

Overview of OSPF routing protocol

Addicam .V.Sanjay

Abstract

This paper attempts to present an analysis of OSPF routing protocol. This paper will describe how OSPF works. This paper looks into the various components and various definitions, which goes into making an OSPF network. This paper will describe the pros and cons of this routing protocol. It will also try to suggest ideas, which overcomes the various limitations this routing protocol may have. This paper will address the various security features and loop holes related to this protocol. The format of an OSPF packet will be examined and the significance of the various fields in a packet will be explained. This paper will look into the algorithm used in this protocol and what sets it apart from the rest.

How does OSPF work????

OSPF is an internal routing protocol. It is a protocol, which is based on the link state routing protocol. The shortest path to a destination is calculated using Dijkstra's algorithm. OSPF is designed to be run internally in 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. OSPF provides support for equal – cost multi paths. An area routing capability is provided, enabling an additional level of routing protection and a reduction in routing protocol traffic. In addition all OSPF routing protocol exchanges are authenticated.

What goes into making an OSPF network????

OSPF introduces a two-level hierarchy that allows an Autonomous system to be partitioned into several groups called *Areas* that are interconnected by a central backbone area. A 32bit number known as the Area ID identifies an area.

Area border routers are routers, which connect two or more areas. These routers summarize the information from other areas.

Backbone router is a router that has links to a backbone. Autonomous system boundary router is a router that has links to another autonomous system.

Designated router, the purpose of a designated router is to allow the LAN to be treated like a node. 'N' routers on the LAN looks to the routing algorithm like 'N +1' nodes with 'N' links, rather than 'N' nodes with 'N^2' links. The designated router issues

the link state routing information on behalf of the LAN and ensures reliable propagation of link state information on the LAN. In OSPF the designated router election is permanent, meaning that after a router has been elected, nobody can usurp the position unless that router goes down. The designated router is elected by exchange of special packets.

In order to make the transition to a new designated router smoother, there is also a back up designated router.

An OSPF area helps in creating hierarchical address space. A good example of OSPF areas benefits can be seen in a campus environment, where each building is defined as an area. For example, let's take a campus where each building has 12 floors and a router on each floor. Without OSPF areas, routers would have to exchange updates with every other router on the campus, creating, in the process, topology databases that represent every routing node and link. When areas are deployed, routers only exchange link state information with routers in the same building. An area border router in each building forms a link b/w the building and the campus backbone.

When an OSPF router is first activated, it uses OSPF "hello protocol" to discover any neighbors to which it's connected. It then exchanges link-state information with these routers in the form of LSAs (link state advertisements). Using this information, each router creates a database that consists of every interface, its corresponding neighbor and a metric representing the speed of that interface. Each router then uses LSAs to pass this information along to all neighboring routers. Every LSA that a router receives from a neighbor is passed along to its other neighbors in turn until every router receives the LSAs of every other router in the network.

.... And now for the algorithm behind the OSPF protocol, the Link state routing protocol.

OSPF makes use of link state routing protocol. The basic idea behind link state routing protocol is simple. Each router is responsible for meeting its neighbors and learning their names. Each router constructs a packet known as a link state packet, or LSP, which contains a list of the names and cost to each of its neighbors. The LSP is somehow transmitted to all the other routers, and each router stores the most recently generated LSP from each other router. Each router, armed now with a complete map of the topology (the information in the LSPs yields complete knowledge of graph), computes routes to each destination. A router R generates an LSP periodically as well as when R discovers that it has a neighbor or if the cost of the link to an existing has changed or if a link to a neighbor has gone down.

How is this protocol different and hopefully better???

The other major competing algorithm is Distance vector protocol. This is used by the RIP routing protocol. We are now going to do a comparison of Link state routing protocol and Distance vector routing protocol.

Memory: Under certain circumstances link state routing protocol occupies more memory than Distance vector routing protocol. In the higher levels of hierarchical routing, it is not necessary to compute routes to each router. If there are significantly more level n routers than level (n -1) sub networks-- For example, s level n-1 sub networks, n level n routers, and each level n router having k neighbor level n routers-- then the memory requirement

for distance vector routing would be $O(K*S)$, whereas for link state routing, it would be $O(K*N)$.

Bandwidth Consumed: It is difficult to compare the bandwidth consumed by the two algorithms. Distance vector algorithm fair better in the case of parallel links. Less traffic is generated by distance vector algorithm, if one of the parallel links goes down. Link state routing protocol works better in the case of a single link change. In the case of link state protocol only one packet is generated to represent this change.

Computation: Computation like “bandwidth consumed” is difficult to compare b/w the two algorithms. Dijkstra’s algorithm requires processing time proportional to the number of links in the net times the log of the number of nodes in the net, so it is $O(n*k\log n)$. In the case of link state routing, if the only change is in an end node then very less computation power is needed to update the database. If the link between the routers changes then the computation power needed will be more

Robustness: Link state routing is better than distance vector routing protocol. A single router failure can completely bring down the router. In the case of distance vector routing the most common problem is when a router advertises a distance vector consisting of all zero’s. This creates a black hole where in all the other routers send their packets to this malfunctioning router. In case of link state router, the most common problems are when a router advertises about a link that does not exist or when it does not advertise about a link state that exists.

Functionality: Link state routing protocol provides more functionality than distance vector routing protocol. It is easier to discover the topology of the entire network. In distance vector routing, mapping the entire network is very difficult, if not impossible.

Trouble shooting a link state network is easier. Source routing is more easy with link state routing.

Speed of Convergence: Link state routing convergence is faster and easy than distance vector routing. A distance vector routing would converge slower, because a router cannot pass routing information on until it has recomputed its distance vector. In contrast, a router can recognize a new link state packet and forward it before recalculating routes.

Route convergence is the critical point of comparison between link state routing and distance vector routing. The chief argument in favor of distance vector routing is that it might require less memory, but when compared to the cost of routers, the cost of memory is very less.. It is not prudent to switch to a distance vector routing protocol, just on the basis of memory.

Working of the OSPF routing protocol.....

A separate copy of OSPFs routing algorithm runs in each area.

When a router starts, it first initializes the routing data structures. The router then waits for indications from the lower-level protocols that its interfaces are functional.

A router then uses the OSPFs hello protocol to acquire neighbors. The router sends hello packet to its neighbor's and in turn receives their hello packets.

The router will attempt to form adjacencies with some of its newly acquired neighbors. Link state databases synchronized between pairs of adjacent routers. Routing updates are sent and received only on adjacencies.

A router periodically advertises its state, which is also called link state. Link state is also advertised when a routers state changes.

Routers adjacencies are reflected in the contents of its LSAs. This relationship between adjacencies and link states allows the protocol to detect dead routers in a timely fashion.

LSAs are flooded through the area. The flooding algorithm is reliable, ensuring that all routers in an area have exactly the same link state database. This database consists of the collection of LSAs originated by each router belonging to the area. From this database each router calculates a shortest-path tree, with itself as root. This path tree in turn yields a routing table for the protocol.

Security and OSPF

All OSPF protocol exchanges are authenticated. OSPF supports multiple types of authentication; the type of authentication can be configured. On a per network segment basis one of OSPFs authentication types, namely the cryptographic authentication option, is believed to be secure against passive attacks and provide significant protection against active attacks. When using the cryptographic authentication option, each router appends a “message digest” to its transmitted OSPF packets. Receivers then use shared secret key and received digest to verify that each received OSPF packet is authentic.

The quality of security provided by the cryptographic authentication option depends completely on the strength of the message digest algorithm (MD5 is currently the only message digest algorithm specified), the strength of the key being used, and the correct implementation of the security mechanism in all communicating OSPF implementations. It also requires that all parties maintain the secrecy of the shared secret key.

In OSPF, the LSP itself does not contain an authentication field. Instead the authentication field is the header of a link state update packet, and inside there are one or more LSAs. A router that is forwarding the information to a neighbor adds the authentication field in OSPF.

Chinks in the security armor of OSPF!!

One of the problems of OSPF security is that none of the OSPF authentication types provide confidentiality. OSPF security does not provide protection against traffic analysis also. Key management is also not addressed by OSPF specification.

Limitations of OSPF

OSPF, without any options, does not have a deterministic method for establishing routes or distinguishing between packet flows. OSPF takes into consideration, only the shortest distance from Point A to Point B, while routing a packet. If the route is heavily congested, OSPF does not re route high priority, high QOS requirement or time delay sensitive packets through an alternate route.

QOS extensions in OSPF!!! (This should help in overcoming some of limitations of OSPF)

OSPF now supports QOS routing. QOS routing is the process of selecting the path to be used by the packets of a flow based on its QOS requirements e.g. bandwidth or delay. QOS routing improves network utilization and the service levels provided to request with QOS requirements.

OSPF supports computation of QOS routes for flows with bandwidth requirements. The QOS routing extensions to OSPF are based on two main ideas: first,

the LSAs and the topology database have to include network resource information such as available bandwidth, and second, the route computation algorithm has to take this information into account.

OSPF hello packets, Data base description packets and all LSAs include OSPF option field, which enables OSPF routers to support optional QOS capabilities, and to advertise their capability level to other routers. With the help of this mechanism, routers of different capability levels can communicate within an OSPF routing domain.

A modified Bellman-Ford algorithm is used to pre-compute paths from a router to all other routers in the network. This algorithm computes paths of all possible bandwidth values for each destination, and builds a QOS routing table, which is kept apart from the basic QOS routing table. This QOS routing table can be considered as a matrix, where a row corresponds to a destination, and column corresponds to paths that are no longer than 'T' hops away, and has the largest amount of bandwidth among all such paths to the destination. Thus a single matrix entry contains the next hop(s) and the available bandwidth on such paths. The information in this routing table is used to identify all paths that can satisfy the bandwidth requirements of a request. This is done by comparing the requested bandwidth to the available bandwidth in successive columns in the flow's destination row. The search is over when an entry with an available bandwidth larger than the requested one is found. At this point the corresponding next hop is returned and the request is forwarded to that address. If there are several possibilities for next hop, one of them is randomly chosen. With the new OSPF extension, the used metric of hop-count is extended with available link bandwidth and link propagation delay. The route selection

is more emphasized on satisfying the bandwidth requirements, since the primary purpose of the delay metric is to identify high latency links and to avoid them.

And now finally...the conclusion!!!!

OSPF is definitely a better routing protocol than RIP. It converges faster than RIP. It has improved security and authentication. One limitation of OSPF is Key management. Key management is not handled by OSPF, and should be handled by OSPF. OSPF provides strong QOS guarantees and is a right step in the right direction.

Alberto Leon-Garcia and Indra Widjaja, Communication Networks, McGraw-Hill, Toronto, 2000

Stallings William, Local & Metropolitan Area Networks, Prentice Hall, New Jersey, 1999

Perlman Radia, Bridges, Routers, Switches and Internetworking Protocols, Addison Wesley Longman Inc, Massachusetts, 1999

Batista, Elisa (2000, September 15). Home Network's Bitter Brawl. Wire Digital at <http://www.wired.com/news/print/0,1294,38703,00.html>.

Rabinovitch,Eddie. To RIP or To OSPF?, at <http://www.networkcomputing.com/unixworld/feature/002.html>

Giacalone,Spencer (2000, July 24). OSPF overhaul boosts IP performance, at <http://www.nwfusion.com/news/tech/2000/0724tech.html>

Flanagan, William and Passmore, Dave (1999, Nov). Fiber Futures: Circuit-Switched IP Backbones at <http://www.tbq.com/public/whitepapers/fiberfutures.html>

WhitePaper. IP Routing OSPF Version 2, at <http://www.locuz.com/routing1.htm>

Morrissey,Peter (2000, Nov27). IP Routing Primer : Part Four at <http://www.networkcomputing.com/netdesign/iprpart4.html>

Ke, Qiaozhong ; Zhang, Yan; Zhan Jun; Fu, Tao (2001, Jan 18) OSPF—Routing & INTSERV/DIFFSERV Qos in OSPF. Retrieved Oct 25 2001 from the internet.

Michael, Bill (2001, July 05). MPLS: Breaking Through, A Status Report at <http://www.cconvergence.com/article/CTM20010425S0001/1>

RFC 2329, J.Moy, “ OSPF standardization Report,” April 1998.

RFC 2676, G. Apostolopoulos, S.Kamat, R.Guerin, A.Orda and T.Przygienda, “ QoS Routing Mechanisms and OSPF Extensions,” August 1999

RFC 2178, J.Moy, “ OSPF version 2,” July 1997.