1. Familiarization of Network Environment, Understanding and using network utilities: ipconfig, netstat, ping, telnet, ftp, traceroute etc.

1. **ipconfig (Internet Protocol Configuration)** ipconfig is a command-line utility available on Windows systems that displays and manages the IP address configuration of network interfaces. It is commonly used to view the current IP address, subnet mask, and default gateway assigned to the system. Advanced options allow users to release and renew IP addresses via DHCP.

Command Examples:

```
ipconfig           # Shows basic network info
ipconfig /all       # Shows detailed info (MAC address, DNS, DHCP status etc.)
```

2. **ifconfig (Interface Configuration)** ifconfig is the Linux/macOS equivalent of ipconfig. It is used to display, configure, and manage network interfaces. It can show IP addresses, MAC addresses, and allow enabling or disabling of interfaces.

Command Examples:

```
ifconfig            # Show IP and MAC of
interfaces sudo ifconfig eth0 down  # Disable a
network interface
```

3. **ping (Packet Internet Groper)** ping is a diagnostic tool used to test the reachability of a host on an IP network. It sends ICMP echo request packets to the target host and measures the time taken for the responses. It helps determine whether the destination device is online and how fast it responds.

Command Example:

```
ping google.com       # Sends packets to Google's
servers ping 192.168.1.1      # Tests connectivity
with local router
```

4. tracert (Windows) / traceroute (Linux/macOS)

This utility traces the route that packets take to reach a destination host. It lists all the intermediate routers the packet passes through, along with the time taken at each hop. This is useful for identifying network bottlenecks or failures.

Command Example:

```
tracert google.com
```

5. **netstat (Network Statistics)** netstat is a command-line utility that displays active network connections, listening ports, and network protocol statistics. It helps users monitor open connections, detect suspicious activity, and troubleshoot network issues.

Command Examples:

```
netstat             # Shows active connections
netstat -a           # Shows all active ports and listening ports
```

6. **telnet (Teletype Network Protocol)** telnet is a network protocol and command-line tool used to establish a text-based communication session with a remote host using the TCP/IP protocol. It is often used to test connectivity to a specific port (like 80 for HTTP or 25 for SMTP), though it is now mostly replaced by more secure alternatives like SSH.

Command Example:

```
telnet google.com 80   # Test connection to port 80 (HTTP)
```

7. ftp (File Transfer Protocol)

ftp is a standard network protocol used to transfer files between a client and a server over a TCP-based network. The ftp command-line tool allows users to upload and download files, authenticate with remote servers, and navigate remote directories.

Command Example:

```
ftp ftp.example.com
```

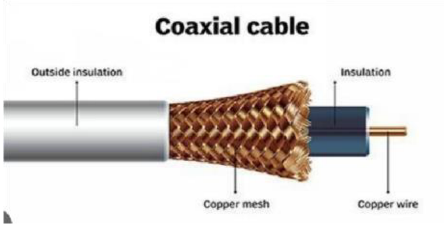
2. Familiarization with Transmission media and tools: Co-axial cable, UTP cable, Crimping tool, Connectors etc. Preparing the UTP cable for cross and direct connection using crimping tool.

1. Coaxial Cable (Co-axial Cable)

A coaxial cable is a type of electrical cable with an inner conductor surrounded by a concentric conducting shield, separated by an insulating layer. It is commonly used for cable television, internet connections, and long-distance communication due to its excellent shielding from electromagnetic interference (EMI).

Use Case: Broadband internet, CCTV, cable TV

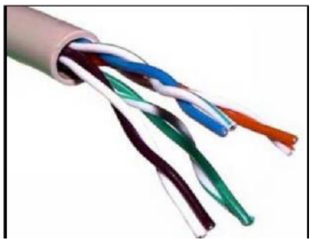
Connector Type: BNC, F-type



2. UTP Cable (Unshielded Twisted Pair)

A UTP cable consists of pairs of insulated copper wires twisted together. It lacks shielding, making it cheaper and more flexible, but more vulnerable to EMI. It is widely used in Ethernet networks and telephone systems. Types: Cat5, Cat5e, Cat6

Max Range (Ethernet): ~100 meters



3. Crimping Tool

A crimping tool is a hand tool used to attach connectors (such as RJ-45) to the ends of UTP cables. It ensures a secure and reliable electrical connection by pressing the connector’s pins into the cable wires.

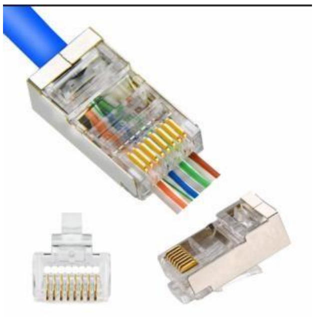
Function: Terminating cables with RJ-45 connectors

4. Connectors (RJ-45)

RJ-45 connectors are modular plugs used to connect UTP cables to networking devices. They have 8 pins that correspond to the 8 wires in a UTP cable. These connectors are crucial in forming both straight-through and crossover cables.

Pin Count: 8P8C (8 Positions, 8 Contacts)

Use: Ethernet, LAN connections



Preparing UTP Cable for Cross and Direct Connection

Straight-through Cable (Direct Connection) Used to connect different types of devices (e.g., PC → Switch, PC → Router).

Wiring Standard:

□ Both ends use same color coding (usually T568B)

T568B Wiring Order:

1. Orange-White
2. Orange
3. Green-White
4. Blue
5. Blue-White
6. Green
7. Brown-White
8. Brown

Crossover Cable (Cross Connection)

Used to connect similar devices (e.g., PC ↔ PC, Switch ↔ Switch). Wiring Standard:

□ One end is T568A, the other is T568B

T568A End:		T568B End:
1. Green-White	↔	Orange-White
2. Green	↔	Orange
3. Orange-White	↔	Green-White
4. Blue	↔	Blue
5. Blue-White	↔	Blue-White
6. Orange	↔	Green
7. Brown-White	↔	Brown-White
8. Brown	↔	Brown

Steps to Crimp a UTP Cable

1. Strip ~1 inch of the cable jacket using the crimping tool.
2. Untwist and align the wires as per the color code (T568A or B).
3. Trim wires evenly using the cutter.
4. Insert wires into the RJ-45 connector — ensure all reach the end.
5. Insert connector into the crimping slot and press hard.
6. Repeat on the other side as per the required cable type (cross/direct).

3. Installation and introduction of simulation tool. (Packet Tracer)

Introduction to Cisco Packet Tracer

Cisco Packet Tracer is a powerful network simulation and visualization tool developed by Cisco Systems. It is widely used in academic environments, particularly in Cisco Networking Academy programs, to provide students and networking professionals with a realistic and interactive platform for designing, configuring, and troubleshooting network topologies without requiring physical networking equipment. Packet Tracer supports a wide range of networking components, including routers, switches, wireless devices, PCs, and IoT devices. It provides both real-time and simulation modes, enabling users to observe packet flow and protocol behavior in detail.

Key Features of Packet Tracer

Feature	**Description**
Device Simulation	Simulates routers, switches, PCs, laptops, servers, firewalls, and IoT devices.
Real-time Mode	Emulates live network behavior for active packet flow and protocol execution.
Simulation Mode	Allows users to step through packet transmission for deeper analysis.
CLI Support	Provides a command-line interface similar to Cisco IOS for configuring devices.
Logical and Physical Views	Users can design topologies logically and visualize physical arrangements.
Multi-User Collaboration	Supports network collaboration in a classroom or remote learning environment.
IoT and Programming	Includes basic IoT device simulation and allows programming using JavaScript or Python.

Importance of Packet Tracer

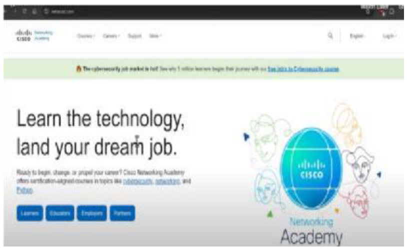
- Enables hands-on learning of networking concepts.
- Eliminates the cost of purchasing physical routers and switches.
- Ideal for practicing CCNA, CCNP, and other networking certifications.
- Facilitates experimentation and troubleshooting in a risk-free environment. □ Supports remote learning, making it accessible to students globally.

Installation Steps for Cisco Packet Tracer

Step-by-Step Installation Process (Windows)

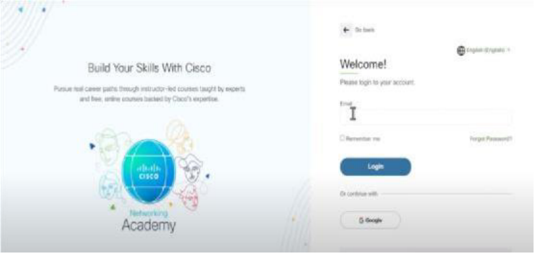
1. Register on Cisco Networking Academy: ○ Visit: https://www.netacad.com ○ Create a free account and enroll in the *Introduction to Packet Tracer* course.
2. Download the Software: ○ After enrollment, navigate to the Packet Tracer download section.
   - ○ Choose the appropriate version for your operating system.
3. Install Packet Tracer: ○ Run the downloaded installer file.
   - ○ Accept the license agreement. ○ Choose the installation directory (default is recommended).
   - ○ Complete the installation process.
4. Launch and Sign In:

- Open Packet Tracer.
- Log in using your Cisco Networking Academy credentials.



Learn the technology, land your dream job.

Ready to begin, change, or propel your career? Cisco Networking Academy offers certification-aligned courses in topics like cybersecurity, networking, and Python.

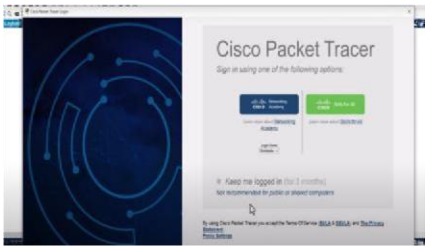


Build Your Skills With Cisco

Pursue real career paths through instructor-led courses taught by experts and free, online courses backed by Cisco's expertise.

Welcome!

Please login to your account.



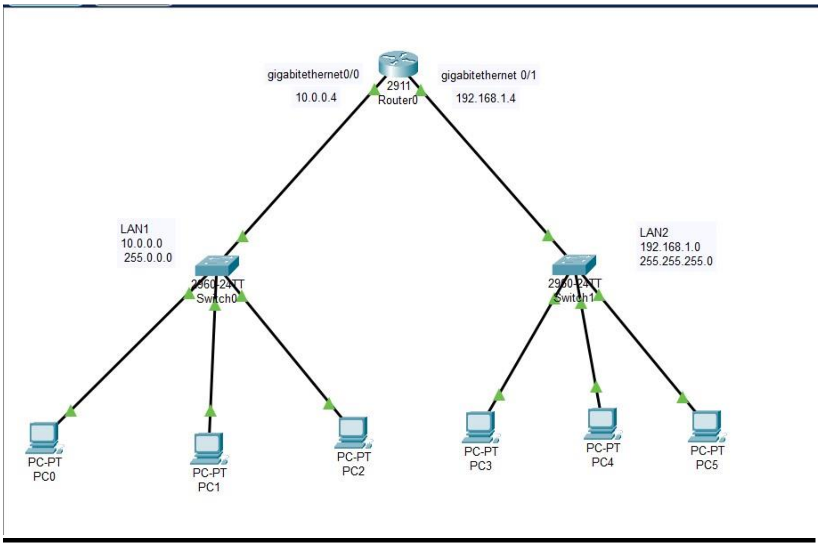
Cisco Packet Tracer

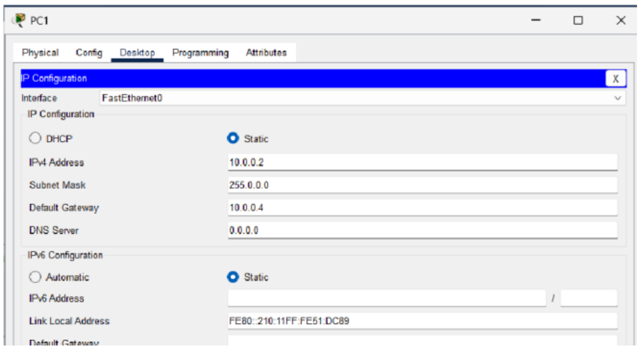
Sign in using one of the following options:

Keep me logged in (for 3 months)

Not recommended for public or shared computers

4. To configure a basic network topology consisting of routers, switches, and end devices such as PCs or laptops. Configure IP addresses and establish connectivity between devices. (Using packet Tracer)





IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 10.0.0.2

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.4

DNS Server: 0.0.0.0

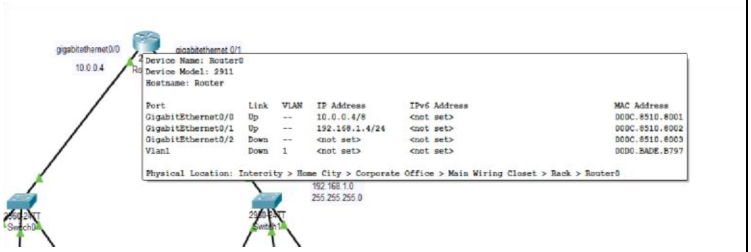
IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::210:11FF:FE51:DC89

Default Gateway



```
Device Name: Router0
Device Model: 2911
Hostname: Router

Port                Link   VLAN   IP Address       IPv6 Address                 MAC Address
GigabitEthernet0/0  Up     --     10.0.0.4/8       <not set>                    000C.8510.8001
GigabitEthernet0/1  Up     --     192.168.1.4/24   <not set>                    000C.8510.8002
GigabitEthernet0/2  Down   --     <not set>        <not set>                    000C.8510.8003
Vlan1               Down   1      <not set>        <not set>                    00D0.BADE.B797

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router0
```

Step 1: Place Devices

- 1 Router (e.g. 2811)
- 2 Switches (e.g. 2960)
- 4 PCs (2 per network, PC0 & PC1 on SW1, PC2 & PC3 on SW2)

Step 2: Connect with Cables
Use copper straight-through cables:

- PC0 → SW1 (any FastEthernet port)
- PC1 → SW1
- PC2 → SW2
- PC3 → SW2
- SW1 → Router (Router's FastEthernet0/0)
- SW2 → Router (Router's FastEthernet0/1)

Use Router interfaces that are FastEthernet (Fa0/0, Fa0/1) or GigabitEthernet depending on router model.

Step 3: Assign IP Addresses
Network 1:

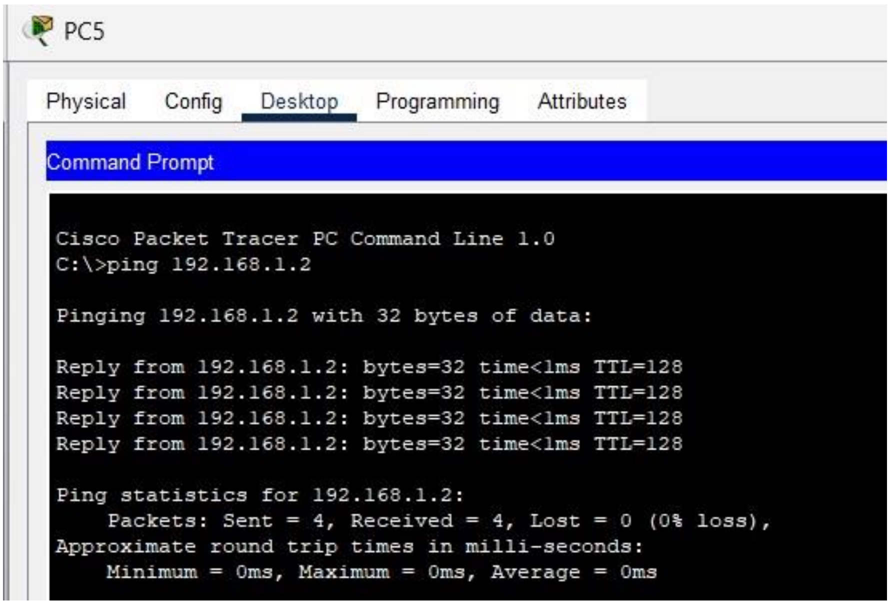
- Router Fa0/0 → 192.168.1.1 /24
- PC0 → 192.168.1.10 /24, Gateway: 192.168.1.1

- PC1 → 192.168.1.11 /24, Gateway: 192.168.1.1 Network 2:
- Router Fa0/1 → 192.168.2.1 /24
- PC2 → 192.168.2.10 /24, Gateway: 192.168.2.1
- PC3 → 192.168.2.11 /24, Gateway: 192.168.2.1

Step 4: Configure Router Interfaces
Click the Router → CLI tab → type the following: enable configure terminal
interface FastEthernet0/0 ip address
192.168.1.1 255.255.255.0
no shutdown interface
FastEthernet0/1 ip address
192.168.2.1 255.255.255.0
no shutdown
exit

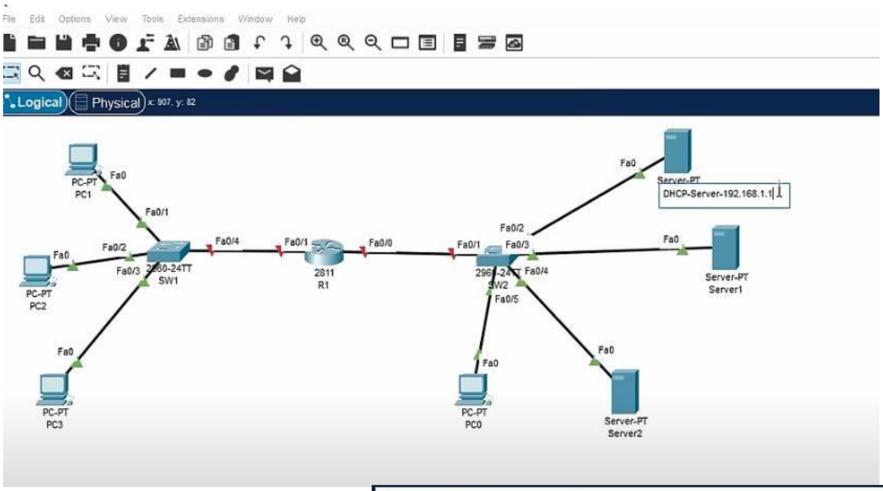
Step 5: Configure PCs
Click on each PC → Desktop tab → IP Configuration: PC0:
IP: 192.168.1.10
Subnet: 255.255.255.0
Gateway: 192.168.1.1
Repeat similar for all PCs using IPs we assigned.

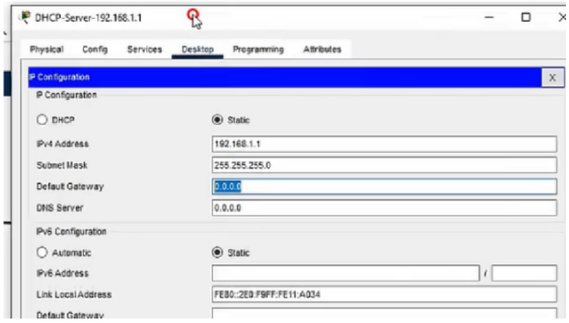
Step 6: Test Connectivity
□ Open PC0 → Desktop → Command Prompt → type:
ping 192.168.1.11 # PC1 (same LAN)
ping 192.168.2.10 # PC2 (other LAN via router)



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

5. To configure a DHCP server on a router or a dedicated DHCP server device. Assign IP addresses dynamically to devices on the network and verify successful address assignment. (Using packet Tracer)





IP Configuration

IP Configuration

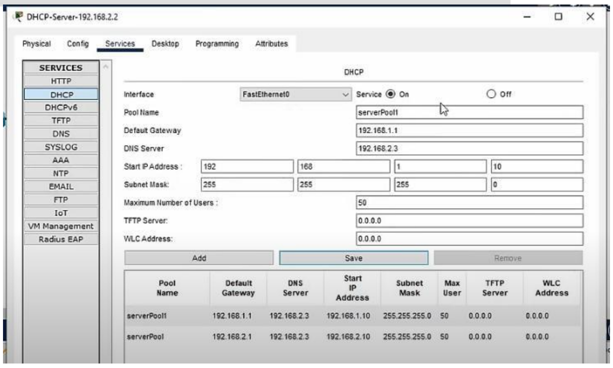
○ DHCP ● Static

IPv4 Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::2E0:F9FF:FE11:A034
Default Gateway	



DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name	serverPool1
Default Gateway	192.168.1.1
DNS Server	192.168.2.3
Start IP Address :	192 . 168 . 1 . 10
Subnet Mask:	255 . 255 . 255 . 0
Maximum Number of Users :	50
TFTP Server:	0.0.0.0
WLC Address:	0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool1	192.168.1.1	192.168.2.3	192.168.1.10	255.255.255.0	50	0.0.0.0	0.0.0.0
serverPool	192.168.2.1	192.168.2.3	192.168.2.10	255.255.255.0	50	0.0.0.0	0.0.0.0

Step 1: Connect devices

- Use **straight-through cables**:

  ○ PC0, PC1, PC2 → Switch ○

  Switch → Router’s FastEthernet0/0

Step 2: Decide IP Pool

Let’s say we want to assign:

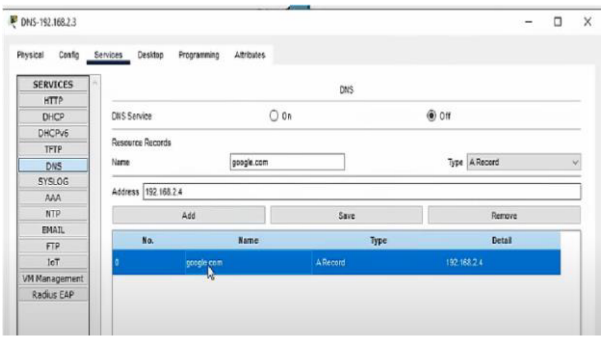
- **Network**: 192.168.10.0/24

 Gateway (router): 192.168.10.1 **IP Pool Range**: 192.168.10.100 to 192.168.10.200 **Step 3: Configure Router as DHCP Server**

Click Router → CLI tab : `enable`

```
configure terminal


! Set up the DHCP pool ip
dhcp pool AyushNet
 network 192.168.10.0 255.255.255.0
default-router 192.168.10.1  dns-
server 8.8.8.8
```

```
! Exclude some addresses (like gateway, servers, etc.) ip
dhcp excluded-address 192.168.10.1 192.168.10.99

! Assign IP to router interface (gateway) interface
FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
no shutdown exit
```



DNS

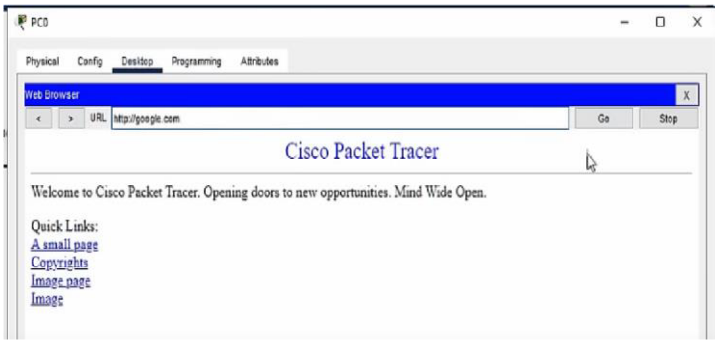
DNS Service ○ On ● Off

Resource Records

Name: google.com　Type: A Record

Address: 192.168.2.4

No.	Name	Type	Detail
0	google.com	A Record	192.168.2.4



URL: http://google.com

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Step 4: Configure PCs for DHCP

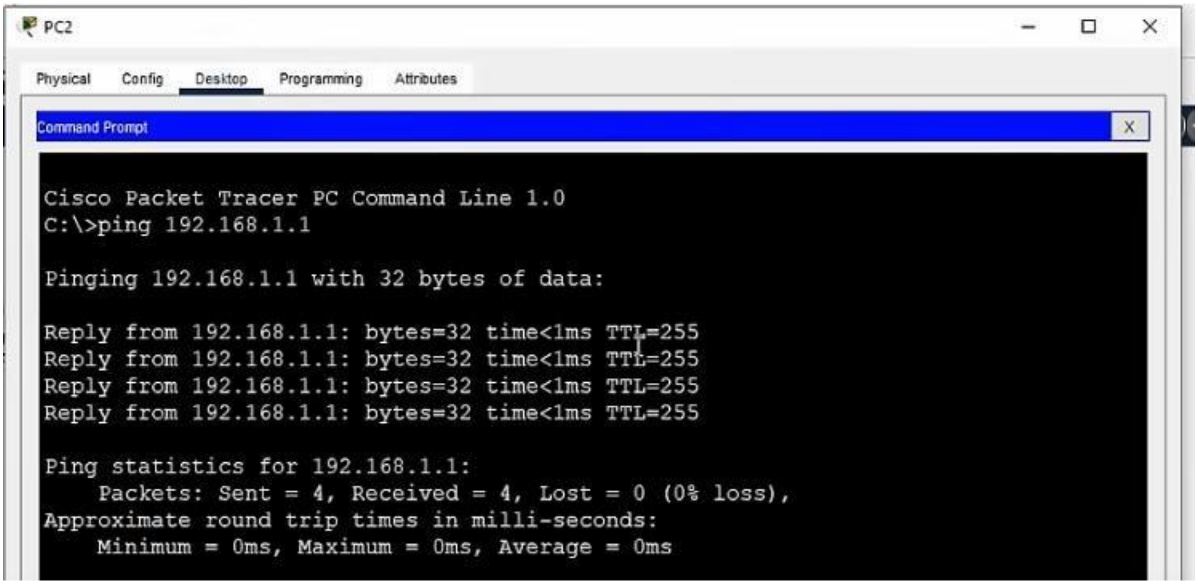
Click PC0 → Desktop → **IP Configuration** → choose

DHCP Do the same for PC1, PC2, etc.

Step 5: Verify

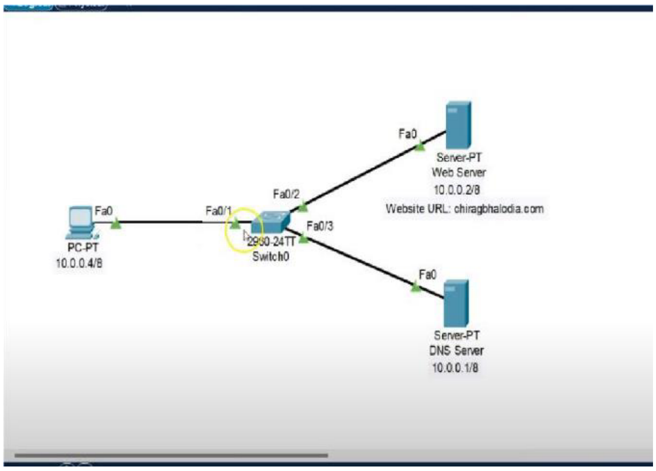
On each PC, after clicking DHCP:

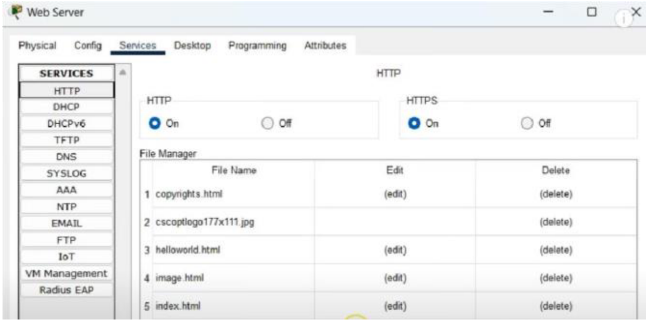
- It should auto-fill with an IP like 192.168.10.100+
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.10.1 Now test it: ping 192.168.10.1 # router ping 192.168.10.101 # other PC



```
Cisco 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 = 0ms, Average = 0ms
```

6. To configure a local DNS server to resolve domain names within a network. (Using packet Tracer)





HTTP

HTTP ● On ○ Off

HTTPS ● On ○ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

Step 1: Connections

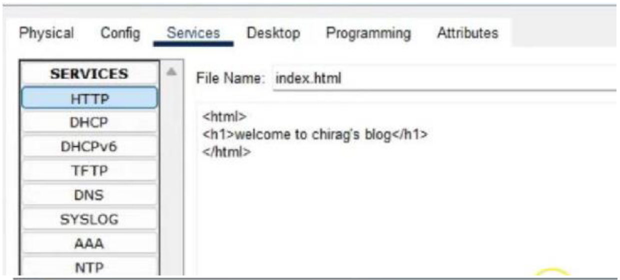
Use **straight-through cables**:

- PC0, PC1 → Switch
- DNS Server → Switch
- Switch → Router (Fa0/0)

Step 2: Assign Static IPs

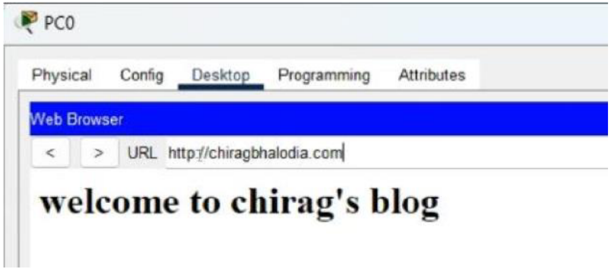
Use the **192.168.10.0/24** network:

Device	**IP Address**	**Notes**
Router (Fa0/0)	192.168.10.1	Default Gateway
DNS Server	192.168.10.2	DNS service runs here
PC0	DHCP or Static	Gets DNS from config
PC1	Same as PC0	



File Name: index.html

```
<html>
<h1>welcome to chirag's blog</h1>
</html>
```



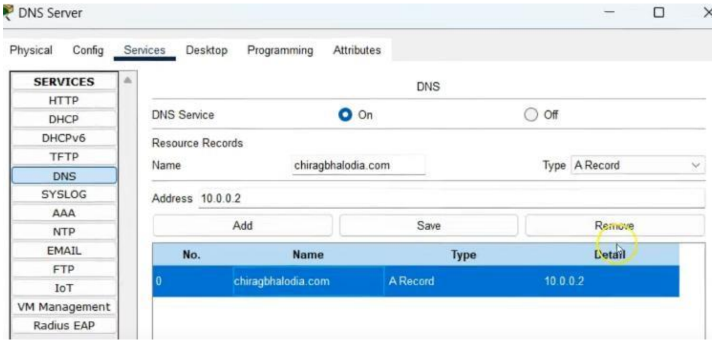
URL http://chiragbhalodia.com

welcome to chirag's blog

Step 3: Configure the DNS Server
Click the Server → **Config tab** → Set static IP (as above)
Then:

- Go to **Services tab** → Select **DNS**
- Turn DNS service **ON**
- Add DNS records (name-to-IP mappings):

Name	**Address**
ayushgod.local	192.168.10.100
packettracer.local	192.168.10.101



DNS Service ● On ○ Off

Resource Records

Name chiragbhalodia.com Type A Record

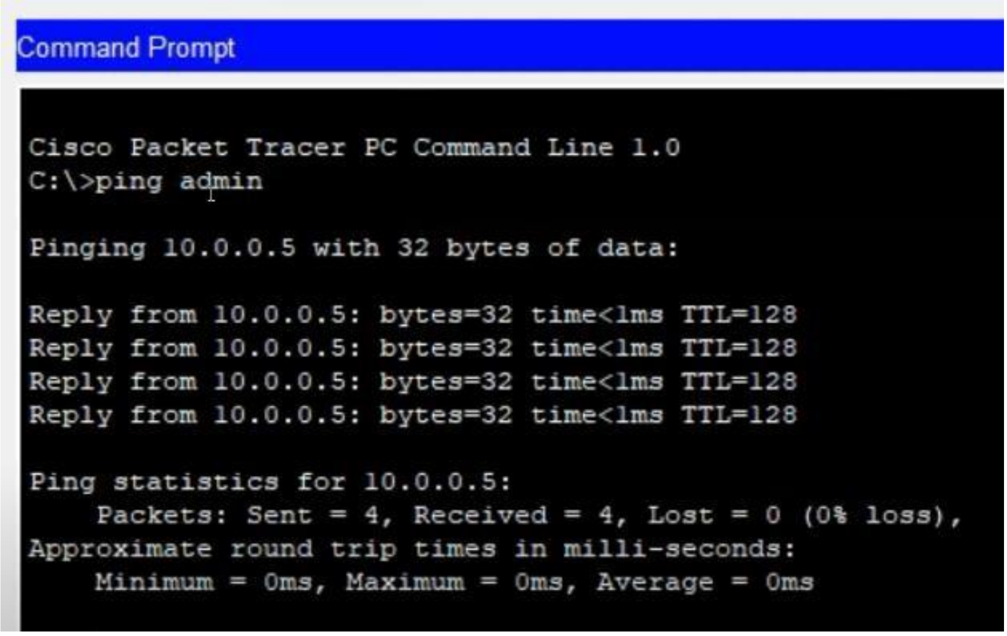
Address 10.0.0.2

No.	Name	Type	Detail
0	chiragbhalodia.com	A Record	10.0.0.2

Step 4: Configure PC to Use the DNS Server
Click PC0 → Desktop → IP Configuration:
IP Address: 192.168.10.10
Subnet Mask: 255.255.255.0
Gateway: 192.168.10.1
DNS Server: 192.168.10.2
(Repeat for PC1 or use DHCP)

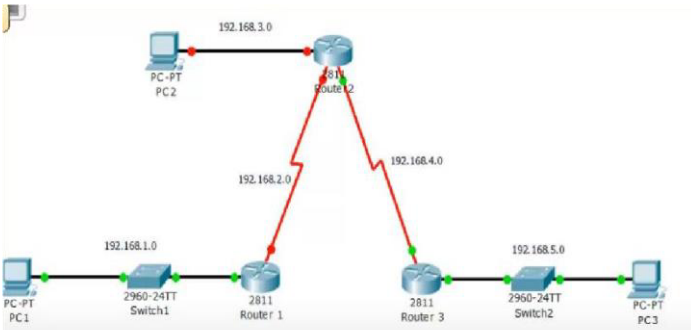
Step 5: Test DNS Resolution

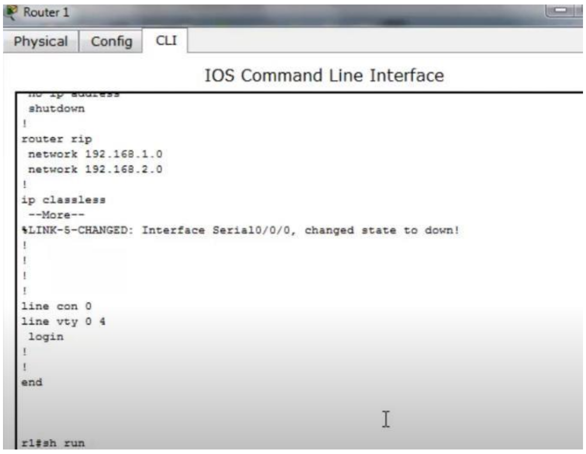
Open PC0 → Desktop → Command Prompt:
ping ayushgod.local



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

Pinging 10.0.0.5 with 32 bytes of data:

Reply from 10.0.0.5: bytes=32 time<1ms TTL=128
Reply from 10.0.0.5: bytes=32 time<1ms TTL=128
Reply from 10.0.0.5: bytes=32 time<1ms TTL=128
Reply from 10.0.0.5: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

7. Network Troubleshooting: Simulate network issues such as connectivity problems, incorrect configurations, or routing failures. Use Packet Tracer's simulation mode to diagnose and troubleshoot the network.





```
 no ip address
 shutdown
!
router rip
 network 192.168.1.0
 network 192.168.2.0
!
ip classless
 --More--
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down!
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end


r1#sh run
```

Step 1: Inject Some Mistakes

Let's deliberately break some stuff:

Issue Type	Problem Introduced
IP Misconfig	Set wrong IP on PC1 (192.168.30.10)
Wrong Gateway	Set PC0's gateway to 192.168.10.254
Cable Cut	Disconnect Fa0/1 to LAN2
Interface Shutdown	shutdown Fa0/0 on router
Routing Failure	No routes configured on multi-router setup

Step 2: Simulation Mode to Sniff Packets

How to Use:

1. Click Simulation Mode (bottom right in Packet Tracer).
2. Click Add Simple PDU (lightning bolt with a +).
3. Click PC0 → PC1.
4. See the packet move hop-by-hop.
5. When it fails — click the red X → analyze the problem in the Event List.

Common Diagnoses & Fixes:

Issue #1: PC IP Misconfig

Symptom: PC1 not pingable, can't reach network.

Fix:

- Click PC1 → Desktop → IP Config → Fix IP:

IP Address: 192.168.20.10
Subnet: 255.255.255.0
Gateway: 192.168.20.1

Issue #2: Wrong Gateway on PC0

Symptom: PC0 can't reach PC1 even though IP is correct.

Fix:

- Set correct gateway:

Gateway: 192.168.10.1

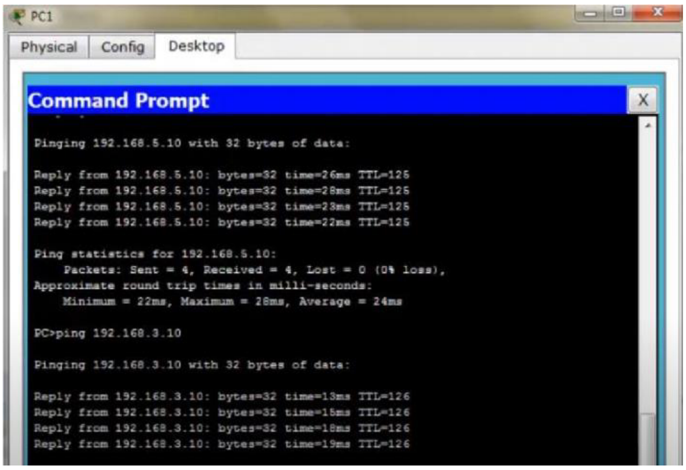
Issue #3: Cable unplugged / Interface Down
Symptom: Link light is red or off, packet dies at router.
Fix:

- Check physical connections.
- On Router CLI: enable configure terminal interface FastEthernet0/1 no shutdown

Issue #4: No Routing Between
Networks If you're using 2 routers, you
need routing. Static Routing Fix:
RouterA(config)# ip route 192.168.20.0 255.255.255.0 [next-hop]
RouterB(config)# ip route 192.168.10.0 255.255.255.0 [next-hop]

Step 3: Verify Fix
After each fix:

- Go back to Simulation Mode
- Re-send PDU
- Make sure the packet reaches the destination
- Green ✓ means success



```
Pinging 192.168.5.10 with 32 bytes of data:

Reply from 192.168.5.10: bytes=32 time=26ms TTL=125
Reply from 192.168.5.10: bytes=32 time=28ms TTL=125
Reply from 192.168.5.10: bytes=32 time=23ms TTL=125
Reply from 192.168.5.10: bytes=32 time=22ms TTL=125

Ping statistics for 192.168.5.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 28ms, Average = 24ms

PC>ping 192.168.3.10

Pinging 192.168.3.10 with 32 bytes of data:

Reply from 192.168.3.10: bytes=32 time=13ms TTL=126
Reply from 192.168.3.10: bytes=32 time=15ms TTL=126
Reply from 192.168.3.10: bytes=32 time=18ms TTL=126
Reply from 192.168.3.10: bytes=32 time=19ms TTL=126
```

8. NAT (Network Address Translation): Set up NAT on a router to translate private IP addresses to public IP addresses for outbound internet connectivity. Test the translation and examine how NAT helps conserve IPv4 address space. (Using packet Tracer)

Objective:

- Set up NAT on a router to translate private IPs to public IPs.
- Test the translation using ping.
- Understand how NAT helps conserve IPv4 addresses.

Step 1: Create Topology

1. **Place devices**: 2 PCs, 1 Router (NAT), 1 Server (simulating public server), 1 Cloud (optional).
2. **Connect using copper cables**:
   - PC0 & PC1 → Router (FastEthernet0/0)
   - Router (Serial or FastEthernet0/1) → Server0 or ISP Router

Step 2: Assign IP Addresses

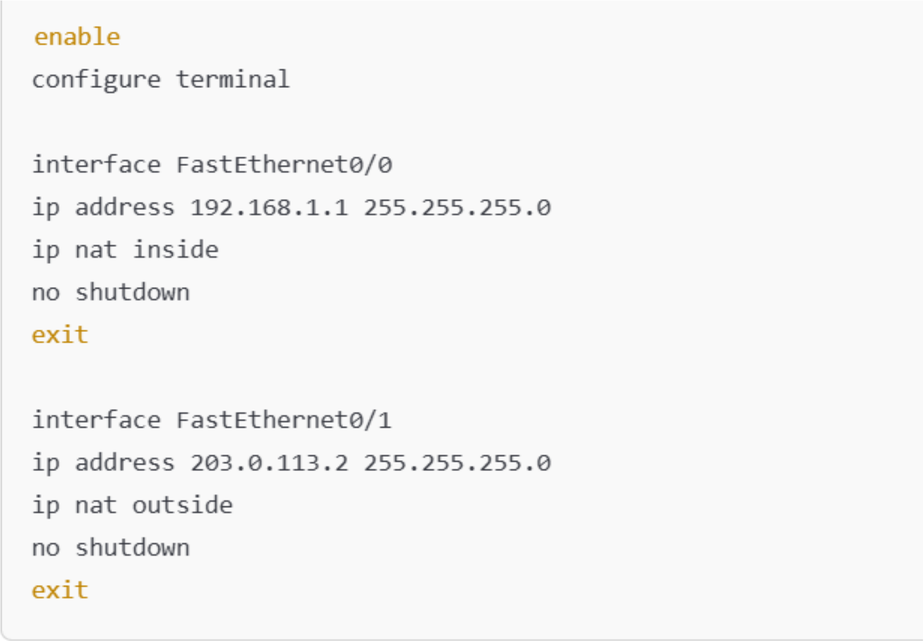
Step 3: Configure IPs

PCs:

- On each PC > Desktop > IP Configuration

Router

Enter CLI and run:



```
enable
configure terminal

interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
no shutdown
exit

interface FastEthernet0/1
ip address 203.0.113.2 255.255.255.0
ip nat outside
no shutdown
exit
```

Step 4: Configure NAT

```
access-list 1 permit 192.168.1.0 0.0.0.255

ip nat inside source list 1 interface FastEthernet0/1 overload
```

Step 5: Configure Routing

```
ip route 0.0.0.0 0.0.0.0 203.0.113.1  ! Assuming 203.0.113.1 is the ISP or next  hop
```

Step 6: Test NAT

1. From PC0/PC1, go to **Command Prompt** > ping 203.0.113.3 (Server).
2. You should receive replies.

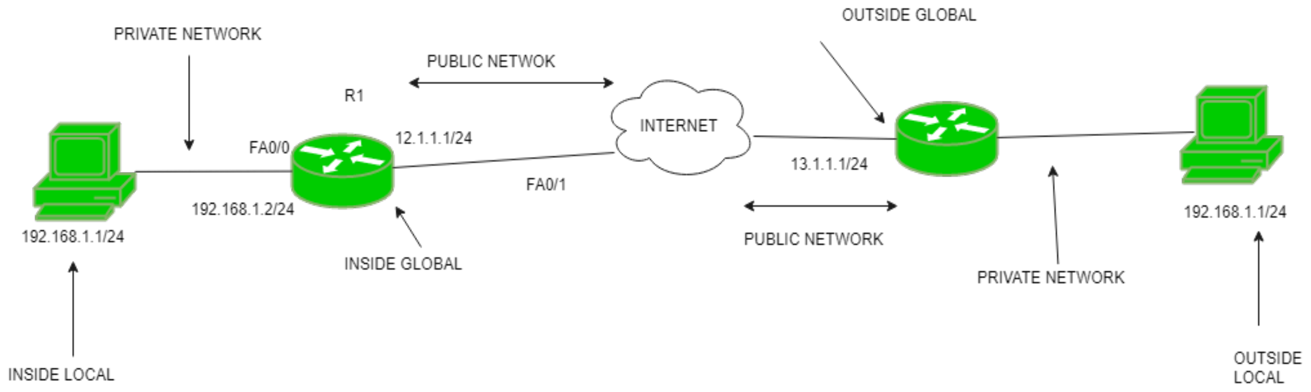
Step 7: View NAT Translations

On Router CLI:

```
show ip nat translations
```

You’ll see mappings like:

```
Inside global: 203.0.113.2   Inside local: 192.168.1.10
```



OUTSIDE GLOBAL
PRIVATE NETWORK
PUBLIC NETWOK
R1
FA0/0
12.1.1.1/24
INTERNET
13.1.1.1/24
192.168.1.2/24
FA0/1
192.168.1.1/24
192.168.1.1/24
PUBLIC NETWORK
INSIDE GLOBAL
PRIVATE NETWORK
INSIDE LOCAL
OUTSIDE
LOCAL