

Design and Implementation of Network Security using Inter-VLAN-Routing and DHCP

Iqbal Ahmad¹, Dr.Javed Ashraf² & Dr.Anisur Rehman Nasir³

¹M.Tech Scholar., Al-Falah University, Haryana, India.

²Assistant Professor, Al-Falah University, Haryana, India.

³Associate Professor, Jamia Millia Islamia (Central University), India.



DOI: 10.38177/ajast.2020.4306

Article Received: 19 May 2020

Article Accepted: 28 June 2020

Article Published: 29 July 2020

ABSTRACT

Enterprise or campus networks are usually large in size and are difficult to manage. Network administrators are required to frequently perform deliberate changes according to the organizational needs. VLANs are broadly used in enterprise or campus networks to improve scalability, flexibility, ease of management, and to reduce broadcast. Therefore it's providing layer 2 security as it limits the number of the broadcast domains. Nowadays in this fast-growing industrial age, every company needs the speed of data transfer from one network to another network in manufacturing to cope up with the customer's requirements. The basic objective of our project is to develop a versatile and low-cost INTER-VLAN-ROUTING which can be utilized in any industry or campus to eliminate this problem. INTER VLAN increases the performance of the network by providing flexibility to the users to log in to any network within the same group without changing their IP address. This also reduces complexity and it also cost-effective

Keywords: LAN, VLAN, Inter-VLAN Routing, IPv4, Trunking, Encapsulation.

1. Introduction

The project is based on the creation of VLANS and then Routing among them. A virtual local area network (VLAN) is a logical separation of network users and resources connected to administratively defined ports on a manageable switch. By creating VLANs, we can create smaller broadcast domains within a switch by assigning different ports in the switch to different subnetworks [1-2]. A VLAN is treated like its own subnet or a broadcast domain. This means that frames broadcast onto a network are only switched between ports in the same VLAN. A host of one VLAN could not directly communicate with the host of another VLAN [4-7]. For this purpose, inter-VLAN routing techniques are used. Inter-VLAN routing is the process of forwarding traffic from one VLAN to another VLAN by using a layer-3 device. Apart from this it also provides facilities for connecting hosts of different virtual LANs to other LANs without changing their IP address.

2. Related Work

Separate physical gateway on the router or called Legacy inter-VLAN routing technique has a significant limitation as routers have a limited number of physical ports to connect to different VLANs. If the number of VLANs increases on a network, having one physical router interface per VLAN will quickly exhaust the physical port capacity of a router. To overcome this in larger networks is to use VLAN Trunking on the switch and creating virtual subinterfaces on the physical interface of the router [7-9]. VLAN Trunking mode will allow a single physical router interface to route traffic for multiple VLANs and this technique is known router-on-a-stick.

Each subinterface is configured separately with its own IP address and subnet mask. This method allows a single physical interface to simultaneously be part of multiple logical networks. While configuring inter-VLAN routing using the router-on-a-stick technique, the physical port of the router must be connected to a trunk link on the adjacent switch network. Each subinterface is assigned an IP address specific to its subnet/VLAN and this is also

configured to tag frames for that VLAN [11]. This way, the router keeps the traffic from each subinterface separated as it traverses the trunk link back to the switch.

3. Virtual Local Area Network (VLAN)

In a LAN, the hosts are connected to each other with switches. Similarly, users belonging to different departments are connected through the switch and it is having one broadcast domain by default. It is not possible to divide the switch into parts physically; however, we can logically divide it into segments [8]. Each logical segment behaves like a separate physical switch. This technique splits a single broadcast domain on the switch into multiple broadcast domains. This technique increases the efficiency as well as provides security. Every segment becomes a separate domain for each department. As a result, flooded broadcast information can be reduced but not eliminated. These Virtual LANs can span across multiple switches with trunk links. Trunks transfer traffic for various VLANs [12-13]. Trunks use special encapsulation to discriminate among different VLANs except for native VLAN.

4. DHCP (Dynamic Host Configuration Protocol)

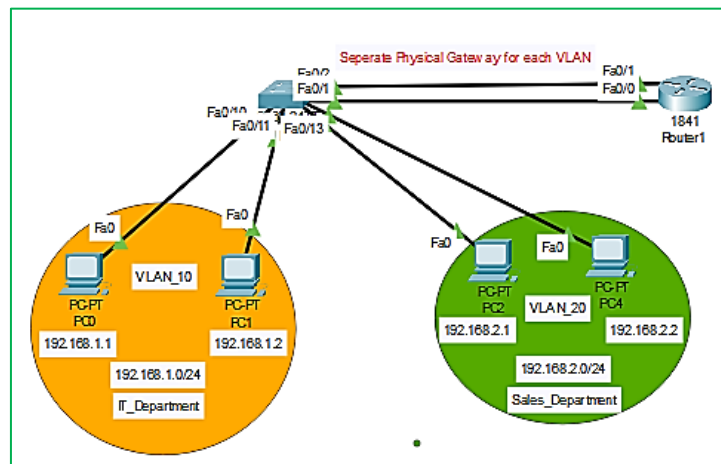
DHCP (Dynamic Host Configuration Protocol) is called as a server-client model or a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device connected on a network so they can communicate using IP. DHCP centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network devices hence it automates this process. DHCP can be configured on small local networks, as well as in big enterprise networks [3-4]. DHCP works at the application layer of the Transmission Control Protocol/IP (TCP/IP) stack to dynamically assign IP addresses to DHCP clients and to allocate TCP/IP configuration information to DHCP hosts and uses ports number 67 & 68. This also includes subnet mask information, default gateway IP addresses, and domain name system (DNS) addresses [9]. Therefore DHCP is used in this network design to assign IPs to the local devices and DHCP configuration is done on the router to facilitate this. Hence this way manual intervention is not required.

5. Inter-VLAN Routing

VLANs classify different users and their traffic from each other by placing them into different VLANs and every VLAN has a single broadcast domain. In this way, a large network is divided into smaller segments called IP sub-nets. A host can communicate with other hosts existing in the same subnet but it can't communicate directly with another host which is located in a different subnet [2-6]. Now the question is how does traffic pass between two different VLANs? The answer is: it is feasible to engage a layer-3 device into subnets to route the traffic among multiple VLANs. Also, VLAN is a separate broadcast domain, so devices on separate VLANs are unable to communicate without the intervention of a routing device. The device that supports Layer 3 routing, such as a router or a multilayer switch, can be used to perform the necessary routing functionality [9]. The process of forwarding network traffic from one VLAN to another VLAN using the routing concept regardless of the device used is termed as inter-VLAN routing. In modern LAN networks; three inter-VLAN routing techniques are used. These are given below:

1. Router-on-a-stick

2. Router-on-a-stick using trunk
3. Layer-3 switch routing (SVI)



5.1 Router-on-a-stick- This network architecture is the most basic method of inter-VLAN routing. In this technique, a router's interface is connected physically to each VLAN [12]. It is simple to understand because the separate physical gateway is used and both layer-2 and layer-3 functions are physically parted. The network diagram showing the router-on-a stick.

5.2 In router-on-a-stick using trunk- In this network architecture, instead of multiple physical interfaces, a single trunk interface is connected to multiple VLAN by using Trunking protocols such as ISL or 802.1q. Sub-interfaces of that physical interface are used to connect the router to each VLAN and IP addresses are assigned to sub-interfaces as a default gateway. This concept is broadly used in this project to design the network.

5.3 In layer-3 switch routing: Switch Virtual Interface (SVI)

SVI is a logical interface on a multilayer switch that provides layer 3 processing for packets to all switch ports associated with that VLAN. SVI for layer 3 switches can provide both management and routing services on the other hand SVI on layer 2 switch provides only management services like creating VLANs or telnet/SSH services. The SVI created for the respective Vlan acts as a default gateway for that Vlan just like the sub-interface of the router (in the process of Router On a stick) [3]. If we need to deliver a packet to different VLAN i.e inter Vlan Routing is to be done on layer 3 switch then first the packet is delivered to layer 3 switch and then to the destination just like in the process of the router on a stick.

6. Network Scenario of Inter-VLAN-Routing and DHCP

Let us consider a company or college campus network which has four departments such as Engineering, Medical, B. Arch, and MBA faculties. All of these departments have their own personal inter-network and one main network is made to connect these four networks and thus the company requires proper inter-network to provide mobility to all of its four departments. Thus we can build a network in which we want to implement user mobility in the network, reducing complexity, and at the same time, we also provide security in the network. By creating a virtual LOCAL AREA NETWORK (VLAN) in a pure switched inter-network and we will be able to provide flexibility for the user to login to any network. And at the same time, the network should be cost-effective also.

Network Architecture

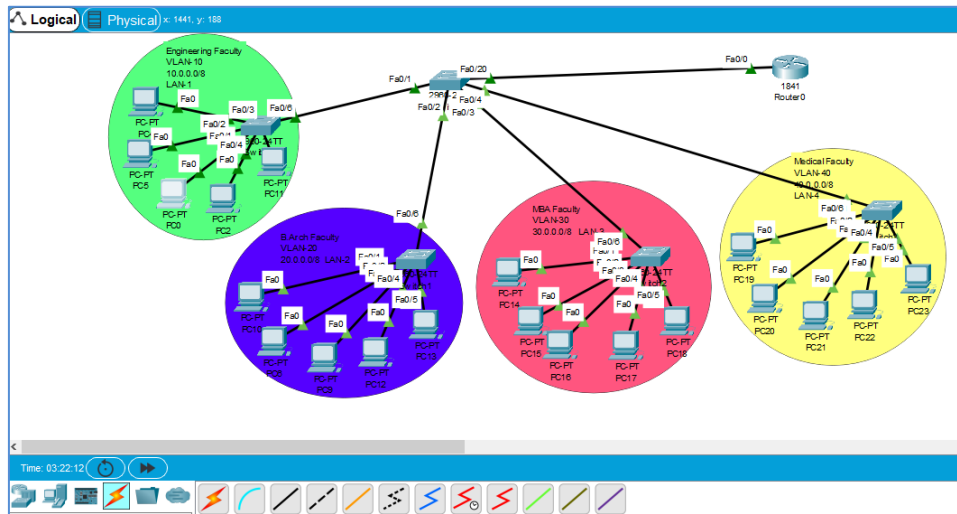


Figure: Enterprise or campus networks Network Design

APPENDIX: Configuration used in Experimentation

ROUTER: Commands and Configuration

```

Router>en
Router#conf t
Router(config)#hostname
M(config)#enable secret ccna
M(config)#line vty 0 4
M(config-line)#password 1234
M(config-line)#login
M(config-line)#exit
M(config)#int f0/0
M(config-if)#no shut
M(config)#int f0/0.10
M(config-subif)#encapsulation dot1Q 10
M(config-subif)#ip add 10.0.0.1 255.0.0.0
M(config-subif)#int f0/0.20
M(config-subif)# encapsulation isl 20
M(config-subif)#ip add 20.0.0.1 255.0.0.0
M(config-subif)# int f0/0.30
M(config-subif)# encapsulation isl 30
M(config-subif)# ip add 30.0.0.1 255.0.0.0
M(config-subif)# int f0/0.40
M(config-subif)# encapsulation isl 40

```

```
M(config-subif)# ip add 40.0.0.1 255.0.0.0  
M(config-subif)#exit
```

DHCP Configuration Command on Router

```
Router(config)#ip dhcp pool engg  
Router(dhcp-config)#network 10.0.0.0 255.0.0.0  
Router(dhcp-config)#default-router 10.0.0.1  
Router(dhcp-config)#exit  
Router(config)#ip dhcp pool MBA  
Router(dhcp-config)#net  
Router(dhcp-config)#network 20.0.0.0 255.0.0.0  
Router(dhcp-config)#def  
Router(dhcp-config)#default-router 20.0.0.1  
Router(dhcp-config)#exit  
Router(config)#
```

Note: The same command syntax will be used for the other LANS to get DHCP IP from Router.

SWITCH 0: Commands and Configuration

```
Switch>en  
Switch#conf t  
Switch(config)#enable password engg  
Switch(config)#enable secret engg  
Switch(config)#line console 0  
Switch(config)#exec-time out 30  
Switch(config)#logging synchronous  
Switch(config)#line vty 0 15  
Switch(config)#exit  
Switch #conf t  
Switch(config)#ip default-gateway 10.0.0.100  
Switch(config)# exit  
Switch(config)#vlan 10  
Switch(config-vlan)#name engg  
Switch(config)#interface range fastEthernet 0/1-6  
Switch(config-if-range)#swit  
Switch(config-if-range)#switchport mode access  
Switch(config-if-range)#switchport access vlan 10  
Switch#sh vlan brief
```

Note: The same command and configuration will be done on the other LAN Switches.

SWITCH 4: Commands and Configuration

```
Switch>en
Switch#conf t
Switch(config)#line console 0
Switch(config)#exec-time out 30
Switch(config)#logging synchronous
Switch(config)#line vty 0 15
Switch(config)#exit
Switch(config)#vlan 10
Switch(config-vlan)#name engg
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
```

Note: The same command will be used for other LAN Network on the switch

```
Switch(config)#conf t
Switch(config)#int
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/20
Switch(config-if)#switchport mode trunk
Switch(config-if)#
Switch#show interfaces trunk
```

7. Objectives

The main objective of the project is to connect all the departments of a campus/organization in which all the departments have their own personal inter-network and one main network is made to connect all the networks to each other. All the departments are interdependent. Thus we want to build a network in which we want to implement user mobility in the network, reducing complexity, and providing security. By creating a VLAN in pure switched inter-network we will be able to provide flexibility for the user to login to any network. And at the same time, the network should be cost-effective also. To sum-up, the objectives are:-To save money, To provide Security, To increase performance, To reduce the size of the broadcast domain, To provide flexibility, To provide mobility, For easy troubleshooting can be implemented easily and can be extended as per the requirements.

8. Conclusion and Future Scopes

Though there are many problems facing network and data communication today where security has always been the most paramount challenge. Every effort is always on how to mitigate insecurity issues and ensure that

information is communicated to appropriate destinations without compromise. This paper had adequately discussed the need of implementing Virtual Local Area Network (VLAN) and Inter-VLAN Routing technologies in college campuses or organization Networks. Going by the usual flat Local Area Network infrastructure where every user belongs to one broadcast domain different series of network insecurities exist. In the case of an enterprise network having critical file servers, application servers, organizational databases, and other confidential information, this would mean that all users would have equal access privileges to these resources. To effectively prevent such situations from the operational networks we need to restrict access at the network level by segmenting the existing network into different broadcast domains, hence, the need for Virtual Local Area Network (VLAN). In contrast to normally flat LAN architecture where every host is connected without segmentation; we break a large broadcast domain into different sizes of broadcast domains by creating Virtual Local Area Networks (VLANs). This VLAN architecture which is a logical grouping of network users and resources connected to administratively defined ports on a switch when deployed in Campus Network would be of immense benefit as outlined in the work. In all, this work exhaustively x-rayed the benefits of VLAN and Inter-VLAN routing in managing and maintaining of any organizational Networks. This can be implemented in any small offices, colleges, hospitals, etc. as per requirements.

References

- [1] Routing and Switching (CCNA R& S), 2013 cisco systems Mega Guide, CCNA 640-802, www.preplogic.com
- [2] Virtual Local Area Network (LAN) communications. (1996). [online]. Available: <http://cio.cisco.com/warp/public/614/13.html>. (October twenty-two, 1998)
- [3] M. Yu, J. Rexford, X. Sun, S. Rao, and N. Feamster, "A survey of VLAN usage in campus networks," *Communications IEEE Magazine*, vol. 49, pp. 98-103, 2011
- [4] Henry, P. D., and De Libero, G. (1996) *Strategic networking: From local area network and WAN to info superhighways*. London: International Thomson Computer Press.
- [5] CompTIA. (n.d.). Retrieved from <https://www.comptia.org>
- [6] Institute of Electrical and Electronics Engineers (1998). IEEE P8021.Q, IEEE standards for local and metropolitan area (MAN) networks: Virtual bridged networks.
- [7] Virtual local area network (VLAN) communications. (1996). [online]. Available: <http://cio.cisco.com/warp/public/614/13.html>. (October twenty-two, 1998)
- [8] M. Zhu, M. Molle, and B. Brahmam, "Design and implementation of application-based secure VLAN," in 37th Annual IEEE Conf. on local computer Networks, 2004, pp. 407-408.
- [9] VLAN info. UC Davis Network twenty-one. (1998). [online]. Available: <http://net21.ucdavis.edu/newvlan.htm>. (October twenty-one, 1998)
- [10] Baker, R. H. (1995). *Network security: how to set up for it and achieve it*. New York: McGraw Hill, Inc.

- [11] Passmore, D. and freeman, J. (1998). The virtual local area network technology report. [online]. Available: <http://www.3com.com/nsc/200374.html>. (October 2, 1998)
- [12] SecureFast services summary. (1998). Cabletron Systems product marketing white papers. Rochester, NH: Cabletron Systems, Inc.
- [13] Roese, J. (1998) Switched LANs: Implementation, operation, maintenance. New York: McGraw-Hill, Inc.