ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

# Identifying the Shortest Path during Data Transmission in Networks Using OSPF Protocol

[1]Karthikeyan.R, [2]Madhusudhanan.M, [3]Precila.A, [4] Dr.Kavitha M ,

[1]*UG Student, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore-641 035,*

[4]*Assistant Professor, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore-641 035,*

*Mail Id: kkeyanr08@gmai.com*

***Abstract*--- New study which contains the details related to the appropriate software and hardware products, IP address schema, required services and features, network diagram and explanation on the integration plan to achieve the solution. OSPF is a complex link-state routing protocol. Link-state routing protocols generate routing updates only when a change occurs in the network topology. OSPF supports complex networks with multiple routers, including backup routers. OSPF executes its own particular transport layer error location and amendment capacities. OSPF utilizes multicast tending to for disseminating course data inside a communicate area. For secure transmission we use SSH and PPP protocols. A secure channel is created for transmission of data in the shortest path in network using SSH protocol. Password authentication to log in is used as a way to implement SSH. To avoid data loss while transmission two routers are connected securely using PPP p OSPF is a complex link-state routing protocol. Link-state routing protocols generate routing updates only when a change occurs in the network topology. OSPF supports complex networks with multiple routers, including backup routers. OSPF executes its own particular transport layer error location and amendment capacities. OSPF utilizes multicast tending to for disseminating course data inside a communicate area. In our proposed system, we use SSH and PPP protocols for secure transmission of data packets. In SSH protocol, a secure channel is created for transmission of data in the shortest path in network which is implemented in the form of password authentication and PPP is used to avoid loss of data during transmission among the routers. We use Cisco Packet Tracer for creating a network topology and to obtain the better results.**

***Keywords* --- Open Shortest Path First(OSPF), Link State Routing protocol(LSR), Secure Socket Shell(SSH), Point-to-Point Protocol(PPP).**

## I. INTRODUCTION

Routers connect networks using the Internet Protocol (IP), and OSPF (Open Shortest Path First) is a router protocol used to find the best path for packets as they pass through a set of connected networks. OSPF is designated by the Internet Engineering Task Force (IETF) as one of several Interior Gateway Protocols (IGPs) -that is, protocols aimed at traffic moving around within a larger autonomous system network like a single enterprise's network, which may in turn be made up of many separate local area networks linked through routers.

The OSPF routing protocol has largely replaced the older Routing Information Protocol (RIP) in corporate networks. Using OSPF, a router that learns of a change to a routing table

(when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information. Unlike RIP, which requires routers to send the entire routing table to neighbors every 30 seconds, OSPF sends only the part that has changed and only when a change has taken place. When routes change -- sometimes due to equipment failure – the time it takes OSPF routers to find a new path between endpoints with no loops (which is called "open") and that minimizes the length of the path is called the convergence time.

Rather than simply counting the number of router hops between hosts on a network, as RIP does, OSPF bases its path choices on "link states" that take into account additional network information, including IT-assigned cost metrics that give some paths higher assigned costs. For example, a satellite link may be assigned higher cost than a wireless WAN link, which in turn may be assigned higher cost than a metro Ethernet link.

OSPF Version 2, as defined by IEEE RFC 2328 for IPv4, is broadly implemented in enterprise routers. IPv6 revisions to this standard are captured in the newer OSPF Version 3 (as defined in IEEE RFC 5340). Although it is intended to replace RIP, OSPF has RIP support built in both for router-to-host communication and for compatibility with older networks using RIP as their primary protocol.

OSPF is usually more efficient than RIP in exchanging routing information when a network is stable; however, for this rule to hold true, it depends on network events. For example, during an external convergence event, OSPF could flood more traffic than RIP. Consider that RIP carries 25 routes per update; on the other hand, OSPF floods a single LSA per external route that is affected by the convergence event. So, provided that you have a (relatively) stable environment, OSPF involves less traffic, and over time, it is statistically more economical than RIP. Using a single LSA per external route is inefficient, but OSPF was never designed to be an EGP. Therefore, OSPF/BGP deployment when large numbers of external routers are present.

OSPF is a link-state protocol in which all routers in the routing domain exchange information and thus know about the complete topology of the network. Because each router knows the complete topology of the network, the use of the SPF algorithm creates an extremely fast convergence. Another popular type of dynamic routing protocol that is based on the Dijkstra SPF algorithm is IS-IS. The use of IS-IS versus OSPF has been hotly debated.

## II.RELATED WORKS

In traditional Local Area Network (LAN), all devices connected on switches belong to one broadcast domain. Virtual Private Local Area Network (VLAN) technology segments a physical LAN into different groups called VALNs and allows only devices on the same VLAN to communicate with one another while restricting devices on other VLANs from sending network traffic. This technology adds security in the LAN and controls network broadcast domain[1]. Virtual LANs (VLANs) offer a method of dividing one physical LAN into multiple broadcast domains. However, VLAN-enabled switches cannot, by themselves, forward traffic across VLAN boundaries. For inter-VLAN communication, a Layer 3 router is required. This research paper discusses the VLAN protocol and different ways and possible protocols involved in creating and implementing Inter-VLAN routing for effective distribution of network services in Ebonyi State

University[3].

One of the benefits provided by the VLAN is network segmentation, for example if you dont have segmented your network all the users will be working on the same broadcast domain, so any user can be able to have access to every computer or data on the same network[2]. For that reason is best practice to create VLAN for the different areas on a company. Now you can provide security a segmented networks using ACL, VLAN ACL, firewalls, etc.

When VLANs span multiple switches, VLAN Tagging is required. A VLAN is a method of creating independent logical networks within a physical network[5]. VLAN Tagging is the practice of inserting a VLAN ID into a packet header in order to identify which VLAN (Virtual Local Area Network) the packet belongs to. More specifically, switches use the VLAN ID to determine which port(s), or interface(s), to send a broadcast packet to[7]. VLAN Tagging support allows administrators to deploy ProxySG appliances inline with switches that are routing VLAN traffic without the risk of losing VLAN ID information[4].

A switch port in access mode sends untagged Ethernet frames, that is, frames without a VLAN tag. Each port is associated with one VLAN (the port-based VLAN, by default, vlan1), and when it receives untagged frames, it associates them with the VID of this VLAN[9]. You can associate the port with another VLAN (using the switchport access VLAN command). This removes it from the default VLAN[6]. Use access mode for any ports connected to devices that do not use VLAN tagging, for instance PC workstations.

A switch port in trunk mode is associated with one or more VLANs for which it transmits VLAN-tagged frames, and for which it identifies incoming tagged frames with these VIDs[8]. To allow a switch port to distinguish and identify traffic from different VLANs, put it in trunk mode (using the switchport mode trunk command), and add the VLANs (using the switchport trunk allowed VLAN command)[10].

## III. LIMITATIONS OF EXISTING SYSTEM

**Lack of scalability:** For the 200 portion organize said beforehand, which potentially contains 200 switches, you could be managing a huge number of steering table sections. Physically ascertaining each one of those courses and staying up with the latest would be a Herculean undertaking and exceptionally inclined to mistake. Regardless of whether you execute a decent system tending to outline that takes into account course synopsis, you are still left with a staggering number of courses to oversee.

**Large network implementation:** When working with a system of 200 switches, the errand of refreshing one course can turn into a mind boggling assignment, particularly on the off chance that you refresh the courses in the wrong request. All things considered, you could lose access to an extensive segment of the system until the point when somebody visits that switch with a rollover link or interfaces from another region of the system.

**No redundancy:** Dynamic steering conventions can refresh directing tables in case of gadget or interface disappointment, so if there are various conceivable ways, these conventions will keep on allowing information stream. Static courses don't take into account this programmed failover or repetitive ways, so on the off chance that you have a disappointment, you should physically change courses to move information through an elective way.

## IV. PROPOSED SYSTEM

The packets containing information can be sent securely in an unsecured network in the shortest path. The routers present can be configured from any remote system securely in the network with the help of SSH protocol. The SSH protocol provides a secure channel for the packets to pass through in an unsecure network. There are several ways to use SSH protocol but here we use password authentication to log on. Another protocol PPP is used for avoiding the data loss during transmission between the routers in the network. It connects two routers directly without any host in between. PPP protocol provides authenticated connection, encryption and compression during transmission etc.,

Although there are many protocols, SSH and PPP are the best way to provide secure transmission connection. Using SSH, non-interactive login is also possible.

It provides a strong identity checking by providing secret private keys. Sniffing of data transmission and Spoofing of IP address are the main advantages of using SSH. SSH is a protocol that can be used for many applications across many platforms including most Unix variants (Linux, the BSDs including Apple's macOS, and Solaris), as well as Microsoft Windows. PPP supports multiple routing protocols and also allows error detection. The PPP protocol is inherently extensible, where new protocols and features can be added on constantly.

## V. METHODOLOGY

**Packet Tracer** is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. Using command line interface, this software allows the configuration of Cisco routers and switches simulation by the users. It makes use of drag and drop interface to make it easy for the users to create a network topology and to work with other features. Packet racer supports all platforms like iOS, Linux and Windows. It can also be used for collaboration.

### *A. Network Design*

Identifying the components of your network and Access the cables section and connect completely and correctly the cables between the network. Configure the IP addresses on all end devices, routers and switches. Click on the device and open the Command Line Interface (CLI) and then type in the right commands to configure the right addresses for the router using the addressing table.

Use a console cable from an end device and connect it to the device you wish to configure and access the terminal platform on the end device and it will take you to the device's Command Line Interface and then you type in the commands in other to configure the right addresses. After configuring the IP addresses, we will need to configure the default gateway also.

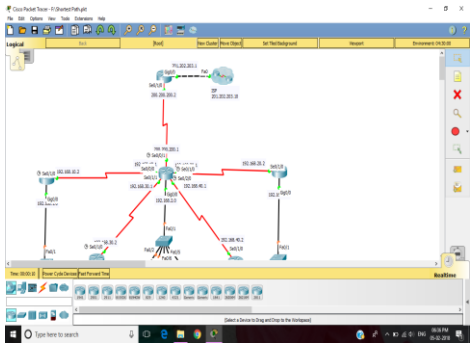

Fig: Network Design

### *B. Internet Service Provider*

An **Internet service provider** (**ISP**) is an organization that provides services for accessing and using the Internet. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting,

Usenet service, and colocation. A router is a networking device that forwards data packets between computer networks.

Routers perform the traffic directing functions on the Internet. A data packet is typically forwarded from one router to another router through the networks that constitute the internetwork until it reaches its destination node. A network switch (also called switching hub, bridging hub, officially MAC bridge) is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device. Unlike less advanced network hubs, a network switch forwards data only to one or multiple devices that need to receive it, rather than broadcasting the same data out of each of its ports.

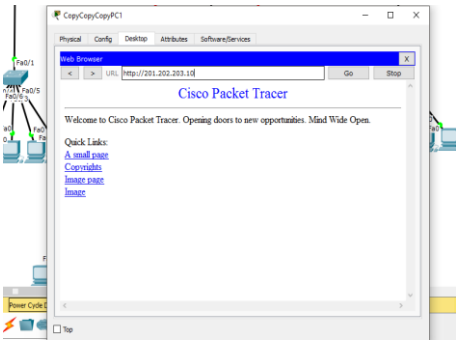


Fig: ISP

### *C. VLAN Configurations*

The VLAN configurations used in this infrastructure:

VLAN 10 – 192.168.10.0/24

VLAN 20 – 192.168.20.0/24

VLAN 30 – 192.168.30.0/24

VLAN 40 – 192.168.40.0/24

VLAN 50 – 192.168.50.0/24

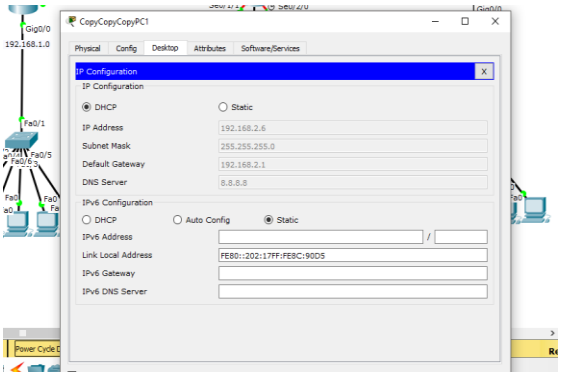


Fig: VLAN Configurations

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.

### *D. SSH Protocol*

SSH gives a protected channel over an unsecured system in a customer server engineering, interfacing a SSH customer application with a SSH server. Common applications incorporate remote summon line login and remote order execution, however any system administration can be secured with SSH. The convention detail recognizes two noteworthy adaptations, alluded to as SSH-1 and SSH-2. The routers present can be configured from any remote system securely in the network with the help of SSH protocol. The SSH protocol provides a secure channel for the packets to pass through in an unsecure network.

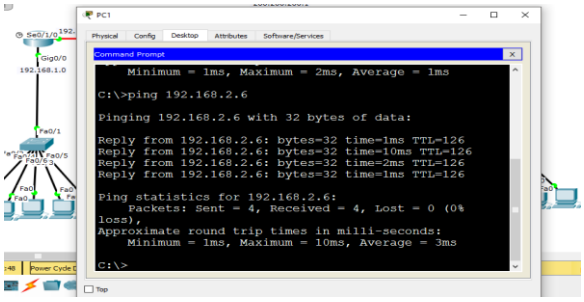


Fig: Ping between two systems in network

### *E. PPP Protocol*

PPP protocol provides An end client authentication framework for the ISP to interestingly validate each end client previously enabling access to utilize the system assets. Point-to-Point Protocol (PPP) is an information interface (layer 2) interchanges convention used to set up an immediate association between two hubs. It interfaces two switches specifically with no host or some other systems administration gadget in the middle. It can give association validation, transmission encryption and pressure.

## V. CONCLUSION

The replacement of VLANs made the network partitions virtually where the connections are not made by any physical networks which are easier and cost effective. OSPF is an interior gateway protocol (IGP) for routing Internet Protocol (IP) packets solely within a single routing domain, such as an autonomous system. It gathers link state information from available routers and constructs a topology map of the network. The topology is presented as a routing table to the Internet layer which routes packets based solely on their destination IP address. It finds the shortest path for the transfer of packets from one system to the other in the network layer. Thus a secure data transmission in the shortest path can be done using SSH and PPP protocol.

## VI. REFERENCES

[1]. Albert Rego, Sandra Sendra, Jose Miguel Jimenez, Jaime Lloret, “OSPF Routing Protocol Performance in Software Defined Networks”, Fourth International Conference on Software Defined Systems, 2017.

[2]. Alex Kirshon and Dima Gonikman, Gabi Nakibly, Dan Boneh, “Persistent OSPF Attacks”, 2017.

[3]. John Cosmas, Hasanein Hasan , Zaharias Zaharis, Pavlos Lazaridis, Sinan Khwandah Maritime, “Development of Performance of OSPF Network by Using SDN Concepts”, IEEE International Black Sea Conference on Communications and Networking, 2016.

[4]. Jianhui, Xingwei Wang, Min Huang, Fuliang Li, Keqin Li, Hui Cheng, “Accomplishing Information Consistency under OSPF in General Networks”, IEEE 22nd International Conference on Parallel and Distributed Systems, 2016.

[5]. Karamjeet Kaur, Sukhjeet Singh, Rahul Malhotra, “Design Of Open Shortest Path First Protocol–A Link State Protocol Using Opnet Modular”, International Journal of Computer Science and Mobile Computing, 2012.

[6]. Kirti, Lokesh Kumar, “Review Paper on OSPF protocol for directed & undirected graph problems”, International Journal of Enhanced Research in Science, Technology & Engineering, 2015.

[7]. Luciana S. Buriol, Paulo M. Franca, Mauricio G.C. Resende, Mikkel Thorup, “Network design for OSPF routing”, Internet and Network Systems Research, 2015.

[8]. Madhuri M. Dharanguttikar, Pingat .S.P, “Novel Approach to Save Energy Through

OSPF Routing Protocol", International Conference on Advances in Communication and Computing Technologies, 2014.

[9]. Shakir James, "OSPF Extensions for Mobile Ad-hoc Networks", A Survey Paper, 2015.

[10]. William V. Wollman, Yosry Barsoum, "Overview Of Open Shortest Path First, Version2 (Ospf V2) Routing In The Tactical Environment", IEEE International Conference, 2015.