Network Design Report

Technical Report · December 2017

Janarthanan Kugathasan
Sri Lanka Institute of Information Technology

NETWORK

DESIGN

REPORT

Module – Distributed Networks (EC 340)
Lecturer In Charge – Mr. Amila Senarathne
Semester – 3rd Year 1st Semester

Submitted to
Sri Lanka Institute of Information Technology

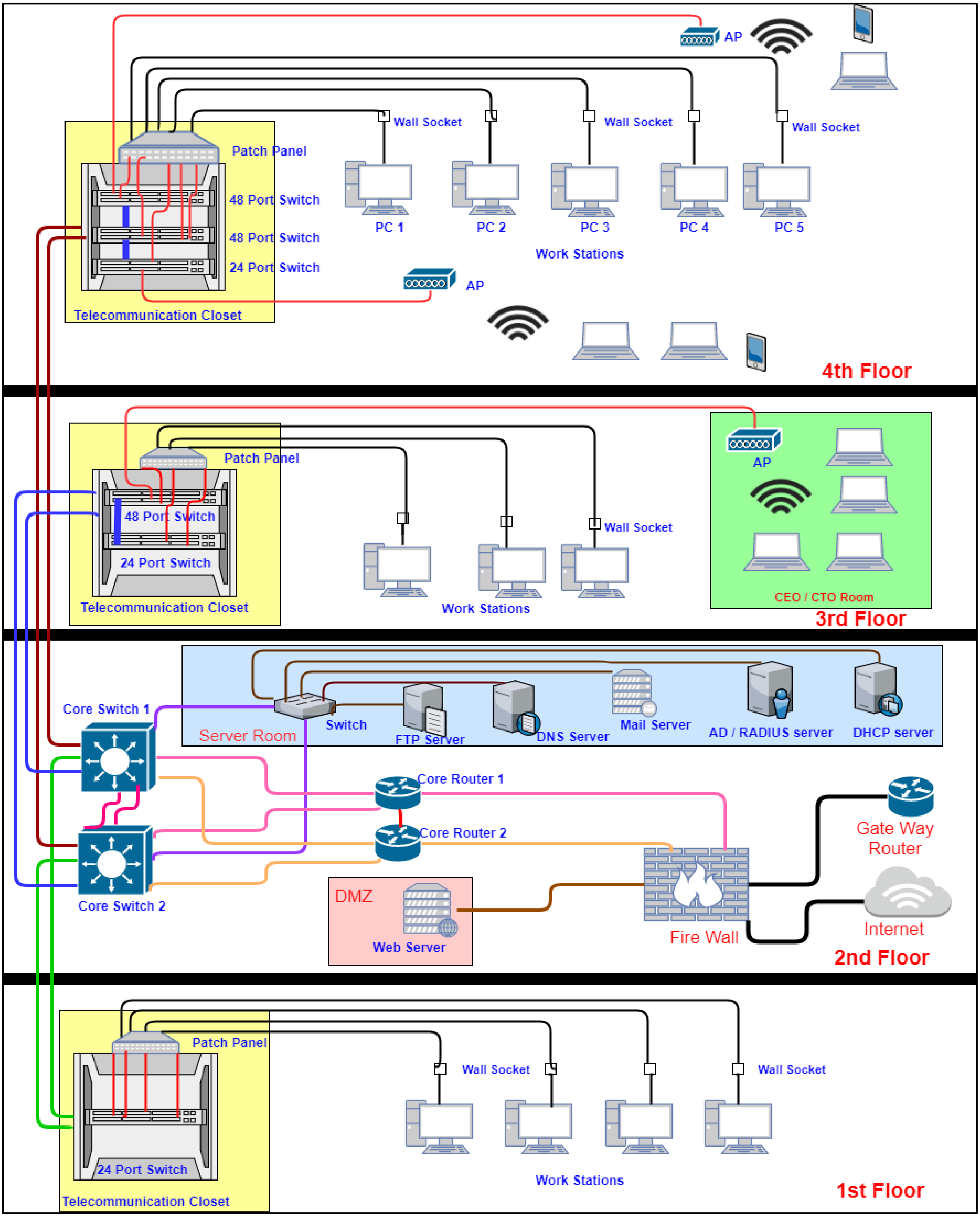
By – K. Janarthanan

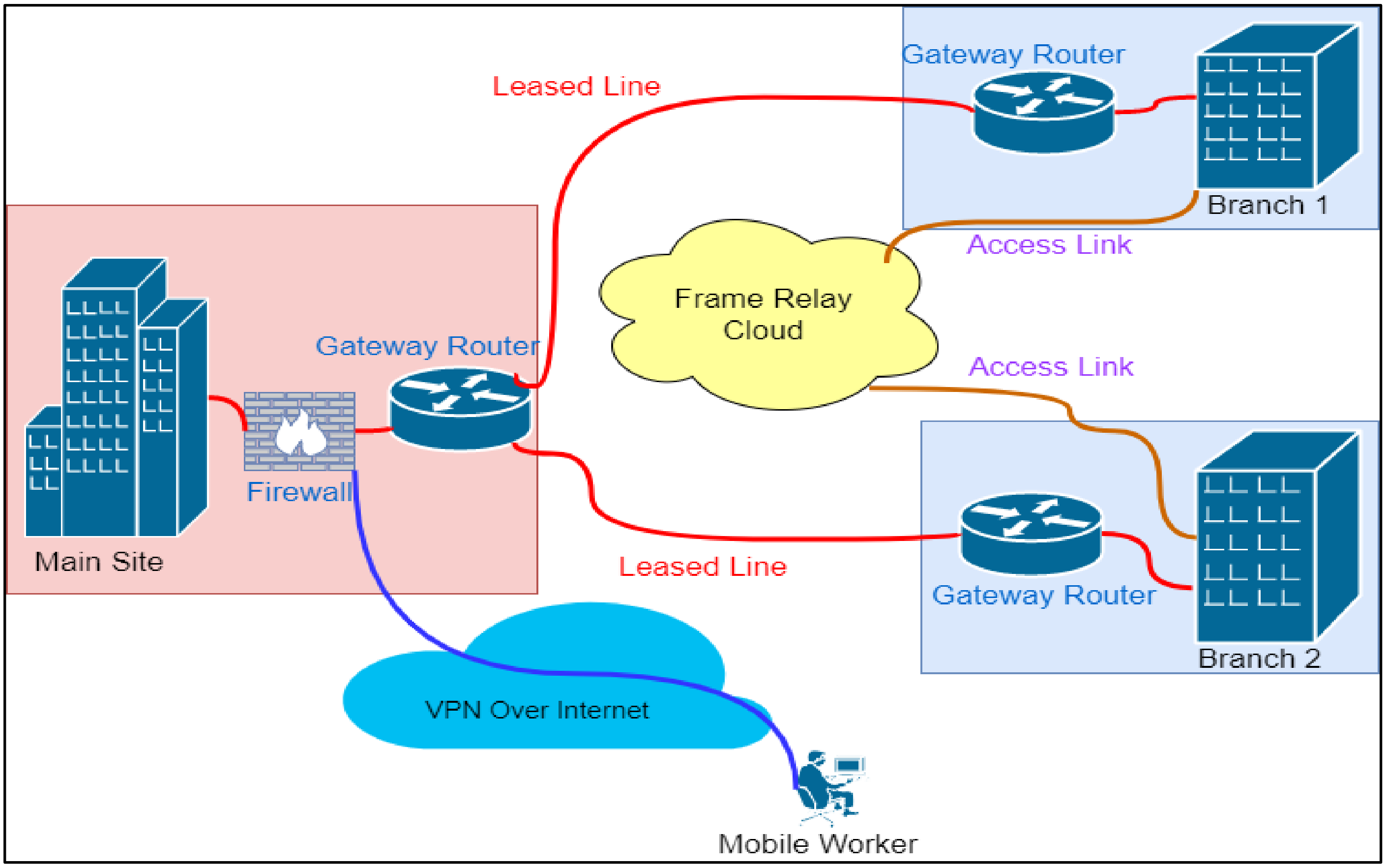
IT Number – IT15051608

Table of Contents

Network design scenario

- The Office consists of 4 floors with different requirements.
- The Top most floor will have to support 100 machines each for the company’s research wing. Furthermore, it will have to have the capacity of providing wireless communication for 50 mobile nodes at any given time.
- The third floor will have to provide wired communication for 60 machines as basic work place
- The CEO’s and CTO’s (Chief Technical officer) offices will also be situated on the Third floors and both require Secure Wireless Access. Therefore, building requires a secure wireless connection for the third floor.
- The Second floor will house the server room with an FTP, Mail and a Web Server together with a corporate Firewall system providing the edge for the internet and branch offices.
- The First floor area 01: will house for all customer handling nodes with 20 machines.


AP
Wall Socket
Wall Socket
Wall Socket
Patch Panel
48 Port Switch
48 Port Switch
24 Port Switch
PC 1
PC 2
PC 3
PC 4
PC 5
Work Stations
AP
Telecommunication Closet
4th Floor
Patch Panel
48 Port Switch
24 Port Switch
Telecommunication Closet
Wall Socket
Work Stations
AP
CEO / CTO Room
3rd Floor
Core Switch 1
Server Room
Switch
FTP Server
DNS Server
Mail Server
AD / RADIUS server
DHCP server
Core Router 1
Core Router 2
Gate Way
Router
Core Switch 2
DMZ
Web Server
Fire Wall
Internet
2nd Floor
Patch Panel
Wall Socket
Wall Socket
24 Port Switch
Telecommunication Closet
Work Stations
1st Floor



- ✓ Main site to Branch 1 and Branch 2 – Point to Point Leased Line Connection made of fiber optics (Always ON, secure, dedicated connection required)
- ✓ Branch 1 and Branch 2 – Frame Relay Connection (PVC point to point topology)
- ✓ Mobile worker can reach the Main site network using **VPN over Internet**

Assumptions made on connection between branches and main site

1. **Heavy data transfer** will take place between the main site and branch office at all time
2. **2 branch offices are located closely to the main head office**. Thus, it takes less cost for having a leased line connection from main site to branch sites
3. **Low data transfer is taking place between the 2 branch offices**, therefore they have a permanent virtual circuit (PVC) connection through frame relay.
4. A PVC with dedicated CIR (committed information rate) is created between 2 branch offices.
5. Leased line is preferred to connect main site and branch sites because of heavy data transfer between sites, short distance and only 2 interface will be used up in gateway router to connect the main site and its branches

Configurations Considerations of this network and Assumptions made

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, **backbone cabling** which interconnects different floors together with high speed cables, **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. Work area also includes wireless station communicating with the nearest access point (AP).

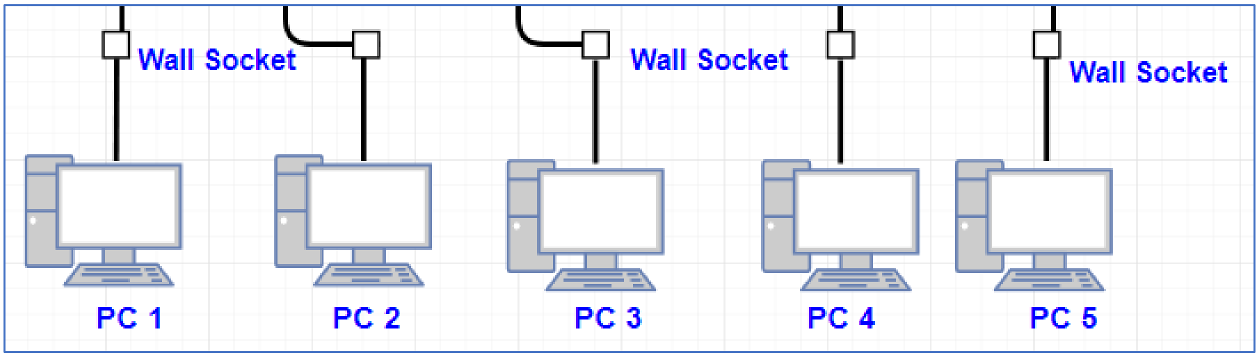


Figure 4.1 – Work Area consists of several PCs connected to wall jack

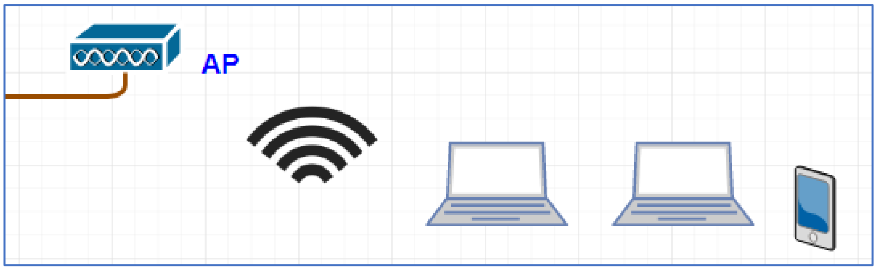


Figure 4.2 – Work Area consists of wireless laptops and PDAs connected to AP

Horizontal cabling in this network design is made up 100Mb/s Ethernet cables (Twisted Pair – CAT5) which joins the wall sockets (terminating point of wired work stations) and the back pane of patch panel.

Telecommunication enclosure subsystem in this network design consists of switch chassis and patch panels. Patch panel wires (Patch cords) are used to connect front end of patch panel and individual switch (switch ports) in the switch chassis. The **reasons to use patch panel** in this network design are,

- Identification – Ports in patch panel can be labeled, to uniquely identify which cable come from which location is getting terminated on which port of patch panel. So, it is easy in disconnecting/connecting and testing a cable
- Small changes in network cabling would not affect the switches in switch chassis. So, changes can be made quickly and easily.
- All the cables can be terminated on the patch panels (irrespective of whether they need to be connected to the switches or not) and they could be selectively connected to the switches by just moving the patch cables, whenever needed.

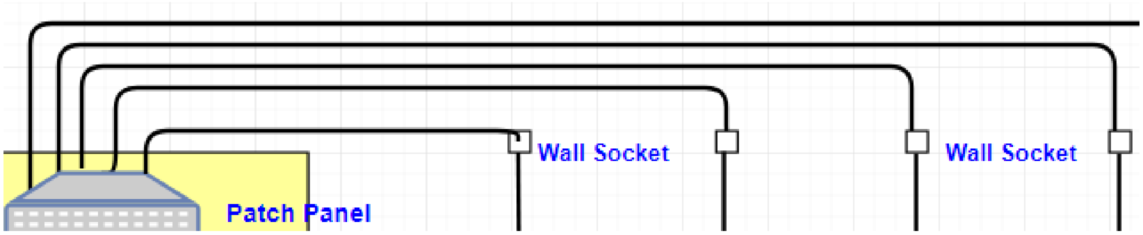


Figure 4.3 – Patch panel and its connection

Another import part of this subsystem is **Switch chassis**. Since around 100 wired end user connections are needed on **4th floor**, 3 switches (two 48 port switch and one 24 port switch) were used in this design. **Switches are stacked on top of each other**. Each **switch inside the stack are interconnected between them using 1Gbps Ethernet ports**. The main **advantages of using stackable switch model in this network design, include**

- Network maintenance becomes easy. In the stack, each switch acts as single unit, so there is a single management interface thus simplifies the operation and configuration of the network

- Scalability – The network can grow by additional switches over the time when needed, thus reducing management complexity.
- Even one unit (switch) fails, data will continue to flow through other units, thus provides resilient connections.
- Switches can function as stackable switches (operate together as single unit), or they can be configured to operate independently, thus provides deployment flexibility.

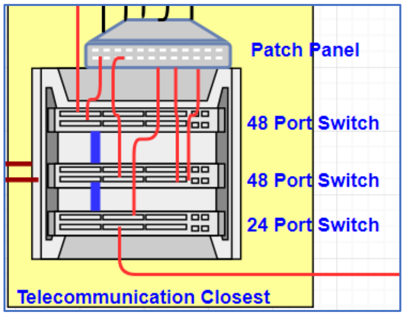


Figure 4.4 – Stackable switches placed in switch chassis inside the telecommunication closest

In **3rd floor** 2 switches (one 48 and one 24 port switches) are configured as stackable in switch chassis. In **1st floor** only one independent switch with 24 port is used.

The other main subsystem of this network design is **backbone cabling**. Backbone cabling is **made of fiber optics and interconnects the back pane of switch chassis and core switch** which reside in 2nd floor. There are **2 backbone links connecting switch chassis in each floor to 2 core switches** (core switch 1 and core switch 2). The reason to use 2 backbone link is to **provide redundant connection during failure**.

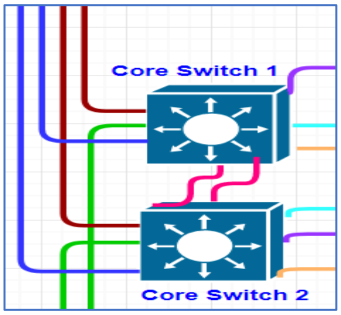


Figure 4.5 – Backbone cabling made of fiber optics terminating at core switches

The other main subsystem is the **equipment room**. The 2nd floor design is to be considered as the equipment room. The **2nd floor consists of 2 core switches, 2 core routers, firewall,**

gateway router, server room and a demilitarized zone (DMZ) which hosts web server for internal access as well as for outside access. The **reason to use 2 core switches is to provide redundancy, and to avoid single point of failure (SPOF)**. Fiber optic cables coming out from the switch chassis in each floor and the switch inside the server room is terminating in each of these core switch separately. These core switches are also interconnected between them. **Core router is used to route traffic with in inside the building (between VLANs) and to route traffic outside of the building (To Internet and other branch offices).** The reason to use **2 core routers is to provide redundancy and to avoid single point of failure**. 2 core routers also interconnected between them and connected to 2 core switches using high speed cables separately. **DMZ** (to separate it from the inside network) is created to host the web server, because it is **assumed to be accessed by insiders as well as outsiders**. So, if any intruders try to attack the web server, then damage to whole network (system) will be minimized. The web server in DMZ is directly connected to the firewall using a high speed cable. **Firewall is used to filter traffic that is coming toward the inside network**. **This is achieved using access control list (ACL) configured inside the firewall**. Firewall is connected to core routers and web server in inside direction and connected to gateway router and Internet in its outside directions. **Gateway router is used to forward/route the traffic to other directly connected branch offices** through the leased lines (Assuming branch offices are connected to the main site through the leased lines as they are situated close to each other and requires heavy data transfer to the main site).

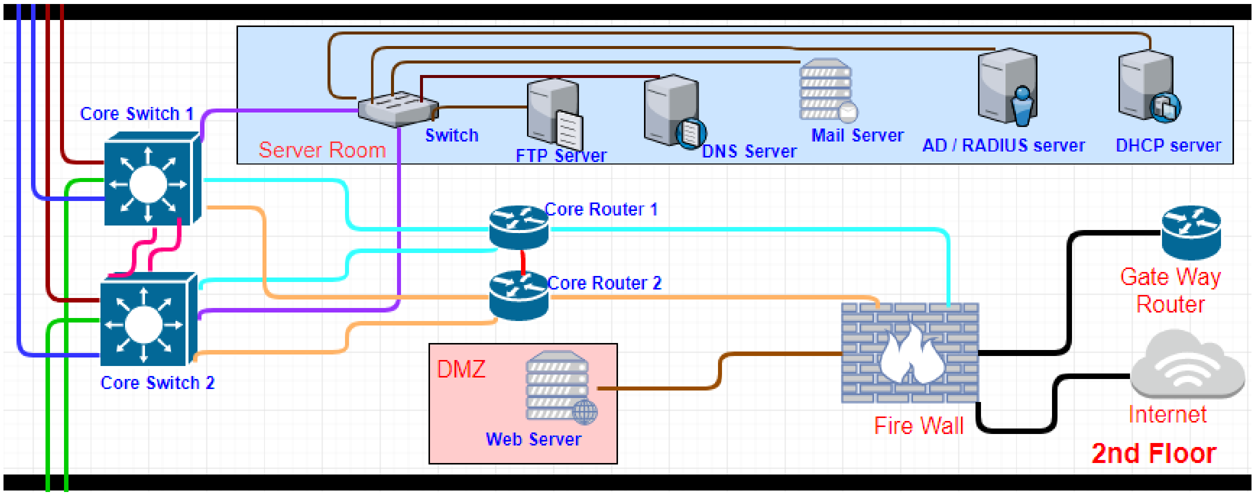


Figure – 4.6 Equipment room hosted inside the 2nd floor

The server room in 2nd floor consists of FTP server, Mail server, **AD /RADIUS (Active Directory / Remote Authentication Dial-In User Service) server which is used for authenticating users for different services that is provided across the network, DNS server for DNS-Lookup services (to translate domain name into IP address) and a DHCP server which dynamically assign IP address to hosts in different VLANs in the network** (thus reduces the difficulty in managing and configuring IP address). All the servers inside the server room and the web server in DMZ is configured with the static IP address. The reason to assign them with static IP address is to reduce the down time in IP renewal process, convenient remote access and stability for the applications running inside these servers. All these servers are connected to the central switch through 100Mbps speed cables and in turn this central switch is connected to the 2 core switches independently through 1Gbps speed cables.

The other subsystem, **entrance facility** is shown by the connection between the Internet cloud (where ISP equipment are also present) and the firewall which is situated at the 2nd floor of the building.

Assumptions made –

- Web server is accessed by public and insiders of the network
- CEO/CTO room have less than 15 people working inside it.
- 2 branch sites are located closely to the main head office. Thus, it takes less cost for having a leased line connection from main site to branch sites.
- Heavy data transfer is taking place between the main site and branch office at all time.
- Low data transfer is taking place between the 2 branch offices, therefore they have a permanent virtual circuit (PVC) connection through frame relay.
- Due to lack of space, only few machines were shown in the network diagram,
  In 1st floor, 1 PC = 5 PCs
  In 3rd floor, 1 PC = 20 PCs
  In 4th floor, 1 PC = 20 PCs

How Secure wireless access is ensured for CEO/CTO offices in 3rd floor?

The secure wireless access for the 3rd floor CEO/CTO office is provided by **creating a separate VLAN for the wireless communication and using WPA-2 Enterprise protocol**. A VLAN helps to logically group the workstations that are connected to the access point (AP) in the 3rd floor. By this unnecessary broadcast traffic, will not reach the 3rd floor wireless network.

WPA-2 Enterprise protocol provides the additional security needed for this wireless network. It helps to centralize the control over this wireless network. Users are preassigned with login credentials and they must provide it when they connect to this wireless network. **User authentication and centralized management is done through the RADIUS server** which is in the 2nd floor. Further the wireless signal from access point will be limited to the CEO/CTO room only, by using an appropriate small range antenna.

VLAN Description

VLAN Number	Description
VLAN 10	This is used to group the 100 wired machines in 4th floor
VLAN 20	This is used to group the 50 mobile nodes in 4th floor (wireless)
VLAN 30	This is used to group the 60 wired nodes in 3rd floor
VLAN 40	This is used to group the workstation that belong to CEO/CTO office in 3rd floor
VLAN 50	This is used to group the servers inside the server room in 2nd floor
VLAN 60	This is used to group the 20 machines in 1st floor
VLAN 70	This is used to group the web server in DMZ

VLANs are created across each floor and for wireless networks. 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

IP Address – 172.20.0.0 /16

VLAN	**Network Address**	**Sub Netmask**	**Host Address Range**	**Broadcast Address**
VLAN 10	172.20.0.0 /25	255.255.255.128	172.20.0.1 - 172.20.0.126	172.20.0.127
VLAN 20	172.20.0.192 /26	255.255.255.192	172.20.0.193 - 172.20.0.254	172.20.0.255
VLAN 30	172.20.0.128 /26	255.255.255.192	172.20.0.129 - 172.20.0.190	172.20.0.191
VLAN 40	172.20.1.32 /28	255.255.255.240	172.20.1.33 - 172.20.1.46	172.20.1.47
VLAN 50	172.20.1.48 /29	255.255.255.248	172.20.1.49 - 172.20.1.54	172.20.1.55
VLAN 60	172.20.1.0 /27	255.255.255.224	172.20.1.1 - 172.20.1.30	172.20.1.31
VLAN 70	172.20.1.56 /30	255.255.255.252	172.20.1.57 - 172.20.1.58	172.20.1.59

- ✓ It is assumed that CEO/CTO office need around 12 IP address for its employees.
- ✓ Servers inside the server room are assigned with static IP address in the range 172.20.1.49 - 172.20.1.54 (VLAN 50)
- ✓ 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

1. Static Routing – Static routes are configured on gateway/core routers of each branches and in main site, to route the traffic from inside network to another branch network. As the next hop (IP of each branch network) is known this can be used. Since this is a **small network using static routes are simple and easy**. It's secure because no any routing advertisements are exchanged between neighbors and computing resources are conserved because no routing algorithm or update mechanisms required.

2. Default routing – This is configured on core routers to route the traffic from inside network to ISP router for unknown traffic (towards internet)

3. 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 in 2nd floor. 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 maintain 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 each floor to the 2 core switches located in 2nd floor. 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 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 is 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 with in inside 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 address used for the translation. **Static NAT** will be used for communication of web server over the Internet. Because 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 1 core router fails**.

VLAN (Virtual Local Area Network)

There are 7 different VLANs created across this network. Each VLAN for different floor and separate VLAN for wireless network in 4th and 3rd floor. 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.

RADIUS (Remote Authentication Dial-In User Service)

RADIUS server is implemented in the server room in 2nd floor. It **provides centralized authentication, authorization and accounting (AAA) services for users** who connect and use the network service. It is mainly used to authenticate the users attached to wireless network in CEO/CTO room in 3rd floor. Reporting and tracking based on the client usernames becomes easy due to this deployment.

FTP (File Transfer Protocol)

FTP server is installed in the server room of 2nd floor. This is used for the file transfer within inside 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**.

SMTP (Simple Mail Transfer Protocol)

SMTP Mail server is placed in the 2nd floor server room. SMTP servers are more reliable when sending mails to clients. They **deliver mail to recipients quickly, they offer reliability in sending email messages (SMTP server will always try to re-send the same email until the**

transmission becomes successful), spam messages can be controlled in the central location and mailbox capacity is limited to hardware capacity.

Other Techniques used

1. **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.
2. **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.

References

[1] CPS Technologies. "The advantages of network patch panels". Internet: http://www.cps-africa.com/index.php/news/item/57-the-advantages-of-network-patch-panels, [Jul.03,2017].

[2] Wikipedia. "Structured cabling". Internet: https://en.wikipedia.org/wiki/Structured_cabling, June.30,2017 [Jul.04,2017].

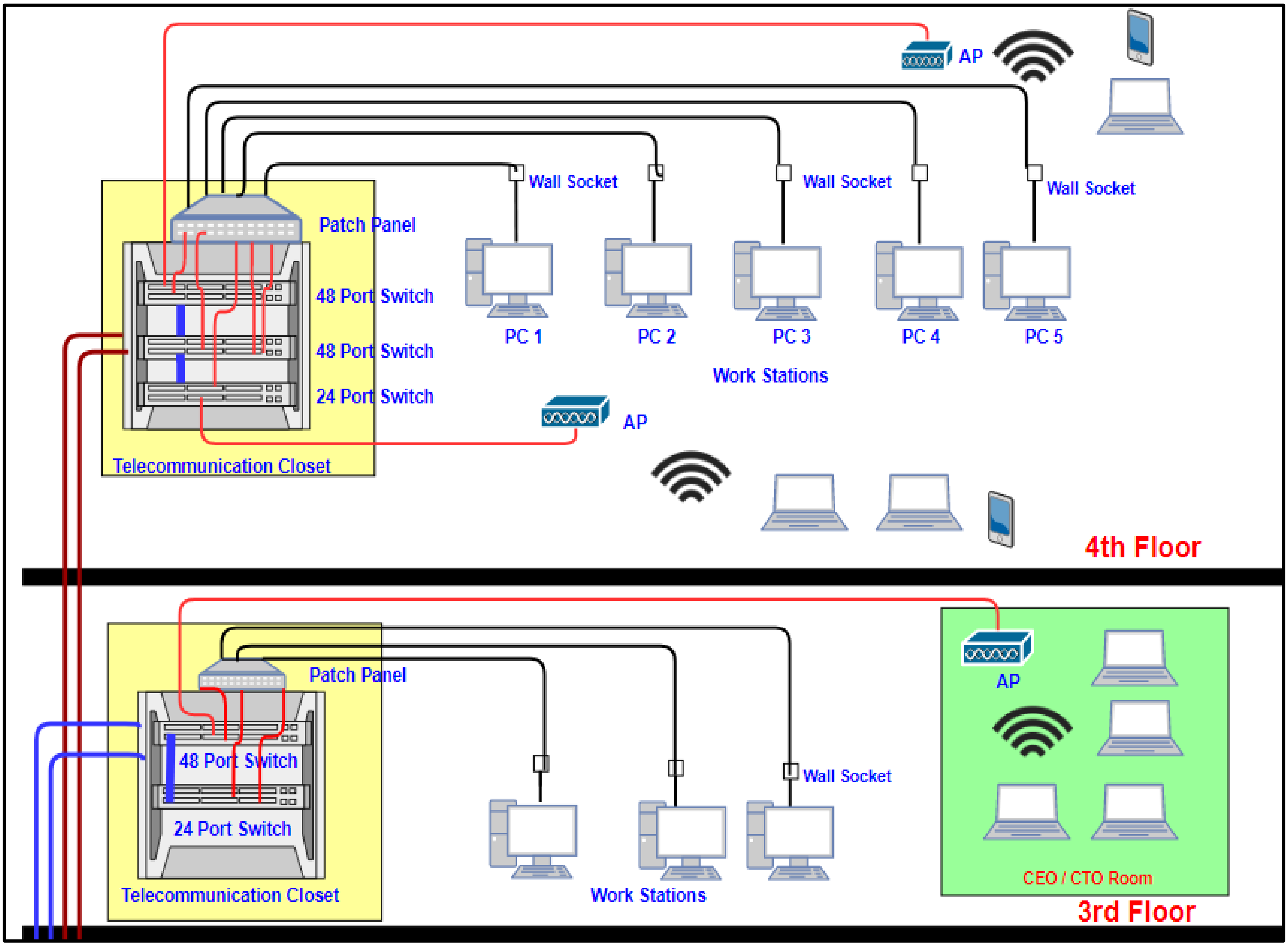
[3] Wikipedia. "Stackable switch". Internet: https://en.wikipedia.org/wiki/Stackable_switch, April.16,2017 [Jul.04,2017].

[4] 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 [Jul.05,2017]

[5] Erwin Z. "Benefits of SMTP". Internet: http://benefitof.net/benefits-of-smtp/, May.09,2012 [Jul.05,2017]

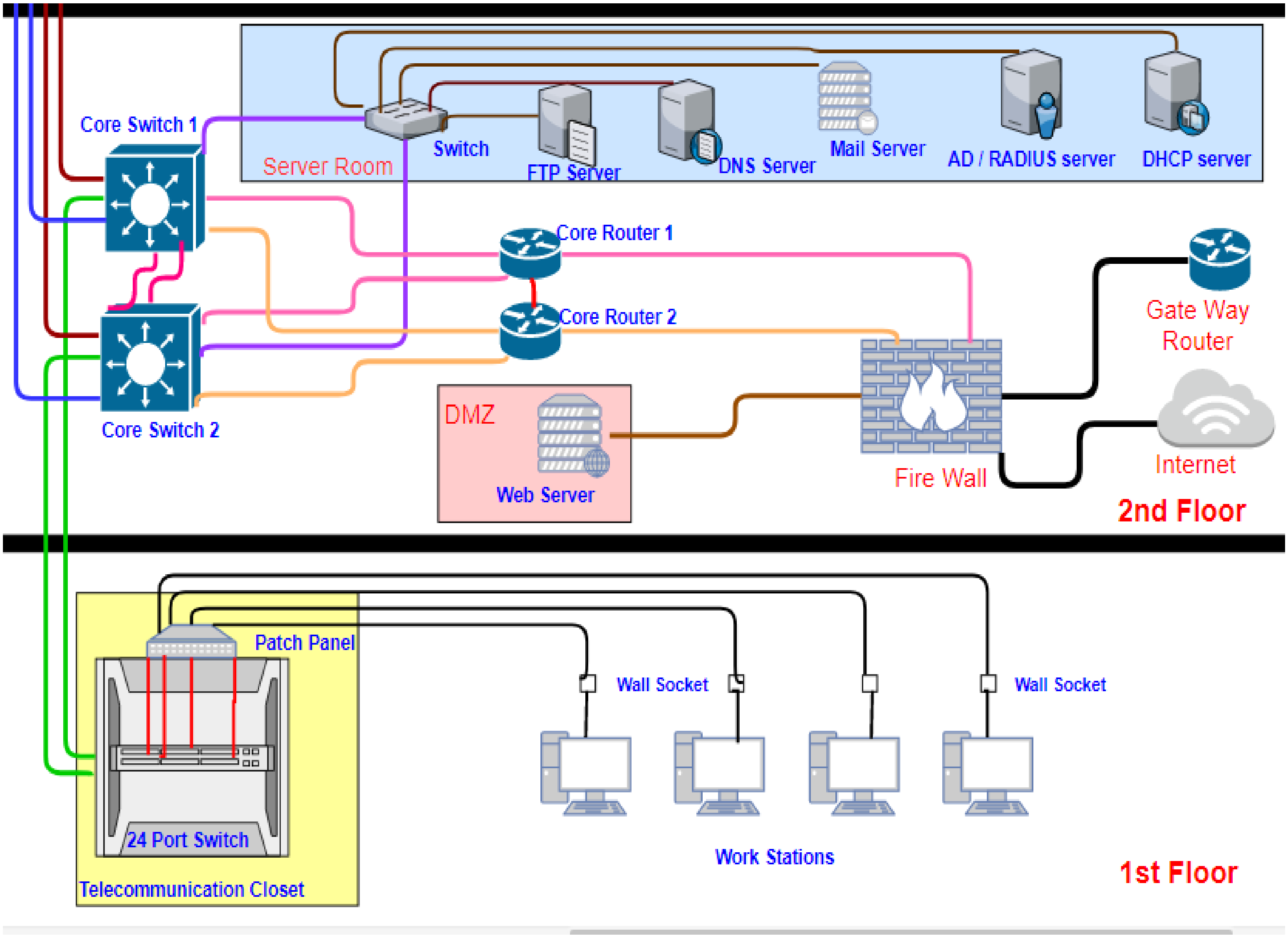
Annex 1

(Enlarged Image of 4th Floor and 3rd Floor of the building)



Annex 2

(Enlarged Image of 2nd Floor and 1st Floor of the building)


Core Switch 1
Server Room
Switch
FTP Server
DNS Server
Mail Server
AD / RADIUS server
DHCP server
Core Router 1
Core Router 2
Gate Way Router
Core Switch 2
DMZ
Web Server
Fire Wall
Internet
2nd Floor
Patch Panel
Wall Socket
Wall Socket
24 Port Switch
Work Stations
Telecommunication Closet
1st Floor