1. Introduction to Dynamic Routing

When the network is small, there is a single connection point to other networks,
and there are no redundant routes, a static routing is enough. But if any of these tree conditions is false, dynamic routing is normally used.

Dynamic routing occurs when routers talk to adjacent routers, informing each other of what network each router is currently connected to. The routers must communicate using a routing protocol that is running by the Routing Daemon. In Contrast to static protocol, the information placed into the routing tables - the routes, are added and deleted dynamically by a routing daemon, as routes change over time. The routing daemon adds a routing policy to the system, choosing which routes to insert into the kernel's routing table. In case of multiple routes to the same destination, the daemon choose which route is the best. In the other side, if a link has gone down, the daemon delete routes connected to that link, and find alternatives to the routes - if exist.

Many different routing protocols are used in big networks. The internet, for example, is divided to collection of autonomous systems ( ASs ) each of which is normally administrated by a single entity. A corporation or University may define an autonomous system. Every autonomous system uses its routing protocol to communicate between the routers in the autonomous system. This is called an Interior Gateway Protocol ( IGP ). The most popular IGP has been RIP. OSPF is a newer IGP that intends to replace RIP, at least in large networks.

RIP , the most widely used routing protocol has some problems: First, RIP has no knowledge of subnet addressing. If the normal 16 bit host ID of a class B address is nonzero, for example, RIP can't tell if the nonzero portion is subnet ID or if the IP address is a complete host address. Some implementations use the subnet mask of the interface through which the RIP information arrived, which isn't always correct.

Second, RIP takes a long time ( some minutes ) to stabilize after the failure of a router or a link. During this time, routing loops may occur.

Third, The use of the hop count as the routing metric omits other variables that should be taken into consideration. Also, a maximum of 15 for the metric limits the sizes of networks on which RIP can be used.

There is an extension to the old RIP , usually called RIP-2. The extensions don't change the protocol , but pass additional information that help with the RIP problems.

The OSPF - Open Shortest Path First - is an alternative to RIP as GIP. It overcomes all the limitations of RIP. OSPF is a link-state protocol, as opposed to RIP , which is distance-vector protocol. In a link-state protocol each router actively tests the status of its link to each of its neighbors, sends this information to its other neighbors and so on. Each router takes this link-state information and build a complete routing table. This method is much faster then the distance-vector protocols, especially in case of changes in the links in the network.

Other features that make OSPF superior to RIP:

1. It can calculate a separate set of routes for each IP type of service.

2. When equal-cost routes to a destination exists, OSPF move the data equally between this routes.

3. OSPF support subnets.

4. Each interface is assigned a dimension-less cost based on throughput,round trip time, reliability and more... . A separate cost can be assigned for each IP type of service.

5. Point to Point links between routers don't need an IP address at each end.
6. OSPF uses multicasting to reduce the load on systems not participating OSPF.

There are more features but we will not mention all of them.

Summary:
The Open Shortest Path First routing protocol may be the answer to managing complex multivendor networks. Common routing protocols, such as IP Routing Information Protocol (RIP), are designed for simple networks that have only a few routers and little redundancy. Such protocols are inefficient in larger networks where routing messages take up significant amounts of bandwidth. One way to address this problem is found in link state protocols, such as OSPF, which produce a more stable network by getting the routers to act on network changes predictably and simultaneously. An OSPF router collects and advertises information about its neighboring routers via a data structure called a router links advertisement. The router calculates and sorts its neighbors, finding all the reachable routers and the most optimal path. Specifics about the OSPF router, including its interface and optimization methods, are discussed in detail.

to go back to the index press here.

2. Abstract

The OSPF is a (link state) routing protocol used by the Internet community. OSPF is classified as an Interior Gateway Protocol (IGP), this means that it distributes routing information between routers belonging to a single Autonomous System. OSPF (Open Shortest Path First) is used over IP. That means that an OSPF packet is transmitted with an IP data packet header. The PROTOCOL field in the IP header is set to 89 for OSPF.

OSPF is designated to be run internal to a single Autonomous System. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a shortest path tree. OSPF recalculates routes quickly in the face of topological changes, utilizing a minimum of routing protocol traffic. Separate routes can be calculated for each IP type of service.

OSPF allows sets of networks to be grouped together. Such a grouping is called an area and it's topology is hidden from the rest of the Autonomous System. This information hiding enables a significant reduction in routing traffic. An area is a generalization of an IP subnetted network.

All OSPF routing protocol exchanges are authenticated. This means that only trusted routers can participate in the AS's routing.

to go to go back to the index press here.
3. Definition of commonly used terms

- **Routing Daemon** - The process on the router that is running the routing protocol.

- **IGP (Interior Gateway Protocol)** - A routing protocol chosen by an Autonomous system.

- **RIP (Routing Information Protocol)** - The world widely used routing protocol. Uses a distance-vector method. The distance vector means the hop counts that every router contains and sent to the other routers.

- **Adjacency** - A relationship formed between selected neighboring routers for the purpose of exchanging routing information. Not every pair of neighboring routers become adjacent.

- **PDU (Protocol Data Unit)** - A fancy word for "packet".

- **AS (Autonomous System)** - A group of routers exchanging routing information via a common routing protocol.

- **DR (Designated Router)** - One router on each multi-access network which generates a link state advertisement for the multi-access network and has other special responsibilities in the running of the protocol. The DR is elected by the Hello Protocol.

- **Hello Protocol** - The part of the OSPF protocol used to establish and maintain neighbor relationships.

- **Link State advertisement (LSP)** - Describes the local state of a router or network. This includes the state of the router's interfaces and adjacencies. Each link state advertisement is flooded throughout the routing domain. The collected link state advertisements of all routers and networks forms the protocol's topological database.

- **Link state routing** - A type of routing protocol in which each router constructs a Link state advertisement listing its neighbors and then broadcasting it to all the routers.

- **Neighboring routers** - Two routers that have an interface to a common network.

- **Router** - A level three Internet Protocol packet switch.

- **2-WAY** - State in which communication between the two routers is bidirectional. This has been assured by the operation of the Hello Protocol. This is the most advanced state short of beginning adjacency establishment. The DR is selected from the set of neighbors in state 2-Way or greater.

4. The topological Database

The AS's topological database describes a direct graph. The vertices of the graph consist of routers and networks. A graph edge connects two routers when they are attached via a physical point-to-point network. An edge connecting a router to a network indicates that the router has an interface on the network. Vertices that can carry transit traffic are indicated on the graph by having both incoming and outgoing edges. There are three types of vertexes: router, network and stub network. Just the first two can carry transit traffic.

OSPF supports three types of physical networks: Point-to-point networks, Broadcast networks and Non-broadcast networks. Each network (stub or transit) in the graph has an IP address and associated network mask. The mask
indicates the number of nodes on the network. Host attached directly to routers appear on the graph as stub network.

The topological database is pieced together from link state advertisements generated by the routers. The neighborhood of each transit vertex is represented in a single, separate link state advertisement.

Figure 1 shows a sample map of an Autonomous System. The rectangle labeled H1 indicates a host, which has a SLIP connection to Router RT12. Router RT12 is therefore advertising a host route. Lines between routers indicate physical point-to-point networks. The only point-to-point network that has been assigned interface addresses is the one joining Routers RT6 and RT10. Routers RT5 and RT7 have EGP (Exterior Gateway Protocol) connections to other Autonomous Systems. A set of EGP-learned routes have been displayed for both of these routers.

A cost is associated with the output side of each router interface. This cost is configurable by the system administrator. The lower the cost, the more likely the interface is to be used to forward data traffic. Costs are also associated with the externally derived routing data (e.g., the EGP-learned routes).

The directed graph resulting from the map in Figure 1 is depicted in Figure 2. Arcs are labeled with the cost of the corresponding router output interface. Arcs having no labeled cost have a cost of 0. Note that arcs leading from networks to routers always have cost 0; they are significant nonetheless. Note also that the externally derived routing data appears on the graph as stubs.
Figure 1: A sample Autonomous System.

the three types of physical networks: point-to-point (RT6<->RT10),
multi-access (N8) and stub access (N7).
Networks and routers are represented by vertices.

An edge of cost X connects Vertex A to Vertex B iff the intersection of Column A and Row B is marked with an X.

5. The shortest-path tree

When no OSPF areas are configured, each router in the Autonomous System has an identical topological database, leading to an identical graphical representation. A router generates its routing table from this graph by calculating a tree of shortest paths with the router itself as root. Obviously, the shortest-path tree depends on the router doing the
The tree gives the entire route to any destination network or host. However, only the next hop to the destination is used in the forwarding process. Note also that the best route to any router has also been calculated. For the processing of external data, we note the next hop and distance to any router advertising external routes.

The resulting routing table for Router RT6 is pictured in Figure 3. Note that there is a separate route for each end of a numbered serial line (in this case, the serial line between Routers RT6 and RT10).

<table>
<thead>
<tr>
<th>Destination</th>
<th>Next Hop</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>N1</td>
<td>RT3</td>
<td>10</td>
</tr>
<tr>
<td>N2</td>
<td>RT3</td>
<td>10</td>
</tr>
<tr>
<td>N3</td>
<td>RT3</td>
<td>7</td>
</tr>
<tr>
<td>N4</td>
<td>RT3</td>
<td>8</td>
</tr>
<tr>
<td>Ib</td>
<td>*</td>
<td>7</td>
</tr>
<tr>
<td>Ia</td>
<td>RT10</td>
<td>12</td>
</tr>
<tr>
<td>N6</td>
<td>RT10</td>
<td>8</td>
</tr>
<tr>
<td>N7</td>
<td>RT10</td>
<td>12</td>
</tr>
<tr>
<td>N8</td>
<td>RT10</td>
<td>10</td>
</tr>
<tr>
<td>N9</td>
<td>RT10</td>
<td>11</td>
</tr>
<tr>
<td>N10</td>
<td>RT10</td>
<td>13</td>
</tr>
<tr>
<td>N11</td>
<td>RT10</td>
<td>14</td>
</tr>
<tr>
<td>H1</td>
<td>RT10</td>
<td>21</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>RT5</td>
<td>RT5</td>
<td>6</td>
</tr>
<tr>
<td>RT7</td>
<td>RT10</td>
<td>8</td>
</tr>
</tbody>
</table>

Figure 3: The portion of Router RT6's routing table listing local destinations.
6. The Hello protocol

The Hello Protocol is responsible for establishing and maintaining neighbor relationships. It also ensures that communication between neighbors is bidirectional. Hello packets are sent periodically out all router interfaces. Bidirectional communication is indicated when the router sees itself listed in the neighbor's Hello Packet. On multi-access networks, the Hello Protocol elects a DR for the network. Among other things, the DR controls what adjacencies will be formed over the network (see below).

The Hello Protocol works differently on broadcast networks, as compared to non-broadcast networks. On broadcast networks, each router advertises itself by periodically multicasting Hello Packets. This allows neighbors to be discovered dynamically. These Hello Packets contain the router's view of the DR's identity, and the list of routers whose Hello Packets have been seen recently.

On non-broadcast networks some configuration information is necessary for the operation of the Hello Protocol. Each router that may potentially become DR has a list of all other routers attached to the network. A router, having DR potential, sends Hello Packets to all other potential DR when its interface to the non-broadcast network first becomes operational. This is an attempt to find the DR for the network. If the router itself is elected DR, it begins sending Hello Packets to all other routers attached to the network.

After a neighbor has been discovered, bidirectional communication ensured, and (if on a multi-access network) a DR elected, a decision is made regarding whether or not an adjacency should be formed with the neighbor. An attempt is always made to establish adjacencies over point-to-point networks and virtual links. The first step in bringing up an adjacency is to synchronize the neighbors' topological databases.

7. The Hello packet

Hello packets are OSPF packet type 1 (see diagram). They are sent out each functioning router interface. They are used to discover and maintain neighbor relationships. On multi-access networks, hellos are also used to elect the DR and the backup DR, and in that way determine what adjacencies should be formed.
In addition, Hello Packets are multicast on those physical networks having a multicast or broadcast capability, enabling dynamic discovery of neighboring routers.

All routers connected to a common network must agree on certain parameters (Network mask, HelloInterval and RouterDeadInterval). These parameters are included in Hello packets, so that differences can inhibit the forming of neighbor relationships.

```
+----------------+----------------+----------------+----------------+
|             0      |             1      |             2      |             3      |
+----------------+----------------+----------------+----------------+
| 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 |
| +----------------+----------------+----------------+----------------+ |
| | Version # | | 1    | | Packet length |
| +----------------+----------------+----------------+----------------+ |
| | Router ID |
| +----------------+----------------+----------------+----------------+ |
| | Area ID |
| +----------------+----------------+----------------+----------------+ |
| | Checksum | | AuType |
| +----------------+----------------+----------------+----------------+ |
| | Authentication |
| +----------------+----------------+----------------+----------------+ |
| | Authentication |
| +----------------+----------------+----------------+----------------+ |
| | Network Mask |
| +----------------+----------------+----------------+----------------+ |
| | HelloInterval | | Options | | Rtr Pri |
| +----------------+----------------+----------------+----------------+ |
| | RouterDeadInterval |
| +----------------+----------------+----------------+----------------+ |
```

8. The Designated router

In OSPF, the DR (which is elected by the hello protocol) is responsible for collecting explicit acknowledgments for each LSP from the other routers. It generates a link state advertisement for the multi-access network. Since the DR in OSPF keeps a lot of state regarding which routers have which LSPs, it would require a lot of time and protocol message for another router to take over in the event that the DR crashed. Therefore, OSPF elects not only a DR but a "backup DR". The backup DR also listens to all the explicit acknowledgments and keeps track of which routers have received which LSPs.
The DR concept enables a reduction in the number of adjacencies required on a multi-access network. This in turn reduces the amount of routing protocol traffic and the size of the topological database.

When a router R has an LSP to propagate on the LAN, R doesn't multicast the LSP to all the other routers. Instead, R transmits it to the DR. But rather than send the LSP to the DR’s personal data link address, R transmits it to the multicast address of all DRs, to which both the DR and the backup DR listen. When the DR receives the LSP, the DR multicasts the LSP to all the other routers. Then the DR collect acks for that LSP, which are transmitted to the multicast address of all the DRs (as described above). If the DR does not receive an ack from a subset of the routers, it sends explicit copies of the LSP to each router in that subset.

So, The DR performs two main functions for the routing protocol:

- The Designated Router originates a network links advertisement on behalf of the network. This advertisement lists the set of routers (including the Designated Router itself) currently attached to the network. The Link State ID for this advertisement is the IP interface address of the Designated Router. The IP network number can then be obtained by using the subnet/network mask.
- The Designated Router becomes adjacent to all other routers on the network. Since the link state databases are synchronized across adjacencies (through adjacency bring-up and then the flooding procedure), the Designated Router plays a central part in the synchronization process.

The Backup Designated Router does not generate a network links advertisement for the network. (If it did, the transition to a new DR would be even faster. However, this is a tradeoff between database size and speed of convergence when the DR disappears.) In some steps of the flooding procedure, the Backup DR plays a passive role, letting the DR do more of the work. This cuts down on the amount of local routing traffic.

Election of the DR

The DR calculation proceeds as follows: Call the router doing the calculation Router X. The list of neighbors attached to the network and having established bidirectional communication with Router X is examined. This list is precisely the collection of Router X's neighbors (on this network) whose state is greater than or equal to 2-WAY. Router X itself is also considered to be on the list. Discard all routers from the list that are ineligible to become DR (routers having router priority of 0).

The following steps are then executed, considering only those routers that remain on the list:

1. Note the current values for the network's DR and backup DR.
2. Calculate the new backup DR for the network as follows: If one or more of the routers have declared themselves backup DR (in their Hello Packets) the one with the highest router priority is declared to be backup DR. In case of a tie, the one having the highest router ID is chosen. If no routers have declared themselves backup DR, choose the router having highest router priority, excluding those routers who have declared themselves DR, and again use the router ID to break ties.
3. Calculate the new DR for the network as follows: If one or more of the routers have declared themselves DR (in their Hello Packets) the one with the highest router priority is declared to be DR. In case of a tie, the one having the highest router ID is chosen. If no routers have declared themselves DR, promote the new backup DR to DR.
4. If router X is now newly the DR (or the backup DR), or is now no longer the DR (or the backup DR), repeat steps 2 and 3. For example, if router X is now the DR, when step 2 is repeated X will no longer be eligible for backup DR election. Among other things, this will ensure that no router will declare itself both DR and backup DR.
5. As a result of these calculations, the router itself may now be DR or backup DR. The router's interface state
should be set accordingly.

6. If the attached network is non-broadcast, and the router itself has just become DR (or backup DR), it must start sending hellos to those that are not eligible to become DR (having a router priority of 0).

7. If the above calculations have caused the identity of the DR (or the backup DR) to change, the set of adjacencies associated with this interface will need to be modified. Some adjacencies may need to be formed, and others may need to be broken (reexamine all the neighbors, whose state is at least 2-WAY, eligibility for adjacency).

Once the DR and the backup DR are elected, OSPF makes every effort to keep them, even if another router subsequently comes up with a higher priority or ID. The reason behind the election algorithm's complexity is the desire for an orderly transition from backup DR to DR, when the current DR fails. This orderly transition is ensured through the introduction of hysteresis: no new backup DR router can be chosen until the old backup accepts its new DR responsibilities.

If router X is not itself eligible to become DR, it is possible that neither a backup DR nor a DR will be selected in the above procedure. Note also that if router X is the only attached router that is eligible to become DR, it will select itself as DR and there will be no backup DR for the network.

to go back to the index press here.

9. OSPF - Algorithm

The OSPF routing algorithm is based on Dijkstra shortest path algorithm. The term "Shortest path" is inaccurate because what we really want to find is the "Optimum path". To find the optimum path in a network means to find a path with a minimal cost, considering factors like time, money and quality of the received data. The route is not chosen only by the cost, because in every network three constraints must be considered:

1. Delay
2. Throughput
3. Connectivity

if delay is excessive or if throughput is too little, the network does not meet the needs of the users. The third constraint is quite obvious: The gateways and networks must be able to reach each other; otherwise, all other least-cost criteria are irrelevant.

The basic algorithm

- Least-cost criteria weights are assigned to the paths in the network.
- Each node is labeled (identified) with its least-cost criteria from the source along to a known path. Initially, no paths are known, so each node is labeled with infinity. However, updates to the values (once the weights are established) are the same as an initialization.
- Each node is examined in relation to all nodes adjacent to it. (The source node is the first node considered and becomes the working node). This step is actually a one time occurrence wherein the source node is initialized with all the costs of all its adjacent nodes.
- Least-cost criteria labels are assigned to each of the nodes adjacent to the working node. Labels change if a shorter path is found from this node to the source node. In OSPF, this would occur with the sending of link status messages on a broadcast basis to all other gateways.
After the adjacent nodes are labeled (or relabeled), all other nodes in the network are examined. If one has a smaller value in its label, its label becomes permanent and it becomes the working node.

If the sum of the node’s label is less than the label on an adjacent node, the adjacent node’s label is changed because a shorter path has been found to the source node.

Another working node is selected and the process repeats itself until all possibilities has been searched. The final labels reveal the least-cost, end-to-end path between the source and the other nodes. These nodes are considered to be within a set N as it pertains to the source node.

The following general statements describe the preceding discussion:

1. Let $D(v) =$ sum of link weights on a given path.
2. Let $C(i,j) =$ the cost between node i and j.
3. Set $N = \{1\}$
4. For each node (v) not in N , set $D(v) = C(1,v)$.
5. For each step, find a node w not in N for which $D(w)$ is a minimum; add w to set N.
6. Update $D(v)$ for all nodes still not in N by $D(v) = \min \{ D(v), D(w) + C(w,v) \}$.
7. Repeat steps 4 through 6 until all nodes are in set N.

The process is performed on each node, and a routing table is created for the node's use. Each node's table is constructed in the same manner just discussed.

Example: Routing topology for node A

<table>
<thead>
<tr>
<th>Step</th>
<th>N</th>
<th>A(B)</th>
<th>A(C)</th>
<th>A(D)</th>
<th>A(E)</th>
<th>A(F)</th>
<th>A(G)</th>
<th>A(H)</th>
<th>A(I)</th>
<th>A(J)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>{A}</td>
<td>8</td>
<td>4</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>1</td>
<td>{A,B}</td>
<td>8</td>
<td>(4)</td>
<td>5</td>
<td>8</td>
<td>.</td>
<td>.</td>
<td>11</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>2</td>
<td>{A,C,D}</td>
<td>7</td>
<td>4</td>
<td>(5)</td>
<td>7</td>
<td>.</td>
<td>.</td>
<td>11</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>3</td>
<td>{A,C,D,B}</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>(7)</td>
<td>11</td>
<td>.</td>
<td>.</td>
<td>11</td>
<td>.</td>
</tr>
<tr>
<td>4</td>
<td>{A,C,D,B,E}</td>
<td>(7)</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>9</td>
<td>.</td>
<td>11</td>
<td>.</td>
</tr>
<tr>
<td>5</td>
<td>{A,C,D,B,E,F}</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>(9)</td>
<td>14</td>
<td>11</td>
<td>.</td>
</tr>
<tr>
<td>6</td>
<td>{A,C,D,B,E,F,G}</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>9</td>
<td>(10)</td>
<td>10</td>
<td>.</td>
</tr>
<tr>
<td>7</td>
<td>{A,C,D,B,E,F,G,H}</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>9</td>
<td>10</td>
<td>(10)</td>
<td>18</td>
</tr>
<tr>
<td>8</td>
<td>{A,C,D,B,E,F,G,H,I}</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>(11)</td>
<td>9</td>
<td>10</td>
<td>10</td>
<td>15</td>
</tr>
</tbody>
</table>
10. OSPF - Routing Protocol

The OSPF routing protocol was designed by the OSPF working group of the Internet Engineering Task Force. This protocol is an IGP: Gateways/routers are all within one autonomous system. Also, as we stated earlier, OSPF is a link state or shortest path first protocol, in contrast to most of the internet protocols, which are based on some type of Bellman-Ford approach. The protocol, although it relies on techniques outside of the internet environment, is tailored specifically for an internet and includes such capabilities as subnet addressing and type of service (TOS) routing.

OSPF bases its routing decisions on two fields in the IP datagram: the destination IP address and the TOS. Once the decision is made on how to the IP datagram, the datagram is routed without additional headers; that is, no additional encapsulation occurs. This approach is different from many networks in which PDUs are encapsulated with some type of internal network header to control the routing protocol within the subnetwork.

OSPF is classified as a dynamic, adaptive protocol in that it adjusts to problems in the network and provides short convergence periods to stabilize the routing table. It is also designed to prevent looping of traffic, which is quite important in mesh networks or in LANs where multiple bridges may be available to connect different LANs.

11. OSPF Operations

Each router contains a routing directory (called a "routing database"). The database contains information about interfaces at the router that are operable as well as status information about each neighbor to a router. the database is the same for all participating routers.

The information focuses on the topology of the networks with a directed graph. Routers and networks forms the vertices of the graph. Periodically this information is broadcast (flooded) to all the routers in the autonomous system. An OSPF router computes the shortest path to all the other routers in the autonomous system regarding itself as the working node (the root).
A very flexible and powerful approach to this protocol is that separate cost metrics can be computed for each TOS. If the calculations reveal that two paths are of equal value, OSPF will distribute the traffic equally on these paths.

OSPF can support one to many networks. The networks can be grouped into what is termed an "area", and the design of the protocol allows an area to be hidden from other areas. Indeed, an area can be hidden from the full autonomous system.

Due to increasing concerns about security, OSPF includes authentication procedures. Routers must go through some simple procedure to authenticate the traffic between them. we have more to say about the authentication aspects of this protocol shortly.

OSPF works with directed graphs which are quite similar to the Dijkstra algorithm explained before. The graph contains values between two points, either networks or gateway. the values represent the weighted shortest path value, with the router established as the root. Consequently, the shortest path tree from the router to any point in an internet is determined by the router performing the calculation. The calculation only reveals the next hop to the destination in the hop-to-hop forwarding process. The topological database used in the calculation is derived from the information obtained by advertisements of the routers to their neighbors, with periodic flooding throughout the autonomous system.

Thus far we have discussed in general terms how OSPF performs routing within the autonomous system. The method to determine routing information outside the autonomous system is referred to as "external routing". Routing information pertaining to this capability is typically derived from OSPF as well as other protocols, such as the EGP. Alternately, routing information could be established through static routes between the autonomous systems.

Two types of external routing capabilities exist with OSPF. In type 1 external routing, the external metrics are the same as the internal OSPF link state metric. Type 2 external metrics only use the cost of the router to the external autonomous system. The type 2 method is simple and based on the assumption that routing between autonomous systems is the major cost of routing the packet (which in some actual operation is not true). This approach eliminates conversion between internal link state metrics of OSPF and external costs. (in which the autonomous system may have little influence).

The OSPF working group also adapted a very sound concept of autonomous system "areas" in which contiguous networks and hosts may be grouped together. In this situation, each area runs its own SPF algorithm. It also has its own topological database that differs from other areas. The purpose of the area is to isolate and partition portions of the autonomous system and to reduce the amount of information a router must maintain about the full autonomous system. Also, having such an area means that the overhead information transmitted between the routers to maintain OSPF routing tables is substantially reduced.

OSPF uses the term "backbone" to define that part of an autonomous system conveys packets between areas. The full path of a packet proceeds as follow:

1. intra-area path to a router attached to the backbone;
2. the backbone path to the destination area router;
3. the destination intra-area path to the destination network.

The resources (Links, Routers) of a backbone should be contiguous. This configuration is permissible; the
OSPF

intervening networks simply become "virtual links" within the backbone for the purposes of constructing the topological database.

OSPF utilizes the Hello protocol for advertising state information between neighbors. Hello packets are used to confirm agreements among routers in a common network about a network mask and certain timers (dead intervals, hello interval). In effect, the Hello protocol is used to make certain that neighbor relationship make sense.

to go back to the index press here

### 12. BIBLIOGRAPHY

- *Internetworking with TCP/IP (Vol I)* - Comer
- *Interconnections, Bridges and Routers* - Radia Perlman
- RFC's 1131, 1245, 1253, 1583

to go back to the index press here