

# Key features

## 1. Router:

connects different networks such as LAN to the internet or to other LANs

## 2. Dynamic Host Configuration Protocol (DHCP):

automatically assigns IP addresses and other network settings to devices on a network

## 3. Domain Name System (DNS):

this resolves domain name into IP addresses so that devices can locate and communicate with websites and services on the internet or internal networks.

## 4. Access Control List (ACLs):

this controls what traffic is allowed or denied on a network by matching specific conditions, helping to enforce security and traffic control.

# Devices and Configurations

## Key Devices

### . Router:

Routes data and manage traffic between different networks

### . Switches:

Connects devices within the same network

### . Servers:

Serve DHCP, DNS and Web application services

### . Endpoint Devices:

PCs and laptop

## Configuration Steps

### 1. Setup the Topology:

- Arrange and connect router, switches and end devices.

### 2. Configure Devices:

- Assign static IP addresses to DHCP,DNS and web servers, also create gateway for each interface.

Devices	IP address
Gateway 1	192.168.1.1
Gateway 2	192.168.2.1
DHCP server	192.168.2.2
DNS server	192.168.2.3
Web server	192.168.2.4

### 3. Configure DHCP Servers:

- Define DHCP pools and scopes for each subnet.
- Bind interfaces to their respective pools.
- Enable DHCP server to assign IP addresses to end devices starting from 10.
- DHCP assigned the following IP addresses to the laptops and PC

Device	IP address
Developer's PC	192.168.1.10
Database Admin's PC	192.168.1.11
Engineer's PC	192.168.1.12

### 4. Apply ACLs:

- Define access rules to permit/deny traffic as required
- Apply rules to the appropriate interfaces.

Step 1: Enter Router CLI

enable

configure terminal

Step 2: Create ACL Using host

access-list 100 permit tcp host 192.168.1.25 host 192.168.2.4 eq 80

```
access-list 100 deny tcp any host 192.168.2.4 eq 80
access-list 100 permit ip any any
```

Step 3: Apply the ACL to the Correct Interface  
interface Fa0/1  
ip access-group 100 out  
exit

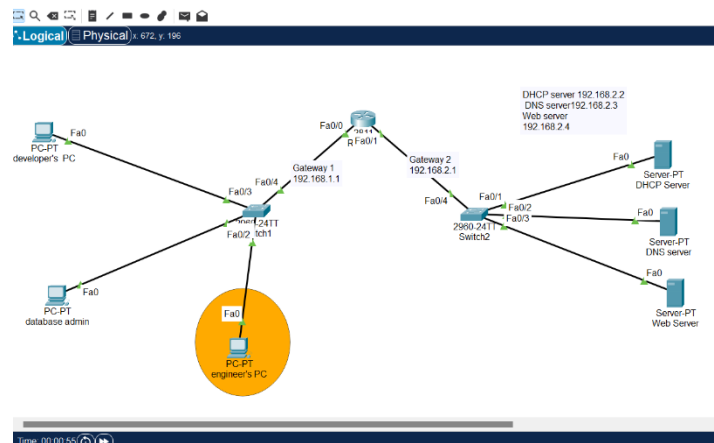
## 5. Test Connectivity:

- Test in web browser:

Device	Action	Result
Laptop0	Visit http:192.168.2.4	Allowed
Other PCs	Visit http:192.168.2.4	Blocked

Attached below are pictures of each step in the network segmentation.

Step 1: setting and connecting devices



DHCP Server

Physical Config Services Desktop Programming Attributes

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.2.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server 192.168.2.3

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80:201:84FF-FEB3:9144

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

DNS server

Physical Config Services Desktop Programming Attributes

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.2.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server 192.168.2.3

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80:209:7CFF-FE78:3522

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

Web Server

Physical Config Services Desktop Programming Attributes

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.2.4

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server 192.168.2.3

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80:20C:CFFF-FED3:5B7B

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

Step 2: setting static IP addresses for DHCP, DNS and Web server

Step 3: setting up server pool for each gateway and starting IP address

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	255.255.255.246	246	0.0.0.0	0.0.0.0
serverPool	192.168.2.1	192.168.2.3	192.168.2.10	255.255.255.246	246	0.0.0.0	0.0.0.0

Result: Engineer's laptop is allowed to access web server while the other PCs are blocked from accessing web server.

engineer's PC

Physical Config **Desktop** Programming Attributes

Web Browser

< > URL: http://192.168.2.4 Go Stop

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](#)

database admin

physical Config Desktop Programming Attributes

Web Browser

< > URL http://192.168.2.4 Go Stop

Request Timeout