OSPF

OSPF is an open version of the link-state or SPF class of routing protocols. OSPF was designed for use in large, heterogeneous IP networks. OSPF, like all SPF routing protocols, is based on the Dijkstra algorithm. The Dijkstra algorithm enables route selection based on link-state versus distance vectors.

NOTE

OSPF is based on the mathematical concept known as Graph Theory.

OSPF has endured several updates, as the following timeline demonstrates:

- October 1989 / 1131 OSPF specification. J. Moy. Oct-01-1989. Format: TXT=268, PS=857280, PDF=398863 bytes. Obsoleted by RFC 1247. Status: Proposed Standard.
- July 1991 / 1247 OSPF Version 2. J. Moy. Jul-01-1991. Format: TXT=433332, PS=989724, PDF=490300 bytes. Obsoletes RFC 1131. Obsoleted by RFC 1583. Also RFC 1246, RFC 1245. Status: Draft Standard.
- March 1994 / 1583 OSPF Version 2. J. Moy. March 1994. Format: TXT=532636, PS=990794, PDF=465711 bytes. Obsoletes RFC 1247. Obsoleted by RFC 2178. Status: Draft Standard.
- July 1997 / 2178 OSPF Version 2. J. Moy. July 1997. Format: TXT=495866 bytes. Obsoletes RFC 1583. Obsoleted by RFC 2328. Status: Draft Standard.
- April 1998 / 2328 OSPF Version 2. J. Moy. April 1998. Format: TXT=447367 bytes. Obsoletes RFC 2178. Also STD0054. Status: Standard.

OSPF, and later OSPFv2, calculates routes based on the destination IP address found in IP datagram headers, with no provisions made for route calculation to non-IP destinations. OSPF was designed to quickly detect and adapt to changes in the network topology within an autonomous system. OSPF routing decisions are based on the state of the router interconnecting links within the autonomous system. Each OSPF router maintains a database of network link states, including information regarding its usable interfaces, known-reachable neighbors, and link-state information.

Routing table updates, known as LSAs, are transmitted, or flooded, to all other neighbors within a router's area. *Areas* are defined as a logical set of network segments and their attached devices. Areas are usually connected to other areas via routers, making up a single autonomous system.

OSPF was introduced to overcome some of the limitations found with RIP and RIPv2, such as the following:

- RIP and RIPv2 both have a limit of 15 hops. A RIP network that spans more than 15 hops (15 routers) is considered unreachable.
- RIP cannot handle VLSM; however, RIPv2 can. Given the shortage of IP addresses and the flexibility that VLSM gives in the efficient assignment of IP addresses, this is considered a major flaw.
- Periodic broadcasts of the full routing table, without common network and split horizon route statements, consume a large amount of bandwidth. This is a major issue with large networks, especially on slow links and WAN clouds.
- RIP and RIPv2 both converge more slowly than OSPF. In large networks, convergence can be on the order of minutes. RIP routers go through a period of a hold-down and slowly timing-out information that has not been received recently. This is inappropriate in large environments and could cause routing inconsistencies.
- RIP and RIPv2 both have 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 lower delays.
- RIP and RIPv2 networks are flat networks without areas or boundaries. With the introduction of classless routing and the use of network aggregation and summarization, RIP networks struggle to provide a coherent networking infrastructure.

Although RIPv2 supports address summarization with the use of VLSM, the concept of areas is not supported.

Link-state protocols, such as OSPF, provide several networking features that enable a more robust and flexible internetworking environment. These OSPF-enabled features are as follows:

- No hop-count limitation exists.
- VLSM support is useful in IP address allocation.
- OSPF uses IP multicast to send link-state updates. This ensures less processing on routers that are not listening for OSPF packets.
- OSPF updates are "event triggered." This means they are sent only in the case of routing changes occurring within the network instead of periodically.
- OSPF allows for better load balancing.
- OSPF allows for a logical definition of networks in a hierarchical network structure where routers can be divided into areas. This limits the explosion of link-state updates over the entire network. This also provides a mechanism for aggregating routes and cutting down on the unnecessary propagation of subnet information.
- OSPF allows for the transfer and tagging of external routes injected into an autonomous system (AS). This keeps track of external routes that are injected by exterior protocols, such as BGP.

OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. The algorithm alone is quite complicated. The following is a high-level, simplified way of looking at the various steps of the algorithm:

- Upon initialization or due to any change in routing information, a router will generate an LSA. This advertisement will represent the collection of all link-states on that router.
- All routers will exchange link states by means of flooding. Each router that receives a link-state update should store a copy in its link-state database and then propagate the update to other routers.

- After the database of each router is completed, the router will calculate a Shortest Path Tree to all destinations. The router uses the Dijkstra algorithm to calculate the shortest path tree. The destinations, the associated cost, and the next hop to reach those destinations form the IP routing table.
- If no changes in the OSPF network occur, such as cost of a link or a network being added or deleted, OSPF should be quiet. Any changes that occur are communicated via link-state packets, and the Dijkstra algorithm is recalculated to find the shortest path.

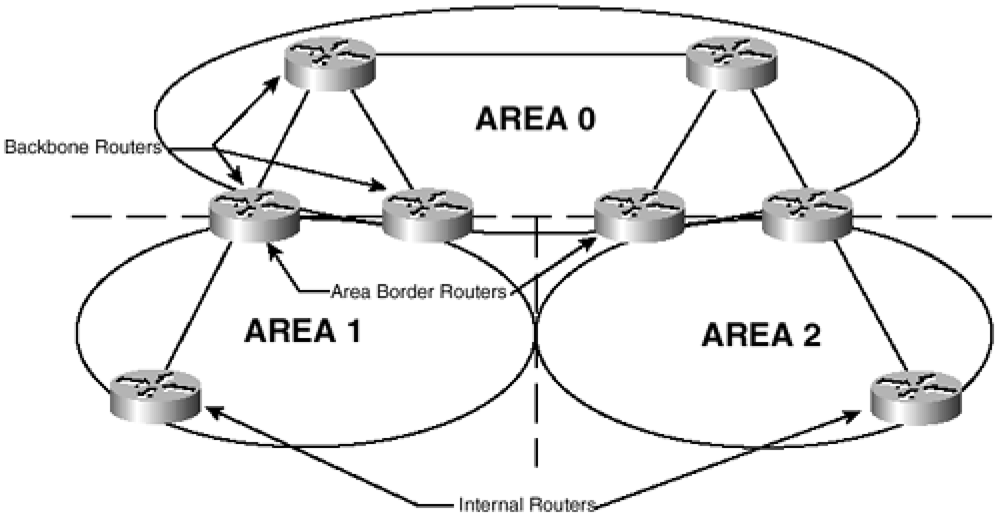
OSPF Areas

OSPF’s rapid convergence is due to its use of areas. OSPF area numbers are 32 bits in length. Area IDs range from 1 to 4,294,967,295 (the theoretical maximum number of OSPF supported areas).

OSPF Area Router Types

Based on area membership, three types of routers exist within an OSPF network (see Figure 24-4):

Figure 24-4. OSPF Areas



- Internal routers— All router interfaces are defined in the same area, but not Area 0 (Backbone Area).
- Area border routers— These interconnect the backbone and its area members.
- Backbone routers— At least one defined interface belongs to Area 0 (Backbone Area).

OSPF Routing Types

OSPF supports two different types of routing:

- Inter-area— Exchanges data between different areas. All inter-area routing must traverse through Area 0. Nonzero OSPF areas are not permitted to communicate directly with each other.
- Intra-area— Routing is self-contained and is limited to the routers internal to a single area.

OSPF Area Types

The area types, listed next, determine what LSAs the area receives. Following are the different area types:

- Stub area— Does not accept external LSAs. LSA Type 5s are rejected. Can accept route summaries.
- Totally stubby areas— Do not accept LSAs with external or summaries.
- Internal routers— Exchange LSAs 1 and 2. They share the same routing database and all interfaces are within the same area.
- Backbone routers (BBR)— Exchange LSAs 1 and 2. Share at least on interface in Area 0.
- Area border router (ABR)— Shares an interface with another OSPF area. This router keeps a database for each area.
- Autonomous system boundary router (ASBR)— Has at least one interface in a non-OSPF network; uses LSA 5s to distribute this routing information into the OSPF network.

OSPF Packets

OSPF uses five different packet types, each designed to support a different specific network function. The packet types include the following:

- Hello packets (Type 1)— Used to establish and maintain relationships, or adjacencies, between neighboring nodes.
- Database description packets (Type 2)— Exchanged between two OSPF routers as they initialize an adjacency. They are used to describe the content of an OSPF router's link-state database. (An adjacency is best defined as the relationship formed between selected neighboring routers and end nodes for the purpose of exchanging routing information. Adjacencies are based on the use of a common media segment.)
- Link-state request packets (Type 3)— Used to request specific pieces of a neighboring router's link-state database.
- Link-state update packets (Type 4)— Used to transport LSAs to neighboring nodes. Eleven types of LSAs exist:

- LSA1— Router Links LSA. Sends information about the routers links.

- LSA2— Network Link LSA. Sent by the designated router (DR) to all routers in the AS containing a list of routers in the segment.

- LSA3— Summary Link LSA. Sent by ABRs that contain a list of networks available outside the area.

- LSA4— Summary Link LSA. Sent by autonomous system boundary routers (ASBRs) that contain a list of networks available outside the area.

- LSA5— External Link LSA. Sent by ASBRs containing a list of external network routes.

- LSA6— Group Membership LSA. Part of Multicast OSPF (MOSPF), which routes multicast packets. As of this writing, Cisco does not support MOSPF, but it does support Protocol Independent Multicast (PIM).

- LSA7— Not-so-stubby area (NSSA) External LSA. Originated by ASBRs in NSSAs. LSA7s operate in the same fashion as LSA5s, with the exception that LSA7s are limited to NSSAs.

- LSA8— External Attributes LSA

- LSA9— Opaque LSA (link-local scope)

- LSA10— Opaque LSA (area-local scope)

- LSA11— Opaque LSA (AS scope)

LSA types 8, 9, 10, and 11 have been proposed, but are not currently implemented.

- Link-state acknowledgement packets (Type 5)— OSPF features a reliable distribution of LSA packets. This reliable distribution means that packet receipt must be acknowledged otherwise source nodes would have no mechanism to determine actual receipt of the LSA.

OSPF Convergence

Regardless of which two methods of route calculation that OSPF uses, the cost of any given route path is the sum of the costs of all interfaces encountered along the path.

OSPF calculates route costs in one of two ways:

- A non-bandwidth–sensitive default value can be used for each OSPF interface.
- OSPF can automatically calculate the cost of using individual router interfaces.

At a minimum, OSPF uses bandwidth to calculate the cost of a route, using the formula ($10^{8/}$Bandwidth). Table 24-7 demonstrates some of these default calculated costs.

Table 24-7. OSPF Link Costs

Interface	OSPF Cost
100 Mbps FDDI/Ethernet	1
45 Mbps T3	2
10 Mbps Ethernet	10
1.544 Mbps T1	~64 (64.7)
56 kbps	1,768

OSPF convergence is based on the adjacency mechanism.

OSPF Adjacencies

Adjacency is the next step after the OSPF neighboring process. Adjacent routers are routers that go beyond the simple Hello protocol exchange and proceed into the database exchange process. To minimize the amount of information exchange on a particular segment, OSPF elects one router to be a DR, and one router to be a backup designated router (BDR), on each multiaccess segment. The BDR is elected as a backup mechanism in case the DR goes down. The idea behind this is that routers have a central point of contact for information exchange. Instead of each router exchanging updates with every other router on the segment, every router exchanges information with the DR and BDR. The DR and BDR relay the information to everybody else.

NOTE

OSPF uses LSAs to become adjacent with each other.

OSPF routers become adjacent when each router has the same link-state database. Following is a brief summary of the states an interface passes through before the router becomes adjacent to another router on that interface:

- Down: No information has been received from anyone on the segment.
- Attempt: On non-broadcast multiaccess clouds such as Frame Relay, this state indicates that no recent information has been received from the neighbor. An effort should be made to contact the neighbor by sending Hello packets at the reduced rate poll interval.
- Init: The interface has detected a Hello packet coming from a neighbor, but bi-directional communication has not yet been established.

- Two-way: Bi-directional communication exists with a neighbor. The router has seen itself in the Hello packets coming from a neighbor. At the end of this stage, the DR and BDR election would have been done. At the end of the two-way stage, routers decide whether to proceed in building an adjacency or not. The decision is based on whether one of the routers is a DR or BDR or the link is a point-to-point or a virtual link.

NOTE

Area 0 is the backbone area that is connected to each OSPF area in the internetwork. In some rare instances, it is impossible to have an area physically connected to the backbone. In this case, a virtual link is used. The virtual link provides the disconnected area a logical path to the backbone.

- Exstart: Routers are trying to establish the initial sequence number that is going to be used in the information exchange packets. The sequence number ensures that routers always get the most recent information. After two OSPF neighboring routers establish bi-directional communication and complete DR/BDR election (on multiaccess networks), the routers transition to the exstart state. In this state, the neighboring routers establish a master/slave relationship and determine the initial database descriptor (DBD) sequence number to use when exchanging DBD packets. The primary router then polls the secondary for information.
- Exchange: Routers describe their entire link-state database by sending database description packets. At this state, packets could be flooded to other interfaces on the router.
- Loading: At this state, routers are finalizing the information exchange. Routers have built a link-state request list and a link-state retransmission list. Any information that looks incomplete or outdated is put on the request list. Any update that is sent is put on the retransmission list until it is acknowledged.
- Full: At this state, the adjacency is complete. The neighboring routers are fully adjacent. Adjacent routers have an identical link-state database.

OSPF Route Summarization

Route summarization is the consolidation of multiple routes in a single route advertisement. Route summarization is normally performed at the area boundaries by the ABRs. It is recommended that you summarize directly into the backbone (Area 0), although summarization can be configured between any two areas. By summarizing routes directly into the backbone, the backbone then turns around and injects these routes into other areas as part of the normal LSA.

Summarization is of two types:

- Inter-area route summarization— Inter-area route summarization is done on ABRs, and it applies to routes from within the AS. It does not apply to external routes injected into OSPF via redistribution.
- External route summarization— External route summarization is specific to external routes that are injected into OSPF via redistribution. It is imperative to ensure that external address ranges being summarized are contiguous. The summarization of overlapping ranges from two different routers could cause packets to be sent to the wrong destination. It is also imperative to ensure that all subnets being summarized are in use within the network; otherwise, routing "black holes" might be created, which leads to dropped traffic.

OSPF Authentication

OSPF provides for link security in the form of routing update authentication. OSPF packets can be authenticated so 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:

- Simple password authentication— 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 must be configured with the same key.

  The drawback of this method is that it is vulnerable to passive attacks. Anyone with a link analyzer could easily get the password off the wire.

- Message Digest authentication (MD5)— Message Digest authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a "message digest" that is appended to the packet. Unlike the simple authentication, the key is not exchanged over the wire. A non-decreasing sequence number is also included in each OSPF packet to protect against replay attacks.

OSPF Security

OSPF configurations can be secured by the following method:

The first step in securing an OSPF routing environment is to configure all participating devices as non-broadcast devices. In non-broadcast, or directed, mode, OSPF devices need to be explicitly configured to communicate with valid OSPF neighbors. This configuration provides a basic layer of security against misconfiguration because valid OSPF devices will only communicate with the OSPF devices with which they have been configured to interoperate. In a broadcast (actually, OSPF is a multicast protocol) OSPF environment, any OSPF devices with the correct configuration parameters for the network will be able to participate in OSPF routing.

On Cisco routers, interfaces will use broadcast OSPF by default. To turn on directed OSPF, use the following interface configuration statement:

```
ip ospf network non-broadcast
```

This command would be issued while at the interface configuration prompt. Under the specific OSPF process configuration, the router’s OSPF neighbors must be explicitly named.

OSPF Authentication

By definition, all OSPF protocol exchanges are authenticated; however, one method of authentication is "none." OSPF authentication can be either none, simple, or MD5.

With simple authentication, the password goes in clear-text over the network. Anyone with a sniffer on the OSPF network segment could pull the OSPF password, and the attacker would be one step closer to compromising the OSPF environment.

With MD5 authentication, the key does not pass over the network. MD5 is a message-digest algorithm specified in RFC 1321. MD5 should be considered the most secure OSPF authentication mode.

To turn on MD5 OSPF authentication on a Cisco router, use the following configuration statement:

```
ip ospf message-digest-key 5 md5 peanutbuttercups
```

This statement should be entered at the interface configuration prompt. In this example, 5 is the key ID and peanutbuttercups is the MD5 key.

Authentication must be turned on for the specific OSPF process ID. This is done with the following statement, at the OSPF process configuration prompt:

```
area 0 authentication message-digest
```

This command turns on MD5 authentication for the OSPF backbone area.

Testing and Troubleshooting

To verify proper OSPF configuration, the following commands might be used:

- **show ip route—** This verifies the routing table.
- **show ip ospf neighbors—** This to verifies the router's OSPF neighbors.
- **debug ip ospf ?—** This turns on OSPF debugging. (Warning: A lot of output can be generated depending on the ? selection.)

OSPF Summary

OSPF is a powerful and feature-rich routing protocol due to its flexibility. OSPF provides a high functionality open protocol standard enabling inter-vendor networking with the TCP/IP protocol suite. Some of the benefits of OSPF include faster convergence than standard distance-vector routing protocols (such as RIP and RIPv2), VLSM support, authentication, hierarchical segmentation, route summarization, and aggregation, which is needed to handle large and complicated networks.

Summary

A router can learn of a network route using two methods: the route is either statically configured or dynamically learned and calculated.