Interior Gateway Routing Protocols

- An Interior gateway routing protocol is used to determine how routing is performed within an autonomous system (AS). These routing protocols are also known as Intra-AS routing protocols.
- Two most popular routing protocols that have been used extensively for routing within an autonomous system in the Internet are :
- Routing Information Protocol (RIP), and
- Open Shortest Path First (OSPF).

Open Shortest Path First (OSPF) - Basics

- Like RIP, OSPF routing is widely used for intra-AS routing in the Internet.
- The Open in OSPF indicates that the routing protocol is open and non proprietary standard.
- OSPF is a link state protocol that uses flooding of link state information and a Dijkstra least cost path algorithm.
- The fundamental concept behind OSPF is a data structure called the link state database (LSDB).
- Each router in an autonomous system maintains a copy of this database, which contains information in the form of a directed graph that describes the current state of the autonomous system.
- Each link to a network or another router is represented by an entry in the database, and each has an associated cost (or metric). The cost of an interface in OSPF is an indication of the overhead required to send packets across a certain interface.
- The cost of an interface is inversely proportional to the bandwidth of that interface. A higher bandwidth indicates a lower cost.
- Cisco uses a simple equation of $10^8\ /bandwidth$, where bandwidth is the configured bandwidth for the interface.

Open Shortest Path First (OSPF) - Basics

- Information about the autonomous system moves around the autonomous system in the form of link state advertisements (LSAs), messages that let each router tell the others what it currently knows about the state of the AS.
- To determine actual routes, each router uses its link state database to construct a shortest path tree.
- This tree shows the links from the router to each other router and network, and allows the lowest cost route to any location to be determined.
- As new information about the state of the internetwork arrives, this tree can be recalculated, so the best route is dynamically adjusted based on network conditions.
- When more than one route with an equal cost exists, traffic can be shared amongst the routes (load balancing).

OSPF VS RIP

- RIP has certain limitations that can cause problems in large networks:
- RIP has a limit of 15 hops. A RIP network that spans more than 15 hops (15 routers) is considered unreachable.
- RIP cannot handle Variable Length Subnet Masks (VLSM).
- Periodic broadcasts of the full routing table consume a large amount of bandwidth.
- RIP converges slower than OSPF.
- RIP has no concept of network delays and link costs. Routing decisions are based on hop counts. The path with the lowest hop count to the destination is always preferred even if the longer path has a better aggregate link bandwidth and less delays.
- RIP networks are flat networks. There is no concept of areas or boundaries.
- OSPF, on the other hand, addresses most of the issues previously presented:
- With OSPF, there is no limitation on the hop count.
- The intelligent use of VLSM is very useful in IP address allocation.
- OSPF has better convergence than RIP. This is because routing changes are propagated instantaneously and not periodically.
- OSPF allows for a logical definition of networks where routers can be divided into areas.

OSPF Terminology

- Link - A link is a network or router interface assigned to any given network. When an interface is added to the OSPF process, it's considered to be a link.
- Router ID - The router ID (RID) is an IP address used to identify the router.
- Neighbor - Neighbors are two or more routers that have an interface on a common network, such as two routers connected on a point-to-point serial link. Neighbors are elected via the Hello protocol. Two routers will not become neighbors unless they agree on the following:
  - Area ID - This represents the area that the originating router interface belongs to.
  - Authentication - This is the authentication type and corresponding information.
  - Hello and Dead Intervals - The period between Hello packets is the Hello time, which is 10 seconds by default. The dead time is the length of time allotted for a Hello packet to be received before a neighbor is considered down. This is usually four times the Hello interval, unless otherwise configured.
- Adjacency - An adjacency is a relationship between two OSPF routers that permits the direct exchange of route updates. Adjacent routers are routers that go beyond the simple Hello exchange and proceed into the database exchange process. In order to minimize the amount of information exchange on a particular segment, OSPF elects one router to be a designated router (DR), and one router to be a backup designated router (BDR).

OSPF Terminology

- Designated router - A designated router (DR) is elected whenever OSPF routers are connected to the same broadcast network to minimize the number of adjacencies formed and to publicize received routing information to and from the remaining routers on the broadcast network or link. Elections are won based upon a router's priority level, with the one having the highest priority becoming the winner. If there's a tie, the router ID will be used to break it. All routers on the shared network will establish adjacencies with the DR and the BDR, which ensures that all routers' topology tables are synchronized
- Backup designated router - A backup designated router (BDR) is a standby for the DR on broadcast, or multi-access, links. The BDR receives all routing updates from OSPF adjacent routers but does not disperse LSA updates.
- Hello protocol - The OSPF Hello protocol provides dynamic neighbor discovery and maintains neighbor relationships. Hello packets and Link State Advertisements (LSAs) build and maintain the topological database.
- Neighborship database - The neighborship database is a list of all OSPF routers for which Hello packets have been seen. A variety of details, including the router ID and state, are maintained on each router in the neighborship database.
- Topological database - The topological database contains information from all of the Link State Advertisement packets that have been received for an area. The router uses the information from the topology database as input into the Dijkstra algorithm that computes the shortest path to every network.

OSPF Adjacency Requirement

- Once neighbors have been identified, adjacencies must be established so that routing information can be exchanged.
- There are two steps required to change a neighboring OSPF router into an adjacent OSPF router:
- Two way communication (achieved via the Hello protocol)
- Database synchronization, which consists of three packet types being exchanged between routers:
  - Database Description (DD) packets - These messages contain descriptions of the topology of the AS or area. That is, they convey the contents of the link state database for the autonomous system or area from one router to another.
  - Link State Request (LSR) packets - After DD packets exchange process, the router may find it does not have an up-to-date database. These messages are used by one router to request updated information about a portion of the LSDB from another router. The message specifies exactly which link(s) about which the requesting device wants more current information.
  - Link State Update (LSU) packets - These messages contain updated information about the state of certain links on the LSDB. They are sent in response to a Link State Request message, and also broadcast or multicast by routers on a regular basis. Their contents are used to update the information in the LSDBs of routers that receive them.

OSPF Adjacency Requirement

- Once database synchronization is complete, the two routers are considered adjacent.
- On point-to-point link , the two neighbors will become adjacent if the Hello packet information for both routers is configured properly.
- On broadcast multi-access networks, adjacencies are formed only between the OSPF routers on the network and the DR and BDR.

OSPF Link State Advertisements

- A Link State Advertisement (LSA) is an OSPF data packet containing link state and routing information that is shared among OSPF routers.
- An OSPF router will exchange LSA packets only with routers to which it has established adjacencies.
- LSA packet contains sufficient information to identify the link. Some of the important fields are:
- LS Age - The LS Age is the equivalent of a time to live, except that it counts up and the LSA expires when the age reaches a defined maximum value.
- Link State ID- Identifies the link. This usually is the IP address of either the router or the network the link represents.
- Advertising Router - The ID of the router originating the LSA.
- LS Sequence Number - A sequence number used to detect old or duplicate LSAs.

OSPF Link State Advertisements

- LS Type - Indicates the type of link this LSA describes.

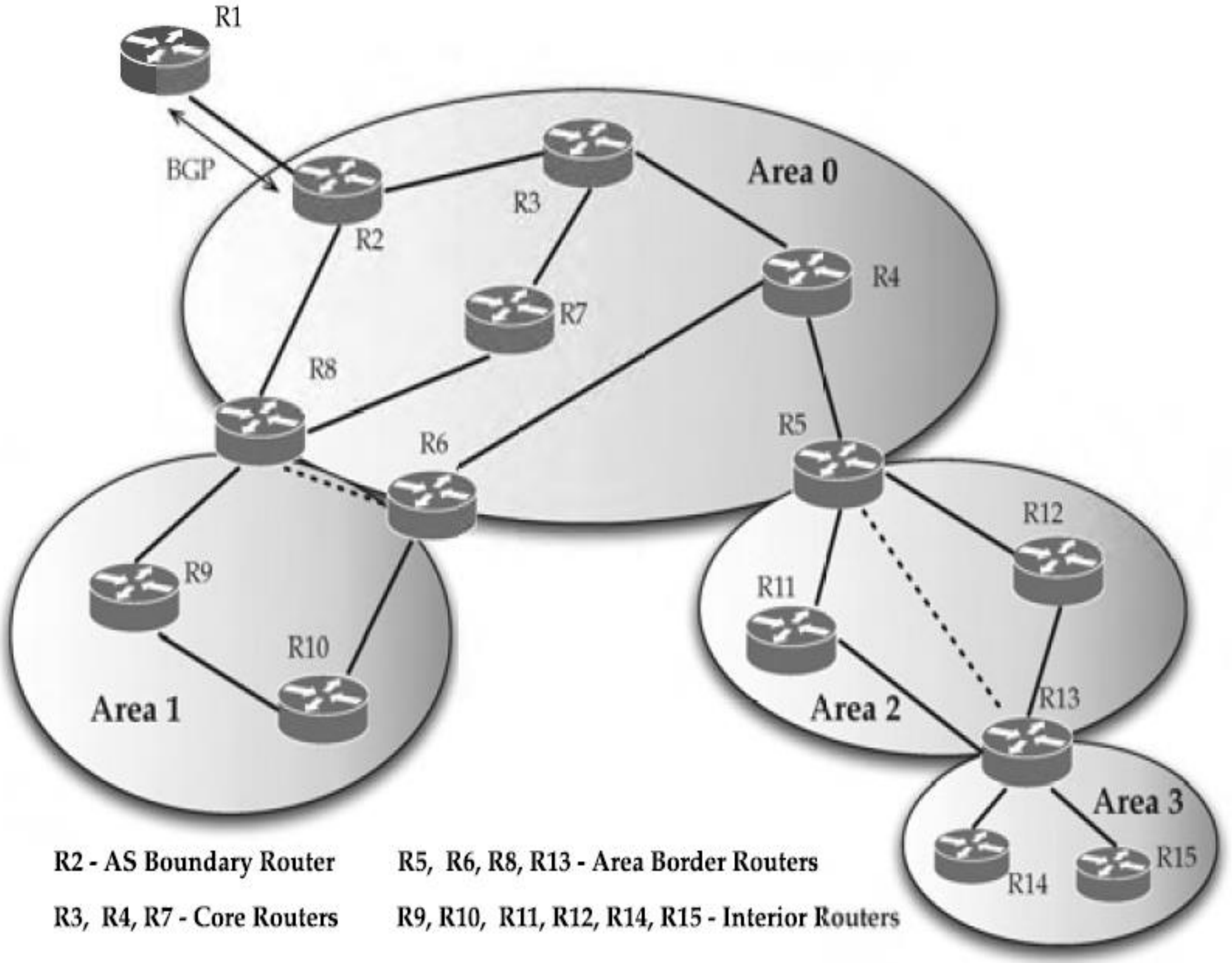
LS Type	Description
1	Router Link advertisements - Generated by each router for each area it belongs to. They describe the states of the router's link to the area. If a router is connected to multiple areas, then it will send separate Type 1 LSAs for each of the areas it’s connected to. These are only flooded within a particular area.
2	Network Link advertisements - Generated by Designated Routers. They describe the set of routers attached to a particular network. Flooded in the area that contains the network.
3 or 4	Summary Link advertisements - Generated by Area Border routers. They describe inter area routes. Type 3 describes routes to networks, also used for aggregating routes. Type 4 describes routes to ASBR.
5	AS external link advertisements - Originated by ASBR. They describe routes to destinations external to the AS.

OSPF Areas

- OSPF provides the functionality to divide an autonomous system into sub autonomous systems , commonly referred to as areas. Every autonomous systems must have a core area, referred to as a backbone area; this is identified with Area ID 0.
- Areas are identified through a 32 bit area field; thus Area ID 0 is the same as 0.0.0.0.
- Usually, areas (other than the backbone) are sequentially numbered as Area 1 (i.e., 0.0.0.1), Area 2, and so on.
- OSPF allows a hierarchical setup with the backbone area as the top level while all other areas, connected to the backbone area, are referred to as low level areas.
- This also means that the backbone area is in charge of summarizing the topology of one area to another area, and vice versa.

OSPF Areas

- With the functionality provided to divide an OSPF network into areas ,the routers are classified into four different types:
- Area Border Routers - These are the routers that sit on the border between the backbone and the low level areas. Each area border router must have at least one interface to the backbone; it also has at least one interface to each area to which it is connected.
- Internal Routers - These are the routers in each low level area that have interfaces only to other internal routers in the same area.
- Backbone Routers - These are the routers located in Area 0 with at least one interface to other routers in the backbone. Area border routers can also be considered as backbone routers.
- AS Boundary Routers - These routers are located in Area 0 with connectivity to other AS; they must be able to handle more than one routing protocol. For example, to exchange information with another AS, they must be able to speak BGP. These routers also have internal interfaces for connectivity to other backbone routers.


R1
BGP
Area 0
R2
R3
R4
R7
R8
R6
R5
R9
R10
Area 1
R11
R12
R13
Area 2
Area 3
R14
R15
R2 - AS Boundary Router
R3, R4, R7 - Core Routers
R5, R6, R8, R13 - Area Border Routers
R9, R10, R11, R12, R14, R15 - Interior Routers

OSPF Network Types

- OSPF is designed to address five different types of networks. They are:
- Point-to-point networks - refers to a type of network topology made up of a direct connection between two routers that provides a single communication path.
- Broadcast networks - refer to networks such as LANs connected by a technology such as Ethernet. Broadcast networks, by nature, are multiaccess where all routers in a broadcast network can receive a single transmitted packet. In such networks, a router is elected as a Designated Router (DR) and another as a Backup Designated Router (BDR).
- Non–broadcast multiaccess networks - use technologies such as ATM or frame relay where more than two routers may be connected without broadcast capability. Thus, an OSPF packet is required to be explicitly transmitted to each router in the network. Such networks require an extra configuration to emulate the operation of OSPF on a broadcast network. Like broadcast networks, NBMA networks elect a DR and a BDR.
- Point-to-multipoint networks - refers to a type of network topology made up of a series of connections between a single interface on one router and multiple destination routers. All interfaces on all routers share the point-to-multipoint connection and belong to the same network.
- Virtual Links - are used to connect an area to the backbone using a non backbone (transit) area. Virtual links are configured between two area-border routers. Virtual links can also be used if a backbone is partitioned into two parts due to a link failure; in such a case, virtual links are tunneled through a non backbone area.

OSPF Operation

- OSPF operation is basically divided into these three categories:
- Neighbor and adjacency initialization – When OSPF is initialized on a router, the router allocates memory for it, as well as for the maintenance of both neighbor and topology tables. Once the router determines which interfaces have been configured for OSPF, it will then check to see if they are active and begin sending Hello packets. The Hello protocol is used to discover neighbors, establish adjacencies, and maintain relationships with other OSPF routers.
- This is done for point-to-point, point-to-multipoint, and virtual link networks. For broadcast and NBMA networks, not all routers become logically adjacent; here, the hello protocol is used for electing DRs and BDRs.
- After initialization the hello protocol is used to keep alive connectivity, which ensures bidirectional communication between neighbors; this means, if the keep alive hello messages are not received within a certain time interval that was agreed upon during initialization, the link/connectivity between the routers is assumed to be not available.
- Broadcast and point-to-point networks send Hellos every 10 seconds, whereas non-broadcast and point-to-multipoint networks send them every 30 seconds.

OSPF Operation

- OSPF operation is basically divided into these three categories:
- LSA flooding - LSA flooding is the method OSPF uses to share routing information. Via Link State Updates (LSU's) packets, LSA information containing link state data is shared with all OSPF routers within an area.
- The network topology is created from the LSA updates, and flooding is used so that all OSPF routers have the same topology map to make SPF calculations with.
- On point-to-point networks, updates use the IP multicast address 224.0.0.5, referred to as AllSPFRouters. A router on receiving an update forwards it to other routers, again using the same multicast address.
- On broadcast networks, all non DR and non BDR routers send link state update and LSA packets using the IP multicast address 224.0.0.6, referred to as AllDRouters. Any OSPF packets that originates from a DR or a BDR, use the IP multicast address 224.0.0.5.
- OSPF flooding must be reliable. OSPF addresses reliable delivery of packets through use of acknowledgments.

OSPF Operation

- OSPF operation is basically divided into these three categories:
- SPF tree calculation - Within an area, each router calculates the best/shortest path to every network in that same area.
- This calculation is based upon the information collected in the topology database and an algorithm called shortest path first (SPF).
- Each router in an area running the SPF algorithm constructs a tree where the router is the root and all other networks are arranged along the branches and leaves.
- This is the shortest path tree used by the router to insert OSPF routes into the routing table. This tree contains only networks that exist in the same area as the router itself does.
- If a router has interfaces in multiple areas, then separate trees will be constructed for each area.

OSPF Authentication

- OSPF packets can be authenticated such that routers can participate in routing domains based on predefined passwords.
- By default, a router uses a Null authentication which means that routing exchanges over a network are not authenticated.
- Two other authentication methods exist. They are:
- Simple password authentication allows a password (key) to be configured per area. Routers in the same area that want to participate in the routing domain will have to be configured with the same key. The drawback of this method is that it is vulnerable to passive attacks.
- Message Digest authentication is a cryptographic authentication. A key (password) and key id are configured on each router. The router uses an algorithm(MD5) based on the OSPF packet, the key, and the key id to generate a "message digest" that gets appended to the packet.