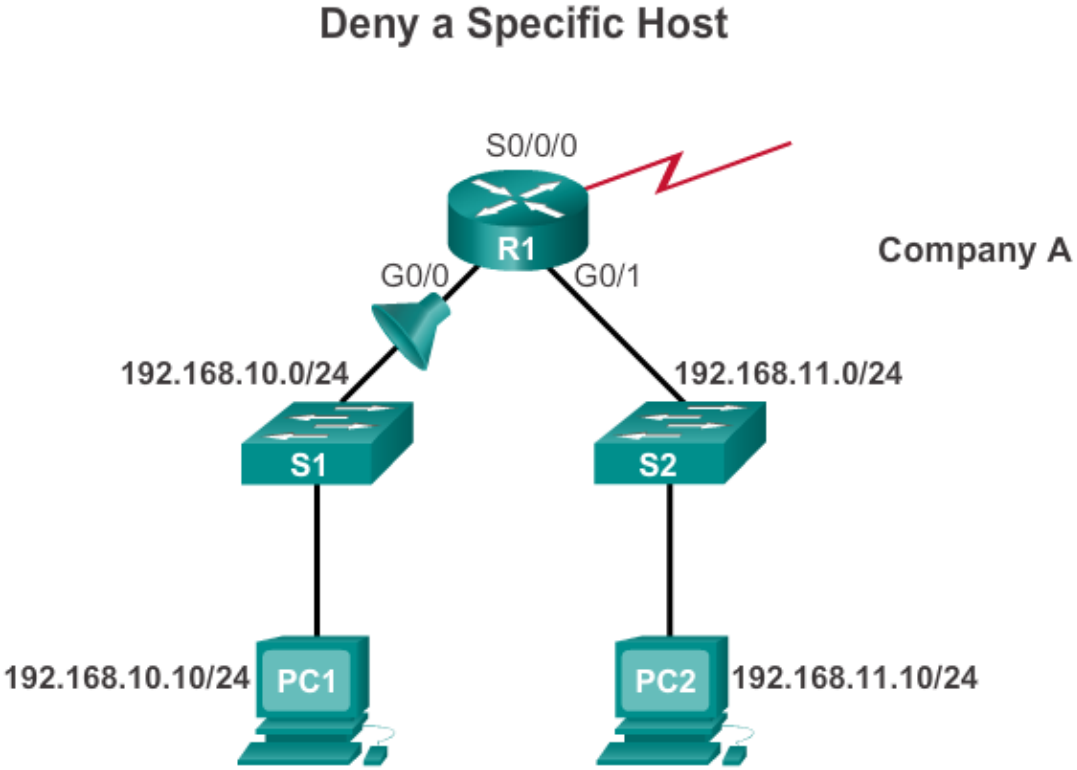
Example 1

	Decimal	Binary
IP Address	192.168.16.0	11000000.10101000.00010000.00000000
Wildcard Mask	0.0.15.255	00000000.00000000.00001111.11111111
Result Range	192.168.16.0 to 192.168.31.255	11000000.10101000.00010000.00000000 to 11000000.10101000.00011111.11111111

APPLYING STANDARD ACLS TO INTERFACES (CONT.)

PacketTracer

IOS

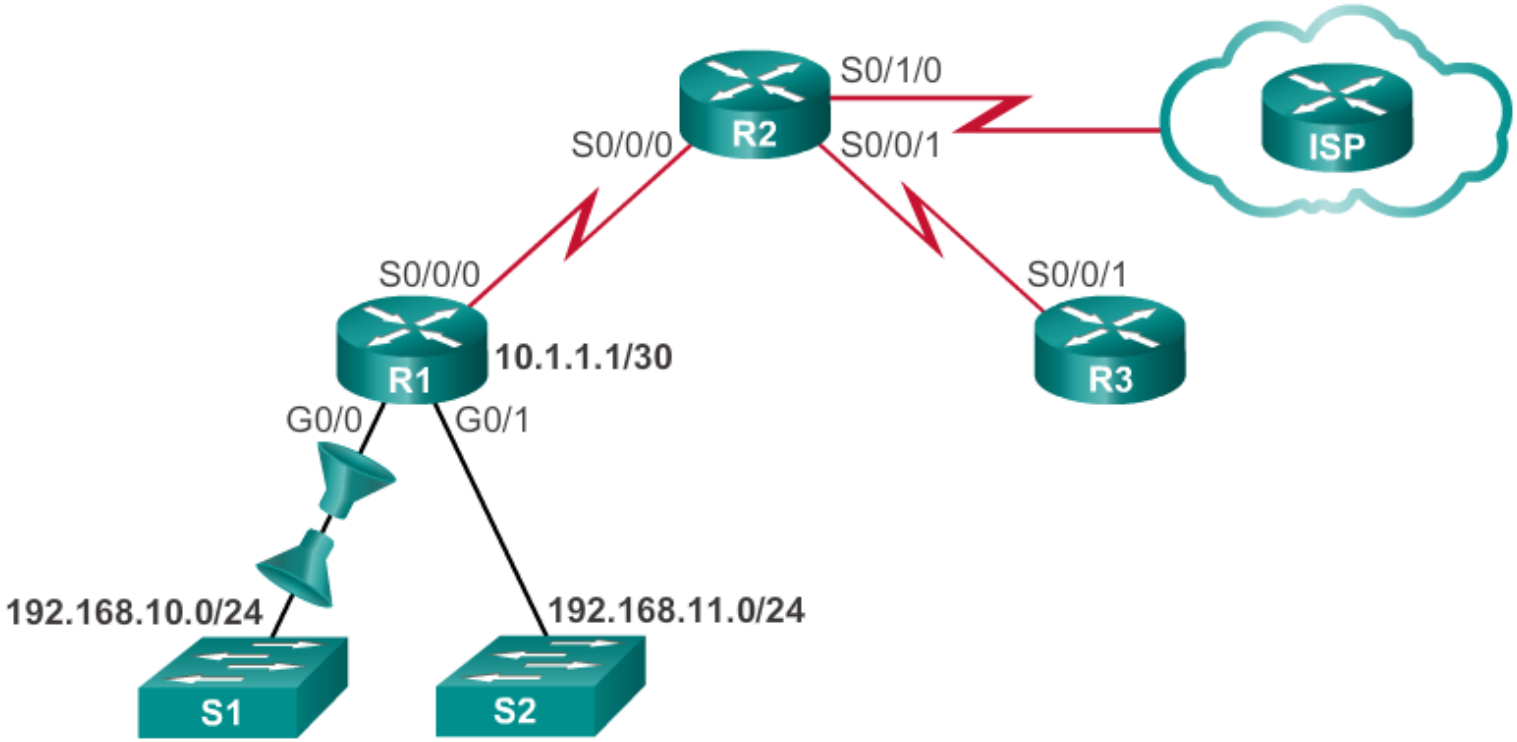



```
R1(config)#no access-list 1
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 permit any
R1(config)#interface g0/0
R1(config-if)#ip access-group 1 in
```

Applying Extended ACLs to

PacketTracer

IOS

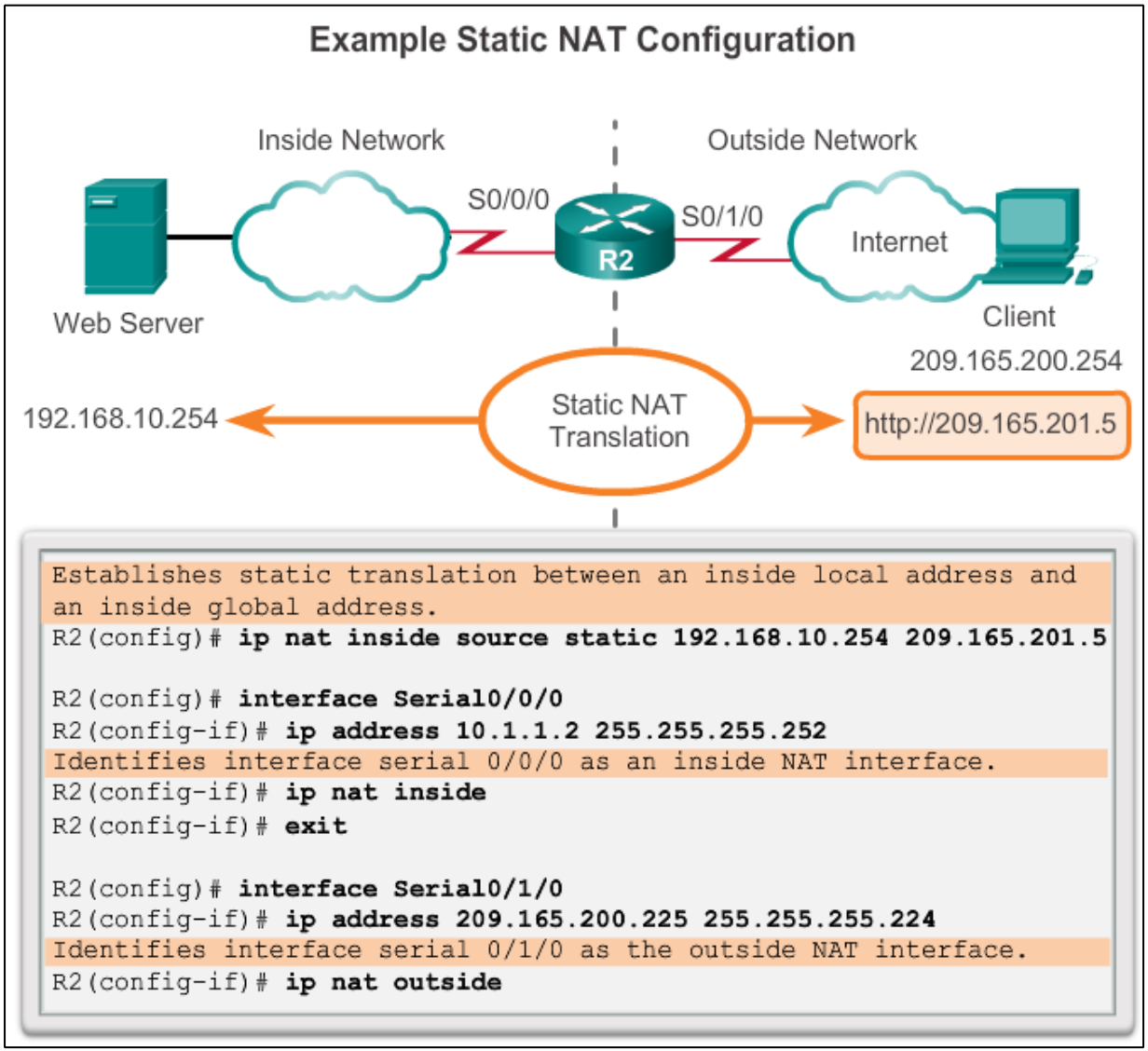



```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)#interface g0/0
R1(config-if)#ip access-group 103 in
R1(config-if)#ip access-group 104 out
```

CONFIGURING STATIC NAT

PacketTracer

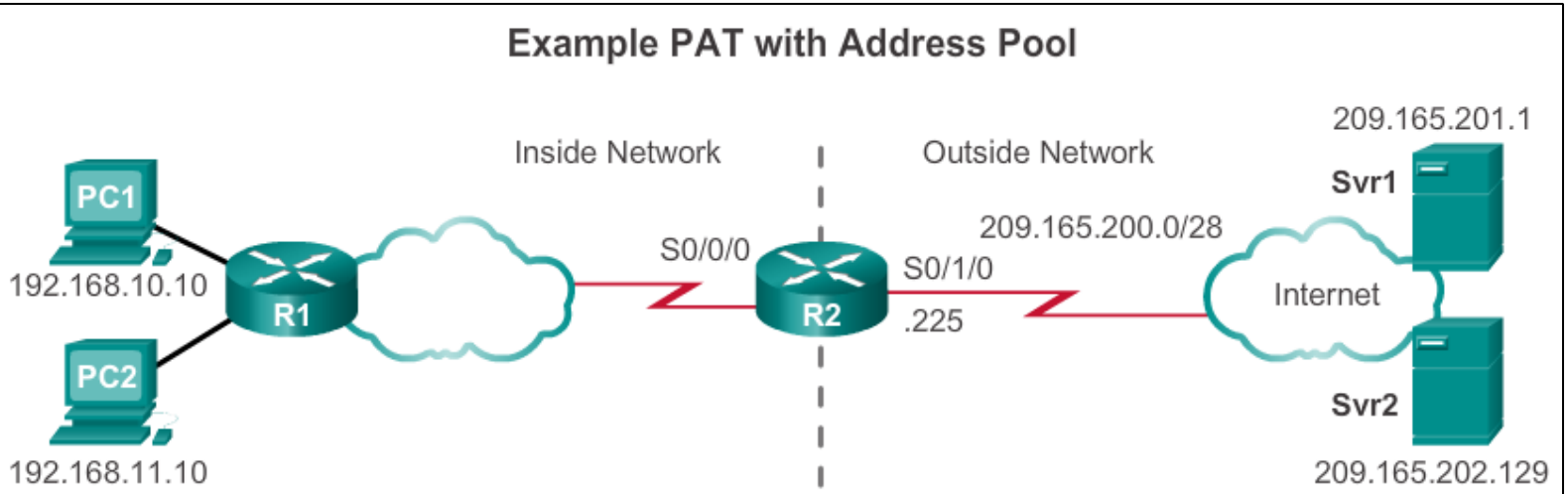
IOS



CONFIGURING PAT

PacketTracer

IOS



Define which addresses are eligible to be translated.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Bind NAT-POOL2 with ACL 1.

```
R2(config)# ip nat inside source list 1 interface s0/1/0
overload
```

Identify interface serial 0/0/0 as an inside NAT interface.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

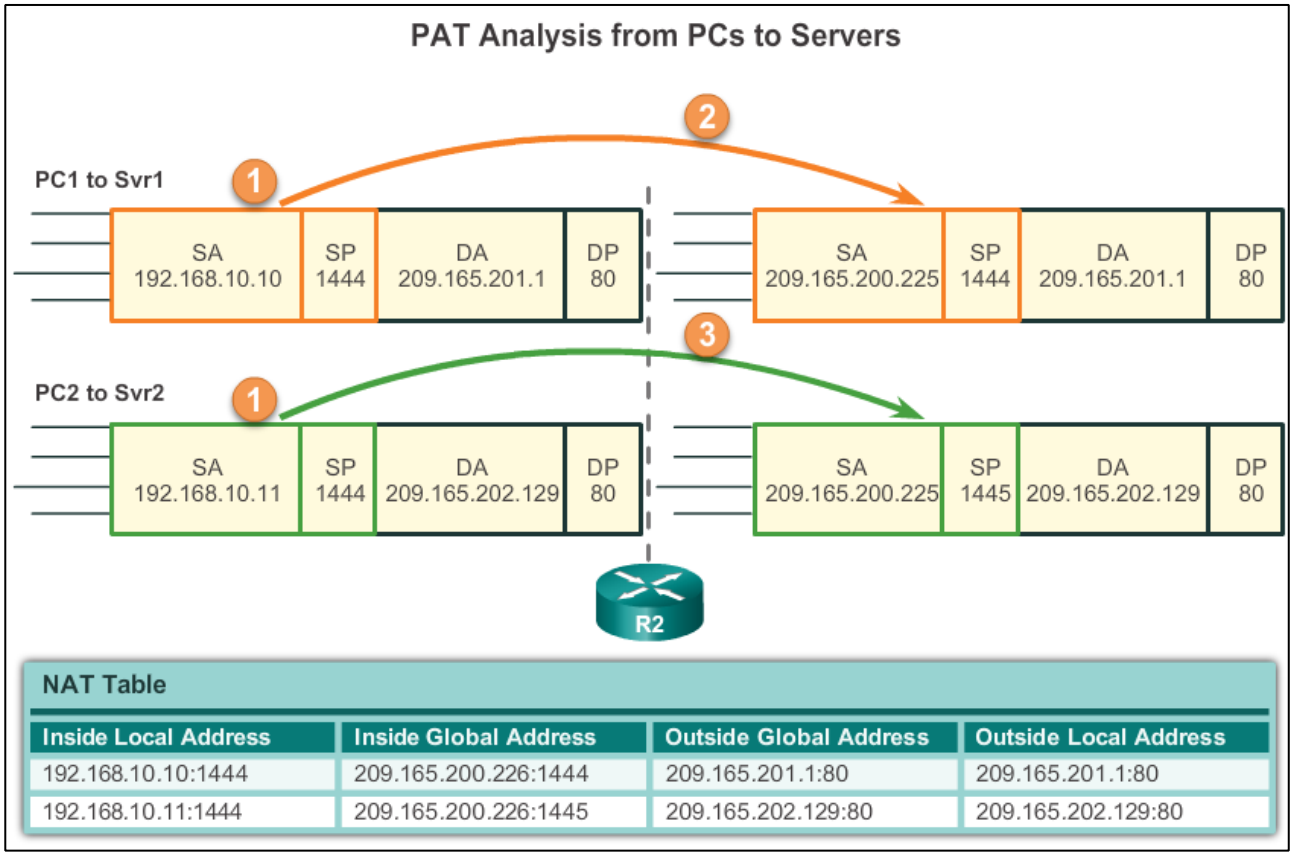
Identify interface serial 0/1/0 as the outside NAT interface.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

VERIFYING NAT

PacketTracer

IOS



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.226:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.226:1445	209.165.202.129:80	209.165.202.129:80

Verifying PAT Translations

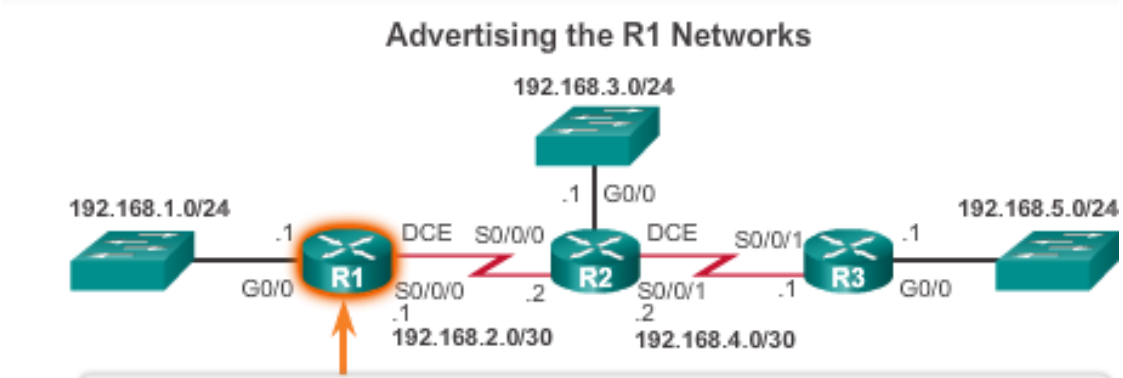
```
R2# show ip nat translations
Pro  Inside global          Inside local       Outside local      Outside global
tcp  209.165.200.226:51839  192.168.10.10:51839  209.165.201.1:80   209.165.201.1:80
tcp  209.165.200.226:42558  192.168.11.10:42558  209.165.202.129:80 209.165.202.129:80
R2#
```

CONFIGURING THE RIP PROTOCOL

PacketTracer

IOS

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# router rip
R1(config-router)#
```




```
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#
```

EXAMINING DEFAULT RIP SETTINGS

PacketTracer

IOS

Verifying RIP Settings on R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 16 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip

  Default version control: send version 1, receive any version
    Interface              Send  Recv  Triggered RIP  Key-chain
    GigabitEthernet0/0     1     1 2
    Serial0/0/0            1     1 2

  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0

  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2          120      00:00:15
  Distance: (default is 120)

R1#
```

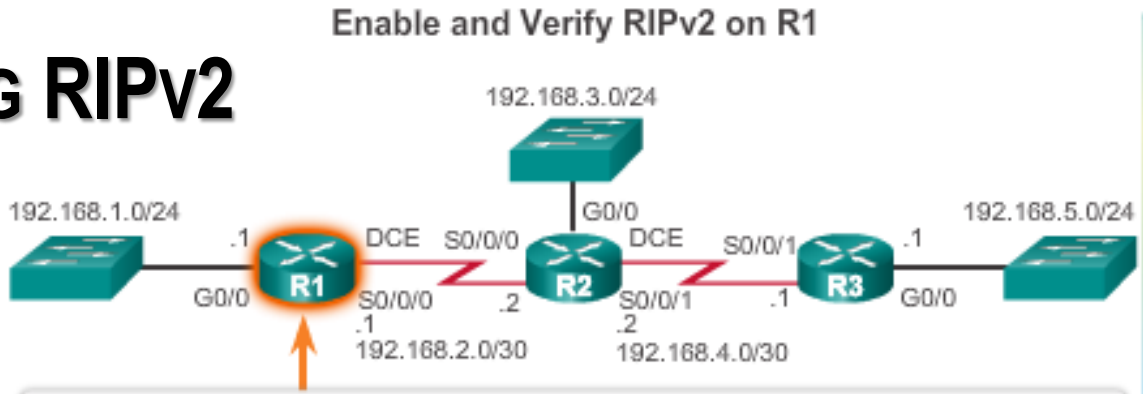
Verifying RIP Routes on R1

```
R1# show ip route | begin Gateway
Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Serial0/0/0
L        192.168.2.1/32 is directly connected, Serial0/0/0
R     192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
R     192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
R     192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:24, Serial0/0/0
R1#
```

ENABLING RIPV2

PacketTracer

IOS



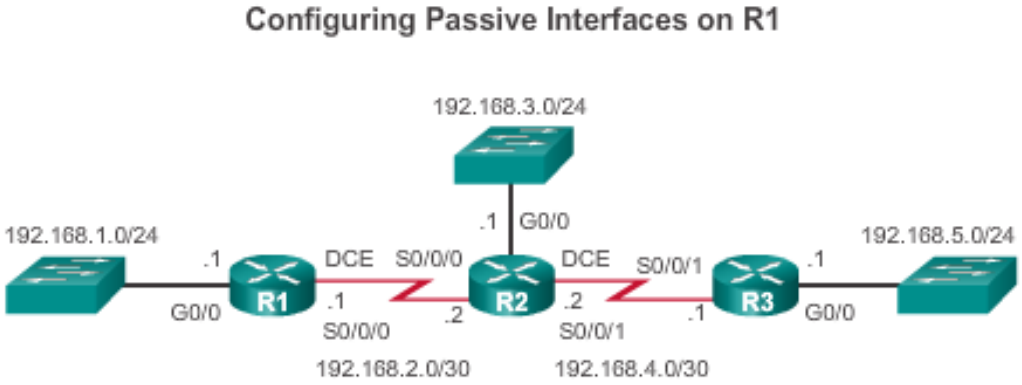

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# ^Z
R1#
R1# show ip protocols | section Default
  Default version control: send version 2, receive version 2
    Interface            Send  Recv  Triggered RIP  Key-chain
    GigabitEthernet0/0   2     2
    Serial0/0/0          2     2
R1#
```

- Similarly to RIPv1, RIPv2 automatically summarizes networks at major network boundaries by default.
- To modify the default RIPv2 behavior of automatic summarization, use the **`no auto-summary`** router configuration mode command

CONFIGURING PASSIVE INTERFACES

PacketTracer

IOS



Sending out unneeded updates on a LAN impacts the network in three ways:

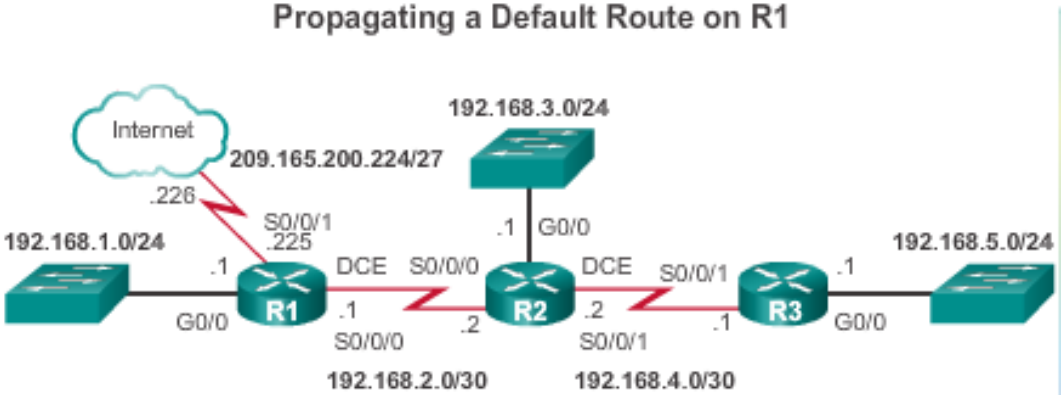
- Wasted Bandwidth
- Wasted Resources
- Security Risk

```
R1(config)# router rip
R1(config-router)# passive-interface g0/0
R1(config-router)# end
R1#
R1# show ip protocols | begin Default
  Default version control: send version 2, receive version 2
    Interface              Send  Recv  Triggered RIP  Key-chain
    Serial0/0/0            2     2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2           120      00:00:06
  Distance: (default is 120)

R1#
```

PROPAGATING A DEFAULT ROUTE

PacketTracer

IOS

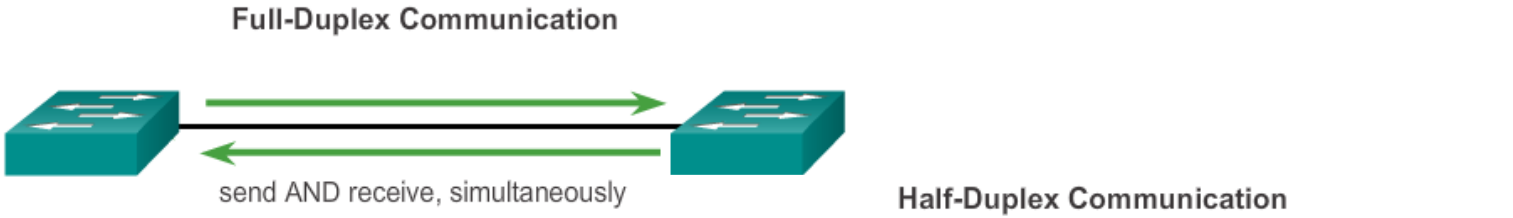


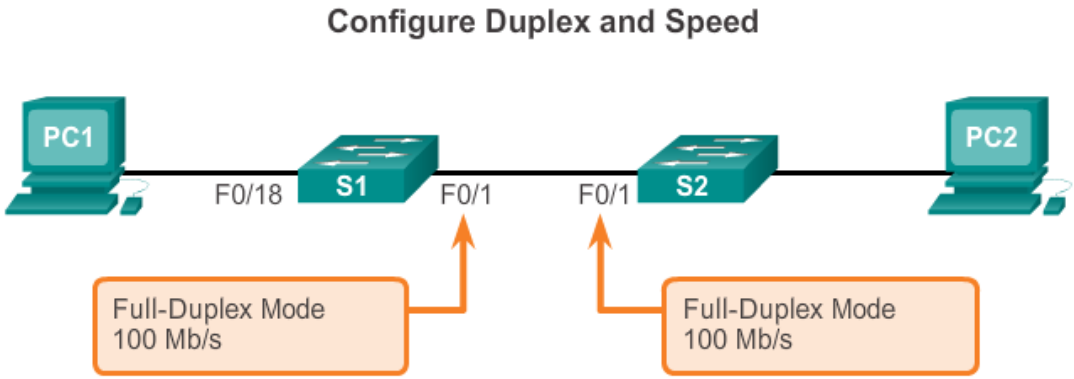

```
R1(config)# ip route 0.0.0.0 0.0.0.0 S0/0/1 209.165.200.226
R1(config)# router rip
R1(config-router)# default-information originate
R1(config-router)# ^Z
R1#
*Mar 10 23:33:51.801: %SYS-5-CONFIG_I: Configured from
console by console
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network
0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.226, Serial0/0/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2
masks
C        192.168.1.0/24 is directly connected,
GigabitEthernet0/0
L        192.168.1.1/32 is directly connected,
GigabitEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2
masks
C        192.168.2.0/24 is directly connected, Serial0/0/0
L        192.168.2.1/32 is directly connected, Serial0/0/0
R     192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:08,
```

CONFIGURING SWITCH PORTS

PacketTracer

IOS





Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface FastEthernet 0/1`
Configure the interface duplex.	`S1(config-if)# duplex full`
Configure the interface speed.	`S1(config-if)# speed 100`
Return to the privileged EXEC mode.	`S1(config-if)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

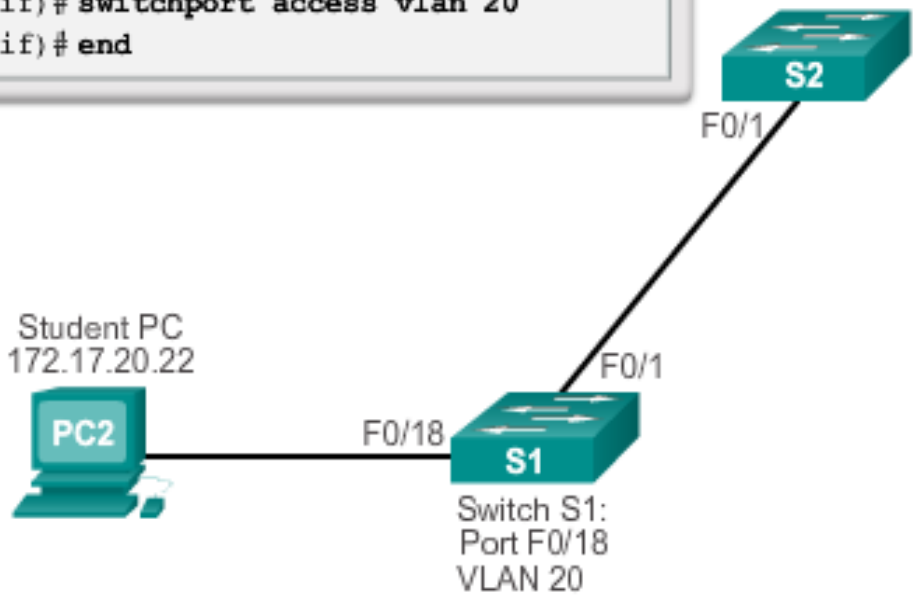
CONFIGURING VLAN

PacketTracer

IOS

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan_id`
Specify a unique name to identify the VLAN.	`S1(config)# name vlan_name`
Return to the privileged EXEC mode.	`S1(config)# end`

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```



VERIFYING VLAN MEMBERSHIP

PacketTracer

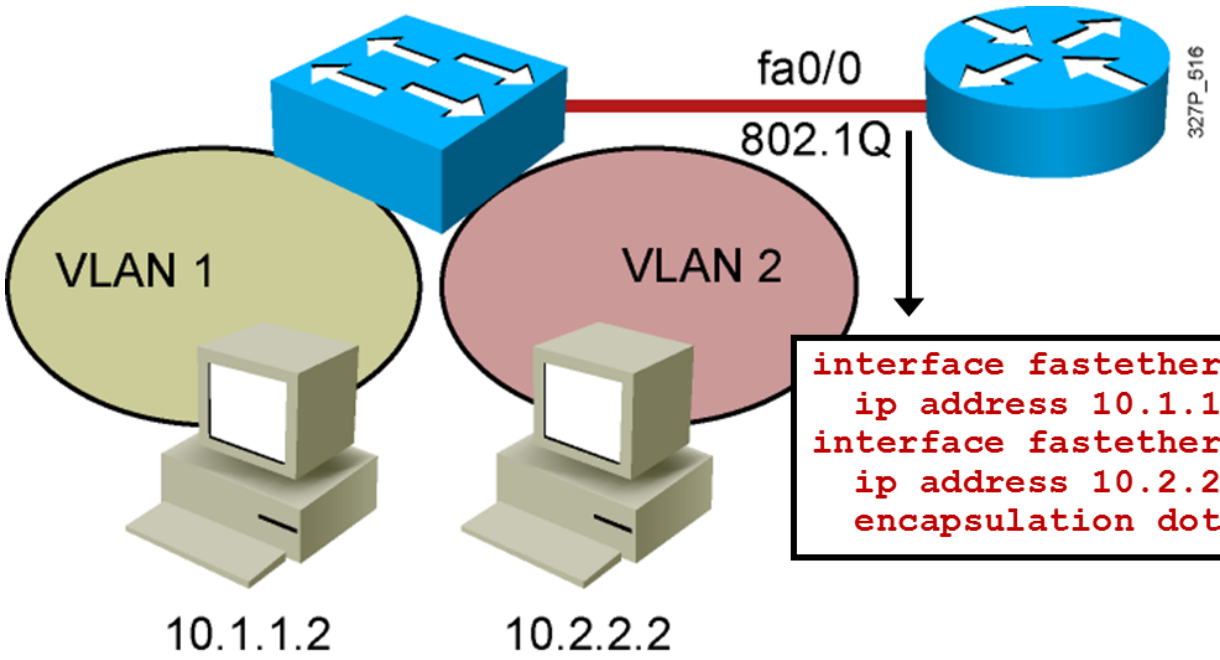
IOS

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

VLAN Name                Status    Ports
---- ----------------    --------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                   Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                   Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                   Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                   Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
S1#
```

ROUTER-ON-A-STICK

PacketTracer

IOS

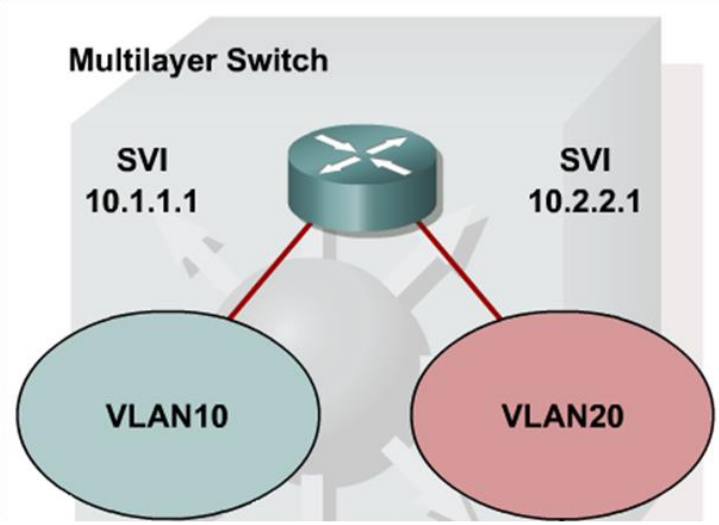



```
interface fastethernet 0/0
  ip address 10.1.1.1 255.255.255.0
interface fastethernet 0/0.2
  ip address 10.2.2.1 255.255.255.0
  encapsulation dot1q 2
```

MULTI-LAYER SWITCHES


```
Switch(config)# ip routing
Switch(config)# vlan 10,20
Switch(config-vlan)# exit
Switch(config)# int vlan10
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# int vlan20
Switch(config-if)# ip address 10.2.2.1 255.255.255.0
```

- `ip routing` enables L3 switching
- This command enables all L3 functions and commands
  - routing table
  - routing protocols



CONFIGURING 802.1Q TRUNK

PacketTracer

IOS

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Force the link to be a trunk link.	`S1(config-if)# switchport mode trunk`
Specify a native VLAN for untagged 802.1Q trunks.	`S1(config-if)# switchport trunk native vlan vlan_id`
Specify the list of VLANs to be allowed on the trunk link.	`S1(config-if)# switchport trunk allowed vlan vlan-list`
Return to the privileged EXEC mode.	`S1(config-if)# end`

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

PacketTracer

IOS

INTRODUCTION TO DTP

- Switch ports can be manually configured to form trunks
- **The Dynamic Trunking Protocol (DTP)** manages trunk negotiation.
  - Switch ports can also be configured to negotiate and establish a trunk link with a connected peer
- DTP is a Cisco proprietary protocol and is enabled, by default, in Cisco Catalyst 2960 and 3560 switches.
  - The default DTP configuration for Cisco Catalyst 2960 and 3560 switches is dynamic auto.
- If the port on the neighbor switch is configured in a trunk mode that supports DTP, it manages the negotiation.
- `(config-if)# switchport mode <mode>`

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

PacketTracer

IOS

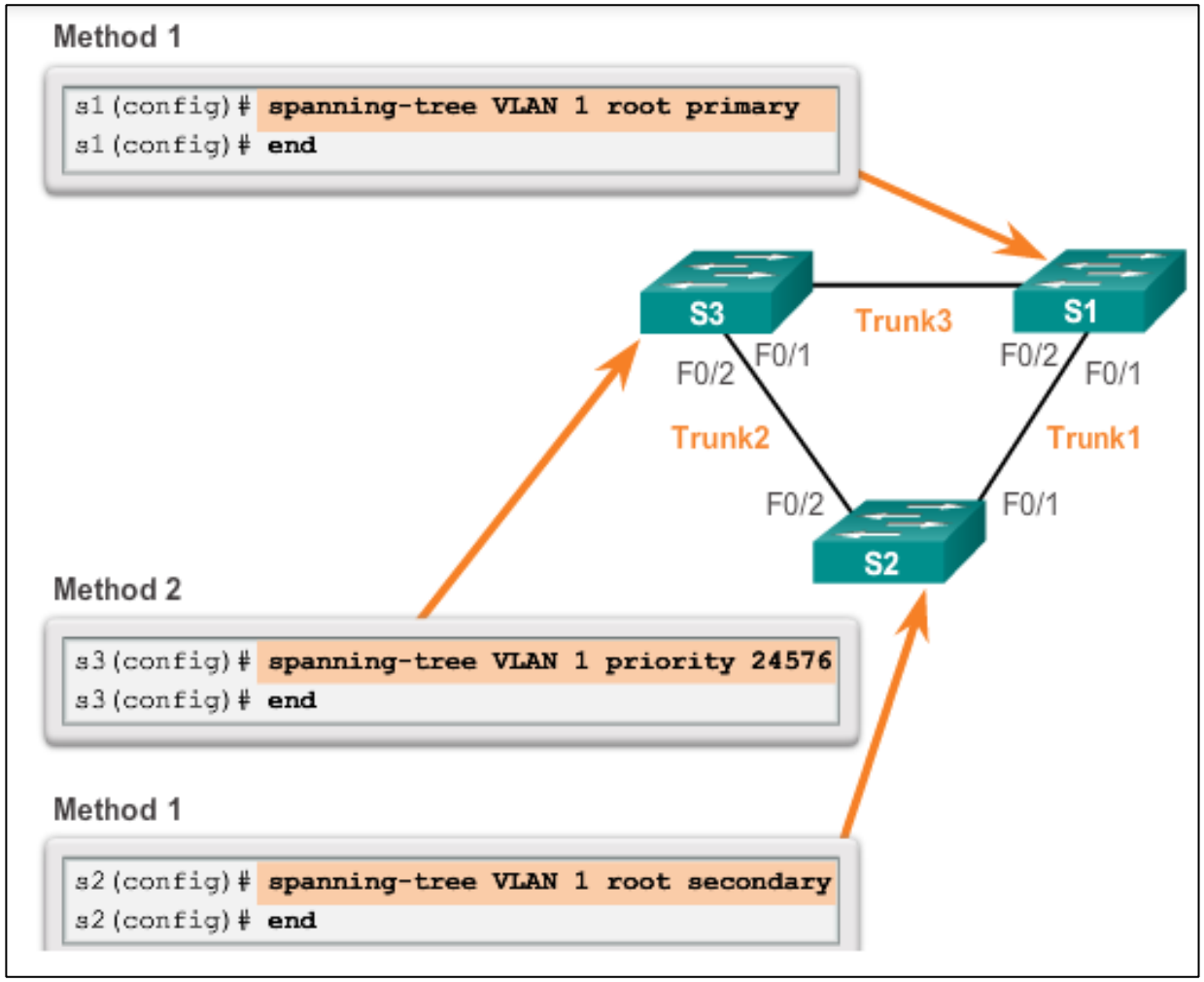
CAT2960 DEFAULT CONFIGURATION

Feature	Default Setting
Enable state	Enabled on VLAN 1
Spanning-tree mode	PVST+ (Rapid PVST+ and MSTP are disabled.)
Switch priority	32768
Spanning-tree port priority (configurable on a per-interface basis)	128
Spanning-tree port cost (configurable on a per-interface basis)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Spanning-tree timers	Hello time: 2 seconds Forward-delay time: 15 seconds Maximum-aging time: 20 seconds Transmit hold count: 6 BPDUs

CONFIGURING THE BRIDGE ID

PacketTracer

IOS

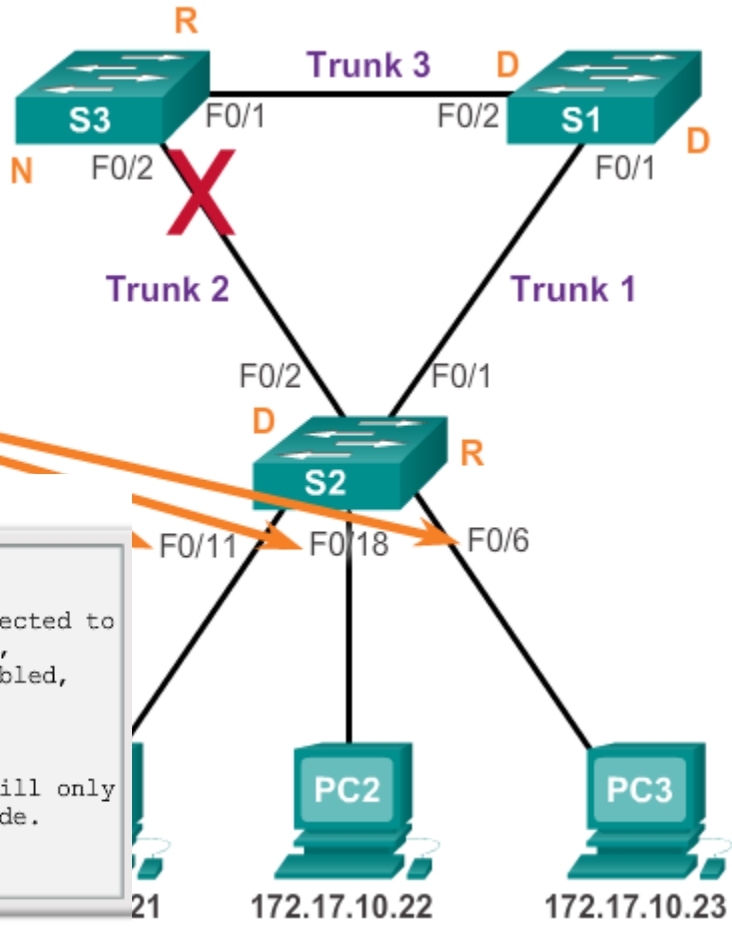


PortFast and BPDU Guard

PacketTracer

IOS

- When a switch port is configured with PortFast that port transitions from blocking to forwarding state immediately.
- BPDU guard puts the port in an *error-disabled* state on receipt of a BPDU.



PortFast and BPDU Guard

```
S2(config)# interface FastEthernet 0/11
S2(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to
a single host. Connecting hubs, concentrators, switches,
bridges, etc... to this interface  when portfast is enabled,
can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
 have effect when the interface is in a non-trunking mode.
S2(config-if)# spanning-tree bpduguard enable
S2(config-if)# end
```

SPANNING TREE MODE

PacketTracer

IOS

```
S1# configure terminal
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/2
S1(config-if)# spanning-tree link-type point-to-point
S1(config-if)# end
S1# clear spanning-tree detected-protocols
```

Rapid PVST+ is the Cisco implementation of RSTP. It supports RSTP on a per-VLAN basis.

Cisco IOS Command Syntax	
Enter global configuration mode.	**configure terminal**
Configure Rapid PVST+ spanning-tree mode.	**spanning-tree mode rapid-pvst**
Enter interface configuration mode and specify an interface to configure. Valid interfaces include physical ports, VLANs, and port channels.	**interface** *interface-id*
Specify that the link type for this port is point-to-point.	**spanning-tree link-type point-to-point**
Return to privileged EXEC mode.	**end**
Clear all detected STP.	**clear spanning-tree detected-protocols**

PORT SECURITY CONFIGURATION

1) Enable port security:

```
Switch(config-if)# switchport port-security
```

2) Set a maximum number of MAC addresses that will be allowed on this port. The default is one:

```
Switch(config-if)# switchport port-security maximum value
```

3) Specify which MAC addresses will be allowed on this port:

```
Switch(config-if)#
   switchport port-secur mac-address {mac-address|sticky}
```

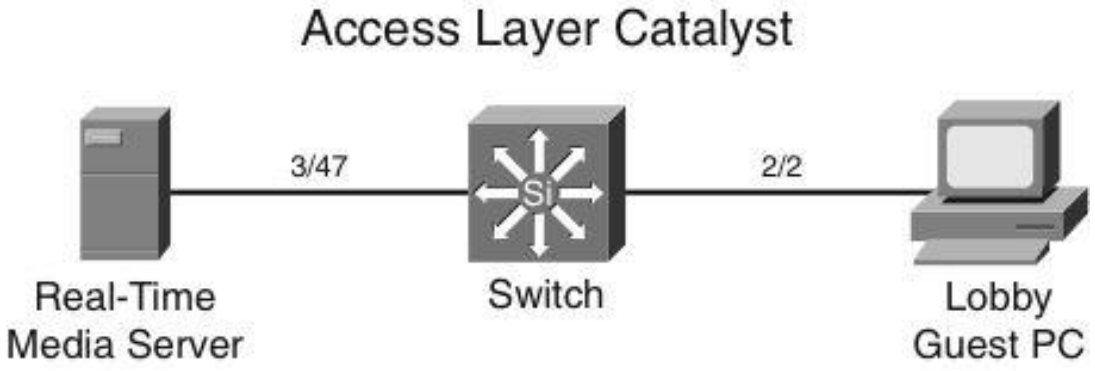
4) Define what action an interface will take if a non-allowed MAC address attempts access:

```
Switch(config-if)# switchport port-security violation {shutdown |
restrict | protect}
```

PORT SECURITY EXAMPLE

PacketTracer

IOS

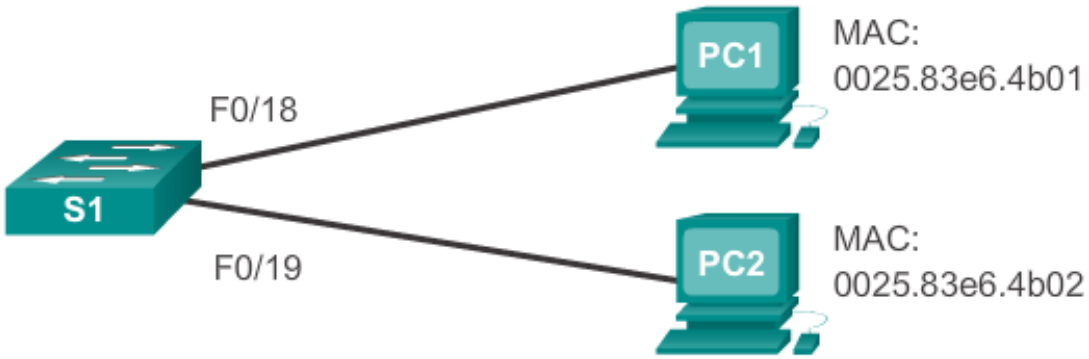



```
Switch(config)# interface FastEthernet 3/47
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.0000.0008
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging static
Switch(config-if)# switchport port-security violation restrict
Switch(config)# interface FastEthernet 2/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging static
Switch(config-if)# switchport port-security violation shutdown
```

VERIFYING PORT SECURITY

PacketTracer

IOS




```
S1# show port-security address
Secure Mac Address Table
-----------------------------------------------------------
Vlan    Mac Address       Type              Ports   Remaining Age
                                                      (mins)
----    -----------       ----              -----   -------------
1       0025.83e6.4b01    SecureDynamic     Fa0/18      -
1       0025.83e6.4b02    SecureSticky      Fa0/19      -
-----------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port
```

DHCP Snooping

- DHCP Snooping specifies which switch ports can respond to DHCP requests

PacketTracer

IOS

- DHCP snooping allows the configuration of ports as trusted or untrusted:
  - Trusted ports can send DHCP requests and acknowledgments.
  - 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.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20
S1(config)# interface fastethernet 0/1
S1(config-if)# ip dhcp snooping trust
S1(config)# interface fastethernet 0/2
S1(config-if)# ip dhcp limit rate 5
```