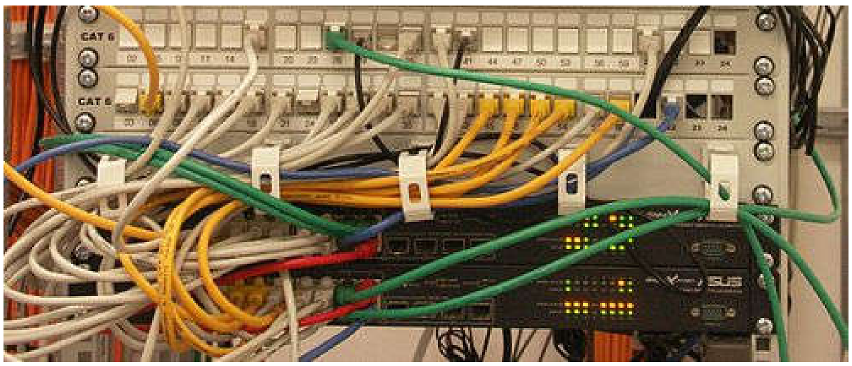


Techstar Data Center Design

Data Center Network Design | 04-27-2018

Contents

Table of figures

1- Executive Summary

In this report we present the design and implementation of Data Center for Techstar Inc. in Wichita Kansas.

A data center or computer Centre (also datacenter) is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices. Data centers have their roots in the huge computer rooms of the early ages of the computing industry.

Data Centre IT equipment's consists of many individual devices like storage devices, servers, network equipment's such as Routers, switches, firewalls etc. The essentials of Data Center are Location –Where in the building, Racks-to mount Servers, Network cables and Network Equipment's in orderly state. Disaster planning, Wiring, Access to Data Centre and Security. Total cost of this project is $1 million

2- Introduction and Scope

In this report the we will design a Data center which has two-story building with four department, with 20 computers having internet connectivity. The Data center also wants to support four additional new constructed departments, each containing 10 computers and and 10 IP phone. DataCenter will be hosting hundered of virtual machines, provide backup for the data on computers, server as a mail server and FTP server.

The HR department will have 10 computers to allow employee access to the resources. Also, 10 computers will be made available for staff and administration. Finally, wireless network should be made available to technical department and staff inside data center premises.

In this project, we'll create design and create a logical, efficient and scalable network. In addition, we'll use industry-specific standards.

3- Reason for Issue/Reissue

Early computer systems were complex to operate and maintain, and required a special environment in which to operate. Many cables were necessary to connect all the components and methods to accommodate and organize these were devised, such as standard racks to mount equipment, elevated floors, and cable trays (installed overhead or under the elevated floor). Also, a single mainframe required a great deal of power, and had to be cooled to avoid overheating. Security was important – computers were expensive, and were often used for military purposes.

As found out that without Data Center the whole IT system is haphazard. The risk factor is high as the IT assets are not centralized. So managing the IT assets is a tiresome job. Whenever there is any issue it becomes difficult for a engineer to identify actually where the issue lies. The company has got fifteen Zonal Offices, Two plants, Head Office and a Sales & Marketing office so to manage the IT infra is very hard. Therefore, a Data Center is made to make the IT work without any downtime and failure. During Research it was found that a very minor system failure causes loss of job which hampers business growth and sometimes loss of data as centralized storage system is not available. So, after suggestions and planning to decide to make IT centralized. [1]

4- Terms and Abbreviations

AAA—Authentication Authorization, Accounting

ARP—Address Resolution Protocol

ACL—Access Control List

DMZ—Demilitarized Zone

DHCP—Dynamic Host Configuration Protocol

DSL—Digital Subscriber Line

EIGRP—Enhanced Interior Gateway Routing Protocol

FTTH—Fiber To The Home

FTTP—Fiber To The Premises

FTP—File Transfer Protocol

LAN—Local Area Network

PPP—Point-to-Point Protocol

SSH—Secure Shell

SSID—Service Set Identifier

5- Design Requirements

1- Data center Boundary & Grounding Implementation

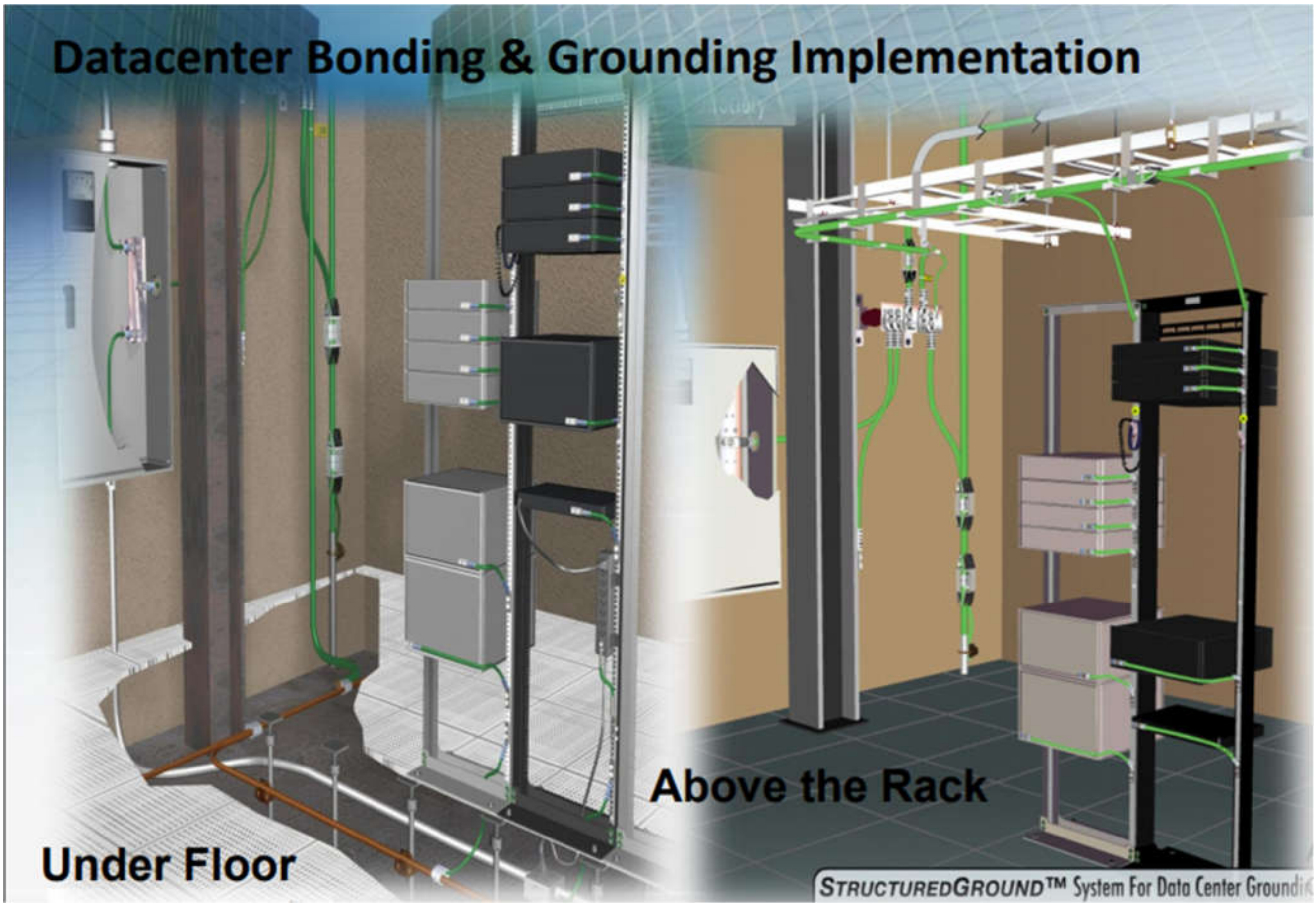


Figure 1 Data center Boundary & Grounding Implementation

2- Pathway Options for fiber optic cable distribution

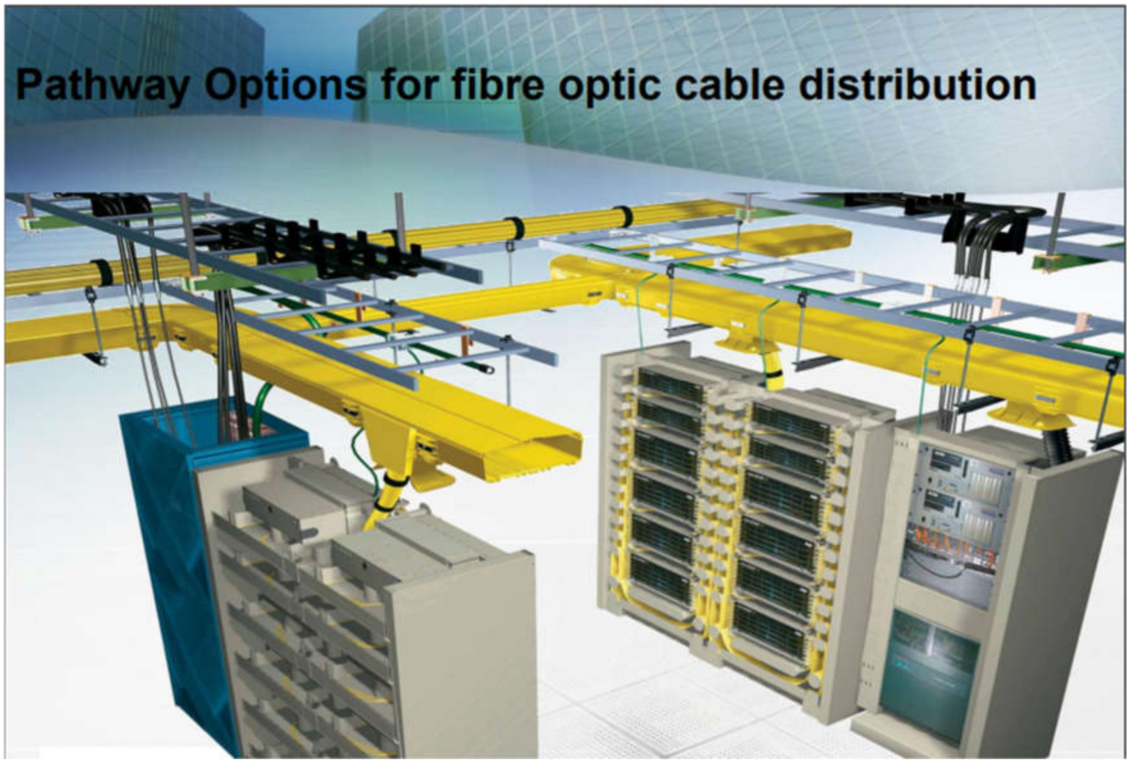
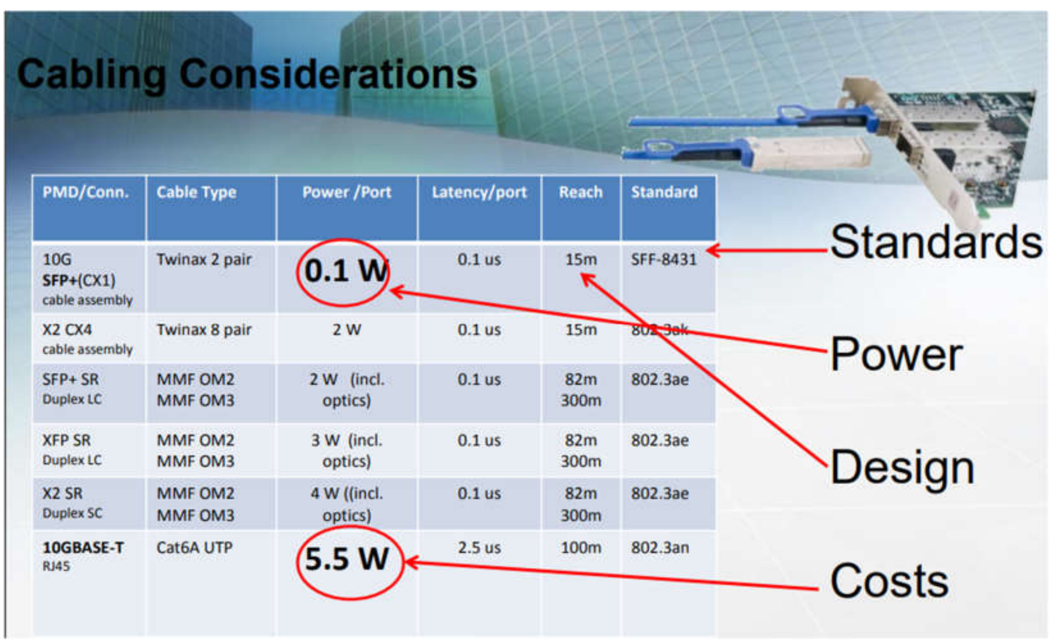


Figure 2 Pathway option Fiber Optic Cable Distribution

3- Cabling Considrations



PMD/Conn.	Cable Type	Power /Port	Latency/port	Reach	Standard
10G **SFP+**(CX1) cable assembly	Twinax 2 pair	0.1 W	0.1 us	15m	SFF-8431
X2 CX4 cable assembly	Twinax 8 pair	2 W	0.1 us	15m	802.3ak
SFP+ SR Duplex LC	MMF OM2 MMF OM3	2 W (incl. optics)	0.1 us	82m 300m	802.3ae
XFP SR Duplex LC	MMF OM2 MMF OM3	3 W (incl. optics)	0.1 us	82m 300m	802.3ae
X2 SR Duplex SC	MMF OM2 MMF OM3	4 W ((incl. optics)	0.1 us	82m 300m	802.3ae
10GBASE-T RJ45	Cat6A UTP	5.5 W	2.5 us	100m	802.3an

Figure 3 Cabling Consideration

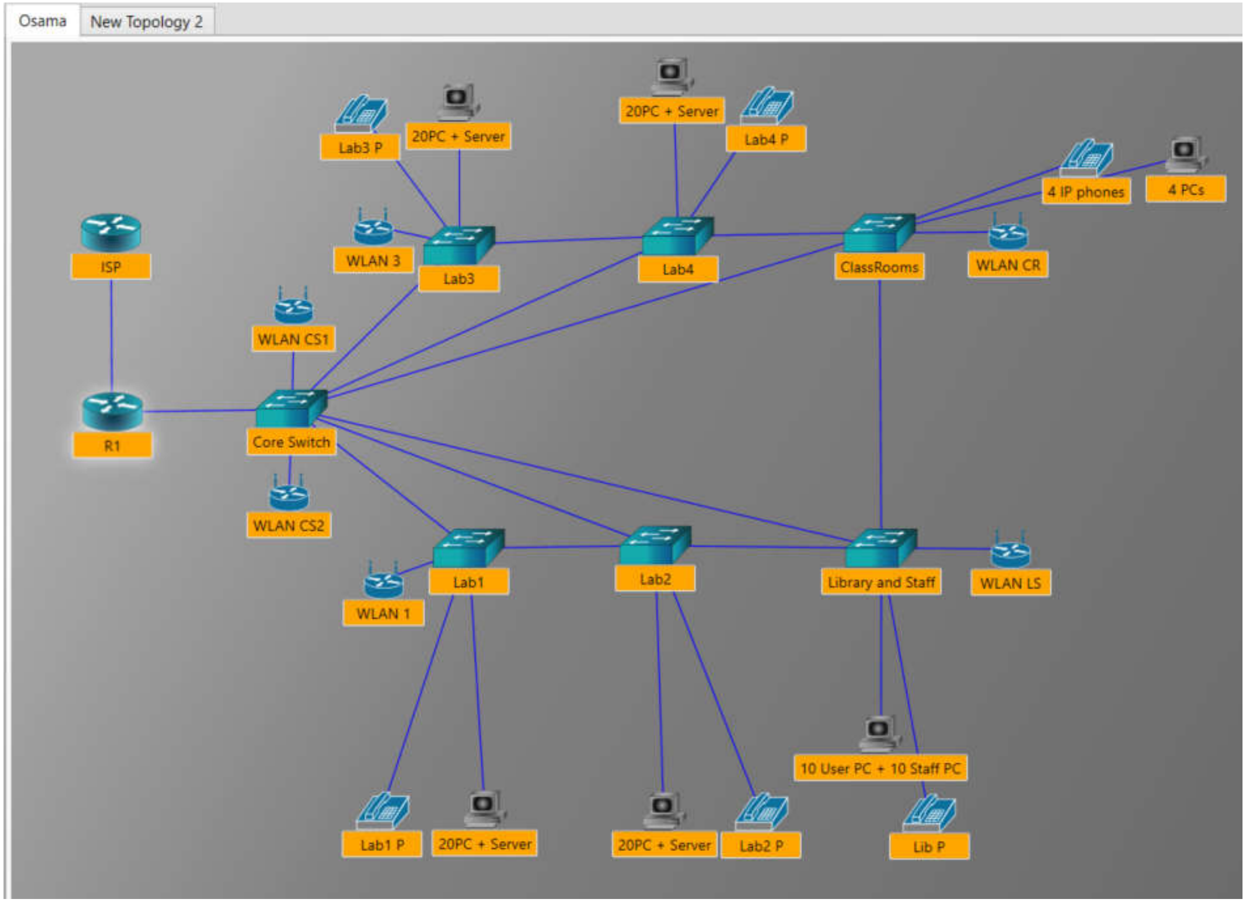
6- Hardware Requirements

For the installation of network, following equipment is required:

1- Router 1 – Cisco 2800 Series – 2811 – 2 FE, 2 Ser,
2- Switches 6 – Cisco 2900 – 2960x – 2GE, 24 FE
3- Switch 1 – Cisco 3500 - 3550 – 2GE, 12 FE
4- AP – 4 - Cisco 802.11ac CAP
5- IP Phones – 8 – Cisco 8841 VoIP.
6- Connecting Cables – STP, CAT6
7- Racks – 4 – for each lab
8- Servers – 4 - HP Proliant ML350 GEN9 6C XEON E5 2.4GHZ 16GB RAM, 10TB SSD
9- PCs – 96 – HP Pavilion Power Desktop 580-150ng AMD Ryzen 3 1200 3.1GHz, 8GB RAM, 500GB HDD
10- Monitors – 100 – HP LEDs

7- Design Overview

a. Topology



We installed one 2960-24TT-L for each Lab and connected it with the Core Switch (3550 Multilayer switch) using Gigabit Ethernet when available. Lab 3 and Lab 1 are connected with Core Switch with Gigabit Ethernet whereas Lab 2, 4, ClassRooms and Library switches are connected to Core Switch with FastEthernet. Lab 3 and Lab 4, Lab 1 and Lab2, Lab4 and ClassRooms, Lab2 and 'Library and Staff' switches are connected with Gigabit Ethernet. This in turn, makes our topology a hybrid topology with star and ring topology characteristics. The advantage is redundancy which gives us fail-over tolerance.

b. Routers

A router is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

Cisco 4000 Series ISR

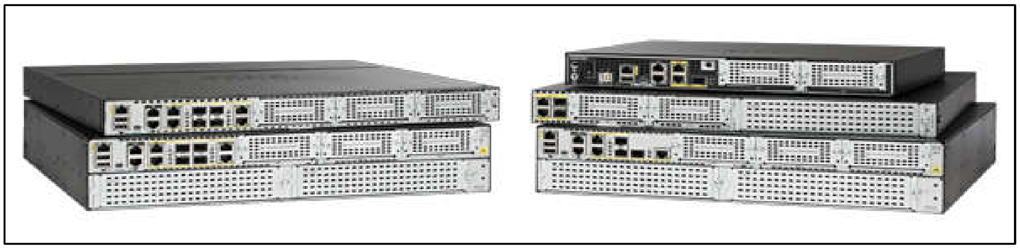


Figure 4 Cisco 4000 Series ISR

c. Switches

A network switch is a computer networking device that links network segments or network devices. A switch is a telecommunication device that receives a message from any device connected to it and then transmits the message only to the device for which the message was meant. This makes the switch a more intelligent device than a hub (which receives a message and then transmits it to all the other devices on its network). The network switch plays an integral part in most modern Ethernet local area networks (LANs). Mid-to-large sized LANs contain a number of linked managed switches. Small office/home office (SOHO) applications typically use a single switch, or an all-purpose converged device such as a residential gateway to access small office/home broadband services such as DS or cable Internet.

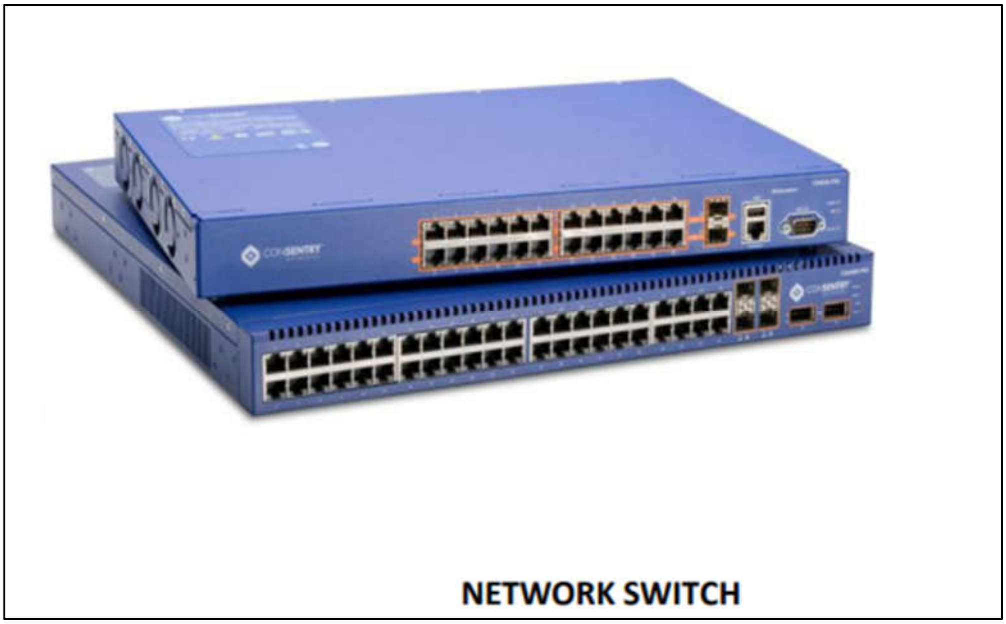


Figure 5 Network Switches

Core Layer: Cisco 3550 Layer 3 Switch with 12 FE and 2 GE ports.

Figure 6 Cisco 3550

Access Layer: Cisco 2960 Layer 2 24 TTL with 24 FE and 2 GE ports.

Figure 7 Cisco 2960 Layer 2 24 TTL

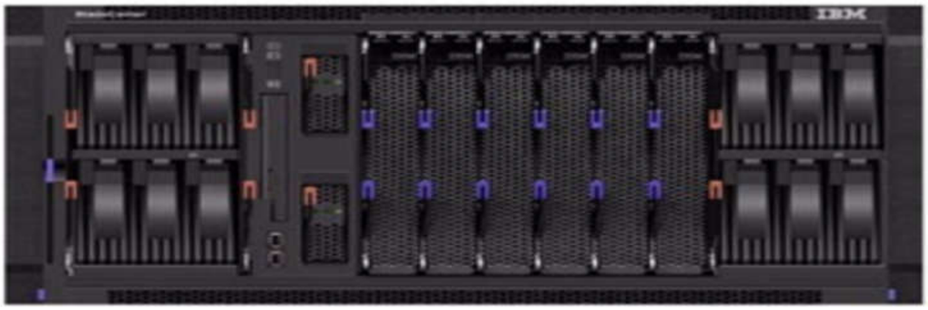
d. Wireless APs – Cisco Aironet 4800 Access Points - Dual radios:

Dual Band with flexible radio assignment to optimize performance based on dynamic network conditions

Figure 8 Cisco Wirless Access Point

e. Server

Servers: A server is a running instance of an application (software) capable of accepting requests from the client and giving responses accordingly. Servers can run on any computer including dedicated computers, which individually are also often referred to as "the server". In many cases, a computer can provide several services and have several servers running. The advantage of running servers on a dedicated computer is security. For this reason most of the servers are daemon processes and designed in such a way that they can be run on specific computer. Servers operate within a client-server architecture. Servers are computer programs running to serve the requests of other programs, the clients. Thus, the server performs some tasks on behalf of clients. It facilitates the clients to share data, information or any hardware and software resources. The clients typically connect to the server through the network but may run on the same computer. In the context of Internet Protocol (IP) networking, a server is a program that operates as a socket listener. Servers often provide essential services across a network, either to private users inside a large organization or to public users via the Internet. Typical computing servers are database server, file server, mail server, print server, web server, gaming server, and application server. Numerous systems use this client server networking model including Web sites and email services. An alternative model, peer-to-peer networking enables all computers to act as either a server or client as needed. [2]



IBM Blade Center S Server

Figure 9 IBM Blade Center S Server

IBM X3500 Series Server

Figure 10 Server

f. IP Addressing

Following table summarizes the subnetting scheme for the network.

Network	# IPs required	Subnet	Description
Wireless	200	192.168.1.0/24	For Wireless Network
Lab 1 – 4	84	192.168.2.0/25	For All Labs
Library + Staff	20	192.168.2.128/27	For Library and Staff
Classrooms	8	192.168.2.160/28	For 4 IP Phones and 4 PCs
R1 – Cswitch	2	192.168.2.176/30	For R1 to Core Switch Link

Figure 11 IP Addressing

8- Configurations

A. Load Balance Configuration

When a load balancer is put into place, incoming traffic – requests for information from the servers from user web browsers – routes through the device prior to hitting the cloud servers. That point all the traffic is reaching, where the load balancer is located, is one network address. As a load balancer receives the requests, it divides work evenly throughout a server cluster.

The reason the servers are a cluster is because a cluster is a number of computers operating in the same basic manner to achieve the same objectives. In a basic load balancing set-up, all of the servers behind the load balancer are performing the same basic function – equal work based on what comes through the load balancer.

B. Firewall Configuration

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.225	255.255.255.248	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	NA
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	NA
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	NA
DMZ Server	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

Figure 12 IP Addressing

Verify connectivity and explore the ASA

- Configure basic ASA settings and interface security levels using CLI
- Configure routing, address translation, and inspection policy using CLI
- Configure DHCP, AAA, and SSH
- Configure a DMZ, Static NAT, and ACLs

Configure the inside and outside interfaces.

You will only configure the VLAN 1 (inside) and VLAN 2 (outside) interfaces at this time.

a. Configure a logical VLAN 1 interface for the inside network (192.168.1.0/24) and set the security level to the highest setting of 100.
   CCNAS-ASA(config)# interface vlan 1
   CCNAS-ASA(config-if)# nameif inside
   CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
   CCNAS-ASA(config-if)# security-level 100
b. Create a logical VLAN 2 interface for the outside network (209.165.200.224/29), set the security level to the lowest setting of 0, and enable the VLAN 2 interface.
   CCNAS-ASA(config-if)# interface vlan 2
   CCNAS-ASA(config-if)# nameif outside
   CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248

CCNAS-ASA(config-if)# security-level 0

Configure Route

CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225

Configuration of DHCP

a. Configure a DHCP address pool and enable it on the ASA inside interface.

   CCNAS-ASA(config)# dhcpd address 192.168.1.5-192.168.1.36 inside

b. (Optional) Specify the IP address of the DNS server to be given to clients.

   CCNAS-ASA(config)# dhcpd dns 209.165.201.2 interface inside

c. Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (inside).

   CCNAS-ASA(config)# dhcpd enable inside

d. Change PC-B from a static IP address to a DHCP client, and verify that it receives IP addressing

information. Troubleshoot, as necessary to resolve any problems.

Configuration of SSH

CCNAS-ASA(config)# ssh 192.168.1.0 255.255.255.0 inside

CCNAS-ASA(config)# ssh 172.16.3.3 255.255.255.255 outside

CCNAS-ASA(config)# ssh timeout 10

Configure a DMZ, Static NAT, and ACLs

a. Configure DMZ VLAN 3, which is where the public access web server will reside

   CCNAS-ASA(config)# interface vlan 3

   CCNAS-ASA(config-if)# ip address 192.168.2.1 255.255.255.0

   CCNAS-ASA(config-if)# no forward interface vlan 1

   CCNAS-ASA(config-if)# nameif dmz

   INFO: Security level for "dmz" set to 0 by default.

   CCNAS-ASA(config-if)# security-level 70

b. Assign ASA physical interface E0/2 to DMZ VLAN 3 and enable the interface.

   CCNAS-ASA(config-if)# interface Ethernet0/2

   CCNAS-ASA(config-if)# switchport access vlan 3

Configure a network object named dmz-server and assign it the static IP address of the DMZ server

(192.168.2.3)

CCNAS-ASA(config)# object network dmz-server

CCNAS-ASA(config-network-object)# host 192.168.2.3

CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227

CCNAS-ASA(config-network-object)# exit

Configure ACL

CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3

CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80

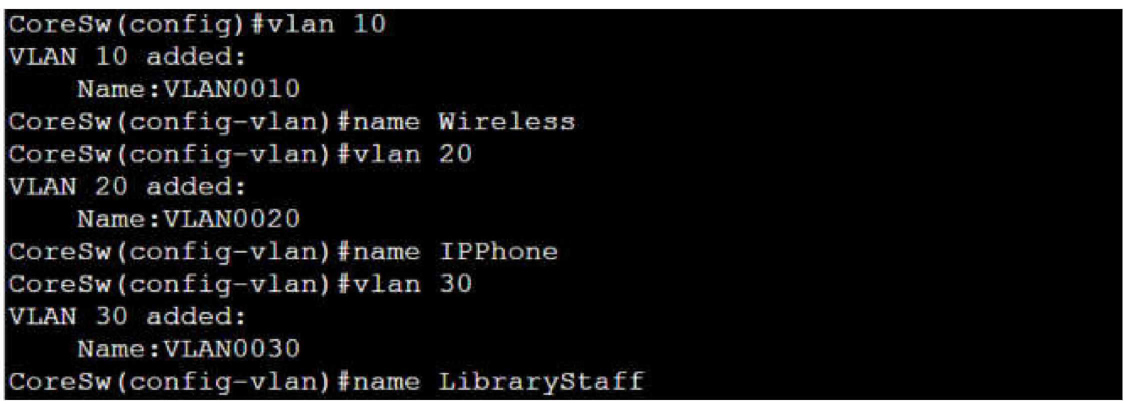
CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface outside [3]

C. VLAN And VTP Configuration on Switches

VLANs are used to divide a physical network to logical segments and VTP is used to distribute VLAN information to whole switched network. [4]

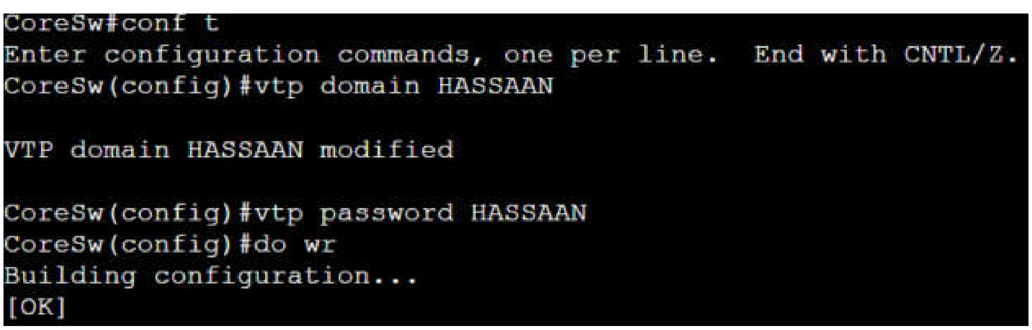
a. Core Switch

VLAN and VTP configuration of CoreSw is given in this section.



```
CoreSw(config)#vlan 10
VLAN 10 added:
    Name:VLAN0010
CoreSw(config-vlan)#name Wireless
CoreSw(config-vlan)#vlan 20
VLAN 20 added:
    Name:VLAN0020
CoreSw(config-vlan)#name IPPhone
CoreSw(config-vlan)#vlan 30
VLAN 30 added:
    Name:VLAN0030
CoreSw(config-vlan)#name LibraryStaff
```

Figure 13 shows creation and naming of VLANs 10, 20, 30



```
CoreSw#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CoreSw(config)#vtp domain HASSAAN

VTP domain HASSAAN modified

CoreSw(config)#vtp password HASSAAN
CoreSw(config)#do wr
Building configuration...
[OK]
```

Figure 14 VTP configuration steps

```
CoreSw(config-vlan)#do show vtp stat
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 64
Number of existing VLANs        : 9

VTP Operating Mode              : Server
VTP Domain Name                 : HASSAAN
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
```

Figure 15 VTP verification

```
CoreSw(config-vlan)#interface fa0/5
CoreSw(config-if)#switchport mode access
CoreSw(config-if)#switchport access vlan 10
CoreSw(config-if)#
CoreSw(config-if)#interface fa0/6
CoreSw(config-if)#switchport mode access
CoreSw(config-if)#switchport access vlan 10
CoreSw(config-if)#
CoreSw(config-if)#^Z
00:10:01: %SYS-5-CONFIG_I: Configured from console by console
CoreSw#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- ----------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa
                                                Fa0/11, Fa0/12
10   Wireless                         active    Fa0/5, Fa0/6
20   IPPhone                          active
30   LibraryStaff                     active

1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 16 Assigning ports to VLANs and verifying

b. Lab1-Switch

VTP configuration and verification on Lab1-S is given in this part.

```
Lab1-S(config)#int fas0/3
Lab1-S(config-if)#switchport mode acc
Lab1-S(config-if)#switchport access vlan 10
Lab1-S(config-if)#int fas0/1
Lab1-S(config-if)#switchport mode acc
Lab1-S(config-if)#switchport access vlan 20
Lab1-S(config-if)#^Z
00:19:39: %SYS-5-CONFIG_I: Configured from console by console
Lab1-S#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
10   Wireless                         active    Fa0/3
20   IPPhone                          active    Fa0/1
30   LibraryStaff                     active
```

Figure 17 Assignment of ports to VLANs + Verification

```
Lab1-S#show vtp stat
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 64
Number of existing VLANs        : 9

VTP Operating Mode              : Server
VTP Domain Name                 : HASSAAN
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xEE 0xB3 0xDC 0x9F 0xE2 0xE0 0x25 0xDF
Configuration last modified by 0.0.0.0 at 3-1-2012 04:55:57
Local updater ID is 0.0.0.0 (no valid interface found)
```

Figure 18 VTP Status

c. Classrooms Switch

```
ClassRooms#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24
10   Wireless                         active    Fa0/4
20   CLASSROOMS                       active    Fa0/3
30   LibraryStaff                     active
100  VLAN0100                         active
```

Figure 19 All switches know about existing VLANs due to VTP

D. DHCP Configuration

a. Core Switch

Following Screenshot contains configuration commands for DHCP:

```
CoreSw(config)#ip dhcp ?
excluded-address        Prevent DHCP from assigning certain addresses
pool                    Configure DHCP address pools
snooping                DHCP Snooping
CoreSw(config)#ip dhcp pool ?
WORD                    Pool name
CoreSw(config)#ip dhcp pool VLAN1 ?
<cr>
CoreSw(config)#ip dhcp pool VLAN1
CoreSw(dhcp-config)#?
client-identifier       Client identifier
default-router          Default routers
dns-server              DNS servers
domain-name             Domain name
exit                    Exit from DHCP pool configuration mode
host                    Client IP address and mask
lease                   Address lease time
network                 Network number and mask
CoreSw(dhcp-config)#network ?
a.b.c.d                 Network number in dotted-decimal notation
CoreSw(dhcp-config)#network 192.168.2.0 ?
/nn or a.b.c.d          Network mask or prefix length
<cr>
CoreSw(dhcp-config)#network 192.168.2.0 /25 ?
<cr>
CoreSw(dhcp-config)#network 192.168.2.0 /25
CoreSw(dhcp-config)#?
client-identifier       Client identifier
default-router          Default routers
dns-server              DNS servers
domain-name             Domain name
exit                    Exit from DHCP pool configuration mode
host                    Client IP address and mask
lease                   Address lease time
network                 Network number and mask
CoreSw(dhcp-config)#default-router 192.168.2.1
CoreSw(dhcp-config)#lease ?
<0-365>                 Days
infinite                Infinite lease
CoreSw(dhcp-config)#lease 0 ?
<0-23>                  Hours
<cr>
CoreSw(dhcp-config)#lease 0 8 ?
<0-59>                  Minutes
<cr>
CoreSw(dhcp-config)#lease 0 8 0
CoreSw(dhcp-config)#exit
CoreSw(config)#ip dhcp excl 192.168.2.1 192.168.2.10
CoreSw(config)#
```

Figure 20 Configuration steps for multiple DHCP Servers on CoreSwitch

```
!
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp excluded-address 192.168.2.1 192.168.2.10
ip dhcp excluded-address 192.168.2.128 192.168.2.134
ip dhcp excluded-address 192.168.2.161
!
ip dhcp pool VLAN1
 network 192.168.2.0 255.255.255.128
 default-router 192.168.2.1
 lease 0 8
ip dhcp pool WIRELESS
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
ip dhcp pool LIBRARY
 network 192.168.2.128 255.255.255.224
 default-router 192.168.2.129
ip dhcp pool CLASSROOMS
 network 192.168.2.160 255.255.255.240
 default-router 192.168.2.161
!
```

Figure 21 All commands in running configuration for Multiple DHCP Pools

b. Host 4PCs

```
Devices: 4PCs [Device #26]

C:>ipconfig /release
C:>ipconfig /renew

%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0 assigned DHCP address 192.168.2.162, mask 255.255.255.240,

C:>

Lab1 | Lab2 | Lab4 | LibraryandStaff | Lab3 | CoreSwitch | ClassRooms | 20PC+Server (1) | 20PC+Server (2) | 20PC+Server (3) | 20PC+Server (4) | 4PCs
```

Figure 22 Host 4PCs got its address via DHCP

c. 20pc + Server (2)

```
Devices: 20PC+Server (2) [Device #23]

Boson BOSS 5.0
Copyright 1998-2018 Boson Software, LLC.
Use the command help to get started

Press Enter to begin
C:>ipconfig /ip dhcp

%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0 assigned DHCP address 192.168.2.12, mask 255.255.255.128,

Lab1 | Lab2 | Lab4 | LibraryandStaff | Lab3 | CoreSwitch | ClassRooms | 20PC+Server (1) | 20PC+Server (2) | 20PC+Server (3) | 20PC+Server (4) | 4PCs
```

Figure 23 Address lease in a different VLAN

d. Core Switch

```
interface Vlan 1
 ip address 192.168.2.1 255.255.255.128
 no ip route-cache
!
interface Vlan0020
 ip address 192.168.2.161 255.255.255.240
 no ip route-cache
!
interface Vlan0030
 ip address 192.168.2.129 255.255.255.224
 no ip route-cache
!
interface Vlan0010
 ip address 192.168.1.1 255.255.255.0
 no ip route-cache
!
vlan 10 name Wireless
vlan 20 name CLASSROOMS
vlan 30 name LibraryStaff
vlan 100 name VLAN0100
!
!
```

Figure 24 SVIs and VLANs in running-config

```
C:>ping 192.168.2.135

Pinging 192.168.2.135 with 32 bytes of data:
Reply from 192.168.2.135: bytes=32 time=64ms TTL=241
Reply from 192.168.2.135: bytes=32 time=65ms TTL=241
Reply from 192.168.2.135: bytes=32 time=50ms TTL=241
Reply from 192.168.2.135: bytes=32 time=64ms TTL=241
Reply from 192.168.2.135: bytes=32 time=66ms TTL=241

Ping statistics for 192.168.2.135:
     Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 50ms, Maximum =  66ms, Average =  62ms

C:>ping 192.168.2.162

Pinging 192.168.2.162 with 32 bytes of data:
Reply from 192.168.2.162: bytes=32 time=51ms TTL=241
Reply from 192.168.2.162: bytes=32 time=56ms TTL=241
Reply from 192.168.2.162: bytes=32 time=66ms TTL=241
Reply from 192.168.2.162: bytes=32 time=72ms TTL=241
Reply from 192.168.2.162: bytes=32 time=66ms TTL=241

Ping statistics for 192.168.2.162:
     Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 51ms, Maximum =  72ms, Average =  62ms

C:>
```

Lab1 | Lab2 | Lab4 | LibraryandStaff | Lab3 | CoreSwitch | ClassRooms | 20PC+Server (1) | 20PC+Server (2) | 20PC+Server (3)

Figure 25 ping test between different VLANS

E. Router Configuration

a. Core Switch

```
CoreSw(config)#int fa0/7
CoreSw(config-if)#ip add

% IP addresses may not be configured on L2 links.
CoreSw(config-if)#no switchport
CoreSw(config-if)#ip address 192.168.2.178 255.255.255.252
CoreSw(config-if)#no sh
CoreSw(config-if)#exit
CoreSw(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.178
%Invalid next hop address (it's this address)
CoreSw(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.177
CoreSw(config)#^Z
03:50:18: %SYS-5-CONFIG_I: Configured from console by console
CoreSw#wr
Building configuration...
```

Figure 26 Setting IP Address to interface connected to Router and IP Route

b. Router-1

```
!
ip route 192.168.0.0 255.255.252.0 192.168.2.178
!
```

Figure 27 IP Route on R1

c. 20pc + Server (3)

```
C:>ping 192.168.2.177

Pinging 192.168.2.177 with 32 bytes of data:
Reply from 192.168.2.177: bytes=32 time=61ms TTL=241
Reply from 192.168.2.177: bytes=32 time=49ms TTL=241
Reply from 192.168.2.177: bytes=32 time=59ms TTL=241
Reply from 192.168.2.177: bytes=32 time=59ms TTL=241
Reply from 192.168.2.177: bytes=32 time=72ms TTL=241

Ping statistics for 192.168.2.177:
     Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 49ms, Maximum =  72ms, Average =  60ms

C:>
```

Lab1 | Lab2 | Lab4 | LibraryandStaff | Lab3 | CoreSwitch | ClassRooms | 20PC+Server (1) | 20PC+Server (2) | 20PC+Server (3)

Figure 28 Ping to R1

9- Conclusion

The Data Center is made to make IT centralized and easy for users as far as possible. The system provides scope for further enhancement depending upon user's requirement. Even though the system satisfies requirements still more and more additional work can be carried out. Finally it can be concluded that the overall Data Center Management process is implemented successfully. The IT process has been centralized and user problem are resolved as soon as they logged a call for complaint

All the requirements were fulfilled including careful IP addressing, redundancy, scalability, wireless, IP phone etc.

10- References

[1] D. Bora, "Project Report On Data Center Management," 12 December 2014. [Online]. Available: https://www.slideshare.net/DipakBora/project-report-on-data-center-management?from_action=save.

[2] L. Kostaras, "Data Centre Design &," Cisco, [Online]. Available: https://www.cisco.com/c/dam/global/hr_hr/assets/ciscoconnect/2013/pdfs/Datacenter_design_n_implementation_trends_a_ROI_approach_Lambros_Kostaras_Business_Manager_South_East_Europe.pdf.

[3] Cisco, "Packet Tracer - Configuring ASA Basic Settings and Firewall Using CLI," [Online]. Available: Configuring ASA Basic Settings and Firewall Using CLI.

[4] Cisco, "Understanding VLAN Trunk Protocol (VTP)," Cisco, 29 September 2014. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html. [Accessed 06 May 2018].

[5] T. Fisher, "What Is DHCP? (Dynamic Host Configuration Protocol)," LifeWire, 08 March 2018. [Online]. Available: https://www.lifewire.com/what-is-dhcp-2625848. [Accessed 7 May 2018].

[6] Cisco, "Configure InterVLAN Routing on Layer 3 Switches," Cisco, 20 April 2016. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html. [Accessed 07 May 2018].