International Journal of Scientific Research in Science, Engineering and Technology (www.ijsrset.com)
© 2020 IJSRSET | Volume 7 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
DOI : https://doi.org/10.32628/IJSRSET2072119

Formal Analysis of Network Properties for Network Validation

Swapnil Wable[a], Divya Punwantwar[b], Manisha Mali[c], Kirti Wanjale[d]

[ab]Post Graduate Student, Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, India
[c]Assistant Professor, Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, India
[d]Associate Professor, Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, India

ABSTRACT

Today's rapidly growing and ever-changing world, the demands of high productivity, security of computer systems and computer networks is very important. In the modern and rapidly growing and changing internet era, network plays a vital role. And for transmitting data over a network or communication network for that various things are used and that things first must know while validating data over the network. And for that purpose, in these paper a detailed study and analysis of some networks key points are presented.

Keywords : Network, Router, COS, Routing, Network Topology.

I. INTRODUCTION

Today's internet is widely complicated and fragile. All the data are transmitted over a network at the same time from one point to another point rapidly. While sending data or transmitting data over a network there are some key points which are required while validation over a network. This paper is presented to study in detailed and for learning about the properties which are used while transmitting data because when the transmission of data is going on, must know that it is transmitting properly or not. And for knowing all these must aware about the properties of network or concept of the network in detailed [1]. This paper presented about the routers, CoS classes right from CoS1 class to CoS4 class, ARP and RARP, routing protocols consisting of static and dynamic protocol as well as types of dynamic protocols like BGP, OSPF, RIP in detailed and routing topology by consisting of Full Mesh, Hub and spoke. This concept is enough for validation of data over a network [2].

II. ROUTER

Primarily routers operate at the third layer that is the network layer of the OSI model and which has a core responsibility to move packets that is the fundamental unit of data transport on modern computer networks and moving the packets across the network using the most appropriate paths that is Network Layer Definition [3]. Routers are the device that route packets from network to network that is from one network to the next network. For networks like internet the routers are a necessity. The internet is made up of many interconnected routers which route messages or data from one network to the next network [4].

III. CLASS OF SERVICE (COS)

Class of Service (COS) its support has become an indispensable function in many of the large Service Provider networks today only because of the competitive nature of the Internet and the diversity in the customer needs. Class of Service i.e. CoS or Quality of Service (QoS) is nothing but a way to

manage multiple traffic profiles all over a network by giving particular types of traffic priority over others.

For example : Can give a Voice traffic priority all over an email, a streaming video, a voice, a large document file for the purpose of transfer or http traffic together as well as treating each type as a class with its own level of service priority. Class of Service technologies do not have guaranteed that a level of service in terms of bandwidth and delivery time and at the same time they offer a best-effort. CoS that is class of service is offered by service providers normally within an MPLS (Multi-Protocol Label Switching) offering [5].

3.1 The CoS implementation needs some techniques, and they are

- Traffic Classification which is used to map types of traffic to different classes of service. The ingress customer premise router will be classified the types of traffic using IP addresses, ports, protocols and a combination of all above or the IP Precedence setting.
- Policing and Marking are mainly the result of the above traffic classification when applied against to an ingress CoS profile. Packets are also exceeding the CoS1 bandwidth allocation, which are strictly policed and that is traffic all above the allocated bandwidth is discarded, while packets in any of the remaining data classes that are from CoS2 to CoS4 are given different markings to indicate whether they are within the bandwidth subscription as per CoS i.e. compliant or exceeding the bandwidth subscription as per CoS i.e. noncompliant.
- Congestion Management and scheduling are the two main methods used to service traffic across the Wide Area Network (WAN) connection as well as from AT&Ts back-bone network. An egress scheduling or queuing CoS profile is being selected to allocate the bandwidth needed for each class [5]. If there is insufficient bandwidth, to the fully service of a class, then at that time noncompliant packets may be discarded within the class to help relieve the congestion by using the Weighted Random Early Detection (WRED) algorithm. Discarded packets also allow TCP (Transmission Control Protocol) applications to throttle back by closing their own TCP windows.

3.2 Information which is required for the CoS Option

To map all your business requirements to the CoS model then you needs to consider and request the some following information:

- Choose one of the available CoS Classification profile for marking packets being sent into the network that is ingress.
- Choose one of the available CoS queuing profile for scheduling traffic from the network that is egress.
- Identify your applications and the desired classes for each other, where Engineers responsible to configuring the customer premise router, and they are also responsible for classifying your traffic into the correct CoS, As well as for marking it appropriates.

3.3 CoS1 is known to be Real-time Applications

A real-time application is suitable to the highest priority classes which have unique performance requirements as well as they are sensitive to delay, packet loss and jitter that is delay variation. And the service is engineered, such that, the Real-time class has the highest priority up to its allocated bandwidth. Packets in the Real-time class are processed ahead of all other classes' up to the allocated bandwidth limit. The oversubscribed packets are being dropped in this class. AT&T doesn't recommend for putting data traffic in the Real-Time class since the larger packet sizes which can interfere with Voice or other Real-time traffic. There are some common applications that can be included in this class, and they are:

- Voice over IP

- Streaming Audio Applications

3.4 CoS2 is known to be Critical Data Applications

A majority of the bandwidth among all data classes which is allocated to this class, it is very effectively the highest priority data class. Profiles which having a large bandwidth allocation in this class that can be used either for applications requiring a large amount of bandwidth or for applications which requiring lower latency. For example: the hourly downloads of accounting files sometimes that may need the assurance that a specific minimum amount of bandwidth is always available. Like that if the mission critical data were frequent credit card transactions or character-based I/O then a larger bandwidth percentage would increase the service frequency and help to control the perceived end-to- end delay during congestion. In these both cases that any bandwidth not actually used by this class would be available to the other classes. And the definition of Critical Data is varies from customer to customer as well as the relevance remains the same. The common applications that considered for this class are:

- Customized Corporate Applications
- ERP applications like SAP, PeopleSoft, Citrix
- Corporate database Applications
- Extranet/Intranet based critical Applications
- Video Conferencing traffic that is if coexists with Voice and therefore is not put into COS1

3.5 CoS3 is known as Business Data Applications

The CoS3 data class is used for applications that have a lower priority such as normal or typical corporate data applications like The Human Resources related web transactions, an email, an inter-office file transfers and so on. The best methodology for choosing the appropriate bandwidth percentage is that the same as for the Critical Data class as well as is based on the type of traffic. There are some common traffic that may reside in these classes are:

- Essential Internet Services
- Non-critical file transfers
- Email

3.6 CoS4 is known as Standard Data Applications

CoS4 class or the default class is used only for all traffic that does not map to any one of the other classes that is CoS1, CoS2 or CoS3 class. At the same times when the other classes are not using their specified bandwidth allocation and the Standard Data Class then still it has access to their unused bandwidth. The default class includes some following traffic types:

- General Internet browsing Traffic
- Personnel file transfers
- Newsgroup participation
- Non-critical corporate business
- Email

IV. ARP AND RARP

ARP (Address Resolution Protocol) is nothing but a network protocol which is used to find out the hardware i.e. MAC address of a device from an IP address. ARP is also used, when a device wants to communicate with some other device on a local network. ARP is used by the sending devices to translate IP addresses to MAC addresses. ARP request message is sent by the device by containing the IP address of the receiving device. All devices which is on local network segment see the message but only device that has IP address which responds with ARP reply message by containing its MAC address. Enough information is available with the sending device to send the packets to the receiving device [6]. ARP in charge of learning, what is the MAC address that is physical address of a computer that has a given IP address and RARP that is Reverse Address Resolution Protocol which does the opposite that it is in charge of finding out that what is the IP address of a computer with a given MAC address.

While the datagram is getting transmitted all over the internet, at that time the MAC address of the target computer then at that situation there is no need. The routers in the middle of the road have only interest in delivering of the datagram to the target network. If once the packet arrives then the target network needs to know the MAC address of the target computer as it will deliver locally datagram that is probably using the Ethernet protocol.

For example: IP address 69.69.69.69 is a target IP address when the datagram arrives at the router of 69.69.69.69 network then at that time it will ask to all the computers that is when a message is sent to all the computers is called broadcast message by using ARP protocol that Hello, which computer is 69.69.69.69 ? Then the computer who is using this IP address will give answer that me.

Congesting of network is done of course only by sending broadcast messages all the time, so the router will keep a table of known IP addresses as well as their corresponding MAC addresses so that it won't need to ask the same question again when it receives a new datagram by targeting to 69.69.69.69.

RARP that is Reverse Address Resolution Protocol, on the other hand, it was used in the past by using the PCs without a hard disk drive or any other boot media using remote boot. And these kinds of computer don't have an operating system installed and also they don't know that which IP address that they are going to use. So they need to know that which IP address they should use in order to start loading the operating system from remote boot server. The use of RARP became to obsolete. Both this ARP and RARP protocol are work on the Network Interface Layer.

V. ROUTING PROTOCOLS

There can be two types of routing which is static or dynamic. Mainly static routing is used on small a network that is datagrams always travel by the exact same path to reach their destination [7]. And dynamic routing is mainly used on the Internet or big networks. Routers can change routes on the fly only with the dynamic routing and only if they feel that there are better paths to reach to a given destination.

For example, to reach a given destination if there is only one way and the current route is longer than another available route then to use the shorter route the routers can reconfigure themselves. Here long and short refers to the number of existing hops that is routers in the way. All Shorter routes are not necessarily the fastest routes.

Using a router protocol the communication between the routers in order to reprogram their routing tables is done. There are three most well-known dynamic routing protocols and the dynamic routing protocols are RIP (Routing Information Protocol), OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol).

5.1 Static Routing

Static routing is nothing but a routing mechanism which is handled by the Internet Protocol (IP) and it also depends on the routing table which is manually configured [8]. Static routers means routers that use static routing. Static routers are mainly used in networks which is smaller and that contains only a couple of routers or when there is an issue regarding security. Static routers never exchange their routing information with other so each static router must be configured and separately maintained.

- How It Works: To function properly for a static router, the routing table should contain a route for each and every network in the inter-network. Hosts on a network are configured, so that static routing default gateway address matches the IP address of the local router interface. Whenever a host needs to send a packet to another network at that time it forwards the packet to the local router

then which checks its routing table and also determines which route is suitable to use to forward the packet.

Static routers are more difficult to administer than dynamic routers, but they can be more secure because the administrator controls the configuration of the router. To spoof dynamic routing protocol packets, to reconfigure the router and hijack network traffic, Static routers are generally immune from any attempt by hackers.

5.2 Border Gateway Protocol (BGP)`

BGP stands for Border Gateway Protocol and it is a standardized exterior gateway protocol. Border Gateway Protocol is mainly used to exchange routing information or data across the Internet. And also BGP was not built to route within an Autonomous System. But rather to route between an Autonomous System. BGP maintains a separate table of routing based on the shortest path mainly, AS (Autonomous System) path. It is considered a "Path Vector" routing protocol. Internet is a collection of interconnected AS's. BGP protocol can connect together with any internetwork of AS (Autonomous System) using an arbitrary topology [8]. There is one dependency that each autonomous system must have at least one router which is able to run BGP and this router connect to at least one other AS's BGP router. The main and basic function of BGP is to exchange network reach-ability information with each other BGP systems. BGP constructs an autonomous systems graph based on the information or data which is exchanged between BGP routers.

1. When to use BGP: When there is required of multiple connections to the internet then contrary to popular opinion, BGP is not necessity. If there is only one connection to an external autonomous system (such as internet) at that time BGP is completely unnecessary. Actually the true and exact benefit of BGP is in controlling how traffic enters into the local autonomous system rather than how traffic exits it [10]. Under the following circumstances BGP can be used:
   - When multiple connections exist to the external autonomous system via different providers.
   - When multiple connections exist to the external autonomous system through the same providers but connect via a separate routing policy.
   - When the existing routing equipment can handle the additional demands at that time BGP's correct benefit is in controlling how traffic enters the local autonomous system rather than how traffic exits it.
2. Characteristics of BGP:
   - Provide communication between two autonomous systems is the main role of BGP.
   - BGP also supports Next hop paradigm.
   - Within the autonomous system there should be coordination among multiple BGP speakers.
   - BGP advertisement also includes path information along with all the reachable destination and next destination pair.
   - Policy support, in that BGP can implement policies that can be configured by administrator.
   - BGP runs over TCP.
   - BGP conserve the bandwidth of network.
   - BGP supports security.
3. Best path determination: BGP contains multiple routes to the same destination and at that time, it compares the routes in pairs from starting with the newest entries and further working to the oldest entries. BGP determines the best path by comparing the attributes of all route pair. And the attributes are compared in some specific order, and they are:
   - Weight: Route having the highest weight.
   - Local preference: Route having the highest local preference.

- Locally originated: Check whether the next hop to the destination 0.0.0.0
- AS Path: Route which having shortest AS path.
- Origin code: From where the route originates. Like IGP, EGP or unknown origin.
- MED: Path having the lowest MED. BGP Route type: The type is eBGP or iBGP.
- Age: Oldest route preferred.
- Router ID: With the lowest BGP router ID which route is originated from the router.
- Peer IP address: Route originated from the router with the lowest IP.

While applying attributes, weight and local preference are applied to inbound routes by dictating the best outbound path. As path and MED are applied to outbound routes by dictating the best inbound path.

5.3 Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is nothing but a protocol which is a link state routing protocol, which is mainly used to find the best path between source and destination router using its own shortest path first i.e. SPF algorithm. OSPF is a protocol which doesn't look for the shortest path but for the fastest path. OSPF protocol is used by the routers, they check first the status of other routers they have access to from time to time sending messages. From that message which is sent time to time they know the status of the router and also check whether the router is online. OSPF based routers allow load balancing, if there is more than one route to the give destination and the router may divide datagrams between them in the order to lower the individual traffic on them. OSPF protocol directly works with IP protocol on the internet layer and it doesn't use TCP or UDP protocols [9]. A link state is a routing protocol nothing but a protocol that uses all the concept of triggered updates. That is, if the there is any change observed in the learned to route ,table then the updates are triggered only but not like the distance vector routing protocol where the routing table are exchanged at the period of time. OSPF protocol is developed by Internet Engineering Tasks Force (IETF) as one of the Interior Gateway Protocol (IGP) [11]. The main aim of this OSPF protocol is that, moving the packet within a large autonomous system or domain of routing.

1. Characteristics of OSPF:

- Using areas the OSPF protocol employs a hierarchical network.
- With adjacent routers in the same area, OSPF will form neighbour relationships.
- OSPF advertises the status of directly connected links using link state advertisements (LSA) instead of advertising the distance to connected networks.
- To determine the shortest path, OSPF protocol uses the Dijkstra Shortest Path First algorithm [12].
- OSPF supports VLSMs because OSPF is a classless protocol.
- OSPF protocol only supports IP routing.
- OSPF routes have some administrative distance and that distance is 110.
- OSPF protocol uses coat as metric which is computed based on bandwidth of link as well as it has no hop count limit.
- OSPF process maintains and builds 3 separate tables an, they are:
    - Neighbor Table: Which contains a list of all neighboring routers?
    - Topology Table: Which contains a list of all possible routes to all the known networks within an area?
    - Routing Table: Which contains the best route for each and every known network?

2. Criteria to form neighbourship in OSPF:
    - In same area it should be present.
    - Router ID must be unique always.
    - Subnet mask should also be same.
    - Hello and dead timer must be same.
    - Stub flag should match every time.

- Authentication also must match.

5.4 Routing Information Protocol (RIP)

If RIP protocol is used by routers then they will send out their routing tables. And these routing tables are sent to all the routers they have access to every 30 seconds. Routing table is nothing but a table that containing all the networks. The routers know that how to reach and also the distance to them. From another router while receiving a new routing table at that time each router can see if there is any network on that list and that has a shorter path than the one, that it is currently configured to use [11]. If present then the router will reconfigure itself for using this new shorter path. And the main problem or concern is that, the shorter paths are not always the best path as this RIP protocol doesn't implement any other way to check the best performance of the that path. And RIP protocol also doesn't check for congestion or the availability of the path. So at that time a longer route may be much faster. On port 520 of UDP is used by the RIP protocol.

VI. NETWORK TOPOLOGY

6.1 Hub and Spoke

Most commonly used topology in MPLS VPN by most of the customer for only specific reason which is that in today's world ever body have ERP Server at their premises and also everyone wanted to access this ERP Server remotely or locally on to the WEB. For that one way is to have Internet Connection at all the respective locations and access the server remotely or use MPLS as a technology where Service Provider offer a VPN as services which gives you security to access the Centralized ERP Server [14]. IN MPLS, CE that is Customer Edge is further connected to Service Provider PE that is Provider Edge. Router which then transport the Customer packet to the rest of Customers location through MPLS Cloud and at the same time it offers low latency. There are so many Routing protocols available which are supported by MPLS like RIPV2, EIGRP, Static, OSPF and BGP [16]. And Static would be the most suitable protocol to be used between CE-Pe only if customer has limited set of LAN Routes as well as BGP to be used only where more number of LAN routes to be advertised from Customer End to Provider End.

Every Customer has separate VRF in MPLS Cloud and all the Customer locations which exchange their Routing information in some particular VRF. So any customer can use same set of IP address into their network and the IP would not clash each other because of different VRF for every customer Service provider Configure RD and RT values Export and Import into Customer VRF as that every spoke can speak to their respective HUB location.

There are Some Technical Arrangement

- In HUB and Spoke, Only spokes location can communicate with their respective Hub location
- Configure Separate VRF for every customer in PE.
- CE Router should have 1 Layer 3 port + 1 Layer2 port.
- CE-PE any Routing protocol supported by MPLS Technology.
- AT HUB, HUB RT values would be export and Spoke RT will be imparted.
- AT Spoke - HUB RT values would be imparted and Spoke RT will be Export.

6.2 Full Mesh Topology

In MPLS VPN this is the second one of the Topology which is used by most of the customers and where any location can speak to any location into that particular MPLS Cloud. In this Scenario, everyone wanted to communicate their ERP Server or video Conference or VOIP and File Transfer that which are anywhere placed in any of the Customers location. IN Mesh all the location are connected to each other at the time which offer better latency so that

applications can be access seamlessly and the reason behind is that traffic flow from CE to CE directly instead of being comes to HUB first and then route to respective CE MPLS CE (Customer Edge) is further connected to Service Provider PE (Provider Edge). Router which transports the Customer packet to the rest of Customers location by MPLS Cloud CE-PE Routing Protocol that are RIP, EIGRP, Static, OSPF and BGP [15]. From all of these Static protocol would be the most suitable protocol to be used between CE-PE. And suppose, If customer has limited set of LAN Routes and BGP to be used where more number of LAN routes to be advertised from CE to PE.

Every Customer has separate VRF in MPLS Cloud and also all the Customer locations exchange their Routing information in that particular VRF. So any customer can use same set of IP address into their network as well as IP would not clash each other because of different VRF for every customer Service provider Configure RD and RT values Export and Import into Customer VRF so that every location can communicate with any location.

There are Some Technical Arrangement

- In Mesh any location can communicate with any location.
- Configure Separate VRF for every customer in PE.
- CE Router should have 1 Layer 3 port + 1 Layer2 port.
- CE-PE any Routing protocol supported by MPLS Technology.
- Import and Export RT will be same for all the locations.
- QOS need to configure as per the application requirement.

VII. CONCLUSION

In this paper we have studied detailed about the terms which are used while validating the details over network. Also presented a comprehensive review of all terms of validation in detailed. The detailed review of routers, routing protocols, topology, CoS classes, ans so on is presented. We all hope that this paper will help readers to understand deeply about the concepts of terms which is used over a network an also an opportunity to rethink and exploit and also find some innovative ideas.

VIII. REFERENCES

[1]. Beckett, Ryan and Gupta, Aarti and Mahajan, Ratul and Walker, David, "A general approach to network configuration verification", 2017, acm

[2]. Beckett, Ryan and Mahajan, Ratul and Millstein, Todd and Padhye, Jitendra and Walker, David, "Network configuration synthesis with abstract topologies", 2017, acm

[3]. Lee, Kyungwoon and Hong, Cheol-Ho and Hwang, Jaehyun and Yoo, Chuck,"Dynamic Network Scheduling for Virtual Routers", 2019, IEEE

[4]. Dua, Aneesh and Tyagi, Vibhor and Patel, ND and Mehtre, BM, " IISR: A Secure Router for IoT Networks", 4th International Conference, 2019, IEEE

[5]. Knoll, Dipl-Ing Thomas Martin, "BGP Class of Service Interconnection", 2017

[6]. Usman, Muhammad and Oberafo, Eromosele Ehimeme and Abubakar, Mahdi Alhaji and Aminu, Tahir and Modibbo, Abubakar and Thomas, Sadiq, "Review of Interior Gateway Routing Protocols", 15th International Conference, 2019, IEEE

[7]. V Monita, ID Irawati, R Tulloh," Comparison of routing protocol performance on multimedia services on software defined network",vol. 9, 2020, beei

[8]. Balasas, E Angelo's and Psannis, Kostas E and Roumeliotis, Manos, " Performance Evaluation of Routing Protocols for BIG Data Application", 2019, Springer

[9]. Srivastava, Rishabh and Singh, Archana,"Route Redistribution Between EIGRP and OSPF Routing Protocol Using GNS3 Software", vol. 5, 2017, International Journal for Research in Applied Science & Engineering Technology

[10]. C Risso, C Mayr, E Gramp´ın, "A Combined BGP and IP/MPLS Resilient Transit Backbone Design" 11th International Conference, 2019, IEEE

[11]. Wai, Khaing Khaing, "Analysis of RIP, EIGRP, and OSPF Routing Protocols in a Network", 2019, academia.edu

[12]. Bauer, David and Yuksel, Murat and Carothers, Christopher and Kalyanaraman, Shivkumar,"A case study in understanding OSPF and BGP interactions using efficient experiment design", 2006, IEEE

[13]. Da Silva, Ricardo Bennesby and Mota, Edjard Souza, "A survey on approaches to reduce BGP interdomain routing convergence delay on the Internet", vol. 19, 2017, IEEE

[14]. Pavani, K and Mishra, Himanshu and Karsh, Ramkumar, "Multi-attached Network Topology with Different Routing Protocols and Stub Network Resolution in OSPF Routing", 2019, springer

[15]. Farkash, Maryam,"Network Topology", 2018, Libyan International Medical University

[16]. Zhalechian, M and Torabi, S Ali and Mohammadi, M,"Hub-and-spoke network design under operational and disruption risks", vol. 109, 2019, Elsevier

Cite this article as :

Swapnil Wable, Divya Punwantwar, Manisha Mali, Kirti Wanjale, "Formal Analysis of Network Properties for Network Validation ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 2, pp. 628-636, March-April 2020. Available at doi : https://doi.org/10.32628/IJSRSET2072119
Journal URL : http://ijsrset.com/IJSRSET2072119