Assignment No. 5: Using A Network Simulator (E.G. Packet Tracer) Configure-Vlan, Dynamic Trunk Protocol And Spanning Tree Protocol OSPF – Explore Neighbor-Ship Condition And Requirement, Neighbor-Ship States, Ospf Metric Cost Calculation. Network Address Translation: Static, Dynamic & Pat (Port Address Translation)

OSPF Fundamental Terminology

OSPF stands for Open Shortest Path First. OSPF is a link state open standard based routing protocol. It was created in mid-1980. Since it is based on open standard, we can use it with any vendor's router.

Features and advantage of OSPF

- It supports both IPv4 and IPv6 routed protocols.
- It supports load balancing with equal cost routes for same destination.
- Since it is based on open standards, it will run on most routers.
- It provides a loop free topology using SPF algorithm.
- It is a classless protocol.
- It supports VLSM and route summarization.
- It supports unlimited hop counts.
- It scales enterprise size network easily with area concept.
- It supports trigger updates for fast convergence.

Just like other routing protocols, OSPF also has its negatives.

Disadvantage of OSPF

- It requires extra CPU process to run SPF algorithm.
- It requires more RAM to store adjacency topology.
- It is more complex to setup and hard to troubleshoot.

Basically OPSF was created to fulfill the requirement of enterprise size network. To scale a large size network it uses area concept. Area concept is similar to Subnetting. It allows us to separate the large internetwork into smaller networks known as areas.

Along with Area concept OSPF also supports Autonomous System (AS). Just like area, AS also divide a large network into smaller networks.

Difference between **AS and Area concept**

Area concept is a feature of OSPF. It is limited only with OSPF. We cannot use it with other routing protocol.

AS is an independent concept originally defined in RFC 1771. We can use it with any routing protocols which understand its concept.

OSPF Neighborship Condition and Requirement

OSPF routers share routing information only with neighbors. OSPF uses hello packets to discover neighbors in segments. A hello packet contains some essential configuration values that must be same on

both routers who want to build an OSPF neighborship. we will explain these configuration values in detail with example.

OSPF Neighborship Requirement: In order to become OSPF neighbor following values must be match on both routers.

- Area ID
- Authentication
- Hello and Dead Intervals
- Stub Flag
- MTU Size

Area ID

OSPF uses area concept to scale an enterprise size network. I have explained OSPF Areas in first part of this article. Just for reference, OSPF areas create a logical boundary for routing information. Following figure illustrate a simple OSPF network. In this network **R1** is eligible to form neighborship with **R4** and **R2** respectively on **S0/0** and **F0/0**.

Hello packets and hello interval

Hello packets are the special type of LSAs (Link State Advertisements) which are used to discover the neighbors in same segment. And once neighborship is built same hello packets are used to maintain the neighborship. Hello packets contain all necessary information that is required to form a neighborship. Default hello interval is **10** seconds.

Dead Intervals

hello packets from neighbor in particular time interval. This time interval is known as dead interval. Dead interval is the number of seconds that a router waits for hello packet from neighbor, before declaring it as dead.Default dead interval is **40** seconds. If a router does not receive hello packet in **40** seconds from neighbor it will declare that as dead. Hello and dead interval must be same between two neighbors. If any of these intervals are different, neighborship will not form.

Stub Area Flag

This value indicates that whether sending router belong to stub area or not. Routers who want to build OPSF neighborship must have same stub area flag.

MTU

Technically MTU (Maximum Transmission Unit) is not a part of compulsory matching conditions. Still we should match this value. If this value does not match routers may stuck in Exstart/Exchange exchange stage.

OSPF Neighbor States Explained With Example

OSPF routers go through the seven states while building neighborship with other routers.

- Down state
- Attempt/Init state
- Two ways state
- Exstart state
- Exchange state
- Loading state
- Full state

Down state

At this point both routers have no information about each other. R1 does not know which protocol is running on R2. Vice versa R2 have no clue about R1. In this stage OSPF learns about the local interfaces which are configured to run the OSPF instance.

RID

RID is a unique identifier of Router in OSPF network. It must be unique within the autonomous system. An OSPF router looks in three places for RID:-

1. Manual configuration
2. Loopback interface IP configuration
3. Active interfaces IP configuration

Key points

- OSPF will follow the sequence (Manual configuration => Loopback interface => Active interface) of options while selecting RID. If RID is found, it will not look in next option.
- OSPF will choose IP address only from operational IP interface. Operational means interface should be listed as line is up and line protocol is up in the output of show ip interface brief command.
- When multiple IP addresses available, OSPF will always pick highest IP address for RID.
- For network stability we should always set RID from either **router-id** command or by using loopback interfaces.
- By default Router chooses OSPF RID when it initialized. Once RID is selected it will use that RID until next reboot.
- If OSPF fails to select the RID, it will halt the OSPF process. We cannot use OSPF process without RID.

Attempt/Init state

Neighborship building process starts from this state. R1 multicasts first hello packet so other routers in network can learn about the existence of R1 as an OSPF router. This hello packet contains Router ID and some essential configuration values such as area ID, hello interval, hold down timer, stub flag and MTU. Essential configuration values must be same on routers who want to build an OSPF neighborship.

Two ways state

If essential configuration values match, R2 will add R1 in neighbour table and reply with its hello packet. As R2 knows the exact address of R1, it will use unicast for reply.

R1 will take following actions:-

- It will read RID from hello packet and look in its neighbor table for existing entry.
- If a match for RID found in neighbor table, it would reset the dead interval timer for that entry.
- If a match is not found in neighbor table, it would read the essential configuration values from packet.
- R1 will reply with a hello packet which contains its neighbor table data.

Point to point network

It is a Cisco specific network type. It connects a single pair of routers. HDLC and PPP are example of point to point network type. In this type of network:-

- All routers form full adjacencies with each other.
- Hello packets are sent using a multicast address 224.0.0.5
- No DR and BDR are required.
- All routers are considered as **AllSPFRouters**.

I will explain the terms adjacencies, DR, BDR and AllSPFRouters shortly.

Broadcast Networks

Broadcast networks are capable in connecting more than two devices. Ethernet and FDDI are the example of broadcast type network. In this type of network:-

- A single transmitted packet can be received by all attached devices.
- DR and BDR are required.
- All routers form full adjacencies only with DR and BDR.
- Routers use a multicast address 224.0.0.6 to update the DR.
- DR uses a multicast address 224.0.0.5 to update the all routers.

NMBA

Non-broadcast Multi-access networks are also capable in connecting more than two devices. But they do not have broadcast capability. X.25 and Frame Relay are the example of NMBA type network. In this type of network:-

- As network does not have broadcast capability, dynamic network discovery will not be possible.
- OSPF neighbors must have to define statically.
- All OSFP packets are unicast.
- DR and BDR are required.

Point to multipoint

Point to multipoint is a special implementation of NMBA network where networks are configured as a collection of point to point links. In this type of network:-

- Network must be configured statically.
- No DR and BRD are selected in this type of network.
- OSPF packets are multicast.

Exstart state

Routers who decided to build adjacency will form a master / slave relationship. In each adjacency router who has higher RID will become master and other will become slave. Do not mix Master /Slave relationship with DR/ BDR/ DROTHER relationship. Master / Slave relationship has limited purpose. It is used to decide the Router who will start exchange process. Always Master starts exchange process.

Exchange state

In exchange state, Master and slave decide how much information needs to be exchange. A router that has more than one interface may learn same network information from different sources. An OSFP router is smart enough to filter the updates before receiving it. It will ask only for the updates which it does not have. In this state, routers will filter the updates which need be to exchange.

Loading state

In this state actual routing information is exchanged. Routers exchange LSAs from LSR list.

Routers will use LSU (Link state update) to exchange the LSAs. Each LSA contains routing information about a particular link. Routers also maintain a retransmission list to make sure that every sent LSA is acknowledged.

Full state

Full state indicates that both routers has been exchanged all LSAs from LSR list. Now they have identical LSDB.

Adjacent routers remain in this state for life time. This state also referred as adjacency. If any change occurs in network, routers will go through this process again.

That's all for this part. In next part, I will explain configuration part of OSPF.Neighboring routers are the routers that have interfaces in common network.Adjacency is a relationship formed between neighboring routers for the purpose of exchanging routing information. Not every pair of neighboring routers becomes adjacent.

OSPF Metric Cost Calculation Formula Explained

OSPF uses SPF (Shortest Path First) algorithm to select the best route for routing table. SPF algorithm was invented in 1956 by Edsger W. Dijkstra. It is also referred as Dijkstra algorithm. SPF is a quite complex algorithm. In this tutorial we will explain a simplified overview of this algorithm.

Shortest Path First (SPF) Algorithm

As we know upon initialization or due to any change in routing information an OSPF router generates a LSA. This LSA (Link State Advertisement) contains the collection of all link-states on that router. Router propagates this LSA in network. Each router that receives this LSA would store a copy of it in its LSA database then flood this LSA to other routers. After database is updated, router selects a single best route for each destination from all available routes. Router uses SPF algorithm to select the best route.

OSPF Metric cost

Logically a packet will face more overhead in crossing a 56Kbps serial link than crossing a 100Mbps Ethernet link. Respectively it will take less time in crossing a higher bandwidth link than a lower bandwidth link. OSPF uses this logic to calculate the cost. Cost is the inverse proportional of bandwidth. Higher bandwidth has a lower cost. Lower bandwidth has a higher cost.

OSPF uses following formula to calculate the cost

Cost = Reference bandwidth / Interface bandwidth in bps.

Reference bandwidth was defined as arbitrary value in OSPF documentation (RFC 2338). Vendors need to use their own reference bandwidth. Cisco uses 100Mbps (10^8) bandwidth as reference bandwidth. With this bandwidth, our equation would be

Cost = 10^8/interface bandwidth in bps

Key points

- Cost is a positive integer value.
- Any decimal value would be rounded back in nearest positive integer.
- Any value below 1 would be considered as 1.

Now we know the equation, let's do some math and figure out the default cost of some essential interfaces.

Default cost of essential interfaces.

Interface Type	bandwidth	Metric Calculation	Cost
Ethernet Link	10Mbps	100000000/10000000 = 10	10
FastEthernet Link	100Mbps	100000000/100000000 = 1	1
Serial Link	1544Kbps(default)	100000000/1544000 = 64.76	64

Cost of common lines

Line	Bandwidth	Metric calculation	Cost
56 Kbps line	56Kbps	100000000/56000 = 1785.71	1785
64 Kbps line	64Kbps	100000000/64000 = 1562.5	1562
128 Kbps line	128Kbps	100000000/128000 = 781.25	781
512 Kbps line	512 Kbps	100000000/512000 = 195.31	195
1 Mbps line	1Mbps	100000000/1000000 = 100	100
10 Mbps line	10Mbps	100000000/10000000 = 10	10
100 Mbps line	100Mbps	100000000/100000000 = 1	1
1 Gbps line	1Gbps	100000000/100000000 0= 0.1	1
10 Gbps line	10Gbps	100000000/10000000000 = 0.01	1

SPT (Shortest Path Tree)

OSPF router builds a Shortest Path Tree. SPT is just like a family tree where router is the root and destination networks are the leaves. SPF algorithm calculates the branch cost between leaves and root. Branch with lowest cost will be used to reach at leaf. In technical language route that has lowest cumulative cost value between source and destination will be selected for routing table.

Cumulative cost = ***Sum of all outgoing interfaces cost in route***

Best route for routing table = ***Route which has the lowest cumulative cost***

Configuration of OSPF Routing Protocol

Interface mode is used to assign the IP address and other parameters. Interface mode can be accessed from global configuration mode. Following commands are used to access the global configuration mode.

```
Router>enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

From global configuration mode we can enter in interface mode. From there we can configure the interface. Following commands will assign IP address on FastEthernet0/0 and FastEthernet0/1.

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

interface fastEthernet 0/0 command is used to enter in interface mode.

ip address 10.0.0.1 255.0.0.0 command would assign IP address to interface.

no shutdown command would bring the interface up.

exit command is used to return in global configuration mode.

Serial interface needs two additional parameters **clock rate** and **bandwidth**. Every serial cable has two ends DTE and DCE. These parameters are always configured at DCE end.

We can use **show controllers *interface*** command from privilege mode to check the cable's end.

```
Router#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 2000000
```

```
[Output omitted]
```

Fourth line of output confirms that DCE end of serial cable is attached. If you see DTE here instead of DCE skip these parameters.Now we have necessary information let's assign IP address to serial interfaces.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.0.1  255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 192.168.2.1  255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

Router#configure terminal Command is used to enter in global configuration mode.

Router(config)#interface serial 0/0/0 Command is used to enter in interface mode.

Router(config-if)#ip address 192.168.0.1 255.255.255.252 Command assigns IP address to interface. For serial link we usually use IP address from /30 subnet.

Router(config-if)#clock rate 64000 In real life environment this parameter controls the data flow between serial links and need to be set at service provider's end. In lab environment we need not to worry about this value. We can use any valid clock rate here.

Router(config-if)#bandwidth 64 Bandwidth works as an influencer. It is used to influence the metric calculation of OSPF or any other routing protocol which uses bandwidth parameter in route selection process. Serial interface has default bandwidth of 1544Kbps. To explain, how bandwidth influence route selection process we will configure (64Kbps) bandwidth on three serial DCE interfaces of our network; R0's Se0/0/0, R1's Se0/0/1 and R2's Se0/0/0.

Router(config-if)#no shutdown Command brings interface up.

Router(config-if)#exit Command is used to return in global configuration mode.

Configure OSPF routing protocol

Enabling OSPF is a two steps process:-

- Enable OSPF routing protocol from global configuration mode.
- Tell OSPF which interfaces we want to include.

For these steps following commands are used respectively.

```
Router(config)# router ospf process_ID
Router(config-router)# network IP_network_# [wild card mask] Area Number area number
```

Router(config)# router ospf process ID

This command will enable OSPF routing protocol in router. Process ID is a positive integer.

Router(config-router)# network IP_network_# [wildcard_mask] area [area number]

Network command allows us to specify the interfaces which we want to include in OSPF process. This command accepts three arguments network number, wildcard mask and area number.

Network number

Network number is network ID. We can use any particular host IP address or network IP address. While targeting multiple interfaces, we use network IP address. So any interface that belongs to specified network ID will be selected.

Wildcard mask

Wildcard mask are used with network ID to filter the interfaces. Wildcard mask is different from subnet mask. Subnet mask is used to separate the network portion and host portion in IP address. While wildcard mask is used to match corresponding octet in network portion. Wildcard mask tells OSPF the part of network address that must be matched. Wildcard masks are explained with examples in access list tutorials of this category.

Key points

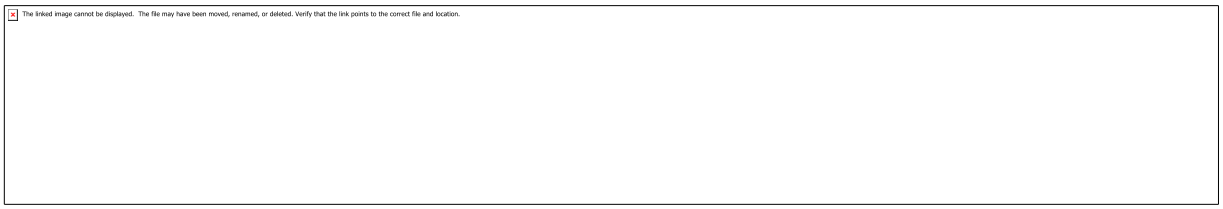
0 (*Decimal – octet format*) Wildcard mask indicates that corresponding octet in network address must be matched exactly.

255 (*Decimal – octet format*) Wildcard mask indicates that we don't care about corresponding octet in network address.

For example

0 (*Binary – bit format*) Wildcard mask indicates that corresponding bit in network address must be matched exactly.

255 (*Binary – bit format*) Wildcard mask indicates that we don't care about corresponding bit in network address.



OSPF is a classless protocol. With wildcard we can also filter Subnetted networks. In classes implementation usually we use Subnetted networks

For example we want to exclude serial interfaces in above configuration. We can use a wildcard mask of 0.0.0.255 to match the subnet mask of /24.

```
Router(config-router)# network 172.168.1.0 0.0.0.255
Router(config-router)# network 172.168.2.0 0.0.0.255
```

Above commands will ask router to match /24 bits of address instead of default /16 bits. Now router will look for 172.168.1.x and 172.168.2.x network. Our serial interfaces have 172.168.3.0/24 and 172.168.4.0/24 networks which do not fall in these search criteria.

Let's take one more example, if we use following network command, which interfaces would be selected.

```
Router(config-router)# network 192.168.0.0 0.0.0.3
```

In this case valid host IP addresses are 192.168.0.1 and 192.168.0.2. So any interface that has these IP address would be selected. /30 network is usually used for serial link connection which need only two valid host IP addresses; one for each end.

Summary

Command	Description
Router(config)#router opsf 10	Enable OSPF routing protocol under process ID 10.
Router(config-router)#network 10.10.0.0 0.0.255.255 area 0	Enable OSPF with area 0 on matching interface.
Router(config)#interface loopback 0	Create a Loopback interface and move in sub interface configuration mode
Router(config-if)#ip address 192.168.250.250 255.255.255.0	Assign IP address to loopback interface.
Router(config-router)#router-id 1.1.1.1	Set 1.1.1.1 as router ID
Router(config)#interface serial 0/0	Inter in sub interface configuration mode
Router(config-if)#ip ospf priority 100	Used to influence DR/BDR selection process. Valid range is 0 to 255. 0 makes router ineligible for DR/BDR while 255 makes router guaranteed DR/BDR. Higher priority value means higher chance of becoming DR/BDR.
Router(config-if)#bandwidth 256	Used to influence route metric cost. Cost is the inverse of bandwidth. Higher bandwidth has lower cost. Bandwidth is defined in Kbps. 256 means 256 Kbps.
Router(config-if)#ip ospf hello-interval timer 15	Set hello interval timer to 15 seconds. Hello timer must be match on both routers in order become neighbors.
Router(config-if)#ip ospf dead-interval 60	Set dead interval timer to 60 seconds. Dead interval timer must be match on both routers in order to become neighbor
Router#show ip route	Display all routes from routing table
Router#show ip route ospf	Display all routers learned through OSPF from routing table
Router#show ip ospf	Display basic information about OSPF
Router#show ip ospf interface	Display information about all OSPF active interfaces

Router#show ip ospf interface serial 0/0/0	Display OSPF information about serial 0/0/0 interface
Router#show ip ospf neighbor List all	OSPF neighbors with basic info
Router#show ip ospf neighbor detail	List OSPF neighbors with detail info
Router#show ip ospf database	Display data for OSPF database
Router#clear ip route *	Clear all routes from routing table.
Router#clear ip route 10.0.0.0/8	Clear particular route from routing table
Router#clear ip ospf counters	Clear OSPF counters
Router#debug ip ospf events	Display all ospf events
Router#debug ip ospf packets	Display exchanged OSPF packets
Router#debug ip ospf adjacency	Display DR/BDR election process state

VLAN

What is VLAN

VLAN is a logical grouping of networking devices. When we create VLAN, we actually break large broadcast domain in smaller broadcast domains. Consider VLAN as a subnet. Same as two different subnets cannot communicate with each other without router, different VLANs also requires router to communicate.

Advantage of VLAN

VLAN provides following advantages:-

- Solve broadcast problem
- Reduce the size of broadcast domains
- Allow us to add additional layer of security
- Make device management easier
- Allow us to implement the logical grouping of devices by function instead of location

VLAN Membership

VLAN membership can be assigned to a device by one of two methods

1. Static
2. Dynamic

These methods decide how a switch will associate its ports with VLANs.

VLAN Connections

During the configuration of VLAN on port, we need to know what type of connection it has.

Switch supports two types of VLAN connection

1. Access link
2. Trunk link

Access Link and Trunk Link

An access link can carry single VLAN information while trunk link can carry multiple VLANs information. Configuring VLANs on single switch does not require trunk link. It is required only when you configure VLANs across the multiple switches.

Trunk link connections are used to connect multiple switches sharing same VLANs information.

- An access link can carry single VLAN information.
- Theoretically we can use access link to connect switches.
- If we use access link to connect switches, we have to use links equal to VLANs.
- Due to scalability we do not use access link to connect the switches.
- A trunk link can carry multiple VLAN information.
- Practically we use trunk links to connect switches.

- **N A T – P A T**

Basic Concepts of NAT

This assignment explains basic concepts of static NAT, dynamic NAT, PAT, inside local, outside local, inside global and outside global in detail with examples.

- **Basic overview of NAT**

  There are several situations where we need address translation such as, a network which do not have sufficient public IP addresses want to connect with the Internet, two networks which have same IP addresses want to merge or due to security reason a network want to hide its internal IP structure from the external world. NAT (Network Address Translation) is the process which translates IP address. NAT can be performed at firewall, server and router. In this assignment we will understand how it is performed at Cisco router.

- **NAT Terminology**

  Before we understand NAT in details let's get familiar with four basic terms used in NAT.

Term	Description
Inside Local IP Address	Before translation source IP address located inside the local network.
Inside Global IP Address	After translation source IP address located outside the local network.
Outside Global IP Address	Before translation destination IP address located outside the remote network.
Outside Local IP Address	After translation destination IP address located inside the remote network.

Types of NAT

There are three types of NAT; Static NAT, Dynamic NAT and PAT. These types define how inside local IP address will be mapped with inside global IP address.

Static NAT

In this type we manually map each inside local IP address with inside global IP address. Since this type uses one to one mapping we need exactly same number of IP address on both sides.

Dynamic NAT

In this type we create a pool of inside global IP addresses and let the NAT device to map inside local IP address with the available outside global IP address from the pool automatically.

PAT

In this type a single inside global IP address is mapped with multiple inside local IP addresses using the source port address. This is also known as PAT (Port Address Translation) or NAT over load. Situations where NAT is used

There are no hard and fast rules about where we should use NAT or where we should not use the NAT. Whether we should use the NAT or not is purely depends on network requirement for example NAT is the best solution in following situations: -

 Our network is built with private IP addresses and we want to connect it with internet. As we know to connect with internet we require public IP address. In this situation we can use NAT device which will map private IP address with public IP address.

 Two networks which are using same IP address scheme want to merge. In this situation NAT device is used to avoid IP overlapping issue.

 We want to connect multiple computers with internet through the single public IP address. In this situation NAT is used to map the multiple IP addresses with single IP address through the port number.

Conclusion: We have successfully configured VLAN, OSPF Protocol & NAT_PAT.