International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

DESIGNING A HIGH LEVEL CO-ORPOREATE NETWORK INFRASTRUCTURE WITH MPLS CLOUD

[1]B. Sarat Sasank , [2]G.V. Eswara Rao, [3]K.S.D. Kuladeep Kumar, [4]V. Balu Veeren, [5]B. Shraavan Kummar

[1]Student, Department of Computer Science & Engineering, Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, India
[2]Assistant professor, Department of Computer Science & Engineering, Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, India
[3,4,5]Student Department of Computer Science & Engineering, Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, India

---

ABSTRACT

The substandard network design makes organizations prone to many security attacks and can lead to information breach since there are many people around us watching and monitoring every possibility to break into the network. So it becomes indispensable to build a network with highly sophisticated techniques and integrating them congruent to the network design. So, we design a network by implementing the technologies that are considered to be the finest in their respective areas thereby providing security to the network from its base. In this paper, we first discuss the protocols and other leading edges that are incorporated in detail for the network design, further their implementations with perspicuous outputs. This document details about MPLS, the technology created over TDM for reliable telecommunication protection along with how efficiently OSPF, HSRP, VLANs, ACLs, and their implicit functionalities are utilized to achieve the intent.

KEYWORDS

Multi Protocol Label Switching (MPLS), Open Shortest Path First (OSPF), Virtual Local Area Network (VLAN), Wide Area Network (WAN), Firs Hop Redundancy Protocol (FHRP), Hot Standby Redundancy Protocol (HSRP), Access Control Lists (ACLs), Network Address Translation (NAT), Time Division Multiplexing (TDM), Border Gateway Protocol (BGP), Link State DataBase (LSDB)

INTRODUCTION

In earlier days of networking there aren't many risks of security attacks and data thefts since the resources of using internet are very less and capitals are high as a result of which a very few people have the cognizance of using the internet but as a consequence of globalization every individual now have the access to the internet and number of people using it has ameliorated drastically. Along with the users, the traffic that is generated has been increasing every day which becomes the major threat in preserving security. Instead of providing the very strict rules and norms for a feeble network it is better to design a well defined and robust network. So, the network design plays a fundamental role in providing security for any organization being the cardinal level of limiting illegal access and authorizations to organizations. The recent survey conducted across the globe has shown that more than 80 percent of the security violations and outbreaks are caused within the organization than outside which depicts the importance of strong network design.

The implementation of routing protocols like OSPF provides packet flow to the external networks and also succor in keeping different areas that are connected to the backbone area and summarizations for minimal traffic congestions. The HSRP is used for the subsecond network convergence in case of the first hop failure by providing the backup gateway making the network uptime to the maximum extent. The VLANs are configured for the inner organizational security by restricting the data transferring to particular subnets and allowing it to flow under certain circumstances. The NAT also plays an important role in network security and from data breach protection by hiding the private addresses and showcasing the public addresses. The type of traffic flow which is the key factor to be examined for illegal entry of packets into the network is provided by the ACLs. The provision of high bandwidth for productive work is accomplished by using route-maps which is called policy-based routing.

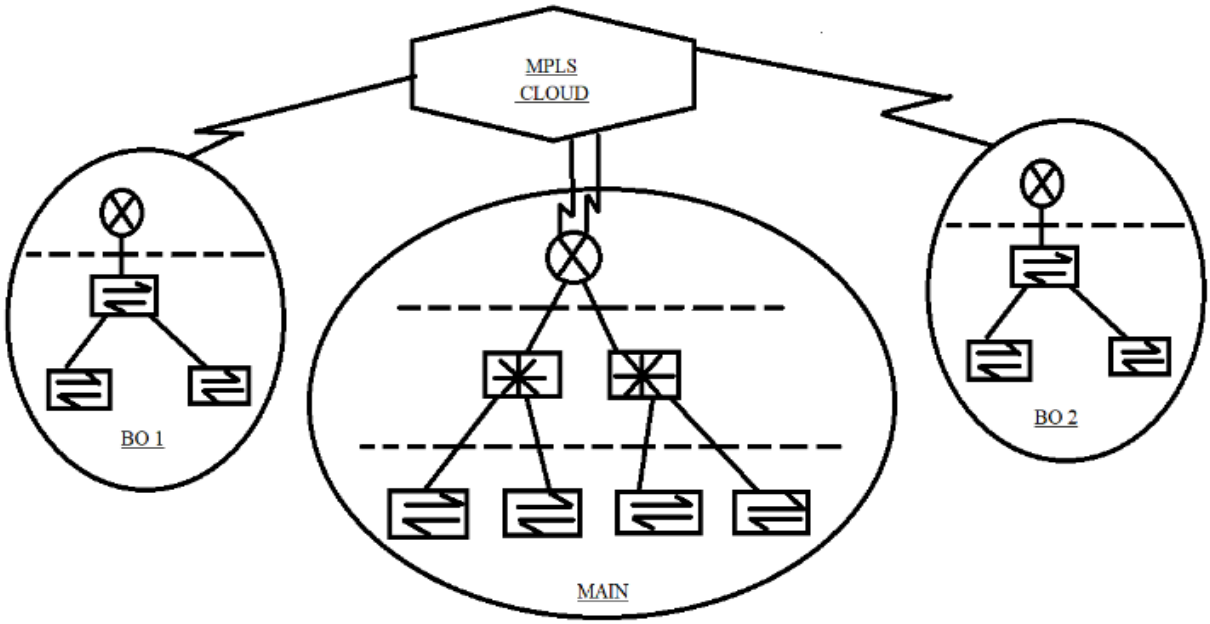
We can be able to provide high security for a network by using all the technologies in the right way and in the right proportions.

The MPLS technology is mainly used for the reliable transmissions and also to allow the minimum packet dropouts from the transmissions. Apart from MPLS, we can also use employ Frame Relay (FR) for this task but it is not so often used nowadays and incompetent when compared to the MPLS. The MPLS promises a better bandwidth, speed, scalability, Quality of Service (QOS) and traffic control making it a first choice for selecting among the point to point connections. The MPLS forwards the packets by swapping the labels of incoming and outgoing packets and their ports. This forwarding is based on the labels which are dependent not only on the ip addresses but also on paths, services management, congestion, QoS and other factors which makes it different from the traditional ip forwarding. All the label switch routers (LSR) which are present in the cloud are not of the same kind. Some give priority for the data, some for the voice and some for the video forwarding. This way MPLS makes its selection and switches the packets accordingly.

LITERATURE SURVEY

There are many research works related to the technologies and protocols that are used in the network design. They have provided the structure and usage of particular technology severally in their distinctive works like OSPF, MPLS, BGP, FHRP. One cannot use the best metrics in the particular technology to make a good network design. The selection of the extent to which these technologies to be used is purely and solely depends on the type of network that is designed. One cannot presume or possess a standard network design but has to use the knowledge of them to design the network of their own in the way they require for the organization. This document is about designing a good network using MPLS as a main and effective use of other technologies to build a high-end secure network according to the requirement and congruence with one another that is not susceptible to the attacks.

SYSTEM ARCHITECTURE



METHODOLOGIES

ROUTING PROTOCOL

It is important to learn the routes not only those which are directly connected to a router but also those that are obliquely connected. The former one's information is obtained from the interface particulars and configurations. For the later ones, we need routing protocols to accomplish the task. The routing protocols allow communication between different routers and help them in exchanging their information with the others.

The routing protocols mainly work by the principle of exchanging hello messages. These multicast messages not only help in establishing the relationship between the routers but also in sustaining the relationship even after the connection was established. The routing protocols are broadly classified into two categories. They are link-state routing protocols and distance-vector routing protocols. The usage of link-state routing protocols is preferred to distance-vector as they contain the complete knowledge on all the routes present in the network whereas the distance-vector just possesses information only about the directly connected routes.

However, the preference is done on the design of the topology.

OSPF

OSPF which stands for Open Shortest Path First is a link-state classless routing protocol that is being widely used in organizations for its many advantages. It maintains a topological table also know as LSDB (Link State DataBase) and uses Dijkstra's shortest path algorithm for its route selection process. It works well on both simple and advanced network topologies that make it feasible for everyone. OSPF unlike RIP uses bandwidth and delay as the metrics for the route selection process and can provide equal load balancing.

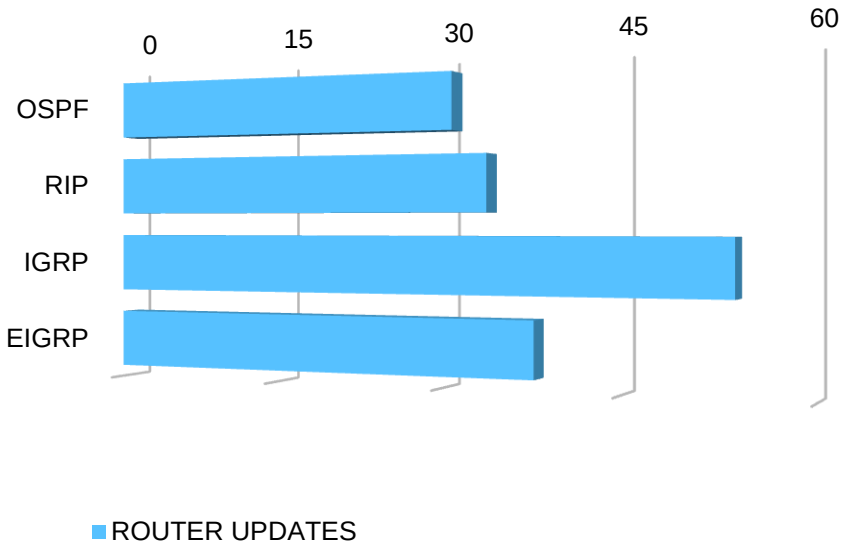
In OSPF, forming the neighbor relation follows some sequences of steps. First, the router must be given a router-id manually or else the highest interface ip-address will be considered as its router-id. The interfaces that are connected are to be added to the link-state database and then hello messages are exchanged between the routers. The hello messages must have the same hello and dead timers, areas, subnet mask, authentication passwords for the successful exchange.

Succeeding the hello message transfer, the routers are related and are said to be in a master-slave relationship and form neighbors. This is followed by required information transfer between the routers from their databases which are acknowledged and reviewed. Finally, after these steps, the neighbors are synchronized and said to be in FULL STATE.

The presence of too many routers in the topology results in network loop when an update occurs because in the link-state routing the updates are being transmitted to every router that creates a network loop. To control this, a router per ethernet will be selected and is assigned the role of transmitting the route updates thereby controlling the chances of a loop. This selected router is known as Designated Router (DR) and a backup for this router is also selected which is called Backup Designated Router (BDR). The DR selection can be done manually by giving more priority or dynamically by selecting the one having the highest router-id. The DR maintains the 2-way relation with the other routers.

The ospf being a link-local routing protocol contains a large database of routes which sometimes leads to overload and congestion within the network. So, in ospf protocol, the network is divided into small groups called areas that are numbered from ‘0’ to facilitate the administration, confinement of routing updates, resource optimization, and traffic control. Area 0 is known as the BACKBONE area and every other area must be connected to the backbone area.

The routers present at the border of two areas are called AREA BORDER ROUTER (ABR) where we can summarize the routes



to provide the feature 'confinement of routing information'. The routers present at the border to two autonomous systems (end of companies ospf) are called AUTONOMOUS SYSTEM BOUNDARY ROUTER (ASBR). Only ABR and ASBR routers are used to summarize the routes but no other router can perform the job in ospf. However, it is known that every area must be connected to area 0 but it can be overruled by connecting to other areas (say area x) by using virtual-links. The virtual-links logically connects the area (x) to the area 0 and spoofs that it is physically connected to area 0.

FHRP

FHRP stands for First Hop Redundancy Protocol, works in layer 3 of the OSI model. It is created typically to provide redundancy for a gateway that provides the internet to a network. The gateway router is the only way that a network or subnet is connected to the internet, the event of failure makes the complete network into isolation.

So when a failover occurs to the active gateway then the redundant gateway must become active and perform the job of gateway until the original gateway comes back to the line. The routers in the group must possess the same ip address for the redundancy operation but since it is not possible to have the same ip in a subnet we keep a virtual ip that is different from their individual ip for this operation. There are 8 types of FHRP of which HSRP, VRRP, GBP are eminent.

HSRP

The Hot Standby Redundancy Protocol (HSRP) is a Cisco proprietary redundancy protocol that is most popularly used among FHRP to achieve maximum percent of network uptime. It was first created in 1994 by Cisco and it was available in two versions having the port number 1985.

The protocol consists of default values in which the priority and decrementing values are 100 and 10 respectively. The virtual MAC address of HSRP has a form of 0000.0C07. AC XX where 0000.0C is the Cisco vendor id, 07.AC is the HSRP id and XX is the standby group number.

The primary gateway or the first hop is regarded as an active gateway and the secondary gateway is considered as standby gateway in the terminology of HSRP. There will be only one gateway that is active and others in the group will be in a standby state. The active and standby states of a router are determined by the priority values that are assigned to them, the highest priority router becomes the active gateway. The active router is the one that is responsible for responding to the network requests. The HSRP group shares a single virtual ip and Mac addresses and every router in the group (in particular is active) responds with the same Mac address upon the ARP requests. It is also possible to keep a separate active gateway for separate VLANs.

HSRP uses multicast messages to exchange the hello messages to keep track of the priority and current values of the gateways. It sends hello messages for every 3 seconds and the hold on or dead timer is set to 10 seconds if it crosses 10 seconds without receiving a hello message the active router goes to the standby state by decrementing the priority value of previous active router which will be gained by the standby to become active. Again if the first-hop gets back from failover then the above process happens automatically making it the active gateway.

VLANs

The main problem with the switches is that they cannot multicast the messages instead of unicasting and broadcasting. It is because switches only break the collision domain but not the broadcast domain as the routers do. In the practical world, it is not appropriate to place routers everywhere as it adds great complexity to the network. So it becomes paramount for a switch to break the broadcast domain so that only a particular group of devices will receive the messages i.e., multicasting.

VLAN stands for Virtual Local Area Network and works at the data-link layer. The VLANs are regarded as broadcast domains that are divided into different logical groups that communicate as if they were directly connected when there are in the same VLAN group. The VLANs works on the principle of tagging, the VLAN ids are assigned to the ports, when the messages or the data passes through the port will be appended by the VLAN id number that the port is assigned to. So, the ports in a switch containing the same VLAN id are considered to be in one broadcast domain. This process achieves the goal of multicasting in switches.

A switch can possess 4094 VLANs that can be used. The VLAN 1 is considered as a default VLAN and in general, it is also regarded as native VLAN but it's not necessarily the same. The native VLAN-id numbers must be the same for two switches that are connected for the communication to takes place. The network management protocols like CDP, LLDP, VTP, DTP flow through the VLAN 1 for the maintenance of the configurations.

The switch usually contains 2 types of ports which are access and trunk ports. The ports connecting computer and switch are the access ports and two network devices are trunk ports. If a message is to transferred to the same VLAN in the other switch then the connecting link between the two switches must be made trunk as they allow the tagged traffic. The Inter-Switch link which is a Cisco proprietary and IEEE's 802.1q which is industry standard are the tagging protocols.

It betides in a practical world to communicate not only within a VLAN group but between the VLANs. Since the communication between two VLANs is regarded as the communication between two broadcast domains this process can be accomplished in three ways in which the first facet is using routers (as it breaks broadcast domain), the second facet is to male use of l3 switching and the final facet is ROAS.

ROAS

The ROAS which is known as Router on a Stick is one of the techniques that is deployed for inter VLAN communication. The main aim here is to break the broadcast domain that paves the path for the communication between the VLANs. This process can be performed by allowing different switches containing single VLAN must be connected to the separate routing interfaces but being the router limited to a very little number of interfaces cannot fully accommodate a large number of VLAN groups which requires more routers that in turn increases the complexity of the network.

To mitigate this problem the sub interfaces of the router are the concept that is emerged which logically divides the single router interface into many sub interfaces that succor in the effective utilization of the router interfaces. Each sub interface is given an ip address to that particular VLAN group and the interface between the router and the switch must be made trunk for the flow of tagged traffic. Eventually, the communication betides between the VLANs

ACCESS CONTROL LISTS

The access-lists are the set of rules that are configured in the router which determines whether a packet to pass through the router or not. These access-lists are used to mitigate the network attacks as it restricts most of the illegal traffic and promotes

network security. One can either permit or deny particular traffic by using their ip addresses and port numbers. Besides access control, they also provide services like NAT, QoS, Demand Dail Routing, Policy routing, Route filtering.

Analogous to the entry list carried by the watchman, the access-lists act like the entry list which checks all the incoming and outgoing traffic from the router. The examination or checking the entries in the access-lists betides from top to bottom and stop at the first match. In general, there are two main types of access-lists they are standard ACLs and extended ACLs. The standard access control lists work only on the source ip address and range from 1-99, 1300-1999. The extended access control lists work on both source and destination ip addresses and have a number range from 100-199, 2000-2699.

NAT

The ipv4 being a 32-bit always have a dread for ip completion. The discovery of private ip addresses made this a long-lasting process. The public ip addresses are brought from the ISP and the ones that are being advertised to the others on the internet. The private ip addresses are the one which is used inside the organization and are not advertised to the outside world. These private addresses can be the same in different organizations but cannot be identified within the organization.

The ip addresses in ipv4 are classified into 5 classes that are used according to the topology.

Class A	10.0.0.0 – 10.255.255.255	16 million hosts on 127 networks
Class B	172.16.0.0 – 172.31.255.255	65,000 hosts on 16,000 networks
Class C	192.168.0.0 – 192.168.255.255	254 hosts on 2 miilion networks
Class D	224.0.0.0 — 239.255.255.255	Multicast addresses
Class E	240.0.0.0 to 254.255.255.254	For military, research purposes and future use

The disclosure of the private ip addresses leads to huge information breach and grievous effects on the security norms of organizations. So it is cardinal to hide the private ip addresses and communicate using the public ip. NAT which stands for Network Address Translation does the job of translating private ip to the organizational public ip thereby safe-guarding the organizational policies. The translation can be done manually by assigning the translation for prescribed addresses or dynamically by providing the pool of addresses that can be chosen when there is more than one public ip address.

In the terminology of NAT, there are four types of addresses that succor in better assimilation of the process of translation they are inside local, inside global, outside local and outside global. These addresses help in the translation of addresses.

POLICY ROUTING

In substantial organizations, some employees perform non-productive work along with productive ones which leads to network and traffic congestions despite owning more than one ISP. So, it becomes paramount to provide greater bandwidth for the productive work employees than that with the entertainment ones. Of many options available, the policy routing is the optimal choice that provides more network uptime for productive work.

The policy routing is accomplished by making the route-maps which decides the next hop or router reach. The route-maps plays a very vital role as it identifies the type of traffic and directs them towards the specified destination ISPs, it makes use of the access control lists for the identification process. These access control lists are created prior to the creation of route-maps and the traffic in the access control lists are classified either on ip addresses or port numbers depending upon the requirement of the organization. After the ACLs are set, the route-maps then match the traffic and provide the route for the next hop, an empty match must be made which is very essential since any traffic that does not match with any of the available access control lists will be treated here and directed to specific ISP.

LAYER-3 SWITCHING

Switches are often regarded as one of the best man-made network devices base on many grounds of which the main reason would be its hardware implementation (ASIC's). They are the layer 2 devices that support many incredible protocols and effective algorithms but are limited only to the switching techniques and cannot be used to transfer packets ou of the subnet or the network.

The l3 switches perform both switching and routing and are effective when compared with the layer 2 switches. They can utilize the routing protocols effectively and can limit the spanning-tree failures. It contains a very less failure domain and more convergence time. It is even faster than the router is sending packets as it works on ASIC's but being incapable of performing some functions like NAT which are completely software-based makes the router still alive.

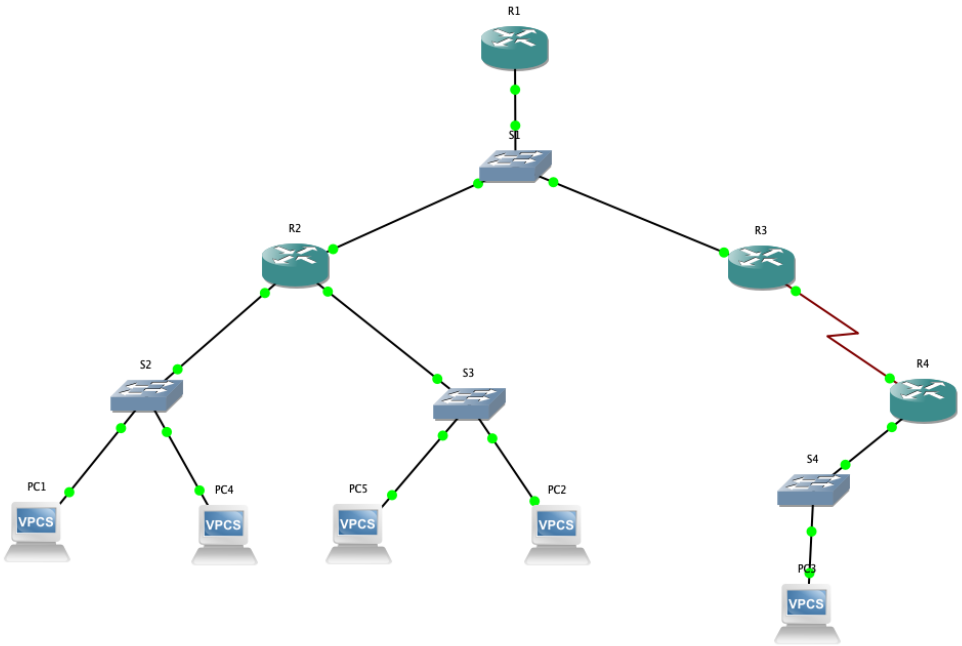
IMPLEMENTATION

The network design is implemented in three modules. In the first module, we design the branch office and its configuration. In the second module, we design the main office and in the third module, we design the MPLS cloud and its redistribution.

Designing Branch Office

In the branch office, we implement OSPF as the routing protocol among the other routing devices due to its flexibility and fine routing capabilities. First, we consider the branch office as more than one-floor building each floor accommodating a router that is connected to the switch where the end system gets access from. We also provide a WAN link between two routers to make sure that OSPF is routing the packets to the external addresses by its entry into its database table.

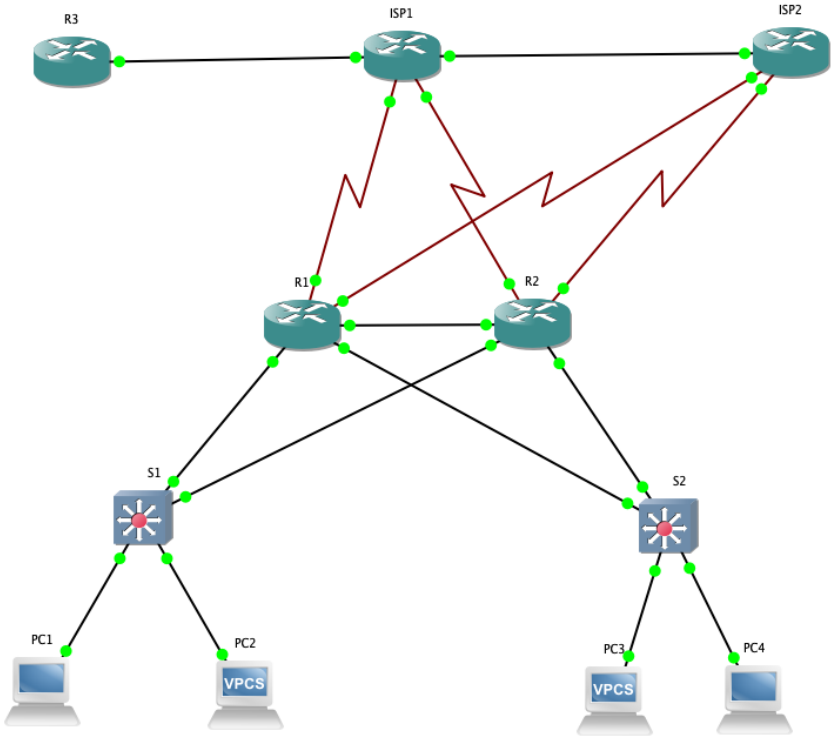
All the routers present on each floor are commonly connected to the main switch that is placed in the server room. The main switch is singly connected to the main router which is directly linked to the outside world or the internet. Internally we provide securities like VLANs which makes a certain group of devices communicate and process the information. The inter-VLAN communication is accomplished by using the ROAS, which is dividing the physical interface of the router into sub interfaces making them more than one logical connection and providing the capability of breaking the broadcast domain.



Designing Main Office

The main office being the core of an organization it needs high-level security measures and also since the branch office is connected to it. The main office is more likely a hub, a data center for the entire organization. We provide redundancy for the main routers since they are the ones who transmit the crucial organization data to the branch offices. For the redundancy we choose HSRP being its quality of keeping high network uptime. The l3 switching is employed for high-speed routing and the other sophistications of l3 over l2 switching techniques make the device for better transmission and routing operations.

The DHCP is also configured differentiating different VLANs present in the network for dynamic allocation of ip and providing the flexibility of adding new end systems. We provide two ISPs connected to the main office for providing larger data transfer and bandwidth. Above all, the policy-based routing using route-maps makes the design more productive for organizational works. This technique classifies the productive and lethargic work using access control lists and thereby directing them to the specific ISPs.



Redistributing BGP routes

The cloud predominantly consists of routers that make use of the BGP routing protocol as it is the only exterior gateway protocol present currently. Since being the branch offices have OSPF as the routing protocol, the BGP routes cannot be routed because of the protocol incompatibility. So, we perform redistribution technique by which the router on both sides i.e., in the cloud and the branch offices learns about each other routes and are been distributed and this process is known as redistribution. This allows very router and device to communicate with one another.

Outputs

```
R2#
R2#
R2#sh ip int b
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  up                    up
FastEthernet0/0.2          10.1.5.1        YES NVRAM  up                    up
FastEthernet0/0.3          10.1.7.1        YES NVRAM  up                    up
FastEthernet0/1            10.1.1.2        YES NVRAM  up                    up
FastEthernet1/0            unassigned      YES NVRAM  up                    up
FastEthernet1/0.2          10.1.4.1        YES NVRAM  up                    up
FastEthernet1/0.3          10.1.6.1        YES NVRAM  up                    up
Serial2/0                  unassigned      YES NVRAM  administratively down down
Serial2/1                  unassigned      YES NVRAM  administratively down down
Serial2/2                  unassigned      YES NVRAM  administratively down down
Serial2/3                  unassigned      YES NVRAM  administratively down down
R2#
R2#
```

Fig-1: ROAS sub interface output

```
R1#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 200.1.1.50         10.1.10.50         ---                ---
```

Fig-2: OSPF neighbor

```
R2#
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 7 subnets
O       10.1.3.0 [110/75] via 10.1.1.3, 00:01:46, FastEthernet0/1
O       10.1.2.0 [110/74] via 10.1.1.3, 00:01:46, FastEthernet0/1
C       10.1.1.0 is directly connected, FastEthernet0/1
C       10.1.7.0 is directly connected, FastEthernet0/0.3
C       10.1.6.0 is directly connected, FastEthernet1/0.3
C       10.1.5.0 is directly connected, FastEthernet0/0.2
C       10.1.4.0 is directly connected, FastEthernet1/0.2
R2#
R2#
```

Fig-3: OSPF routes

```
R2#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/DROTHER    00:00:33    10.1.1.1        FastEthernet0/1
3.3.3.3           1   FULL/DR         00:00:33    10.1.1.3        FastEthernet0/1
R2#
```

Fig-4: NAT addresses

```
R1#sh route-map
route-map pbr, permit, sequence 10
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    ip next-hop 200.1.1.1
  Policy routing matches: 0 packets, 0 bytes
route-map pbr, permit, sequence 20
  Match clauses:
    ip address (access-lists): 191
  Set clauses:
    ip next-hop 201.1.1.1
  Policy routing matches: 0 packets, 0 bytes
route-map pbr, permit, sequence 30
  Match clauses:
  Set clauses:
    ip next-hop 201.1.1.1
  Policy routing matches: 0 packets, 0 bytes
R1#
```

Fig-5: HSRP report

```
*Mar  1 00:01:26.227: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet1/2 from LOADING to FULL, Loading Done
*Mar  1 00:01:26.231: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet1/1 from LOADING to FULL, Loading Done
R1#sh standby
FastEthernet1/1 - Group 1
  State is Standby
    1 state change, last state change 00:00:58
  Virtual IP address is 10.1.10.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 200 msec, hold time 600 msec
    Next hello sent in 0.000 secs
  Preemption enabled, delay reload 60 secs (0 remaining)
  Active router is 10.1.10.3, priority 100 (expires in 0.500 sec)
  Standby router is local
  Priority 110 (configured 110)
    Track interface FastEthernet0/0 state Up decrement 20
  Group name is "hsrp-Fa1/1-1" (default)
FastEthernet1/2 - Group 2
  State is Standby
    1 state change, last state change 00:00:58
  Virtual IP address is 10.1.20.1
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 200 msec, hold time 600 msec
    Next hello sent in 0.000 secs
  Preemption enabled, delay reload 60 secs
  Active router is 10.1.20.3, priority 110 (expires in 0.396 sec)
  Standby router is local
  Priority 100 (default 100)
    Track interface FastEthernet0/0 state Up decrement 20
  Group name is "hsrp-Fa1/2-2" (default)
R1#
```

Fig-6: policy-based routing using route maps

CONCLUSION

The need for a well-designed network is always been a major asset for any organization. Creating a network is not a simple task of imbibing all the available protocols, it involves huge care, supervision, management, and confidentiality. The understanding of requirements and availabilities of an organization and implementing the protocols that are needed in such a way that they are compatible is the best way of building a network. In this paper, we have assumed the ideal network requirements and selected the finest protocols like MPLS, OSPF, HSRP, NAT, VLAN, DHCP and many more to design and provide the security to the network.

REFERENCES

[1] TRILLIUM: Multiprotocol Label Switching (MPLS).

[2] Enovate: Multiprotocol Label Switching (MPLS).

[3] HUAWEI Technologies Proprietary: Quidway MA5200G MPLS Configuration Guide, June 2007.

[4] Alcatel: The Role of MPLS Technology In Next Generation Networks, October 2000.

[5] Technical University of Madrid: Network Convergence over MPLS.

[6] COMPREHENSIVE MPLS VPN SOLUTIONS: Meeting the Needs of Emerging Services with Innovative Technology. 3510324-003-EN.pdf, Jan 2010.

[7] IP Solution Center-MPLS VPN: Deploying MPLS VPN Service. White Paper, Cisco Systems, Inc. [17] Cisco MPLS based VPNs: Equivalent to the security of Frame Relay and ATM, White Paper. March 30, 2001.

[8] Neha Grang and Anuj Gupta, "Compare OSPF Routing Protocol with other Interior Gateway Routing Protocols", IJEBEA 13-147, Vol 1, pp.2-4, 2013

[9] Nikhil Hemant Bhagat," Border Gateway Protocol –A Best Performance Protocol When Used For External Routing than Internal Routing", Vol 1, pp.1-2, 2012

[10] A.Alaettinoglu,C.Villamizar,E.Gerich,D.Kessens,D.Meyer, T. Bates, D. Karrenberg, M. Terpstra, "Routing policy specification language (RPSL)," IETF RFC 2622, June 1999.

[11] T. Griffin, A. Jaggard, V. Ramachandran, "Design principles of policy languages for path vector protocols," in Proc. ACM SIG- COMM, August 2003.

[12] L. Subramanian, M. Caesar, C. Ee, M. Handley, Z. Mao, S. Shenker, I. Stoica, "HLP: A next-generation interdomain routing protocol," in Proc. ACM SIGCOMM, August 2005