RESEARCH ARTICLE OPEN ACCESS

Comparative Analysis of Link State Routing Protocols OPSF and IS-IS

Amanpreet Kaur [1], Er.Dinesh Kumar [2]
Department of Computer Science and Engineering
GZS PTU Campus, Bathinda
Punjab - India

ABSTRACT

IP Routing is used to find the best path for an IP packet from source to destination. Major routing protocols used for interior gateway routing are link state routing protocols, as they are more scalable than their counterparts Distance Vector Routing Protocols. Link State routing protocols has two protocols listed in its category and both of them uses the same Dijkstra's Shortest Path First Algorithm, and both came to existence at about same time. But which protocol is best between the two always creates confusion in the network engineer's minds all around the world. This paper explains the two link state routing protocols used for internal routing purposes in enterprise or service provider networks. Link state routing protocols use the same algorithm but have so many differences. This paper compares both the link state routing protocols on the basis of performance, security and scalability.

Keywords:- IP, OSPF, IPv6, LSA, PDU, LSU, LSR, IS-IS

I. INTRODUCTION

When a datagram is sent between source and destination devices that are on the different networks, the process is known as routing. For IP routing, two types of methods can be used, either we can use Static Routing or we can use Dynamic Routing. In static routing, we add the routes towards destination manually and in dynamic routing, we use dynamic routing protocols that find the best path towards destination dynamically. Dynamic routing protocols are further divided into two categories i.e. Interior Gateway Protocols(IGP) and Exterior Gateway Protocols(EGP). EGPs are used when we need to connect with some other routing domain, currently Border Gateway Protocol is the only EGP in the world. IGPs are used when we need to perform routing on different routers within a single routing domain. IGPs are further divided into two types: Distance Vector Routing Protocols - Based on distance and direction. Routing Information Protocol(RIP),Enhanced Interior Gateway Routing Protocol(EIGRP) and Link State Routing Protocols. As our main emphasis is on Link State Routing Protocols, therefore they are described in the next section.

A. Link State protocols

Link State protocols, also known as shortest path first or distributed database protocols, are built around a well-known algorithm of graph theory, E.W. Dijkstra's shortest path first algorithm. Link State protocols behave like a road map. Each router shares its link information in the form of Link State Advertisement(LSA), or Link State PDU(LSP). A link state router uses link state information to create a topology map and to select the best path to the destination in the topology. LSAs propagates to every neighbor router using protocol specific multicast address, each router that receives the LSA, updates its Link-State-Database(LSDB) and forwards the LSA to its neighbor routers within an area. SPF tree is then applied to the LSDB to find the best path to reach the destination and the best path is then added to the routing table. Dijkstra Algorithm is given :

Dijkstra ( )

{ **//Initialization**

Path={s} **//s means self**

for (i = 1 to N)

{

If (I is a neighbor of s and $I \neq s$) $D_i = C_{si}$

If (I is a not a neighbor of s) $D_i = \infty$

}

$D_s = 0$

}// **Dijkstra**

//**Iteration**

Repeat

{

// Finding the next node to be added

Path = Path $\cup$ i if D_i is minimum among all remaning nodes

// Update the shortest distance for the rest

For(j=1 to M) **//M number of remaining nodes**

{

D_j = minimum $(D_j, D_j + c_{ij})$

} until (all nodes include in the path , M = 0)

Link State Routing Protocol includes -

B. Open Shortest Path First(OSPF)

OSPF is a routing protocol, which is deployed in both enterprise and service provider networks. Network is divided into areas. Area 0 is known as backbone area, for every other area 0 connect with any other area except area 0, they have to reach via area 0 as transit area. OSPF behaves like a distance vector routing protocol when sharing routes from one area to other area. OSPF uses Link State Advertisements(LSAs) to share information regarding routes in the network. Figure showing basic OSPF implementation is shown below:

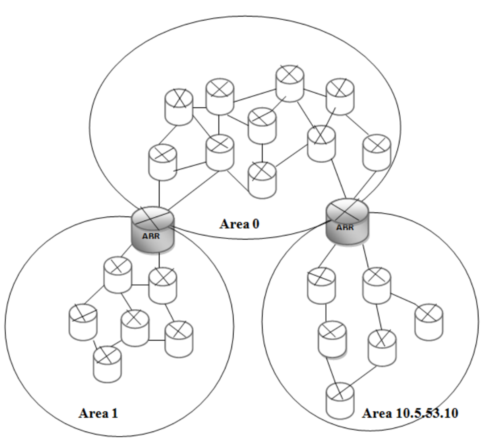

Figure 1: Basic OSPF Implementation

C. Intermediate-System-to-Intermediate-System(IS-IS)

It is a link state protocol similar to OSPF, used in core of SP networks. It was originally not an IP protocol, and is a part of CLNS stack, Integrated IS-IS is an IP extension of IS-IS. It is highly scalable and have a simple flat network design. It supports both IPv4 and IPv6. IS-IS use Dijkstra's SPF algorithm to find the best path. IS-IS also uses a different addressing format than of OSPF. It uses ISO NSAP Addressing format, whose maximum size is 20 bytes and minimum size of 8 bytes. It uses two "levels" of adjacency - Level 2(L2) and Level 1(L1).

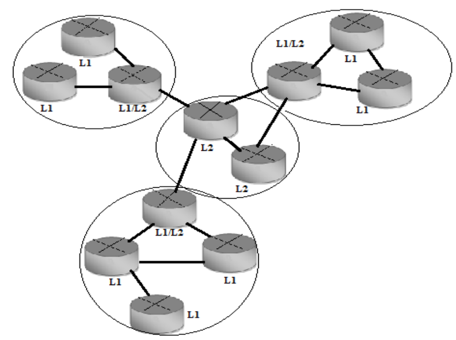

Figure2: Basic Integrated IS-IS implementation.

II. LITERATURE SURVEY

OSPF Version 2 [1] by J. Moy in Internet Engineering Task Force(IETF) RFC - 2328 documents version 2 of the OSPF protocol. This document represents international standard document used for OSPF. It is designed 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. IETF RFC 2328 is the standard in use for IPv4 OSPF design and implementation.

The OSPF Not-So-Stubby Area (NSSA) Option[2] by P. Murphy of US Geological Survey in IETF RFC 3101 documents an optional type of Open Shortest Path First(OSPF) area that is referred to as "not-so-stubby" area (or NSSA). NSSAs are similar to the existing OPSF stub area configuration option but have the additional capability of importing AS external routes in a limited fashion. OSPF NSSA option was originally defined in IETF RFC 1587. RFC 3101 is the current document used in NSSA implementation.

Graceful OSPF Restart[3] by J. Moy of Sycamore Networks, P. Pillay-Esnault of Juniper Networks and A. Lindem of Redback Networks in IETF RFC 3623 documents an enhancement to the OSPF routing protocol, whereby an OSPF router can stay on the forwarding path even as its OPSF software is restarted. This is called"graceful restart" or "non-stop forwarding". A restarting router may not be capable of adjusting its forwarding in a timely manner when the network topology changes. In order to avoid the possible resulting routing loops, the procedure in this memo automatically reverts to a normal OSPF restart when such a topology change is detected, or when one or more of the restarting router's neighbors do not support the enhancements in this memo. Proper network operation during a graceful restart makes assumptions upon the operating environment of the restarting router; these assumptions are also documented.

Routing Extensions for Discovery of Multiprotocol (MPLS) Label Switch Router (LSR) Traffic Engineering (TE) Mesh Membership[4] by S. Yasukawa of NTT, S. Previdi, P. Psenak of Cisco Systems and P. Mabbey of Comcast in IETF RFC 4972 specifies the setup of a full mesh of Multi-Protocol Label Switching(MPLS) Traffic Engineering(TE) Label Switched Paths(LSP) among a set of Label Switch Routers(LSR), which is a common deployment scenario of MPLS Traffic Engineering either for bandwidth optimization, bandwidth guarantees or fast rerouting with MPLS Fast Reroute. Such deployment may require the configuration of a potentially large number of TE LSPs.

OSPF for IPv6 [5] by R. Coltun of Acoustra Productions, D. Ferguson of Juniper Networks, J. Moy of Sycamore Networks and A. Lindem, Ed of Redback Networks in IETF RFC 5340 describes the modifications to OSPF to support version 6 of the Internet Protocol (IPv6). Changes between (OSPF for IPv4, OPSF v2) and (OSPF for IPv6, OSPF v3) are described in this document. Addressing semantics have been removed from OSPF packets and the basic Link State Advertisements(LSAs). New LSAs have been created to carry IPv6 addresses and prefixes. OSPF now runs on a per-link basis rather than on a per-IP-subnet basis. Flooding scope for LSAs has been generalized. Authentication has been removed from the OSPF protocol and instead relies on IPv6's Authentication Header and Encapsulating Security Payload.

OSPFv3 Graceful Restart [6] by P. Pillay-Esnault of Cisco Systems and A. Lindem of Redback Networks in IETF RFC 5187 describes the OSPFv3 graceful restart. The OSPFv3 graceful restart is identical to that of OSPFv2 except for the differences described in this document. These differences include the format of the grace Link State Advertisements (LSAs) and other considerations.

Traffic Engineering Extensions to OSPF Version 3 [7] by K. Ishiguro, V. Manral of IP Infusion, A. Davey of Data Connection Limited and A. Lindem, Ed. of Redback Networks in IETF RFC 5329 describes extensions to OSPFv3 to support intra-area Traffic Engineering (TE). This document extends OSPFv2 TE to handle IPv6 networks. A new TLV and several new sub-TLVs are defined to support IPv6 networks.

OSPF Extensions in Support of Inter-Autonomous System (AS) MPLS and GMPLS Traffic Engineering [8] by M. Chen, R. Zhang of Huawei Technologies, X. Duan of China Mobile in IETF RFC 5392 describes extensions to the OSPF version 2 and 3 protocols to support Multiprotocol Label Switching (MPLS) and Generalized MPLS (GMPLS) Traffic Engineering (TE) for multiple Autonomous Systems (ASes). OSPF-TE v2 and v3 extensions are defined for the flooding of TE information about inter-AS links that can be used to perform inter-AS TE path computation.

OSI IS-IS Intra-domain Routing Protocol [9] by D. Oran of Digital Equipment Corporation in IETF RFC 1142 is a republication of ISO DP 10589 as a service to the Internet community.

Use of OSI IS-IS for Routing in TCP/IP and Dual Environments [10] by R. Callon of Digital Equipment Corporation in IETF RFC 1195 specifies an integrated routing protocol, based on the OSI Intra-Domain IS-IS Routing Protocol, which may be used as an interior gateway protocol (IGP) to support TCP/IP as well as OSI. This allows a single routing protocol to be used to support pure IP environments, pure OSI environments, and dual environments. This specification was developed by the IS-IS working group of the Internet Engineering Task Force.

Restart Signaling for IS-IS[12] by M . Shand and L.Ginsberg of Cisco Systems in IETF RFC 5306 describes a mechanism for a restarting router to signal to its neighbors that it is restarting, allowing them to reestablish their adjacencies without cycling through the down state, while still correctly initiating database synchronization. This document additionally describes a mechanism for a restarting router to determine when it has achieved Link State Protocol Data Unit (LSP) database synchronization with its neighbors and a mechanism to optimize LSP database synchronization, while minimizing transient routing disruption when a router starts.

IS-IS Extensions for Traffic Engineering [13] by T. Li of Redback Networks in IETF RFC 5305 describes extensions to the Intermediate System to Intermediate System (IS-IS) protocol to support Traffic Engineering(TE). This document extends the IS-IS protocol by specifying new information that an Intermediate System (router) can place in Link State Protocol Data Units (LSP). This information describes additional details regarding the state of the network that are useful for traffic engineering computations.

Routing IPv6 with IS-IS[14] by C. Hopps of Cisco Systems in IETF RFC 5308 specifies a method for exchanging IPv6 routing information using the IS-IS routing protocol. The described method utilizes two new TLVs: a reachability TLV and an interface address TLV to distribute the necessary IPv6 information throughout a routing domain. Using this method, one can route IPv6 along with IPv4 and OSI using a single intra-domain routing protocol.

IPv6 Traffic Engineering in IS-IS [15] by J. Harrison , J. Berger and M. Barlett of Metaswitch Networks in IETF RFC 6119 specifies a method for exchanging IPv6 traffic engineering information using the IS-IS routing protocol. This information enables routers in an IS-IS network to calculate traffic-engineered routes using IPv6 addresses.

OSPF and IS-IS: A Comparative Anatomy [16] by Dave Katz, of Juniper Networks does a comparative analysis of OSPF and IS-IS protocol.

III. PROBLEM DEFINITION

As stated in the Introduction part of this document, when IETF was to choose between OSPF and IS-IS routing protocol to make them as the standard Interior Gateway Routing Protocol of the internet, they left that to Internet Service Providers and Enterprise Networks by making both protocols as standards and let the ISP and Enterprise select which routing protocol they want to use.

- There are no perfect documentation on which is the better routing protocol of the two.
- ISO engineers say that ISIS is best, while according to IETF engineers, OSPF is the best.
- Both protocols use the same algorithm, yet they are so different.

IV. OBJECTIVE

- To find the best link-state routing protocol on the basis of performance, security, scalability, and usage of CPU resources.

- To find the best link-state routing protocol for service provider networks for their core network.

V. RESULTS

A. Performance Analysis of OSPF and ISIS protocol using default parameters

OSPF and IS-IS both define their network within areas. OSPF has a backbone area i.e. Area 0.0.0.0 or Area 0. In OSPF, there is a prerequisite for every non-backbone area, that in order for a non-backbone area to connect or share routes with any other non-backbone area, there has to be a backbone area as a transit point in between them. Without Area 0 in between two non-backbone areas by default do not share their routes. OSPF topology can be either single-area or multiple-area. A single area OSPF design is show below.

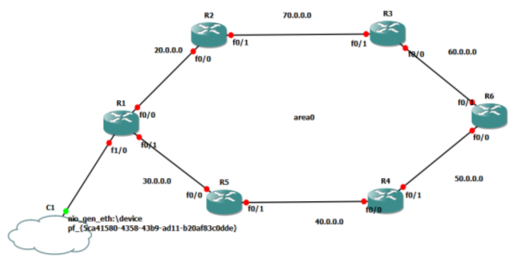

Figure 3-OSPF and ISIS design

In the above OSPF single area network design, six routers are used and all are in the same area i.e. Area 0, and the cloud C1 is our Laptop's loopback address used to connect PRTG Traffic Analyzer and Monitoring Tool with our topology. Here we will monitor R6's loopback address 6.6.6.6 with PRTG, which will send a simple ping to 6.6.6.6 every second to monitor its performance and availability. We have two paths towards destination and the best path is via R1-R2-R3-R6-6.6.6.6, Following graph in Figure 1.2 will show the amount of time that the link takes to converge if the best link to 6.6.6.6 is failed. Graph shown below is taken without tuning any OSPF timers and LSA pacing mechanism, also no other faster convergence mechanism like Bi-directional Forwarding Detection (BFD)or SPF Throttling is used :

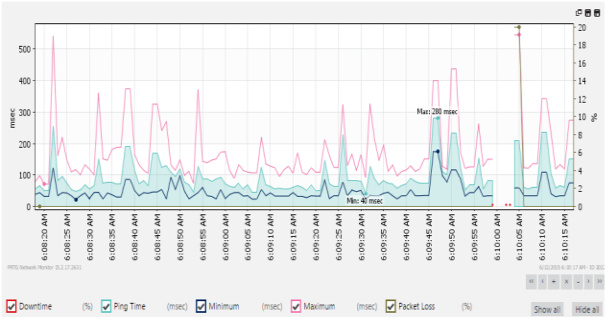

Figure 4-PRTG Graph shows the amount of time it takes to converge the link from primary to secondary link

In the above graph created from PRTG Traffic Monitoring Tool, amount of time(minimum or maximum) in msec is shown for a packet to reach destination is also shown. Its clear from the above PRTG generated graph that OSPF takes around 5 seconds to converge from primary to backup link, if the primary link goes down. In the above topology we have not used any faster convergence protocol like Bidirectional Forwarding Detection or Fast Routing Convergence method like Throttling Shortest Path First(SPF) timers.

IS-IS on the other hand is also used in service provider networks for their internal networks. There is always a debate regarding the best interior gateway routing protocol in service provider networks. OSPF and ISIS have so many similarities as both are link-state routing protocols and uses the same Shortest Path First(SPF) algorithm, yet they are so different as one of them is used is IP based, and other one is created for ISO CLNS environments and then it was adopted by IETF and named it Integrated IS-IS. Topology that we used is show below :

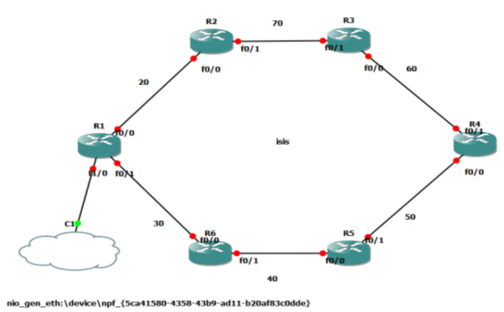

Figure 5 - Integrated IS-IS Single Area Topology

IS-IS is conceptually similar to OSPF in so many ways, originally developed by ISO, ISIS referred a router as an IS(Intermediate System) and a host or end system as an ES(End System).

In the above IS-IS network design, all the routers come under the same IS-IS area, with R1-R2-R3-R4- 4.4.4.4 as the primary link and R1-R6-R5-R4-4.4.4.4 as secondary link with 4.4.4.4 is connected with R4. The convergence time in IS-IS with default setting without tuning any timers or changing any other parameters is show below with the help of a graph created in PRTG traffic monitoring tool :

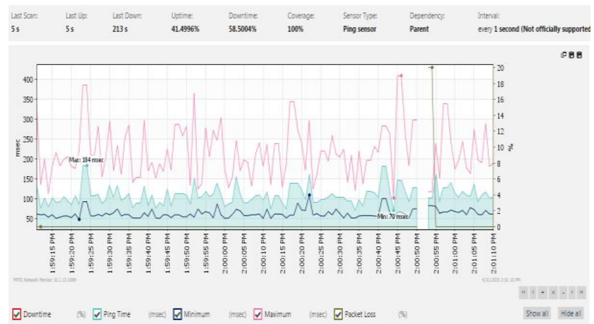

Figure 6- IS-IS Convergence time graph in PRTG

Now as shown above, IS-IS gives much lesser downtime as compared to OSPF.

IS-IS, when use same area for its entire network has a much lesser convergence time by default, i.e. 3 seconds. IS-IS protocol supports a two level hierarchy to scale routing in large networks. Table below displays default convergence difference between ISIS and OSPF.

TABLE 1-Default convergence difference between ISIS and OSPF

Protocol	**Convergence Time**
OSPF	5 seconds
Integrated IS-IS	3 seconds

As we can see in the above table, 5 seconds and 3 seconds are the default convergence time that OSPF and IS-IS can take, in case if the primary link goes down and convergence needs to happen towards Backup Link. Default convergence time is way too much for today's networks, but we can shorten the times by using techniques like decreasing the hello and SPF calculation timers of protocols or we can also use Bidirectional Forwarding Detection feature with OSPF and ISIS, which can provide sub-second convergence from primary to backup link in case of primary link failure.

As both OSPF and IS-IS routing protocols use the same Dijkstra's Shortest Path First(SPF) algorithm, i have tries to fasten the SPF calculations in order to check what effect does it make to the convergence time. What i have done is, i changed the "Delay between receiving a change to SPF calculation to 100msec", "Delay between first and second SPF calculation to 100msec" and "Maximum wait time for SPF calculations to 120msec". The result after configuring SPF timers is shown below in a graph :

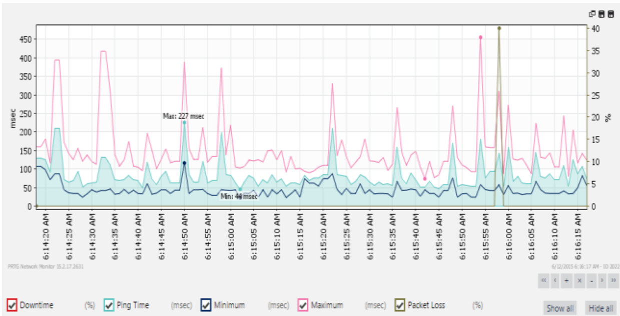

Figure 7-Convergence Time after fasten the process of SPF calculation

As we can see from the above graph, after tuning SPF timers, convergence time has decreased to sub-second, which is much better than the default timers. Both ISIS and OSPF can give sub-second convergence after tuning SPF timers.

TABLE 2-SPF fast convergence between ISIS and OSPF:

Protocol	Convergence Time (Default Parameters)	Convergence Time (With SPF timers tuned)
OSPF	5	Sub-Second
ISIS	3	Sub-Second

B. Performance Analysis of Link State Routing Protocols using IPv6

OSPF and ISIS, both can run in IPv4 and IPv6 environments, OSPF when used with IPv6 is known as OSPFv3 and is quite different than OSPFv2. I have also used OSPFv3 for performance analysis. Topology used for OSPFv3 performance analysis is shown below:

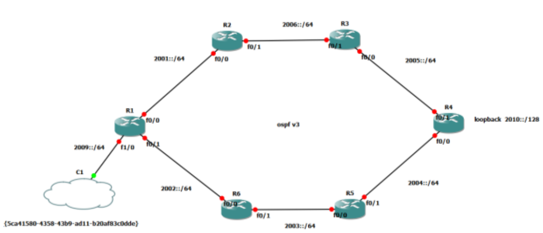

Figure 8- OSPFv3 topology used for Performance Analysis

Above topology is used for OSPFv3 performance analysis, cloud shown in above diagram is acting as a PC having PRTG installed and is testing the reachability towards R4's loopback address 2010::1 address. In the topology, R1 has two paths to reach R4, one via R2 and R3 and the other one via R5 and R6, By default the best path is decided on the basis of cost from source to destination, path with the least cost becomes the best path towards destination, if two paths have same cost from source to destination, then both enters into routing table. In our case, traffic is going through R2 and R3 which is the better link with the better cost, but when the link between R2 and R3 goes down, how fast does the network converge is shown in the graph below:

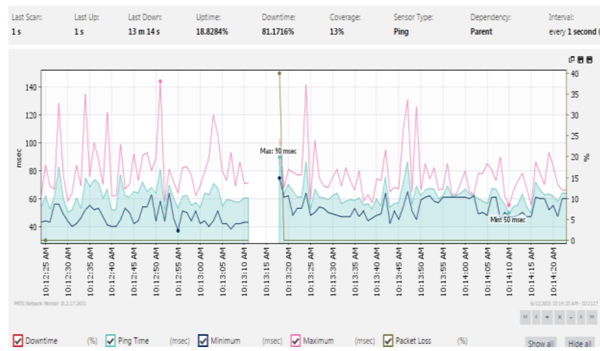

Figure 9- Graph showing the maximum, minimum and convergence time in OSPFv3 implementation using PRTG

On the other hand, when i use ISIS with IPv6, it is much easier to implement, as it has the same version for both IPv4 and IPv6. Topology used for ISIS with IPv6 is same as in the OSPFv3 with just routing protocol is changed from OSPFv3 to ISIS. IPv6 addressing is used is still the same. Results taken from the ISIS with IPv6 topology in case of primary link failure is shown below:

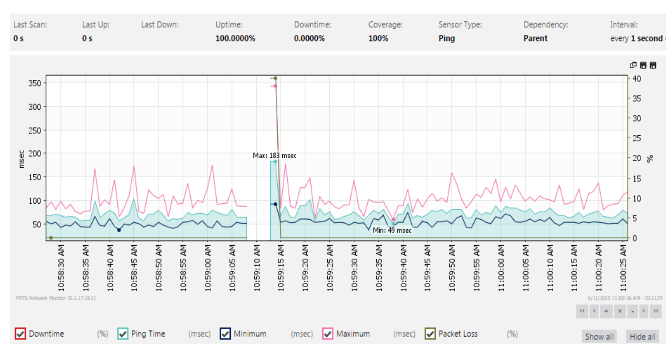

Figure 10- Graph showing the maximum, minimum and convergence time in ISIS with IPv6 implementation using PRTG

As the above graph shows, the maximum time to complete a simple ping packet is 183msec, minimum time is 49msec and the convergence time between the primary link failure and traffic shift from primary link towards backup link is 5 seconds. Therefore with default parameters, ISIS with IPv6 is again better than OSPFv3. Table below shows the comparison of convergence times of both OSPFv3 and IS-IS with IPv6.

TABLE 3- Convergence between OSPFv3 and ISIS with IPv6.

Protocol	**Convergence Time**
Open Shortest Path First-Version 3 (OSPFv3)	7 seconds
Intermediate-System to Intermediate-System with Ipv6 (ISIS with IPv6)	5 seconds

C. *Security Analysis of Link State Routing Protocols:*

Security is always one of the major concerns of Network Industry. By default routing protocols share routing information with their neighbor routers in a very insecure manner. We can use passwords for neighbor authentication, so that routing protocols can share their routing information only if their passwords match. I have used neighbor authentication with both the link state routing protocol and captured the OSPF and ISIS packets in Wireshark Packet Sniffer to gather some more information regarding the authentication in order to compare both authentication mechanisms.

1) *IS-IS Neighbor Authentication*

ISIS supports both clear-text and MD5 based authentication. In ISIS, we can apply authentication on three levels: between routers, area-wide(Level 1), and Domain-wide(Level2). Authentication is always configured separately for L1 and L2 adjacencies. If no level is defined during authentication process, then authentication is applied to both L1 and L2 levels. Authentication in ISIS authenticates the Hello Protocol Data Units(PDUs). ISIS uses key-chain mechanism for password authentication which is used mainly to configure multiple passwords according to time.

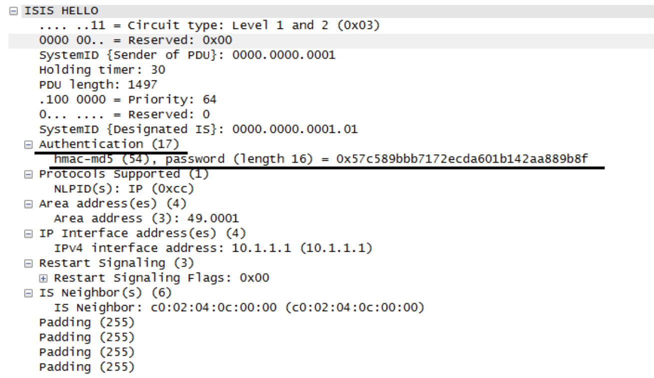

Figure 11- Wireshark Capture of a Hello Protocol Data Unit with authentication applied.

Above capture in Wireshark shows the Hello PDU in ISIS protocol, It also displays the neighbor authentication is used with MD5 hashing algorithm is in use.

2) *OSPF Neighbor Authentication*

In OSPF, authentication can be configured in two ways; either it can be for area or for specific neighbor connected with some interface. If area based authentication is applied, then it must be configured for the entire area, while interface passwords need not to be matched on entire area. OSPF supports three authentication types: Null Authentication, Clear Text Passwords, MD5 cryptographic checksums.Authentication keys are locally significant to an interface in case of interface based passwords, and can be different on a per interface basis.

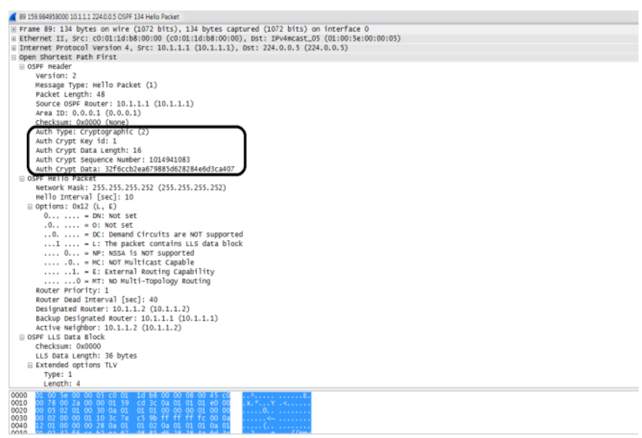

Figure 12- Wireshark capture of OSPF Hello packet showing Authentication Applied.

3) *Link State Routing Protocols with IPSec Applied*

IPSEC is a protocol suite or a collection of protocols and algorithms to protect IP packets at Layer 3, which is the reason, its also known as IPSecurity or IPSec. IPSec provides the benefits of confidentiality through encryption, data integrity through hashing and hmac, and authentication using pre-shared keys and digital signatures. Apart from these, IPSec also provides anti-replay support. A graph below shows the IP traffic from source to destinations and packets which are encrypted and decrypted.Below graph is taken from Cisco Configuration Professional.

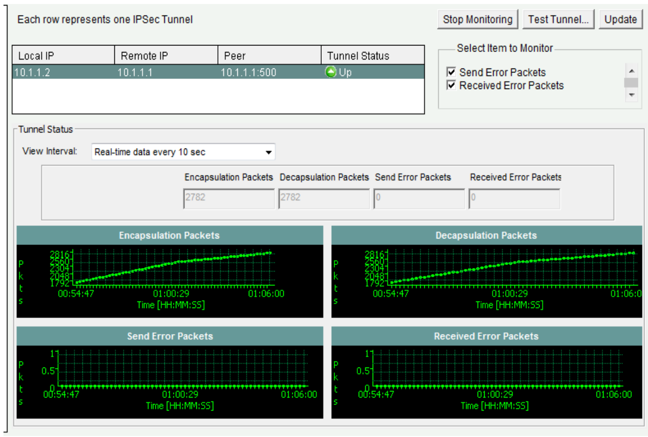

Figure 13- Graphs showing Encrypted and Decrypted IP traffic.

D. *Scalability Analysis of OSPF and IS-IS Protocol*

Large Internet Service Provider networks can be created by building a large Level-1(L1) area without adding any hierarchies in IS-IS and it can still work in better manner than if OSPF has a large number of routers present in a single area. Inter-Area traffic engineering has lots of issues and is not easy to manage, therefore most service providers prefer to use single area design which can be much easy to manage. With ISIS, big networks can be made without having hierarchical design as all IP prefixes are considered as leaf nodes in the Shortest Path First for IS-IS. The best thing with SPF in ISIS is that full SPF calculation is not triggered for an interface or a route flapping instance, while OSPF does full SPF calculation every time any information changes. Graph below shows rising CPU utilization with ISIS and OSPF:

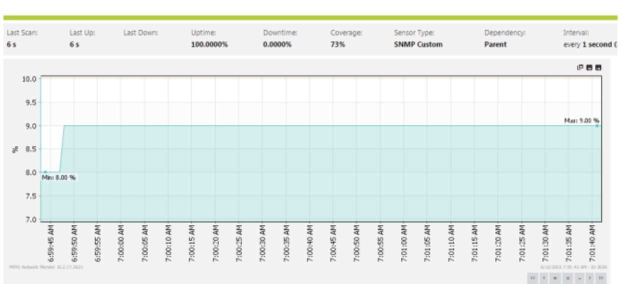

Figure 14 - ISIS Scalability graph with rising traffic.

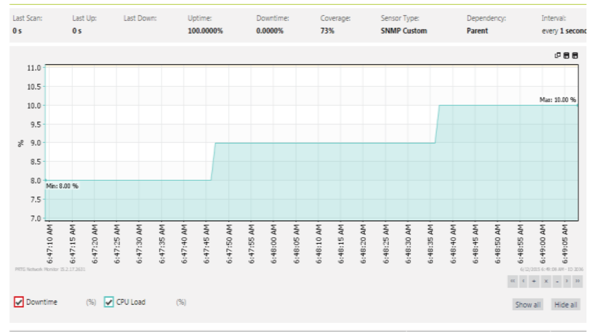

Figure 15- OSPF scalability graph with rising traffic

TABLE 4- Performance Table of Link State Routing Protocols

Protocol	**Convergence Time**	**Convergence Time with SPF Timers**
Open Shortest Path First v2	5 seconds	Sub-Second
Intermediate-System to Intermediate-System	3 seconds	Sub-Second
Open Shortest Path First-Version 3 (OSPFv3)	7 seconds	1.5-2seconds
Intermediate-System to Intermediate-System with Ipv6 (ISIS with IPv6)	5 seconds	Sub-Second

VI. CONCLUSION AND FUTURE SCOPE

OSPF and ISIS, both use the same algorithm to find the best path.ISIS behaves much better with default parameters, and converges the network in 3 seconds while OSPF takes around 5 seconds. When SPF timers are decreased to milliseconds then the convergence time also decreased to sub-second for both protocols. For security analysis, neighbor authentication passwords for secure sharing of IP packets between both the routing protocols have used. OSPF and ISIS both uses MD5 hashing technique but ISIS has the ability to use the key-chain, with which we can create multiple passwords according to time, while OSPF uses interface or area based passwords. To secure IP routing process of OSPF and ISIS, IPSec is also used, which provides encryption, hashing, authentication features to both the protocols providing them security over Public networks like internet. In scalability perspective, ISIS behaves better than OSPF in larger Service Provider Networks, as it can have a large single area and it doesn't run full SPF calculation when some route flaps, therefore it straightway results in lesser consumption of CPU resources. Also ISIS uses TLV format, with which if we want to add some new feature, it can be easily added with new TLV, which is not the case with OSPF.

OSPF and ISIS are the pioneer IGPs used in Service Provider Industry for their Core Networks. Link State routing protocols are improving with the time. With all the IP traffic increasing at rate higher than ever, there needed to be some improvements needed in terms of scalability as the service provider and enterprise routers will get more routing traffic than before and it can only increase with time therefore there is need of more efficiency in Link State Routing Protocols.

ACKNOWLEDGMENT

This paper has been made possible through the constant efforts and help from my parents and guide. I would like to thank Assosiate Prof. Er. Dinesh Kumar, for his guidance, help and valuable suggestions.

REFERENCES

[1] OSPF Version 2 by J. Moy in Internet Engineering Task Force(IETF) RFC - 2328

[2] The OSPF Not-So-Stubby Area (NSSA) Option by P. Murphy of US Geological Survey in IETF RFC 3101

[3] Graceful OSPF Restart by J. Moy of Sycamore Networks, P. Pillay-Esnault of Juniper Networks and A. Lindem of Redback Networks in IETF RFC 3623

[4] Routing Extensions for Discovery of Multiprotocol (MPLS) Label Switch Router (LSR) Traffic Engineering (TE) Mesh Membership by S. Yasukawa of NTT, S. Previdi, P. Psenak of Cisco Systems and P. Mabbey of Comcast in IETF RFC 4972

[5] OSPF for IPv6 by R. Coltun of Acoustra Productions, D. Ferguson of Juniper Networks, J. Moy of Sycamore Networks and A. Lindem, Ed of Redback Networks in IETF RFC 5340

[6] OSPFv3 Graceful Restart by P. Pillay-Esnault of Cisco Systems and A. Lindem of Redback Networks in IETF RFC 5187

[7] Traffic Engineering Extensions to OSPF Version 3 [7] by K. Ishiguro, V. Manral of IP Infusion, A. Davey of Data Connection Limited and A. Lindem, Ed. of Redback Networks in IETF RFC 5329

[8] OSPF Extensions in Support of Inter-Autonomous System (AS) MPLS and GMPLS Traffic Engineering by M. Chen, R. Zhang of Huawei Technologies, X. Duan of China Mobile in IETF RFC 5392

[9] OSI IS-IS Intra-domain Routing Protocol by D. Oran of Digital Equipment Corporation in IETF RFC 1142

[10] Use of OSI IS-IS for Routing in TCP/IP and Dual Environments by R. Callon of Digital Equipment Corporation in IETF RFC 1195

[11] Routing Extensions for Discovery of Multiprotocol (MPLS) Label Switch Router (LSR) Traffic Engineering (TE) Mesh Membership by JP. Vasseur, Ed. , S. Previdi, P. Psenak of Cisco Systems, JL. Leroux, Ed. of France Telecom, S. Yasukawa of NTT, and P. Mabbey of Comcast in IETF RFC 4972

[12] Restart Signaling for IS-IS by M . Shand and L.Ginsberg of Cisco Systems in IETF RFC 5306

[13] IS-IS Extensions for Traffic Engineering by T. Li of Redback Networks in IETF RFC 5305

[14] Routing IPv6 with IS-IS by C. Hopps of Cisco Systems in IETF RFC 5308

[15] IPv6 Traffic Engineering in IS-IS by J. Harrison , J. Berger and M. Barlett of Metaswitch Networks in IETF RFC 6119

[16] OSPF and IS-IS: A Comparative Anatomy by Dave Katz,of Juniper Networks-http://www.nanog.org/meetings/nanog19/presentations/katz.ppt

[17] Cisco OSPF Configuration Guide- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/12-4t/iro-12-4t-book/iro-cfg.html

[18] Cisco IS-IS for IP Configuration Guide- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/15-mt/irs-15-mt-book/is-is_overview_and_basic_configuration.html