**Efficiency of Different Routing Protocols**

**Sharda University**

**School of Engineering and Technology**

**Computer Science Engineering**

Prepare by:

Yar Mohammad Hafizy

Roll no: 130101202

08/02/2017

# Overview

Routing is a process of sending data packet from network to another network. Data is routed from its source to its destination through a series of routers, and across multiple networks.

In this paper i am going to configure open shortest path first (OSPF), and OSPF authentication, border gateway protocol (BGP), and BGP authentication.

I going to start by setting a network topology, assigning IP addresses to the router’s interfaces, enabling routing protocols to the specific topology, providing different types of authentication to specified routing protocols, and verification of each configuration in the routers.

**The definition of the keywords which is used in the paper**

**Interface fa0/0:** interface is a predefined command and fa0/0 is the interface of the router which is connected to local area network. By using this command we can go into an interface and provide IP address to the interface.

**IP address:** using this command we can define the ip address of the router interface and we can give the subnet mask to the specific IP address. It is (20.20.20.1) the IP address, and it is (255.0.0.0) the subnet mask which specifies the network portion of the IP address.

**Configure terminal:**  by using this command we can go to configuration terminal interface of the router and configure the router, without going to this interface we cannot configure the router.

**Network:** this command is used to specify the networks that the router is connected. It can be either LAN network or serial interface.

**No shut:**  this command is used to enable the router’s interface; by default all the interfaces of routers are disabled.

**What is an autonomous system number?**

Within the Internet, an autonomous system (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the Internet.

**No auto-summary**: By default routing protocol like RIP and EIGRP summarize subnets into major class full network at class full boundary. In other word, these protocols perform an auto-summarization each time they crosses a border between two different major networks. To disable this behavior and advertise subnets, 'no auto-summary' command is used. Let's say router has two subnets 192.168.10.0/24 and 172.16.4.0/24 of Class B network and one subnet 10.2.0.0/16 of Class A. When auto-summary is enabled, router will advertise only summarized major class full network 172.16.0.0/16 for class B addresses into its Class A interface

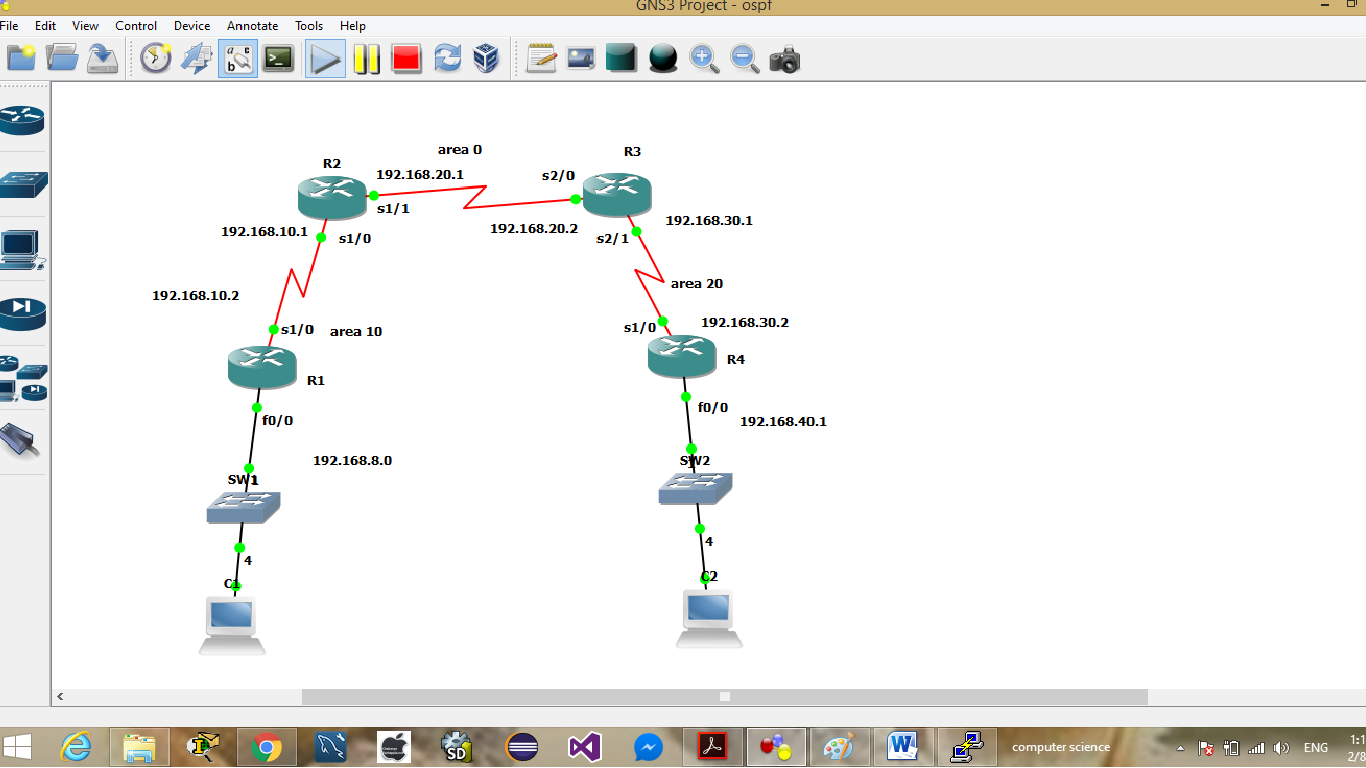
**Open shortest path first (OSPF)**

The Open Shortest Path First (OSPF) protocol is a link state protocol that handles routing for IP traffic. Its newest implementation, version 2, which is explained in RFC 2328, is an open standard. Open Shortest Path First (OSPF) is an open standard (not proprietary) and it will run on most routers independent of make. Open Shortest Path First (OSPF) uses the Shortest Path First (SPF) algorithm, developed by Dijkstra, to provide a loop-free topology. Open Shortest Path First (OSPF) provides fast convergence with triggered, incremental updates via Link State Advertisements (LSAs). Open Shortest Path First (OSPF) is a classless protocol and allows for a hierarchical design with VLSM and route summarization.

**Objective:** our aim is to configure OSPF routing protocol using multiple area, and provide authentication on interfaces of router.

For configuring multiple area OSPF, we should have area zero, and it should act as transaction between other areas. Data packet should be transferred between different other areas through area zero.

**OSPF Configuring Multi-Area:**

****

**Objective**

In this lab we show how to configure OSPF routing protocol with multi area.

**Step 1:** assign IP address to the interfaces of routers.

For assigning ip address we follow same process as we did in RIP V2

Assign IP address to router one (R1)

configure terminal

interface fa0/0

ip add 192.168.8.1 255.255.255.0

no shut

exit

int s1/0

ip add 192.168.10.2 255.255.255.0

R1(config-if)#no shut

R1(config-if)#exit

**Assign IP address to the router 2 (R2)**

configure terminal

interface s1/0

ip address 192.168.10.1 255.255.255.0

no shut

exit

interface s1/1

ip add 192.168.20.1 255.255.255.0

no shut

exit

**Assign IP address to the router 3 (R3)**

configure terminal

interface s2/0

ip address 192.168.20.2 255.255.255.0

no shut

exit

interface s2/1

add 192.168.30.1 255.255.255.0

no shut

exit

**Assign IP address to the router 4 (R4)**

configure terminal

int fa0/0

ip add 192.168.40.1 255.255.255.0

no shut

exit

int s1/0

ip add 192.168.30.2 255.255.255.0

no shut

exit

**Exit:** this command is used for going one step back to the previous interface.

**Step 2: configuring OSPF routing protocol on router one**

Assign router one’s interfaces in area 10

configure terminal

router ospf 10

network 192.168.8.0 0.0.0.255 area 10

network 192.168.10.0 0.0.0.255 area 10

exit

**Router ospf 10:** this command is used to specify the type of dynamic routing protocol is use and the autonomous system number (10).

**network 192.168.8.0 0.0.0.255 area 10:** network is predefined keyword, used to define the network address which we use. **192.168.8.0** This is the network address which is directly connected to our router, **0**.**0.0.255** this is the mask address which identifies the network portion and host portion of the network address. **area 10** : this keyword is used to provide the area number in which our outer is belong.

**What is area?**

An OSPF network can be divided into sub-domains called areas. An area is a logical collection of OSPF networks, routers, and links that have the same area identification. A router within an area must maintain a topological database for the area to which it belongs.

**network 192.168.8.0 0.0.0.255 area 10:** this command is used to identify the network address and subnet mask. It also provide the area, it tells the current network is in part of area 10.

**configuring OSPF routing protocol on router two(R2)**

assign the router interfaces s1/0 network (192.168.10.0) to area 10 and assign the router interface se1/1 to area zero

configure terminal

router ospf 20

network 192.168.2.0 0.0.0.255 area 0

network 192.168.10.0 0.0.0.255 area 10

exit

**configuring OSPF routing protocol on router three(R3)**

assign the router interfaces s2/0 network (192.168.20.0) to area zero and assign the router interface se2/1 to area 20

configure terminal

router ospf 30

network 192.168.2.0 0.0.0.255 area 0

network 192.168.30.0 0.0.0.255 area 10

exit

**configuring OSPF routing protocol on router four(R4)**

Assign router one’s interfaces in area 20

configure terminal

router ospf 40

network 192.168.3.0 0.0.0.255 area 20

network 192.168.40.0 0.0.0.255 area 20

exit

**For verifying OSPF routes**

show ip route

Or

**show ip protocol**

This command is used to show the type of configured routing protocol from flush memory

**show ip ospf database**

This command is used to show the complete database of router about the networks, it gives the complete routes which exist in the network.

**R1#show ip ospf neighbor**

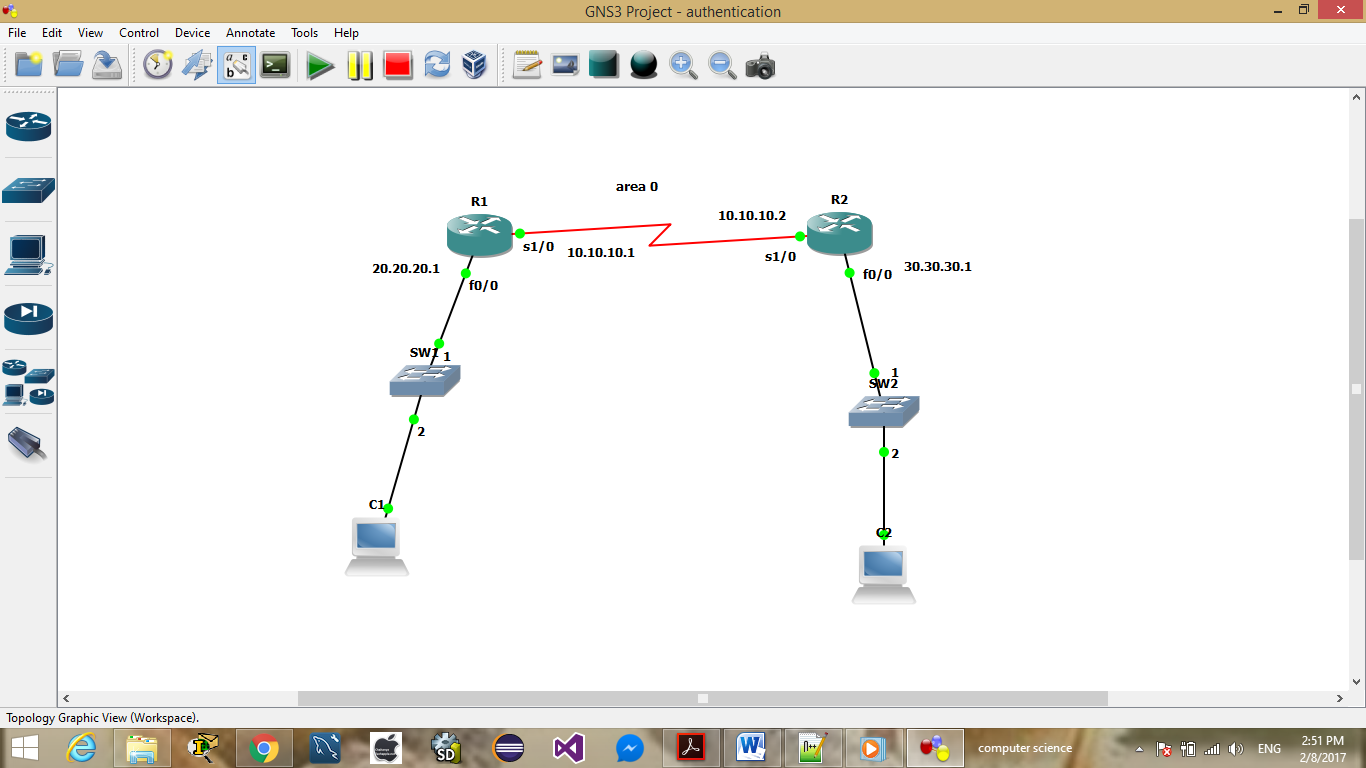
This command is used to show the directly connected neighbors from flush memory.

**Note:** area zero should be backbone it means all other areas should be connected to area zero and area 0 should be as transit.

**Configuring OSPF Authentication**

OSPF authentication comes in two forms: plain-text and MD5. Because a secure method was specified, we have to use MD5 authentication in our environment (plain-text is not secure).

We configure clear text authentication and message digest five on this topology:



**Configurations for Plain Text Authentication**

Plain text authentication is used when devices within an area cannot support the more secure MD5 authentication. Plain text authentication leaves the internetwork vulnerable to a "sniffer attack," in which packets are captured by a protocol analyzer and the passwords can be read. However, it is useful when you perform OSPF reconfiguration, rather than for security. For example, separate passwords can be used on older and newer OSPF routers that share a common broadcast network to prevent them from talking to each other. Plain text authentication passwords do not have to be the same throughout an area, but they must be the same between neighbors.

**For configuring plain text authentication we should follow the following process:**

**Step 1:** assign IP address to the interfaces of routers

**Step 2:** configure OSPF routing protocol on each router

**Step3:** configure clear text authentication

**Step 1:** assign IP address to the interfaces of router one (R1)

interface se1/0

ip address 10.10.10.1 255.0.0.0

no shut

interface f0/0

ip address 20.20.20.1 255.0.0.0

no shut

**Step 2: configure OSPF routing protocol on each router**

router ospf 10

network 10.0.0.0 0.255.255.255 a 0

network 20.0.0.0 0.255.255.255 a 0

exit

**Step3: configure clear text authentication**

interface se1/0

ip ospf authentication

ip ospf authentication-key cisco123

exit

**Authentication on router two (R2)**

**Step 1:** assign IP address to the interfaces of routers

int se1/0

ip add 10.10.10.2 255.0.0.0

no shut

interface f0/0

ip add 30.30.30.1 255.0.0.0

no shut

**Step 2:** configure OSPF routing protocol on R2

router ospf 10

network 10.0.0.0 0.255.255.255 a 0

network 30.0.0.0 0.255.255.255 a 0

exit

**Step3:** configure clear text authentication

interface se1/0

ip ospf authentication

ip ospf authentication-key cisco123

exit

**Exit:** it is used to go one step back to the configuration

**ip ospf authentication-key cisco123:** in this command, **ip ospf**  is used to say that, it is using ospf routing protocol for authentication, **authentication-key** it is a predetermined command and used for configure authentication in ospf routing protocol, and **cisco123**  is the actual password for authentication, it is user defined password, it means you can give any kind of password according to your wish.

**Message digest 5 authentication**

When you use MD5 OSPF authentication, a key and a key id must be configured on routers. From this key and key id a hash is generated, which is added to OSPF packet header.

This authentication does encrypts the password, so, hackers cannot easily hack the password.it is very secure as compare to plain text authentication.

We work on the same topology which we did for clear text authentication

**Step 1**: assign IP address to each interfaces of router

**Step 2:** configure OSPF on each router

We did these two steps in above clear text authentication. We need to configure MD5 only on each interface of routers

**Now configure MD5 on router one (R1)**

int se1/0

ip ospf ip ospf authentication message-digest

ip ospf message-digest-key 2 md5 cisco123

exit

**Now configure MD5 on router two (R2)**

ip ospf authentication message-digest

ip ospf message-digest-key 2 md5 cisco123

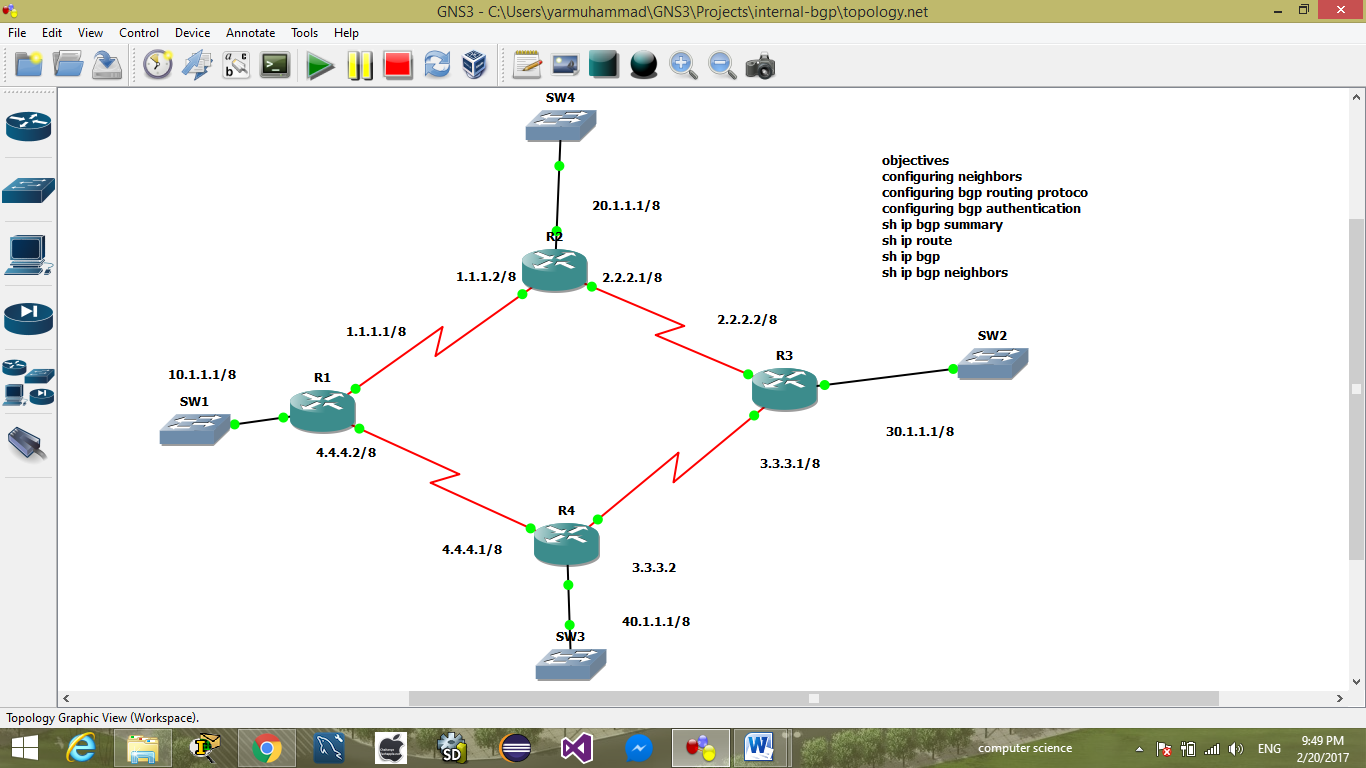
exit

**ip ospf ip ospf authentication message-digest:** this command is used to configure MD5 authentication on the interface. Here we specify the type of routing protocol which is OSPF and the mode of authentication, which is message-digest (MD5).

**Border gateway routing protocol (BGP)**

BGP is an open standard protocol, means all manufacture routers support BGP. It is used to connect and make communication between two different autonomous system number, it grantees loop free routing protocol. It supports VLSM, FLSM, CIDR IP addressing. Updates are incremental as OSPF and EIGRP.

We are going to configure BGP on the following topology.



**Objectives:** configuring neighbors, assigning ip address to the each interface, defining network addresses, and providing authentication.

**Step 1:** assigning IP address to the interfaces of each router.

**Assign IP address to R1**

Interface se1/0

ip address 1.1.1.1 255.0.0.0

no shutdown

interface se1/1

ip address 4.4.4.2 255.0.0.0

no shut

**Assign IP address to R2**

int fa0/0

ip add 20.1.1.1 255.0.0.0

no shut

int se1/0

ip add 1.1.1.2 255.0.0.0

no shut

int se1/1

ip add 2.2.2.1 255.0.0.0

no shut

**Assign IP address to R3**

int fa0/0

ip add 30.1.1.1 255.0.0.0

no shut

int se1/0

ip add 2.2.2.2 255.0.0.0

no shut

int se1/1

ip add 3.3.3.1 255.0.0.0

no shut

**Assign IP address to R4**

int fa0/0

ip add 40.1.1.1 255.0.0.0

no shut

int se1/0

ip add 3.3.3.2 255.0.0.0

no shut

interface se1/1

ip add 4.4.4.1 255.0.0.0

no shut

**Step 2: configuring BGP routing protocol**

R1:

router bgp 500

neighbor 1.1.1.2 remote-as 500

neighbor 4.4.4.1 remote-as 500

neighbor 2.2.2.2 remote-as 500

network 10.0.0.0

network 1.0.0.0

network 4.0.0.0

end

copy run start

**router bgp 500:** using this command we can defined the type routing protocol we use in outer network and the autonomous system number. And autonomous system is a collection of routers under a single administrative domain.

**Neighbor 1.1.1.2 remote-as 500:**  this command defines the neighbor address in which it is directly connected, and the autonomous number the neighbor is belong to.

**Network:** this command identifies the networks or links in which the router itself is connected.

R2:

router bgp 500

neighbor 1.1.1.1 remote-as 500

neighbor 2.2.2.2 remote-as 500

neighbor 3.3.3.2 remote-as 500

network 20.0.0.0

network 1.0.0.0

network 2.0.0.0

R3:

router bgp 500

neighbor 3.3.3.2 remote-as 500

neighbor 2.2.2.1 remote-as 500

neighbor 1.1.1.1 remote-as 500

net 30.0.0.0

net 2.0.0.0

net 3.0.0.0

R4:

router bgp 500

neighbor 3.3.3.1 remote-as 500

neighbor 4.4.4.2 remote-as 500

neighbor 2.2.2.1 remote-as 500

net 40.0.0.0

net 4.0.0.0

net 3.0.0.0

end

copy run start

**copy run start** : this command is used to store the configurations from RAM to non-volatile RAM.

**Configuring authentication in bgp network**

BGP supports only MD5 authentication, the concept is same as OSPF, EIGRP, and RIP.

Steps to be followed for configuring MD5

Step 1: assign IP address

Step 2: configure BGP routing protocol

We did the two steps in above section (BGP configuration)

Step 3: implement MD5

Configuring MD5 on R1

R1

router bgp 500

neighbor 1.1.1.2

neighbor 1.1.1.2 password cisco123

neighbor 2.2.2.2 password cisco123

neighbor 4.4.4.1 password cisco123

end

copy run start

Configuring MD5 on R2

router bgp 500

neighbor 1.1.1.1 password cisco123

neighbor 2.2.2.2 password cisco123

neighbor 3.3.3.2 password cisco123

end

copy run start

Configuring MD5 on R3

router bgp 500

neighbor 1.1.1.1 password cisco123

neighbor 2.2.2.1 password cisco123

neighbor 3.3.3.2 password cisco123

end

copy run start

Configuring MD5 on R4

router bgp 500

neighbor 4.4.4.2 password cisco123

neighbor 2.2.2.1 password cisco123

neighbor 3.3.3.1 password cisco123

end

copy run start

**password cisco123:** here the **password** is predefined keyword which is used to provide password for authentication, **cisco123** is the real password