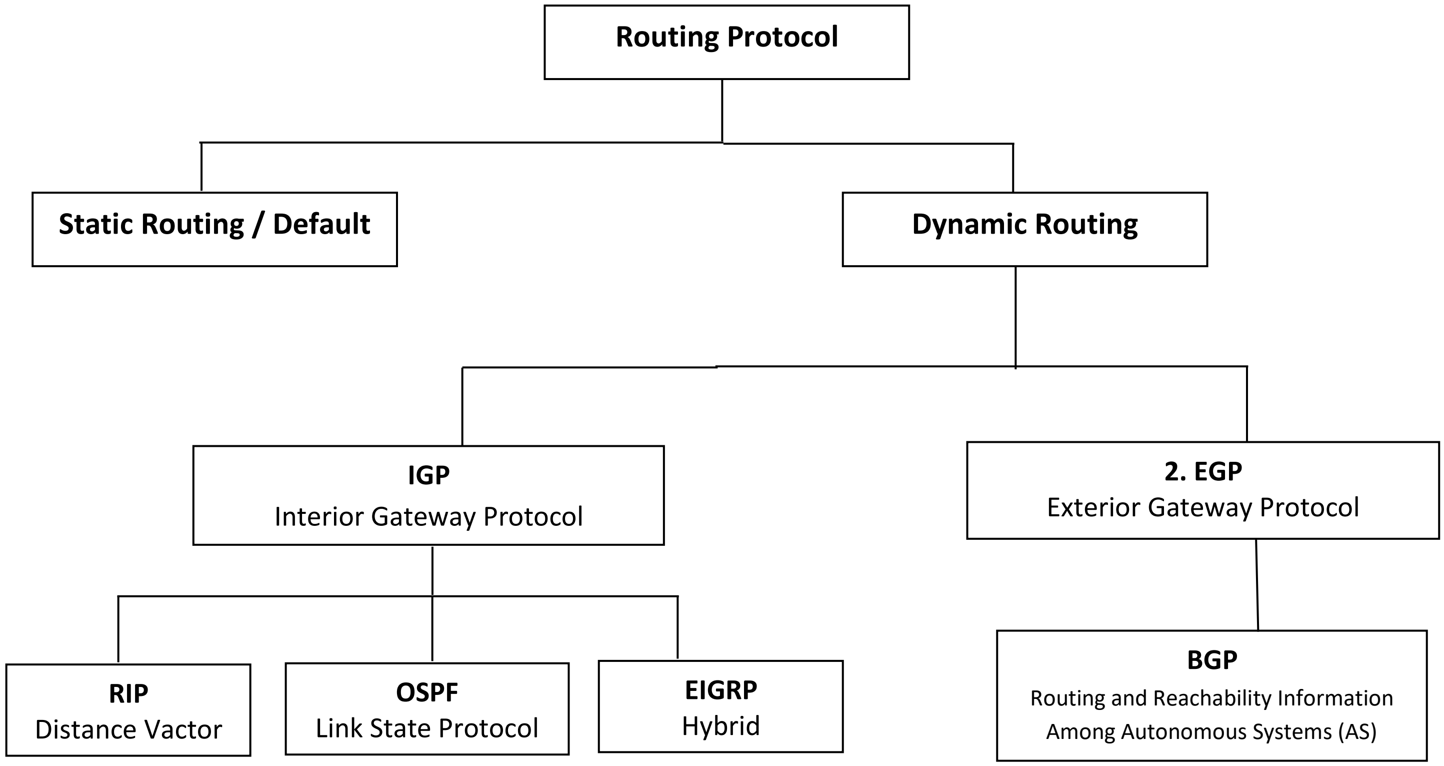
Routing Protocol



1. Interior Gateway Protocol (IGP)

Interior Gateway Protocol (IGP) is a dynamic class routing protocol used by autonomous system routers running on TCP/IP hosts. IGP overcomes Routing Information Protocol (RIP) network limitations and supports multiple routing metrics, including delay, bandwidth, load and reliability.

<u>The two IGP types are:</u>

a) Distance-Vector Routing Protocol (DVRP)- RIP:

- Distance vector routing protocols represent some of the oldest routing protocols still in use today.
- DVRP protocol requires that a router inform its neighbors of topology changes periodically.
- One key point here is that distance vector routing protocols only talk to their directly connected neighbors.
- Each router does not have first-hand information about all the routes in its routing table. As a matter of fact, most of the routes in the routing table will be from second-hand information.
- Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).
- The Distance Vector protocols do not check who is listening to the updates which they sent and Distance Vector protocols broadcast the updates periodically even if there is no change in the network topology.
- Distance Vector protocols are the simplest among three types of dynamic routing protocols.
- They are easy to set-up and troubleshoot. They require less router resources.
- They receive the routing update, increment the metric, compare the result to the routes in the routing table, and update the routing table if necessary. Three core examples are RIP, Interior Gateway Routing Protocol and Enhanced Interior Gateway Routing Protocol.

b) Link State Routing Protocol (LSRP)-OSPF:

- Link-state routing protocols are generally more robust than their distance vector counterparts. They are used more widely in larger networks.
- They generally use a slightly more advanced algorithm for computing the best route to a destination. One commonly used algorithm is the Dijkstra Shortest Path First Algorithm.
- Link-state routing protocols can transmit routing information to all other routers running the same protocol, not just directly connected neighbors.
- This way, all routers are receiving first-hand information. This makes the routes more reliable. Hence, routes created by link-state routing protocols generally have lower administrative distances.
- The updates sent by link-state routing protocols are called link-state advertisements (LSAs). These LSAs are processed by other routers on the networks. The routers then update their routing tables.
- Link-state routing protocols generally keep three different routing tables. The first table tracks all the router's neighbors. The second table tracks the entire network topology and all the possible routes to a destination. The third table tracks the preferred route to a destination network and is generally what is thought of when discussing routing tables.
- When routers running link-state routing protocols start up, there is an initial discovery and synchronization. After the initial discovery and synchronization period, each router will send periodic hello messages. These hello messages are used to let the router's neighbors know that the router is still functioning. If a series of these hello messages are missing, then a router will be assumed to be down and unavailable.
- Convergence happens much faster with link-state routing protocols than with distance vector protocols. Because routing updates only include changes to the network, there is far less processing that needs to be done when updates are sent. For this reason, link-state protocols are often preferred in larger, more complex networks.

2. Exterior Gateway Protocol (EGP)

An Exterior Gateway Protocol is a routing protocol which is used to exchange routing information between autonomous systems. Exterior Gateway Protocol (EGP) is a Routing Protocol which is used to find network path information between different networks. It is commonly used in the Internet to exchange routing table information between two neighbor gateway hosts (each with its own router) in a network of autonomous systems. Border Gateway Protocol (BGP) is the only Exterior Gateway Protocol (EGP) at the time.

Exterior Gateway Protocol (EGP) is a protocol for exchanging routing information between two neighbor gateway hosts (each with its own router) in a network of autonomous systems. EGP is commonly used between hosts on the Internet to exchange routing table information. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. Each router polls its neighbor at intervals between 120 to 480 seconds and the neighbor responds by sending its complete routing table. EGP-2 is the latest version of EGP. A more recent exterior gateway protocol, the Border Gateway Protocol (BGP), provides additional capabilities.

Classful & Classless Routing Protocols

Another key concept that crops up when examining dynamic routing protocols is classful and classless routing protocols. The difference between these two is that classful routing protocols don’t send subnet mask information with routing updates and classless routing protocols do include the subnet mask and network address in routing updates.

Most modern networks rely on classless routing protocols because they support more complex network topologies and variable-length subnet masks (VLSM). On the other hand, classful routing protocols can function within modern enterprise environments but they are more restricted in terms of when they can be used. For instance, they can't be used when a network has been subnetted with multiple subnet masks.

- Classful routing protocols DO NOT send the subnet mask along with their updates.
- Classless routing protocols DO send the subnet mask along with their updates.

IGP Comparison

SL.	RIP	EIGRP	IGRP	OSPF
1	RIP Stands For Routing Information protocol.	EIGRP Stands For Enhanced Interior Gateway Routing protocol.	IGRP Stands For Interior Gateway Routing protocol.	OSPF stands For Open shortest path First.
2	It Is a Industry standard dynamic routing protocol.	It Is a Cisco standard routing protocol.	It is a Cisco standard routing protocol.	It Is a Industry standard routing protocol.
3	It is not a more intelligent dynamic routing protocol.	It Is a more intelligent routing protocol than RIP and IGRP.	It is a more intelligent routing protocol than RIP	It is a more intelligent routing protocol than RIP, IGRP and EIGRP.
4	It is basically use for smaller size organization.	It is basically use for medium to lager size organization in the network.	It is basically use for medium to larger size organization in the network.	It is basically use for larger size organization in the network
5	It support maximum 15 routers in the network. 16 router is unreachable	It supports maximum 255 routers in the network.	It supports maximum 255 routers in the network.	It supports unlimited router in the network
7	It's Administrative Distance Is 120.	It's Administrative distance Is 90.	It's Administrative Distance Is 100.	It's Administrative distance is 110.

8	In RIP routing protocol we cannot create a separate administrative boundary in the network.	In EIGRP routing protocol we can create a separate administrative boundary in the network with the help of autonomous system No.	In IGRP routing protocol we can create a separate administrative boundary in the network with the help of autonomous System No.	In OSPF routing protocol we can create a separate administrative boundary in the network through area no. within the same area all of the routers are exchanging the route information from neighbor router in the network.
9	It calculates the metric In terms of Hop Count from source network to destination network. Lower the Hop count that is the best route for that particular network.	It calculates the metric In terms of bandwidth and delay.	It calculates the metric in terms of bandwidth and delay. It Is also called composite metric.	It calculates the metric in terms of bandwidth.
11	RIPv1 Do Not Support VLSM. RIPv2 support VLSM.	EIGRP Supports VLSM.	IGRP do Not Support VLSM.	OSPF Supports VLSM.
12	RIP routing protocol creates two table in the router: Routing Table ,Topology Table.	EIGRP routing protocol creates three table In the router : Neighbor Table, Topology Table, Routing Table.	IGRP routing protocol creates three table In the router : Neighbor Table , Topology Table, Routing Table.	OSPF routing protocol creates three Table in the router: Neighbor Table, Database Table , Routing Table.

VLSM

VLSM Configuration

Total required hosts = 165

Total Network Bits = 2^8 = 256

32-8 = 24 bits needed

192.168.1.0/24

Banani (85 hosts)

2^7=128

32-7=25 bits

192.168.1.0/25

Network Address	**Usable Host Range**	**Broadcast Address:**
192.168.1.0	192.168.1.1 - 192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129 - 192.168.1.254	192.168.1.255

Gulshan (48 hosts)

2^6=64

32-6=26 bits

192.168.1.0/26

Network Address	Usable Host Range	Broadcast Address:
192.168.1.0	192.168.1.1 - 192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65 - 192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129 - 192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193 - 192.168.1.254	192.168.1.255

Tejgaon (21 hosts)

2^5=32

32-5=27 bits

192.168.1.0/27

Network Address	Usable Host Range	Broadcast Address:
192.168.1.0	192.168.1.1 - 192.168.1.30	192.168.1.31
192.168.1.32	192.168.1.33 - 192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65 - 192.168.1.94	192.168.1.95
192.168.1.96	192.168.1.97 - 192.168.1.126	192.168.1.127

192.168.1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
192.168.1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
192.168.1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

Hatirjheel (11 hosts)

2^4=16

32-4=28 bits

192.168.1.0/28

Network Address	Usable Host Range	Broadcast Address:
192.168.1.0	192.168.1.1 - 192.168.1.14	192.168.1.15
192.168.1.16	192.168.1.17 - 192.168.1.30	192.168.1.31
192.168.1.32	192.168.1.33 - 192.168.1.46	192.168.1.47
192.168.1.48	192.168.1.49 - 192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65 - 192.168.1.78	192.168.1.79
192.168.1.80	192.168.1.81 - 192.168.1.94	192.168.1.95
192.168.1.96	192.168.1.97 - 192.168.1.110	192.168.1.111
192.168.1.112	192.168.1.113 - 192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129 - 192.168.1.142	192.168.1.143
192.168.1.144	192.168.1.145 - 192.168.1.158	192.168.1.159
192.168.1.160	192.168.1.161 - 192.168.1.174	192.168.1.175
192.168.1.176	192.168.1.177 - 192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193 - 192.168.1.206	192.168.1.207
192.168.1.208	192.168.1.209 - 192.168.1.222	192.168.1.223
192.168.1.224	192.168.1.225 - 192.168.1.238	192.168.1.239
192.168.1.240	192.168.1.241 - 192.168.1.254	192.168.1.255

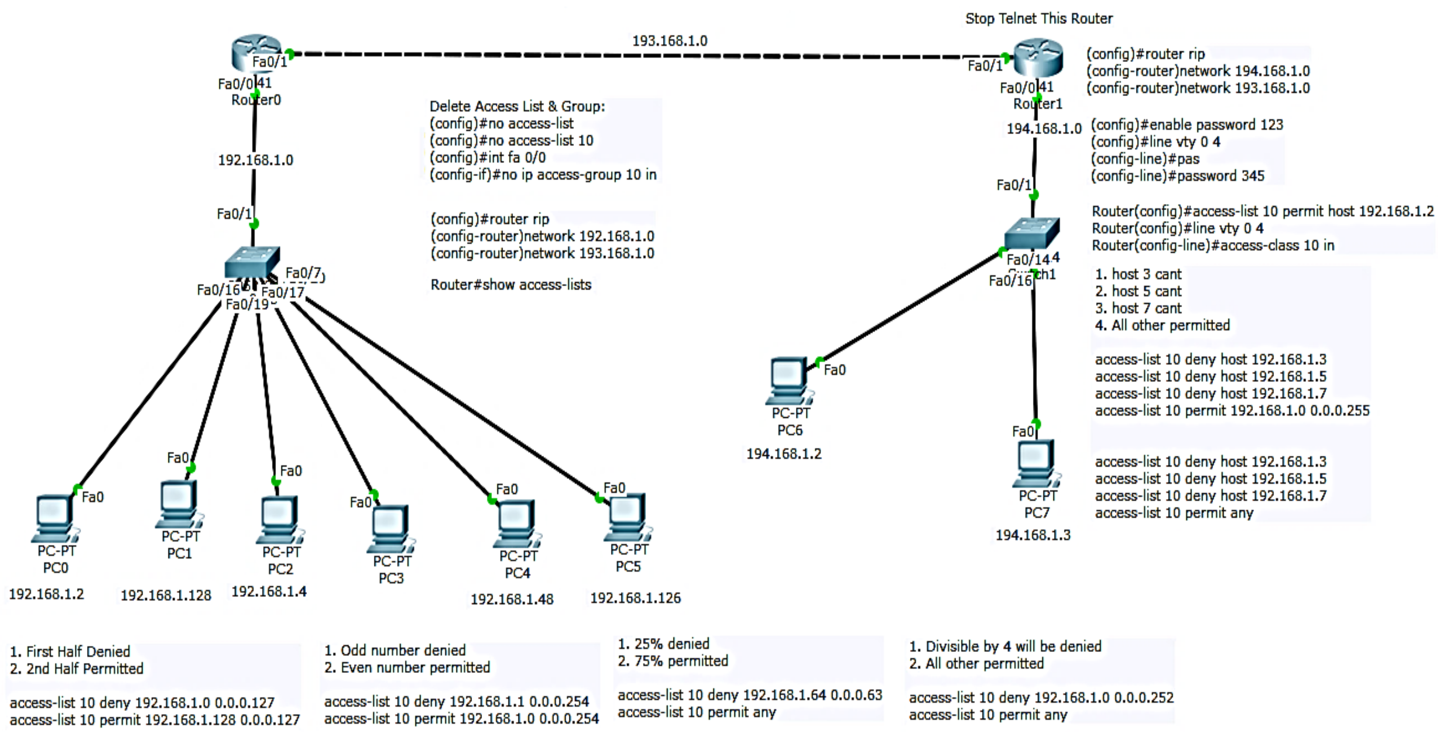
Access Control Lists (ACLs)

Access Control Lists (ACLs) are very powerful security feature of Cisco IOS. Access Control Lists (ACLs) are used to permit or deny access between networks, based on conditions like source IP address, destination IP Address, source TCP/UDP port number, destination TCP/UDP port number etc. Access Control Lists (ACL) topics are a part of CCNA Routing and Switching exam also. Please find below important Access Control Lists (ACL) exam topics which are required for CCNA Security examination.

Difference between standard access list and extended access list:

Standard ACL	Extended ACL
Allow filtering based on source address.	Allow filtering based on source and destination addresses, as well as protocol and port number.
Used to block particular host, network or subnet.	Used to block particular services.
Standard ACL is implemented closet to the destination	Extended ACL is implemented closet to the source.
Standard ACL Range–> 1 – 99 & 1300- 1999.	Extended ACL Range–> 100 – 199 &2000 – 2699
In Standard ACL, two-way communications will be blocked	In Extended ACL, one-way communication will be blocked
In Standard ACL, all services will be blocked	Extended ACL, particular services will be blocked.

Standard ACL



Extended ACL