11th International Conference on Recent Development in Engineering Science, Humanities and Management
Nutan Maharashtra Institute of Engineering & Technology, Talegaon Dabhade, Pune ESHM-18
24th-25th March 2018 www.conferenceworld.in ISBN : 978-93-87793-14-9

Implementation of VLAN Switching and VLAN Networks for Cyber Petronet

CHEW YI SIANG

BSc(Hons) in Cyber Security, Asia Pacific University, Kuala Lumpur, Malaysia

ABSTRACT

WAN technology provides exchanging data with a wide geographical area compared to LAN. This is why WAN technology is used by a lot of companies that needs to connect building to other building in different locations. In the nutshell, here the author has created a network topology that archived the Cyber Petronet Limited Company requirement by using VLAN to separate LAN according department, Inter-VLAN routing to let VLAN communicate with each other, access control list to limit the access to server and WAN technology to connect existing building.Security is one of the reason makes VLAN more important. Within the layer 2 switched internetwork that is single broadcast domain, which mean all users can see all devices. VLAN use to split broadcast domains decreasing the overhead on a network segment and enhance network security by put a group of user into a VLAN, so that no users outside of the VLAN can communicate with them. In this situation, VLAN also allow users access to network services based on department, not limited to location of the physical switches.

Keywords:Communication, LAN, Routing, VLAN, WAN

I.INTRODUCTION

In the modern age of advanced technology, major company transforms from paper files to digital because not only encourage concept of paperless, also give people a lot of convenience. For example, save a lot of time when searching some files, easy to modify the files, etc. Since information become digital, we protect the information or data by configure the routers and switches. However, the router and switch are expensive, so we create a virtual local area network (VLAN), to maximize the usage of switch. Concept is like, a VLAN is combination of all of the usable port, and restructure according to configuration, and it shows that VLAN are flexibility and scalability. VLAN can be create that reduce the number of router hops and enhance the performance by increase the apparent bandwidth for network users. In addition, access control list (ACL) can be add into VLAN interface. We can create interface in VLAN, and apply the ACL to it. This not only enhance the security of network, also get control of the packet traffic between VLAN [1].

As the topology below “Fig.1” is the design of a network that can avoid bandwidth consumption by using VLAN. Below is the “Table.1” shown VLAN, department and color.

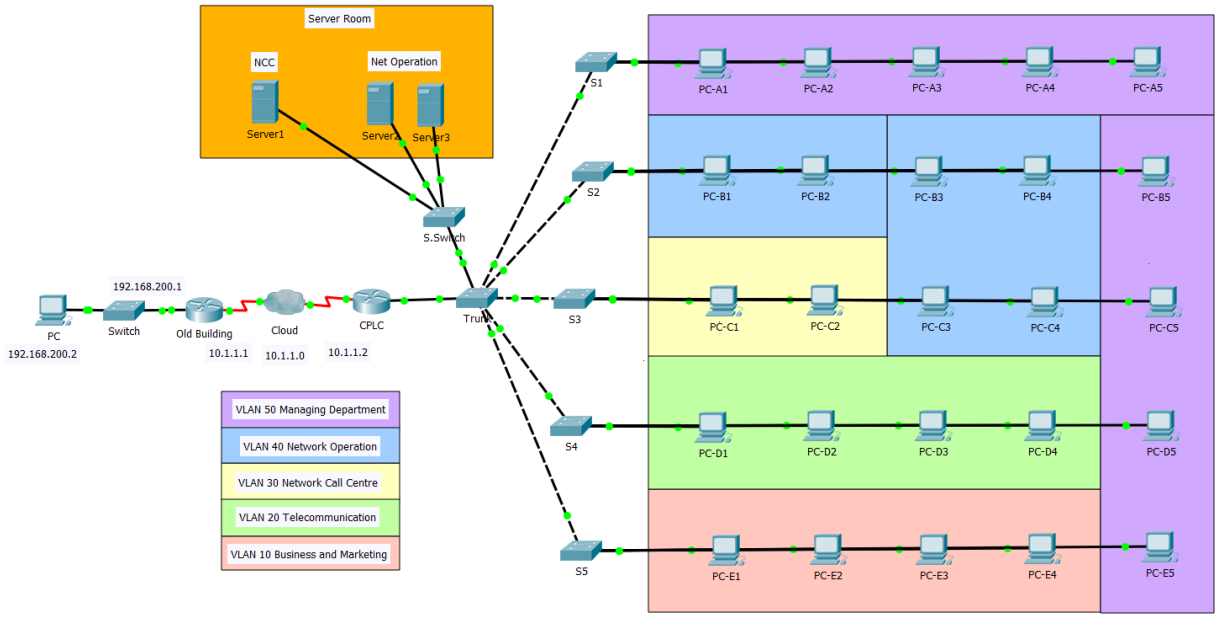

Figure.1 Network Topology

VLAN	**Department**	**Color**
VLAN 10	Business and Marketing	Red
VLAN 20	Telecommunication	Green
VLAN 30	Network Call Centre	Yellow
VLAN 40	Network Operation	Blue
VLAN 50	Managing Department	Purple

Table.1 VLAN department and color

As Cyber Petronet Limited Company required, I design a server room which having few server, and one of those is can only be access by employees in NCC. Others are manage by Network Operation. In addition, that is a WAN connection between the new building and existing building in Cyberjaya. There are two type of VLAN membership, which is static VLANs and Dynamic VLANs [2]. Static VLANs is assigns each port in the switch to each VLANs

and dynamic VLANs is configure the switches to assign VLANs dynamically whenever a host is plugging into the switch.

II.STATIC VLANS

The switch port that administer assign to a VLAN association to always maintain that association until an administrator manually changes that port assignment. This type of VLANs membership is more secure, because only the IP address you assigns in the port of switch can access the network.

III.DYNAMIC VLANS

A dynamic VLAN can determines VLAN assignment automatically according on hardware MAC address, protocols by using intelligent management software. For example, a hardware's MAC address had been enter in to a centralized VLAN management software. When the hardware connect to an unassigned switch port, the VLAN management software can look up the MAC address and auto assign to specific VLAN. It is very convenience, but that is a lot of work initially setting up the database. As the plan I designed, I choose the static VLANs, because it is more secure compare to the dynamic VLAN. It only can be manually change by administrator. Besides, it is easy to set up and easy to monitor the configuration compare to dynamic. Dynamic VLAN require more workers and cost compare to static VLAN. The tables shown in the following "Table.3.1" addressing table, "Table.4" switch port assignment statement.

3.1 ADDRESSING TABLE

Device	Interface	IP Address	Subnet Mask	Default Gateway
CPLC Router	G0/0.10	192.168.10.1	255.255.255.0	N/A
	G0/0.20	192.168.20.1	255.255.255.0	N/A
	G0/0.30	192.168.30.1	255.255.255.0	N/A
	G0/0.40	192.168.40.1	255.255.255.0	N/A
	G0/0.50	192.168.50.1	255.255.255.0	N/A
	Lo0	209.165.200.255	255.255.255.224	N/A
PC-A1	NIC	192.168.50.2	255.255.255.0	192.168.50.1

PC-A2	NIC	192.168.50.3	255.255.255.0	192.168.50.1
PC-A3	NIC	192.168.50.4	255.255.255.0	192.168.50.1
PC-A4	NIC	192.168.50.5	255.255.255.0	192.168.50.1
PC-A5	NIC	192.168.50.6	255.255.255.0	192.168.50.1
PC-B1	NIC	192.168.40.2	255.255.255.0	192.168.40.1
PC-B2	NIC	192.168.40.3	255.255.255.0	192.168.40.1
PC-B3	NIC	192.168.40.4	255.255.255.0	192.168.40.1
PC-B4	NIC	192.168.40.5	255.255.255.0	192.168.40.1
PC-B5	NIC	192.168.50.7	255.255.255.0	192.168.50.1
PC-C1	NIC	192.168.30.2	255.255.255.0	192.168.30.1
PC-C2	NIC	192.168.30.3	255.255.255.0	192.168.30.1
PC-C3	NIC	192.168.40.6	255.255.255.0	192.168.40.1
PC-C4	NIC	192.168.40.7	255.255.255.0	192.168.40.1
PC-C5	NIC	192.168.50.8	255.255.255.0	192.168.50.1
PC-D1	NIC	192.168.20.2	255.255.255.0	192.168.20.1
PC-D2	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC-D3	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC-D4	NIC	192.168.20.5	255.255.255.0	192.168.20.1
PC-D5	NIC	192.168.50.9	255.255.255.0	192.168.50.1
PC-E1	NIC	192.168.10.2	255.255.255.0	192.168.10.1

PC-E2	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-E3	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-E4	NIC	192.168.10.5	255.255.255.0	192.168.10.1
PC-E5	NIC	192.168.50.10	255.255.255.0	192.168.50.1
Server1	NIC	192.168.30.100	255.255.255.0	192.168.30.1
Server2	NIC	192.168.40.100	255.255.255.0	192.168.40.1
Server3	NIC	192.168.40.101	255.255.255.0	192.168.40.1

IV. SWITCH PORT ASSIGNMENT SPECIFICATIONS

Device	**Ports**	**Assignment**	**Network**
Trunk	F0/1-6	802.1Q Trunk	N/A
S1	F0/1	802.1Q Trunk	N/A
	F0/2-6	VLAN 50 – Managing Department	192.168.50.0/24
S2	F0/1	802.1Q Trunk	N/A
	F0/2-5	VLAN 40 – Network Operations	192.168.40.0/24
	F0/6	VLAN 50 – Managing Department	192.168.50.0/24
S3	F0/1	802.1Q Trunk	N/A
	F0/2-3	VLAN 30 – Network Call Centre	192.168.30.0/24
	F0/4-5	VLAN 40 – Network Operations	192.168.40.0/24
	F0/6	VLAN 50 – Managing Department	192.168.50.0/24

S4	F0/1	802.1Q Trunk	N/A
	F0/2-5	VLAN 20 – Telecommunication	192.168.20.0/24
	F0/6	VLAN 50 – Managing Department	192.168.50.0/24
S5	F0/1	802.1Q Trunk	N/A
	F0/2-5	VLAN 10 – Business & Marketing	192.168.10.0/24
	F0/6	VLAN 50 – Managing Department	192.168.50.0/24
Server Switch	F0/1	802.1Q Trunk	N/A
	F0/2	VLAN 30 – Network Call Centre	192.168.30.0/24
	F0/3-4	VLAN 40 – Network Operation	192.168.40.0/24

V.COMMON ISSUES IN VLAN

5.1 IP ADDRESSING

Different IP networks communicate through a router; therefore, devices within a VLAN must have the same IP network to communicate.

5.2 TRUNKS

5.2.1 NATIVE VLAN MISMATCHES

If the trunk ports are configure with different native VLAN, it generates console notification, causes control and management traffic to be misdirected. This will result poses a security risk and creates unintended results [3].

5.2.2 TRUNK MODE MISMATCHES

If any trunk port configured with trunk mode off and the other with trunk mode on, will causes loss of network connectivity.

5.2.3 ALLOWED VLANS ON TRUNK

If the list of allowed VLANs on a trunk has not been update with the current VLAN trunking requirements, unexpected traffic or no traffic is being send over the trunk.

VI. IMPORTANCE OF SPANNING TREE ALGORITHM (STA)

In a local area network (LAN), the heavy load of network bandwidth will cause the network slow down. Spanning Tree Protocol (STP) meant to reduce the possibility of this problem. The STP will change its algorithm to fit the situation that delay the network and maintain the quality of the network.Besides, STP avoids the bridging logic problem when many computers are using same LAN. Algorithms of STP will establishing a root bridge that can see all traffic and ensures efficient data forwarding when each device uses different paths to confusing the logic of the network. STP algorithm will stop network loops by monitor the network to find all links and shutting down any redundant links [4]. The STP algorithm limits the number of open paths and monitor in a way where data sent from one device to another. This helps devices communicate with each other freely. STP always have a backup, it will active when connection lost.

VII.VLAN MANAGEMENT

Network management in large-scale can be critical problem if you do not manage properly. Network operation manager and engineer have to cover the IT services that include monitoring, securing, expanding and optimising networking environment. They need to make sure the networking is going smooth and efficiently with no complain from the customer. As networks grow, they become busier and more task to do.According with business expansion and requirements, network manager need to constantly updated network metrics from historic analysis to provide report and analytics [6]. Network management makes network manager easier to work with all the information. That is why the network management tools shows up.There are many networks management tools nowadays. One of all is Network Performance Monitor, developed by Solarwinds Software Company [7]. It is easy to setup because it will automatically discovers networks devices and deploys no more than one hour. Besides, the interface can be customize by user, so it is easy to manage and arrange the dashboard, charts and views. Except of automatically network discovery, it have many extensive feature. For example, multi-vendor network monitoring, performance analysis dashboard, intelligent alerts, network insight for cisco ASA and F5 BIG-IP, wireless heat maps etc. Furthermore, ConnnectWise Automate is a cloud-based manager [8]. It can track of your IT infrastructure devices from a single location. This tools also provides a feature called “Patch Management”, it allow you to protect all your system with simultaneous patching from a centralized manager by using Windows Patch management or third-party software.

VIII. WAN SWITCHING TECHNOLOGY

There are three types of WAN switching technology.

8.1 LEASED LINES

Typically, there are refer to as a point-to-point connection. It is very simplicity and quality. HDLC and PPP encapsulations are frequently use on lease lines.

8.2 CIRCUIT SWITCHING

Circuit switching is like a phone call, meant only pay while you actually use. It is low cost compare to leased line. The two most common types of circuit switching technology are public switched telephone network (PSTN) and integrated services digital network (ISDN) [5].

8.3 PACKET SWITCHING

Packet switching allows you to share bandwidth with other companies to save cost. It splits traffic data into packets that routed over a shared network. It also allow many pairs of nodes to communicate over the same channel.Frame Relay has become one of the most popular WAN services because it frequently saves money over alternatives. It is more complex than simple leased-line network, which is HDLC and PPP protocols. Frame relay will in many cases cheaper than a leased line. The basic idea behind Frame Relay networks is to allow users to communicate between two DTE devices through DCE devices. Frame relay works by providing a portion of dedicated bandwidth to each user, and also allowing the user exceed when resources on the telco network are available. I decide to use this method in my design is because it is layer 2 and layer 1 specification that provides high performance. Moreover, it save a lot of money instead of using leased line.

IX. CONCLUSION

VLAN provides easier administration, a better confinement in broadcast domains. With the presence of VLAN, it will reduce the broadcast traffic, and security policies. Besides, VLAN enable end-stations that are physically dispersed on a network groups logically, with that saying, when users move to a new physical location to perform same function, the end stations need no reconfiguration.VLAN also reduce the utilization of routers on a network during broadcast. It will limit the packet of switch ports that belongs to VLAN when it comes to flooding packet.Inter-VLAN is much more cost effective than VLAN, as it does not require expensive switches to implement the communications between VLAN. It is also very simple to implement the communications between VLANs. This is because switches do not have to support layer 3, VLANs and trunking will do the job.Access control list works as a pass for selective services to access the destination, some particular system object, such as a directory or an individual file whom had the whitelist in the access control list gains the access to the end file. Each object has their own security attributes that identifies them from the access control list. WAN technology provides exchanging data with a wide geographical area compared to LAN. This is why WAN technology is used by a lot of companies that needs to connect building to other building in different locations.In the nutshell, I had created a network topology that archived the Cyber Petronet Limited Company requirement by using VLAN to separate LAN according department, Inter-VLAN routing to let VLAN communicate with each other, access control list to limit the access to server and WAN technology to connect existing building.

X.ACKNOWLEDGMENT

Author would like to thank Mr Umapathy Eaganathan, Lecturer in Computing, Asia Pacific University for his constant support and encouragement also thank to Miss Angel Rubavathy for her help to participate in this international conference with journal publication.

REFERENCES

[1] Mather, M., 2017. *TechTarget.* [Online]
Available at: http://itknowledgeexchange.techtarget.com/itanswers/benefits-of-vlans/
[Accessed 1 December 2017].

[2] Popeskic, V., n.d. *How does Internet Network.* [Online]
Available at: https://howdoesinternetwork.com/2012/static-vs-dynamic-vlans

[3] Lammle, T., 2005. *CCNA: Cisco Certified Network Associate Stude Guide.* Fourth Edition ed. Alameda: Neil Edde.

[4] Spector, H., n.d. *Techwalla.* [Online]
Available at: https://www.techwalla.com/articles/the-advantages-of-spanning-tree-protocol

[5] Toit, J. d., 2014. *Iris Network System.* [Online]
Available at: https://www.irisns.com/importance-integrated-network-management-system/

[6] Venezia, P., 2017. *Network World.* [Online]
Available at: https://www.networkworld.com/article/2825879/network-management/7-free-open-source-network-monitoring-tools.html

[7] Anon., n.d. *ConnectWise.* [Online]
Available at: https://www.connectwise.com/software/automate

[8] Anon., n.d. *Solarwinds.* [Online]
Available at: https://www.solarwinds.com/network-performance-monitor