Name : Aditya Somani Roll No: T1851061 PRN NO:71901204L

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)

Title of the Assignment: Using a Network Simulator (e.g. packet tracer) configure VLAN protocol

---

Objective of the Assignment: To understand Switches applying VLAN configuration

---

Prerequisite: Students must have knowledge of Packet tracer simulator.

Theory :

What is VLAN?

Theory:

A **VLAN** is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because **VLANs** are based on logical instead of physical connections, they are extremely flexible.

Any port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in that VLAN. Each VLAN is considered a logical network. Packets destined for stations that do not belong to the VLAN must be forwarded through a router

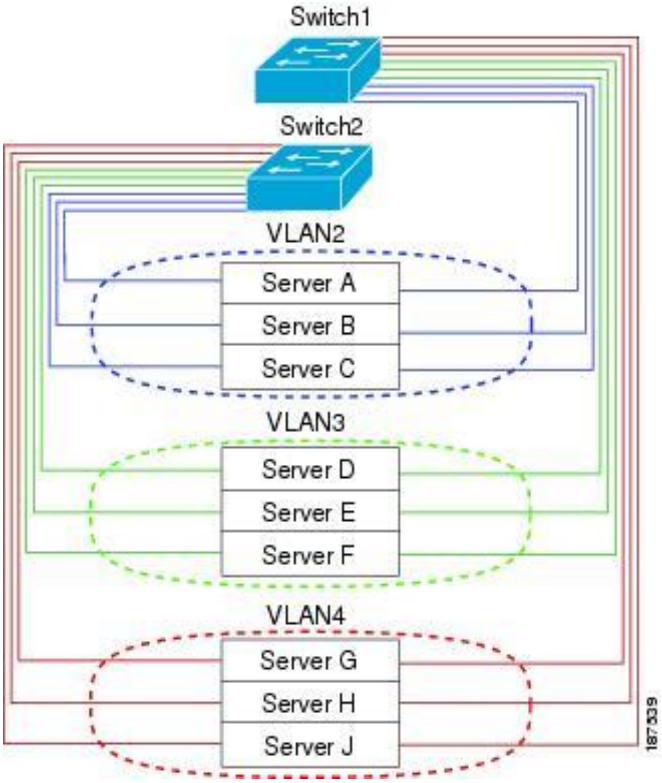


Figure 1: VLANs as Logically Defined Networks

VLANs are usually associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. To communicate between VLANs, you must route the traffic.

By default, a newly created VLAN is operational; that is, the VLAN is in the no shutdown condition. Additionally, you can configure VLANs to be in the active state, which is passing traffic, or the suspended state, in which the VLANs are not passing packets. By default, the VLANs are in the active state and pass traffic.

VLAN table ranges:

	Range	Usage
1	Normal	Cisco default. You can use this VLAN, but you cannot modify or delete it.
2—1005	Normal	You can create, use, modify, and delete these VLANs.
1006—4094	Extended	You can create, name, and use these VLANs. You cannot change the following parameters: • State is always active. • VLAN is always enabled. You cannot shut down these VLANs.

3968—4047 and 4094	Internally allocated	These 80 VLANs, plus VLAN 4094, are allocated for internal use. You cannot create, delete, or modify any VLANs within the block reserved for internal use.

VLAN Configuration Commands

Table 1 lists the base commands used to create a VLAN on a switch.

Table 1

Adding a VLAN Directly and Entering into VLAN Configuration Mode

Step	Actions	Commands
1	Enter global configuration mode.	switch#**configure terminal**
2	Enter VLAN configuration mode and/or create a VLAN.	switch(config)#**vlan***vlan-id*
3	Configure a name for the VLAN.	switch(config-vlan)#**name***name*

NOTE

The VLAN isn't added until you leave VLAN configuration mode.

Table 2 shows another method of creating a VLAN: assigning an interface into a VLAN.

Table 2

Assigning the VLAN to a Switchport (and Possibly Creating a New VLAN)

Step	Actions	Commands
1	Enter global configuration mode.	switch#**configure terminal**
2	Enter interface configuration mode.	switch(config)#**interface***interface*
3	Configure the interface into a specific VLAN. (If the VLAN doesn't exist, it will be created.)	switch(config-if)#**switchport access vlan***vlan-id*

On the flipside, use the commands shown in Table 3 to delete a VLAN.

Table 3

Deleting a VLAN

Step	Actions	Commands
1	Enter global configuration mode.	switch#**configure terminal**
2	Delete a configured VLAN. If an interface is configured into the VLAN being deleted, it will become inactive and will not be displayed in the output of the **show vlan** command.	switch(config)#**no vlan***vlan-id*

To verify VLAN assignment, use the command shown in Table 4.

Table 4

1. *Verifying Existing VLANs*

Step	Action	Command
1	Display the current VLANs and their assignments.	switch#**showvlan** [**brief**]

Table 5

2. *VLAN Configuration*

Step	Actions	Commands
1	Enter global configuration mode.	switch#**configure terminal**
2	Create VLAN 100.	switch(config)#**vlan 100**

3	Create VLAN 200. Notice that the configuration mode changed to VLAN configuration mode (config-vlan), but this command is still configured as if the user is in global configuration mode.	switch(config-vlan)#**vlan 200**
4	Move into interface configuration mode for switchports Fast Ethernet 0/1–0/12.	switch(config-vlan)#**interface range fastethernet0/1-12**
5	Configure the switchports into VLAN 100.	switch(config-if)#**switchport access vlan 100**
6	Move into interface configuration mode for the switchports Fast Ethernet 0/13–0/24.	switch(config-if)#**interface range fastethernet0/13-24**
7	Configure the switchports into VLAN 200.	switch(config-if)#**switchport access vlan 200**

MODES IN VLAN :

There are 3 modes :

1) Access
2) Dynamic
3) Trunk

By default, all ports are configured **as switchport mode dynamic desirable**, which means that if the port is connected to another switch with an port configured with the same default mode (or desirable or auto), this link will become a trunking link.

When the **switchport access vlan command** is used, the switchport mode access command is not necessary since the switchport access vlan command configures the interface **as an "access"** port (non-trunk port).

SHOW Commands in VLAN:

Command	Command Mode	Purpose
show	VLAN configuration	Display status of VLANs in the VLAN database.
show current [*vlan-id*]	VLAN configuration	Display status of all or the specified VLAN in the VLAN database.
show interfaces [**vlan**vlan-id]	Privileged EXEC	Display characteristics for all interfaces or for the specified VLAN configured on the switch.
show running-configvlan	Privileged EXEC	Display all or a range of VLANs on the switch.
show vlan[**id** vlan-id]	Privileged EXEC	Display parameters for all VLANs or the specified VLAN on the switch.

```
SydneySwitch#show vlan

VLAN Name                Status    Ports
---- ------------------- ------- -------------------------------

VLAN Name                Status    Ports
---- ------------------- ------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2               active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3               active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                   Fa0/12
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active

VLAN Type SAID MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ---- ---- ---- ------ ------ -------- ---------- ------ -------
1    enet 100001 1500  -      -      -        -   -     1002   1003
2    enet 100002 1500  -      -      -        -   -     0      0
```

```
SydneySwitch#show vlan brief

VLAN Name                    Status    Ports
---- ----------------------- --------- -------------------------------
1    default                 active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                   active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                   active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                       Fa0/12
1002 fddi-default            active
1003 token-ring-default      active
1004 fddinet-default         active
1005 trnet-default           active
```

vlan database commands

- Optional Command to add, delete, or modify VLANs.
- VLAN names, numbers, and VTP (VLAN Trunking Protocol) information can be entered which “may” affect other switches besides this one. (Discussed later).
- This does not assign any VLANs to an interface.

Switch#vlan database

Switch(vlan)#?

VLAN database editing buffer manipulation commands:

abort Exit mode without applying the changes

apply Apply current changes and bump revision number

exit Apply changes, bump revision number, and exit mode

no Negate a command or set its defaults

reset Abandon current changes and reread current database

showShow database information

vlan Add, delete, or modify values associated with a single VLAN

vtp Perform VTP administrative functions.

Deleting a Port VLAN Membership

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#no switchport access vlan 300
```

Switch(config-if)#no switchport access vlanvlan_number

Deleting a VLAN

Switch**#vlan database**

Switch(vlan)#No vlanvlan_number

Switch(vlan)#exit

Benefits of VLANs:

- The key benefit of VLANs is that they permit the network administrator to organize the LAN
- logically instead of physically.

- This means that an administrator is able to do all of the following:
- Easily move workstations on the LAN.
- Easily add workstations to the LAN.
- Easily change the LAN configuration.
- Easily control network traffic.
- Improve security.

VLANs also have some disadvantages and limitations as listed below:

- High risk of virus issues because one infected system may spread a virus through the whole logical network
- Equipment limitations in very large networks because additional routers might be needed to control the workload
- More effective at controlling latency than a WAN but less efficient than a LAN

Conclusion: Students have successfully understood the concept of VLAN configuration with its commands.

Title of the Assignment: Using a Network Simulator (e.g. packet tracer) configure DTP protocol

---

Objective of the Assignment: To understand trunking and different modes to access the connection between two switches.

Prerequisite: Students must have knowledge of Packet tracer simulator.

Theory :

What is Trunking ?

- A trunk is a physical and logical connection between two switches across which network traffic travels.
- A trunk may be a physical or logical connection between devices.
- A trunk is a point-to-point link capable of supporting multiple VLAN's.
- Trunking will bundle multiple virtual links over one physical link by allowing the traffic for several VLAN's to travel over a single cable between the switches.

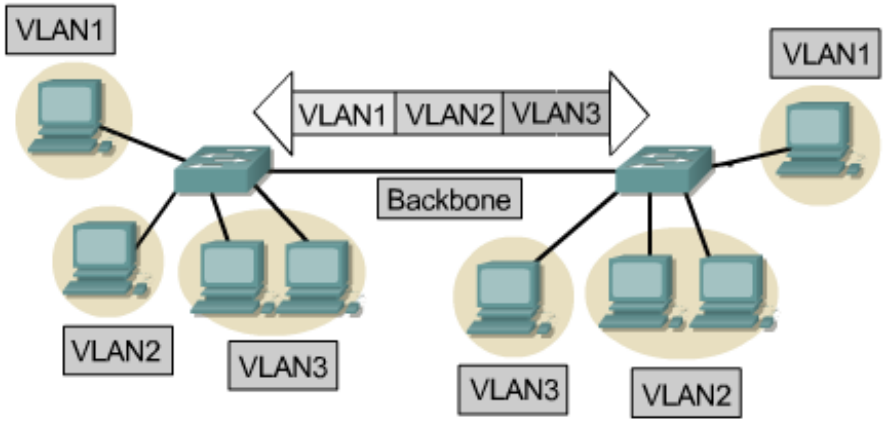


Fig : Multiple Virtual links

Trunking operation:-

- **Two main methods are used to enable trunking:**
  - **Cisco proprietary protocol, Inter-Switch Link (ISL)**
  - **IEEE 802.1q**
- **Both use frame-tagging to identify multiple VLAN information to pass on a single trunk link.**

1) ISL :-

- Cisco's proprietary method of frame-tagging.
- Encapsulates the Ethernet frame with information that contains the VLAN ID.
- Only used on Cisco devices.

2) IEEE 802.1q :-

- IEEE 802.1q is the open standard Trunking protocol used by most switches.
- Places a unique identifier in the header to identify which VLAN a frame is communicating on.
- The ID is removed when the frame reaches it's final switch destination.

What is DTP?

The **Dynamic Trunking Protocol** (DTP) is a proprietary networking **protocol** developed by Cisco Systems for the purpose of negotiating **trunking** on a link between two VLAN-aware switches, and for negotiating the type of **trunking** encapsulation to be used. It works on Layer 2 of the OSI model.

VLAN trunks formed using DTP may utilize either IEEE 802.1Q or Cisco ISL trunking protocols.

DTP should not be confused with VTP, as they serve different purposes. VTP communicates VLAN existence information between switches. DTP aids with trunk port establishment. Neither protocol transmits the data frames that trunks carry.

Switch port modes

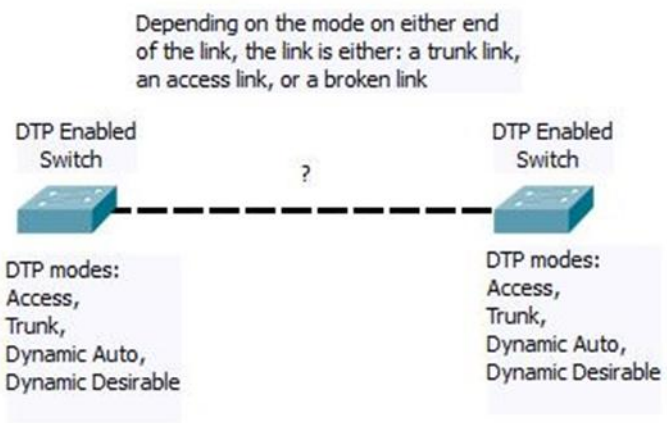


Fig : Modes between two switches

The following switch port mode settings exist:

- ***Access*** — Puts the Ethernet port into **permanent nontrunking** mode and negotiates to convert the link into a nontrunk link. The Ethernet port becomes a nontrunk port even if the neighboring port does not agree to the change.
- ***Trunk***— Puts the Ethernet port into **permanent trunking** mode and negotiates to convert the link into a trunk link. The port becomes a trunk port even if the neighboring port does not agree to the change.
- ***Dynamic Auto***— Makes the **Ethernet port willing to convert** the link to a trunk link. The port becomes a trunk port if the neighbouring port is set to trunk or *dynamic desirable* mode. This is the default mode for all Ethernet ports.

- ***Dynamic Desirable*** — Makes the **port actively attempt to convert** the link to a trunk link. The port becomes a trunk port if the neighbouring Ethernet port is set to trunk, *dynamic desirable*, or *dynamic auto* mode.
- ***Nonegotiate***— **Disables DTP.** The port will not send out DTP frames or be affected by any incoming DTP frames. If you want to set a trunk between two switches when DTP is disabled, you must manually configure trunking using the (switchport mode trunk) command on both sides.

DTP auto-negotiation resulting link states				
Port Mode	Access	Trunk	Dynamic Auto	Dynamic Desirable
Access	*access*	*not recommended*	*access*	*access*
Trunk	*not recommended*	*trunk*	*trunk*	*trunk*
Dynamic Auto	*access*	*trunk*	*access*	*trunk*
Dynamic Desirable	*access*	*trunk*	*trunk*	*trunk*

Fig :DTP auto-negotiation resulting link states

DTP Trunk and Access Modes

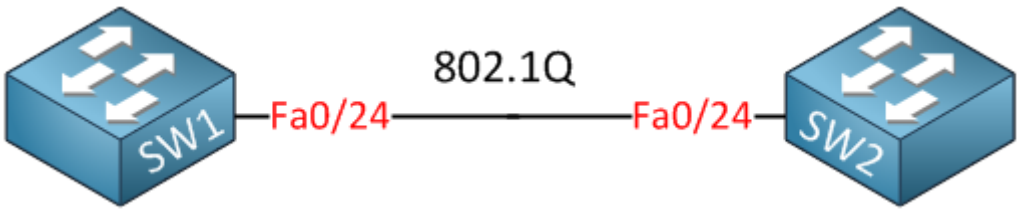


Figure : DTP configuration

Switch(config-if)#**switchport mode access** – Sets trunking **OFF**

Switch(config-if)#**switchport mode trunk** – Sets trunking **ON**

Figure 2

Switch(config)#**inter fa 0/24**

Switch(config-if)#**switchport trunk encapsulation dot1q**

Switch(config-if)#**switchport mode trunk**

Using the **switchport mode** interface command, two of the DTP modes set trunking to "off" or "on".

Access mode

For example, Switch1 and Switch2 are connected on their FastEthernet 0/24 interfaces. If both switches are set to **access** mode, then the link is a non-trunking link. Both interfaces must be on the same VLAN and only that single VLAN is transmitted across the link.

Switch1(config)#**inter fa 0/24**

Switch1(config-if)#**switchport mode access**

Switch2(config)#**inter fa 0/24**

Switch2(config-if)#**switchport mode access**

Trunk mode

If both switches are set to **trunk** mode, then the link is a trunking link. By default, all VLANs will be transmitted across this trunk.

Switch1(config)#**inter fa 0/24**

Switch1(config-if)#**switchport mode trunk**

Switch2(config)#**inter fa 0/24**

Switch2(config-if)#**switchport mode trunk**

SHOW Commands for DTP :

SW1#show interfaces fa0/24 switchport

Name: Fa0/24

Switchport: Enabled

Administrative Mode: dynamic auto

Operational Mode: static access

Administrative Trunking Encapsulation: negotiate

Operational Trunking Encapsulation: native

Negotiation of Trunking: On

SW2#show interfaces fastEthernet 0/24 switchport

Name: Fa0/24

Switchport: Enabled

Administrative Mode: dynamic auto

Operational Mode: static access

Administrative Trunking Encapsulation: negotiate

Operational Trunking Encapsulation: native

Negotiation of Trunking: On

Without configuring anything on the interfaces, we are using dynamic auto mode and as a result the interfaces are in access mode.

Depending on the switch model and IOS version, the default might be “dynamic auto” or “dynamic desirable”.

Nonegotiate mode operation

The switchportnonegotiate interface command stops DTP negotiation packets sending and engaging in trunk election. This command is valid only when the interface switch port mode is access or trunk. This command returns an error if you attempt to execute it in dynamic (auto or desirable) mode. When in nonegotiate configuration, the port trunks only if the other end of the link is specifically set to trunk. The switchportnonegotiate command does not form a trunk link with ports in either dynamic desirable or dynamic auto mode.

There are two ways to disable DTP negotiation:

- Configure the interface for access mode.
- Use the switchportnonegotiate command on the interface.

Configuring the interface for trunking does not disable DTP negotiation, let me give you an example. First we'll configure the interfaces for access mode:

SW1(config)#**interface fastEthernet 0/24**

SW1(config-if)#switchport mode access

SW2(config)#**interface fastEthernet 0/24**

SW2(config-if)#switchport mode access

When we look again at the switchport settings we can see that DTP negotiation is now disabled:

SW1#**show interfaces fastEthernet 0/24 switchport**

Name: Fa0/24

Switchport: Enabled

Administrative Mode: static access

Operational Mode: static access

Administrative Trunking Encapsulation**: negotiate**

Operational Trunking Encapsulation: native

Negotiation of Trunking: Off

Conclusion: -Thus wepractically performed the trunking between two switches and also implemented various commands for trunking.

Assignment Name: STP

Title of the Assignment: Using a Network Simulator (e.g. packet tracer) configure STP protocol

---

Objective of the Assignment: To understand multiple protocols on same network

---

Prerequisite: Students must have knowledge of Packet tracer simulator.

Theory :

What is STP?

STP is a derivative of network redundancy which is very common in business networks. Let me explain it the simple way.

Suppose you have a situation where you need to connect two switches in your office network, and then you decide to put two connection cables between the switches so that in case if any one of the link fails then the other one can take over (network switch redundancy). This is the simplest redundancy scenario and it'll look like this.

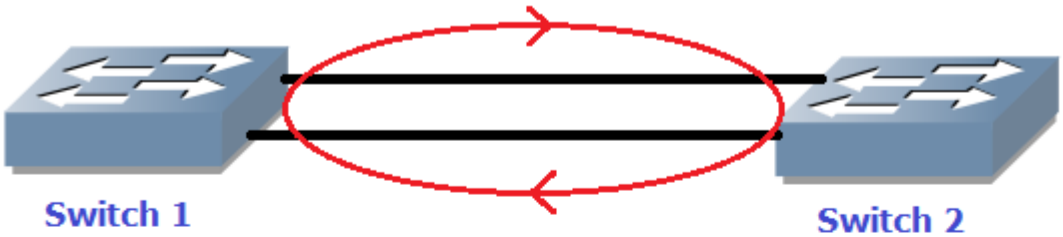


Diagram 1

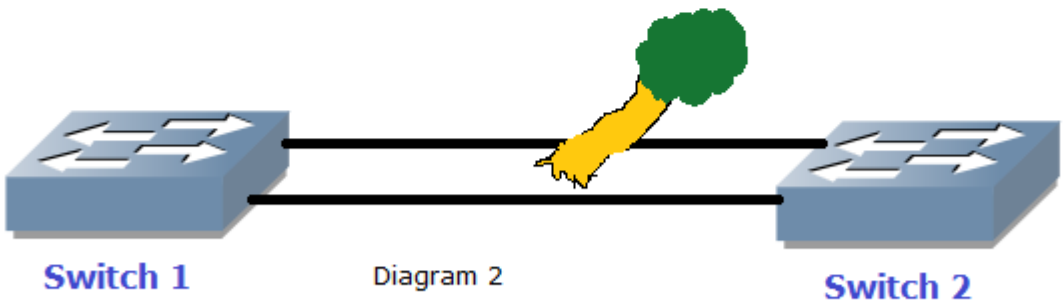
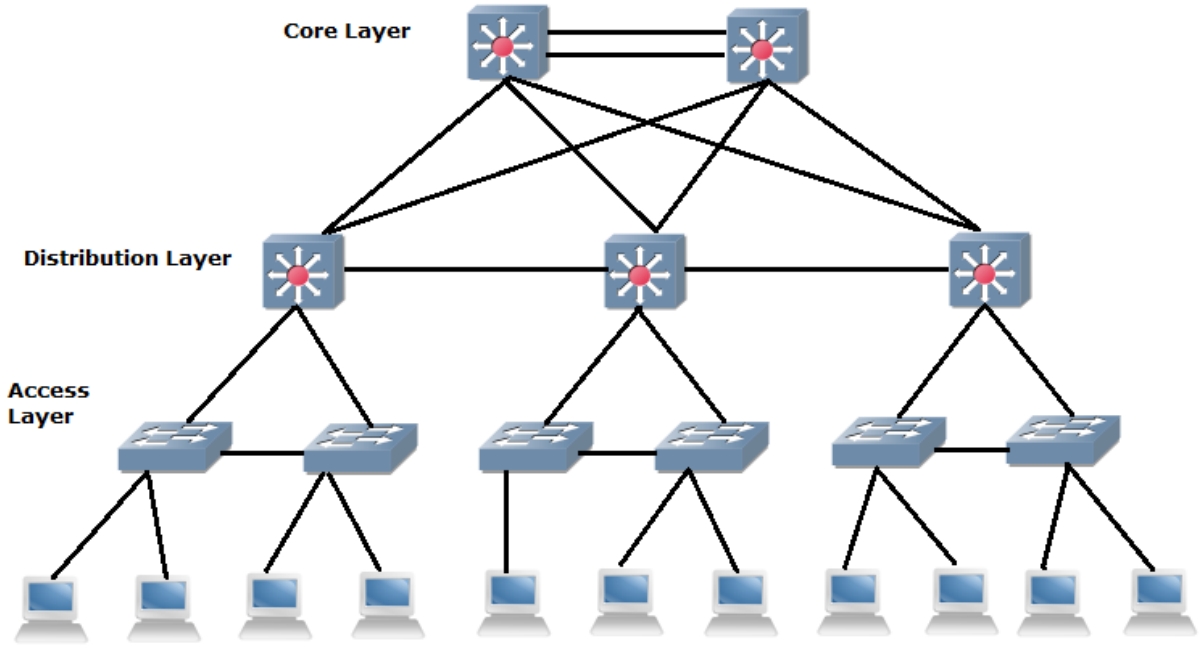


Diagram 2

However, in these cases there's a possibility that data frame units may loop around the network continuously causing overload to the processors [Diagram 1]. This is where

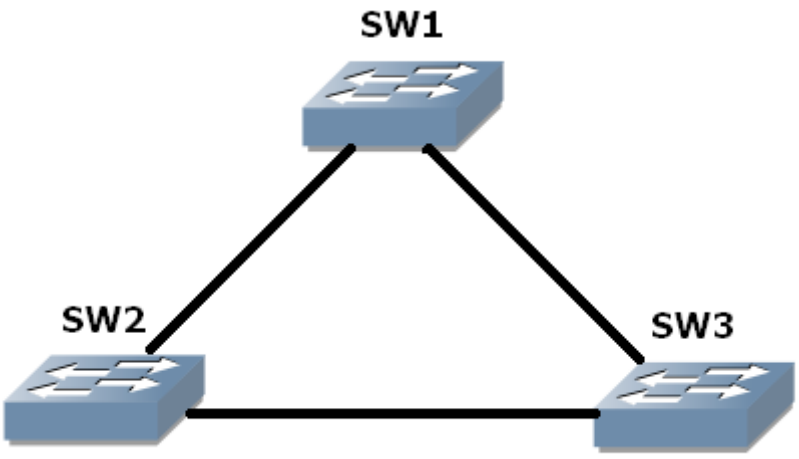
spanning tree comes into action. It was developed in order to avoid these looping, by temporarily blocking the redundant links [Diagram 2] and enabling them only when the active links are down.

Here's a typical redundant network topology.



How does STP work?

There's a whole bunch of processes taking place inside the STP switch for convergence. Let's see them in detail by taking the simple network topology below. Our aim is to break up any one of the link logically thus avoiding the loop.



- All the switches in the network multicast **BPDU**'s (Bridge Protocol Data Unit) to discover if there are any loops out there. BPDU's are data frames that contain STP parameters.
- If a switch receives back its own BPDU, it establishes that there are loops in the network.

After the discovery of loops there are a series of elections going on between the switches. Let's study them step by step.

Election of Root Bridge

- Each switch has a Bridge ID which is a combination of its priority value and MAC address. The priority can be any value between 0-65535. By default the priority value of switches are 32768.

  Bridge ID= Priority Value + MAC Address

- The switches then compare their **Bridge IDs and the one with the lowest value is chosen as the root bridge** (reference switch for all path calculation).

Note: Lower priority value/older MAC address has higher chances to become root bridge.

Election of root ports

- Root ports are the best ways to reach the root switch. It's calculated on the basis of port cost which depends on the bandwidth of the link. You can see the STP cost for different bandwidth below as given by IEEE

Link Speed(Bandwidth)	Port Cost
10 mbps	100
100 bmps	19
1 gbps	4
10 gbps	2

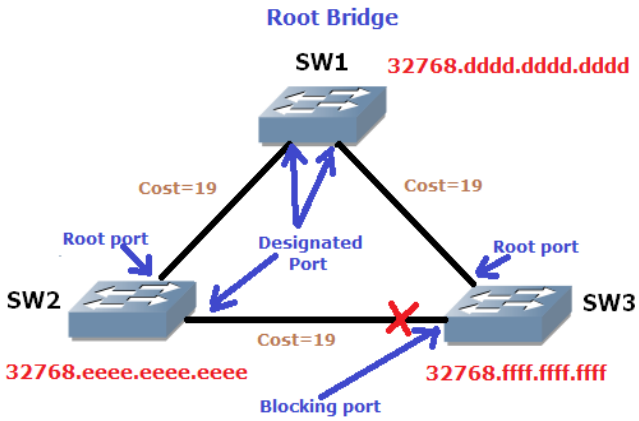
- So the port which has the least cost will be the root port.

Election of Designated port

- These are the ports that are forwarding data, and there is condition here i.e. one link can have only one designated port. All ports of the root bridge are designated ports.
- They are elected based on the lowest cost, and if there is tie there then the port of the switch which has the least bridge id becomes designated port.

Election of Non-Designated port

- All other remaining ports are the non-designate ports or blocking ports. These are the ports which prevents the loop by means of the tree (blocking).



So the effect will be a loop-free network as below.

2.1 Configuration and verification:

Everything we discussed above like the loop discovery and election process takes place automatically within the switches. You can view the switch configuration by the privilege mode command 'show spanning-tree'. Look at the screenshot below for the possible outcome. You can check 'show spanning-tree ?' to find out other verification commands.

```
Switch>enable
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.4397.A657
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.4397.A657
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p

Switch#
```

However you can change the switch priority through certain command.

There is an animation on the Cisco website regarding STP protocol, it helps a lot in understanding convergence/ election of Root Bridge. However you can change the switch priority through certain command.

Conclusion: Students have successfully implemented STP protocol.

Assignment Name : OSPF

Title of the Assignment: Using a Network Simulator (e.g. packet tracer) configure OSPF

Objective of the Assignment: To understand Link State Advertisement and how to configure OSPF protocol .

Prerequisite: Students must have knowledge of Packet tracer simulator.

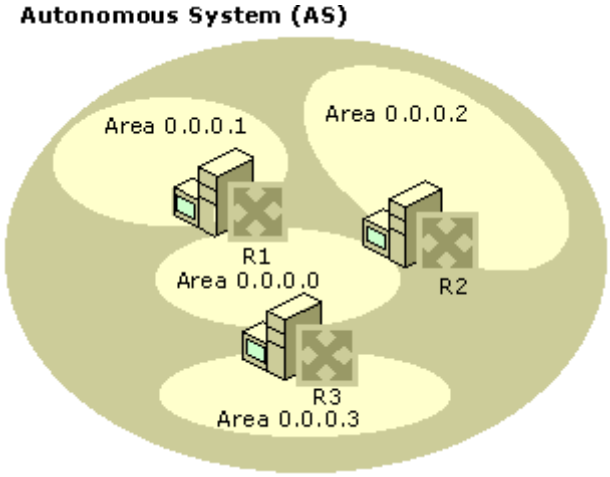
Theory: There are 2 kind classes in routing protocol viz. **Distance vector Protocol** and **Link state protocol**. OSPF stands for **Open Shortest Path First** and belongs to Link-State routing protocol. Cisco **OSPF** routing protocol is categorized as **best dynamic protocol**s that be present nowadays. It is also regarded as the advanced routing protocol that targets to maintain **loop-free** and **precise routing tables**. The important key feature of OSPF is that it is an **open source** routing protocol. It will run on most routers, since it is an open standard.

What is OSPF (Open Shortest Path First)?

- OSPF stands for Open Shortest Path First. OSPF uses **SPF algorithm** which is developed by **Dijkstra**, to deliver a loop-free topology.
- OSPF is an **open source** Link state routing protocol hence capable of running all network routers.
- It supports **VLSM** (variable Length Subnet Mask).
- Uses **COST as a metric** which CISCO explain as the inverse of the bandwidth.

- To allow measurability OSPF bears two important theories: **Autonomous systems** (Discussed in previous article) and **Areas**.
- ***What is OSPF area?*** OSPF network can be separated into **sub-domains** known as areas. An area is a **logical group** of OSPF networks, routers, and links that have the same area identification number.

- A router belong to an area should keep a topological database for the area. The router does not have enough information about network configuration external of its area, in that way reducing the size of OSPF database.



- **he default or else central area is Area 0 (Zero) and all other areas directly connected to it.**

- **Within an area OSPF router exchange LSAs (Link State Advertisements) by which routers forms adjacency. (*Time being remember LSA means routing information, I will be posting different kinds of LSAs in later, Keep in touch*)**

How OSPF Works?

By comparing to other Routing Protocol OSPF is little bit complex and hassle. But if you have the complete idea about OSPF working, it is easy to configure and Tshoot.

Now we'll go over the process of working of an OSPF protocol. While dealing with OSPF there are two important terms; Designated Router (DR) and Backup Designated Router (BDR).

What is Designated Router in OSPF?

Exchanging LSA between all routers significantly increase the traffic and reduce the response time. In an OSPF network instead of broadcasting LSA between to all routers each other, the network selects a router as Designated Router just like a master router.

<u>All other routers exchange routing information to the elected router (Designated Router)</u> only. Then Designated Router broadcasts routing information to all other routers residing at same area thereby reducing the traffic. DR serves as the central point for exchanging OSPF routing information.

What is Backup Designated Router (BDR)?

In any case DR fails BDR coming in to action. Backup Designated Router works as a stand by router for OSPF information.

When Designated Router fails, Backup Designated Router (BDR) takes over its role of spreading routing information across the OSPF area.

DR-BDR Election in OSFP Area

- **The selection process of Designated Router (DR) and Backup Designated Router (BDR) occurs at the beginning of OSPF network established.**

- **Each router in an OSPF network allotted with number called Router Identifier Number (router-id). OSPF uses this to identify DR-BDR. (Routerid can be assigned by different methods)**

- **Once the OSPF links are active router with maximum router-id (highest loopback IP) elected as DR and the router with second highest router-id chosen as BDR.**

- **What happens if the designated router fails or drops connectivity, the backup designated router turns to Designated Router and a new BDR election carried out in the OSPF domain.**

- **Process of electing DR and BDR called DR-BDR election in OSPF network.**

How to Configure OSPF in Cisco router?

OSPF Configuration syntax as follows

Router(config)#router ospf <OSPF Process number>
Router(config-router)#network <Network ID> <Wild Card Mask> area <Area number>

- ***OSPF Process number:*** Is just a number local to the router only. This value does not ensure be the same on all router within the area. Though, it is better to keep this as same for all routers inside an area for better administration.

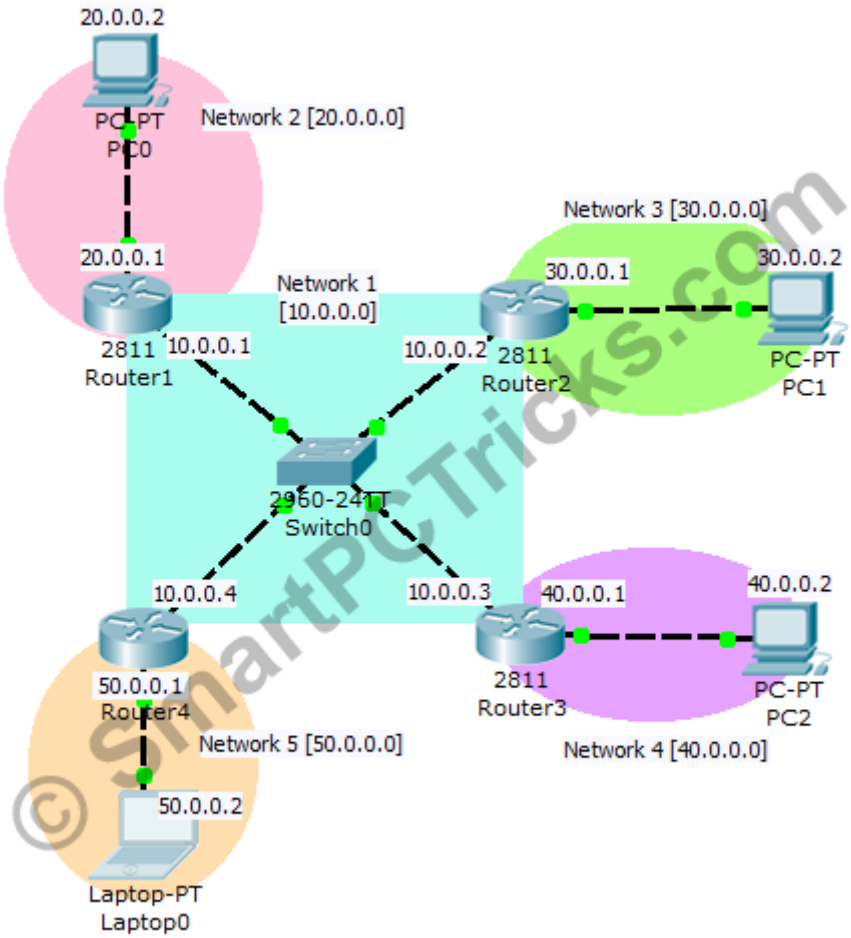
- ***Network ID:*** Is the directly connected network addres**s.**

- ***Wildcard mask:*** Is the inverse of Subnet mask

- ***Area number :*** Logical group of OSPF network.

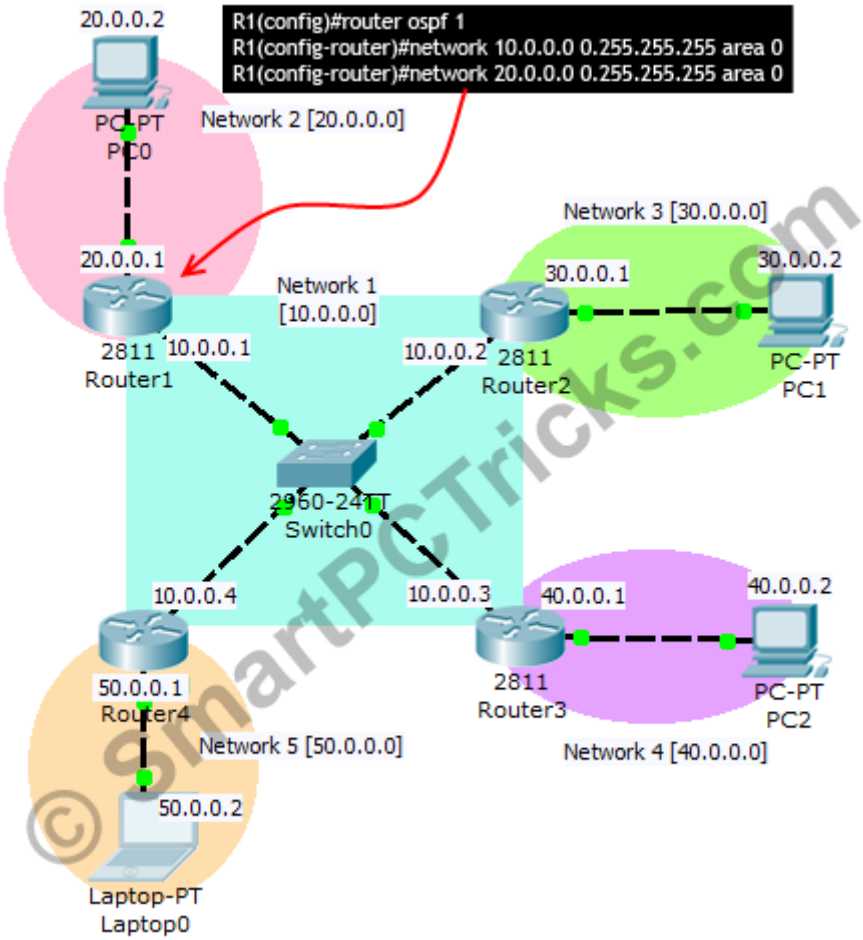
Cisco Packet Tracer OSPF Configuration Example

Let's consider the following Packet Tracer scenario for Cisco OSPF configuration examples.



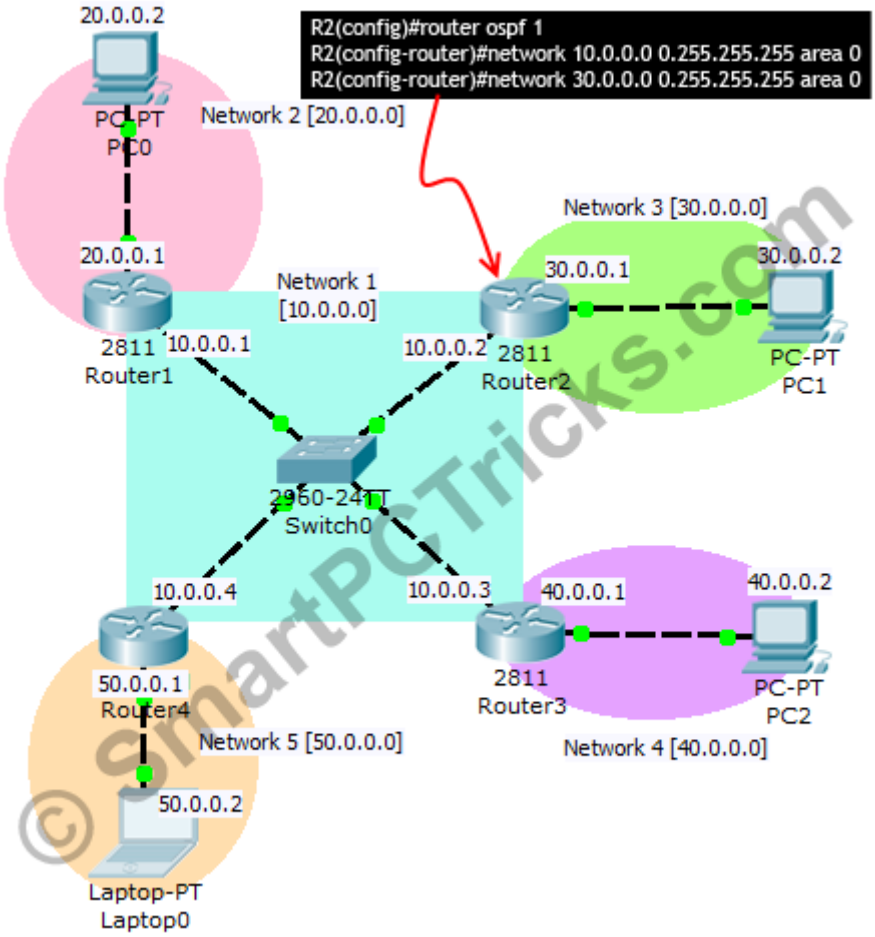
Basic Cisco OSPF configuration commands are follows, Cisco OSPF wildcard mask is used here. If you are new to wildcard mask checkout this Cisco [OSPF wildcard mask calculator tool](#)**.**

(The IP assigning configuration steps are not given in here, assign IP to each interfaces as shown in above scenario.)



OSPF configuration using packet tracer in Router 1

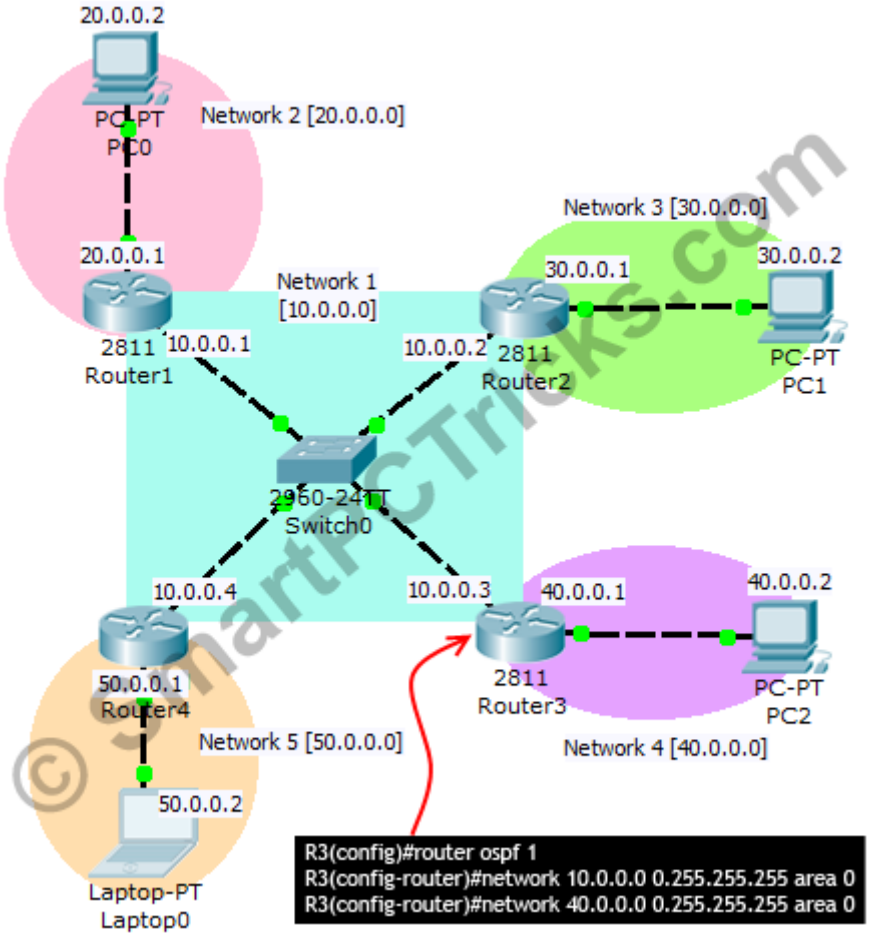
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 10.0.0.0 0.255.255.255 area 0
R1(config-router)#network 20.0.0.0 0.255.255.255 area 0
R1(config-router)#exit
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console



Cisco OSPF network command for Router 2

R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 10.0.0.0 0.255.255.255 area 0
R2(config-router)#network 30.0.0.0 0.255.255.255 area 0
R2(config-router)#exit
R2(config)#
R2#
%SYS-5-CONFIG_I: Configured from console by console

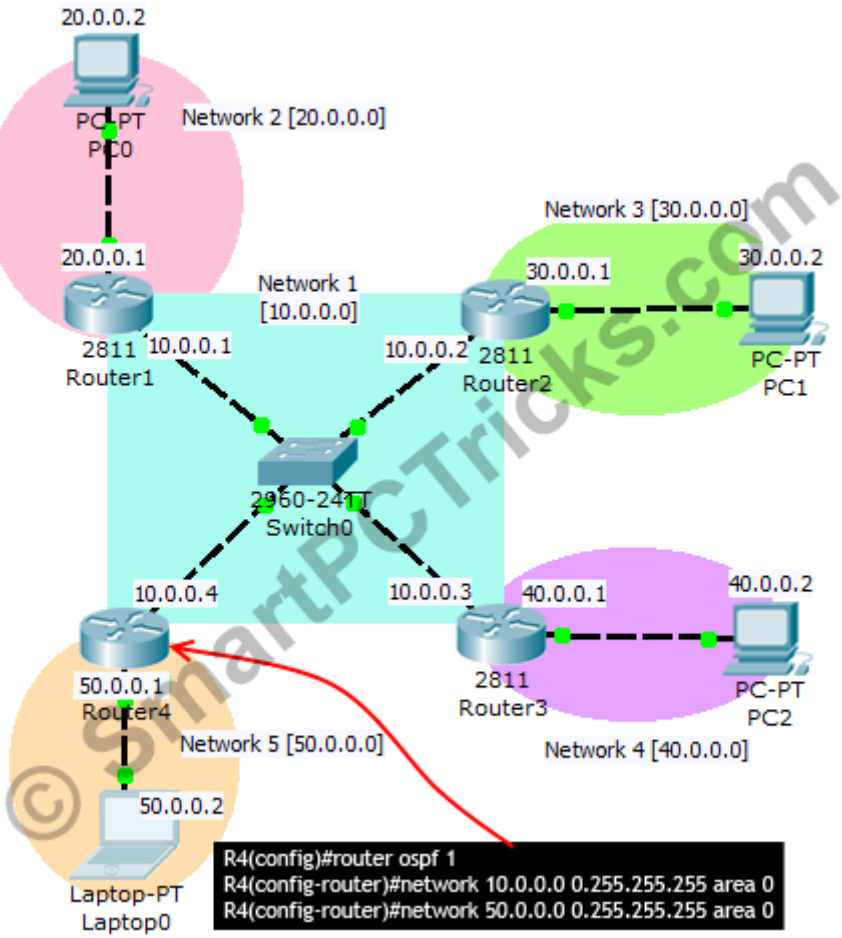
R2#



OSPF configuration examples packet tracer for Router 3

R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#network 10.0.0.0 0.255.255.255 area 0
R3(config-router)#network 40.0.0.0 0.255.255.255 area 0
R3(config-router)#exit
R3(config)#
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#



Router 4 OSPF configuration in packet tracer

R3>enable

R3#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R4(config)#router ospf 1

R4(config-router)#network 10.0.0.0 0.255.255.255 area 0

R4(config-router)#network 50.0.0.0 0.255.255.255 area 0

R4(config-router)#exit

R4(config)#

R4#

%SYS-5-CONFIG_I: Configured from console by console

R4#

- In the above example Router 4 elected as DR, because its fast Ethernet interface having IP address 50.0.0.1 which is greater than any other IP in the OSPF domain.
- The second highest IP goes to Router 3; of course Router 3 is the BDR.
- OSPF Configuration commands are completed. Do as many Cisco OSPF lab exercises that you can to get familiar with configuration. Now there are some OSPF verification commands.

—

OSPF Verification and Testing Commands

A network admin must know these commands to properly manage the topology.

#show ip ospf

List OSPF status

R1#show ip ospf
Routing Process "ospf 1" with ID 20.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE(0)
Number of interfaces in this area is 2
Area has no authentication
SPF algorithm executed 3 times
Area ranges are
Number of LSA 5. Checksum Sum 0x02f34a
Number of opaque link LSA 0. Checksum Sum 0x000000

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

—

#show ip ospf interface

Displays OSPF information associated with all available interfaces.

R1#**show ip ospf interface**

FastEthernet0/1 is up, line protocol is up

Internet address is 20.0.0.1/8, Area 0

Process ID 1, Router ID 20.0.0.1, Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 20.0.0.1, Interface address 20.0.0.1

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:00

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

FastEthernet0/0 is up, line protocol is up

Internet address is 10.0.0.1/8, Area 0

Process ID 1, Router ID 20.0.0.1, Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DROTHER, Priority 1

Designated Router (ID) 50.0.0.1, Interface address 10.0.0.4

Backup Designated Router (ID) 40.0.0.1, Interface address 10.0.0.3

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:00

Index 2/2, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 3, Adjacent neighbor count is 2

Adjacent with neighbor 50.0.0.1 (Designated Router)

Adjacent with neighbor 40.0.0.1 (Backup Designated Router)

Suppress hello for 0 neighbor(s)

R1#

#show ip ospf interface <interface name>

To show OSPF information associated a specific interface

R1#show ip ospf interface fastEthernet 0/0

FastEthernet0/0 is up, line protocol is up

Internet address is 10.0.0.1/8, Area 0

Process ID 1, Router ID 20.0.0.1, Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DROTHER, Priority 1

Designated Router (ID) 50.0.0.1, Interface address 10.0.0.4

Backup Designated Router (ID) 40.0.0.1, Interface address 10.0.0.3

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:02

Index 2/2, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 3, Adjacent neighbor count is 2

Adjacent with neighbor 50.0.0.1 (Designated Router)

Adjacent with neighbor 40.0.0.1 (Backup Designated Router)

Suppress hello for 0 neighbor(s)

R1#

—

#debug ip ospf events

Displays OPSF events

R1#debug ip ospf events
OSPF events debugging is on
R1#
00:08:20: OSPF: Rcv hello from 40.0.0.1 area 0 from FastEthernet0/0 10.0.0.3

00:08:20: OSPF: End of hello processing

00:08:20: OSPF: Rcv hello from 50.0.0.1 area 0 from FastEthernet0/0 10.0.0.4

00:08:20: OSPF: End of hello processing

00:08:20: OSPF: Rcv hello from 30.0.0.1 area 0 from FastEthernet0/0 10.0.0.2

00:08:20: OSPF: End of hello processing

R1#

—

#show ip ospf neighbor

Shows OSPF neighbor network and its state (DR-BDR)

R1#**show ip ospf neighbor**

Neighbor ID Pri State Dead Time Address Interface

40.0.0.1 1 FULL/BDR 00:00:30 10.0.0.3 FastEthernet0/0

50.0.0.1 1 FULL/DR 00:00:30 10.0.0.4 FastEthernet0/0

30.0.0.1 1 2WAY/DROTHER 00:00:30 10.0.0.2 FastEthernet0/0

R1#

—

#show ip ospf neighbor detail

View all OSPF neighbor details

R1#show ip ospf neighbor detail

Neighbor 40.0.0.1, interface address 10.0.0.3

In the area 0 via interface FastEthernet0/0

Neighbor priority is 1, State is FULL, 7 state changes

DR is 10.0.0.4 BDR is 10.0.0.3

Options is 0x00

Dead timer due in 00:00:39

Neighbor is up for 00:13:50

Index 1/1, retransmission queue length 0, number of retransmission 0

First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)

Last retransmission scan length is 0, maximum is 0

Last retransmission scan time is 0 msec, maximum is 0 msec

Neighbor 50.0.0.1, interface address 10.0.0.4

In the area 0 via interface FastEthernet0/0

Neighbor priority is 1, State is FULL, 5 state changes

DR is 10.0.0.4 BDR is 10.0.0.3

Options is 0x00

Dead timer due in 00:00:39

Neighbor is up for 00:13:50

Index 2/2, retransmission queue length 0, number of retransmission 0

First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)

Last retransmission scan length is 0, maximum is 0

Last retransmission scan time is 0 msec, maximum is 0 msec

Neighbor 30.0.0.1, interface address 10.0.0.2

In the area 0 via interface FastEthernet0/0

Neighbor priority is 1, State is 2WAY, 8 state changes

DR is 10.0.0.4 BDR is 10.0.0.3

Options is 0x00

Dead timer due in 00:00:39

Neighbor is up for 00:13:50

Index 3/3, retransmission queue length 0, number of retransmission 0

First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)

Last retransmission scan length is 0, maximum is 0

Last retransmission scan time is 0 msec, maximum is 0 msec

R1#

—

#clear ip ospf process

Resets full OSPF process, pushing OSPF to rebuild neighbors, database, and routing table

R1#clear ip ospf process
Reset ALL OSPF processes? [no]: no

R1#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

00:17:16: %OSPF-5-ADJCHG: Process 1, Nbr 40.0.0.1 on FastEthernet0/0 from FULL to DOWN, Neighbor Down: Adjacency forced to reset

00:17:16: %OSPF-5-ADJCHG: Process 1, Nbr 50.0.0.1 on FastEthernet0/0 from FULL to DOWN, Neighbor Down: Adjacency forced to reset

00:17:16: %OSPF-5-ADJCHG: Process 1, Nbr 30.0.0.1 on FastEthernet0/0 from 2WAY to DOWN, Neighbor Down: Adjacency forced to reset

00:17:16: %OSPF-5-ADJCHG: Process 1, Nbr 40.0.0.1 on FastEthernet0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

00:17:16: %OSPF-5-ADJCHG: Process 1, Nbr 50.0.0.1 on FastEthernet0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

00:17:16: %OSPF-5-ADJCHG: Process 1, Nbr 30.0.0.1 on FastEthernet0/0 from 2WAY to DOWN, Neighbor Down: Interface down or detached

R1#
00:17:20: %OSPF-5-ADJCHG: Process 1, Nbr 50.0.0.1 on FastEthernet0/0 from LOADING to FULL, Loading Done

00:17:20: %OSPF-5-ADJCHG: Process 1, Nbr 40.0.0.1 on FastEthernet0/0 from LOADING to FULL, Loading Done

R1#

#show ip ospf database

Displays OSPF database

R1#show ip ospf database
OSPF Router with ID (20.0.0.1) (Process ID 1)

Router Link States (Area 0)

Link ID ADV Router Age Seq# Checksum Link count
20.0.0.1 20.0.0.1 404 0x80000004 0x0042a7 2
50.0.0.1 50.0.0.1 404 0x80000004 0x00e1aa 2
40.0.0.1 40.0.0.1 399 0x80000004 0x00f1b9 2
30.0.0.1 30.0.0.1 399 0x80000004 0x0002c8 2

Net Link States (Area 0)
Link ID ADV Router Age Seq# Checksum
10.0.0.4 50.0.0.1 399 0x80000003 0x00da78
R1#

#show ip protocols

To know which routing protocol is enabled in specific router

R1#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 20.0.0.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
20.0.0.0 0.255.255.255 area 0
10.0.0.0 0.255.255.255 area 0
Routing Information Sources:
Gateway Distance Last Update
20.0.0.1 110 00:10:20
30.0.0.1 110 00:10:20
40.0.0.1 110 00:10:20
50.0.0.1 110 00:10:20
Distance: (default is 110)

R1#

#show ip route

Shows the routing table of router

R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

*** - candidate default, U - per-user static route, o - ODR**
P - periodic downloaded static route

Gateway of last resort is not set

C 10.0.0.0/8 is directly connected, FastEthernet0/0
C 20.0.0.0/8 is directly connected, FastEthernet0/1
O 30.0.0.0/8 [110/2] via 10.0.0.2, 00:11:15, FastEthernet0/0
O 40.0.0.0/8 [110/2] via 10.0.0.3, 00:11:15, FastEthernet0/0
O 50.0.0.0/8 [110/2] via 10.0.0.4, 00:11:15, FastEthernet0/0
R1#

How to Set Priority for a Router Becomes DR-BDR?

- **Network Administrator can manually assign priority for routers belong to an area by using OSPF priority VALUE configuration command [Router(config-if)#ip ospf priority priority-value]**
- **By default, routers allotted a priority of 128.**
- **By configuring a priority 0 results the router as ineligible to become the designated router.**
- **Priority value 255 makes a router always be the designated router.**

In the above example Router 4 is DR and Router 3 is BDR. I'm gonna to change manually the DR to Router 1 and BDR to Router 2.
Enter the following commands in Router 1

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip ospf priority 255
R1(config-if)#exit

Now enter the following commands in Router 2

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface fastEthernet 0/0
R2(config-if)#ip ospf priority 254
R2(config-if)#exit

To enable these changes you should restart the OSPF process by entering #clear ip ospf process command.

—

Now let's verify whether the DR-BDR changed or not by entering #show ip ospf interface in Router 1.

R1#show ip ospf interface
FastEthernet0/1 is up, line protocol is up
Internet address is 20.0.0.1/8, Area 0
Process ID 1, Router ID 20.0.0.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 20.0.0.1, Interface address 20.0.0.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
Internet address is 10.0.0.1/8, Area 0
Process ID 1, Router ID 20.0.0.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 254

Designated Router (ID) 20.0.0.1, Interface address 10.0.0.1

Backup Designated Router (ID) 30.0.0.1, Interface address 10.0.0.2

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:05

--More--

Yes, now the state of Router 1 changed to DR.

For Router 2 enter#show ip ospf interface

R2#show ip ospf interface

FastEthernet0/0 is up, line protocol is up

Internet address is 10.0.0.2/8, Area 0

Process ID 1, Router ID 30.0.0.1, Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State BDR, Priority 253

Designated Router (ID) 20.0.0.1, Interface address 10.0.0.1

Backup Designated Router (ID) 30.0.0.1, Interface address 10.0.0.2

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:03

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 3, Adjacent neighbor count is 3

Adjacent with neighbor 20.0.0.1 (Designated Router)

Adjacent with neighbor 50.0.0.1

Adjacent with neighbor 40.0.0.1

Suppress hello for 0 neighbor(s)

FastEthernet0/1 is up, line protocol is up

Internet address is 30.0.0.1/8, Area 0

Process ID 1, Router ID 30.0.0.1, Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State DR, Priority 1

Designated Router (ID) 30.0.0.1, Interface address 30.0.0.1

--More--

We can see that Router 2 state is BDR. Apart from assigning IP OSPF priority number you may configure a loopback interface having highest IP will also give priority for BR-BDR.

–

How to Remove OSPF Configuration?

How to remove OSPF configurations settings from a router? Router(config)#no router ospf <number> command do that job

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no router ospf 1
R1(config)#exit

%SYS-5-CONFIG_I: Configured from console by console
R1#

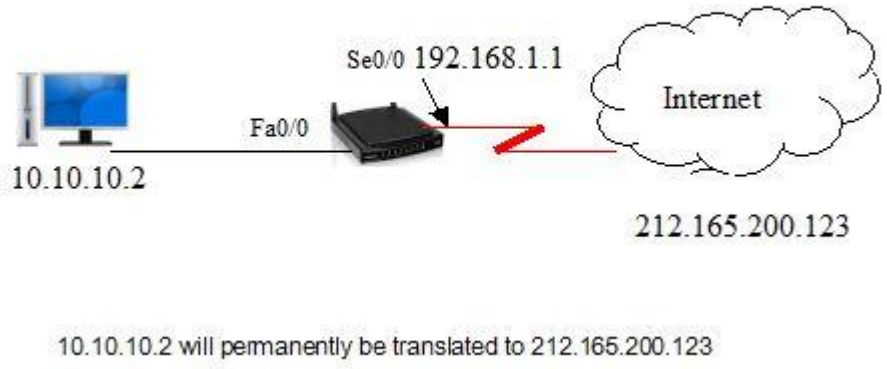
Assignment Name: **Static and Dynamic NAT & PAT**

Static and Dynamic NAT

Both static and dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.

Static NAT

Static NAT also called inbound mapping, is the process of mapping an unregistered IP address to a registered IP address on a one-to-one basis. The unregistered or mapped IP address is assigned with the same registered IP address each time the request comes through. This process is particularly useful for web servers or hosts that must have a consistent address that is accessible from the Internet.



Simply, Static NAT enables a PC on a stub domain to maintain an assigned IP address when communicating with other devices outside its network or the Internet.

Static NAT configuration commands example:

```
R1#config t
R1(config)#ip nat inside source static 10.10.10.2 212.165.200.123
R1(config)#interface fa0/0 10.10.10.1 255.255.255.0
R1(config)#ip nat inside
R1(config)#interface se0/0 192.168.1.1 255.255.255.0
R1(config)#ip nat outside
```

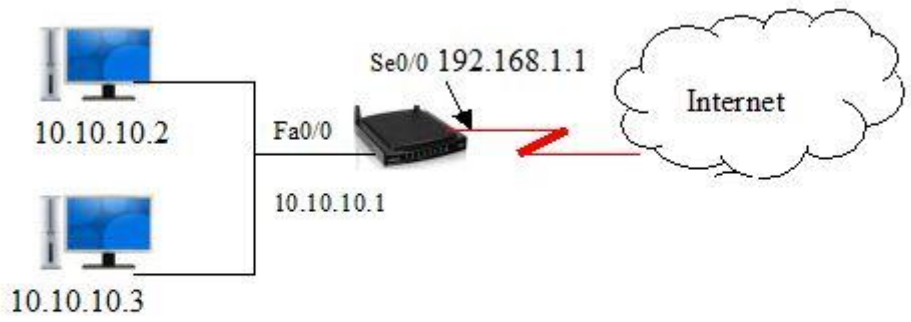
The above configuration creates a permanent entry in the NAT table as long as the configuration is present and enables both inside and outside hosts to initiate a connection.

All you need to do in static NAT configuration is to define the addresses to translate and then configure NAT on the right interfaces. Packets arriving on an inside interface from the identified IP addresses are subject to translation. Packets arriving on an outside interface addressed to the identified IP address are subject to translation.

Dynamic NAT

Unlike static NAT that provides a permanent mapping between an internal address and a specific public address, dynamic NAT maps private IP addresses to public addresses. Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis.

When a host with a private IP address requests access to the Internet, dynamic NAT chooses an IP address from the pool that is not already in use by another host. Dynamic NAT is useful when fewer addresses are available than the actual number of hosts to be translated.



In dynamic NAT, the computer with the IP address of 10.10.10.2 will translate to the first available address in the range from 179.9.8.80. to 179.9.8.95

Dynamic NAT configuration commands example:

```
R1#config t
R1(config)#ip nat-pool 179.9.8.80 179.9.8.95 netmask 255.255.255.0
R1 (config #ip nat inside source list 1 pool nat-pool1
R1 (config)#interface fa0/0 10.10.10.1 255.255.255.0
R1(config)#ip nat inside
R1(config)#interface se0/0
R1(config)#ip address 192.168.1.1 255.255.255.0
R1(config)#ip nat outside
R1(config)#access-list 1 permit 10.10.10.0 0.0.0.255
```

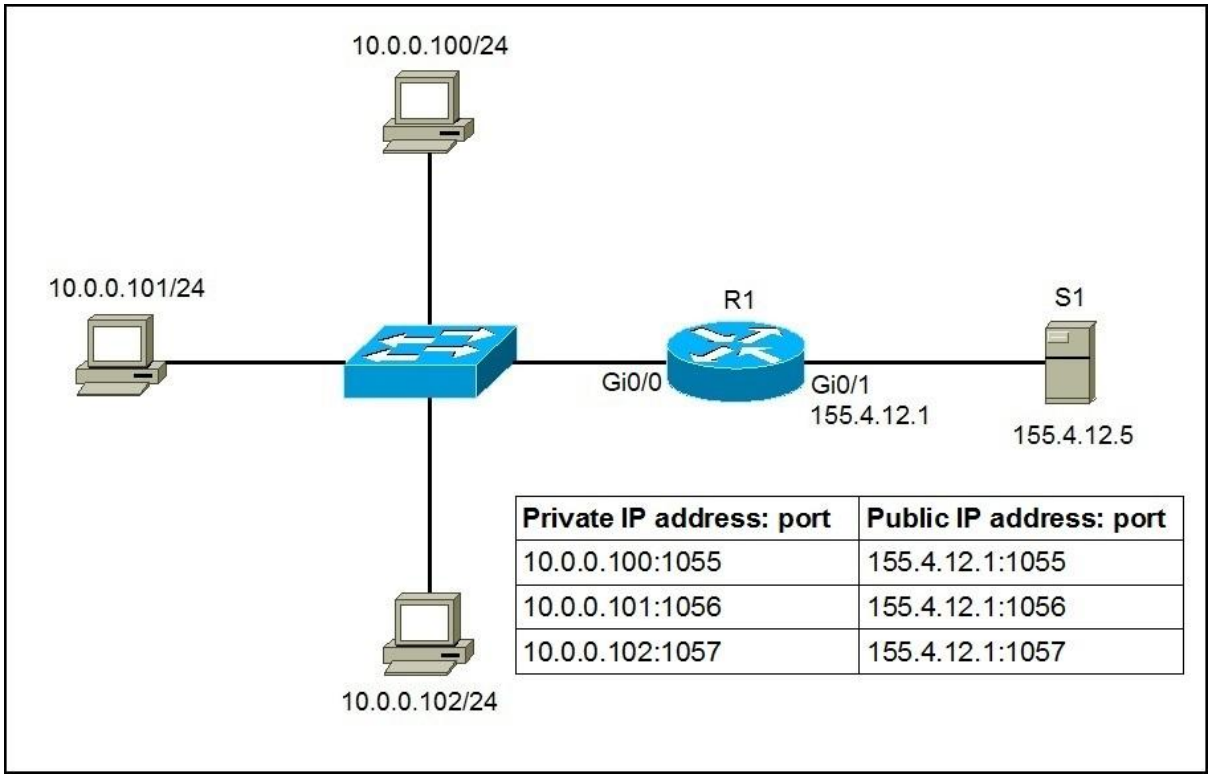
While static NAT provides a permanent mapping between an internal address and a specific public address, dynamic NAT maps private IP addresses to public addresses. These public IP addresses come from a NAT pool.

PAT

With **Port Address Translation (PAT)**, a single public IP address is used for all internal private IP addresses, but a different port is assigned to each private IP address. This type of NAT is also known as **NAT Overload** and is the typical form of NAT used in today's networks. It is even supported by most consumer-grade routers.

PAT allows you to support many hosts with only few public IP addresses. It works by creating dynamic NAT mapping, in which a global (public) IP address and a unique port number are selected. The router keeps a NAT table entry for every unique combination of the private IP address and port, with translation to the global address and a unique port number.

We will use the following example network to explain the benefits of using PAT:



Private IP address: port	Public IP address: port
10.0.0.100:1055	155.4.12.1:1055
10.0.0.101:1056	155.4.12.1:1056
10.0.0.102:1057	155.4.12.1:1057

As you can see in the picture above, PAT uses unique source port numbers on the inside global (public) IP address to distinguish between translations. For example, if the host with the IP address of 10.0.0.101 wants to access the server S1 on the Internet, the host's private IP address will be translated by R1 to 155.4.12.1:1056 and the request will be sent to S1. S1 will respond to 155.4.12.1:1056. R1 will receive that response, look up in its NAT translation table, and forward the request to the host.

To configure PAT, the following commands are required:

- configure the router's inside interface using the *ip nat inside* command.
- configure the router's outside interface using the *ip nat outside* command.

- configure an access list that includes a list of the inside source addresses that should be translated.
- enable PAT with the *ip nat inside source list ACL_NUMBER interface TYPE overload* global configuration command.

Here is how we would configure PAT for the network picture above.

First, we will define the outside and inside interfaces on R1:

R1(config)#int Gi0/0

R1(config-if)#ip nat inside

R1(config-if)#int Gi0/1

R1(config-if)#ip nat outside

Next, we will define an access list that will include all private IP addresses we would like to translate:

R1(config-if)#access-list 1 permit 10.0.0.0 0.0.0.255

The access list defined above includes all IP addresses from the 10.0.0.0 – 10.0.0.255 range.

Now we need to enable NAT and refer to the ACL created in the previous step and to the interface whose IP address will be used for translations:

R1(config)#ip nat inside source list 1 interface Gi0/1 overload

To verify the NAT translations, we can use the *show ip nat translations* command after hosts request a web resource from S1:

R1#show ip nat translations

Pro Inside global Inside local Outside local Outside global

tcp 155.4.12.1:1024 10.0.0.100:1025 155.4.12.5:80 155.4.12.5:80

tcp 155.4.12.1:1025 10.0.0.101:1025 155.4.12.5:80 155.4.12.5:80

tcp 155.4.12.1:1026 10.0.0.102:1025 155.4.12.5:80 155.4.12.5:80

Notice that the same IP address (155.4.12.1) has been used to translate three private IP addresses (10.0.0.100, 10.0.0.101, and 10.0.0.102). The port number of the public IP address is unique for each connection. So when S1 responds to 155.4.12.1:1026, R1 look into its NAT translations table and forward the response to 10.0.0.102:1025