

Engineering Journal

CIT 167

Chaz Davis

BCTC

Spring 2020

March 13, 2020

Contents

Useful Commands: Basics	3
Useful Bits: Basics	6
1 Configuring Basic Router	9
2 Documenting The Network	15
3 Configuring IPv4 and IPv6	19
Useful Commands: Static Routing	26
Useful Bits: Static Routing	30
4 Troubleshooting Static Routes	32
5 Configuring IPv6 Static Routes	35
6 Configuring IPv4 Static	40
Useful Commands: Dynamic Routing	47
Useful Bits: Dynamic Routing	49
7 Configuring RIPv2	53
8 Configuring Basic RIPv2	56
Useful Bits: SSH and Port Security	61
Useful Commands: SSH and Port Security	63
9 Basic Switch Configuration	66
10 Configuring Switch Security	73
11 Troubleshooting Vlan	77
12 Troubleshooting Vlans Scenario 2	80
13 Configuring Vlans and Trunks	82
14 Legacy InterVlan Implementation	84

Basic Commands

2020

Packet Tracer Labs
Spring 2020

CIT 167
Chaz Davis

Basic Router Commands

```
Router> ---User EXEC mode exit
Router> ?
Router> enable
-----
Router# ---Privileged EXEC mode disable, exit
Router# ?
-----
Router# configure terminal
Router(config)# ---Global Config mode exit, end, Ctrl+c, Ctrl+z
Router(config)# ?
-----
Router(config)# line vty 0 15
Router(config)# line console 0
Router(config-line)# ---Line configuration mode exit, end, Ctrl+c, Ctrl+z
Router(config-line)# ?
-----
Router(config)# interface gigabitEthernet 0/0/0
Router(config-if)# ---Interface configuration mode exit, end, Ctrl+c, Ctrl+z
Router(config-if)# ?
```

Router Config Commands

```
Router#
Router# configure terminal
Router# show ?
Router# show running-config
Router# copy running-config startup-config
Router# ping 192.168.1.100
Router# traceroute 192.168.1.100
Router# ssh 192.168.1.100
Router# telnet 192.168.1.100
Router# debug ?
Router# clock set 07:14:00 October 15 2019
Router# reload
-----
Router(config)#
Router(config)# hostname R1
Router(config)# banner motd "No unauthorized access allowed!"
Router(config)# enable password class
Router(config)# enable secret class
Router(config)# service password-encryption
Router(config)# line vty 0 15
Router(config)# line console 0
Router(config)# interface gigabitEthernet 0/0/0
-----
Router(config-line)#
Router(config-line)# password cisco
Router(config-line)# login
Router(config-line)# transport input all (line vty)
-----
Router(config-if)#
Router(config-if)# interface gigabitEthernet 0/0/0
Router(config-if)# int g0/0 //command abbreviation
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

Basic Switch Commands

```
Switch> ---User EXEC mode exit
Switch> enable
-----
Switch# ---Privileged EXEC mode disable, exit
-----
Switch# configure terminal
Switch(config)# ---Global Config mode exit, end, Ctrl+c, Ctrl+z
-----
Switch(config)# line vty 0 15
Switch(config)# line console 0
Switch(config-line)# ---Line configuration mode exit, end, Ctrl+c, Ctrl+z
-----
Switch(config)# interface vlan 1
Switch(config-if)# ---Interface configuration mode exit, end, Ctrl+c, Ctrl+z
-----
Switch#
Switch# configure terminal
Switch# show ?
Switch# show running-config
Switch# copy running-config startup-config
Switch# ping 192.168.1.100
Switch# traceroute 192.168.1.100
Switch# ssh 192.168.1.100
Switch# telnet 192.168.1.100
Switch# debug ?
Switch# clock set 07:14:00 October 15 2019
Switch# reload
-----
Switch(conf)#
Switch(conf)# hostname R1
Switch(conf)# banner motd "No unauthorized access allowed!"
Switch(conf)# enable password class
Switch(conf)# enable secret class
Switch(conf)# service password-encryption
Switch(config)# line vty 0 15
Switch(config)# line console 0
Switch(config)# interface vlan 1
-----
Switch(config-line)#
Switch(config-line)# password cisco
Switch(config-line)# login
Switch(config-line)# transport input all (line vty)
-----
Switch(config-if)#
Switch(config-if)# interface vlan 1
Switch(config-if)# ip address 192.168.1.2 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip default-gateway 192.168.1.1
```

Extra helpful commands:

```
Router(conf)# no ip domain-lookup //prevents miss-typed commands from being "translated..."
Router(conf-line)# logging synchronous //prevents logging output from interrupting your command input
```

Useful Bits: Basics

2020

Packet Tracer Labs
Spring 2020

CIT 167
Chaz Davis

User can interact with a shell with a CLI or a GUI.

Cisco IOS is used for cisco devices

The most common way to configure a HOME router is with a web browser

Methods to access the CLI environment:

- Console : Physical management port that provides out of band access, works even without connectivity
- SSH : Secure CLI connection, requires active networking services
- Telnet: Like SSH but insecure because everything is sent in cleartext

Some devices also support a legacy AUX port used to establish remote CLI session using a modem. It works similarly to console connection.

Some useful terminal emulators via SSH/Telnet:

- PuTTY
- Tera term
- OS X terminal
- SecureCRT

For security Cisco IOS separates management access into two modes:

- User EXEC mode: Limited capabilities but useful for basic operations and monitoring, Doesn't allow change to configurations
CLI prompt ends with a >
referred as 'view-only' mode

- Privileged EXEC mode: Higher configuration modes can only be accessed this mode
CLI prompt ends with a #

To configure the device the user must enter Global configuration mode:

- it is identified by a command prompt that ends with (config)#
- changes here affect the device as a whole
- from here you can access more specific sub-configuration mode for specific function of the IOS device:

Two common subs are:

- Line configuration Mode: (config-line)#
- Interface configuration Mode: (config-if)#

If you type 'enable' on command line you go from user EXEC to privileged EXEC mode
If you type 'disable' on command line you return to the user EXEC mode

From privileged EXEC mode if i type 'configure terminal' i go to Global configuration mode
To return to privileged EXEC mode type 'exit'

From Global configuration mode if i type 'interface <interface-name> <interface-number>' i get to the specific interface configuration for the specified interface, the same for line 'line <line-name> <line-number>'. You don't need to return to global configuration mode to switch between sub-configurations. To return to Global Configuration mode (from sub-configuration) type 'exit'. To return directly to Privileged exec mode type 'end' or press 'Ctrl+Z'

The general command syntax is the command followed by keywords and arguments:
 -Keyword : a specific parameter defined in the operating system
 -Argument: not predefined, a variable or value user-defined.

Convention:
 boldface: commands and literals that you enter as shown
 italics: arguments for which you supply values
 [x] : Optional element
 {x} : Required element
 [x {y | z}]: Required choice within an optional argument

IOS helps:
 -Context-sensitive help:
 Helps you find quickly which command are available in each command mode
 To access it type '?' at the CLI
 It can even be used to check what parameters a particular command accept or to finish the name of a command.
 Command syntax check:
 If a command is entered wrong, the CLI provides the user a feedback about what is wrong.

Cisco IOS shortcuts

IMPORTANT SHORTCUTS : Ctrl-Shift-6 To abort a command mid-stream
 (Useful for mistyped commands and cisco IOS attempting translate it with DNS)
 Ctrl+R refresh last command (example if an output of a interface down/up shows in the middle of typing a command)

Hostnames:
 -Case sensitive
 -to change hostname use the command 'hostname <hostname>' in Global Config Mode
 -to reset default hostname use the command 'no hostname' in Global Config Mode

Passwords:
 -use 'enable secret <password>' in Global Config Mode to set password for Privileged Exec Mode
 -to set a password in user EXEC mode, type 'password <password>' in line console configuration mode ('line console 0' global config command)

next enable user login with the 'login' command
 -to set a password for VTY (Virtual terminal) lines used for SSH and Telnet enter line VTY config mode with 'line vty 0 15' (if 16 vty lines)
 next set password with 'password <password>' and enable login with 'login'
 -To encrypt passwords:
 Use command 'service password-encryption', this applies only to configuration files

To check the config for encryption run 'show running-config'

To add a banner message of the day use 'banner motd # the message of the day # '

There are two types of config:
 -startup config ,stored in NVRAM, to view it use 'show startup-config'
 -running config ,stored in RAM
 To save changes made to the running config in the startup config do 'copy running-config startup-config'
 To restore the startup config run in privileged EXEC mode 'reload'
 If unwanted changes were made to the startup config file it is possible to remove it by using 'erase startup-config'

Types of network media include twisted-pair copper cables, fiber-optic cables, coaxial cables, or wireless as shown in the figure.

Difference between them:

Distance the media can successfully carry a signal

Environment in which the media is to be installed

Amount of data and the speed at which it must be transmitted

Cost of the media and installation

Cisco IOS Layer 2 switches have physical ports for devices to connect. These ports do not support Layer 3 IP addresses. Therefore, switches have one or more switch virtual interfaces (SVIs)

IP address information can be added:

- manually
- using DHCP

To configure SVI use 'interface vlan 1' in global config mode.
Assign an ip address using 'ip address <ip-address> <subnet-mask>'
Enable the interface using 'no shutdown'

To see a brief interface ip screen : 'show ip interface brief'

To test the connectivity of a device on a network or of a website use the command 'ping <ip-address>'

Lab 1

Configuring Basic Router Settings

Jan 23, 2020

Packet Tracer Lab 1
Spring 2020

CIT 167
Chaz Davis

- Important Commands for the Lab

- no ip domain lookup suppresses all DNS-lookups from the router to the configured DNS servers
allows for sloppy typing keeps from doing a lookup everytime
better practice configure ip name-server
then disable automatic telnetting to "hostnames"
transport preferred none and set that for con, aux, and vty
- exec-timeout 5 0
configure the inactive session timeout on console port
parameter passed in is minutes
if two numbers passed the second is seconds
- logging synchronous
for when long commands are interrupted by console message
tells the router to hold messages until it detects no input from the keyboard
- service password-encryption
normally all passwords, except enable secret, are stored in clear-text
stores all passwords in an encrypted form
stores them using an MD5 hashing algorithm
- ? allows you to look up help from commandline
similar to -help on linux
if no help available, returns <CR>

- Important Concepts

- Understand the process of setting up new schemes
- Logging in over ssh and telnet from the commandline
- Finding info through the long lines of output

Part 1: Set Up the Topology

i) **Cable the Network** I started off by placing the the router(1941), the switch(2960), and 2 windows 7 pcs on the the canvas.

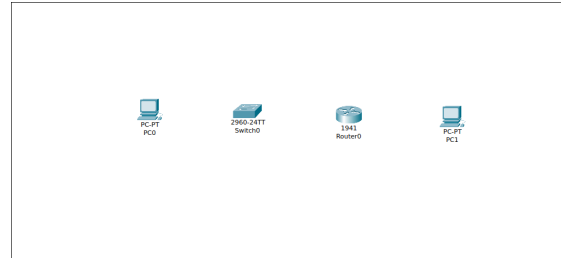


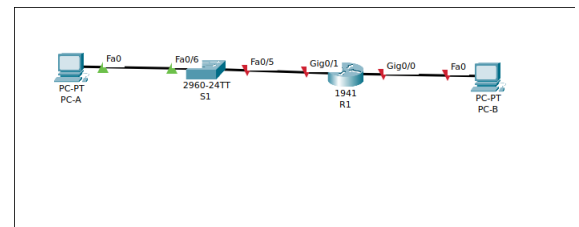
Figure 1.1: View of the Network Topology

ii) **Wiring up the routers**

Next I used straight copper wiring to connect the router the switch and the two pcs and renamed the accordingly. See Fig 1.2.

Device	connected on	connected to
PC-A	FA0	S1 Fa0/6
S1	Fa0/6	PC-A Fa0/6
R1	gig 0/1	S1 Fa0/5
PC-B	FA0	R1 gig0/0

(a) IP table



(b) Showing the Network

Figure 1.2: Configuring the Network

Part 2: Configure Devices and Verify connectivity

I started off by configuring the ipaddress, subnet mask, and default gateways on PC-A and PC-B

i) **Configuring the PCs** I started off by configuring the IPs for the PC's. See Fig 1.3.

(a) IP Config PC-A

(b) IP Config PC-B

Figure 1.3: Configuring the IPs

ii) Configuring the router

Next I logged into the router went to the commandline, and escalated to priveleged exec mode.

1

Name and passwords

```
Router>ena
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain lookup
R1(config)#no ip domain-lookup
R1(config)#security passwords min-length 10
R1(config)#enable secret cisco12345
R1(config)#line con 0
R1(config-line)#password coscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)# exit
R1(config)#service password-encryption
R1(config)#banner motd #Unauthorized access prohibited!#
```

2

Connections

```
R1(config)#int g0/0
R1(config-if)#description Connection to PC-B
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#clock set 10:00:00 28 Jan 2020
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

I then did the same for PC-A

```
R1(config)#int g 0/1
R1(config-if)#description Connection to S1
R1(config-if)#ip address 192.168..1.1 255.255.255.0
^
% Invalid input detected at '^' marker.

R1(config-if)#ip address 192.168.
^
% Invalid input detected at '^' marker.

R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut

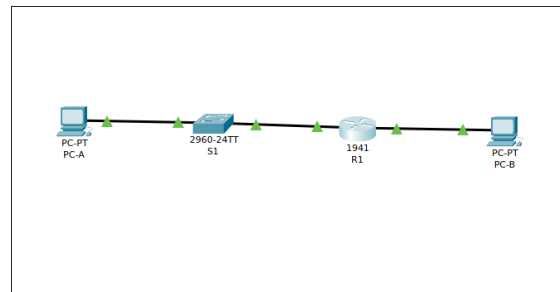
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

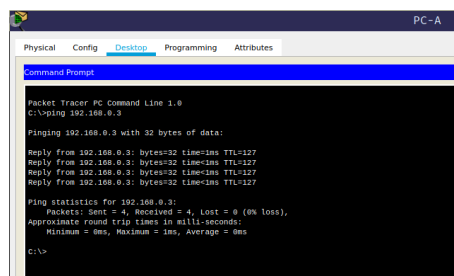
R1(config-if)#
```

3

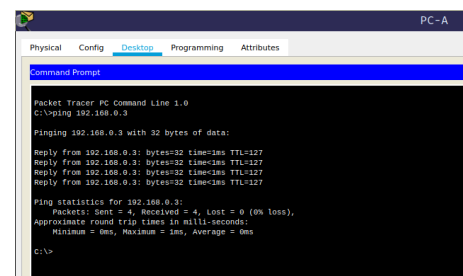
Verifying network connectivity



(a) R1 Enable



(b) Pingin PC-B from PC-A



(c) Telnet PC-A to R1

Figure 1.4: Verifying the Network Connectivity

Part 3: Display Router Information

i) important hardware and software info

While logged in with telnet I ran the following commands

```

R1>show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M),
Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 1 hours, 19 minutes, 11 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload
  
```

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
```

We can see that the IOS image on the router is Cisco IOS Software,

```
C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
```

We can also see that the NVRAM by using show flash:

```
R1#show flash

System flash directory:
File Length Name/status
  3  33591768 c1900-universalk9-mz.SPA.151-4.M4.bin
  2   28282  sigdef-category.xml
  1   227537  sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

ii) Display Startup Info

```
R1#show startup-config
Using 959 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname R1
!
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUU1.
!
ip cef
no ipv6 cef
!
license udi pid CISC01941/K9 sn FTX1524C630-
no ip domain-lookup
spanning-tree mode pvst
!
interface GigabitEthernet0/0
description Connection to PC-B
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip flow-export version 9
banner motd ^CUnauthorized access prohibited!^C
!
line con 0
exec-timeout 5 0
password 7 0822435D0A1606181C1B0D1739
logging synchronous
login
!
line aux 0
!
line vty 0 4
exec-timeout 5 0
password 7 0822455D0A1613030B1B0D1739
logging synchronous
login
```

```
!
end
```

From this we can see that the passwords are encrypted

I used show startup-config | begin vty

It did not like that command wouldnt show any info

iii) Display the routing table on the router

i ran show ip route

```
R1#show ip route
Codes:
L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
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,
ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

    192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly connected, GigabitEthernet0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.1/32 is directly connected, GigabitEthernet0/1

R1#
```

There are two entries with a C encoding

iv) Display a summary list Display a summary list of the interfaces on the router

I ran the show ip interface brief command:

```
show ip interface brief
Interface      IP-Address  OK? Method Status      Protocol
GigabitEthernet0/0  192.168.0.1 YES manual up          up
GigabitEthernet0/1  192.168.1.1 YES manual up          up
Vlan1            unassigned YES unset  administratively down down
```

when we gave the command 'no shut' that changed the gig ethernet ports from down to up.

Lab 2

Documenting The Network

Jan 26, 2020

Packet Tracer Lab 2
Spring 2020

CIT 167
Chaz Davis

- Important Commands for the Lab

- show interface displays the status of the router's interfaces
 - interface status up/down
 - Protocol status on the device
 - Utilization
 - Errors
 - MTU
 - MTU
- show ip interface (brief) tons of useful info:
 - IP protocol status
 - all its services
 - all of its interfaces and their protocols and status'
 - Ip address
 - Layer 2 status
 - layer 3 status
 - it is the config thats in the routers memory.
 - sh run this is not updated upon changes. but upon running the command copy running-configuration startup-configuration
- show ip route
 - lists all networks that the router can reach
 - their metric - the routers preference for them and how to get there
- show version gives the routers config register (firmware settings)
 - the last time it was booted
 - the version of the IOS
 - the model of router
 - the amount of ram and Flash

Part 1: filling in the table

i) R2 I logged into R2 and ran the following commands i ran show ip config

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.255.255.245	YES	manual	up	up
GigabitEthernet0/1	10.255.255.249	YES	manual	up	up
GigabitEthernet0/2	10.10.10.1	YES	manual	up	up
Serial0/0/0	64.100.100.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	up	up
Serial0/0/1.1	64.100.200.2	YES	manual	up	up
Vlan1	unassigned	YES	unset		
administratively down down					

I then ran show interfaces

```
GigabitEthernet0/0 is up, line protocol is up (connected)
Hardware is CN Gigabit Ethernet, address is
0001.969a.1d01 (bia 0001.969a.1d01)
Internet address is 10.255.255.245/30
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 63 bits/sec, 0 packets/sec
5 minute output rate 65 bits/sec, 0 packets/sec
241 packets input, 16664 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 1017 multicast, 0 pause input
0 input packets with dribble condition detected
```

I then ran show running-config

```
Building configuration...

Current configuration : 2258 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R2
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip cef
no ipv6 cef
username Tier3a password 0 cisco
username administrator password 0 cisco
license udi pid CISC02911/K9 sn FTX15249169
ip ssh version 2
ip domain-name Central
ip host R1 10.255.255.254 10.255.255.246 10.2.0.1
ip host R3 10.255.255.253 10.255.255.250 10.3.0.1
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.255.255.245 255.255.255.252
 ip ospf priority 255
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.255.255.249 255.255.255.252
 ip ospf priority 255
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.10.10.1 255.255.255.0
```

```

duplex auto
speed auto
interface Serial0/0/0
ip address 64.100.100.1 255.255.255.252
encapsulation ppp
ppp authentication pap
ppp pap sent-username R2 password 0 cisco
interface Serial0/0/1
no ip address
encapsulation frame-relay
clock rate 2000000
interface Serial0/0/1.1 point-to-point
ip address 64.100.200.2 255.255.255.252
frame-relay interface-dlci 202
clock rate 2000000
interface Vlan1
no ip address
shutdown
router ospf 1
log-adjacency-changes
passive-interface Serial0/0/0
passive-interface Serial0/0/1
network 10.255.255.244 0.0.0.3 area 0
network 10.255.255.248 0.0.0.3 area 0
network 10.10.10.0 0.0.0.255 area 0
network 64.100.100.0 0.0.0.3 area 0
default-information originate
ip classless
ip route 0.0.0.0 0.0.0.0 64.100.100.2
ip route 0.0.0.0 0.0.0.0 64.100.200.1 200
ip flow-export version 9
ip access-list extended PERMIT_LOCAL
permit udp any any eq domain
permit tcp any any eq domain
permit ip 64.100.200.0 0.0.0.3 any
permit ip 64.104.223.0 0.0.0.3 any
permit icmp 64.100.200.0 0.0.0.3 any
permit icmp 64.104.223.0 0.0.0.3 any
permit icmp any any echo-reply
deny ip any any
banner login Username: administrator
Password: cisco Enable: class
banner motd Username:administrator
Password:cisco Enable:class
line con 0
line aux 0
line vty 0
login local
transport input ssh
line vty 1 4
no login
end

```

ii) Filling in part of the table

we now have enough information to fill in pieces of the table

R2		connecting device		
interface	address	subnetmask	name	interface
G0/0	10.255.255.245	255.255.255.252	D1	Gi 0/1
G0/1	10.255.255.249	255.255.255.252	D2	G 0/1
G0/2	10.10.10.1	255.255.255.0	S3	G 0/1

Part 2: S3

i) **Gathering data** I continued to do the same for the rest of the switches and interfaces

ii) **full table**

here is the completed table

R2		connecting device		
interface	address	subnetmask	name	interface
G0/0	10.255.255.245	255.255.255.252	D1	Gi 0/1
G0/1	10.255.255.249	255.255.255.252	D2	G 0/1
G0/2	10.10.10.1	255.255.255.0	S3	G 0/1
S0/0/0	64.100.100.1	255.255.255.252	Internet	N/A
s0/0/1.1	64.100.200.2	255.255.255.252	Intranet	N/A
S3				
VLAN 1	10.10.10.254	255.255.255.0	N/A	N/A
F0/1	N/A	N/A	Cent. Srvr	NIC
G0/1	N/A	N/A	R2	G0/2
c. srvr				
NIC	10.10.10.2	255.255.255.0	S3	F0/1
D1				
VLAN2	10.2.0.1	255.255.255.0	N/A	N/A
G0/1	10.255.255.246	255.255.255.252	R2	G0/0
G0/2	10.255.255.254	255.255.255.252	D2	G0/2
F0/23	N/A	N/A	S2	F0/23
F0/24	N/A	N/A	S1	G0/1
S1				
VLAN2	10.2.0.2	255.255.255.0	N/A	N/A
F0/23	N/A	N/A	D2	F0/23
G0/1	N/A	N/A	D1	F0/24
D2				
F0/23	N/A	N/A	S1	F0/23
F0/24	10.3.0.1	255.255.255.0	S3	G0/1
G0/1	10.255.255.250	255.255.255.252	R2	G0/1
G0/2	10.255.255.253	255.255.255.252	D1	G0/2
S2				
VLAN1	10.3.0.1	255.255.255.0	N/A	N/A
F0/23	N/A	N/A	D1	F0/23
G0/1	N/A	N/A	D2	F0/24

Lab 3

Configuring IPv4 and IPv6

Jan 28, 2020

Packet Tracer Lab 3
Spring 2020

CIT 167
Chaz Davis

- Important Commands for the Lab

- config start off in user mode
 - enable moves you from user to privileged mode
 - config terminal you can change the global parameters
 - interface router
 - router from global you can go into router settings instead of interface routerprotocol
- ip address... followed by the ip address and the subnet mask of the pc to be configured
- no shutdown this enables the interface or 'brings it up' must be in interface configuration mode
- interface... Followed by the name of the interface to be configured ie.
 - GigabitEthernet0/0
 - FastEthernet0...
 - can be shortened to int g 0/0 or int Fa 0

- Important Concepts

- Difference between IPv6 and IPv4
- How to ping from the commandline

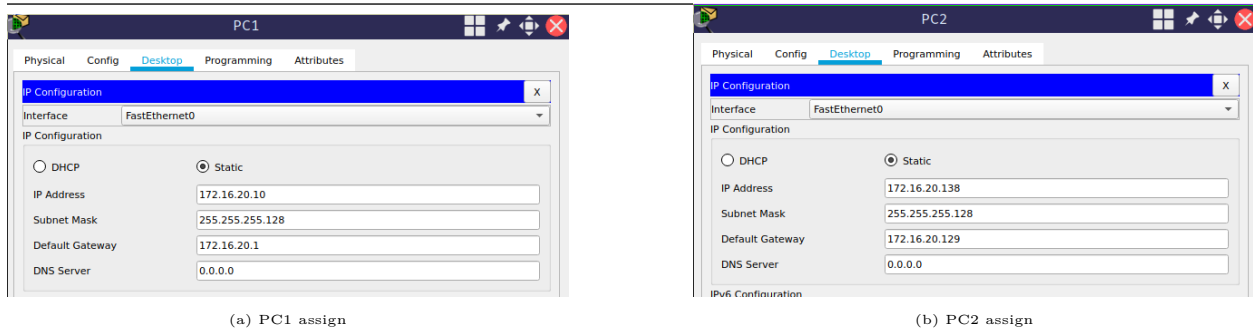


Figure 3.1: Assigning IPv4 addressing

Part 1: Configuring IPv4

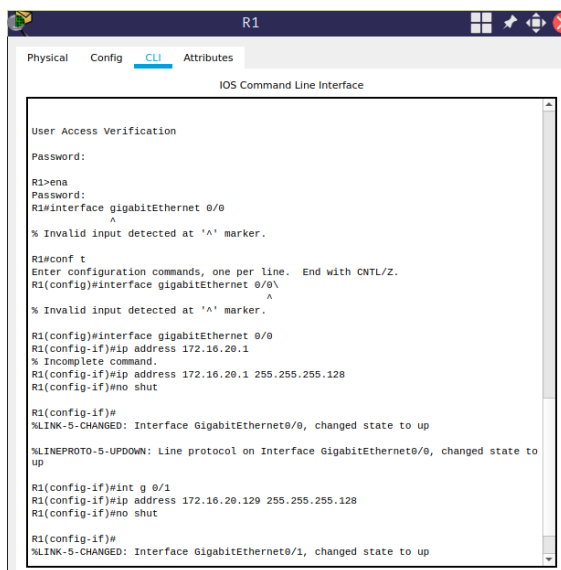
i) Assign IPv4 addressing

I opened up PC1 and clicked on the desktop. I then opened the IP configuration box and entered the information from the table. See Fig 3.1a.

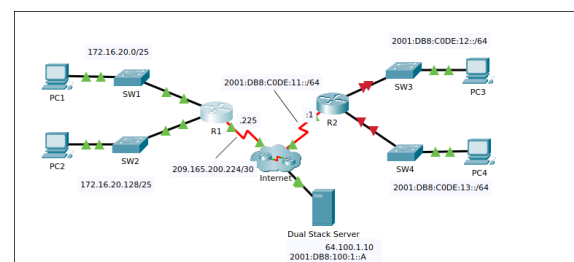
I opened up PC2 and clicked on desktop and opened the ip configuration box and entered the information from the table. See Fig 3.1b.

I opened up R1 and used the commandline tool to enter the information according to the chart. See Fig 3.2a.

We can now see that PC1 PC2 and R1 are all connected to each other. See Fig 3.2b.



(a) R1 assign



(b) Connected Network Layout

Figure 3.2: Network Connectivity

ii) Verify connectivity

I opened PC1 went the command line and successfully pinged the Dual stack server and then successfully pinged PC2. See Fig 3.3a

I opened PC2 went the command line and successfully pinged the Dual stack server and then successfully pinged PC1 See Fig 3.3b

```

Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 64.100.1.10

Pinging 64.100.1.10 with 32 bytes of data:

Request timed out.
Reply from 64.100.1.10: bytes=32 time=1ms TTL=126
Reply from 64.100.1.10: bytes=32 time=1ms TTL=126
Reply from 64.100.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 64.100.1.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 172.16.20.138

Pinging 172.16.20.138 with 32 bytes of data:

Request timed out.
Reply from 172.16.20.138: bytes=32 time<1ms TTL=127
Reply from 172.16.20.138: bytes=32 time<1ms TTL=127
Reply from 172.16.20.138: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.20.138:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

(a) PC1 Successfully pinging the server and PC2

```

PC2

Physical Config Desktop Programming Attributes

Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 64.100.1.10

Pinging 64.100.1.10 with 32 bytes of data:

Reply from 64.100.1.10: bytes=32 time=2ms TTL=126
Reply from 64.100.1.10: bytes=32 time=1ms TTL=126
Reply from 64.100.1.10: bytes=32 time=1ms TTL=126
Reply from 64.100.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 64.100.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 172.16.20.10

Pinging 172.16.20.10 with 32 bytes of data:

Reply from 172.16.20.10: bytes=32 time=1ms TTL=127
Reply from 172.16.20.10: bytes=32 time=1ms TTL=127
Reply from 172.16.20.10: bytes=32 time=1ms TTL=127
Reply from 172.16.20.10: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

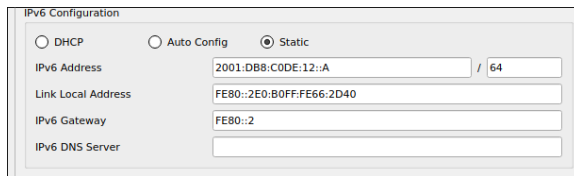
C:\>

```

(b) PC2 successfully pinging the server and PC1

Figure 3.3: Network Verification

Part 2: configuring IPv6



IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

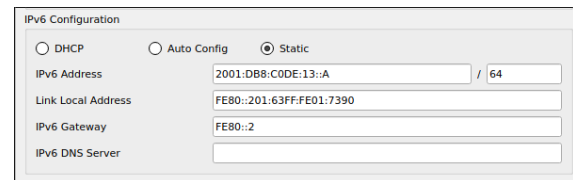
IPv6 Address: 2001:DB8:C0DE:12::A / 64

Link Local Address: FE80::2E0:B0FF:FE66:2D40

IPv6 Gateway: FE80::2

IPv6 DNS Server:

(a) IPv6 Configuration for PC3



IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

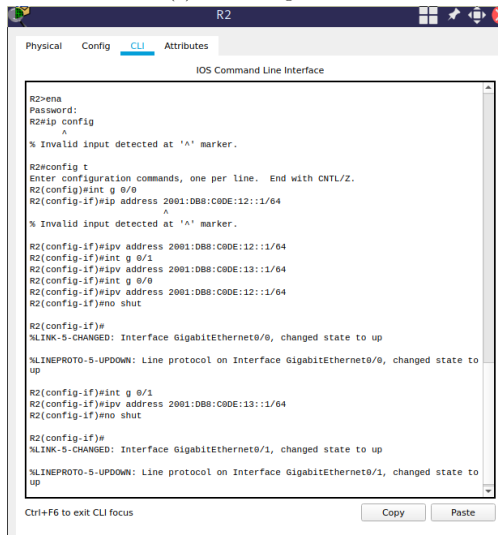
IPv6 Address: 2001:DB8:C0DE:13::A / 64

Link Local Address: FE80::201:63FF:FE01:7390

IPv6 Gateway: FE80::2

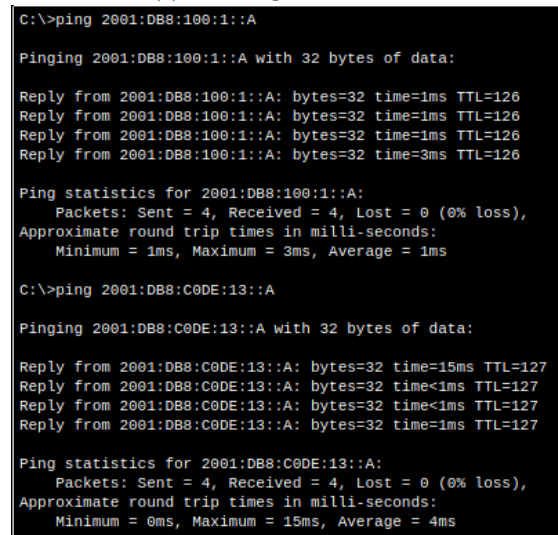
IPv6 DNS Server:

(b) IPv6 Configuration for PC4



```
R2>ena
Password:
R2#ip config
% Invalid input detected at '^' marker.
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int g 0/0
R2(config-if)#ip address 2001:DB8:C0DE:12::1/64
% Invalid input detected at '^' marker.
R2(config-if)#ip address 2001:DB8:C0DE:12::1/64
R2(config-if)#int g 0/1
R2(config-if)#ip address 2001:DB8:C0DE:13::1/64
R2(config-if)#int g 0/0
R2(config-if)#ip address 2001:DB8:C0DE:12::1/64
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config-if)#int g 0/1
R2(config-if)#ip address 2001:DB8:C0DE:13::1/64
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

(c) Configuring R2 Interface



```
C:\>ping 2001:DB8:100:1::A

Pinging 2001:DB8:100:1::A with 32 bytes of data:

Reply from 2001:DB8:100:1::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:100:1::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:100:1::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:100:1::A: bytes=32 time=3ms TTL=126

Ping statistics for 2001:DB8:100:1::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\>ping 2001:DB8:C0DE:13::A

Pinging 2001:DB8:C0DE:13::A with 32 bytes of data:

Reply from 2001:DB8:C0DE:13::A: bytes=32 time=15ms TTL=127
Reply from 2001:DB8:C0DE:13::A: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:C0DE:13::A: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:C0DE:13::A: bytes=32 time=1ms TTL=127

Ping statistics for 2001:DB8:C0DE:13::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 4ms
```

(d) PC3 PC4 and R2 Connections

Figure 3.4: IPv6 Configuration

i) Assign IPv6 addressing and verify connectivity

I opened up PC3 and clicked on desktop and opened the ipconfiguration box and entered the information from the table. See Fig 3.4a.

I opened up PC4 and clicked on desktop and opened the ipconfiguration box and entered the information from the table. See Fig 3.4b

I opened up R2 and used the commandline tool to enter the information according to the chart. See Fig 3.4c.

We can now see in Fig 3.4d that PC3 PC4 and R2 are all connected to each other.

ii) Verify connectivity

I opened PC3 went the command line and successfully pinged the Dual stack server and then successfully pinged PC4

```
C:\>ping 2001:DB8:100:1::A

Pinging 2001:DB8:100:1::A with 32 bytes of data:

Reply from 2001:DB8:100:1::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:100:1::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:100:1::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:100:1::A: bytes=32 time=3ms TTL=126

Ping statistics for 2001:DB8:100:1::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\>ping 2001:DB8:C0DE:13::A

Pinging 2001:DB8:C0DE:13::A with 32 bytes of data:

Reply from 2001:DB8:C0DE:13::A: bytes=32 time=15ms TTL=127
Reply from 2001:DB8:C0DE:13::A: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:C0DE:13::A: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:C0DE:13::A: bytes=32 time=1ms TTL=127

Ping statistics for 2001:DB8:C0DE:13::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 4ms
```

(a) Pinging the Server and PC4 from PC3

```
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:100:1::A

Pinging 2001:DB8:100:1::A with 32 bytes of data:

Reply from 2001:DB8:100:1::A: bytes=32 time=10ms TTL=126
Reply from 2001:DB8:100:1::A: bytes=32 time=1ms TTL=126
Reply from 2001:DB8:100:1::A: bytes=32 time=2ms TTL=126
Reply from 2001:DB8:100:1::A: bytes=32 time=1ms TTL=126

Ping statistics for 2001:DB8:100:1::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 3ms

C:\>ping 2001:DB8:C0DE:12::A

Pinging 2001:DB8:C0DE:12::A with 32 bytes of data:

Reply from 2001:DB8:C0DE:12::A: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:C0DE:12::A: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:C0DE:12::A: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:C0DE:12::A: bytes=32 time=1ms TTL=127

Ping statistics for 2001:DB8:C0DE:12::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

(b) Pinging the Server and PC3 from PC4

Activity Results

Configuration Wizard has completed the activity

Overall Feedback: [View Feedback](#) | [View Log](#) | [View Details](#) | [View](#) | [Export](#) | [Print](#)

Connectivity Tests

Assignment Items	Status	Results	Components	Feedback
1. R1	Correct	2	IPv4 Address C...	
2. R2	Correct	2	IPv4 Address C...	
3. R3	Correct	2	IPv4 Address C...	
4. R4	Correct	2	IPv4 Address C...	
5. R5	Correct	2	IPv4 Address C...	
6. R6	Correct	2	IPv4 Address C...	
7. R7	Correct	2	IPv4 Address C...	
8. R8	Correct	2	IPv4 Address C...	
9. R9	Correct	2	IPv4 Address C...	
10. R10	Correct	2	IPv4 Address C...	
11. R11	Correct	2	IPv4 Address C...	
12. R12	Correct	2	IPv4 Address C...	
13. R13	Correct	2	IPv4 Address C...	
14. R14	Correct	2	IPv4 Address C...	
15. R15	Correct	2	IPv4 Address C...	
16. R16	Correct	2	IPv4 Address C...	
17. R17	Correct	2	IPv4 Address C...	
18. R18	Correct	2	IPv4 Address C...	
19. R19	Correct	2	IPv4 Address C...	
20. R20	Correct	2	IPv4 Address C...	
21. R21	Correct	2	IPv4 Address C...	
22. R22	Correct	2	IPv4 Address C...	
23. R23	Correct	2	IPv4 Address C...	
24. R24	Correct	2	IPv4 Address C...	
25. R25	Correct	2	IPv4 Address C...	
26. R26	Correct	2	IPv4 Address C...	
27. R27	Correct	2	IPv4 Address C...	
28. R28	Correct	2	IPv4 Address C...	
29. R29	Correct	2	IPv4 Address C...	
30. R30	Correct	2	IPv4 Address C...	
31. R31	Correct	2	IPv4 Address C...	
32. R32	Correct	2	IPv4 Address C...	
33. R33	Correct	2	IPv4 Address C...	
34. R34	Correct	2	IPv4 Address C...	
35. R35	Correct	2	IPv4 Address C...	
36. R36	Correct	2	IPv4 Address C...	
37. R37	Correct	2	IPv4 Address C...	
38. R38	Correct	2	IPv4 Address C...	
39. R39	Correct	2	IPv4 Address C...	
40. R40	Correct	2	IPv4 Address C...	
41. R41	Correct	2	IPv4 Address C...	
42. R42	Correct	2	IPv4 Address C...	
43. R43	Correct	2	IPv4 Address C...	
44. R44	Correct	2	IPv4 Address C...	
45. R45	Correct	2	IPv4 Address C...	
46. R46	Correct	2	IPv4 Address C...	
47. R47	Correct	2	IPv4 Address C...	
48. R48	Correct	2	IPv4 Address C...	
49. R49	Correct	2	IPv4 Address C...	
50. R50	Correct	2	IPv4 Address C...	

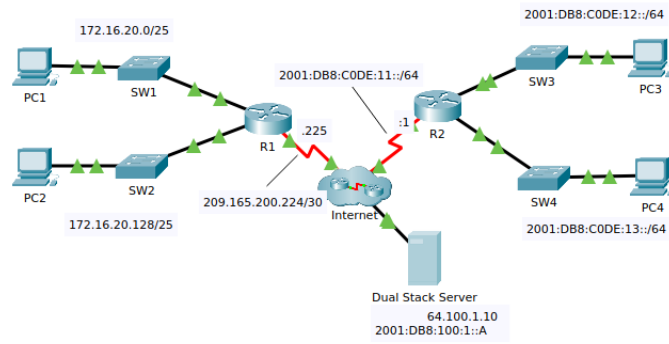
Score: 100/100
Item Count: 14/14

Components: IPv4 Address Configuration 12/12 100%
IPv6 Address Configuration 12/12 100%

(c) Topology of the Completed Network

Figure 3.5: Verifying Connectivity of the Network

I opened PC4 went the command line and successfully pinged the Dual stack server and then successfully pinged PC3



Part 3: Wrap Up

i) Success

Clicked the Check results button 100% success

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 01:09:13

Congratulations Guest! You completed the activity.

Overall Feedback **Assessment Items** Connectivity Tests

Expand/Collapse All Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
PC1				
Default Gateway	Correct	2	IPv4 Address C...	
Ports				
FastEthernet0				
IP Address	Correct	2	IPv4 Address C...	
Subnet Mask	Correct	1	IPv4 Address C...	
PC2				
Default Gateway	Correct	2	IPv4 Address C...	
Ports				
FastEthernet0				
IP Address	Correct	2	IPv4 Address C...	
Subnet Mask	Correct	1	IPv4 Address C...	
PC3				
Default Gateway IPv6	Correct	2	IPv6 Address C...	
Ports				
FastEthernet0				
IPv6 Addresses				
2001:DB8:C0DE:12::A				
IP Address	Correct	2	IPv6 Address C...	
Prefix Length	Correct	1	IPv6 Address C...	
PC4				
Default Gateway IPv6	Correct	2	IPv6 Address C...	
Ports				
FastEthernet0				
IPv6 Addresses				
2001:DB8:C0DE:13::A				
IP Address	Correct	2	IPv6 Address C...	
Prefix Length	Correct	1	IPv6 Address C...	
R1				
Ports				
GigabitEthernet0/0				
IP Address	Correct	10	IPv4 Address C...	
Port Status	Correct	2	IPv4 Address C...	
Subnet Mask	Correct	8	IPv4 Address C...	
GigabitEthernet0/1				
IP Address	Correct	10	IPv4 Address C...	
Port Status	Correct	2	IPv4 Address C...	
Subnet Mask	Correct	8	IPv4 Address C...	
R2				
Ports				
GigabitEthernet0/0				
IPv6 Addresses				
2001:DB8:C0DE:12::1				
IP Address	Correct	10	IPv6 Address C...	
Prefix Length	Correct	8	IPv6 Address C...	
Port Status	Correct	2	IPv6 Address C...	
GigabitEthernet0/1				
IPv6 Addresses				
2001:DB8:C0DE:13::1				
IP Address	Correct	10	IPv6 Address C...	
Prefix Length	Correct	8	IPv6 Address C...	
Port Status	Correct	2	IPv6 Address C...	

Score : 100/100
Item Count : 24/24

Component	Items/Total	Score
IPv4 Address Configuration	12/12	50/50
IPv6 Address Configuration	12/12	50/50

Close

Configuring Static Routes

2020

Packet Tracer Labs
Spring 2020

CIT 167
Chaz Davis

Configuring Static Routes

- There are two common types of static routes in the routing table:
 - Static route to a specific network
 - Default static route

IPv4 Routing

```
ip route <network-address> <subnet-mask> { next-hop-ip | exit-intf }
```

- Next-hop-ip: IP-address of the connecting router to use for forwarding.
- Exit-intf: the outgoing interface to use to forward the packet to the next hop.

Configure a IPv4 Default Static Route

```
ip route 0.0.0.0 0.0.0.0 { exit-intf | next-hop-ip }
```

The distance parameter is used to create a floating static route by setting an administrative distance that is higher than a dynamically learned route.

Configure an IPv4 Floating Static Route

- Given an example where R1 is attached to R2 (172.16.2.2) and R3 (10.10.10.2), the following would create a default static route to R2, and a floating static route to R3:

```
ip route 0.0.0.0 0.0.0.0 172.16.2.2      # Default route to R2
ip route 0.0.0.0 0.0.0.0 10.10.10.2 5    # Floating default route to R3
```

- Default route to R2 has no administrative distance specified, so would default to 1. This is the preferred route..
- Floating default route to R3 has administrative distance 5. Since this value is greater than that of the default route, this route "floats" - it is not present in the routing table unless the preferred route fails.

Default Administrative Distances

Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Verify a Static Route

```
show ip route
show ip route static          # Displays contents of static routes
show ip route static | begin Gateway
show ip route <network>

show running-config | section ip route

# displays the routes that packets will actually take when traveling to their
destination
traceroute <ip-address>
trace <destination>

#displays detailed info about neighboring devices discovered using Cisco Discovery
Protocol
show cdp neighbors
show cdp neighbors detail
```

Command Sequence

```
enable
configure terminal

ip route 192.168.3.0 255.255.255.0 192.168.2.2
exit

show ip route
ping 192.168.3.1
trace 192.168.3.1

exit
```

IPv6 Routing

```
ipv6 route <ipv6-prefix>/<prefixlength> {ipv6-address | exit-intf}
```

Displaying and Testing IPv6 Routes

```
show ipv6 route
show ipv6 route static
show ipv6 route <network>
show running-config | section ipv6 route

ping ipv6 <ipv6-address>
traceroute
```

Configure a Directly Connected Static IPv6 Route

```
ipv6 route <ipv6-address>/<network-prefix> <interface>
ipv6 route 2001:db8:acad:2::/64 s0/0/0
```

Configure a Fully Specified Static IPv6 Route

```
ipv6 route <ipv6-address>/<network-prefix> <interface> <next-hop ipv6-address>  
ipv6 route 2001:db8:acad:2::/64 s0/0/0 fe80::2
```

Configure a Default IPv6 Static Route

```
ipv6 route ::/0 {ipv6-address | exit-intf}  
ipv6 route ::/ 2001:db8:acad:4::2
```

Configure an IPv6 Floating Static Route

```
ipv6 route ::/0 <ipv6-address> <administrative-distance>  
ipv6 route ::/0 2001:db8:aad:4::2  
ipv6 route ::/0 2001:db8:aad:6::2 5
```

Common IOS Troubleshooting Commands

```
ping  
ping <ip-address> source <source_ip>  
tracertoute <ip-address>  
show ip route | begin Gateway  
show ip interface brief  
show cdp neighbors detail
```

Static Routing

2020

Packet Tracer Labs
Spring 2020

CIT 167
Chaz Davis

Important Concepts for Static Routing

- Routing is the process of selecting paths in a network along which to send network traffic
- Static routing involves manual updating of routing tables with fixed paths to destination networks.
- Static routing uses include:
 - Defining an exit point from a router when no other routes are available or necessary.
 - Small networks that require only one or two routes.
 - To provide a failsafe backup in the event that a dynamic route is unavailable.
 - To help transfer routing information from one routing protocol to another.
- Static routing disadvantages include:
 - Potential for human error
 - Lack of fault tolerance
 - Default prioritization over dynamic routing
 - Administrative overhead
- To display the current state of the routing table use the show ip route command in user EXEC or privileged EXEC mode.
- To display the entries in the Address Resolution Protocol (ARP) table use the show arp command in user EXEC or privileged EXEC mode.
- To establish static routes use the ip route command in global configuration mode. To remove static routes, use the no form of this command.
- To discover the routes that packets will actually take when traveling to their destination, use the trace / traceroute privileged EXEC command.
- To display detailed information about neighboring devices discovered using Cisco Discovery Protocol (CDP), use the show cdp neighbors privileged EXEC command.

Important Terms to know

- ARP table

A table of IP and hardware addresses resolved using the Address Resolution Protocol.
- Cisco Express Forwarding (CEF)

An advanced layer 3 switching technology used mainly in large core networks or the Internet to enhance the overall network performance.
- Internet Control Message Protocol (ICMP)

Used by network devices to send error messages on an IP network.
- Layer 3 switch

A device capable of both routing and switching operations using dedicated application-specific integrated circuit (ASIC) hardware.
- next-hop router

The next router in the path between source and destination.[20]
- outgoing interface

The local network interface used to connect to a next-hop router.
- routing table

A data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes.
- static route

A manually-configured routing entry.
- summary route

A route containing the highest-order bits that match all addresses for a given collection of destination networks.
- traceroute

A computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.

Lab 4

Troubleshooting Static Routes

Feb 4, 2020

Packet Tracer Lab 4
Spring 2020

CIT 167
Chaz Davis

- Important Commands for the Lab

- show ip route [ip-address] to display the current state of the routing table
command can be used in EXEC or privileged EXEC mode
- no ip route To remove static routes, use this command in global configuration
`no ip route prefix mask <ip address | interface-type interface-number> [permanent]`
- ip route To establish static routes, use this command in global configuration
`ip route prefix mask <ip address | interface-type interface-number> [permanent]`
`ip route 192.168.3.0 255.255.255.0 192.168.2.2`

Part 1: Locate The Problem

Based on the output of the commands I've run, from PC1 and from R1 and R2 and R3.

It appears that R2 is incorrectly configured and it has R1 as the wrong ip addresses in its routing table. See Fig.

It also appears that R3 is incorrectly configured and has no route for pc1 in its tables.

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       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, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

172.31.0.0/16 is variably subnetted, 8 subnets, 5 masks
C       172.31.0.0/24 is directly connected, GigabitEthernet0/0
L       172.31.0.1/32 is directly connected, GigabitEthernet0/0
S       172.31.1.0/25 [1/0] via 172.31.1.198
S       172.31.1.128/26 [1/0] via 172.31.1.194
C       172.31.1.192/30 is directly connected, Serial0/0/0
L       172.31.1.193/32 is directly connected, Serial0/0/0
C       172.31.1.196/30 is directly connected, Serial0/0/1
L       172.31.1.197/32 is directly connected, Serial0/0/1
```

(a) R2 misconfiguration of static Route

Figure 4.1: Network Misconfigured:
R2 - not set up for R1

Part 2: Determine the solution

I believe the solution is going to be statically configuring the routes for router 2 and 3, making sure that all are connected.

Part 3: Implement the solution

I went to R2 first, and configured the network settings. First, by removing the incorrect routing tables by running the

commands `no ip route 172.31.1.0 255.255.255.128 172.31.1.198` and `no ip route 172.31.1.128 255.255.255.192 172.31.1.194` Then, I repopulated the table by running the

commands `ip route 172.31.1.0 255.255.255.128 172.31.1.194` and `ip route 172.31.1.128 255.255.255.192 172.31.1.198`.

I then went to R3 and configured it for PC1 by running `ip route 172.31.1.0 255.255.255.128 serial 0/0/1`

Part 4: Verify that the issue is resolved

Finally I verified that the network is now working properly. Table on Pg. 34

As you can see in Fig. 4.2a I was successfully able to ping the server from PC1.

I then opened the web browser on PC1 Fig. 4.2b and PC2 Fig. 4.2c and entered the servers address and got the congratulations message.

```
C:\>ping 172.31.1.190

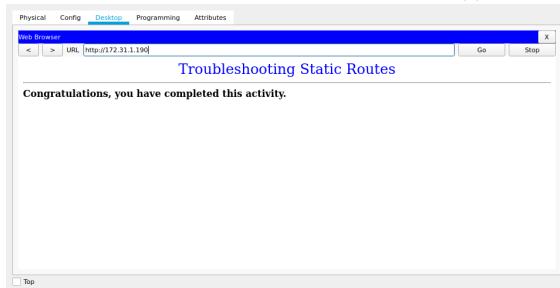
Pinging 172.31.1.190 with 32 bytes of data:

Reply from 172.31.1.190: bytes=32 time=4ms TTL=125
Reply from 172.31.1.190: bytes=32 time=2ms TTL=125
Reply from 172.31.1.190: bytes=32 time=2ms TTL=125
Reply from 172.31.1.190: bytes=32 time=2ms TTL=125

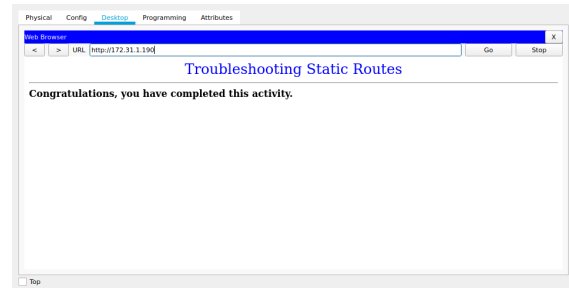
Ping statistics for 172.31.1.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\>
```

(a) Successful Ping of the server from PC1



(b) Successful Webpage Login PC1



(c) Successful Webpage Login from PC2

Figure 4.2: Successful Verification

Lab 5

Configuring IPv6 Static Routes

Feb 6, 2020

Packet Tracer Lab 5
Spring 2020

CIT 167
Chaz Davis

- Important Commands for the Lab

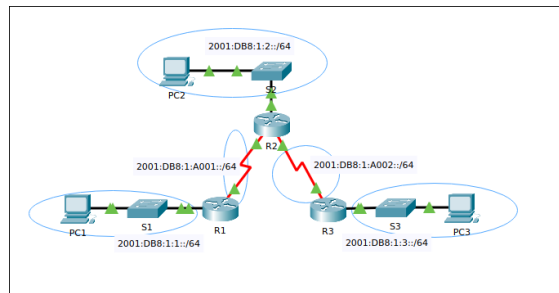
- `ipv6 unicast-routing`
- `ipv6 route`
- `show ipv6 interface brief`

- Important notes about IPv6

IPv6 uses a new mechanism for mapping IP addresses to link layer addresses (MAC addresses), because it does not support the broadcast addressing method, on which the functionality of the Address Resolution Protocol (ARP) in IPv4 is based. IPv6 implements the Neighbor Discovery Protocol (NDP, ND) in the link layer, which relies on ICMPv6 and multicast transmission. IPv6 hosts verify the uniqueness of their IPv6 addresses in a local area network (LAN) by sending a neighbor solicitation message asking for the link layer address of the IP address. If any other host in the LAN is using that address, it responds.

Part 1: Examine the Network

i) a There are 5 networks connected in the current topology



(a) Topology

Figure 5.1: Topology of the Network

ii) b

In Fig 5.1 we can see the R1 and R3 each have two connected networks, and that R2 has three connected networks.

iii) c

ipv6 route then we specify [the network, and prefix] then we specify either [next hop address or exit interface]

Part 2: Configure IPv6 static and default routes

i) Enabling the Routers

I logged into Each of the routers ena, conf t, and then typed in `ipv6 unicast-routing` into each terminal as seen in Fig 5.2.

```
R1>ena
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#
```

(a) R1 Enable

```
R2> ena
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#
```

(b) R2 Enable

```
R3>ena
R3#
R3#
R3#ena
R3#
R3#
R3#
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 unicast-routing
R3(config)#
```

(c) R3 Enable

Figure 5.2: Enabling IPv6

ii) Configuring the routers

Next I went to the three routers and manually entered the info for the network configuring each destination and each hop on the network. See Fig 5.3.



Figure 5.3: Manually Configuring the Destination IPv6 address, as well as the next hop address and Exit address

iii) Verifying Static Route Configurations

```

C:\>ipv6config

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::20A:F3FF:FE15:580C
IPv6 Address.....: 2001:DB8:1:1::F/64
Default Gateway.....: FE80::1
DHCPv6 Client DUID.....: 00-01-00-01-00-2B-D5-EC-00-0A-F3-15-58-0C

Bluetooth Connection:

Link-local IPv6 Address.....: ::
IPv6 Address.....: ::/0
Default Gateway.....: ::
DHCPv6 Client DUID.....: 00-01-00-01-00-2B-D5-EC-00-0A-F3-15-58-0C

C:\>

```

(a) IPv6Config

```

R3#show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::3
    2001:DB8:1:3::1
GigabitEthernet0/1      [administratively down/down]
    unassigned
Serial0/0/0             [administratively down/down]
    unassigned
Serial0/0/1             [up/up]
    FE80::3
    2001:DB8:1:A002::2
Vlan1                   [administratively down/down]
    unassigned
R3#

```

(b) IPv6 Interface brief

```

R3#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S    ::/0 [1/0]
    via 2001:DB8:1:A002::1
C    2001:DB8:1:3::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L    2001:DB8:1:3::1/128 [0/0]
    via GigabitEthernet0/0, receive
C    2001:DB8:1:A002::/64 [0/0]
    via Serial0/0/1, directly connected
L    2001:DB8:1:A002::2/128 [0/0]
    via Serial0/0/1, receive
L    FF00::/8 [0/0]
    via Null0, receive
R3#

```

(c) show ipv6 route

Figure 5.4: Verifying the Network

1

PC command

From the command prompt in the PC terminals, I entered the command `ipv6 config` for information on the network See Fig 5.4a

2

routing address

From the routers terminals

I entered `show ipv6 interface brief` to display the configured addresses. See Fig 5.4b

3

Routing Table

Finally, I entered `Show ipv6 route` into each of the prompts to display the routing tables. See Fig 5.4c

Congratulations chaz! You completed the activity.

Overall Feedback

Assessment Items

Connectivity Tests

Expand/Collapse All

Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
R1				
Routerv6				
Static Routes				
Route0	Correct	10	Static IPv6 Rou...	
Route1	Correct	10	Static IPv6 Rou...	
Route2	Correct	10	Static IPv6 Rou...	
R2				
Routerv6				
Static Routes				
Route0	Correct	10	Static IPv6 Rou...	
Route1	Correct	10	Static IPv6 Rou...	
R3				
Routerv6				
Static Routes				
Route0	Correct	10	Static IPv6 Rou...	

Score

: 60/60

Item Count

: 6/6

Component	Items/Total	Score
Static IPv6 Route Configuration	6/6	60/60

Lab 6

Configuring IPv4 Static Routes

Feb 8, 2020

Packet Tracer Lab 6
Spring 2020

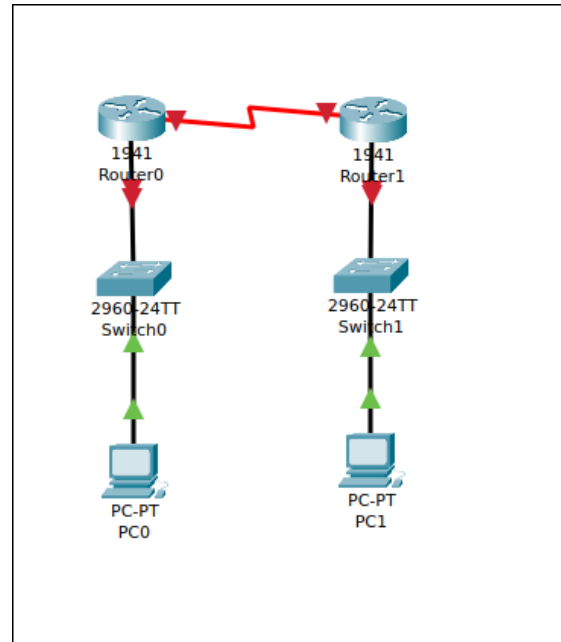
CIT 167
Chaz Davis

- Important Concepts for the Lab

- Recursive static route
a route whose next hop and destination network are covered by another learned route in the Routing Information Database (RIB).
Such static routes cannot be installed in the RIB because they are considered redundant routes.
- Directly Connected Static Route
A directly connected static route is one that uses the exit interface to forward traffic to the intended destination.
This is in contrast to the recursive static route which used the next hop IP address of the router along the path to the destination
- Loopback
A loopback interface is a logical, virtual interface in a cisco router.
A loopback interface is not a physical interface like Fast Ethernet or Gigabit Ethernet interface.
- A loopback interface has many uses
Loopback interface's IP Address determines a routers OSPF Router ID.
A loopback interface is always up and allows Border Gateway Protocol (BGP) neighborhood between two routers to stay up even if one of the outbound physical interfaces is down.

Part 1: Setting up the topology

i) **Cabling the Network** I've configured the network with two routers, 2 switches, and 2 pcs as seen in Fig. 6.1a.



(a) Cabling the topology

ii) Initialization

I flipped the switches and restarted the routers and switches.

Part 2: Configuring Basic Device Settings

i) **Configuring the PC Interfaces** I configured the PCs according to the table. As you can see in Fig. 6.2a and Fig. 6.2b on Pg. 42.

ii) Verify the LANs

Next, I ran commands on the routers to configure the device names, setup DNS lookup, added passwords, and then ran the configuration and startup styles.

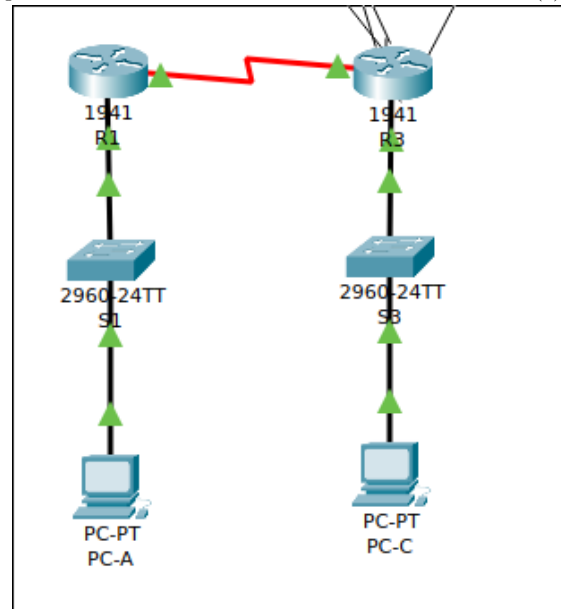
iii) Configuring IP settings on the routers

Finally i configured the ip addresses on the routers and set up the static routing tables fir the addresses. See Fig. 6.2d and Fig. 6.2e on Pg. 42.

<input checked="" type="radio"/> Static	192.168.1.10
192.168.0.10	255.255.255.0
255.255.255.0	192.168.1.1
192.168.0.1	0.0.0.0
0.0.0.0	

(a) PC-A IP config

(b) PC-B IPConfig



(c) The network now

```

Router>ena
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 10.1.1.2 255.255.255.252
Router(config-if)#
Router(config-if)#clock rate 128000
Router(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#exit
Router(config)#interface
% Incomplete command.
Router(config)#interface loopback 0

Router(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

Router(config-if)#ip address 209.165.200.225 255.255.255.224
Router(config-if)#no shut
Router(config-if)#exit interface loopback 1
^
% Invalid input detected at '^' marker.

Router(config-if)#exit
Router(config)#interface loopback 1

Router(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

Router(config-if)#ipaddress 198.133.219.1 255.255.255.0
^
% Invalid input detected at '^' marker.

Router(config-if)#ip address 198.133.219.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

```

(d) Router 3 config

```

Router>ena
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/1
Router(config-if)#ipaddress 10.1.1.1 255.255.255.252
^
% Invalid input detected at '^' marker.

Router(config-if)#ip address 10.1.1.1 255.255.255.252
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

Router(config-if)#exit
Router(config)#interface gig
Router(config)#interface gigabitEthernet 0/
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
Router(config-if)#interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shut
^
% Invalid input detected at '^' marker.

Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

```

(e) router 1 config

Figure 6.2: Configuring the network interfaces

iv) Verify Connectivity of LANs

I tested connectivity by pinging from each PC. I was able to ping from PC to router but from PC-A I was unable to reach PC-C or either loopback. See Fig. 6.3a. and Fig. 6.3b on Pg. 43.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=78ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time=12ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 78ms, Average = 22ms

C:\>
```

(a) Pinging the default gateway from PC-A
Pinging PC-C, Lo0, and Lo1 from PC-A

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

(b) Pinging the default gateway from PC-C

```
Router#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/15 ms

Router#
```

(c) Pinging S0/0/0 and R3 from R1

Figure 6.3: Verifying Connections between devices on the network

Part 3: Configure Static Routes

i) Configure recursive static route I went to R1 and entered the command `ip route 192.168.1.0 255.255.255.0 10.1.1.2` in to the command line.

The new `show ip route` shows us the static routing configuration.

In the last line we see `s 192.168.1.0/24 [1/0] via 10.1.1.2 .`

ii) Configure directly connected static route

I went to R3 and entered `ip route 192.168.0.0 255.255.255.0 serial 0/0/0.`

When I run the `show ip route` command from R3 we can now see the static exit interface in the line `s 192.168.0.0/24 is directly connected, Serial0/0/0`

iii) Configure Static Route

I went to R1 and ran `ip route 198.133.219.0 255.255.255.0 serial 0/0/1.`

iv) Remove static Routes for Loopback

I went to R1 and

ran `ip route 209.165.200.224 255.255.255.224 10.1.1.2`

and now we can see with the lines:

```
S    198.133.219.0/24 is directly connected, Serial0/0/1
      209.165.200.0/27 is subnetted, 1 subnets
S      209.165.200.224/27 [1/0] via 10.1.1.2
```

That we are correctly configured.

Part 4: Configure and verify the default route

I went to R1 and entered `ip route 0.0.0.0 0.0.0.0`.

I then went to PC-A and Pinged 209.165.200.225 see Fig. 6.4a

Lastly, I pinged 198.133.219.1 from PC-A. See Fig. 6.4b

```
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

(a) Pinging PC-C from PC-A

```
Pinging 198.133.219.1 with 32 bytes of data:

Reply from 198.133.219.1: bytes=32 time=2ms TTL=254
Reply from 198.133.219.1: bytes=32 time=1ms TTL=254
Reply from 198.133.219.1: bytes=32 time=2ms TTL=254
Reply from 198.133.219.1: bytes=32 time=1ms TTL=254

Ping statistics for 198.133.219.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

(b) Pinging R1 from PC-A

Figure 6.4: Verifying the default routes

Reflection

If we added a new network we could run `ip route 192.168.3.0 255.255.255.0 s0/0/0` `ip route 192.168.3.0 255.255.255.0 10.1.1.1` from R3

With a recursive static route perform lookups in the routing table before forwarding the packets. With a directly connected static route, the exit-interface parameter is specified, which allows the route to resolve a forwarding decision in one lookup.

A default gateway tells the device to contact the next hop of the default route if they don't have a more specific route. Without a default route, a router will drop a request for a network that is not in its routing table and send ICMP Destination unreachable.

Configuring Dynamic Routing

2020

Packet Tracer Labs
Spring 2020

CIT 167
Chaz Davis

Access RIP configuration mode

router rip

- Prompt will show up as `Router(config-router)#`
- When enabling RIP, the default version is RIPv1.
- To disable and eliminate RIP, use the 'no router rip' global configuration command. This command stops the RIP process and erases all existing RIP configurations.
- Upon enabling, need to advertise networks with 'network <network-address>'

Enable and Verify RIPv2

By default, when a RIP process is configured on a Cisco router, it is running RIPv1, as shown in Figure 1. However, even though the router only sends RIPv1 messages, it can interpret both RIPv1 and RIPv2 messages. A RIPv1 router ignores the RIPv2 fields in the route entry.

Use the 'version 2' router configuration mode command to enable RIPv2, as shown in Figure 2. Notice how the 'show ip protocols' command verifies that R2 is now configured to send and receive version 2 messages only. The RIP process now includes the subnet mask in all updates, making RIPv2 a classless routing protocol.

Note: Configuring 'version 1' enables RIPv1 only, while configuring 'no version' returns the router to the default setting of sending version 1 updates but listening for version 1 and version 2 updates.

Propagate a Default Route

The 'default-information originate' router configuration command. This instructs R1 to originate default information, by propagating the static default route in RIP updates.

RIP Routing Configuration Mode Commands

```
...
network <network-address>      # Enables RIP on all interfaces on that network.
version 2                      # Enables RIPv2
version 1                      # Enables RIPv1 only
no version                     # Returns to default setting: send v1, listen v1+v2
no auto-summary                # Disables default automatic summarization (RIPv2)

passive-interface <interface>  # Prevent transmission of routing updates out interface
# However, still allows network to be advertised
passive-interface g0/0
passive-interface default      # Makes all interfaces passive
no passive-interface <intf>    # Re-enables passive transmission of routing updates
...
```

Verify RIP Routing

```
...
show ip protocols
show ip route
...
```

Propagate a Default Route

To propagate a default route in RIP,
the edge router must be configured with a default static route
using the `ip route 0.0.0.0 0.0.0.0` command:

```
...
ip route 0.0.0.0 0.0.0.0 <exit-interface> <next-hop IP>
...
```

Next configure router to propagate the static default route in RIP updates:

```
...
router rip
default-information originate
...
```

Useful Bits

Dynamic Routing

2020

Packet Tracer Labs
Spring 2020

CIT 167
Chaz Davis

RIP Overview

The Routing Information Protocol (RIP) uses broadcast UDP data packets to exchange routing information. Cisco software sends routing information updates every 30 seconds, which is termed advertising. If a device does not receive an update from another device for 180 seconds or more, the receiving device marks the routes served by the nonupdating device as unusable. If there is still no update after 240 seconds, the device removes all routing table entries for the nonupdating device.

A device that is running RIP can receive a default network via an update from another device that is running RIP, or the device can source the default network using RIP. In both cases, the default network is advertised through RIP to other RIP neighbors.

The Cisco implementation of RIP Version 2 (RIPv2) supports plain text and message digest algorithm 5 (MD5) authentication, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).

RIP Routing Updates

The Routing Information Protocol (RIP) sends routing-update messages at regular intervals and when the network topology changes. When a device receives a RIP routing update that includes changes to an entry, the device updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP devices maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the device immediately begins transmitting RIP routing updates to inform other network devices of the change. These updates are sent independently of the regularly scheduled updates that RIP devices send.

RIP Routing Metric

The Routing Information Protocol (RIP) uses a single routing metric to measure the distance between the source and the destination network. Each hop in a path from the source to the destination is assigned a hop-count value, which is typically 1. When a device receives a routing update that contains a new or changed destination network entry, the device adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop. If an interface network is not specified in the routing table, it will not be advertised in any RIP update.

Authentication in RIP

The Cisco implementation of the Routing Information Protocol (RIP) Version 2 (RIPv2) supports authentication, key management, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).

By default, the software receives RIP Version 1 (RIPv1) and RIPv2 packets, but sends only RIPv1 packets. You can configure the software to receive and send only RIPv1 packets. Alternatively, you can configure the software to receive and send only RIPv2 packets. To override the default behavior, you can configure the RIP version that an interface sends. Similarly, you can also control how packets received from an interface are processed.

RIPv1 does not support authentication. If you are sending and receiving RIP v2 packets, you can enable RIP authentication on an interface.

The key chain determines the set of keys that can be used on the interface. Authentication, including default authentication, is performed on that interface only if a key chain is configured. For more information on key chains and their configuration, see the “Managing Authentication Keys” section in the “Configuring IP Routing Protocol-Independent Features” chapter in the Cisco IOS IP Routing: Protocol-Independent Configuration Guide.

Cisco supports two modes of authentication on an interface on which RIP is enabled: plain-text authentication and message digest algorithm 5 (MD5) authentication. Plain-text authentication is the default authentication in every RIPv2 packet.

Note

Do not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIPv2 packet. Use plain-text authentication when security is not an issue; for example, you can use plain-text authentication to ensure that misconfigured hosts do not participate in routing.

Exchange of Routing Information

Routing Information Protocol (RIP) is normally a broadcast protocol, and for RIP routing updates to reach nonbroadcast networks, you must configure the Cisco software to permit this exchange of routing information. To control the set of interfaces with which you want to exchange routing updates, you can disable the sending of routing updates on specified interfaces by configuring the passive-interface router configuration command.

You can use an offset list to increase increasing incoming and outgoing metrics to routes learned via RIP. Optionally, you can limit the offset list with either an access list or an interface. Routing protocols use several timers that determine variables such as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better suit your internetwork needs. You can make the following timer adjustments:

The rate (time, in seconds, between updates) at which routing updates are sent The interval of time, in seconds, after which a route is declared invalid The interval, in seconds, during which routing information about better paths is suppressed The amount of time, in seconds, that must pass before a route is removed from the routing table The amount of time for which routing updates will be postponed You can adjust the IP routing support in the Cisco software to enable faster convergence of various IP routing algorithms, and hence, cause quicker fallback to redundant devices. The total effect is to minimize disruptions to end users of the network in situations where quick recovery is essential

In addition, an address family can have timers that explicitly apply to that address family (or Virtual Routing and Forwarding [VRF] instance). The timers-basic command must be specified for an address family or the system defaults for the timers-basic command are used regardless of the timer that is configured for RIP routing. The VRF does not inherit the timer values from the base RIP configuration. The VRF will always use the system default timers unless the timers are explicitly changed using the timers-basic command.

RIP Route Summarization

Summarizing routes in RIP Version 2 improves scalability and efficiency in large networks. Summarizing IP addresses means that there is no entry for child routes (routes that are created for any combination of the individual IP addresses contained within a summary address) in the RIP routing table, reducing the size of the table and allowing the router to handle more routes.

Summary IP address functions more efficiently than multiple individually advertised IP routes for the following reasons: The summarized routes in the RIP database are processed first. Any associated child routes that are included in a summarized route are skipped as RIP looks through the routing database, reducing the processing time required. Cisco routers can summarize routes in two ways: Automatically, by summarizing subprefixes to the classful network boundary when crossing classful network boundaries (automatic summary).

Note

Automatic summary is enabled by default.

As specifically configured, advertising a summarized local IP address pool on the specified interface (on a network access server) so that the address pool can be provided to dialup clients. When RIP determines that a summary address is required in the RIP database, a summary entry is created in the RIP routing database. As long as there are child routes for a summary address, the address remains in the routing database. When the last child route is removed, the summary entry also is removed from the database. This method of handling database entries reduces the number of entries in the database because each child route is not listed in an entry, and the aggregate entry itself is removed when there are no longer any valid child routes for it.

RIP Version 2 route summarization requires that the lowest metric of the "best route" of an aggregated entry, or the lowest metric of all current child routes, be advertised. The best metric for aggregated summarized routes is calculated at route initialization or when there are metric modifications of specific routes at advertisement time, and not at the time the aggregated routes are advertised.

The `ip summary-address rip` router configuration command causes the router to summarize a given set of routes learned via RIP Version 2 or redistributed into RIP Version 2. Host routes are especially applicable for summarization.

See the "Route Summarization Example" section at the end of this chapter for examples of using split horizon.

You can verify which routes are summarized for an interface using the `show ip protocols EXEC` command. You can check summary address entries in the RIP database. These entries will appear in the database only if relevant child routes are being summarized. To display summary address entries in the RIP routing database entries if there are relevant routes being summarized based upon a summary address, use the `show ip rip database` command in EXEC mode. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table.

Lab 7

Configuring RIPv2

Jan 31, 2020

Packet Tracer Lab 7
Spring 2020

CIT 167
Chaz Davis

- Important Commands for the Lab

- router rip
 - version 2
- no auto-summary
- network
 - for when long commands are interrupted by console message
- passive-interface

Part 1: Configure RIPv2

i) Configure RIPv2 on R1 I configured the Router for default route all internet traffic through serial 0/0/1

```
R1>ena
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#
```

Next I, configured the router to use rip protocol, then to use version 2, and then passed it the no auto-summary command

```
R1>ena
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#
```

I set the networks on R1, and then Used the passive interface command to setup the LAN port, and then default-information originate to advertise the routes that I've configured see: 7.1a.

Lastly, I stepped out of config router mode and ran the command: copy-running config startup-config to save my work see:7.1b

```
R2>ena
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#netw
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.4.0
R2(config-router)#passive
R2(config-router)#passive-interface gi
R2(config-router)#passive-interface gigabitEthernet 0/0
R2(config-router)#z
R2#
%SYS-5-COMP16.1: Configured from console by console

R2#run
R2#run
R2#runin
R2#copy
R2#copy run
R2#copy running-config st
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

(a) setting networks R1

```
R1#copy runn
R1#copy running-config star
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

(b) Finishing up R1

Figure 7.1: Configuring R1 for RIPv2

ii) Configure RIPv2 on R2 and R3 Next I configured R2 and R3 for their networks

```
R2>ena
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#netw
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.4.0
R2(config-router)#passive
R2(config-router)#passive-interface gi
R2(config-router)#passive-interface gigabitEthernet 0/0
R2(config-router)#z
R2#
%SYS-5-COMP16.1: Configured from console by console

R2#run
R2#run
R2#runin
R2#copy
R2#copy run
R2#copy running-config st
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

(a) Configuring R2

```
R3>ena
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#no auto-summary
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#pass
R3(config-router)#passive-interface gi
R3(config-router)#passive-interface gigabitEthernet 0/0
R3(config-router)#z
R3#
%SYS-5-COMP16.1: Configured from console by console

R3#copy
R3#copy run
R3#copy running-config st
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#
```

(b) Configuring R3

Figure 7.2: Configuring the Routers for RIPv2

Part 2: Verify Configurations

i) View Routing Tables of R1, R2, and R3



Figure 7.3: IP Routing Tables for the Routers

ii) Success

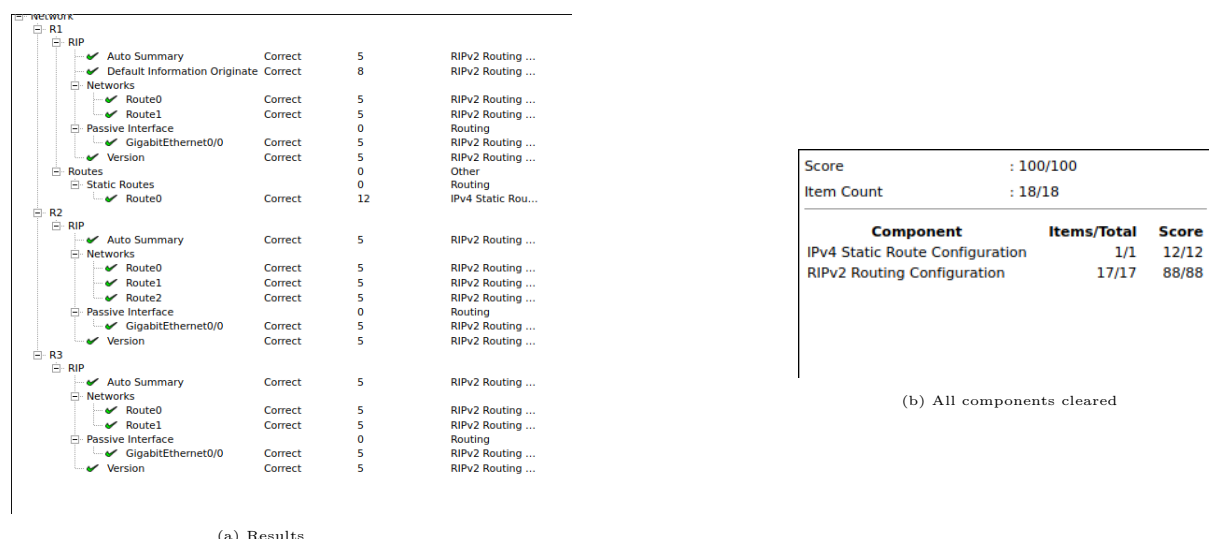


Figure 7.4: Successful Completion

Lab 8

Configuring Basic RIPv2

Jan 31, 2020

Packet Tracer Lab 8
Spring 2020

CIT 167
Chaz Davis

- Important Commands for the Lab

```
enable
configure terminal

router rip
network 192.168.0.0
version 2
exit
exit

show ip route
ping 192.168.3.1
trace 192.168.3.1

exit
```

- Important Concepts

- Dynamic or adaptive routing involves automatic updating of the routing tables based on information carried by routing protocols.
- Link-state protocols require that a router inform all the nodes in a network of topology changes. Each node shares info regarding the nodes it can connect to with the entire network so that each node can build its own network map and determine for itself the least cost path to any given node.
- RIP is a distance vector routing protocol which employs the hop count as a routing metric. RIP uses UDP as its transport protocol, and is assigned the reserved port number 520.
- auto summarization a feature which allows RIP to summarize its routes to their classful networks automatically.

Part 1: Build the Network and Configure Basic Device Settings

I did as the Lab specified, I placed three 1941 routers, making sure to turn them off and add on the Serial ports, turning them back on when finished. I then placed two 2960 switches, and then three end user PCs as instructed.

i) **Cable The Network** I ran the cabling between as shown in the diagram Fig 8.1, connecting the correct ports and interfaces.

ii) **Initialize the Router and Switch and Configure basic settings for each** I configured each of the routers and then their serial interfaces, i then configured the switches

iii) **Configure PC IP Addressing** I went to the desktop of each pc and set it up according to the addressing table. See Fig 8.2.

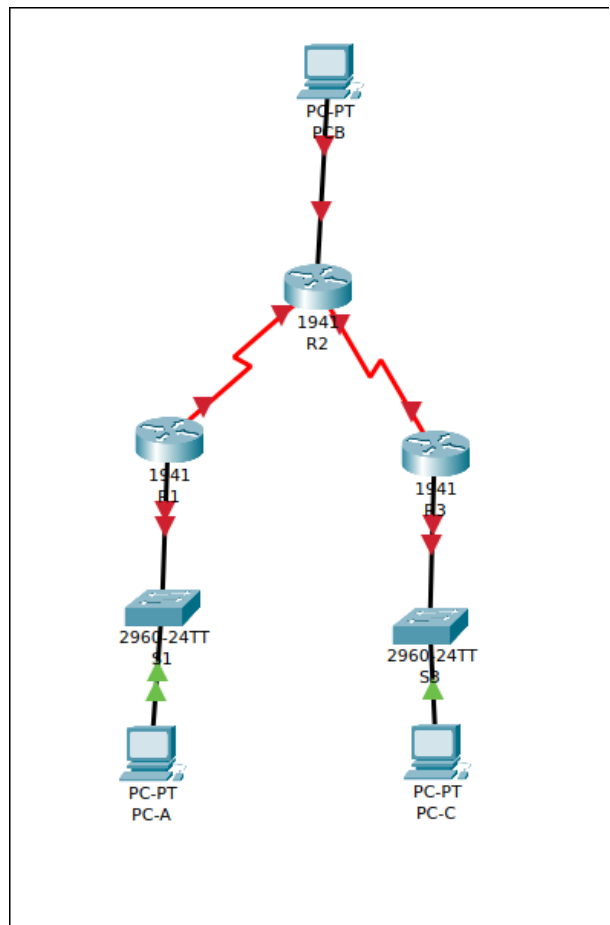


Figure 8.1: Cabling the Network

<input checked="" type="radio"/> Static
172.30.10.3
255.255.255.0
172.30.10.1
0.0.0.0

(a) Configuring PC A

<input checked="" type="radio"/> Static
209.165.201.2
255.255.255.0
209.165.201.1
0.0.0.0

(b) Configuring PC B

<input checked="" type="radio"/> Static
172.30.30.3
255.255.255.0
172.30.30.1
0.0.0.0

(c) Configuring PC C

Figure 8.2: Setting up the PC's according to the addressing Table

iv) Test Connectivity

To test connectivity I went to the command prompt on each of the PCs and pinged their routers. See Fig 8.3.

```
C:\>ping 172.30.10.1

Pinging 172.30.10.1 with 32 bytes of data:

Reply from 172.30.10.1: bytes=32 time=1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time=2ms TTL=255
Reply from 172.30.10.1: bytes=32 time=1ms TTL=255

Ping statistics for 172.30.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

(a)

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.30.30.1

Pinging 172.30.30.1 with 32 bytes of data:

Reply from 172.30.30.1: bytes=32 time=1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.30.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

(b)

```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

(c)

Figure 8.3: Testing Connectivity

Part 2: Configure and Verify RIPv2 Routing

i) **Configure RIPv2 routing** I ran the commands for setting up router rip version two on each router see Fig 8.4a.

ii) **Examine the current state of the network**

I ran show ip interface brief from router 2. See Fig 8.4b.

iii) **Disable automatic summarization**

I ran No auto-summary from each of the routers, cleared the ip routing tables

iv) **Configure and redistribute a default route for internet access**

I went to R2 set the default route and then gave the command to distribute the table amongst the network

v) **Verify the routing configuration**

I went to R1 and typed show ip route to verify the network configurations as you can see in Fig 8.5a.

I then Pinged PC-B from PC-A's interface. See Fig 8.5b.

Finally, I pinged PC-C from PC-B. Fig 8.5c.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
  10.1.1.0/30 is directly connected, Serial0/0/0
  10.1.1.1/32 is directly connected, Serial0/0/0
172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
  172.30.10.0/24 is directly connected, GigabitEthernet0/1
  172.30.10.1/32 is directly connected, GigabitEthernet0/1

R1#
```

(a) Setting Up RIPv2 on Each Router

```
R2#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  209.165.201.1  YES manual up          up
GigabitEthernet0/1  unassigned      YES unset  administratively down down
Serial0/0/0        10.1.1.2        YES manual up          up
Serial0/0/1        10.2.2.2        YES manual up          up
Vlan1            unassigned      YES unset  administratively down down
R2#
```

(b) show ip interface brief ran from router 2

Figure 8.4: Configuring RIPv2 on the network

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       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, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
  10.1.1.0/30 is directly connected, Serial0/0/0
  10.1.1.1/32 is directly connected, Serial0/0/0
  10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:25, Serial0/0/0
172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
  172.30.10.0/24 is directly connected, GigabitEthernet0/1
  172.30.10.1/32 is directly connected, GigabitEthernet0/1
  172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:25, Serial0/0/0
* 0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:25, Serial0/0/0

R1#
```

(a) Running show ip route from R1

```
C:\>ping 209.165.201.2

Pinging 209.165.201.2 with 32 bytes of data:

Reply from 209.165.201.2: bytes=32 time=2ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126
Reply from 209.165.201.2: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.201.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

(b) Pinging PC-B from PC-A

```
C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=2ms TTL=125
Reply from 172.30.30.3: bytes=32 time=2ms TTL=125
Reply from 172.30.30.3: bytes=32 time=5ms TTL=125
Reply from 172.30.30.3: bytes=32 time=2ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 5ms, Average = 2ms
```

(c) Pinging PC-C from PC-A

Figure 8.5: Verifying connectivity

Part 3: Reflection

i) Why would you turn off auto-summary? Route summarization reduces the amount of routing information in the routing tables. If you are using RIP Version 2, you can turn off automatic summarization by specifying no auto-summary. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is off, subnets are advertised.

ii) How did R1 and R3 learn the pathway to the internet? they are using rip routing updates from the router default config. RIPv2 multicasts the entire routing table to all adjacent routers at the address

SSH and Port Security

2020

Packet Tracer Labs
Spring 2020

CIT 167
Chaz Davis

Configuring SSH

- All switch ports (interfaces) should be secured before the switch is deployed for production use.
 - Specify a single MAC address or a group of valid MAC addresses allowed on a port.
 - Specify that a port automatically shuts down if unauthorized MAC addresses are detected.
- Sticky secure MAC addresses
 - MAC addresses that can be dynamically learned or manually configured, then
 - stored in the address table and added to the running configuration by stick learning:
- If the sticky secure MAC addresses are saved to the startup configuration file
 - then when the switch restarts or the interface shuts down, the interface does not need to relearn the addresses.
 - If the sticky secure addresses are not saved, they will be lost.
- If sticky learning is disabled by using the `no switchport port-security mac-address sticky` interface configuration mode command
 - the sticky secure MAC addresses remain part of the address table, but are removed from the running configuration.

Characteristics of sticky secure MAC addresses:

- Learned dynamically, converted to sticky secure MAC addresses stored in the running-config.
- Removed from the running-config if port security is disabled.
- Lost when the switch reboots (power cycled).
- Saving sticky secure MAC addresses in the startup-config makes them permanent and the switch retains them after a reboot.
- Disabling sticky learning converts sticky MAC addresses to dynamic secure addresses and removes them from the running-config.

Note: The port security feature will not work until port security is enabled on the interface using the `switchport port-security` command.

Port Security: Violation Modes

- **Protect** When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. There is no notification that a security violation has occurred.
- **Restrict** When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. In this mode, there is a *notification that a security violation has occurred*.
- **Shutdown** In this (**default**) mode, a port security violation causes the interface to immediately become error-disabled and turns off the port LED. It increments the violation counter.

When a secure port is in the error-disabled state, it can be brought out of this state by entering the **shutdown** interface configuration mode command followed by the **no shutdown** command.

Port Security: Configuring

Default Port Security on a Cisco Catalyst Switch

- Port security and Sticky address learning: Disabled
- Max number of secure MAC addresses: 1
- Violation mode: Shutdown (Port shuts down when max number of secure MAC addresses exceeded).

Ports in Error Disabled State

- When a port is error disabled, it is effectively shut down and no traffic is sent or received on that port.
- Port protocol and link status is changed to down; port LED will turn off; port goes into the error disabled state.
- **show interfaces** identifies port status as **err-disabled**
- **show port-security interface** shows port status as **secure-shutdown**

The administrator should determine what caused the security violation before re-enabling the port. If an unauthorized device is connected to a secure port, the port should not be re-enabled until the security threat is eliminated. To re-enable the port, use the **shutdown** interface configuration mode command (Figure 3). Then, use the **no shutdown** interface configuration command to make the port operational.

SSH and Port Security

2020

Packet Tracer Labs
Spring 2020

CIT 167
Chaz Davis

Configuring SSH

SSH configuration

```
show ip ssh                # Verify that switch supports SSH, shows version

ip domain-name <domain-name> # Device must be minimally configured with a hostname
ip ssh version 2            # Recommended to only enable version 2 (more secure)
crypto key generate rsa
username <username> privilege <level> secret <password>
```

Enable SSH protocol on VTY lines

```
line vty 0 15
transport input ssh
login local                # Require local authentication from local username database
```

To delete a RSA key pair

```
crypto key zeroize rsa      # SSH automatically disabled when key pair is deleted.
```

Port Security

Disable Unused Ports - Good practice to disable unused ports; can configure range:

```
interface range <type module>/<first number>-<last number>
shutdown
```


Port Security: Operation Static Secure MAC Address:

```
interface <interface-id>
switchport port-security mac-address <mac-address>
```

Sticky secure MAC addresses - MAC addresses that can be dynamically learned or manually configured, then stored in the address table and added to the running configuration by stick learning:

```
switchport port-security mac-address sticky          # (Intf-config)
```

- *All sticky secure MAC addresses are added to the address table and to the running configuration*.
- Sticky secure MAC addresses can also be manually defined (also added to running-config):

```
switchport port-security mac-address sticky <mac-address>
```

Port Security: Violation Modes

To change the violation mode on a switch port:

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

Port Security: Configuring

Configure Port Security on an Interface

```
interface <interface_id>
switchport mode access          # Sets interface mode to access
switchport port-security        # Enables port security on the interface
switchport port-security maximum 10 # Max number of secure addresses allowed
switchport port-security mac-address sticky # Enables sticky learning
```

- Violation mode is set to shutdown by default.

Port Security: Verifying

Verify Port Security Settings:

```
show port-security interface <interface_id>
```

Verify Secure MAC Addresses:

```
show port-security address
```

Lab 9

Basic Switch Configuration

February 21, 2020

Packet Tracer Lab 09
Spring 2020

CIT 167
Chaz Davis

switch shit

- something something commands

Part 1: Cable the Network and Verify the Default Switch Configuration

i) Cable the Network I set up the network according to the topography, see Fig. 9.1a on Pg. 68. I went to the flash memory on the switch, and there was no vlan.dat configuration. So I proceeded to the next step.

ii) Verify the default switch Configuration

a) I ran the enable command to log into privileged exec mode and ran the following commands:

b) We can see in Fig. 9.1b on Pg. 68 that the switch has 24 fast ethernet ports and that the switch has 2 gigabit ethernet ports. We can also see that the vty lines have the values 0 4 and 5 15.

c) In Fig. 9.2a on Pg. 69 that we do indeed get the response `startup-config is not present`, this is because we have not configured any settings, and have in fact reset the switch.

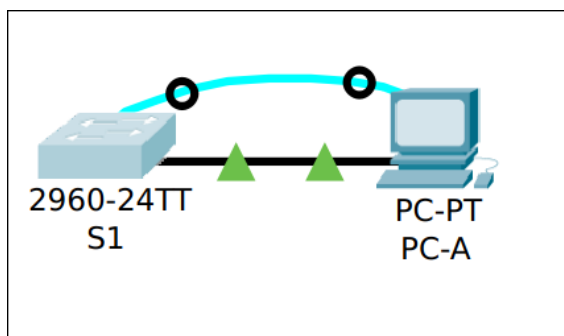
d) From the output of Fig. 9.2b on Pg. 69 that there is no ip address assigned yet, because we have not set it up yet, and that the mac address is 00e0.f9bd.263e.

e and f) You can see in Fig. 9.2 c on Pg. 69 that protocols are down and vlan 1 is not set up yet. It's showing multicast and fifo settings after hookup.

g) You can see in Fig. 9.3 a on Pg. 69 that the Cisco IOS version on the switch is 12.2(25)FX, and the system image filename C2960-LANBASE-M, and the mac address is 00e0.f9bd.263e.

h) You can see in Fig. 9.3 b on Pg. 69 that the interface is up because we connected it to the PC. mac address is 00e0.b037.9co6. The speed of the switch is 100mb/s and it is full duplex.

i) You can see in Fig. 9.3 c on Pg. 69 that the name of vlan 1 is default, currently all ports on on vlan 1, the default type is ethernet.



(a) Cabling the Network

```

Switch#show run
Building configuration...

Current configuration : 1000 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
end

```

(b) show running config output

Figure 9.1: Configuring and verifying the switch Pt 1

```
Switch#
Switch#show startup-config
startup-config is not present
Switch#
```

(a) show startup config

```
Switch#show interface Vlan 1
Vlan1 is administratively down, line protocol is down
Hardware is CPU Interface, address is 00e0.f9bd.263e (bia 00e0.f9bd.263e)
MTU 1500 bytes, BW 1000000 Kbit, DLY 1000000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 21:40:21, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1682 packets input, 530955 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
563859 packets output, 0 bytes, 0 underruns
0 output errors, 23 interface resets
0 output buffer failures, 0 output buffers swapped out
```

(b) show interface vlan1

```
Switch#show ip interface vlan 1
Vlan1 is administratively down, line protocol is down
Internet protocol processing disabled
```

(c) show ip interface vlan1 after connecting the ethernet cable

Figure 9.2: Configuring and Verifying the switch Pt 2

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (rc4)

System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32900) processor (revision C0) with 21899K bytes
of memory.

24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

83488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address : 00E0.F9BD.263E
Motherboard assembly number : 73-0832-06
Power supply part number : 341-0007-02
Motherboard serial number : FOC103248MJ
Power supply serial number : DCA102133JA
Model revision number : B0
Motherboard revision number : C0
Model number : WS-C2960-24TT
System serial number : FOC103212V
Top Assembly Part Number : 800-26071-02
Top Assembly Revision Number : B0
Version ID : V02
CLEI Code Number : CMXK0088RA
Hardware Board Revision Number : 0x01

Switch Ports Model SW Version SW Image
-----
1 20 WS-C2960-24TT 12.2 C2960-LANBASE-M

Configuration register is 0x0
```

(a) show version output

```
Switch#show int f0/6
FastEthernet0/6 is up, line protocol is up (connected)
Hardware is Lance, address is 00e0.b037.9c06 (bia 00e0.b037.9c06)
BW 1000000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000000/s
Input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
0 output errors, 0 collisions, 10 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

(b) show interface f0/6

```
Switch#show vlan
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, Fa0/11,
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, Gig0/1, Gig0/2
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active

VLAN Type SAID          MTU Parent RingNo BridgeNo Stp BrgdMode Trans1
Trans2
-----
1 enet 100001 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fddnet 101004 1500 - - - - - ieee 0 0
1005 trnet 101005 1500 - - - - - lbn 0 0

VLAN Type SAID          MTU Parent RingNo BridgeNo Stp BrgdMode Trans1
Trans2
-----
Remote SPAN VLANs
-----
Primary Secondary Type Ports
-----
```

(c) show vlan

```
Switch#show flash
Directory of flash:/

 1 -rw- 4414921 <no date> c2960-lanbase-mz.
122-25.FX.bin

64016384 bytes total (59601463 bytes free)
```

(d) show flash

Figure 9.3: Configuring and Verifying the switch Pt 3

Part 2: Configure Basic Network Device Settings

i) Configure basic switch settings I ran pasted the commands as shown by you. I ran the commands to setup the ip address and default ip address. I set up the console and setup the vty. The login command is required because it logs in the first time and makes us use the password afterwards.

ii) Configure IP address on PC-A

I logged into PC-A and configured the ip configuration according to the table

Part 3: Verify and Test Network Connectivity

i) Display the switch configuration You can see in Fig. 9.4 a on Pg. 71 and Fig. 9.4b on Pg. 71 that the bandwidth is 100,000 bytes, its state is up and its protocol is up.

ii) Test end-to-end connectivity with ping

I ran ping from PC-A to PC-A as seen in Fig. 9.4c on Pg. 71.

I then, Pinged S1 from PC-A, the first ping was lost due to address resolution, as you can see in Fig. 9.4d on Pg. 71.

iii) Test and Verify Remote management of S1

From PC-A I remotely logged into S1 via telnet. See Fig. 9.4e on Pg. 71.

iv) Saving the Switch Running Configuration File

I saved the switches configuration file.

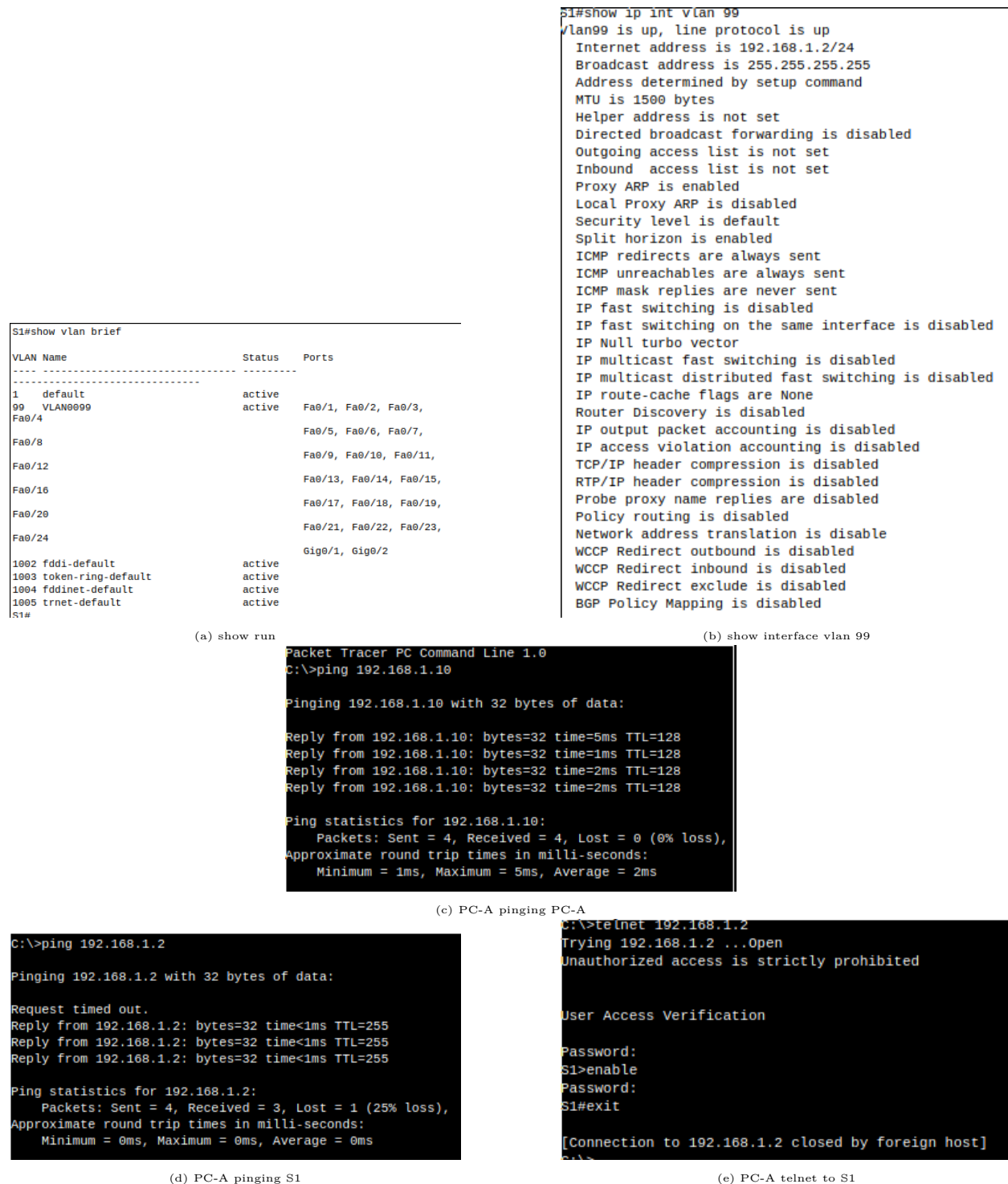


Figure 9.4: Verifying and Testing Network Connectivity

Part 4: Manage the MAC Address table

i) Record the MAC address of the host

there were none listed in the table. zero in total.

ii) Determine the MAC Addresses that the switch has learned

There are three options for Mac addressing dynamic, interfaces, or static.

iii) List the show mac address-table options

There are three options, dynamic, interfaces, or static.

iv) Set up a static MAC address

I ran the commands as shown and set up the mac address, statically.

Reflection

i) Why should you configure the vty password for the switch?

To protect it from unwanted usage where someone could set up a way into the network and where they would have root access to the network.

ii) Why change the default VLAN 1 to a different VLAN number?

harder to find from cursory looks at the network.

iii) How can you prevent passwords from being sent in plain text?

set encryption

iv) Why configure a static MAC address on a port interface?

so that it stays the same and doesnt try to ask the DNS to resolve it and risk losing it and resetting the main ports of the network.

Lab 10

Configuring Switch Security Features February 26, 2020

Packet Tracer Lab 10
Spring 2020

CIT 167
Chaz Davis

Sec features

- some thing

Part 1: The Lab

- i) **Cable the Network** I created and cabled the network according to the diagram.
- ii) **Initialize and reload the router and switch** I went into router configuration, and checked the flash.
- iii) **Configure an IP address on PC-A** I then went to PC-A and setup the IP configuration.
- iv) **Configure basic settings on R1** I went into R1 and entered the commands and then copied the running and startup configs.
- v) **Configure basic settings on S1** I ran the commands from the diagram, setting up basic settings and then creating and configuring vlan 99.

When I issued the `show vlan` command it shows vlan 99 as active.

When I ran the command `show ip interface brief` the status was ok and protocol was down.

It shows as down because it's not connected to a network.

After assigning f0/5 and f0/6 to vlan 99 no when running the `show ip int brief` command we can see vlan 99 as up.

vi) Verify Connectivity between Devices

As you can see in Fig. 10.1 All of the pings were successful.

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.99.1

Pinging 172.16.99.1 with 32 bytes of data:

Reply from 172.16.99.1: bytes=32 time=87ms TTL=255
Reply from 172.16.99.1: bytes=32 time<1ms TTL=255
Reply from 172.16.99.1: bytes=32 time<1ms TTL=255
Reply from 172.16.99.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.99.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 87ms, Average = 21ms
```

(a) PC-A pinging R1

```
C:\>ping 172.16.99.11

Pinging 172.16.99.11 with 32 bytes of data:

Request timed out.
Reply from 172.16.99.11: bytes=32 time<1ms TTL=255
Reply from 172.16.99.11: bytes=32 time<1ms TTL=255
Reply from 172.16.99.11: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.99.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

(b) PC-A pinging S1

```
S1#ping 172.16.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

(c) S1 pinging R1

Figure 10.1: Successful pings on the network

vii) Configure SSH access on S1

The ssh-version is 1.99

SSH will allow 3 retries

the default timeout is 120 secs

viii) Modify the SSH configuration on S1

It will now allow 2 retries, so a total of 3 attempts.

The timeout would be 75 seconds. So, 1 minute and 15 seconds.

a) It was successful, and the prompt said unauthorized access is strictly prohibited, and the gave the S1 prompt with the octothorpe signifying the admin account.

ix) Configure general security features on S1

b)

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited. Violators will be prosecuted to the full extent of the law. #
S1(config)#exit
```

Figure 10.2: Banner MOTD update

c) The physical ports that are open are Fa0/5 and Fa0/6

c & d) I ran the commands the output of `show ip int brief` gives us:

```
S1#show ip int brief
Interface          IP-Address      OK? Method Status                Protocol
FastEthernet0/1    unassigned      YES manual administratively down  down
FastEthernet0/2    unassigned      YES manual administratively down  down
FastEthernet0/3    unassigned      YES manual administratively down  down
FastEthernet0/4    unassigned      YES manual administratively down  down
FastEthernet0/5    unassigned      YES manual up                up
FastEthernet0/6    unassigned      YES manual up                up
FastEthernet0/7    unassigned      YES manual administratively down  down
FastEthernet0/8    unassigned      YES manual administratively down  down
FastEthernet0/9    unassigned      YES manual administratively down  down
FastEthernet0/10   unassigned      YES manual administratively down  down
FastEthernet0/11   unassigned      YES manual administratively down  down
FastEthernet0/12   unassigned      YES manual administratively down  down
FastEthernet0/13   unassigned      YES manual administratively down  down
FastEthernet0/14   unassigned      YES manual administratively down  down
FastEthernet0/15   unassigned      YES manual administratively down  down
FastEthernet0/16   unassigned      YES manual administratively down  down
FastEthernet0/17   unassigned      YES manual administratively down  down
FastEthernet0/18   unassigned      YES manual administratively down  down
FastEthernet0/19   unassigned      YES manual administratively down  down
FastEthernet0/20   unassigned      YES manual administratively down  down
FastEthernet0/21   unassigned      YES manual administratively down  down
FastEthernet0/22   unassigned      YES manual administratively down  down
FastEthernet0/23   unassigned      YES manual administratively down  down
FastEthernet0/24   unassigned      YES manual administratively down  down
GigabitEthernet0/1 unassigned      YES manual down                down
GigabitEthernet0/2 unassigned      YES manual down                down
Vlan1              unassigned      YES manual administratively down  down
Vlan99             172.16.99.11    YES manual up                up
S1#
```

Figure 10.3: Output of `show ip int brief`

x) Configure and verify port security on S1

- a) The macaddress is 0004.9a08.6602
- b) fa0/5 has a mac address of 0004.9a08.6602 and fa0/6 doesnt show on the table.
- c & d) The port status is Secure-Up.
- e) From R1 I pinged PC-A as seen in Fig. 10.4a.
- l) The ping from R1 to PC-A was not successful.
- m) See Fig. 10.4b for the output of `show int f0/5`.
- p) This time the ping was successful again. See Fig. 10.4c

```
R1#ping 172.16.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

(a) With a MAC-address

```
R1#ping 172.16.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

(b) With no mac-address

```
R1#ping 172.16.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

(c) With S1 back on

Figure 10.4: Ping from R1 to PC-A

Reflection

- i) **Why would you enable port security on a switch?** To prevent unauthorized users to gain access to the LAN.
- ii) **Why should unused ports on a switch be disabled?**
Any enabled port not in use could allow someone to come in and plug into your network and gain access. So, it's best practice to disable any unused ports.

Lab 11

Troubleshooting Vlans

Scenario 1

February 29, 2020

Netlab Lab 11
Spring 2020

CIT 167
Chaz Davis

troubleshooting vlans

- something something blah

Part 1: Test Connectivity between PCs on the Same VLAN

i) Can PC1 ping PC4

Attempt to ping PC4 from PC1 was unsuccessful. See Fig. 11.1 a.

ii) Can pc2 ping pc5

Attempt to ping PC5 from PC2 was unsuccessful. See Fig. 11.1 b.

iii) Can pc3 ping pc6

Attempt to ping PC6 from PC3 was unsuccessful. See Fig. 11.1 c.

```
C:\>ping 172.17.10.24

Pinging 172.17.10.24 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.10.24:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

(a) PC1 pinging PC4

```
C:\>ping 172.17.20.25

Pinging 172.17.20.25 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.20.25:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

(b) PC2 pinging PC5

```
C:\>ping 172.17.30.26

Pinging 172.17.30.26 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.17.30.26:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

(c) PC3 Pinging PC6

Figure 11.1: Testing Connections on the same networks

Part 2: Investigate Connectivity Problems by Gathering Data

i) Verify Configurations on the PCs

I checked configurations for IP address and subnetmasks on all pcs. PC5 had an incorrect IP address.

ii& 3) Verify Confgs on the Switches

On switch2 vlan for subnet 30 had the 10 and 30 subnets attached to it, so I moved the Fa0/11 interface to 10 faculty/staff. Also on S2, G0/1 was not setup as a trunk.

PC5 appears to be connected on port Fa0/17 when it should be Fa0/18.

Switch3, vlan 20 and vlan 30 are switched on their connections.

Part 3: Implement the Solution and Test Connectivity

On S2 I ran `int fa 0/11` and then `switchport access vlan 10` to correct the first issue. Then I ran, `int g0/1` and then `switchport mode trunk`.

On S1, I ran `int g0/1` and then `switchport mode trunk`.

On S3, I ran `int f0/18` and then `switchport access vlan 20`. I then ran `int f0/6` and then `switchport access vlan 30`.

I'll now attempt to ping each of the connected networks. All pings were successful. See Fig. 11.2.

```
C:\>ping 172.17.10.24

Pinging 172.17.10.24 with 32 bytes of data:

Reply from 172.17.10.24: bytes=32 time=12ms TTL=128
Reply from 172.17.10.24: bytes=32 time<1ms TTL=128
Reply from 172.17.10.24: bytes=32 time<1ms TTL=128
Reply from 172.17.10.24: bytes=32 time<1ms TTL=128

Ping statistics for 172.17.10.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

(a) PC1 pinging PC4

```
C:\>ping 172.17.20.25

Pinging 172.17.20.25 with 32 bytes of data:

Reply from 172.17.20.25: bytes=32 time=24ms TTL=128
Reply from 172.17.20.25: bytes=32 time<1ms TTL=128
Reply from 172.17.20.25: bytes=32 time<1ms TTL=128
Reply from 172.17.20.25: bytes=32 time<1ms TTL=128

Ping statistics for 172.17.20.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 24ms, Average = 6ms
```

(b) PC2 pinging PC5

```
C:\>ping 172.17.30.26

Pinging 172.17.30.26 with 32 bytes of data:

Reply from 172.17.30.26: bytes=32 time=2ms TTL=128
Reply from 172.17.30.26: bytes=32 time<1ms TTL=128
Reply from 172.17.30.26: bytes=32 time<1ms TTL=128
Reply from 172.17.30.26: bytes=32 time<1ms TTL=128

Ping statistics for 172.17.30.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

(c) PC3 pinging PC6

Figure 11.2: Network connections are now all successful

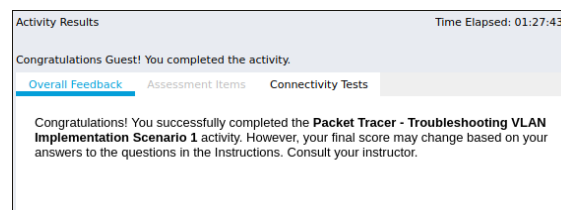


Figure 11.3: Successful Completion of the Activity

Lab 12

Troubleshooting Vlan Scenario 2

March 2, 2020

Packet Tracer Lab 12
Spring 2020

CIT 167
Chaz Davis

troubleshooting

- stuffs

Part 1: Discover and Documentation Issues in the Network

Table 12.1: Documentation

Problems	Solutions
S1 not configured with any vlan	Configure Vlans
S1 Native vlan 56	set Native VLAN 56
S2 g0/1 is an access port not a trunk port	Implement switchport mode trunk command
s3 ports are not assigned to a VLAN	Implement switchport access vlan# command based on the Port assignment table

Lab 13

Configuring Vlans and Trunks

March 4, 2020

Packet Tracer Lab 13
Spring 2020

CIT 167
Chaz Davis

vlans and trunks

- blah blah blah

Part 1: Configuration

I set up the configurations for each pc on the network. I then copied and pasted the commands from the handout for each of the switches. The network is all up and running.

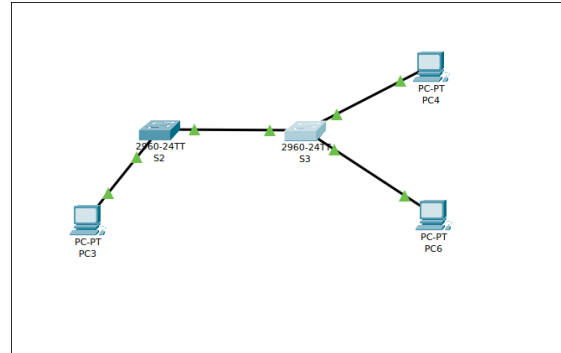


Figure 13.1: The Network Up and Running

Lab 14

Legacy InterVlan Implementation

March 5, 2020

Packet Tracer Lab 14
Spring 2020

CIT 167
Chaz Davis

implement

- vlans
- trunks

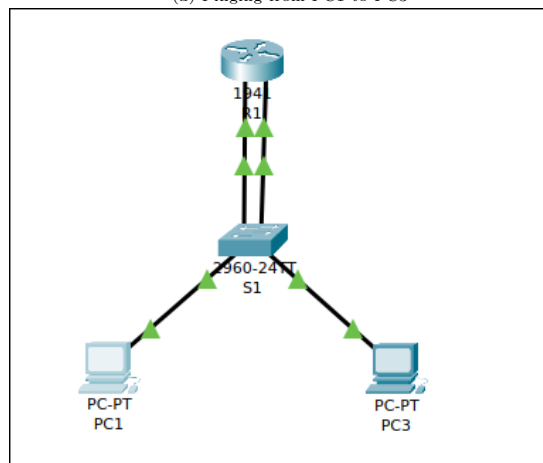
Part 1: Configuring and verifying the network

I setup the Configuration according to the handout. I then, configured the IP address, default gateways, and subnet masks on each of the PCs. I Next ran the commands on R1, and then the commands on S1. I had to go back and run `int g0/1 no shut` on R1.

After that I was able to successfully ping from PC1 to PC3.

```
Pinging 172.17.30.23 with 32 bytes of data:  
  
Request timed out.  
Reply from 172.17.30.23: bytes=32 time<1ms TTL=127  
Reply from 172.17.30.23: bytes=32 time<1ms TTL=127  
Reply from 172.17.30.23: bytes=32 time<1ms TTL=127  
  
Ping statistics for 172.17.30.23:  
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

(a) Pinging from PC1 to PC3



(b) Successful network architecture

Figure 14.1: Successful Lab layout

Lab 15

Router On a Stick

March 8, 2020

Packet Tracer Lab 15
Spring 2020

CIT 167
Chaz Davis

sticks

- N shit

Part 1: Configuring and verifying the Network

I First set up the network according to the diagram. I then, Configured the Ip address, subnet masks, and default gateways for the PCs according the chart. I then, configured the Switch and router according to the handout.

Successfully able to ping PC3 from PC1.

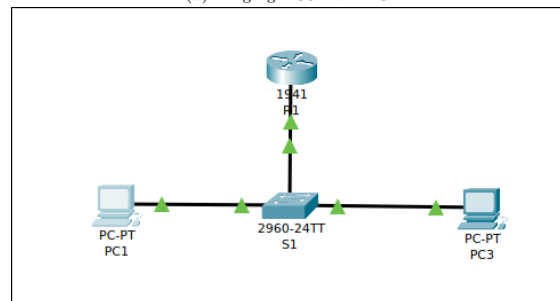
```
C:\>ping 172.17.30.10

Pinging 172.17.30.10 with 32 bytes of data:

Reply from 172.17.30.10: bytes=32 time=1ms TTL=127
Reply from 172.17.30.10: bytes=32 time<1ms TTL=127
Reply from 172.17.30.10: bytes=32 time<1ms TTL=127
Reply from 172.17.30.10: bytes=32 time<1ms TTL=127

Ping statistics for 172.17.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

(a) Pinging PC3 from PC1



(b) Successful Network COnfiguration

Figure 15.1: Successful network setup