International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
(Volume 31, Issue: Special), June 2019
An Indexed and Referred Journal with Impact Factor: 2.75
ISSN (Online): 2347-601X
www.ijemhs.com

Review of Protocols used in Enterprise Networks

Rahul Ray, Assistant Professor, Department of Computer Science & Engineering, NM Institute Of Engineering & Tech, Bhubaneswar
Soumitra Sahu, Assistant Professor, Department of Computer Science & Engineering, Krupajal Engineering College, Bhubaneswar
Aniket Kumar, UG Student, Department of Computer Science & Engineering, Krupajal Engineering College, Bhubaneswar
Pratiksha, UG Student, Department of Computer Science & Engineering, Krupajal Engineering College, Bhubaneswar

***Abstract*—The backbone of the internet is governed by protocols. Enterprise networks are secure networks which enable enterprises to operate several transactions on a daily basis across their network. This form of seamless communication is made possible by Routing and Switching protocols. In this paper, a review of the most used protocols in Enterprise networks are surveyed and understood in detail.**

Keywords—OSPF, EIGRP, BGP, Routing, SNMP

I. INTRODUCTION

Enterprises are huge conglomerates of organizations that do business or operate on a large scale across countries spanning several branches and franchises. Their operations involve several hundreds of transactions on their network which needs a stable architecture and backbone for robust usage.
Generally, Enterprise Networks encompass a great magnitude of network devices comprising of switches and routers. However, on a general architecture template, they follow the 3-tier architecture which is highly scalable. These devices need to run several network protocols between them for seamless connectivity across the network.

II. THE 3-TIER ARCHITECTURE

Huge Enterprises generally follow the 3-tier-architecture as part of designing their network for enhanced scalability and increased redundancy in case of device failure. It primarily involves segmenting the network into 3 layers' design-wise for increased ease in troubleshooting as well.
The 3 layers of the architecture include:

1. Access Layer
2. Distribution Layer
3. Core layer

The **Access Layer** is the first layer in the 3 tier architecture which directly connects the users to the network. This layer generally consists of Layer 2 switches which have pure switching capabilities and can switch packets only within the network

The **Distribution Layer** is the second layer in the 3 tier architecture. This layer generally consists of Layer 3 switches to which the access layer switches connect.
This layer also can perform routing in case it is a compressed 3-tier architecture. It serves as the backbone for all users connected, as it establishes connection across all access switches. Also the VLANs and default gateways generally happen to be in this layer. Additionally, distribution policies can be applied at this layer as well.

The **Core Layer** is the last layer in the 3 tier architecture. This layer consists of Industry capable routers capable of handling routing across networks. This layer just forwards packets in the shortest possible way to the destination. Distribution policies are not applied here. This layer has routing protocols running for communication with the Distribution Layer.

All the Layers have multiple redundant connections as backup for failure of a device. This ensures maximum uptime of the network. Also in this model, additional users can be added/removed to/from the network without having to disturb the core of the network.

This fundamental architecture enables resilience to the fullest as it is inherently designed to back up quickly from failures. Having taken care of resilient network recovery as part of the network design, further security strategies act as superior strengthening mechanisms and only empower the network even in an even better way. The above explained architecture is depicted in the Fig 1.1 below.

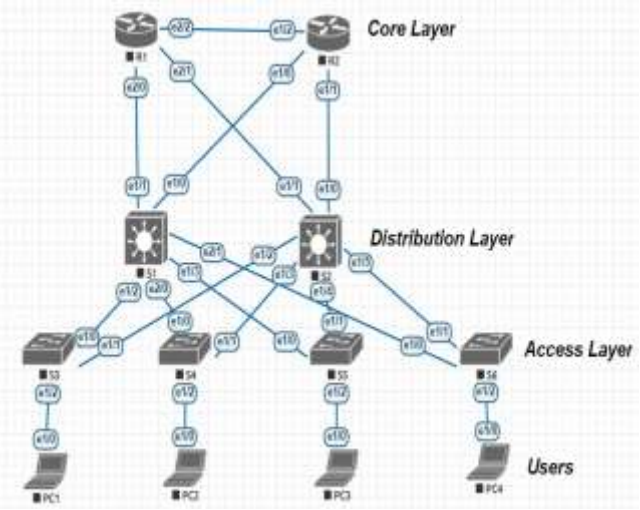

Fig 1.1 The 3-tier network architecture

III. PROTOCOLS USED IN ENTERPRISE NETWORKS

Enterprise networks need extensive connectivity and hence use a variety of protocols at every layer in the architecture.
The different protocols used at the routing level include:

1. OSPF
2. EIGRP
3. BGP

The different protocols used between switches in the enterprise architecture include:

1. STP
2. RSTP
3. PVST+
4. Rapid PVST+

In [2]. a study about OSPF (Open Shortest Path First) and its behavior in Enterprise Networks was conducted. OSPF is an Interior Gateway Protocol(IGP) for routing within an Autonomous System. It collects Link State data from other routers in the network and builds the routing table to forward the packet. Routers running OSPF reliably flood LSA's (Link State Advertisements) to gain information about the Topology. OSPF triggers an update only upon change in the network. It calculates the shortest possible path

OSPF segments the network into smaller areas. It has a backbone area called **Area 0** in case of multiple areas. All areas communicate with each other via **Area 0**. In a multi-area configuration every area is supposed to have its own topology table. Two or more areas are connected by means of Area Border Routers(ABR).

OSPF fundamentally has 2 primary stages of operations:

1. Neighbor adjacency initialization & LSA Flooding
2. SPF Calculation

1.Neighbor and adjacency initialization & LSA Flooding: This stage starts once the router detects the interfaces configured for OSPF and starts sending hello packets out of those interfaces. The different OSPF neighbor states are:

1. Down
2. Attempt
3. Init
4.2-way
5.Exstart
6.Exchange
7.Loading
8.Full

At the end of the eight stages, the routers Link State Advertisements are exchanged and the databases are fully synchronous with each other and the neighbor adjacencies are established.

2.SPF Calculation: Every area will calculate the best possible path to the destination and using an SPF algorithm and the database having the topology. This tree has the source router as the root and the remaining networks are arranged as the branches/leaves of the tree.

In [3], a study about EIGRP and its behavior was conducted. It is also an IGP used in Enterprise networks which is a based on an advanced working of Distance-Vector approach. Unlike the Routing Information Protocol(RIP) it has a maximum hop count of 255. It also supports VLSM. Path selection in EIGRP is done by means of the DUAL Algorithm which uses several parameters in selecting the ideal path to a destination For any protocol, the fundamental requirement to operate is to establish adjacency in the fastest possible manner.

The Steps in EIGRP to establish adjacency include:

1. Hello packet sent and ACK received from the neighbor
2. The Autonomous System numbers of the devices intending to establish neighbourship must match
3. There are several other parameters such as ***bandwidth, reliability, delay, load, MTU*** which are termed as K values.

Using the K values, the best possible path with the lowest Feasible Distance(FD) is chosen. EIGRP uses different kinds of packets to maintain a consistent routing database throughout its scope of operation.

The different types of packets used by EIGRP include:

1. *Update Packet*: This packet which have information regarding routing. It is transmitted via the Reliable Transport Protocol(RTP).
2. *Query Packet*: This packet is used by a network device if it loses a path to the destination. It is also sent using the Reliable Transport Protocol.
3. *Reply Packet:* This packet is sent as a unicast reply to the above query packet.
4. *Hello Packet:* This packet is used generally to establish and maintain neighbor adjacencies.
5. *Acknowledgement Packet:* This packet is sent as a response to the Hello packet.

As part of updating the status of the neighbors, EIGRP pings all its neighbors periodically. This interval is known as the *Hello interval.* The hello interval is **15 secs** by default.

The time the protocol waits before pinging the respective device again without a response is called *hold time*. It is generally three times the hello interval. The default hold time is **180 secs**.

The effectiveness of EIGRP is the fact that it supports VLSM, has a mechanism which is dynamic in nature for the purpose of route recovery and can query its neighbors for Alternate/backup routes. The algorithm facilitating the above features as part of EIGRP is the DUAL (Diffusing Update Algorithm)

The features DUAL illustrates include:

1. Neighbors' activity is monitored and is declared active or dead within a stipulated amount of time.
2. Transmitted packets/messages should be received in the same order.
3. Changes/Messages are bound to be handled in the order received.

With the five K metrics mentioned above EIGRP can perform Load balancing (equal cost and unequal cost) on links as well.

Fig 1.2 EIGRP in an Enterprise Topology

In [4], a study on BGP, its operation and behavior was conducted. BGP is the Border Gateway Protocol which

connects the current day internet by connecting multiple Autonomous Systems has had several revisions the latest being BGPv4 released in 1995. (RFC 1771) BGP enables connection between several ASes configured with different protocols. Communication over the internet has been seamless due to the extensive operation of this protocol.

BGP has two versions namely:

1. iBGP: Routers should be configured as a neighbor to another iBGP peer in the same area.
2. eBGP: Routers can be an eBGP or iBGP neighbor for adjacency.

BGP is the routing protocol of choice to get to remote networks.

In [5], Spanning Tree Protocol(STP) was studied with respect to its operation and behavior. It is used to prevent looping between switches in a topology. Switches have only the capability to switch frames within the same network (Level 2 switches). Hence if there is a loop between a group of switches that are in a network, it leads to a situation called *Broadcast Storm.* This situation generates a lot of unnecessary traffic due to redundant packets in a loop.

This situation of a loop is prevented by the Spanning Tree Protocol.

By default on configured switches, STP is up and running and monitoring all loops. STP keeps sensing for redundant links and the following steps are performed:

1. Election of the root bridge. This is done by selecting the Switch with the lowest priority. In case of a tie the switch with the lowest MAC address is chosen as the root bridge. All ports on the Root bridge are Designated Ports and are in forwarding state.
2. The remaining switches choose the port with the shortest path facing the root bridge and the corresponding port is made the **root port** for the switch.
3. The root port is moved to the forwarding state and the remaining ports are moved to the ALT/BLK state.

Using these steps a loop less Spanning tree is constructed which will eliminate loops within the switches.

The different states that STP switch ports go through are:

1.Disabled
2. Blocking
3.Listening
4.Learning
5.Forwarding

STP is an IEEE 802.1D protocol which can be used by any switch for the intended purpose. The convergence time after a topology change in STP is around 30-50 seconds. As a result, the RSTP was designed.

RSTP (Rapid Spanning Tree Protocol) is an IEEE 802.1W standard protocol. It reduced the convergence time after a topology time from 30 seconds to almost instantly or a few milliseconds. The port states were significantly reduced.

The states include:

1.Disabled
2.Blocking

3. Learning.

Both the above discussed protocols do not support multiplelogical instances of the device network. In order to bring insupport for each VLAN, the PVST+ protocol was designed. *PVST+ (Per Vlan Spanning Tree Protocol)* facilitates separateroot bridges for every VLAN. This reduces the ambiguity in amulti-VLAN environment. It is a Cisco proprietary protocol. *Rapid PVST+* facilitates Spanning Tree protocol for everyVLAN with enhanced convergence times as compared toPVST+. It is a Cisco proprietary protocol.

Another important aspect to be taken into keen consideration is that of ensuring highly reliable security especially in large-scale enterprises. Although, currently Intrusion Detection Systems (IDS) are popular, and incorporated in organizations today in their security infrastructures, it does not promise guaranteed protection from the increasing attacks from malicious network traffic from hosts located in the same network as the victim host. In [6], SNMP (Simple Network Management Protocol) integrated with security mechanisms and Network Management Systems (NMS), the scenario is able to be curbed to a significant extent.

SNMP is an application layer protocol primarily used to monitor and manage network devices along with their functions in enterprise networks, it serves the purpose of having proactive maintenance for organizations. It is offered extensive support by a wide array of hardware, ranging from conventional network specific equipment including routers, switches, wireless access points to end-points like scanners, printers, Internet of Things (IoT) devices, and can retrieve subsequent amount of information from the devices in real-time. SNMP is always used as part of another software package, like a Network Management System, also termed as the SNMP manager. Manually managing several nodes would be extremely resource-intensive and time consuming, particularly in evident networks of large size. SNMP used with an NMS enables a Network Administrator to view the status of the network through one single interface, which typicallysupports automatic alerts and batch commands, The SNMP agent software must be installed in all the network devices, hardware or on the services being monitored, that collect data about various metrics like CPU utilization, disk space or bandwidth use and establish a connection with the Network Management Console, i.e. the SNMP manager, the nodes on which the SNMP agent runs are the managed devices orresources. All objects itemized and described, that can be queried or controlled using SNMP, are consolidated in the form of a text file (. Mib), must be loaded onto the NMS that it can identify and monitor the status of the mentioned parameters, these are termed as MIB (Management Information Base) items, each of these items is assigned an Object Identifier (OID) for ease of access.

IV. COMPARISON BETWEEN ROUTING PROTOCOLS

Different Enterprises use various protocols as per their requirement. Among the various protocols used, we now compare the OSPF and EIGRP protocols.

We can define a few parameters for comparison:

1.CPU Utilization: OSPF has a lot of processes running in the background for it to come up and proceed with its course of operation. They include electing the Designated Router(DR) and Backup Designated Router (BDR) and comparing Router ID's. This eventually introduces a lot of delay when compared to EIGRP. Hence more resources are utilized by OSPF leading to higher CPU utilization.

2.Bandwidth utilization: In OSPF a client-server model is established. The DR must be robust enough to handle all traffic within the area failing which the operations in the area might collapse. All routing updates need to go to the DR which then sends it to the required destination. This leads to bandwidth jamming. In case of EIGRP, there is no concept of client-server and hence there is very little scope for jamming of bandwidth.

3.Recovery from path loss: In case of a path loss, OSPF will have to send out Link State Advertisements and initiate the neighbor discovery process all over again while EIGRP has alternative/backup routes called Feasible Successor which can be used in case if a successor is down. So in case of high speed networks OSPF will fail to act quickly when compared to EIGRP.

4.Equipment Cost: OSPF needs a Backbone router as compared to EIGRP which increases the equipment cost in case of OSPF.

5.Administrative Distance: AD of EIGRP is 90 while OSPF has an AD of 110. Hence in a router having both the protocols, EIGRP is preferred.

6.Load Balancing: EIGRP is capable of performing both equal and unequal cost load balancing. But OSPF has the capability of only equal cost load balancing.

V.CONCLUSION AND FUTURE WORK

From the survey conducted, multiple protocols at various layers and their comparisons was studied and observed. Although Open Standard protocols are available for industry usage, Cisco Proprietary protocols in case of both switching and routing levels are found to have superior performance capabilities. As majority of the internet backbone was pioneered by Cisco, it is easier and better to use those protocols for enhanced performance and compatibility. Although the current networking arena comprises mostly of traditional routing and switching techniques, virtualizing the control plane and easier operation can be achieved by means of Software Defined Networking. Migration to Software Defined Networking is a continuous process and essential for enhanced scalability and control over the network.

V. REFERENCES

[1] https://www.ictshore.com/free-ccna-course/three-tier-architecture/
[2] Aman Shaikh, Mukal Goyai, Albert Greenberg, Raju Rajan, andK.K. Ramakrishnan, "An OPSF Topology Server: Design and Evaluation," IEEE J. Selected Areas in Communications, vol. 20,no. 4, May 2002.
[3] E. Menggunakan, S. Jaringan, and O. Modeler, "Simulasi Kinerja Routing Protokol Open Shortest Path First (Ospf) Dan Enhanced Interior Gateway Routing Protocol (Eigrp) Menggunakan Simulator Jaringan Opnet Modeler v. 14.5," pp. 1–6
[4] T.G. Griffin and B.J. Premore, "An experimental analysis of BGP convergence time," in Proc. ICNP 2001, Riverside, California, Nov. 11– 14, 2001, pp. 53–61.
[5] https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html
[6] A. Pras, T. Drevers, R. Meent, D. Quartel, Comparing the Performance of SNMP and Web Services-Based Management, IEEE Transactions on Network and Service Management, 1(2), December, 2004.
[7] G.J. Holzmann, Design and Validation of Computer Protocols, Prentice Hall, 1991.