Aditya Arunkumar Vishwakarma. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 11, Issue 3, (Series-II) March 2021, pp. 01-05

RESEARCH ARTICLE OPEN ACCESS

Network Architecture Made Easy

Aditya Arunkumar Vishwakarma
D. G. Ruparel College of Science, Matunga West, Mumbai 400 016

ABSTRACT
In today's world, all our devices be it mobile phones, laptops, PCs, tablets, etc are connected over wireless networks what we call WiFi or LAN. These networks will be driving the future of every field related to computers like cloud computing, virtual storages online websites, services, advertisements and what not. Hence learning how these networks are created is very necessary to be ready for changes in the future for network architects.
Keywords **-** Cloud computing, LAN, network architects, virtual storages, wireless networks, WiFi

---

Date of Submission: 10-03-2021 Date of Acceptance: 25-03-2021

I. INTRODUCTION

Each network architecture begins with some or the other diagram and after knowing the requirements of the organization. We will start by learning requirements of the organization by preparing a questionnaire. According to the answers given by the team of keypersons, it would be much easier to select devices. For the network diagram/blueprint, we will start in virtual network development applications like Cisco Packet Tracer, Wireshark, etc.
For this project we will select Cisco Packet Tracer v7.2

In this network diagram, we will create a new virtual office and connect it via WAN to the Primary Datacenter and will also add Corporate Office.

II. THREE PHASES OF NETWORK ARCHITECTURE:

- Creating a questionnaire for the organization for learning all the core requirements and devices required.
- Creating the network architecture in simulator.
- Deployment of devices and configurations in real world.

2.1 Questionnaire

A questionnaire is a very useful instrument to gather information/collect data from respondents. In our case, we will create a questionnaire for our organization to estimate the devices performance, HA, etc. We will create the questionnaire and collect information from the keypersons of the organisation. Our questionnaire will contain some crucial points for this project such as:

a. Which company devices should we use to cater the required network?
b. Can we see the network infrastructure of other offices so that we can create in-line with?
c. What kind of deployment is required: Traditional type (Branch, campus) or SDA (virtual networks)?
d. What is the scale/number of employees?
e. Do we need wired or wireless connection? And if wireless, do we require guest network and employee network (ACL) separately?

These are some basic questions. Now, we will see some questions based on security point of view:

a. Do we want to establish ACL – (to restrict access for employees) or security?
b. Is a AAA server/ Authentication server or ISE required?
c. Where are shared services hosted?

Next, we will see the questions based on departments and employees:

a. How many departments do you need?
b. Do we want to create VLAN, ACL/ISE for all these departments?
c. Where are the DNS and DHCP, IPS hosted?
d. How many people are there in one department approximately?

Our next step is to specify the required devices in simulator for this project which may be as follows.

- Routers- ASR1k, Cisco 3600ME
- Switches- C9500, C-9600, C-9400/C-9300 with SVL/stack
- Wireless Access Points- Cisco WAP-121
- Firewall- ASA 5500-X Series
- Wireless controllers- 9800-1 HA

However we use the actual firewall which is installed in old office along with some new devices.

- Core Switch (L3):- Cisco -9300 (new device)
- Access Switch (L2) Cisco-9200 (new device)
- Wireless Controller :- Cisco-3504 (new device)
- Access Point:- Cisco-2800 (new device)
- Firewall - Fortigate FG-201E. (existing device – firewall)

2.2 Main Site network design diagram

- Now we can create the network diagram with cisco packet tracer. For this, we need the image files of all these devices. If the image files are not available, we can use these device's low end counterparts for trial and testing of the architecture.
- As per basic diagrams, we have to set up the architecture in 3 layers as shown in 'Fig 1' namely – core, distribution and access layers.

- Firewall on top
- VLAN (Core Switch) & Wi-Fi Controller
- Next LAN (Access Switch) & Access Point
- Next User Desktop

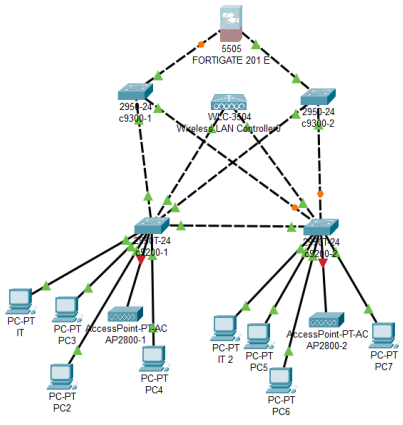

Fig 1- simulator diagram

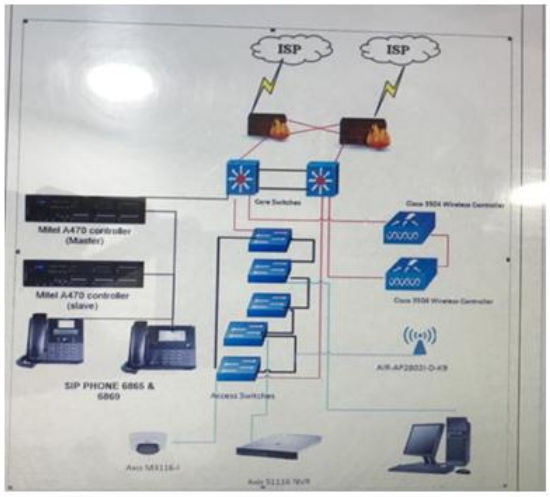

Fig 2 – actual diagram

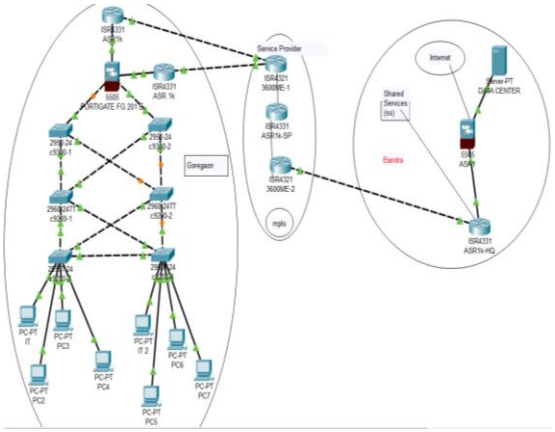

Fig 3- main site and branches interconnected design diagram

Main site to Headquarters – Point to Point Leased Line connection made of fibre optics (Always ON, secure, dedicated connection required). As shown in 'Fig 3'.

2.3 Deployment in Real World

Configurations Considerations of this network

Stacking

Now, when we setup the network rack, we have 5 c9200 distribution layer switches. For future expansion, the organization wants the switches to be stacked. For stacking, we will connect the stacking port of first switch to the stacking port of the second one. Similarly, 2nd to 3rd, 3rd to 4th, and 4th to 5th. Lastly, we will connect the second stacking port of the first switch to the first stacking port of the last switch. Thus completing physical stacking.

Some monitoring commands for the newly stacked devices are given below:

Command	Description
show module	Displays summary information about the stack.
show switch detail	Displays detailed information about the stack.
show switch neighbors	Displays the stack neighbors.
show switch stack-ports [**summary**]	Displays port information for the stack. Use the **summary** keyword to display the stack cable length, the stack link status, and the loopback status.
show redundancy	Displays the redundant system and the current processor information. The redundant system information includes the system uptime, standby failures, switchover reason, hardware, configured and operating redundancy mode. The current processor information displayed includes the active location, the software state, and the uptime in the current state and so on.
show redundancy state	Displays all the redundancy states of the active and standby devices.

Cabling:
It will be always efficient to follow the **structured cabling** approach in designing a network. Structured cabling is made up of number of standardized elements called subsystems. The subsystems are **entrance facility** where ISP network ends and connects to customer devices, **equipment room** where several equipment and other parts of network that serve the clients inside the building, **horizontal cabling** which interconnects the components inside the same floor, **work area** where the end user equipment connect together with horizontal cabling and **telecommunication enclosure** which interconnects horizontal cabling and backbone cabling together.

So, in this network design also structured cabling approach is followed. **Work area subsystem** is comprised of several end user workstations which are connected to the wall socket through RJ45 cables (Fig 4 & Fig 5). Work area also includes wireless station communicating with the nearest access point (AP).

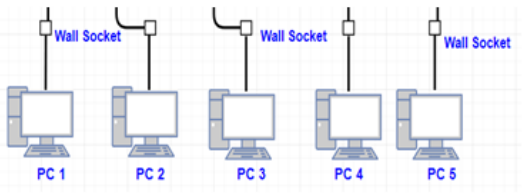

Fig 4 – A.P. (Access Points)

Fig 5 – AP to LAN to End devices

VLAN Description
Work area consists of wireless laptops and PDAs connected to AP

Web server is accessed by public and insiders of the network. Heavy data transfer is taking place between the main site and branch office at all time.

VLANs are created across the floor for wireless networks and Lan Connectivity. This is to remove the uncontrolled broadcast traffic reaching another network. VLAN

Also provides a layer of network security and cost reduction option by logically separating hosts which is connected to the same switch (no need for additional switches)

IP Address scheme used in this network design

VLAN	Network Address	Sub Netmask
VLAN 101	192.168.11.192 /24	255.255.255.0
VLAN 102	10.22.240.0 /24	255.255.255.0
VLAN 103	192.168.8.0 /24	255.255.255.0
VLAN 104	192.168.9.0 /24	255.255.255.0
VLAN 105	192.168.11.0 /26	255.255.255.192
VLAN 106	192.168.11.128 /27	255.255.255.224
VLAN 107	192.168.11.160 /27	255.255.255.224
VLAN 108	192.168.4.0 /24	255.255.255.0

Other VLAN addresses are assigned to the hosts through the DHCP server (by creating a pool of address for different VLAN)

Network Protocols used in this network design
Routing
Static Routing – Static routes are configured on gateway/core routers of each branch and in main site, to route the traffic from one network to another branch network. As we know the next hop (IP of each branch network), this can be used. Since this is a **small network, using static routes are simple and easy**. It's secure because no routing advertisements are exchanged between neighbours and computing resources are conserved because no routing algorithm or update mechanisms are required.
Default routing – This is configured on core routers to route the traffic from inside network to ISP router for unknown traffic (towards internet).
Inter VLAN routing – Core routers are configured to route the traffic between different VLAN in the network. The traffic will reach the core routers from core switch which are connected by trunk link. All VLAN networks will be shown as directly connected routes in routing table (sub interfaces are used).

DNS (Domain Name System)
DNS is configured in DNS server, which is in the server room at new site. All the hosts in this network are assumed to be connected to domain. So, each hosts (workstations) have their unique domain name. So, inside users can use the specific domain name to connect to each host remotely. But computers cannot understand the name. It should be converted to numbers called IP address. So, **DNS server maintains the map of domain name of each host to its corresponding IP address**. **Thus, management and complexity of network can be reduced**.

DHCP (Dynamic Host Configuration Protocol)
DHCP service is installed in the DHCP server which resides in server room. IP address pool for different VLAN will be created in DHCP server. So DHCP server dynamically assign the IP address to the hosts in the network. Static IP address that will be used with in the VLAN can be removed from the IP address pool (excluded address) in DHCP server. Main advantage of using this protocol is **reliable IP address configuration to hosts** (reduce configuration errors caused by manual IP assignment), and **reduced network administration** (centralized management).

STP (Spanning Tree Protocol)
The redundant link connection is provided between the switches in the office to the 2 core switches located in Main office. Also redundant link is added between 2 core routers and 2 core switches as well as between server room switch and 2 core switches. The purpose of having an extra link is that, if one link goes down, still the network components can communicate with each other using the redundant link. So, there will be **less down time in the network**. But there is a concern of adding an extra link between network switches that, it will create a broadcast storm (loop). To avoid this problem, STP protocol is used with in switches in this network. So, at a time one active link will be present and another link will be in blocked mode. Once the active link fails, the redundant link come into active mode from blocked mode.

NAT (Network Address Translation)
Class B private range IP address is used within this network. But the hosts cannot communicate with this private IP address over Internet because private IP address are not routable in Internet. Therefore, they must be converted to public IP address for the communication over Internet. So, NAT becomes an essential part of this network design. **PAT** (Port Address Translation) is used in the core router to map one/two public IP address provided by ISP to map the private IP address used inside the network. By using PAT, we can save the number of public IP addresses used for the translation. **Static NAT** will be used for communication of web server over the Internet as the web server should be visible and accessible from the Internet. By using NAT, **public IPv4 address can be saved and internal IP plan of this network can be hidden from the outside world**.

HSRP (Hot Standby Router Protocol)
HSRP is configured by combining the 2 core routers in this network. Therefore the 2 core routers will act as a single virtual router for the internal hosts. 1 core router will assume the responsibility as active router while other will take responsibility as standby router. If active router fails, the standby router assumes the role of the active router. Since the new forwarding router uses the same MAC and IP addresses, the **hosts can communicate without any disruption even when 1 core router fails**.

VLAN (Virtual Local Area Network)
There are 7 different VLANs created across this network. This is to **remove the uncontrolled broadcast traffic reaching another network**. VLAN also provides **a layer of network security and cost reduction option by logically separating**

hosts which is connected to the same switch (no need for additional switches). Here each VLAN is assigned with different IP address subnet. **VTP** (VLAN Trunking Protocol) is used here to manage VLANs and maintain consistency throughout the network. VTP can manage the addition, renaming, deletion of VLANs from a centralized point without manual intervention thus it reduces the overhead of network administration.

FTP (File Transfer Protocol)

FTP server is installed in the server room. This is used for the file transfer within the network. The files that needs to be shared, is uploaded to the FTP server. So, the clients can access the shared files using a specialized program called FTP client. The main reasons to use FTP server for file transfer within the network include **that data can be transferred in bulk efficiently, allows to transfer not only multiple files but multiple directories at one time, ability to resume a file transfer**.

ACL - Access control lists are used in firewall to filter traffic from outside, reaching the internal network. This provide security from intruders and to avoid suspicious traffic entering the network.

VPN - Virtual private network is used for the communication between main site and the mobile worker. VPN is using an encrypted tunnel for the data transfer over the existing Internet infrastructure. Thus, provide secure and cheap communication for data transfer**.**

Reference Diagram for Future Branch Networks

The Diagrams below 'Fig 6' and 'Fig 7' elaborate more about the deployment of the new branch and they give extra knowledge of the devices which can be used in a bigger architecture.

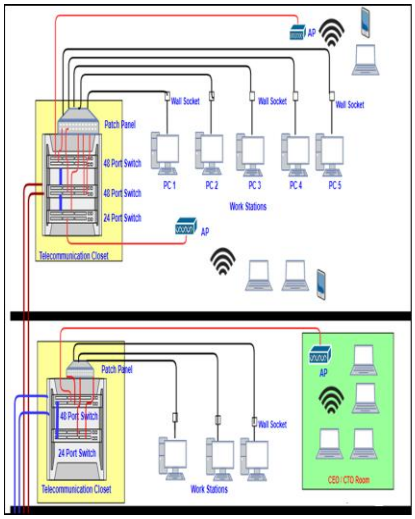

Fig 6– 24 and 48 port switch architectural design from server room to the whole floor

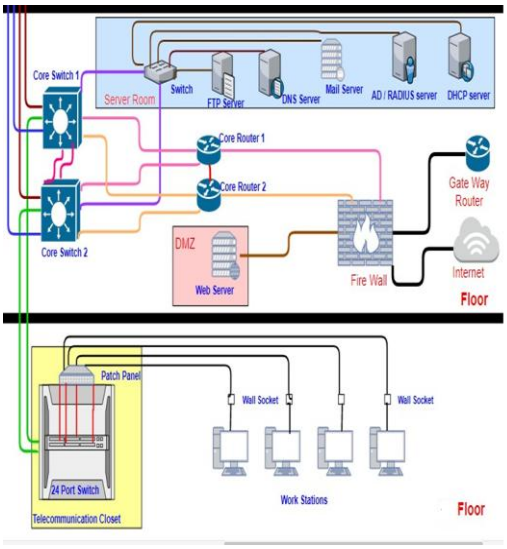

Fig 7- Branch communicating/ using information from servers in head office and other branches

III. CONCLUSION

This will help common people how they get WiFi connections, view websites and browse the internet just on their phones just by connecting it to a router. The science with which they get internet on their phones is necessary for them to learn. That said, this is a new kind of architecture which is used in offices and company headquarters (HQ)

REFERENCES

[1]. Wikipedia. "Structured cabling". Internet: https://en.wikipedia.org/wiki/Structured_cabling, December 18, 2020 [December 18, 2020].

[2]. Wikipedia. "Stackable switch". Internet: https://en.wikipedia.org/wiki/Stackable_switch, Feb.12, 2020.

[3]. Martin Horan. "How Does an FTP Server Work & The Benefits". Internet: https://blog.ftptoday.com/how-does-an-ftp-server-work-the-benefits, Sep.08, 2016 [December 18, 2020.]

[4]. Erwin Z. "Benefits of SMTP". Internet: http://benefitof.net/benefits-of-smtp/, May.09, 2012 [December 19, 2020.]