Kingdom of Saudi Arabia
Qassim University
College of Computer

المملكة العربية السعودية
جامعة القصيم
كية الحاسب

COMPUTER NETWORKS

COE 351 PROJECT

Students:

- Ragheed Almasry - 412117664
- Abdullah Alshami - 412117701
- Anas Alarbeed - 411116054
- Kareem Majed - 412117553
- Suliman Alfawzan - 412111550

Supervisor:
Dr.Jamal Alotaibi

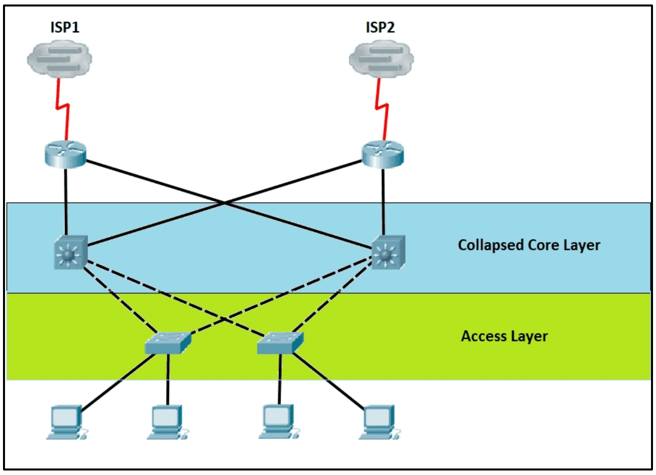
Table of Contents

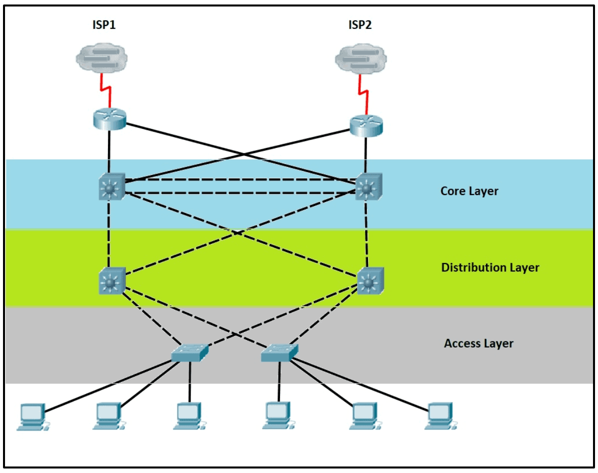
Network Topology

Collapsed Core Architecture

Collapsed Core Architecture is a campus network design wherein we combine the core and distribution layers. We do not use a separate set of core switches in addition to the distribution switches. The core and distribution functions are implemented by a single device.

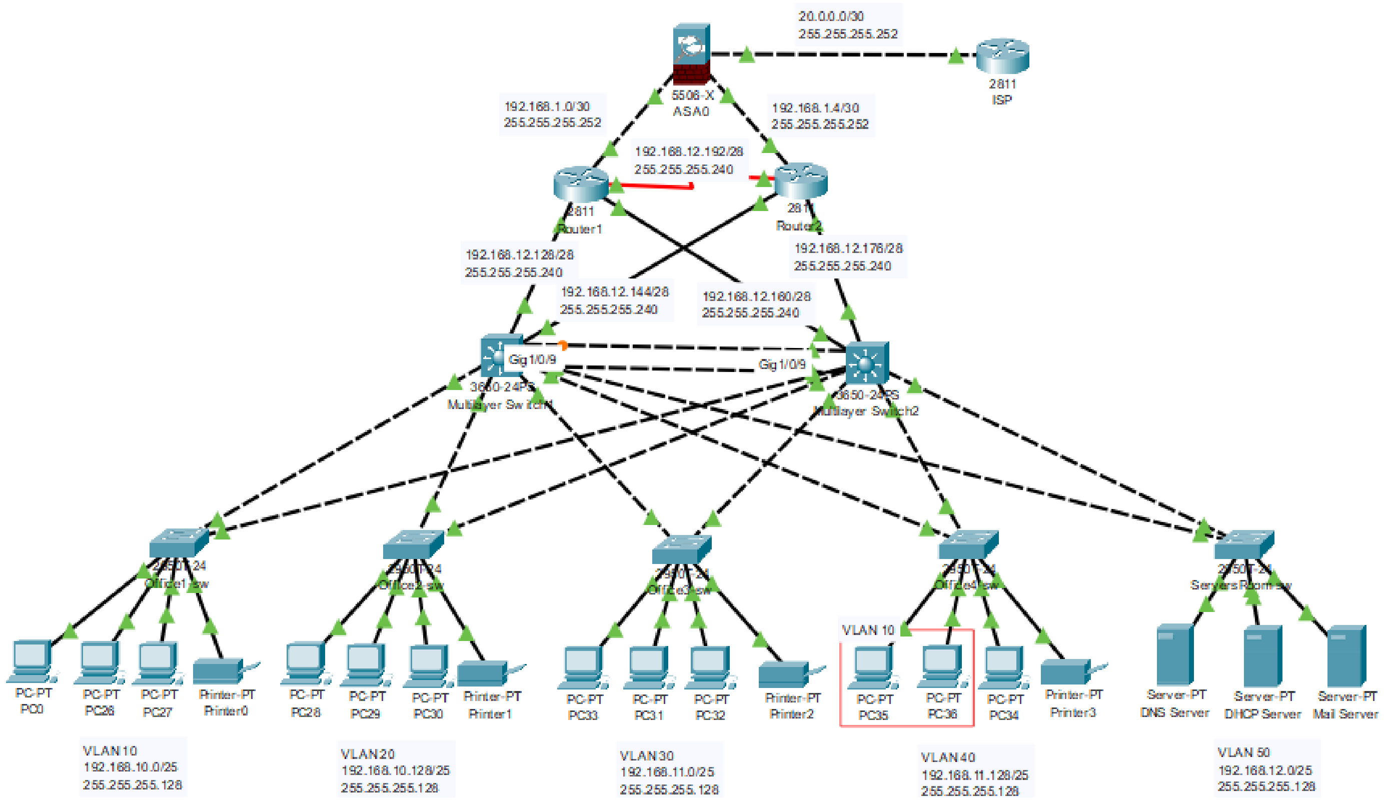
Core layers are responsible for forwarding large amounts of packets both reliably and quickly. The distribution layer, on the other hand, is routing and filtering, and the communication point between the access layer and the core. This design is often deployed in small and medium campus networks.





Collapsed Core (2 Tier Architecture)	**3 Tier Architecture**
2 Layers	3 Layers
Core and Distribution functions combined	Core and Distribution layers are separated
Small and medium sized networks	Large campus networks
Less cost	More expensive
Lacks redundancy	More fault tolerance
Less resiliency	More resilient
Simplified design	More complex design and requires more technical skills to maintain

- So we’ve designed our LAN network topology in packet tracer as Collapsed Core Architecture.



Network components:

- 12 PC
- 4 Printers
- 5 Switches
- 2 Multilayer Switches
- 2 Routers
- One DHCP Server
- One DNS Server
- One Mail Server
- One Firewall Server

IP Addresses and Subnetting

- IP address: 32-bit identifier associated with each host or router *interface*.
- interface: Connection between host/router and physical link.
- Subnet: device interfaces that can physically reach each other without passing through an intervening router.
  - each isolated network is called a *subnet*

- CIDR: Classless Inter Domain Routing (pronounced "cider").
  - subnet portion of address of arbitrary length.
  - address format: a.b.c.d/x, where x is # bits in subnet portion of address.

IP Addresses and Subnetting Table:

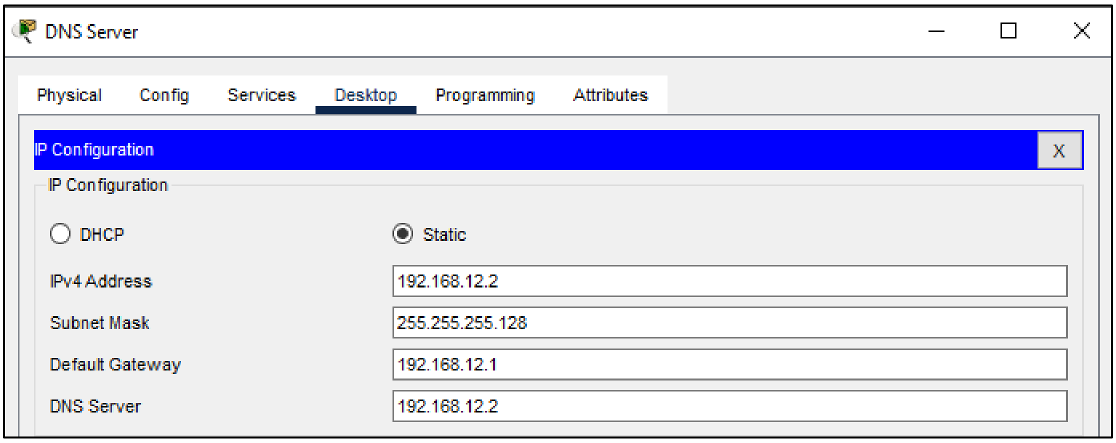
Net: 192.168.0.0						
Subnet	CIDR notation	Subnet mask	Wildcard mask	No. of hosts	No. of usable hosts	VLAN
192.168.1.0	30	255.255.255.252	0.0.0.3	4	2	-
192.168.1.4	30	255.255.255.252	0.0.0.3	4	2	-
192.168.10.0	25	255.255.255.128	0.0.0.127	128	126	10
192.168.10.128	25	255.255.255.128	0.0.0.127	128	126	20
192.168.11.0	25	255.255.255.128	0.0.0.127	128	126	30
192.168.11.128	25	255.255.255.128	0.0.0.127	128	126	40
192.168.12.0	25	255.255.255.128	0.0.0.127	128	126	50
192.168.12.128	28	255.255.255.240	0.0.0.15	16	14	-
192.168.12.144	28	255.255.255.240	0.0.0.15	16	14	-
192.168.12.160	28	255.255.255.240	0.0.0.15	16	14	-
192.168.12.176	28	255.255.255.240	0.0.0.15	16	14	-
192.168.12.192	28	255.255.255.240	0.0.0.15	16	14	-

DNS and DHCP Configurations

▪ Domain Name System (DNS):

Distributed database implemented in hierarchy of many name servers. It's an application-layer protocol Hosts, DNS servers communicate to resolve names (address/name translation).

Static IP configuration:



DNS Server

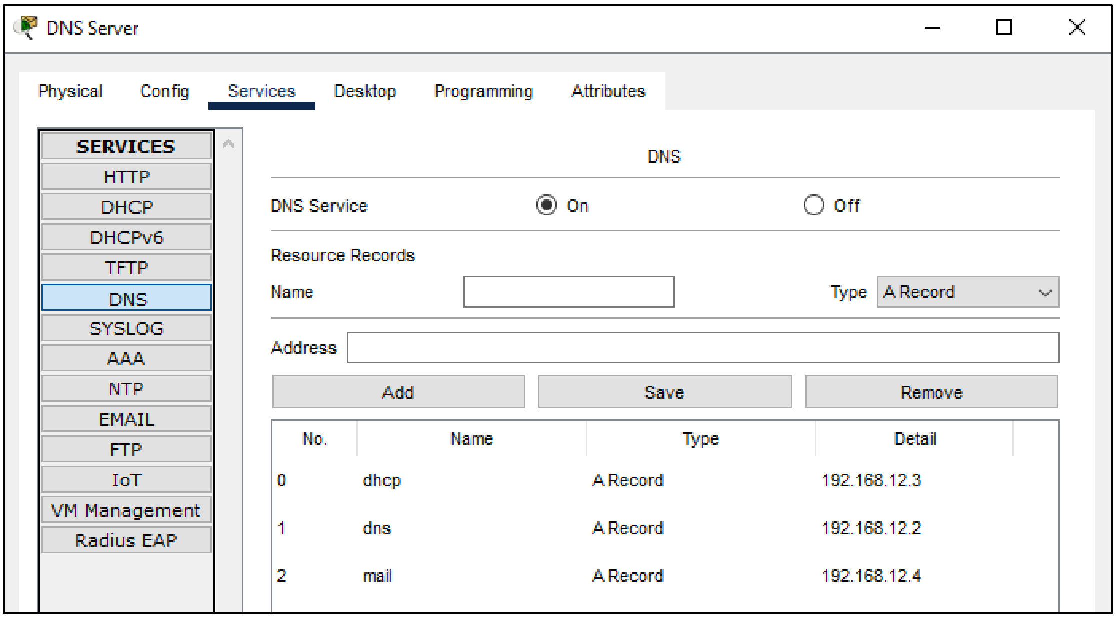
IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.12.2
Subnet Mask	255.255.255.128
Default Gateway	192.168.12.1
DNS Server	192.168.12.2

DNS Service configuration:



DNS Server

DNS

DNS Service ● On ○ Off

Resource Records

Name: Type: A Record

Address:

No.	Name	Type	Detail
0	dhcp	A Record	192.168.12.3
1	dns	A Record	192.168.12.2
2	mail	A Record	192.168.12.4

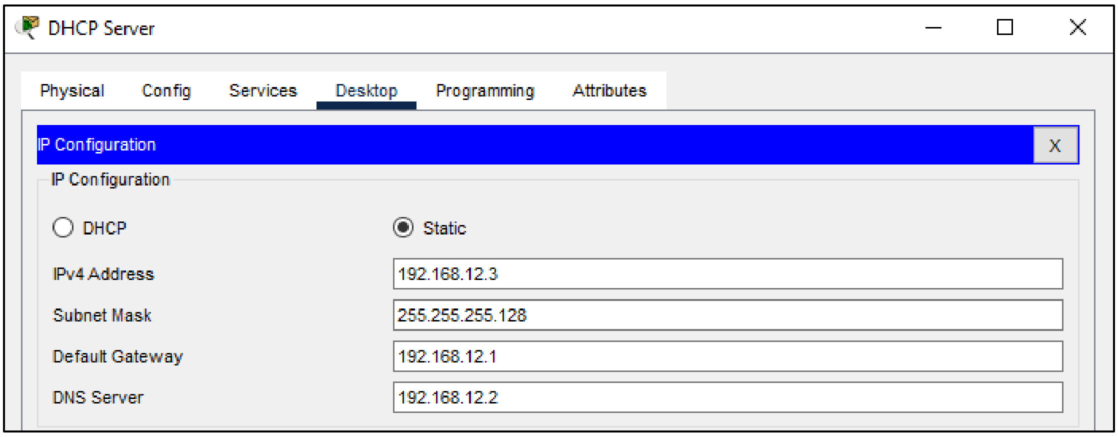
- **Dynamic Host Configuration Protocol (DHCP):**

is a network server that automatically provides and assigns IP addresses to devices on the network. DHCP is a standardized networking protocol used on IP networks to simplify the process of configuring devices with a valid IP address and other parameters such as the default gateway and DNS servers.

DHCP overview:

host broadcasts DHCP discover msg [optional].
DHCP server responds with DHCP offer msg [optional].
host requests IP address: DHCP request msg.
DHCP server sends address: DHCP ack msg.

Static IP configuration:

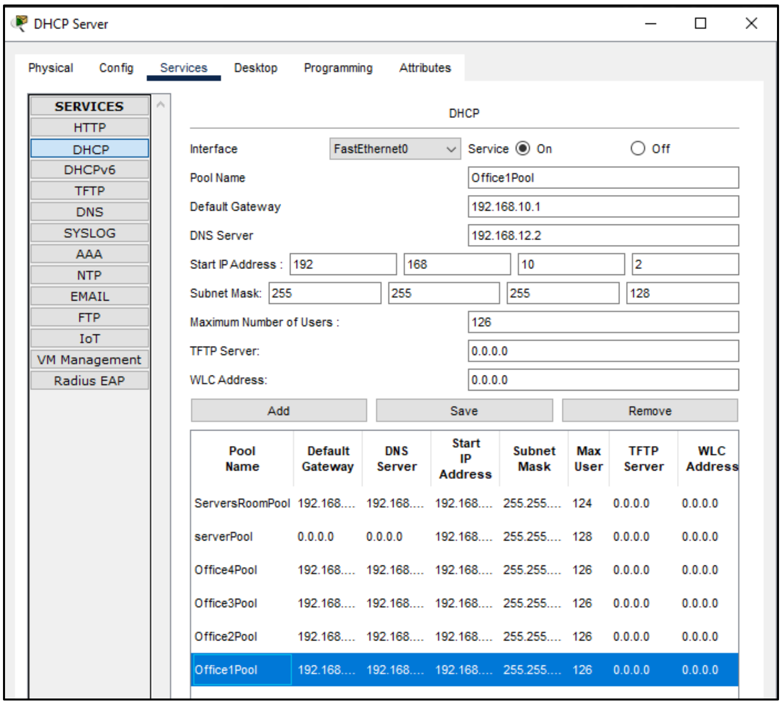


IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.12.3
Subnet Mask	255.255.255.128
Default Gateway	192.168.12.1
DNS Server	192.168.12.2

DHCP service configuration:



Interface: FastEthernet0 Service ● On ○ Off

Pool Name	Office1Pool
Default Gateway	192.168.10.1
DNS Server	192.168.12.2
Start IP Address :	192 168 10 2
Subnet Mask:	255 255 255 128
Maximum Number of Users :	126
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
ServersRoomPool	192.168....	192.168....	192.168....	255.255....	124	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168....	255.255....	128	0.0.0.0	0.0.0.0
Office4Pool	192.168....	192.168....	192.168....	255.255....	126	0.0.0.0	0.0.0.0
Office3Pool	192.168....	192.168....	192.168....	255.255....	126	0.0.0.0	0.0.0.0
Office2Pool	192.168....	192.168....	192.168....	255.255....	126	0.0.0.0	0.0.0.0
Office1Pool	192.168....	192.168....	192.168....	255.255....	126	0.0.0.0	0.0.0.0

Switches & VLANs Configuration

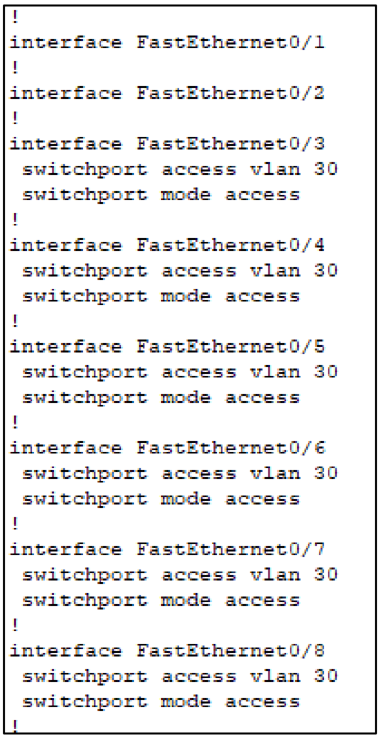
Switch: It's a link-layer device takes an active role store, forward Ethernet frames.
examine incoming frame's MAC address, selectively forward frame to one-or-more outgoing links when frame is to be forwarded on segment, uses CSMA/CD to access segment.

Virtual Local Area Network (VLAN): Switch(es) supporting VLAN capabilities can be configured to define multiple virtual LANS over single physical LAN infrastructure.

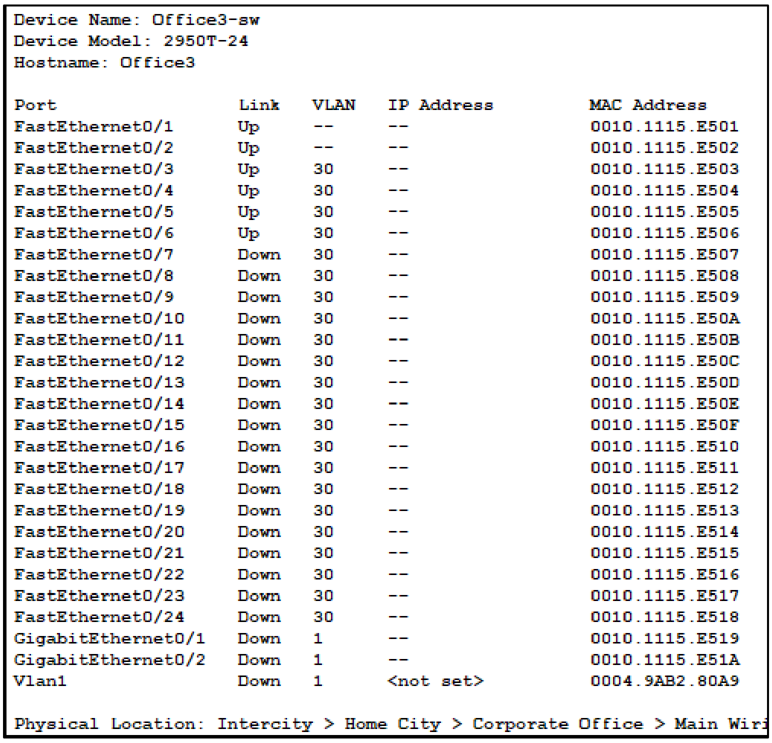
port-based VLAN: Switch ports grouped so that *single* physical switch operates as multiple virtual switches.

To set the VLANs to switches we did the following:

Switch 3 for example:



```
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
!
```



```
Device Name: Office3-sw
Device Model: 2950T-24
Hostname: Office3

Port                Link   VLAN   IP Address         MAC Address
FastEthernet0/1     Up     --     --                 0010.1115.E501
FastEthernet0/2     Up     --     --                 0010.1115.E502
FastEthernet0/3     Up     30     --                 0010.1115.E503
FastEthernet0/4     Up     30     --                 0010.1115.E504
FastEthernet0/5     Up     30     --                 0010.1115.E505
FastEthernet0/6     Up     30     --                 0010.1115.E506
FastEthernet0/7     Down   30     --                 0010.1115.E507
FastEthernet0/8     Down   30     --                 0010.1115.E508
FastEthernet0/9     Down   30     --                 0010.1115.E509
FastEthernet0/10    Down   30     --                 0010.1115.E50A
FastEthernet0/11    Down   30     --                 0010.1115.E50B
FastEthernet0/12    Down   30     --                 0010.1115.E50C
FastEthernet0/13    Down   30     --                 0010.1115.E50D
FastEthernet0/14    Down   30     --                 0010.1115.E50E
FastEthernet0/15    Down   30     --                 0010.1115.E50F
FastEthernet0/16    Down   30     --                 0010.1115.E510
FastEthernet0/17    Down   30     --                 0010.1115.E511
FastEthernet0/18    Down   30     --                 0010.1115.E512
FastEthernet0/19    Down   30     --                 0010.1115.E513
FastEthernet0/20    Down   30     --                 0010.1115.E514
FastEthernet0/21    Down   30     --                 0010.1115.E515
FastEthernet0/22    Down   30     --                 0010.1115.E516
FastEthernet0/23    Down   30     --                 0010.1115.E517
FastEthernet0/24    Down   30     --                 0010.1115.E518
GigabitEthernet0/1  Down   1      --                 0010.1115.E519
GigabitEthernet0/2  Down   1      --                 0010.1115.E51A
Vlan1               Down   1      <not set>          0004.9AB2.80A9

Physical Location: Intercity > Home City > Corporate Office > Main Wiri
```

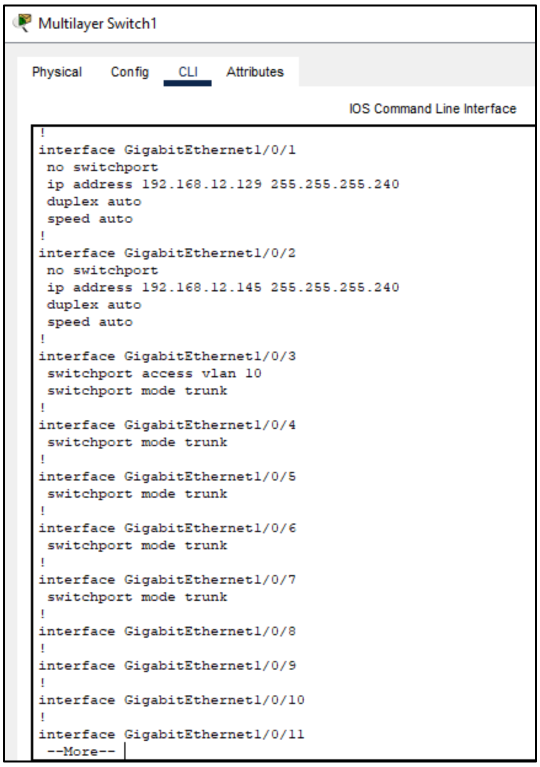
The rest of switches is exactly the same except the number of VLAN of each.

Multilayer Switch

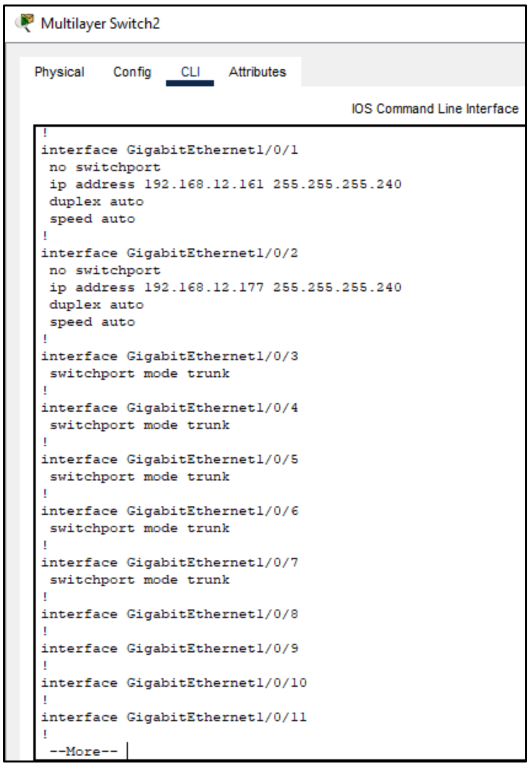
Multilayer Switch: It’s a network switch that operates at both Layer 2 (Data Link Layer) and Layer 3 (Network Layer). Unlike traditional switches that primarily operate at Layer 2 by forwarding frames based on MAC addresses, multilayer switches have additional capabilities to perform routing functions at Layer 3 by making forwarding decisions based on IP addresses.

- ## Static IP addresses on Multilayer Switches

  Before assigning IP addresses to interfaces we must perform the “no switchport” command that converts the interface from Layer 2 to Layer 3, effectively turning it into a routed interface.

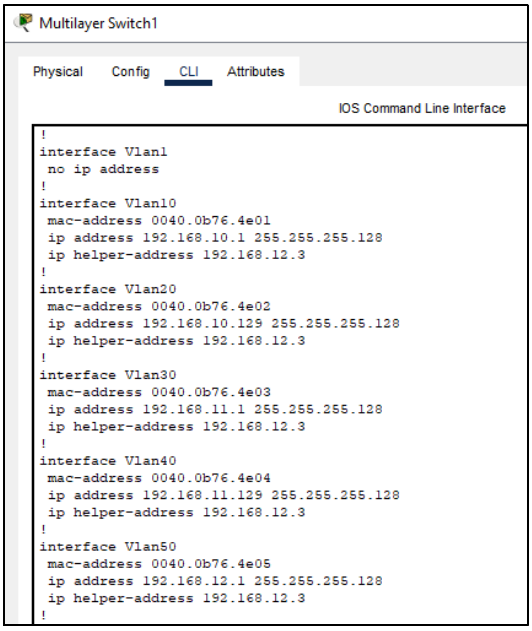


```
!
interface GigabitEthernet1/0/1
 no switchport
 ip address 192.168.12.129 255.255.255.240
 duplex auto
 speed auto
!
interface GigabitEthernet1/0/2
 no switchport
 ip address 192.168.12.145 255.255.255.240
 duplex auto
 speed auto
!
interface GigabitEthernet1/0/3
 switchport access vlan 10
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 switchport mode trunk
!
interface GigabitEthernet1/0/5
 switchport mode trunk
!
interface GigabitEthernet1/0/6
 switchport mode trunk
!
interface GigabitEthernet1/0/7
 switchport mode trunk
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
 --More--
```

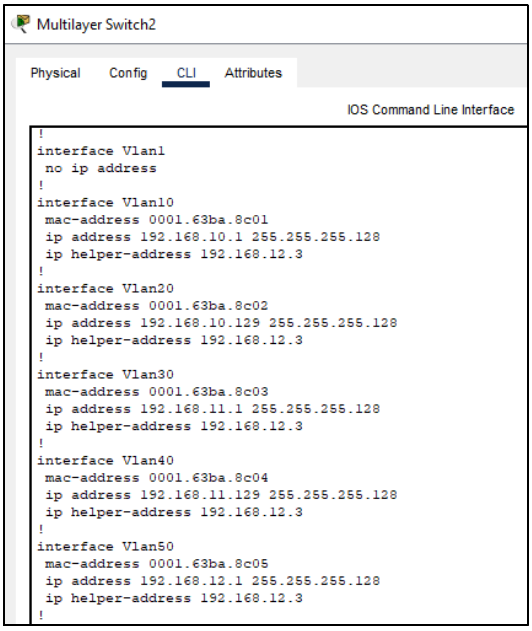


```
!
interface GigabitEthernet1/0/1
 no switchport
 ip address 192.168.12.161 255.255.255.240
 duplex auto
 speed auto
!
interface GigabitEthernet1/0/2
 no switchport
 ip address 192.168.12.177 255.255.255.240
 duplex auto
 speed auto
!
interface GigabitEthernet1/0/3
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 switchport mode trunk
!
interface GigabitEthernet1/0/5
 switchport mode trunk
!
interface GigabitEthernet1/0/6
 switchport mode trunk
!
interface GigabitEthernet1/0/7
 switchport mode trunk
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
 --More--
```

VLANs Configuration on Multilayer Switches



```
!
interface Vlan1
 no ip address
!
interface Vlan10
 mac-address 0040.0b76.4e01
 ip address 192.168.10.1 255.255.255.128
 ip helper-address 192.168.12.3
!
interface Vlan20
 mac-address 0040.0b76.4e02
 ip address 192.168.10.129 255.255.255.128
 ip helper-address 192.168.12.3
!
interface Vlan30
 mac-address 0040.0b76.4e03
 ip address 192.168.11.1 255.255.255.128
 ip helper-address 192.168.12.3
!
interface Vlan40
 mac-address 0040.0b76.4e04
 ip address 192.168.11.129 255.255.255.128
 ip helper-address 192.168.12.3
!
interface Vlan50
 mac-address 0040.0b76.4e05
 ip address 192.168.12.1 255.255.255.128
 ip helper-address 192.168.12.3
!
```



```
!
interface Vlan1
 no ip address
!
interface Vlan10
 mac-address 0001.63ba.8c01
 ip address 192.168.10.1 255.255.255.128
 ip helper-address 192.168.12.3
!
interface Vlan20
 mac-address 0001.63ba.8c02
 ip address 192.168.10.129 255.255.255.128
 ip helper-address 192.168.12.3
!
interface Vlan30
 mac-address 0001.63ba.8c03
 ip address 192.168.11.1 255.255.255.128
 ip helper-address 192.168.12.3
!
interface Vlan40
 mac-address 0001.63ba.8c04
 ip address 192.168.11.129 255.255.255.128
 ip helper-address 192.168.12.3
!
interface Vlan50
 mac-address 0001.63ba.8c05
 ip address 192.168.12.1 255.255.255.128
 ip helper-address 192.168.12.3
!
```

What is IP helper-address?

The IP helper-address command is used in networking to specify the IP address of a DHCP server. This command is typically configured on a router or Layer 3 switch interface that acts as an intermediary between client devices in one network segment and a DHCP server in another segment.

Here's where the IP helper-address command comes into play. By configuring this command on the router or Layer 3 switch interface that connects the two subnets, you tell the router to forward DHCP broadcasts as unicast messages to the specified DHCP server. This allows devices in one subnet to obtain IP addresses from a DHCP server located in another subnet.

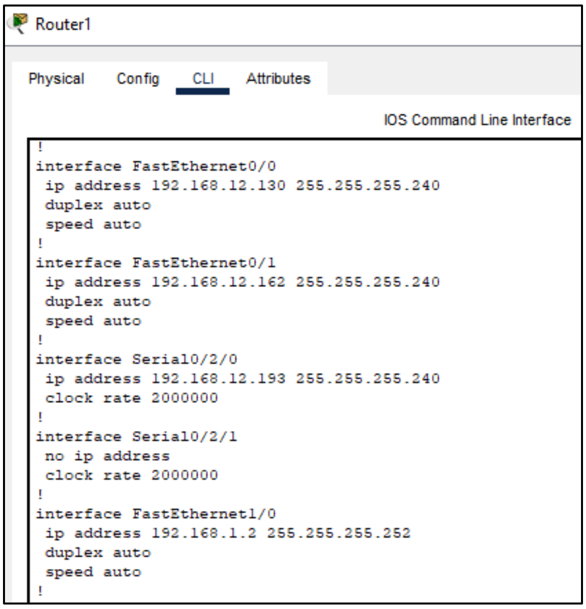
Router

A Router is a networking device that forwards data packets between computer networks. Routers operate at the network layer (Layer 3) of the OSI (Open Systems Interconnection) model.

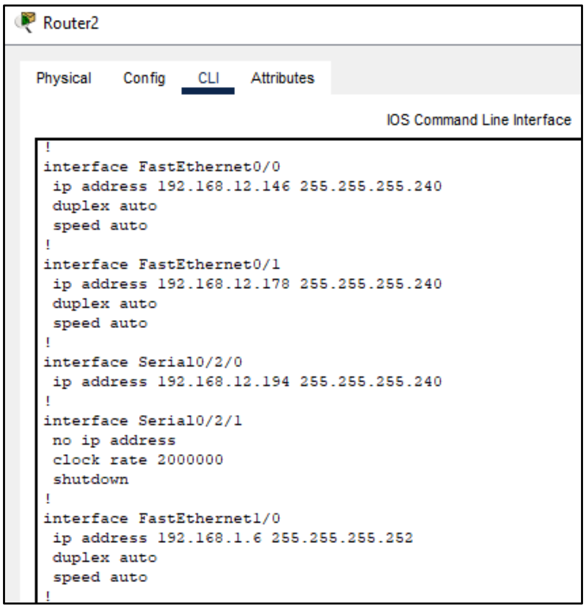
Key functions of a Router include:

- **Packet Forwarding:** Routers examine the destination IP address of data packets and determine the best path for forwarding them to their destination. They use routing tables and routing protocols to make these decisions.
- **Network Address Translation (NAT):** Routers often perform NAT, which allows multiple devices on a local network to share a single public IP address. This is common in home networks where multiple devices connect through a single Internet connection.
- **Routing:** Routers use routing algorithms and protocols to determine the most efficient path for data to travel between networks. Dynamic routing protocols, such as OSPF (Open Shortest Path First) and RIP (Routing Information Protocol).
- **Security:** Routers can implement various security features, such as firewalls and access control lists (ACLs), to control the flow of data between networks and protect against unauthorized access.

Static IP addresses on Routers



```
!
interface FastEthernet0/0
 ip address 192.168.12.130 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.12.162 255.255.255.240
 duplex auto
 speed auto
!
interface Serial0/2/0
 ip address 192.168.12.193 255.255.255.240
 clock rate 2000000
!
interface Serial0/2/1
 no ip address
 clock rate 2000000
!
interface FastEthernet1/0
 ip address 192.168.1.2 255.255.255.252
 duplex auto
 speed auto
!
```



```
!
interface FastEthernet0/0
 ip address 192.168.12.146 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.12.178 255.255.255.240
 duplex auto
 speed auto
!
interface Serial0/2/0
 ip address 192.168.12.194 255.255.255.240
!
interface Serial0/2/1
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet1/0
 ip address 192.168.1.6 255.255.255.252
 duplex auto
 speed auto
!
```

Firewall

Firewall: Is a network security device or software that acts as a barrier between a trusted internal network and untrusted external networks (such as the internet). It monitors and controls incoming and outgoing network traffic based on an organization's previously established security policies.

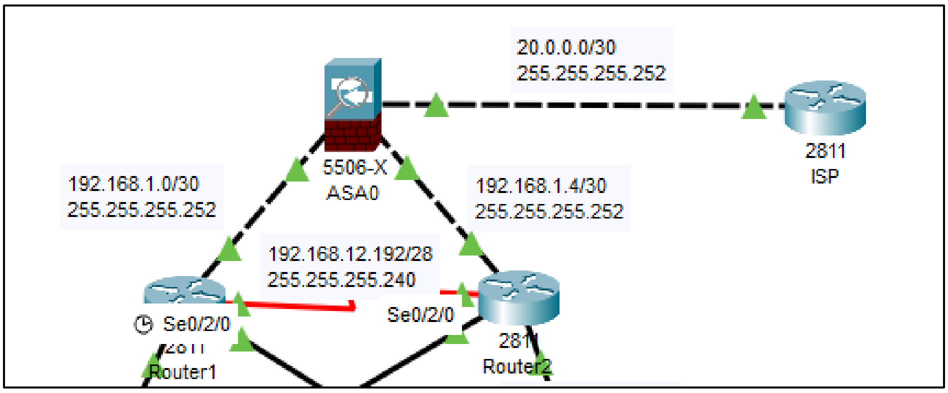
Functions:

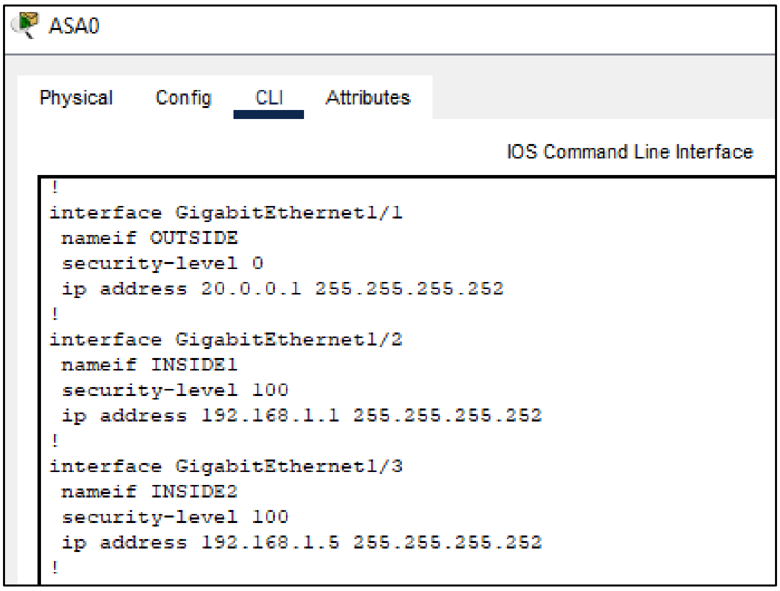
Packet Filtering: Examines packets and decides whether to allow or block them based on predetermined rules.

Stateful Inspection: Keeps track of the state of active connections and makes decisions based on the context of the traffic.

Proxying and Network Address Translation (NAT): Hides internal network structure and IP addresses.

- We've applied the firewall on the topology as an ASA firewall server connects to the routers from the inside and to the ISP router from outside as following:





```
!
interface GigabitEthernet1/1
 nameif OUTSIDE
 security-level 0
 ip address 20.0.0.1 255.255.255.252
!
interface GigabitEthernet1/2
 nameif INSIDE1
 security-level 100
 ip address 192.168.1.1 255.255.255.252
!
interface GigabitEthernet1/3
 nameif INSIDE2
 security-level 100
 ip address 192.168.1.5 255.255.255.252
!
```

Routing Protocols

Routing protocol goal: determine "good" paths (equivalently, routes), from sending hosts to receiving host, through network of routers

- path: sequence of routers packets traverses from given initial source host to final destination host

- Two types of routing algorithms

	Link-State Routing	***Distance-Vector Routing***
Algorithm Basis	• *Information Basis:* Each router has a complete map of the network. • *Computation:* Based on the complete topology information. • *Updates:* Routers share information about their directly connected links with all other routers.	• *Information Basis*: Routers only know the distance (cost) to their neighbors. • *Computation*: Based on iterative updates between neighboring routers. • *Updates*: Routers periodically exchange information about their routing tables with neighboring routers.
Routing Table	• *Content*: Detailed and accurate information about the entire network. • *Storage*: Each router stores a complete map of the network.	• *Content*: Contains information about the distance and next-hop router for each destination. • *Storage*: Each router stores the distance to all destinations.
Algorithm used	• *Path Computation*: Uses Dijkstra's algorithm to calculate the shortest path. • Optimality: Results in an optimal path based on current network conditions.	• *Path Computation*: Uses the Bellman-Ford algorithm to update routing tables iteratively. • *Optimality*: May not always result in the optimal path due to the count-to-infinity problem.
Convergence	• *Convergence Time*: Generally faster convergence as routers have more information about the network. • *Event-Driven*: Updates are triggered by changes in the network.	• Convergence Time: Slower convergence, especially in larger networks. • Triggered Updates: Updates are triggered by changes in the network, and convergence may take multiple iterations.

Examples	- *Open Shortest Path First* (OSPF): A widely used link-state routing protocol.	- *Routing Information Protocol* (RIP): A classic distance-vector routing protocol. - *Border Gateway Protocol* (BGP): Used for inter-domain routing on the Internet.

Considerations:

- *Scalability:* Link-state protocols tend to scale better in larger networks.
- *Convergence:* Link-state protocols often converge faster.
- *Overhead:* Distance-vector protocols may have more routing table updates.

Hybrid Protocols: Some modern routing protocols, like Enhanced Interior Gateway Routing Protocol (EIGRP), incorporate elements of both link-state and distance-vector algorithms, aiming to achieve a balance between the advantages of each.

▪ Intra and Inter domains approaches

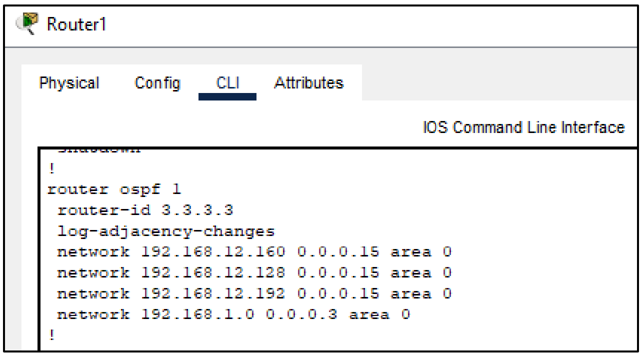
	Intra Domain	*Inter Domain*
Definition	"Intra" means within or inside. In the context of routing, intra-domain refers to routing within a single administrative domain or autonomous system (AS). Intra-domain routing protocols are used to exchange routing information within a single network or organization (within AS).	"Inter" means between or among. Inter-domain refers to routing between different administrative domains or autonomous systems (AS). Inter-domain routing protocols are used for routing between multiple networks or organizations (between AS'es).
Examples	OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol)	BGP (Border Gateway Protocol)
Use cases	- Routing within a corporate network. - Communication within a single organization. - Exchange of routing information within an autonomous system.	- Routing between different service providers. - Communication between organizations. - Exchange of routing information between distinct autonomous systems.

Considerations:

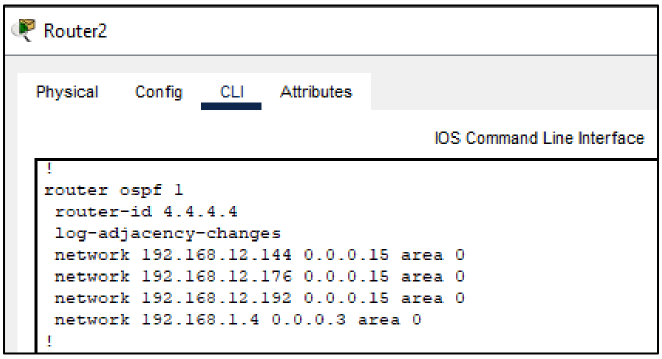
- *Security:* Intra-domain routing is often more trusted and may use internal security measures.
- *Scaling:* Inter-domain routing protocols need to handle the scale of the entire Internet.
- *Policy:* Organizations have more control over intra-domain routing policies.

- Based on the previous theoretical knowledge we applied OSPF routing protocol on our LAN topology as following:

- OSPF Configuration on Routers:

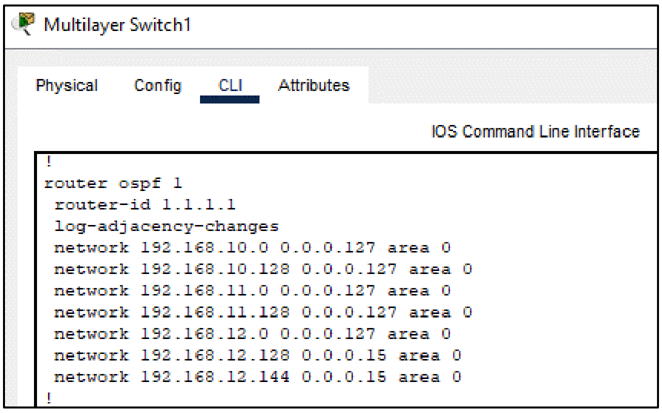


```
 shutdown
!
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 192.168.12.160 0.0.0.15 area 0
 network 192.168.12.128 0.0.0.15 area 0
 network 192.168.12.192 0.0.0.15 area 0
 network 192.168.1.0 0.0.0.3 area 0
!
```

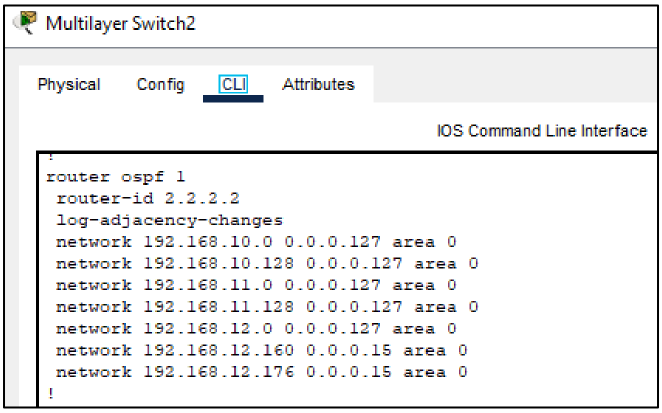


```
!
router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
 network 192.168.12.144 0.0.0.15 area 0
 network 192.168.12.176 0.0.0.15 area 0
 network 192.168.12.192 0.0.0.15 area 0
 network 192.168.1.4 0.0.0.3 area 0
!
```

- OSPF Configuration on Multilayer Switches:

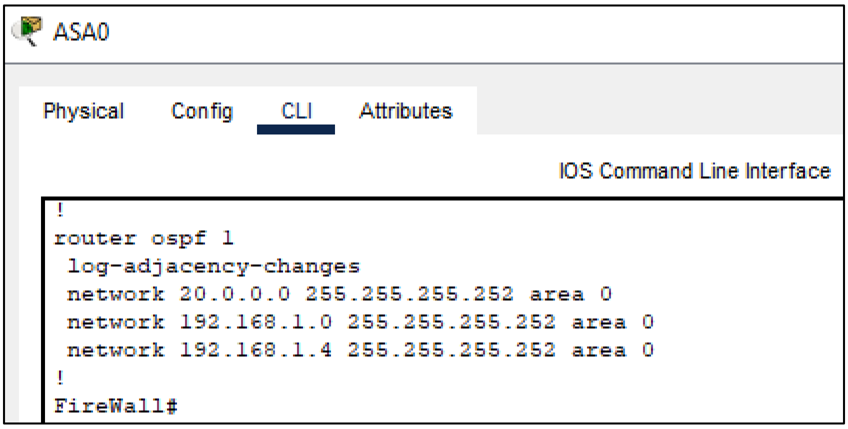


```
!
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 192.168.10.0 0.0.0.127 area 0
 network 192.168.10.128 0.0.0.127 area 0
 network 192.168.11.0 0.0.0.127 area 0
 network 192.168.11.128 0.0.0.127 area 0
 network 192.168.12.0 0.0.0.127 area 0
 network 192.168.12.128 0.0.0.15 area 0
 network 192.168.12.144 0.0.0.15 area 0
!
```



```
!
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 192.168.10.0 0.0.0.127 area 0
 network 192.168.10.128 0.0.0.127 area 0
 network 192.168.11.0 0.0.0.127 area 0
 network 192.168.11.128 0.0.0.127 area 0
 network 192.168.12.0 0.0.0.127 area 0
 network 192.168.12.160 0.0.0.15 area 0
 network 192.168.12.176 0.0.0.15 area 0
!
```

- OSPF Configuration on Firewall:

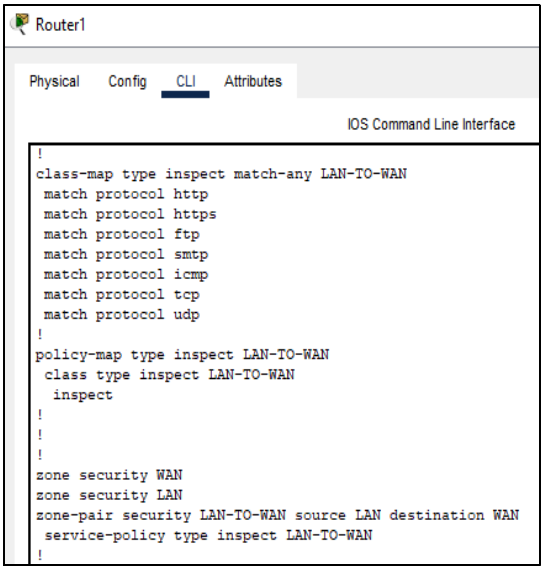


```
!
router ospf 1
 log-adjacency-changes
 network 20.0.0.0 255.255.255.252 area 0
 network 192.168.1.0 255.255.255.252 area 0
 network 192.168.1.4 255.255.255.252 area 0
!
FireWall#
```

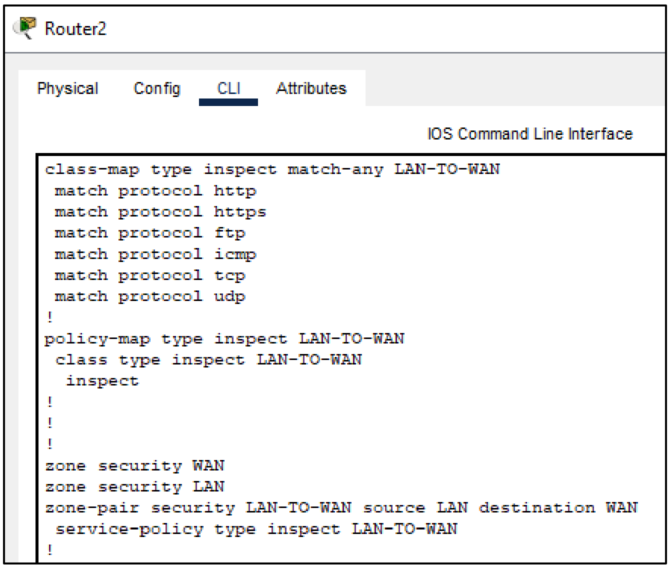
Network Security Policy

network security policy: An extensive document that describes the standards, procedures, and recommendations for guaranteeing the security of a company's computer networks. This policy, which is intended to safeguard the availability, confidentiality, and integrity of the company's network resources, is an essential part of a comprehensive information security strategy.

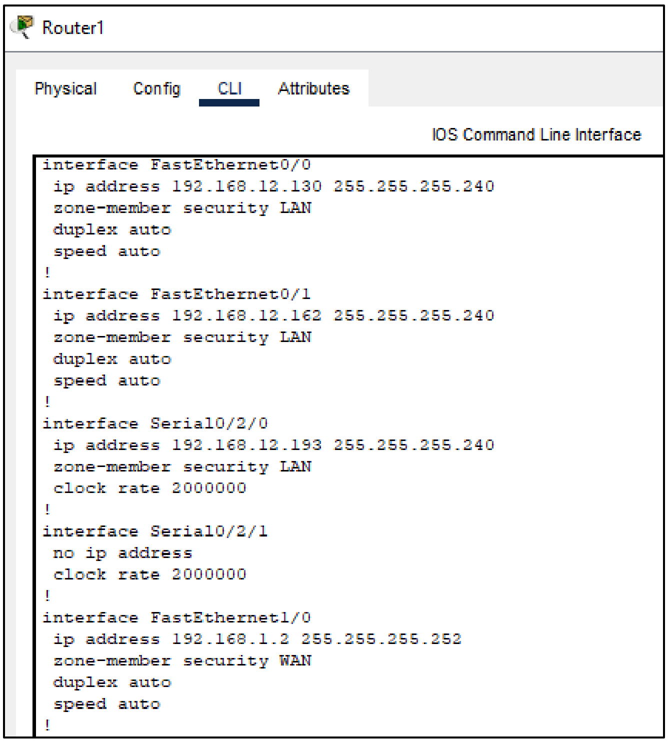
- Configuring basic security policy on routers



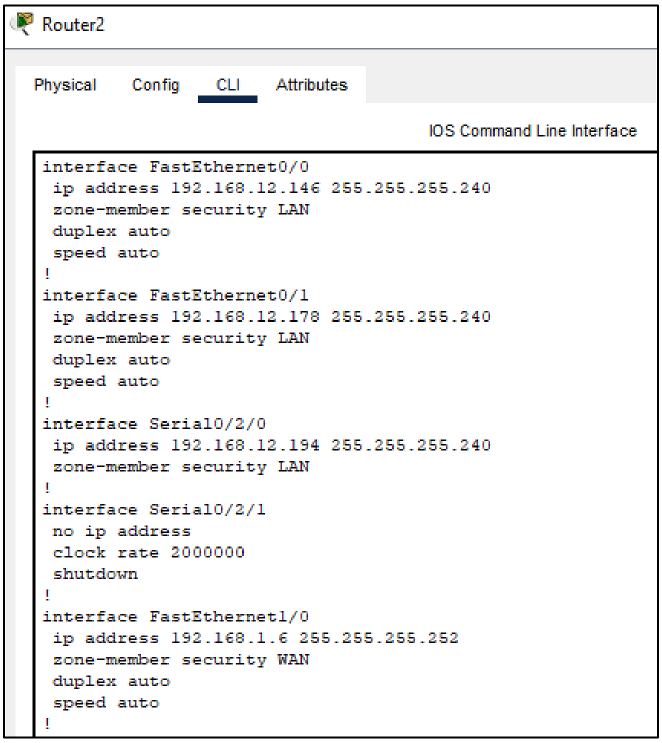
```
!
class-map type inspect match-any LAN-TO-WAN
 match protocol http
 match protocol https
 match protocol ftp
 match protocol smtp
 match protocol icmp
 match protocol tcp
 match protocol udp
!
policy-map type inspect LAN-TO-WAN
 class type inspect LAN-TO-WAN
  inspect
!
!
!
zone security WAN
zone security LAN
zone-pair security LAN-TO-WAN source LAN destination WAN
 service-policy type inspect LAN-TO-WAN
!
```



```
class-map type inspect match-any LAN-TO-WAN
 match protocol http
 match protocol https
 match protocol ftp
 match protocol icmp
 match protocol tcp
 match protocol udp
!
policy-map type inspect LAN-TO-WAN
 class type inspect LAN-TO-WAN
  inspect
!
!
!
zone security WAN
zone security LAN
zone-pair security LAN-TO-WAN source LAN destination WAN
 service-policy type inspect LAN-TO-WAN
!
```



```
interface FastEthernet0/0
 ip address 192.168.12.130 255.255.255.240
 zone-member security LAN
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.12.162 255.255.255.240
 zone-member security LAN
 duplex auto
 speed auto
!
interface Serial0/2/0
 ip address 192.168.12.193 255.255.255.240
 zone-member security LAN
 clock rate 2000000
!
interface Serial0/2/1
 no ip address
 clock rate 2000000
!
interface FastEthernet1/0
 ip address 192.168.1.2 255.255.255.252
 zone-member security WAN
 duplex auto
 speed auto
!
```

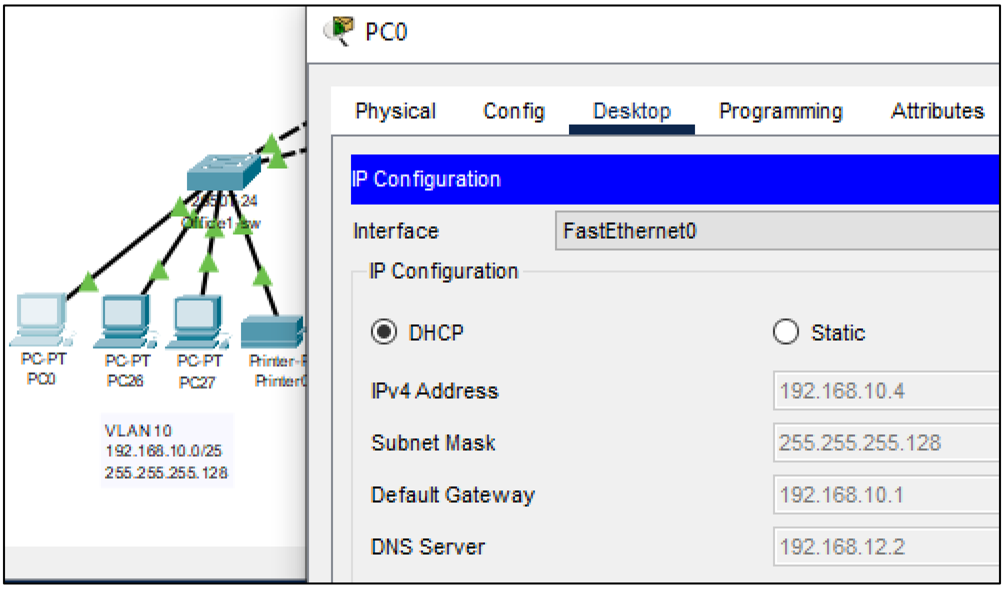


```
interface FastEthernet0/0
 ip address 192.168.12.146 255.255.255.240
 zone-member security LAN
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.12.178 255.255.255.240
 zone-member security LAN
 duplex auto
 speed auto
!
interface Serial0/2/0
 ip address 192.168.12.194 255.255.255.240
 zone-member security LAN
!
interface Serial0/2/1
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet1/0
 ip address 192.168.1.6 255.255.255.252
 zone-member security WAN
 duplex auto
 speed auto
!
```

User Devices Configuration

Dynamic IP addresses configuration using DHCP server.

- **On VLAN 10**



PC0

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

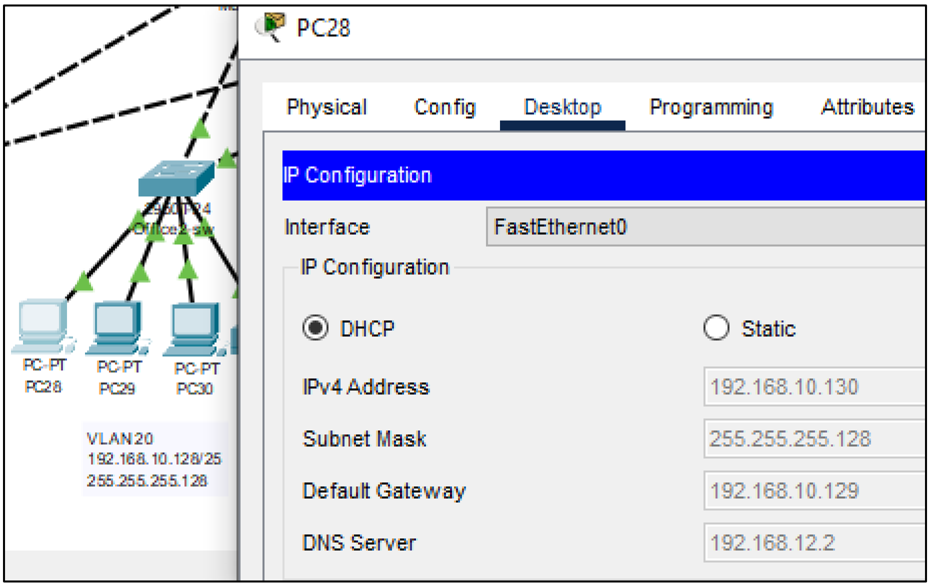
IPv4 Address: 192.168.10.4

Subnet Mask: 255.255.255.128

Default Gateway: 192.168.10.1

DNS Server: 192.168.12.2

- **On VLAN 20**



PC28

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

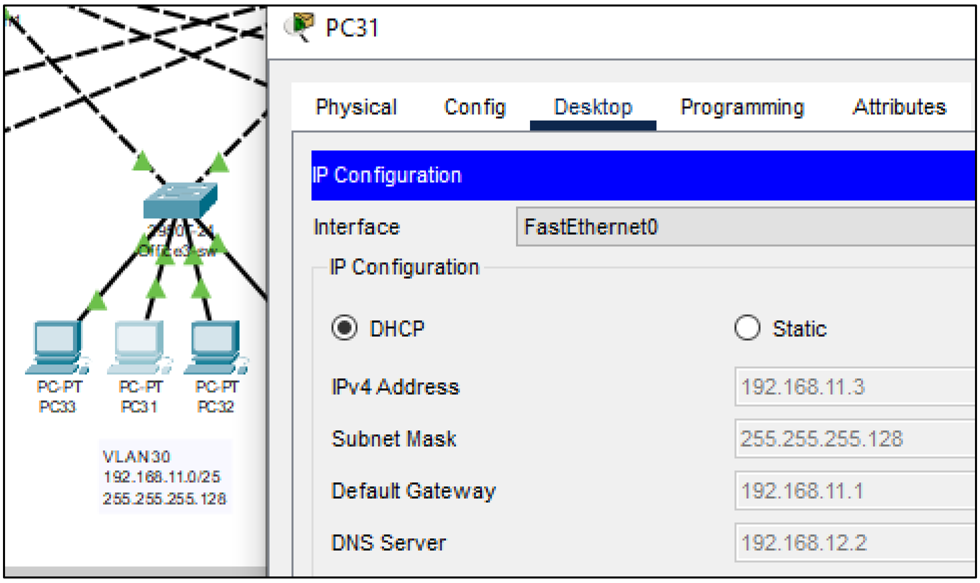
IPv4 Address: 192.168.10.130

Subnet Mask: 255.255.255.128

Default Gateway: 192.168.10.129

DNS Server: 192.168.12.2

- **On VLAN 30**



PC31

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

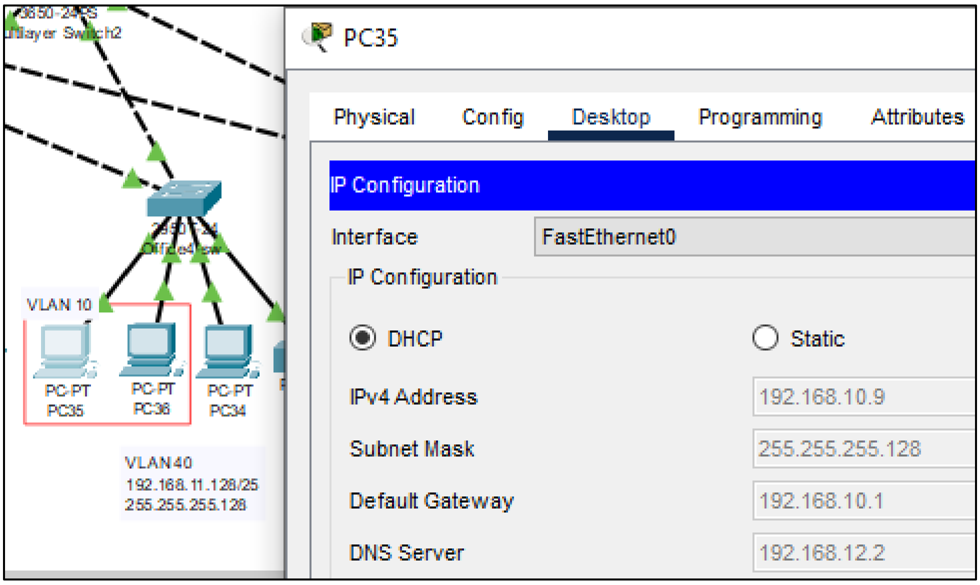
IPv4 Address: 192.168.11.3

Subnet Mask: 255.255.255.128

Default Gateway: 192.168.11.1

DNS Server: 192.168.12.2

- **On VLAN 10 of Office 4 Switch**



PC35

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

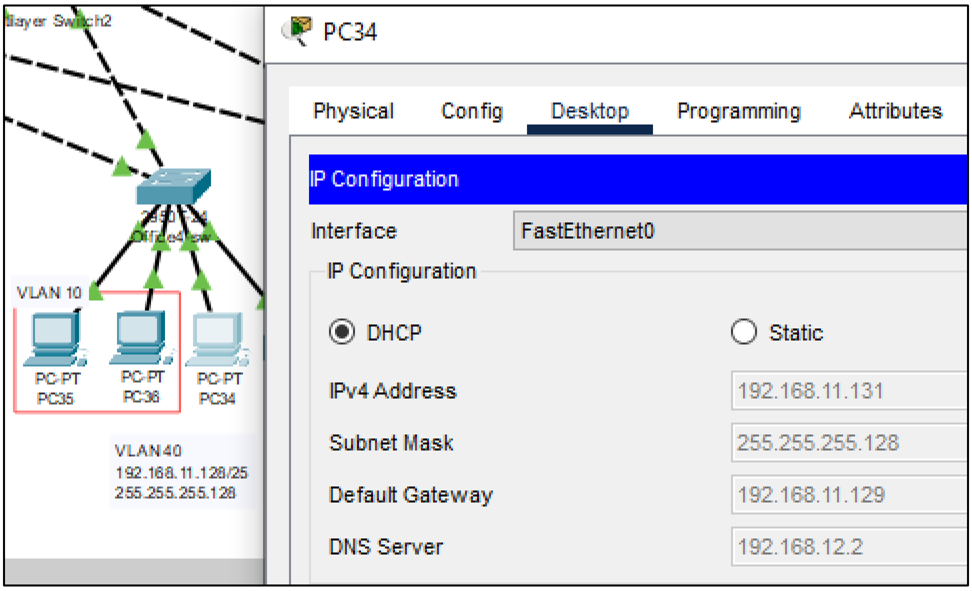
IPv4 Address: 192.168.10.9

Subnet Mask: 255.255.255.128

Default Gateway: 192.168.10.1

DNS Server: 192.168.12.2

- **On VLAN 40**



PC34

IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static

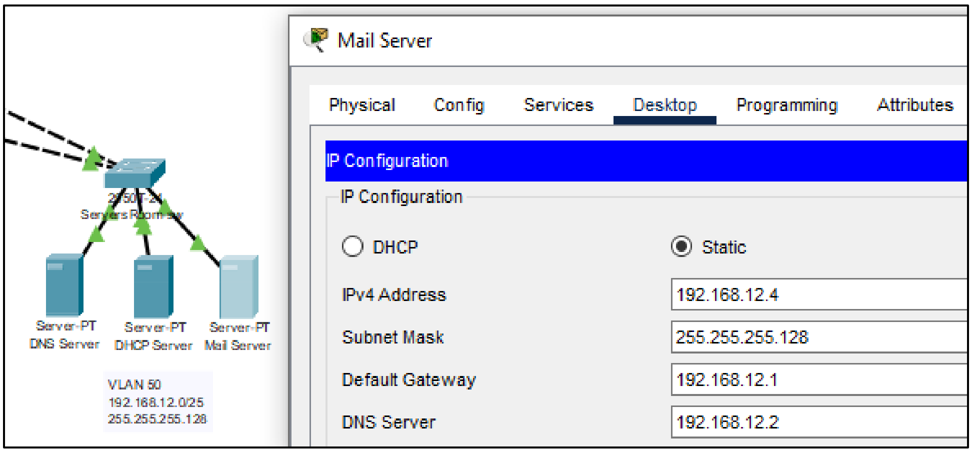
IPv4 Address 192.168.11.131

Subnet Mask 255.255.255.128

Default Gateway 192.168.11.129

DNS Server 192.168.12.2

- **On VLAN 50 servers configured staticlly**



Mail Server

IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.12.4

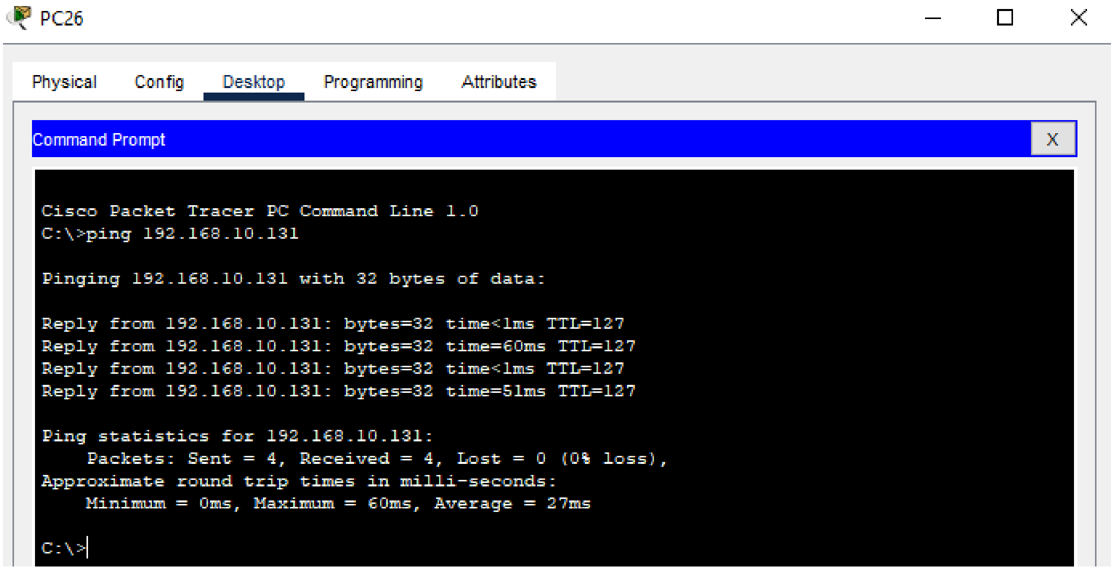
Subnet Mask 255.255.255.128

Default Gateway 192.168.12.1

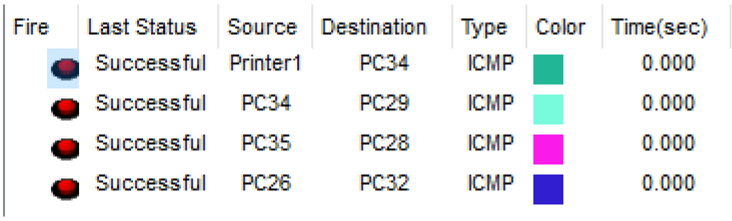
DNS Server 192.168.12.2

Testing Connectivity

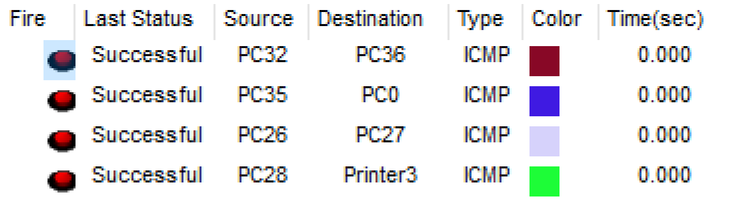
- Testing Internal network



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.131

Pinging 192.168.10.131 with 32 bytes of data:

Reply from 192.168.10.131: bytes=32 time<1ms TTL=127
Reply from 192.168.10.131: bytes=32 time=60ms TTL=127
Reply from 192.168.10.131: bytes=32 time<1ms TTL=127
Reply from 192.168.10.131: bytes=32 time=51ms TTL=127

Ping statistics for 192.168.10.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 60ms, Average = 27ms

C:\>
```

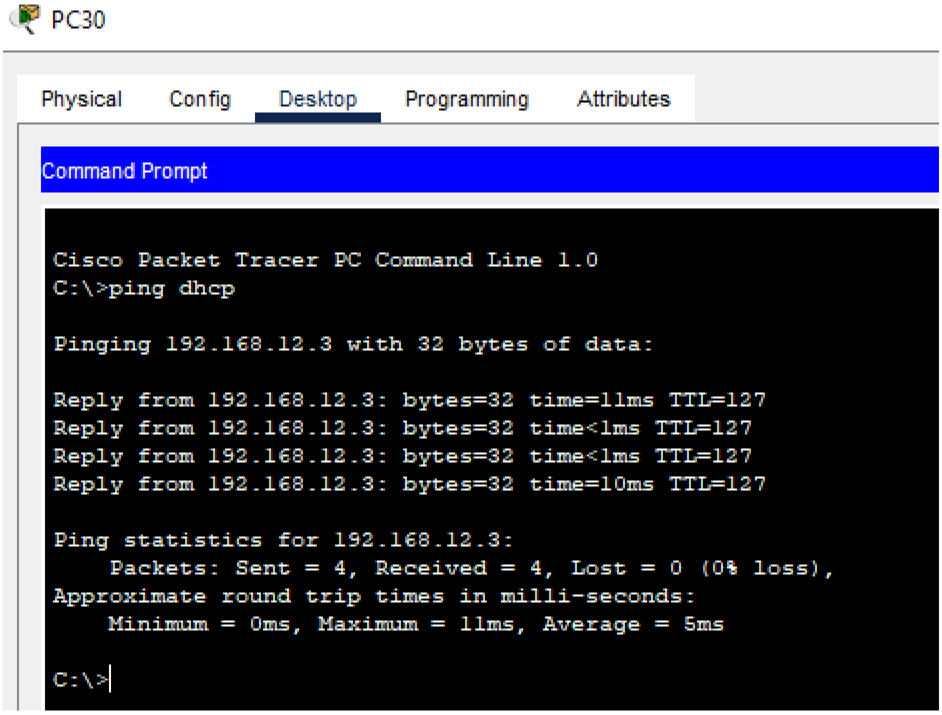


Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	Printer1	PC34	ICMP	🟩	0.000
●	Successful	PC34	PC29	ICMP	🟩	0.000
●	Successful	PC35	PC28	ICMP	🟪	0.000
●	Successful	PC26	PC32	ICMP	🟦	0.000



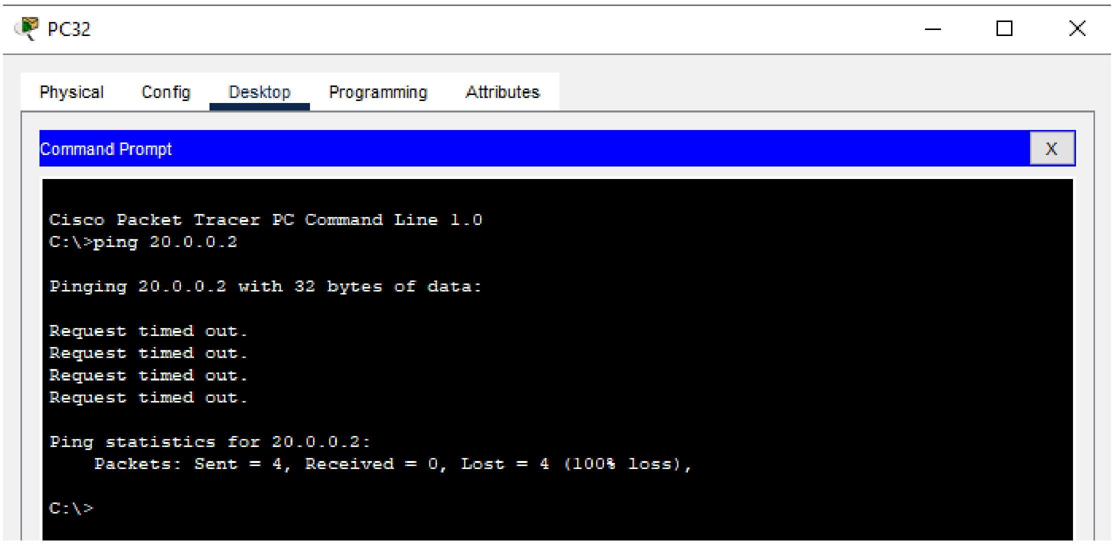
Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Successful	PC32	PC36	ICMP	🟥	0.000
●	Successful	PC35	PC0	ICMP	🟦	0.000
●	Successful	PC26	PC27	ICMP	🟪	0.000
●	Successful	PC28	Printer3	ICMP	🟩	0.000

- Testing DNS

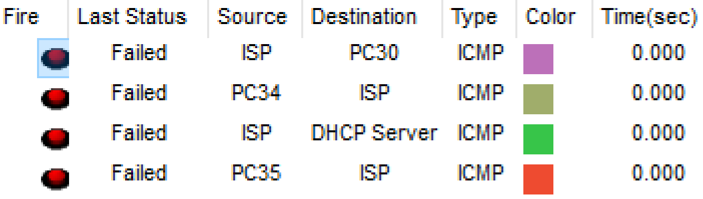


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping dhcp

Pinging 192.168.12.3 with 32 bytes of data:

Reply from 192.168.12.3: bytes=32 time=11ms TTL=127
Reply from 192.168.12.3: bytes=32 time<1ms TTL=127
Reply from 192.168.12.3: bytes=32 time<1ms TTL=127
Reply from 192.168.12.3: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.12.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>
```

- Testing Network Security



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

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

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



Fire	Last Status	Source	Destination	Type	Color	Time(sec)
●	Failed	ISP	PC30	ICMP	🟪	0.000
●	Failed	PC34	ISP	ICMP	🟩	0.000
●	Failed	ISP	DHCP Server	ICMP	🟩	0.000
●	Failed	PC35	ISP	ICMP	🟥	0.000

References

- TechTarget.com
- NetworkLessons.com
- Community.Cisco.com
- AlgoSec.com
- Guru99.com
- Check Point software.com