

---

# **ENTERPRISE NETWORK DESIGN**

---

## **PROJECT REPORT**

### **PROJECT NAME: YALE HOSPITALS NETWORK**

**Date: 12-06-2018**



**Submitted to: Dr. Amir Esmailpour**

# Abstract

The aim of this project is to design an enterprise network (LAN and WAN) for Yale New Haven hospital. The purpose of choosing this is to design a safe, secured wireless network for the employees, staff, patients and visitors with proper bandwidth and high network availability with minimal down time. Our network consists of main branch New Haven with North, South, East, West buildings and two remote locations Guilford and Bridgeport with total of 4200 staff, 200 doctors and 10,000 patients. The data in hospital system is huge, some of them is sensitive, confidential and real-time information, the database server is running for 24 hours a day, if the whole network system is in the failure of man-made or accidental, this will cause huge losses and social impact. From the view point of server maintenance, data security and backup, user management, management and maintenance of network security is highly important.

# Contents

<b>Phase 1: Client Network</b>	6
Yale New Haven Hospital (YNHH) .....	6
Business Goal and Constraints .....	7
Technical Goals .....	7
Network Applications .....	9
YNHH Departments.....	9
User Communities .....	10
Data Stores .....	12
Network Topology .....	13
Traffic Flow .....	14
<b>Phase 2: Logical Network Design</b>	
Logical Network Design .....	18
Designing a Network Topology .....	18
The Core Layer.....	19
The Distribution Layer .....	20
The Access Layer .....	20
LAN Topology.....	21
WAN Topology .....	22
IP Addressing and DNS .....	23
IP Addressing .....	23
Condition need to take consideration .....	24
Server .....	25
Printer & Scanner .....	25
DNS Naming.....	25
Routing and Switching .....	26
Switching .....	26
Routing .....	26
Security .....	27
Security Risk .....	28
Security Policy .....	28
Security Mechanism .....	28
ACL .....	29
Securing Wireless Networks .....	29
Network Management.....	29
<b>Phase 3: Physical Network Design</b>	
Transmission Media Of YNHH .....	32
Bandwidth .....	32
Transmission impairments .....	32
Core Layer Transmission Media SONET .....	33

Distribution Layer Transmission media .....	34
Access Layer Transmission Media .....	34
Device Selection .....	34
Core layer equipment .....	34
Feature and capabilities of equipment in Core Layer ...	34
Distribution Layer Equipment (WAN) .....	34
Access Layer Equipment (LAN) .....	34
<b>Phase 4: Testing</b>	<b>35</b>
Testing .....	35
Appendices :	
LAN in AWS.....	41
Switching Configurations.....	78
References.....	82

## **Introduction:**

### **Yale New Haven Hospital (YNHH)**

Yale New Haven Hospital was founded as the General Hospital Society of Connecticut in 1826. It was founded as a charitable institution for the care of the poor, the role of the hospital soon expanded to include care for the entire community. YNHH is regularly included among the Best Hospitals in the U.S. in the annual U.S. News & World Report rankings of specialty services. With two main campuses, Yale New Haven is the largest acute care provider in southern Connecticut and one of the Northeast's major referral centers. YNHH have several branches in Connecticut including the main and larger hospital in New haven. The three main branches we are going to work with when building a LAN and WAN networks are as following:

- 1)Yale New Haven Hospital in New Haven
- 2)Yale New Haven Health in Bridgeport
- 3)Yale New Haven Shoreline Medical Center in Guilford

### **Yale New Haven Hospital in New Haven:**

Today, YNHH is a 1,541-bed private, non-profit teaching hospital that ranks among the premier medical centers in the nation with approximately 12,991 employees including 4136 medical staff.

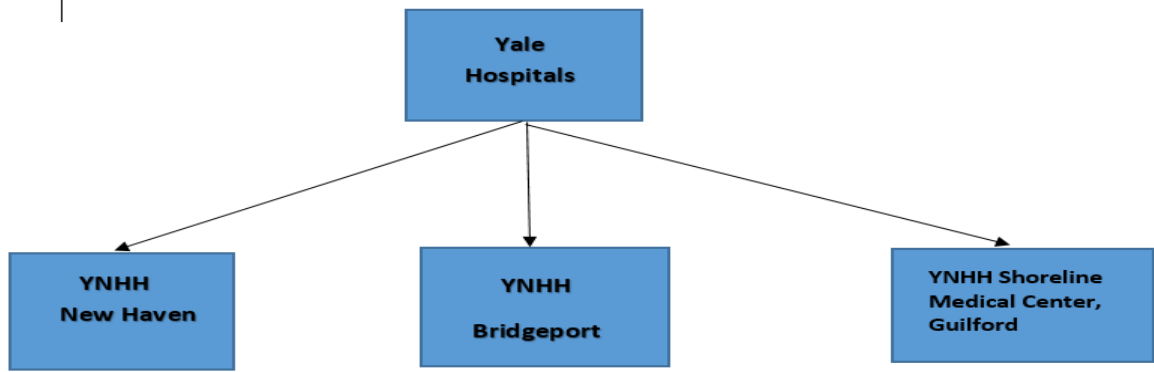
### **Yale New Haven Health in Bridgeport:**

Bridgeport Hospital has 383 licensed beds plus 42 beds licensed under Yale New Haven Children's Hospital, more than 2,600 employees, more than 1100 active physicians representing more than 60 sub-specialties and 230 medical/surgical residents and fellows in programs affiliated with Yale School of Medicine.

### **Yale New Haven Shoreline Medical Center in Guilford:**

YNHH Shoreline Medical Center in Guilford relies on the skill and expertise of more than 4,500 university and community physicians and advanced practitioners, including more than 600 resident physicians, Yale New Haven Hospital (YNHH) provides comprehensive, multidisciplinary, family-focused care in more than 100 medical specialty areas.

In total Yale new haven hospitals in New haven, Bridgeport and Guilford has 2166 number of beds and 19191 employees including community physicians, advanced practitioners, medical/surgical fellows and resident physicians.



**Figure: Three branches of YNHH**

# PHASE 1

## Identifying Customer Needs/ Goals:

### 2. Analysing Business Goals and Constraints:

YNHH is regularly included among the Best Hospitals in the United States. The hospital includes different features. Yale New Haven Health enhances the lives of the people by serving and providing access to high value, patient-centred care. It is committed to innovation and excellence in patient care, teaching, research and service to communities. They are precisely focusing on some values like integrity, patient centred, respect, accountability and compassion.

The business goals included are as follows:

- Improve services and facilities for patients
- Appoint a greater number of doctors
- Allow both patients and visitors to access WLAN
- Conduct research on new diseases
- Provide better financial assistance

### 2.1 Analysing Technical Goals and Constraints:

Yale New Haven Hospital provides better treatment and facilities for their customer or patient. They provide comprehensive, individualized care to every patient who walks through their doors. YNHH not only provides best medical health care system to their customers but also focus on wide range of aspects like teaching, training and research. YNHH serves as the primary teaching hospital for Yale School of Medicine and attracts the brightest young minds in medicine and educate them for medical leadership in clinical practice, teaching. YNHH also providing support and setting for the ongoing clinical research that leads to major medical advances and breakthroughs.

The technical goals included are as follows:

- Provide secure/ private wireless access for doctor and nurses
- Provide open wireless access for the visitors and patient
- Provide hospitals network availability 99.999 sec
- Provide response times 1/10 second for emergency apps
- Provide proper bandwidth to support all application
- Provide much more security for inside network by implementing cisco firewall
- Provide scalability and multimedia applications
- Protect our network from intruders

### 2.2 Availability of downtime in minutes:

**Table 1: Availability of downtime in minutes**

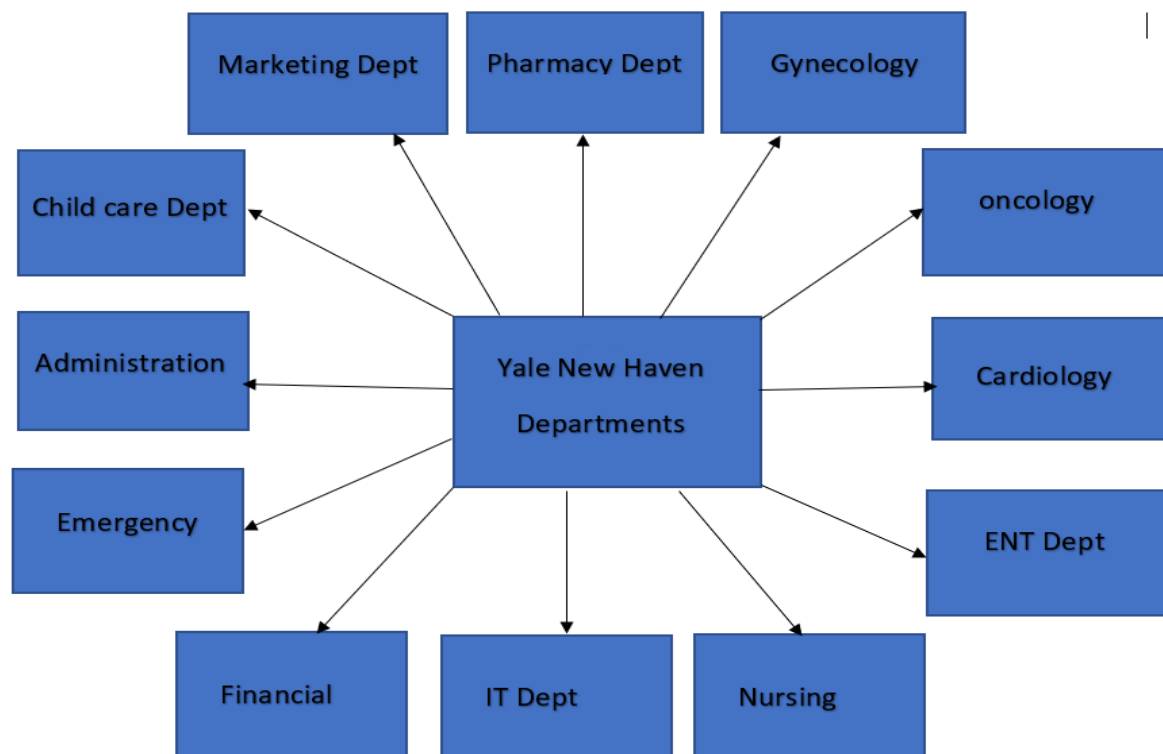
Availability	Downtime per year	Downtime per month
99.999	5.26	0.43
99.99	52.59	4.38

99.95	262.8	21.19
99.9	526.2	43.83
99	5256	438

**Table 2: Availability of downtime in hour/day/week/year in minutes and seconds**

Availability	Per hour	Per day	Per week	Per year
99.999	0.04 sec	0.86 sec	6.05 sec	5.26 min
99.99	0.36 sec	8.64 sec	1.01 min	52.59 min
99.95	1.80 sec	43.20 sec	5.04 min	262.8 min
99.9	3.6 sec	1.44 min	10.08 min	526.2 min
99	36 sec	14.4 min	100.8 min	5256 min

### 3. Yale New Haven Hospital Departments:



**Figure: Yale New Haven Hospitals Departments**



#### 4. Network Applications:

A network application is nothing but is an application which runs on one host and provides communication to another application running on a different host. Network applications use a client-server architecture, where the client and server are two computers connected to the network. The server is programmed to provide some service to the client. The application may use an existing application layer protocols such as HTTP, SMTP. The application may not use any existing protocols and depends on the socket programming to communicate to another application.

These are the Network Applications that our client is using.

- App1 = Web Search
- App2 = Email
- App3 = Appointment
- App4 = CCTV
- App5 = Medicines
- App6 = Laboratory
- App7 = Payroll
- App 8 = Proximity Card
- App 9 = Bandwidth Management
- App10 = Cloud Applications

#### 5. User Communities:

User Community Name	Size of community	Location of Community	Applications used by community
Administrative Department	80	Administration Block	Email, CCTV, Web Search, Proximity card
Emergency Department	25	Emergency Block	Web search, Email, CCTV, Laboratory, Medicines, Proximity card
Financial Department	30	Payroll Block	Email, Web Search, CCTV, Laboratory
IT Department	15	IT Block	Email, CCTV, Web search, Proximity, Cloud Apps, Bandwidth, Management
Nursing Department	120	Nursing Block	Email, Web Search, CCTV, Laboratory, Medicines, Proximity card.

ENT Department	20	ENT block	Email, Web Search, Laboratory, Proximity, Medicines, CCTV, Appointment/Catalog.
Cardiology Department	15	Cardiology Block	Email, Web Search, Laboratory, CCTV, Medicines, Appointment/Catalog, Proximity card.
Gynaecology Department	15	Gynaecology Block	Email, Web Search, Laboratory, CCTV Medicines, Proximity, Appointment/Catalog.
Oncology Department	20	Oncology Block	Email, Web Search, Medicines, CCTV, Laboratory, Proximity card.
Pharmacy Department	40	Pharmacy Block	Web Search, Email, Laboratory, Medicines, CCTV, Proximity card.
Marketing Department	50	Marketing Block	Email, Web Search, CCTV Medicines, Proximity card.
Child care Department	25	Child Health Department	Email, Web Search, Laboratory, CCTV, Medicines, Proximity, Appointment/Catalog.
Patients/Visitors	1500	All	Email, Web Search, Appointment/Catalog, Medicines, Laboratory

## 6. Data Stores

A datastore is a repository for storing, managing and distributing data sets on an enterprise level. It is a broad term that incorporates all types of data that is produced, stored and used by an organization. The term references data that is at rest and used by one or more data-driven applications, services or individuals.

Depending on the organization, a datastore may be classified as an application-specific datastore, operational data store or centralized datastore. Moreover, a datastore may be designed and implemented by using purpose-built software or through typical database applications. Most of the servers can be accessed by the all departments, but some of them are restricted. And all servers will be located in IT department.

1. **Windows File/Print Server** is used for supporting enterprise level applications such as for data storage applications, security, networking and for further improvements.
2. **Windows Web Server** is a http application used for accessing the static web pages by all the departments. It provides access compatibility, ease of usage for employees.

3. **Mail Server is an Outlook express** which restricts visitors from using and email system is a secure, private and confidential mode of information transmission.
4. **DNS Server:** .dns is a Named file, Reverse Zone, Forward Zone application [www.ynhh.org](http://www.ynhh.org) and can be accessed by all the departments.
5. **DHCP Server** is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices and can be used by all departments.
6. **Proximity Server** is a Card reader application which can be accessed by all departments except visitors.
7. **Database Server SQL** is a Citrix application and can be accessed by all departments.
8. **Proxy Server (LINUX)** is a gateway and can be accessed by all departments.
9. **Windows Hospital Management Server** is an MSI application and can be accessed by every department except visitors.
10. **CCTV Server** (Standalone DVR) is a DVR application and can be accessed by every department except visitors.
11. **Data backup Server** is a backup application and can be accessed by every department except visitors.
12. **PACS Server** which stores a database containing the images, and of multiple clients that can retrieve and display these images on medical imaging software, can be used by all departments except visitors.

**Table 4: Data Stores**

Data Store	Location	Application	Used by user community
Windows File/ Print server	IT Department	Office application	All
Windows Web Server	IT Department	http	All
Mail Server	IT Department	Outlook express	All except visitors
DNS Server	IT Department	Named file Reverse zone Forward zone <a href="http://www.ynhh.org">www.ynhh.org</a>	All

DHCP Server	IT Department	boot. p file, Dhcpd Range of network /scope	All
Proximity Server	IT Department	Card reader	Except visitors and guest
Database Server SQL	IT Department	Apps, Citrix	All
Proxy Server (LINUX)	IT Department	Gateway	All
Windows Hospital Management Server	IT Department	MSI application	Except visitors
CCTV Server (Stand Alone DVR)	IT Department	DVR applications	Except visitors
Data Backup Server	IT Department	Backup	Except Visitors
PACS Server	IT Department	Storing Images	Except Visitors

## 7. Network Topology:

Yale New Haven Hospitals is located in 3 different areas, so we have been using three layer 3 in each destination. ISP provide connection to main layer 3 switch in each area which works as layer three technology. Main layer 3 switch works as a gateway of our network. In our LAN network main layer 3 switch gets connected to two different switches which are in Administration and IT departments. In case of failure of one switch, the other one acts as backup for all (HA pair). All switches in each department connected through mesh topology.

## Traffic flow:

Traffic flow, packet flow or network flow is a sequence of packets from a source computer to a destination, which may be another host, a multicast group, or a broadcast domain. A flow could consist of all packets in a specific transport connection or a media stream.

Name of user community	Number of users	Application	Total Bandwidth
------------------------	-----------------	-------------	-----------------

Administrative Department	80	Email =180Kbps CCTV =173.7 Kbps Web Search=288 Kbps Proximity card=150 Kbps	29.49Mbps
Emergency Department	25	Web Search=288 Kbps Email=180Kbps CCTV=173.7 Kbps Laboratory=101 Kbps Medicines=120 Kbps Proximity Card=150 Kbps	30.12Mbps
Financial Department	30		10.69Mbps
IT department	15	Email=180Kbps CCTV=173.7 Kbps Web search=288 Kbps Proximity card=150 Kbps Cloud apps=7168 Kbps Bandwidth management=120 Kbps	36.81Mbps
Nursing Department	120	Email=180Kbps Web search=288 Kbps CCTV=173.7 Kbps laboratory=101 Kbps Proximity card=150 Kbps Medicines=120 Kbps	30.12Mbps
ENT Department	20	Email=180Kbps Web search=288 Kbps CCTV=173.7 Kbps laboratory=101 Kbps Proximity card=150 Kbps Medicines=120 Kbps Appointment=101 Kbps	30.3Mbps
Cardiology Department	15	Email=180Kbps Web search=288 Kbps Laboratory=101 Kbps CCTV=173.7 Kbps medicines=120 Kbps Proximity card=150 Kbps Appointment=101 Kbps	12.4 Mbps
Gynaecology Department	15	Email=180Kbps Web search=288 Kbps Laboratory=101 Kbps CCTV=173.7 Kbps	14.2 Mbps

		medicines=120 Kbps Proximity card=150 Kbps Appointment=101 Kbps	
Oncology Department	20	Email=180Kbps Web search=288 Kbps Laboratory=101 Kbps CCTV=173.7 Kbps medicines=120 Kbps Proximity card=150 Kbps	30.12Mbps
Pharmacy Department	40	Email=180Kbps Web search=288 Kbps Laboratory=101 Kbps CCTV=173.7 Kbps medicines=120 Kbps Proximity card=150 Kbps	30.12Mbps
Marketing Department	50	Email=180Kbps Web search=288 Kbps CCTV=173.7 Kbps medicines=120 Kbps Proximity card=150 Kbps	9.9Mbps
Child Care Department	25	Email=180Kbps Web search=288 Kbps Laboratory=101 Kbps CCTV=173.7 Kbps medicines=120 Kbps Proximity card=150 Kbps Appointment=101 Kbps	30.3Mbps
Patients/Visitors	1500	Email=180Kbps Web search=288 Kbps Appointment=101 Kbps Medicines=120 Kbps Laboratory=101 Kbps	30.3Mbps

#### Calculating bandwidth for each Department:

Administration Department= 80 users

Bandwidth=  $\{[(280+180+150) * 80] + (28880*5)\}$  Kbps = 193.2 Mbps

Emergency Department= 25 users

Bandwidth=  $\{[(250+180+150+380) * 25] + (28880*5)\}$  Kbps =161.8 Mbps

Financial Department= 30 users

Bandwidth=  $\{[(280+180+150) * 30] + (28880 * 10) = 7200 * 5\}$  Kbps = 307.1Mbps

IT Department=15 users

Bandwidth=  $\{[(280+180+150+120) * 15] + (28880 * 5) + 7200 * 5\}$  Kbps = 191.3 Mbps

Nursing Department =120 users

Bandwidth=  $\{[(280+180+150+250+380) * 120] + (28880 * 5)\}$  Kbps = 293.2Mbps

ENT Department=20 users

Bandwidth=  $\{[(280+180+150+250+380+180) * 20] + (28880 * 10)\}$  Kbps= 317.2Mbps

Cardiology Department= 15 users

Bandwidth=  $\{[(280+180+150+250+380+180) * 15]\}$  Kbps= 21.3 Mbps

Gynaecology Department= 15 users

Bandwidth=  $\{[(280+180+150+250+380+180) * 15]\}$  Kbps= 21.3 Mbps

Oncology Department =20 users

Bandwidth=  $\{[(280+180+150+250+380) * 20] + (28880 * 5)\}$  Kbps=169.2 Mbps

Pharmacy Department= 40 users

Bandwidth=  $\{[(280+180+150+250+380) * 40] + (28880 * 5)\}$  Kbps= 194 Mbps

Marketing Department=50 users

Bandwidth=  $\{[(280+180+150+380) * 50]\}$  Kbps= 49.5 Mbps

Child Care Department=25 users

Bandwidth=  $\{[(280+180+150+250+380+180) * 25] + (28880 * 5)\}$  Kbps = 179.9 Mbps

**Total Bandwidth =2.09Gbps**

# PHASE 2



## Logical Network Design:

The three branches of Yale hospital in the state of Connecticut are connected through Internet Service Provider (ISP). Yale hospitals have 4,200 users, based on this the ISP provide a range of 172.168.0.0 to 172.16.5.255 (Class B). Yale New Haven hospital is the Headquarter of all the Yale hospital branches. Yale New Haven hospital has 1400 employees and 5000 patients. Headquarter have three buildings that are in New Haven. The three branches are New Haven (NH), Bridgeport and Guilford. There are four buildings in Yale New Haven hospital and they are North Building(Main Building), South Building, East Building and West Building. The following departments such as Administration, Emergency, Financial, IT, Nursing, Pharmacy, Child car department Gynaecology are situated in North Building. Administration, Emergency, Financial, IT, Nursing, Pharmacy, Oncology, Marketing are situated in South building. Administration, Emergency, Financial, IT, Nursing, Pharmacy, cardiology is situated in West Building. Administration, Emergency, Financial, IT, Nursing, Pharmacy, ENT are situated in East building. There is also a remote router in Yale New Haven Hospital to provide access to the remote users through VPN connection. All servers situated in North building in New haven.

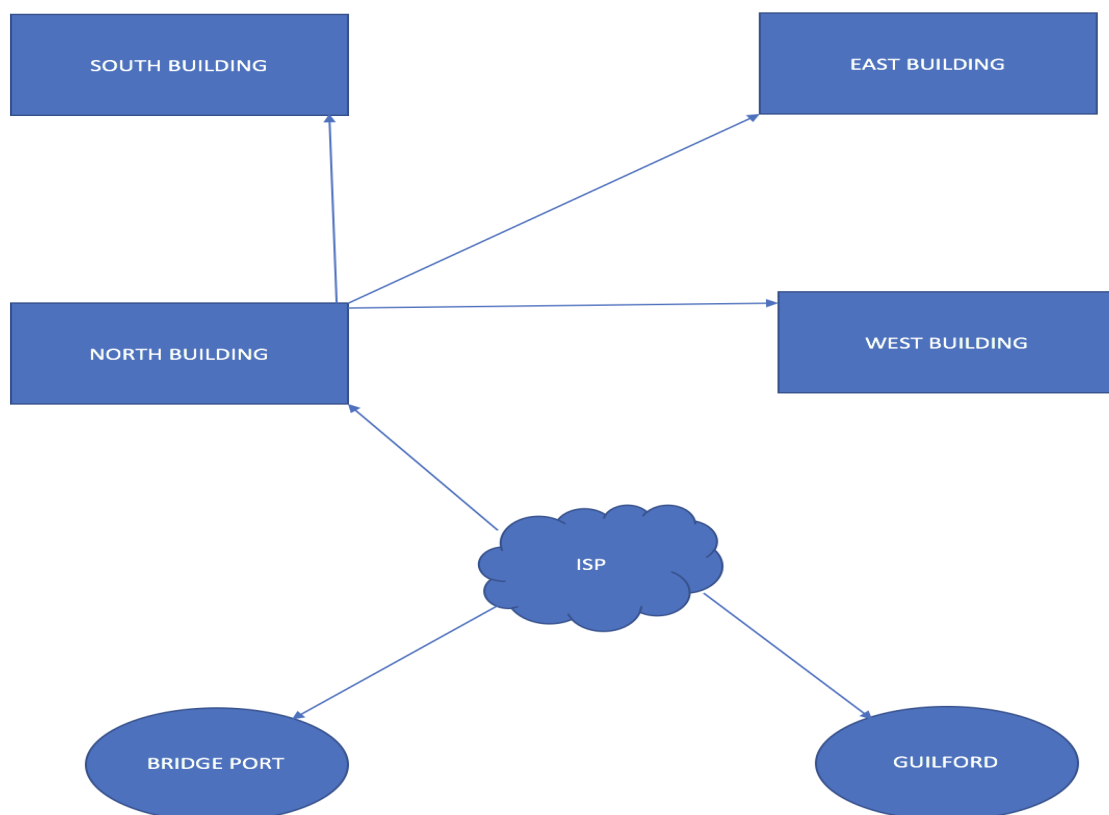


Figure: Logical Diagram of YNHH

Topology is a structure of network that is designed to show where the physical components are installed. It is also structure of network that is designed to illustrates on how the communication take places in terms of data flow. Logical network is the first step to design to any enterprise network. Yale hospitals implementing the hierarchical network model to have following advantages.

Yale New Haven hospital has a capability of 12,000 IP addresses, right now there are only 4200 IP addresses are in use. The remaining are stored for the future use.

With hierarchical network model, scalability, redundancy, modularity and security are easier to maintain. A hierarchical model is used to design in every sector of the organization to get the better performance from the network.

The Yale New Haven Hospital hierarchical model has three types Access Layer, Distribution Layer and Core Layer. Some basic principles are followed to design a successful network such as Hierarchy, Modular, Resilience and Flexibility. The hierarchical design provides three different layers, where each layer provides a specific function, its role over the entire network design. This model can be implemented in both LAN and WAN. The three layer of the Cisco hierarchical model are as follow:

#### **The Core layer:**

The core layer is responsible for transporting large amounts of traffic both reliably and quickly. The only purpose of the network's core layer is to switch traffic as fast as possible. It is used to prevent slowing down the switching process. The core layer should not be burdened with security or traffic control measures or any unnecessary additional equipment. The primary device at this layer is a high-end layer 3 switch essentially the backbone of the network.

In the Core layer, network devices required more memory, processor and bandwidth, so Cisco Catalyst 9200 48 Port layer 3 Switch will be matched this requirement. The switch (172.168.0.0/25) is connected to ISP through PPP (Point to Point Connection) in the core layer. The gateway IP is 172.168.0.1. The layer 3 switch connected to other three buildings through the Layer 2 switches which are in distributed layer. Some of the Core function would include:

- Access List checking
- Data encryption
- Address translation

#### **The Distribution Layer:**

The distribution layer is referred to as the workgroup layer and is the major communication point between the access layer and the core. The primary function of the distribution layer is to provide routing, filtering, and WAN access and to determine how packets can access the core, if needed. The IP addressing hierarchy is managed at this layer. IP addressing is the process of assigning unique IP addresses to devices on the network. Typically involves routers and includes all of the router functions and Provides almost all of the connectivity tasks. It Implements network policies, and provides many networking services such as:

- Network Address Translation (NAT)
- Firewall protection and
- Quality of service (QoS).

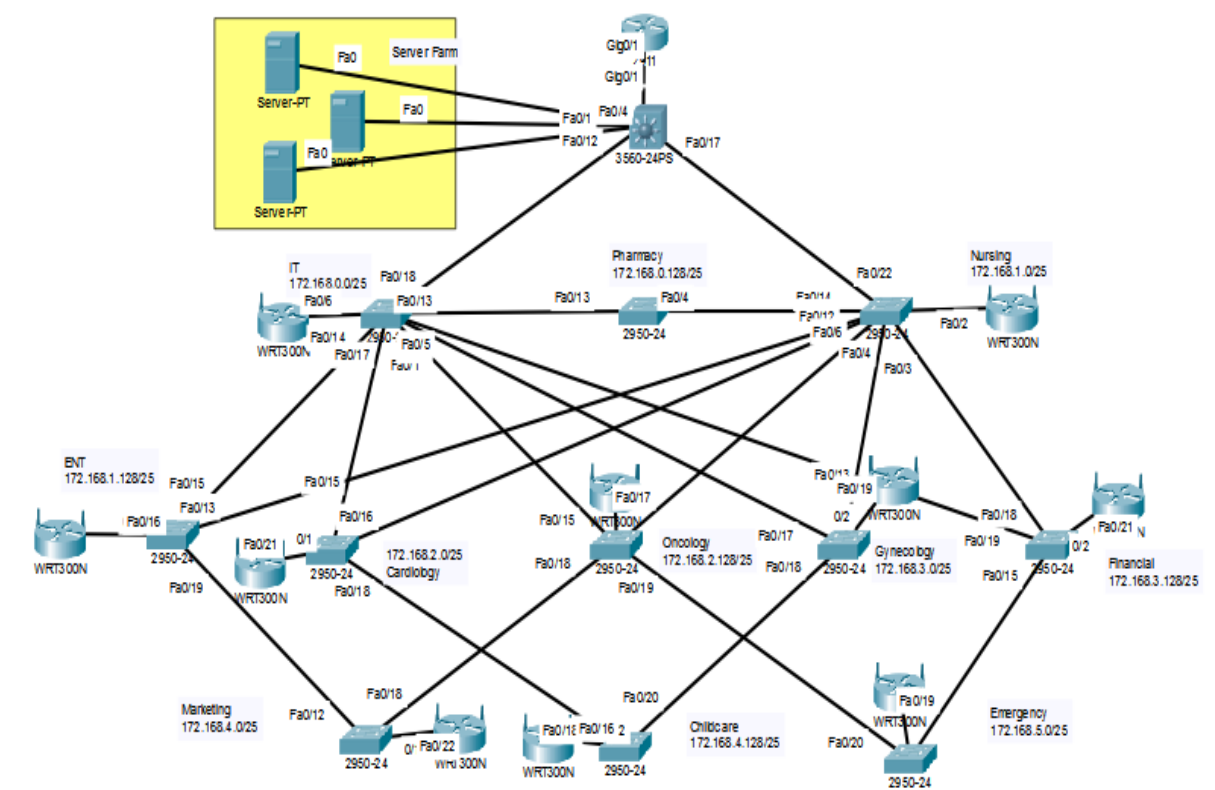
In distribution layer, network devices don't require much memory, processors, and bandwidth. Cisco switch SG 300-52P Layer 2 Switch used in distribution layer for cost effective. East building user are using up to 2.45 Gbps Bandwidth. North building user are using 2.85 Gbps bandwidth and West building users are using 2.67 Gbps Bandwidth and South building users are using 2.90 Gbps Bandwidth as well. In Distribution Layer, all the routers are connected through Partial Mesh Topology.

### The Access layer:

It controls user and workgroup access to the resources on the network. This layer usually incorporates Layer 2 switches and access points that provide connectivity between workstations and servers. You can manage access control and policy, create separate collision domains, and implement port security at this layer. Sometimes called the desktop layer because it deals with connecting workstations to the network

The LAN connection provides 10/100 Mbps connection speed. All servers are situated in New Haven branch and separated by Cisco ASA Firewall. All server IPs are static.

### Lan Design:



## **LAN Topology:**

LAN topology works with Access layer. Three Switches from each building connected to Layer 3 switch in Main building New Haven.

The North Building is connected with 10/100 Mbps switch. There are total eight department in this building. In every department, all users connected to a switch. There are total Eight switches in North building and can carry 10/100 Mbps. All these eight switches connected each other as partial mesh topology. In North building, total 1400 users sharing 2.45 Gbps data of our network. The main IT department located in North building where all servers are configured/separated as DMZ(Demilitarized Zone).

A DMZ is an interface that sits between a trusted network segment and an untrusted network segment (Internet), providing physical isolation between the two networks enforced by a series of connectivity rules within the firewall. The physical isolation aspect of a DMZ is important because it enables Internet access only to the servers isolated on the DMZ and not directly into the internal network. The biggest benefit to a DMZ is in isolating all unknown Internet requests to the servers on the DMZ and no longer allowing them into the internal network. However, some additional benefits to deploying a firewall with a DMZ can help better understand what happens in the network and thereby increases security.

The South Building is connected with 10/100 Mbps switch. There are total eight department in this building. In every department, all users connected to a switch. There are total Eight switches in North building and can carry 10/100 Mbps. All these eight switches connected each other as partial mesh topology. In North building, total 2250 users sharing 2.90 Gbps data of our network.

The West Building is connected with 10/100 Mbps switch. There are total eight department in this building. In every department, all users connected to a switch. There are total Eight switches in North building and can carry 10/100 Mbps. All these eight switches connected each other as partial mesh topology. In North building, total 2000 users sharing 2.67 Gbps data of our network.

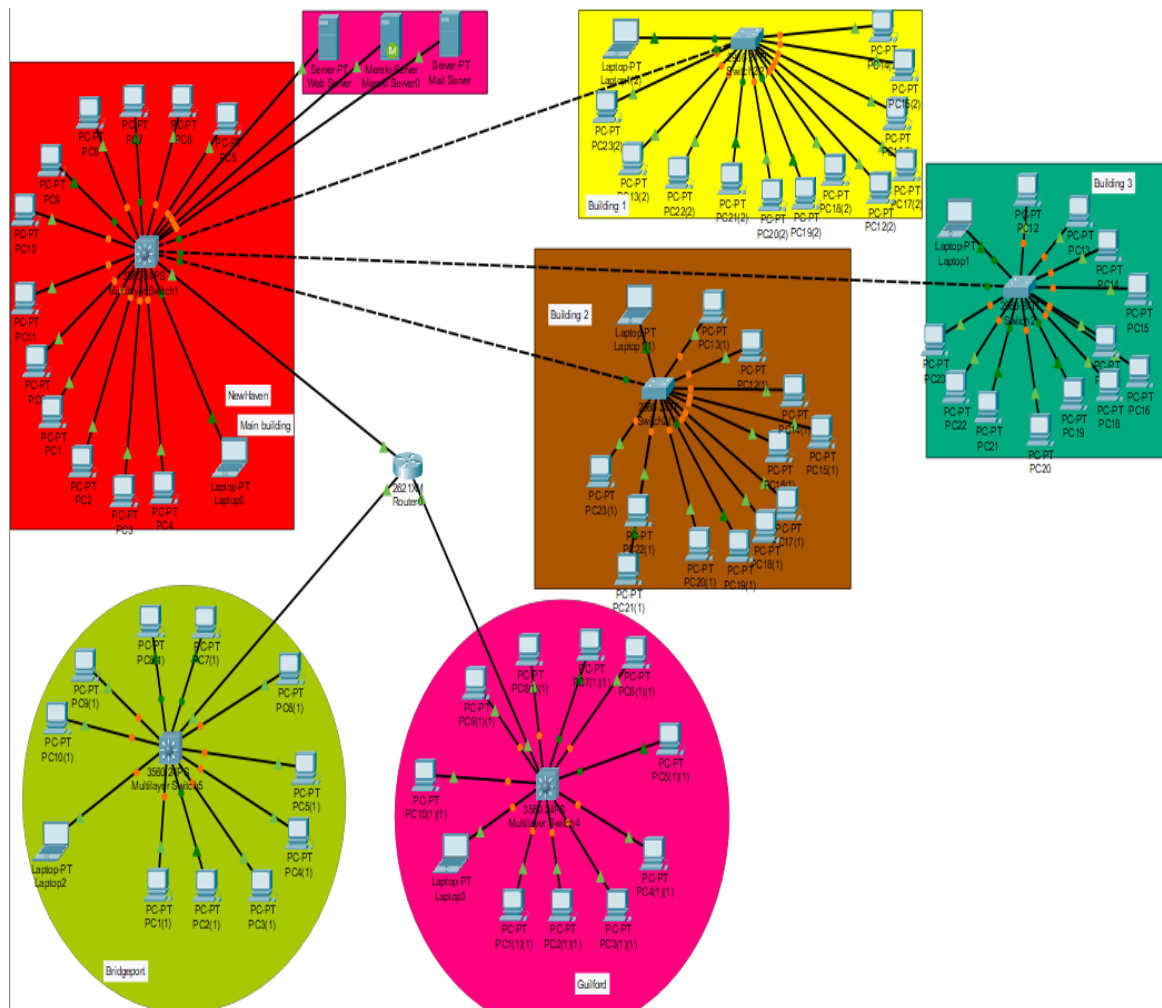
The East Building is connected with 10/100 Mbps switch. There are total eight department in this building. In every department, all users connected to a switch. There are total Eight switches in North building and can carry 10/100 Mbps. All these eight switches connected each other as partial mesh topology. In North building, total 1500 users sharing 2.45 Gbps data of our network.

All switches of these four buildings connected to Layer 3 Switch. This router connected to ISP router (Core router) and get connected to the internet.

## **WAN Topology:**

A wide area network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, including local area networks (LAN) and metro area networks (MAN). In WAN topology, all branches of different cities are connected through ISP. We are using Layer 3 Switches for cost efficient because not needed much memory and processor in distribution layer. The router is configured as Point to Point Connection. In every branch Cisco ASA firewall will be configured as IDS/IPS to protect

from outside. In every branches and Head Office, Cisco ASA firewall will be configured as Intrusion Detection System as well as Intrusion Prevention System (IDS/IPS) to protect each of the Mail Server, Active Directory Server 2012, DNS server, DHCP server, File Server, Print Server, FTP server, Web Server, SQL Server, Proximity Server, Proxy Server, CCTV server from different types of malicious activity and port hacking.



## IP Addressing and DNS

### IP Addressing:

Every device in the network needs IP address to get connected with internet. In our network, all the devices are using IP address such as router, switches, network printer, wireless router to run the network. In our network, we are using IP4 address to get connected to the rest of the world.

As we know, we must buy public IP address from ISP (Internet Service Provider). In our network, we are using both public and private IP address. Public IP is only using to get connected from our Head Office to ISP and all the branch office are using private IP inside private network. Public IP addresses will be issued by an Internet Service Provider and will have number ranges from 1 to 191 in the first Octet. We have decided to take Class B IP for our purpose from the Internet Service Provider. Class B IP address ranges from 172.168.0.0 to 172.168.5.255.

The Private IP address that we have decided to use from 172.16.0.0 to 172.16.255.255. The IPs are assigned to devices as either static and dynamically. We have decided to use static private IP address for every server which are maintained by IT department. For rest of the network IPs will be allocated by DHCP server dynamically.

#### **IP Address ranges:**

#### **IPv4 Addressing**

##### **IP Class: Class B**

**IP Address: 172.168.0.0**

**Subnet Mask:255.255.255.128**

**CIDR value: 25**

**Usable IP host range: 172.168.0.1 - 172.168.0.126**

Network Address	Usable Address	Broadcast Address
172.168.0.0	172.168.0.1 - 172.168.0.126	172.168.0.127
172.168.0.128	172.168.0.129 - 172.168.0.254	172.168.0.255
172.168.1.0	172.168.1.1 - 172.168.1.126	172.168.1.127
172.168.1.128	172.168.1.129 - 172.168.1.254	172.168.1.255
172.168.3.0	172.168.3.1 - 172.168.3.126	172.168.3.127
172.168.3.128	172.168.3.129 - 172.168.3.254	172.168.3.255
172.168.4.0	172.168.4.1 - 172.168.4.126	172.168.4.127
172.168.4.128	172.168.4.129 - 172.168.4.254	172.168.4.255
172.168.5.0	172.168.5.1 - 172.168.5.126	172.168.5.127
172.168.5.128	172.168.5.129 - 172.168.5.254	172.168.5.255

**Condition need to take consideration:**

Our head quarter is situated in Newhaven where 1150 employees and 5000 patients are using different types of devices to get access to our network. Keeping consideration for scalability we should reserve some IP for our future use. For Dhcp configuration we should allocated private IP address rather than public IP. Public ip are using only main router to ISP connection and rest of the server and other network devices such as printer, scanner, workstation, iPad, laptop, iPhone are using private IP address.

**Devices Types:**

The following devices are used in our network.

**Servers:**

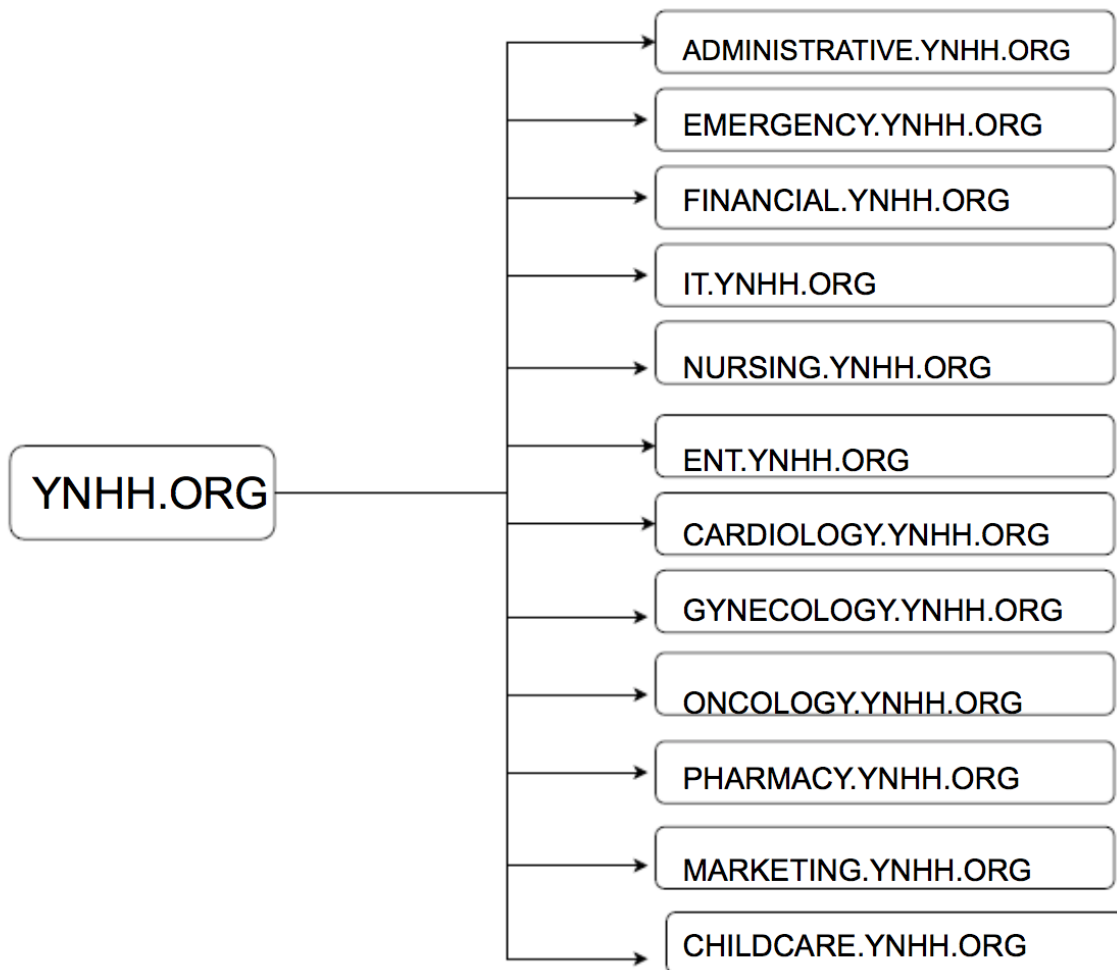
We are using servers such as DNS server, DHCP server, Mail Server, Proxy server, Ftp server, SQL server, print server, backup server, Active Directory (AD) server, Proximity server, Web server, CCTV servers. Most of the servers are situated Headquarter (New Haven). All the server that are using static ip address are separated by DMZ Demilitarized Zone through Cisco ASA Firewall that is connected to Cisco 3600 series router known as distribution layer of YNHH Hospitals.

**Printers & Scanners:**

We assume that there are 212 printers and scanners together.

**DNS Naming:**

Our machine can understand hexadecimal from our domain, but for human it is very difficult to memories all the IP or hexadecimal format number. So, human identify that it requires a naming address rather than IP address to identify the domain name very easily. DNS basically a decentralize naming system for computers that can memorize and translates, domain names to their numerical IP address for locating & identifying computer services and devices underlying a network protocol. System administrator is responsible to make other subdomain under the root domain to the name servers. As we have designing the network for our Yale Hospitals we have planned to categories each department into their individual sub-domain, that should be under a universal domain of [www.ynhh.org](http://www.ynhh.org).



## Routing and Switching:

### Routing:

Router always looking for shortest path of the network. After analysis, the WAN network it has been observed that there are different types of routing protocols have been using in Yale hospital. There are two type of routing protocols:

- Distance Vector
- Link State Protocol

Some of the most common protocols are used in the network:

- OSPF, EIGRP, IS-IS, Rip v1, Rip v2, Static

To branch to branch connection, we have decided to point to point connectivity such as p2p connection. In distribution layer, there are several types of routing protocols have been configured such as OSPF area 0, area 1, area 2, BGP, and also point to point static route. Inside the headquarter all the servers are using static route protocols whereas wireless router is using DHCP protocol such as rip version1 and rip version 2. we have decided to using rip version 2 protocol because as we know that rip version 2 can support VLSM. There have some facilities of VPN (Virtual Private Network) connection for the remote user those who should travel 100 miles far away from our Headquarter.



Now a days routing and switching are very important to maintain network. In the network, all the switches are working in access layer to get connected with the user. In LAN technology, 24 switches are working around three buildings. There are 10 VLAN have been configured for our individual department. we also must configure VLAN Trunking Protocol (VTP). VTP is a Cisco proprietary protocol that propagates the definition of Virtual Local Area Networks (VLAN) overall local area network. To do this, VTP carries VLAN information to all the switches in a VTP domain. VTP advertisements can be sent over 802.1Q, and ISL trunks. The following diagram describe the how the VLAN are connected around our three building inside the head quarter.

### **Applications used in our Network:**

The routing protocol used in this network:

- Rip v2

**Routing Information protocol (RIP):** We have used RIP for network exchange information. It is characterized as interior gateway protocol and is used in small and medium sized networks. It uses hop count as the routing metric for finding the best path between source and destination. The path with the lowest hop count is considered as the optimized route. It prevents routing loops by limiting the number of hops allowed in a path from source and destination.

**Multilayer switch:** In our network, we have used a multilayer switch for high performance. A multilayer switch can function as router and switch at high speed. It can inspect the data packet at a deeper level i.e., at a packet level or segment level.

**Spanning-Tree Protocol (STP):** It prevents loops from being formed when switches or bridges are interconnected via multiple paths. Spanning-Tree Protocol implements the 802.1D IEEE algorithm by exchanging BPDU messages with other switches to detect loops, and then removes the loop by shutting down selected bridge interfaces. This algorithm guarantees that there is one and only one active path between two network devices.

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on bridges and switches. The specification for STP is IEEE 802.1D. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network.

## **SECURITY**

Before designing any network for an organization, we have to have keen insight into security and safety maintenance. The hospital management system also has different problems on safety and security of the network. It follows the 12-step network security design program step by step as follows.

### **Network Security Design follows a 12 Step Program as below:**

#### **1. Network assets**

There are numerous network assets of hospital management system which comes into consideration. Such as

- **Hardware**
- **Software**
- **Applications**
- **Data**

- **Intellectual property**
- **Trade secrets**
- **Company's reputation**

## 2. Security Risks

Now a days every system has security concerns and risks. They are becoming increasingly high day by day. In this scenario the first thing to do is identifying the numerous security risks. Hospital management deals with the sensitive information and huge information about the patient private data every day. In this case there are certain things that come on the way as follows:

- **Hacking:** Hacking is one such issue which can cause lot of damage especially to the hospital system because of the data which is extremely sensitive and private. The data that we are transferring is not encrypted properly in which it results in easy decryption of data in a network in which case the hackers have wide possibility of decrypting the data.
- **Cloud threats:** If a hospital system uses cloud-based services, it should understand exactly what information assets are in the cloud. It then needs to map out which systems, people and processes will need to access those assets. There should be no unnecessary or unrestricted access permissions given to any of them which may be a security threat in the upfront future.
- **Phishing:** These days phishing threats are becoming much more common. This is the problem which occurs when the staff in the hospital open attachments or click on links from which come from unfamiliar senders. In this case the staff should never share personal information or credentials without reading or double checking exactly who the request came from. This threat is becoming more common as doctors share electronic health records Doctors should always closely evaluate any requests that come in for file sharing, ensuring it's a real request from a verified healthcare professional before sending anything, since hackers are getting extremely creative and more convincing every day.
- **Authentication Issues:** In the healthcare industry, biometrics are being increasingly used for access control to drugs and patient records. However, as seen in the UK NHS WannaCry attack, some hospitals that used biometric drug access were unable to access the drugs, and override keys had to be used.

## 3. Security Requirements and Trade-offs

Security trade-offs are one which must be made between security goals and other goals that implies security is valuable to any organization or system, but it always comes with cost. In which case the main things of security trade-offs will be Affordability, Usability, Performance, Availability and Manageability.

The hospital system security trade-offs will be the following:

- **Affordability:** Security is not free of cost as improving security we can require replacement or purchase of new equipment in the hospital, software's, staffing etc, Initial integration costs are just the beginning as going forward costs are also part of the network design. When multiple vendors and products are instituted, the cost of management can be very high due to the complexity.
- **Usability:**
- **Performance:**
- **Availability:**

- **Manageability:**

#### **4. Security Plan**

Maintaining high level standards of security by an organization is always important. The organization issues certain policies/rules to implement by the staff to protect the data from malicious attacks.

#### **5. Security Policy**

Security policy is one which is done after specifying the security plan of the hospital system. In healthcare each and every employee of the hospital which has full access to the company emails and internet facilities they should be educated before ahead about not using any personal information or credentials through the company provided system. A clear and comprehensive computer and Internet usage policy, coupled with proactive monitoring, will ensure a culture of compliance. The hospital IT managers need to take an assertive approach to ensuring that policies are adhered to, since they are ultimately accountable when security leaks result in damage to the hospital reputation.

#### **6. Procedures for applying security policies**

Security procedures implement security policies. Procedures define configuration, login, audit, and maintenance processes. Security procedures should be written for end users, network administrators, and security administrators. Security procedures should specify how to handle incidents (that is, what to do and who to contact if an intrusion is detected). Security procedures can be communicated to users and administrators in instructor-led and self-paced training classes.

#### **7. Technical Implementation Strategy**

#### **8. Achieve buy-in from users, managers, and technical staff**

#### **9. Train users, managers, and technical staff**

#### **10. Implement the technical strategy and security procedures**

#### **11. Test the security**

**and update it if any problems are found**

#### **12. Maintain security**

Security must be maintained by scheduling periodic independent audits, reading audit logs, responding to incidents, performing security testing, training security administrators, and updating the security plan and policy. Network security should be a perpetual process. Risks change over time, and so should security. Cisco security experts use the term security wheel to illustrate that implementing, monitoring, testing, and improving security is a never-ending process.

**Security Topology:** Used DMZ.

#### **ACL:**

The primary reason to apply access control list is to provide a basic level of security for the network. ACLs are not as complex and in depth of protection as firewalls, but they do provide protection on higher speed interfaces where line rate speed is important, and firewalls may be restrictive.

ACLs are a network filter utilized by routers and some switches to permit and restrict data flows into and out of network interfaces. When an ACL is configured on an interface, the

network device analyses data passing through the interface, compares it to the criteria described in the ACL, and either permits the data to flow or prohibits it.

## **Securing Wireless Networks**

Wireless networks are not as secure as wired ones. Without security measures, installing a wireless LAN can pose a serious problem to our network. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network. Therefore, all the devices must be secured properly by installing anti-virus software's and by running personal firewalls.

## **Network Management:**

Network management solutions are key to providing IT administrators the control necessary to support the number of devices accessing the network, and to prioritizing the traffic so mission-critical data gets through.

Some of the major concern that we should consider for the Layer 2 security for implementing, managing and maintaining the network of YNHH Head Quarter. Network Management has been controlled through North Building IT Department where all the servers are located. All the network in YNHH Hospital, also monitoring from IT Department North Building in 4<sup>th</sup>Floort through MRTG, Nagios and network monitoring tools such as Wireshark.

- Devices communicating abnormally can cause security problems for the network. Without a management solution, administrators may never detect small and potentially dangerous malfunctions, therefore constant supervision is necessary.
- The internet service providers (ISPs) was connected to the firewall to control the data exchange from outside to inside the network.
- We have used a dedicated VLAN ID for all the trunk ports in our switches
- Authentication and authorization in the router and firewall md5 authentication are applicable
- If hacker try to enter our network through router or firewall mistakenly, he/she must be wait for another three hours to login those devices
- We have used ACL's to filter the undesirable traffic.

Segregated the network traffic by configuring VLANs for each department.

# PHASE 3

## Transmission Media Of YNHH:

The transmission media are basically used to convey information can be classified as guided or unguided. Guided media provide a physical path along which the signals are propagated, these include twisted pair, coaxial cable, and optical fibre. Unguided media employ an antenna for transmitting through air, vacuum, or water. In YNHH hospital, physical network design we have been using both mediums to improve our network performance

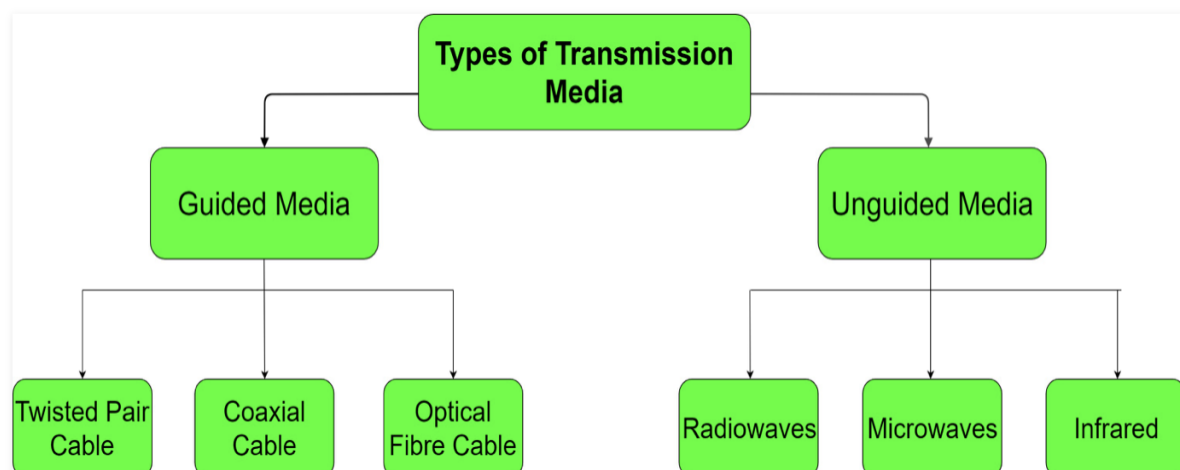
In considering the design of data transmission systems of our hospitals network, key concerns are data rate and distance: the greater the data rate and distance the better. Several design factors relating to the transmission medium and the signal determines the data rate and distance for our hospitals networks are as follows:

### Bandwidth

Bandwidth is the communication capacity of a network. We know that higher the bandwidth, data transfer rate is also higher. Since, the healthcare sector is experiencing explosive growth in bandwidth demand from transmitting MRI images to wearable devices to video consultations, networks must work at higher-than-ever speeds to deliver services that ensure patient safety, we have decided, in our YNHH Hospitals Head Office network, to use 8.5 Gbps of bandwidth.

**Transmission impairments:** Impairments, such as attenuation, limit the distance. For guided media, twisted pair generally suffers more impairment than coaxial cable, which in turn suffers more than optical fibre.

The Following diagram show the types of Communication that are used in Yale Hospitals network.



**Figure: Communication of Yale Hospital Network**

Media Type	Bandwidth	Performance Rate	Error
Unshielded Twisted pair for voice application	1 MHz	Poor to fair	
Coaxial Cable	1 GHz	Good	
Microwave	100 GHz	Good	
Satellite	100 GHz	Good	
Fiber	75 THz	Good	

### **Core Layer Transmission Media SONET:**

Synchronous optical networking (SONET) is a standardized digital communication protocol that is used to transmit a large volume of data over relatively long distances using a fibre optic medium. With SONET, multiple digital data streams are transferred at the same time over optical fibre using LEDs and laser beams. SONET is a product of the American National Standards Institute (ANSI).

SONET supports multiple data streams at the same time. It was designed to provide efficient services in telecommunication systems and therefore became widely adopted. SONET uses standardized rates so that all kinds of organizations can be interconnected.

SONET is using in core network of the Head Quarter Hospitals and it is always used to connect as ring topology of the network. The main purpose of this technology in our hospitals network is used to perform Fiber Channel, HIPPI (high-performance parallel interface) that are typical first-generation optical network, which use fiber as a transmission medium, but do all switching, processing, and routing electronically. The Primary Ring OC-192 provides data speed up to 9.9 Gbps for Yale hospitals Headquarter Network. On the other hand, **Subtending Ring OC-96** data speed up to 4.9 Gbps has been configured for the Yale Hospital branch office and other customer site branches of the network. Ethernet of the YNHH network can run by SONET up to 10 Gbps.

The main internet Connection that we have taken from ISP also using SONET in their internal network. Yale Hospitals also using voice traffic Carrier by using SONET for their respective network

### **Distribution Layer Transmission media:**

In distribution layer, YNHH Hospital consist of different type of transmission media that are using in the WAN network such as Fiber Optic Cable. In YNHH Head Office LAN network fiber optical cable has been using to connect with the three buildings such as South Building, East Building and West Building from North building. Scalability, redundancy and performance always the first concern before deploying this media (fiber cable).

In YNHH Head Office, all the other three buildings users uses 2.09 Gbps bandwidth for each building.

### **Access Layer Transmission Media:**

The access layer plays a very important because it is connected with application layer (Layer-7) where user is using different types of application. The CAT 6 cable are using to connected from pc to switch. YNHH hospitals LAN Ethernet data capacity should be 10/100 Mbps. The access layer basically ensures the delivery of the packet to the user. The data transmission rate cat 6 cable up to 10 Gbps. The UTP CAT 6 cable has been using inside the four buildings from one floor to another floor connection that can support up to 100 meters. In every floor, 20 ports Gigabyte Smart Switch has been using where data capacity Ethernet speed up to 10 Gbps. Switch always provide a faster data rate connectivity in access layer and it breaks the traffic collision by creating individual collision domain in each port. All the switch and computer Ethernet port has been connected through Rj-45 Connector that are using in CAT 6 cabling. In IT department of YNHH hospitals, all the servers are using static ip and all the cabling is of are same technology.

### **Connection and Cable:**

To maintain and support the bandwidth for the proper functioning of the network we have use different types of Connection. The connection that we are used:

LAN: 100Base T Link, 100 Mbps Bandwidth

WAN: 1000Base T link 1 Gbps Bandwidth

Media Type	Bandwidth	Performance Rate	Error
Unshielded Twisted pair for voice application	1 MHz	Poor to fair	
Coaxial Cable	1 GHz	Good	
Microwave	100 GHz	Good	
Satellite	100 GHz	Good	
Fiber	75 THz	Good	



## PHASE 4

## Testing

### Web server

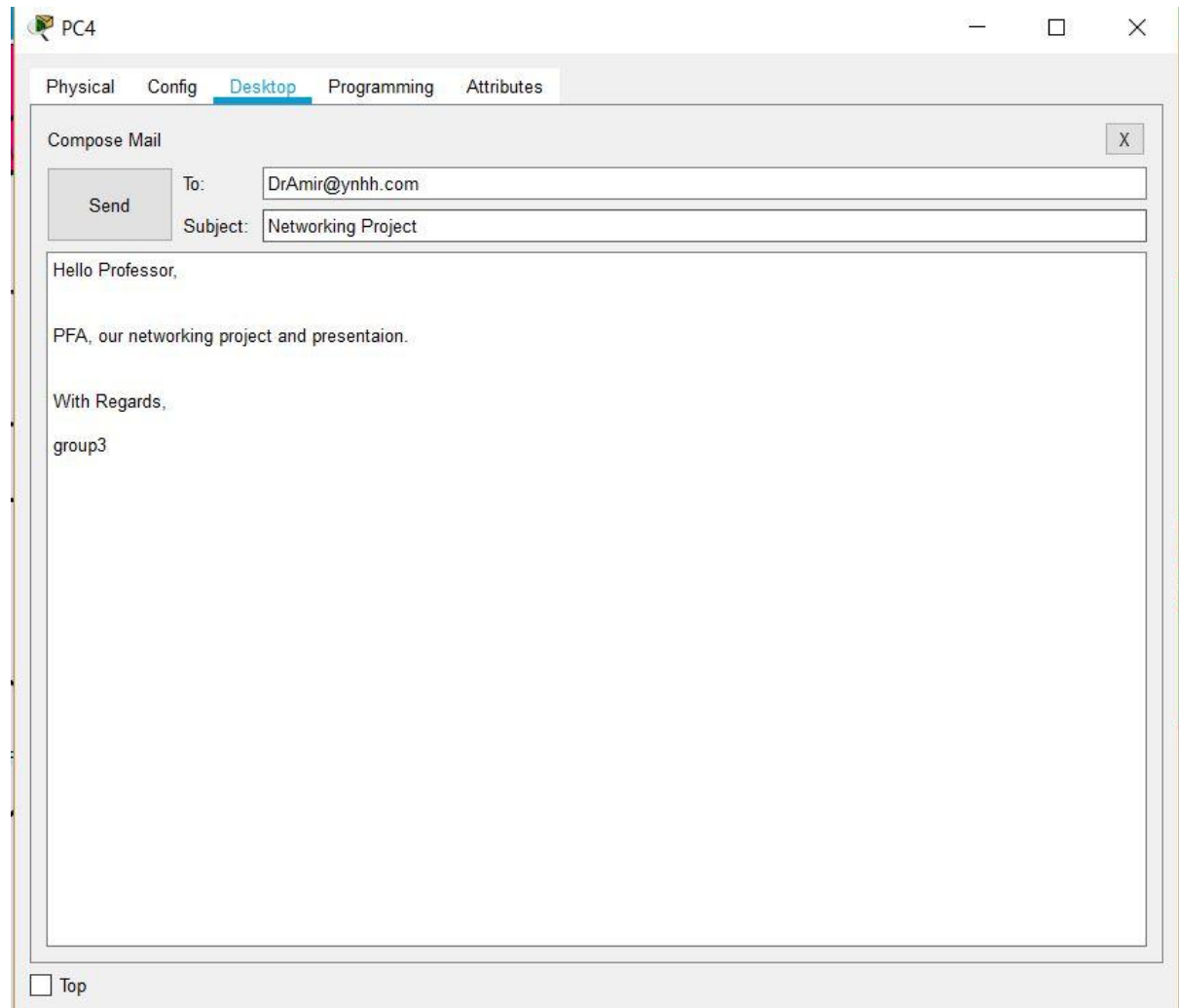
Below is the following web page displayed when we access a web server.



Figure: Web page

## Mail Server

Sending mail from source to destination



The screenshot shows a window titled 'PC4' with standard Windows window controls (minimize, maximize, close). Inside the window, there are four tabs: 'Physical', 'Config', 'Desktop' (which is selected and highlighted in blue), and 'Programming'. Below the tabs is a 'Compose Mail' form. The form has a 'Send' button on the left. To the right of the button are two input fields: 'To:' with the value 'DrAmir@ynhh.com' and 'Subject:' with the value 'Networking Project'. Below these fields is a large text area containing the following text: 'Hello Professor,', 'PFA, our networking project and presentaion.', 'With Regards,', and 'group3'. At the bottom left of the window, there is a checkbox labeled 'Top'.

PC4

Physical Config **Desktop** Programming Attributes

Compose Mail X

Send To: DrAmir@ynhh.com

Subject: Networking Project

Hello Professor,

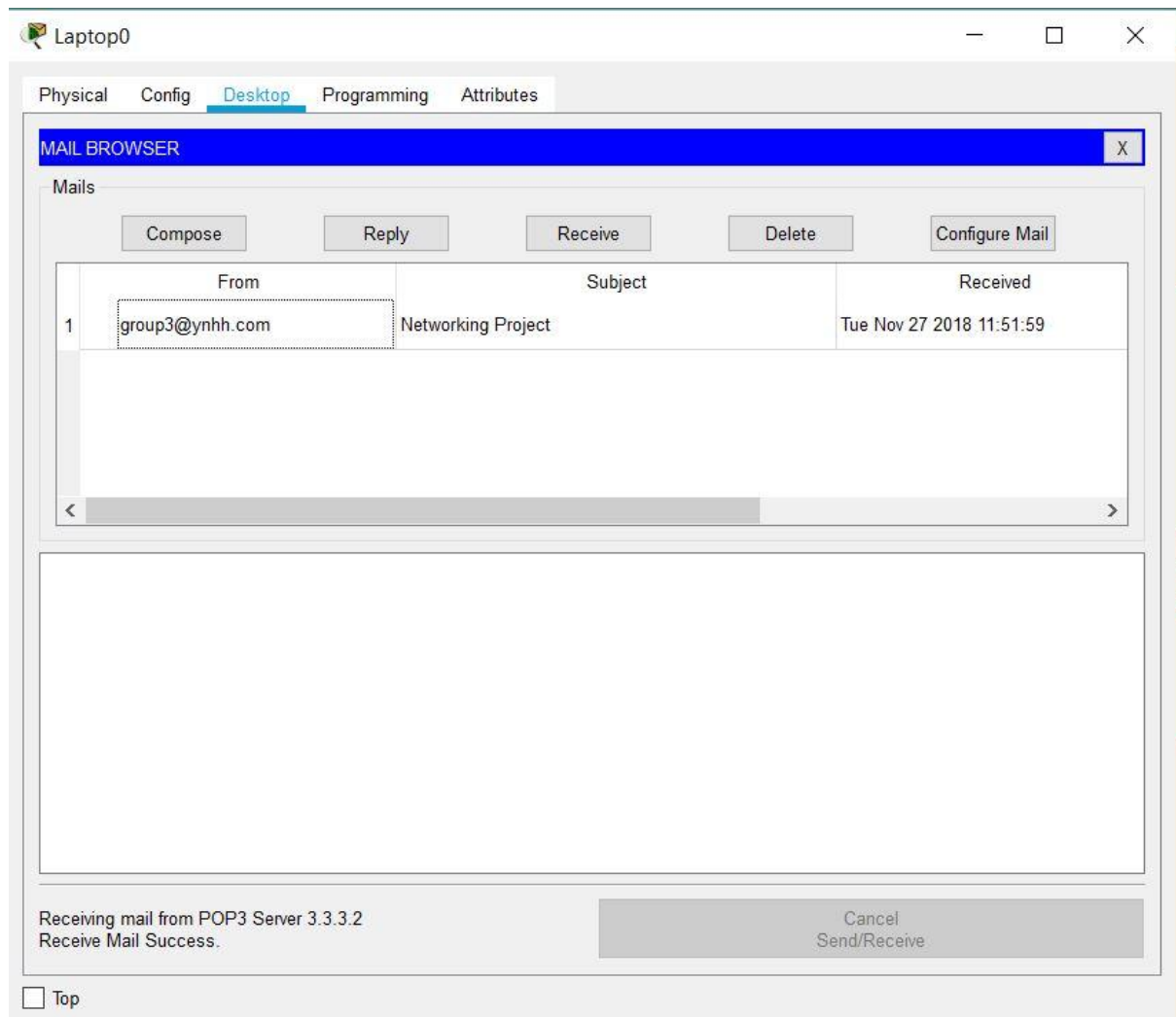
PFA, our networking project and presentaion.

With Regards,

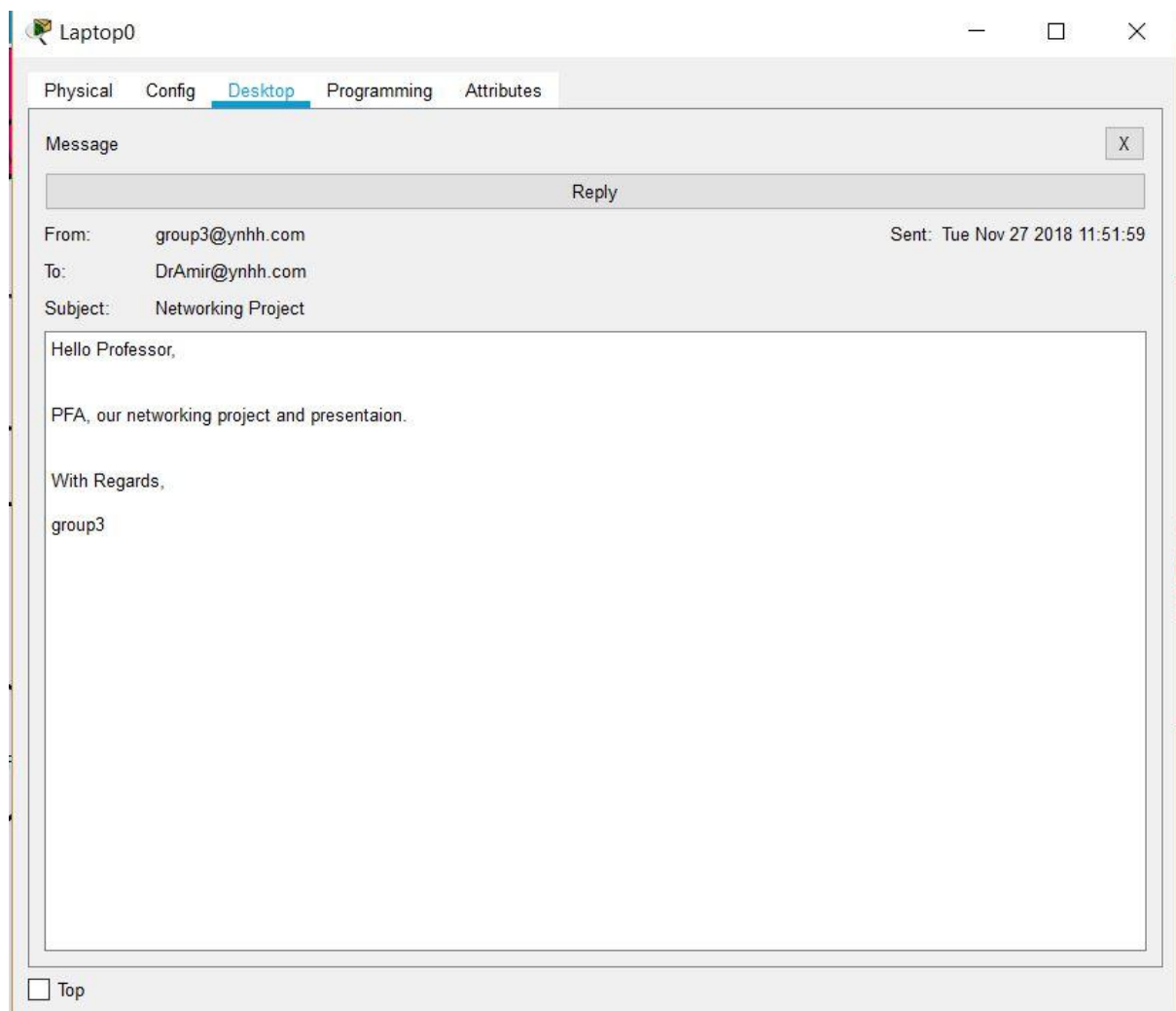
group3

☐ Top

Email sent to destination

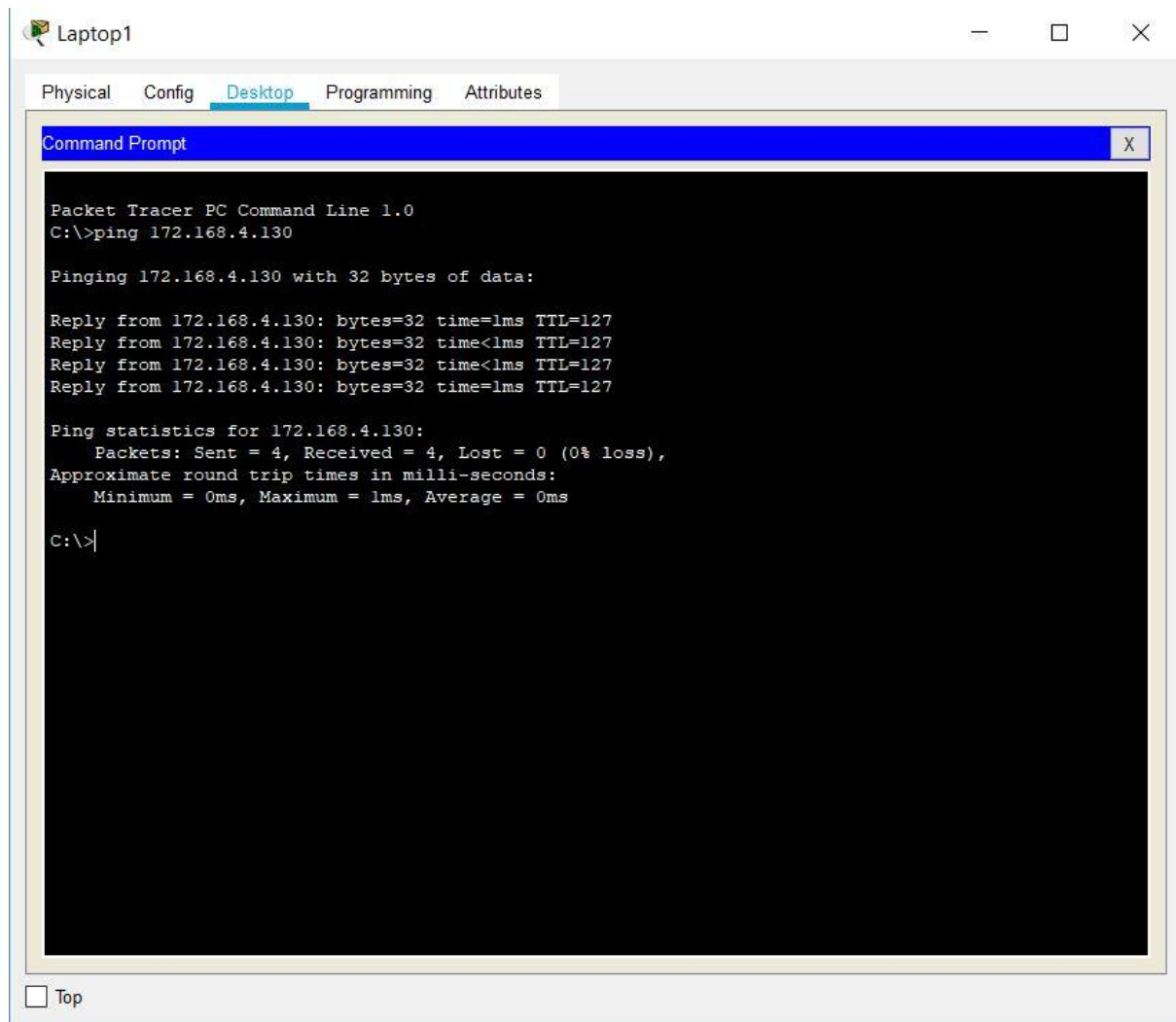


Email reached to destination



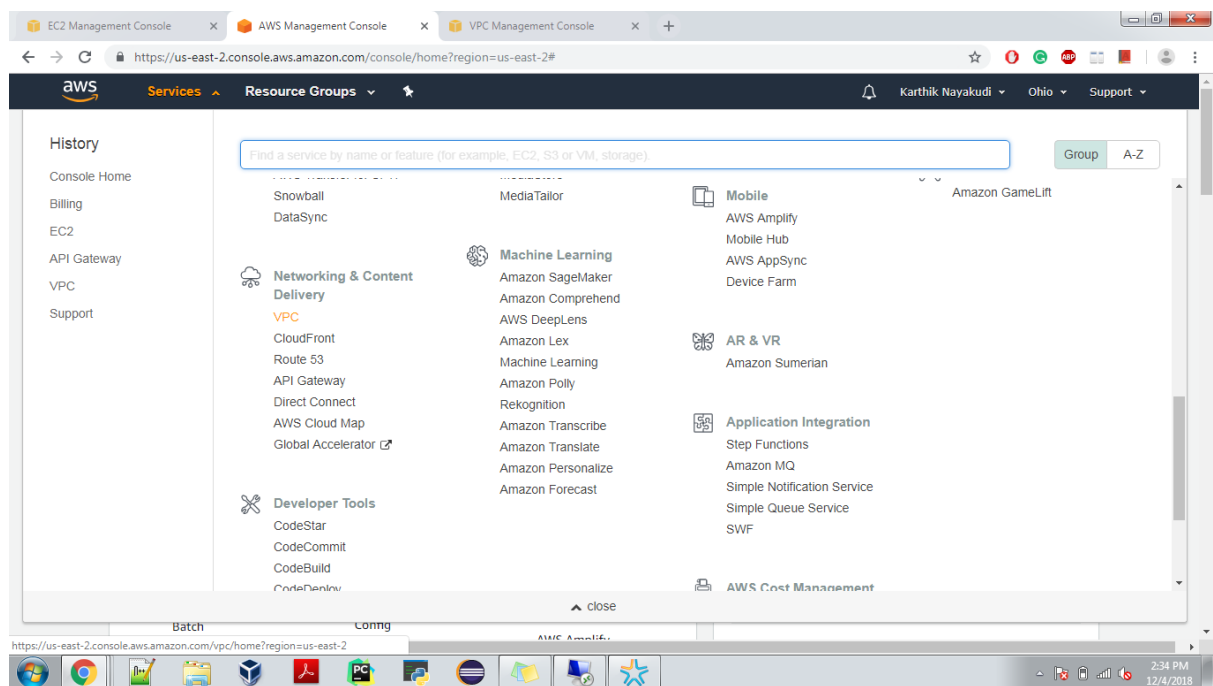
Mail received at destination

Pinging from one system to another system

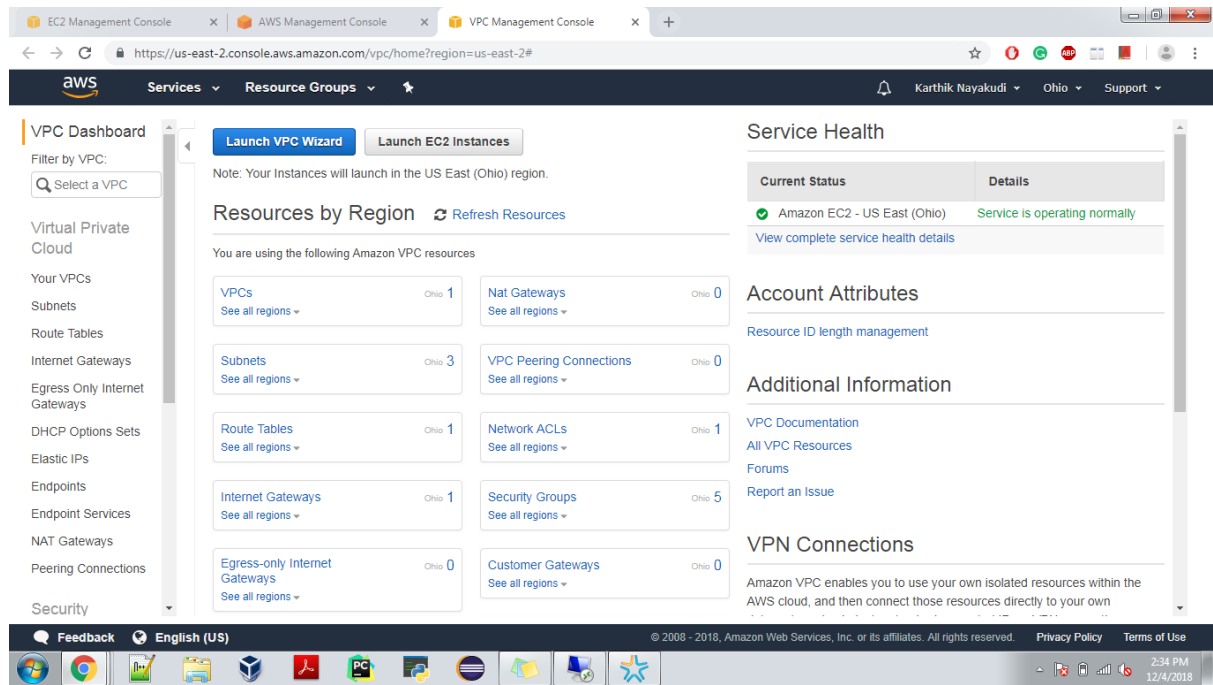


Pinging systems

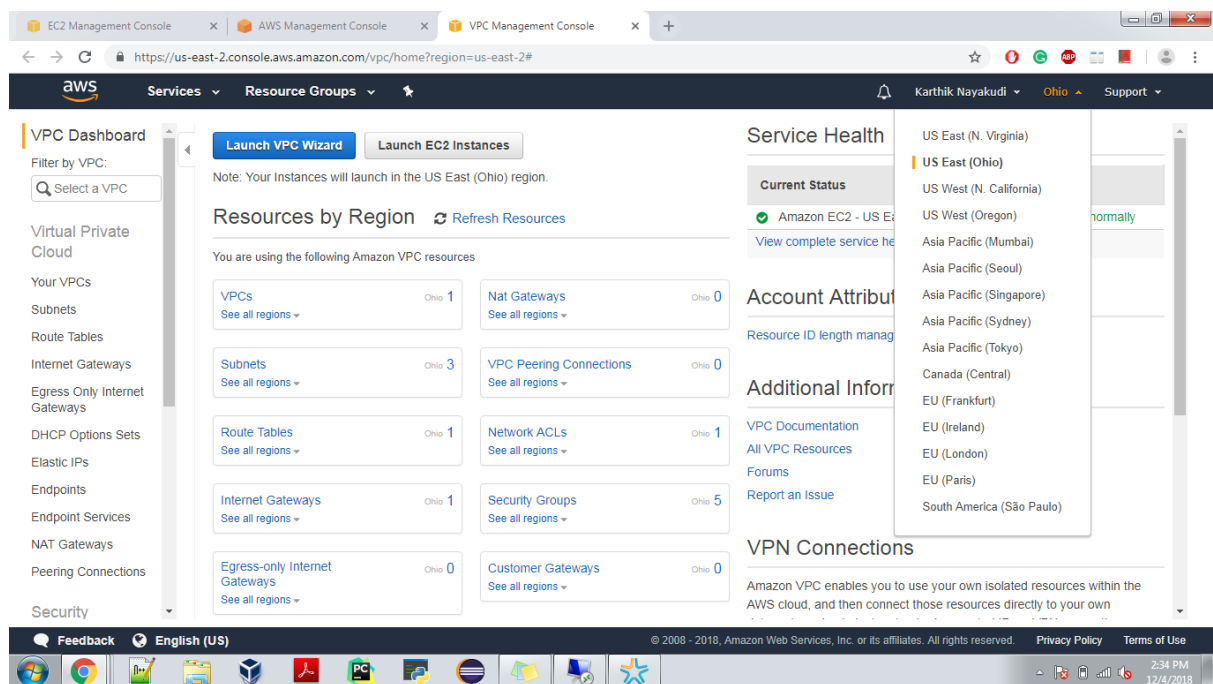
## AWS Console:



## VPC Dashboard



Zone:



We have use default VPC



The screenshot shows the AWS VPC Management Console. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, and Security. The main content area displays a table of VPCs with columns: Name, VPC ID, State, IPv4 CIDR, IPv6 CIDR, DHCP options set, and Route table. The selected VPC is vpc-51777639, which is in an 'available' state with an IPv4 CIDR of 172.31.0.0/16, DHCP options set dopl-5c8a9134, and route table rtb-0727e96c. Below the table, the 'Description' tab is active, showing details for VPC ID, State, IPv4 CIDR, DNS resolution, DNS hostnames, Route table, Tenancy, Default VPC, IPv6 CIDR, Network ACL, DHCP options set, and Owner.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table
vpc-51777639	vpc-51777639	available	172.31.0.0/16	-	dopl-5c8a9134	rtb-0727e96c

**VPC: vpc-51777639**

Property	Value
VPC ID	vpc-51777639
State	available
IPv4 CIDR	172.31.0.0/16
DNS resolution	Enabled
DNS hostnames	Enabled
Route table	rtb-0727e96c
Tenancy	default
Default VPC	Yes
IPv6 CIDR	-
Network ACL	acl-4ec22e25
DHCP options set	dopt-5c8a9134
Owner	731738806014

## EC2 Dashboard

The screenshot shows the AWS EC2 Dashboard. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Capacity Reservations), IMAGES (AMIs, Bundle Tasks), ELASTIC BLOCK STORE (Volumes, Snapshots, Lifecycle Manager), and NETWORK & SECURITY. The main content area displays the 'Resources' section, which shows the number of EC2 resources in the US East (Ohio) region: 1 Running Instances, 0 Elastic IPs, 0 Dedicated Hosts, 0 Snapshots, 2 Volumes, 0 Load Balancers, 0 Key Pairs, and 5 Security Groups. Below this, the 'Create Instance' section provides a 'Launch Instance' button and a note that instances will launch in the US East (Ohio) region. The 'Service Health' section shows the service status for US East (Ohio) as 'OK'. The 'Scheduled Events' section shows no events. The 'Account Attributes' section displays supported platforms, default VPC, resource ID length management, and console experiments. The 'Additional Information' section provides links to the Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, and Contact Us. The 'AWS Marketplace' section offers free software trial products and popular AMIs.

**Resources**

You are using the following Amazon EC2 resources in the US East (Ohio) region:

1 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
2 Volumes	0 Load Balancers
0 Key Pairs	5 Security Groups
0 Placement Groups	

[Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the EC2 Videos.](#)

**Create Instance**

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

[Launch Instance](#)

Note: Your instances will launch in the US East (Ohio) region

**Service Health**

**Service Status:**

US East (Ohio): OK

**Availability Zone Status:**

**Scheduled Events**

US East (Ohio): No events

**Account Attributes**

**Supported Platforms**

VPC

**Default VPC**

vpc-51777639

**Resource ID length management**

Console experiments

**Additional Information**

[Getting Started Guide](#)

[Documentation](#)

[All EC2 Resources](#)

[Forums](#)

[Pricing](#)

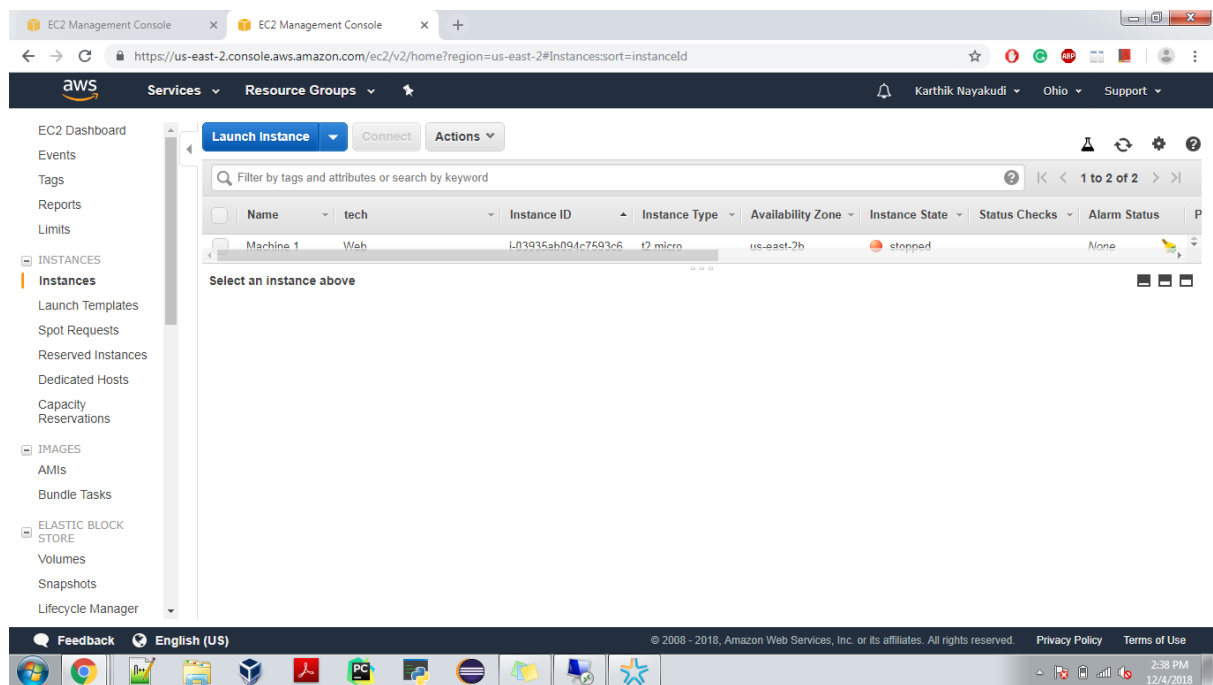
[Contact Us](#)

**AWS Marketplace**

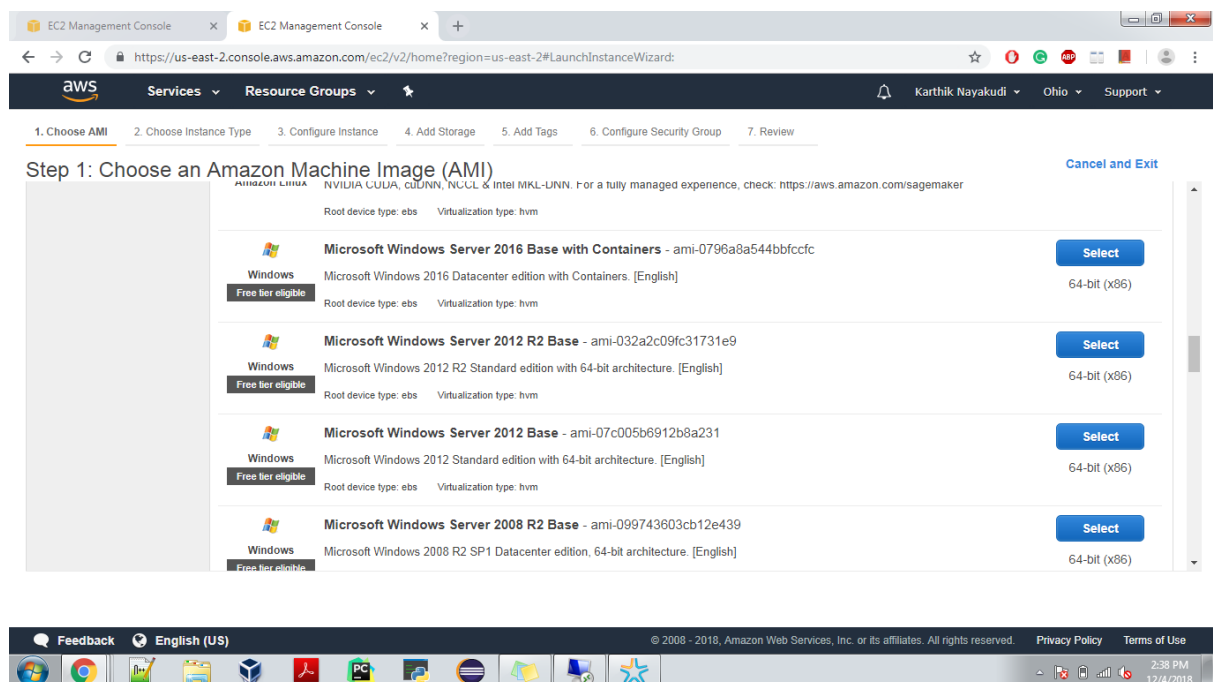
Find free software trial products in the AWS Marketplace from the [EC2 Launch Wizard](#). Or try these popular AMIs:

[Barracuda CloudGen Firewall for AWS](#)

## Launching Instance



## Choosing AMI



## Instance Type

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: **All Instance types** **Current generation** [Show/Hide Columns](#)

**Currently selected:** t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

Feedback English (US) © 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use 2:38 PM 12/4/2018

## Configuring Instances

EC2 Management Console

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot instances

Network: vpc-51777639 (default) [Create new VPC](#)

Subnet: No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: ☐ Add instance to placement group.

Capacity Reservation: Open [Create new Capacity Reservation](#)

Domain join directory: No directory [Create new directory](#)

IAM role: None [Create new IAM role](#)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

2:38 PM 12/4/2018

## Adding Storage

EC2 Management Console

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-0e3d56fe3f3e197c4	30	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

Feedback English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

2:39 PM 12/4/2018

## Adding Tags

EC2 Management Console

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

aws Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.  
A copy of a tag can be applied to volumes, instances or both.  
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	Instances	Volumes
Name	Machine 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tech	ADDS, DNS & DHCP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

Feedback English (US) © 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

2:39 PM 12/4/2018

## Security groups:

EC2 Management Console

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

aws Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

**Assign a security group:** ☒ Create a new security group ☐ Select an existing security group

**Security group name:** launch-wizard-5

**Description:** launch-wizard-5 created 2018-12-04T14:40:01.838-05:00

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

[Add Rule](#)

**Warning**

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review and Launch](#)

Feedback English (US) © 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

2:40 PM 12/4/2018

## About Instance

The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Capacity Reservations, IMAGES, AMIs, Bundle Tasks, ELASTIC BLOCK STORE, Volumes, Snapshots, and Lifecycle Manager. The main content area shows the 'Instances' page with a table of instances. 'Machine 2' is selected, and its details are shown in the 'Description' tab.

Name	tech	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
Machine 1	Web	i-03935ab094c7593c6	t2.micro	us-east-2b	stopped	2/2 checks ...	None
Machine 2	ADDS, DNS & DHCP	i-050756b99b2ea9357	t2.micro	us-east-2b	running	2/2 checks ...	None

**Description** | Status Checks | Monitoring | Tags

Instance ID: i-050756b99b2ea9357

Instance state: running

Instance type: t2.micro

Elastic IPs: -

Availability zone: us-east-2b

Security groups: launch-wizard-4 - view inbound rules - view outbound rules

Scheduled events: No scheduled events

AMI ID: Windows\_Server-2012-R2\_RTM-English-64Bit-Base-2018.11.19 (ami-032a2c09fc31731e9)

Platform: windows

Public DNS (IPv4): ec2-18-191-104-144.us-east-2.compute.amazonaws.com

IPv4 Public IP: 18.191.104.144

Private DNS: ip-172-31-16-86.us-east-2.compute.internal

Private IPs: 172.31.16.86

Secondary private IPs: -

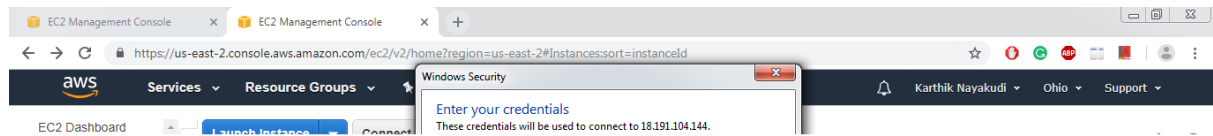
VPC ID: vpc-51777639

Subnet ID: subnet-13a5c269

Network interfaces: eth0

## Connecting to Instance:

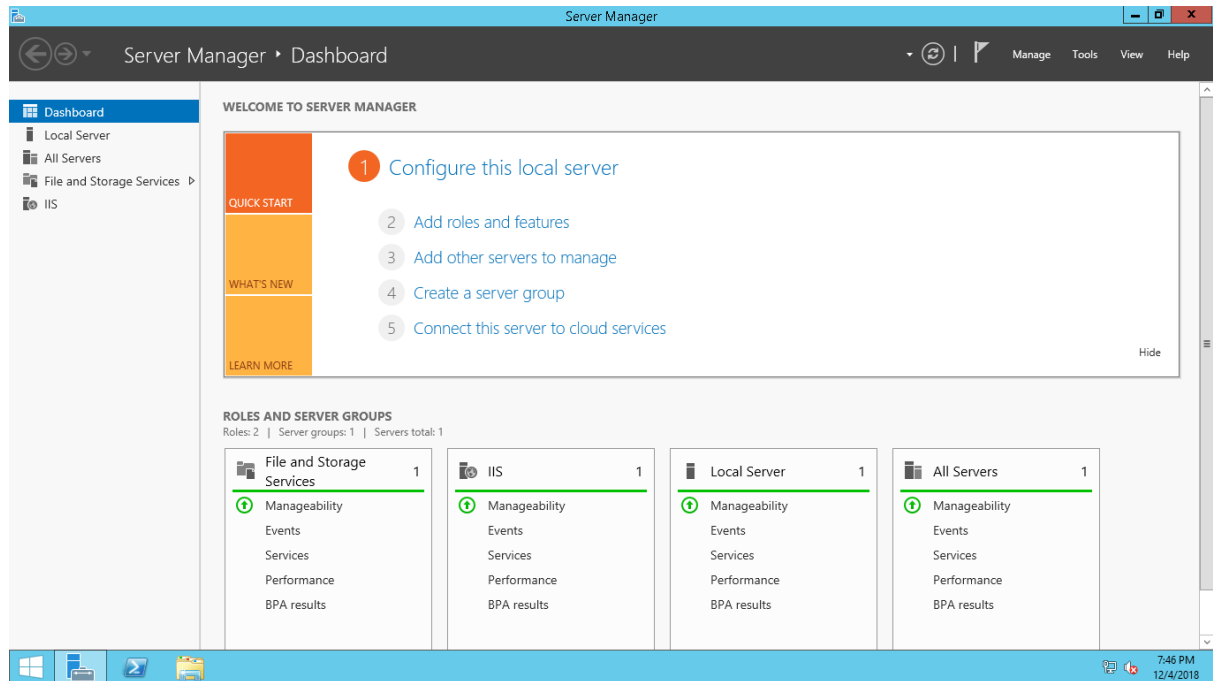
The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for EC2 Dashboard, Launch Instance, Connect, and Remote Desktop Connection. The main content area shows the 'Instances' page with a table of instances. 'Machine 2' is selected, and the 'Connect' button is highlighted. A 'Remote Desktop Connection' window is visible in the background.



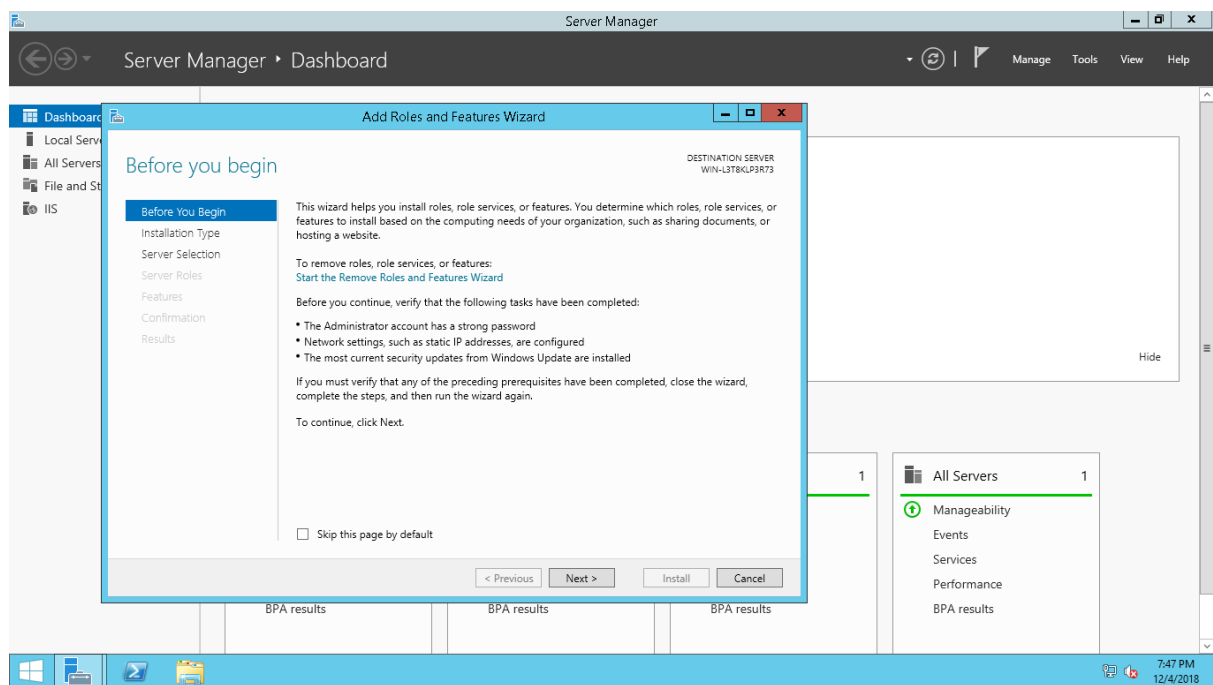
## Windows server 2012 R2



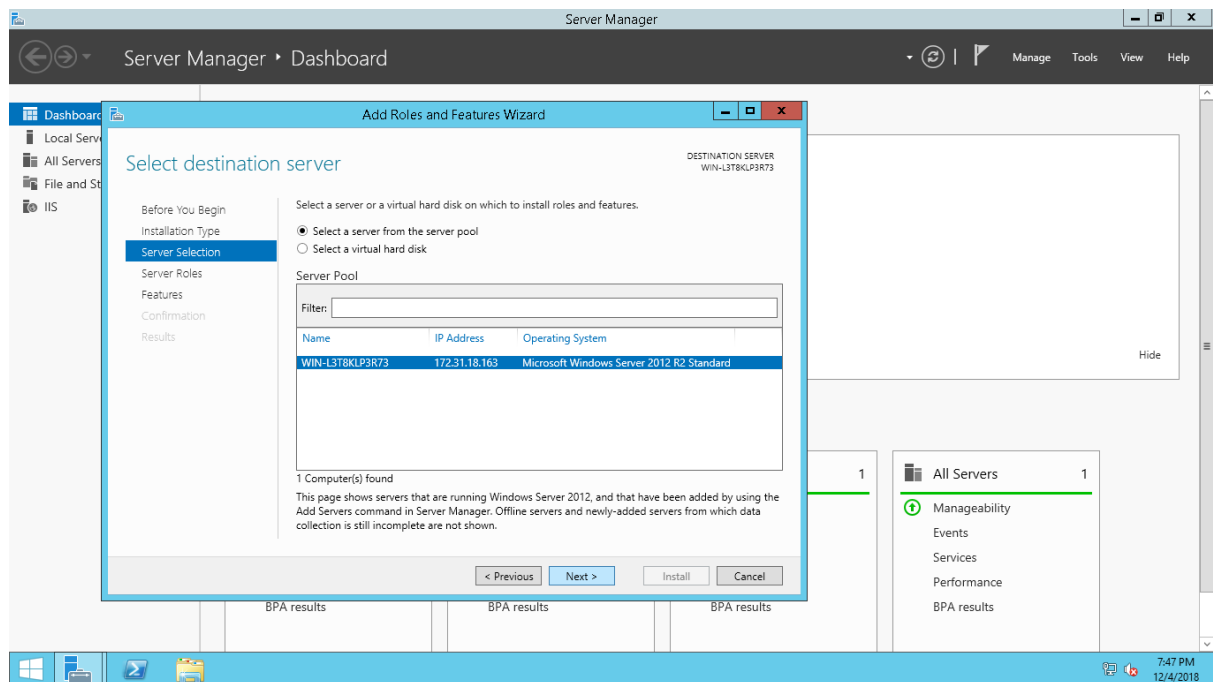
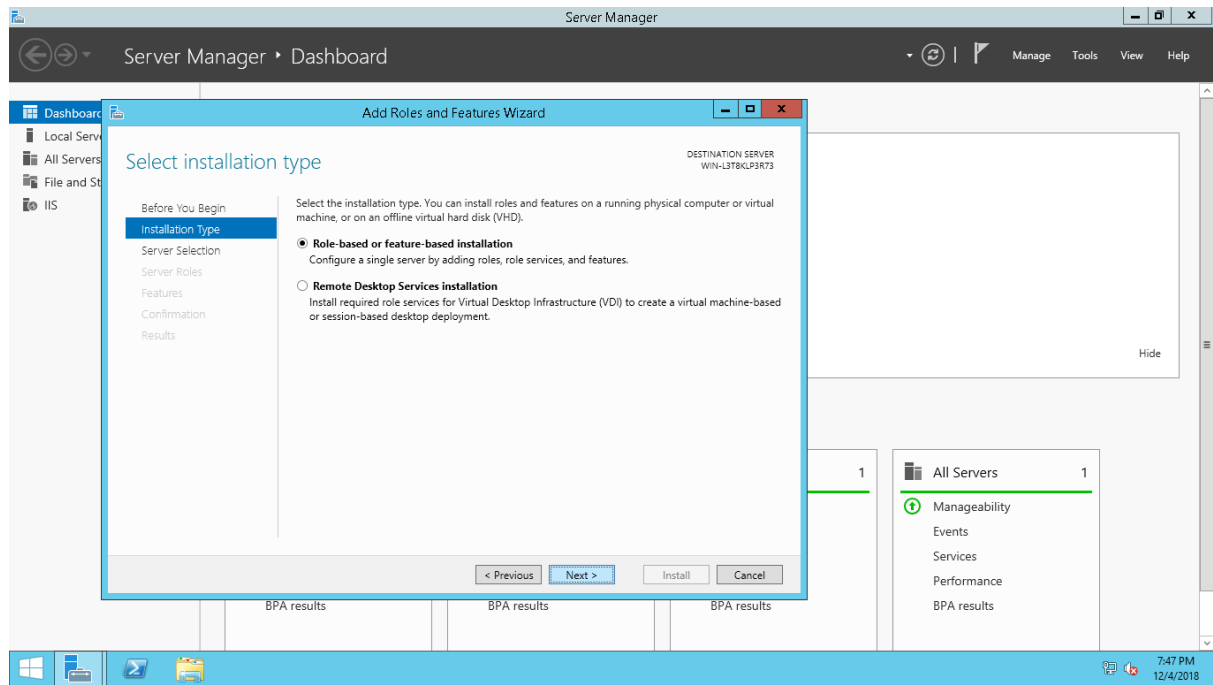
## Adding Services:

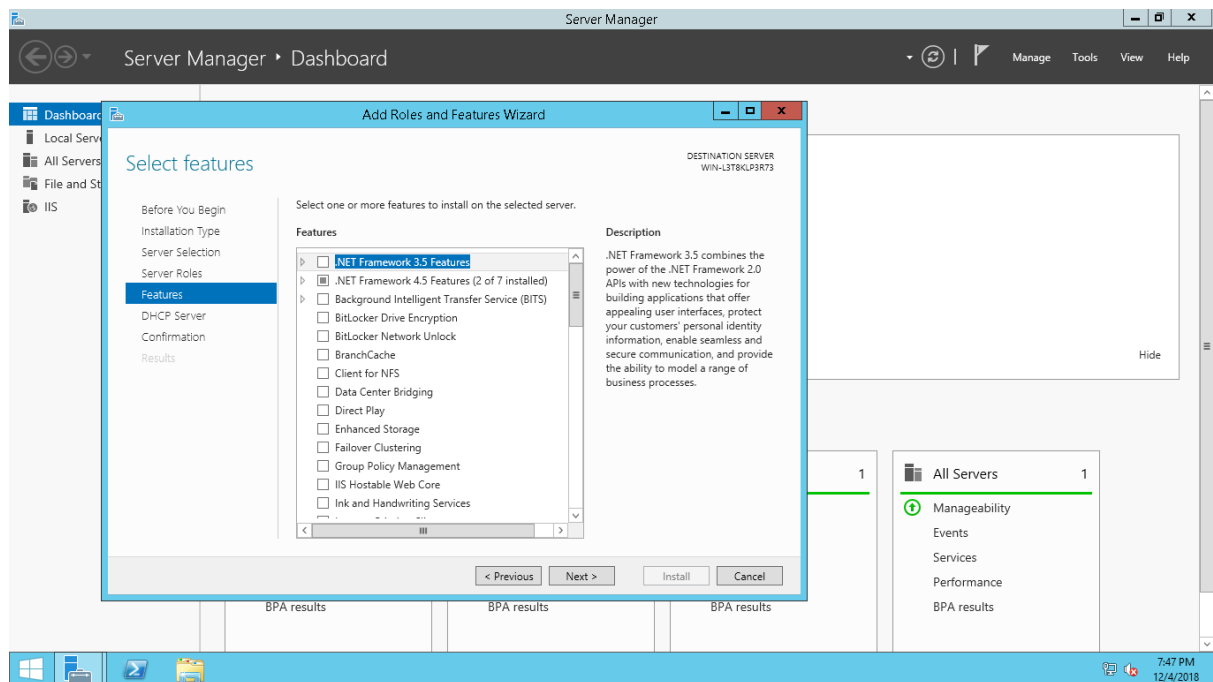
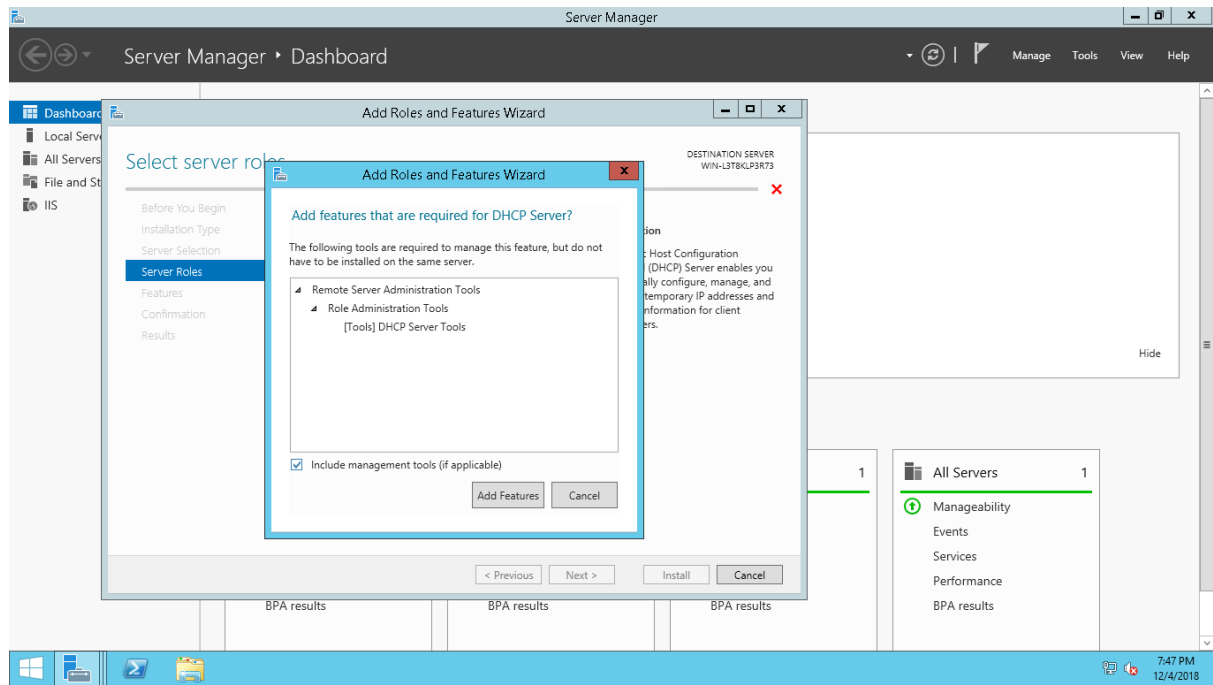


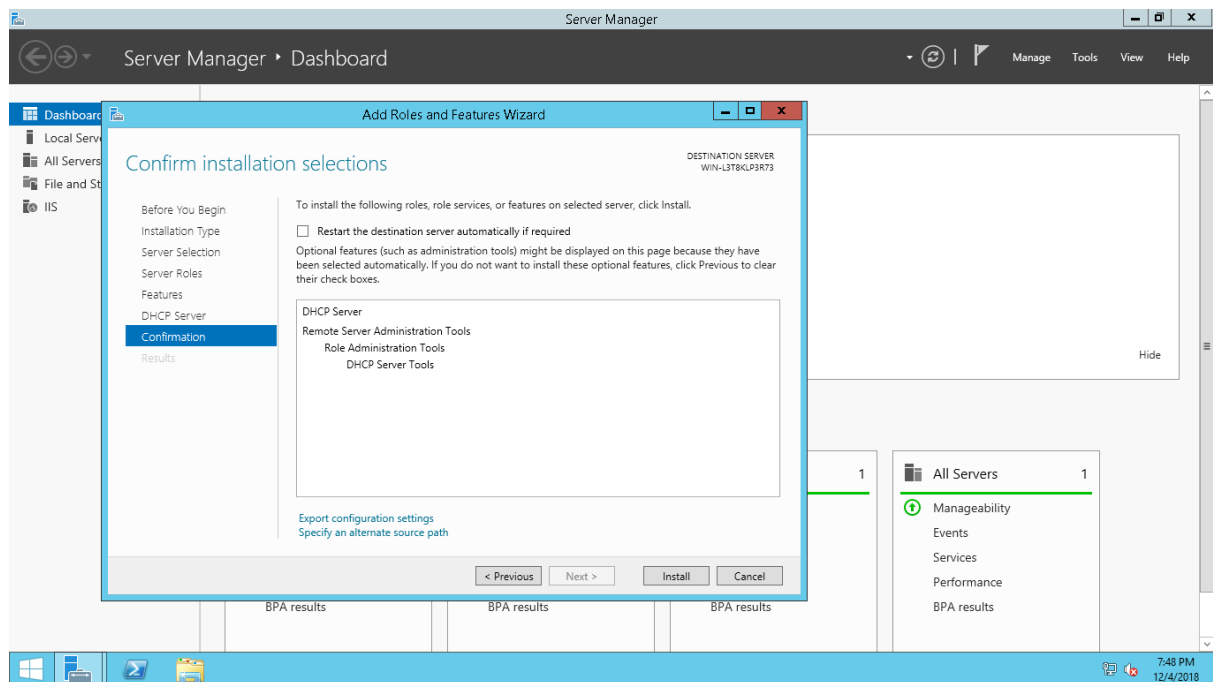
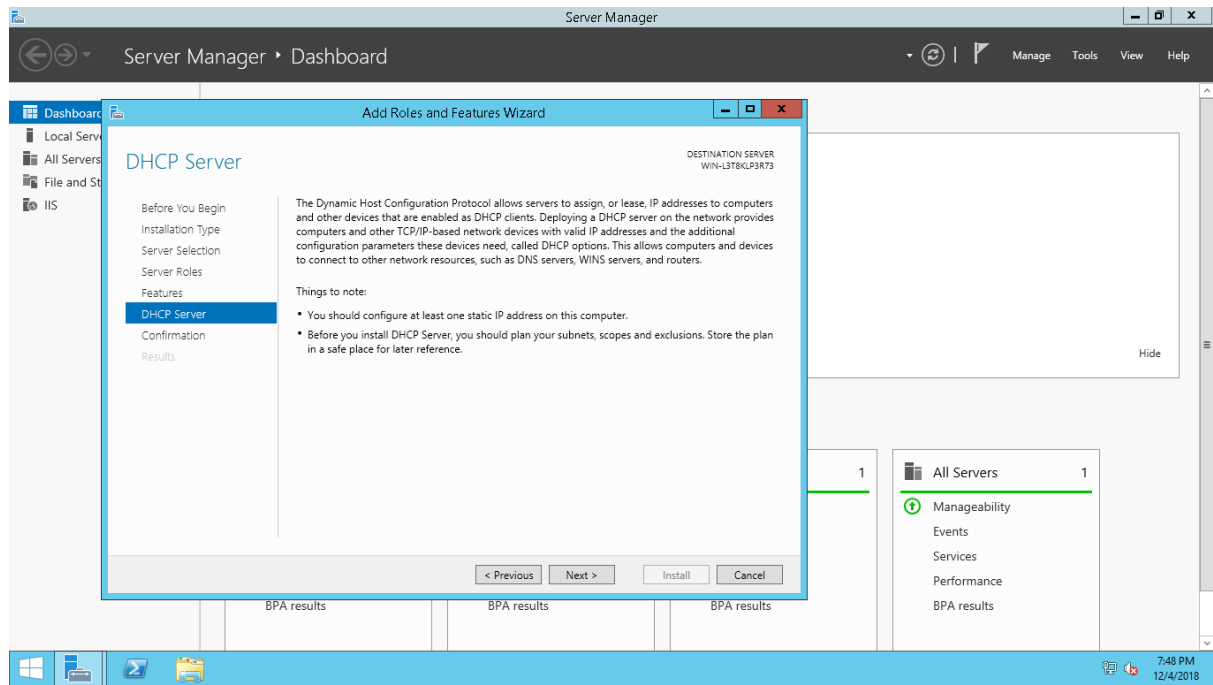
## Adding DHCP Service:

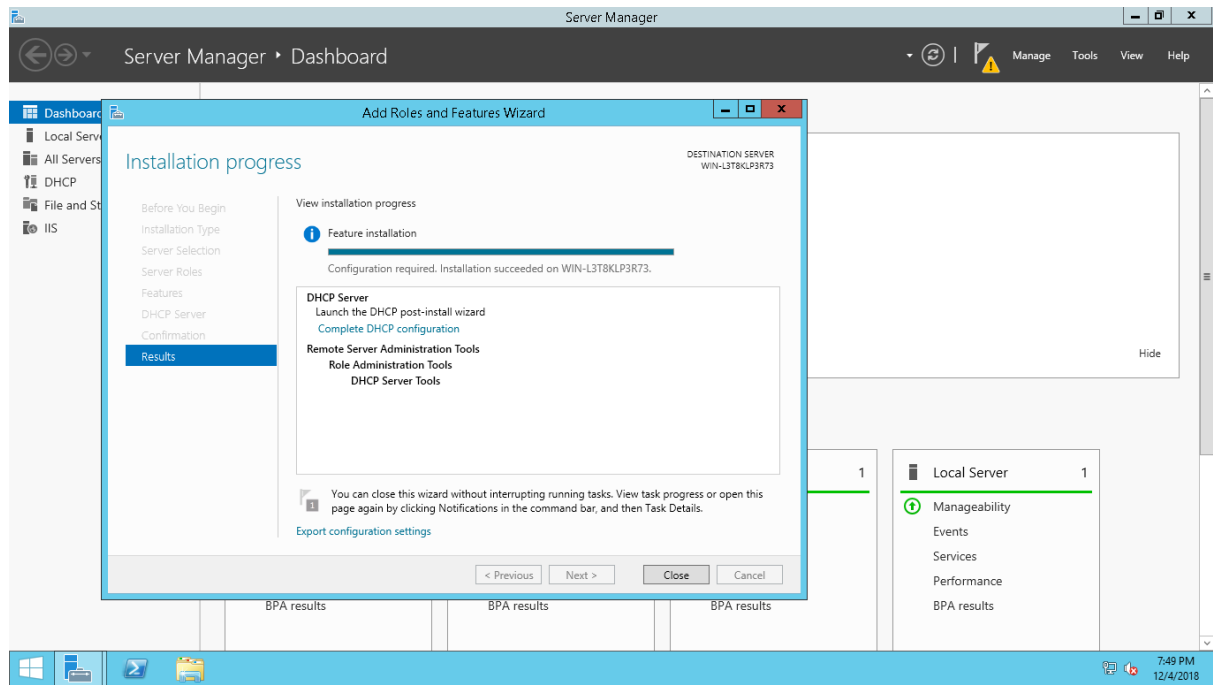




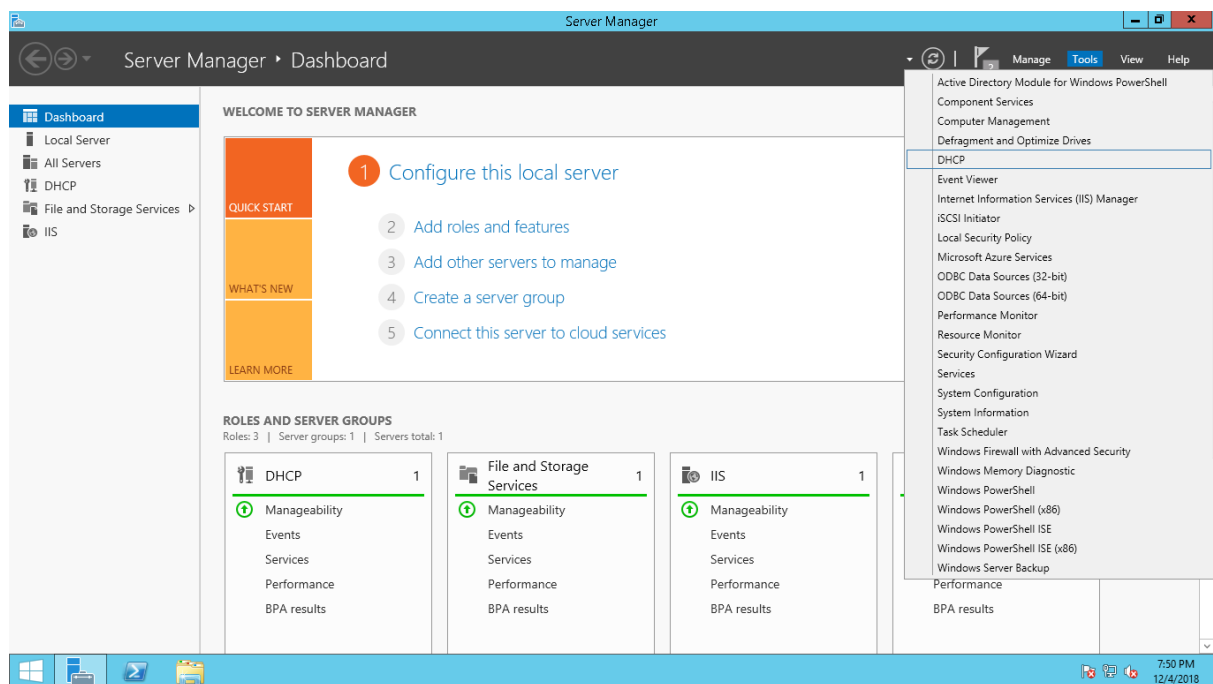


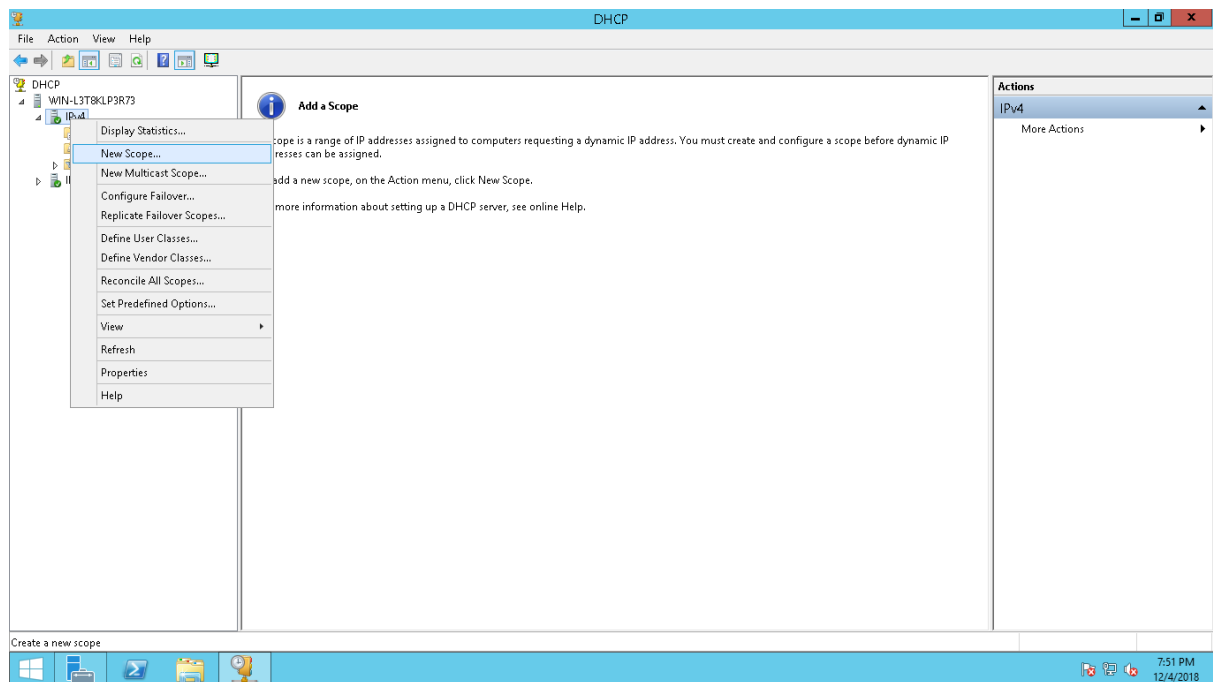
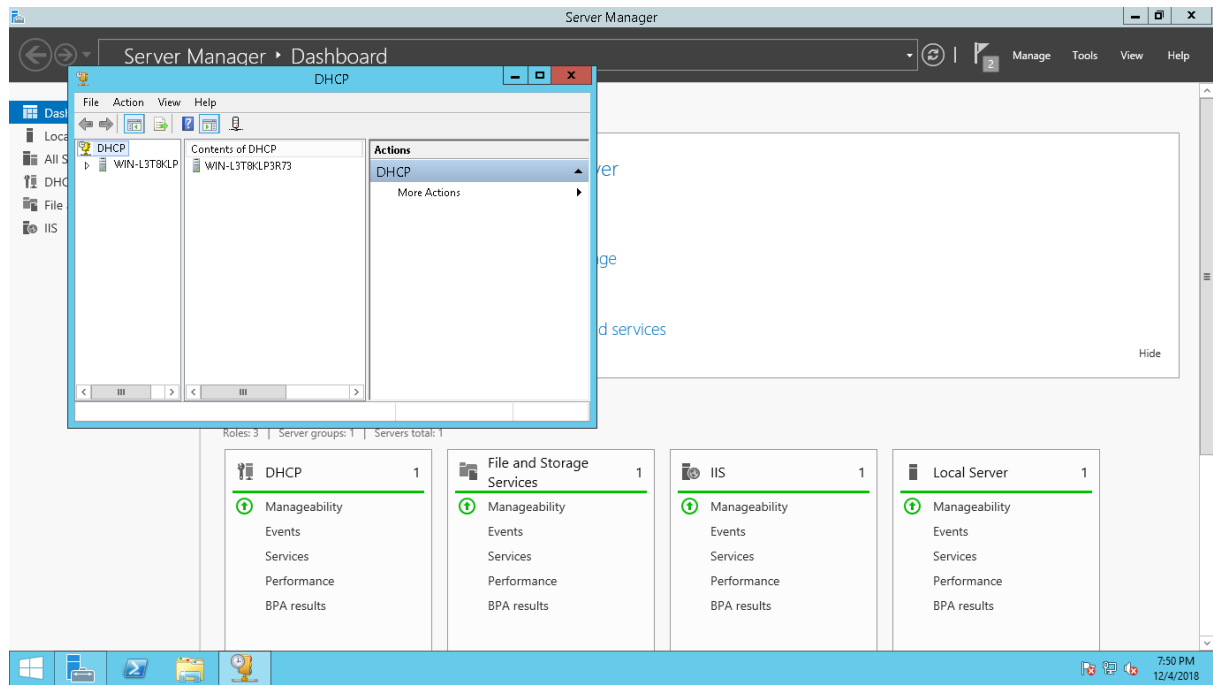


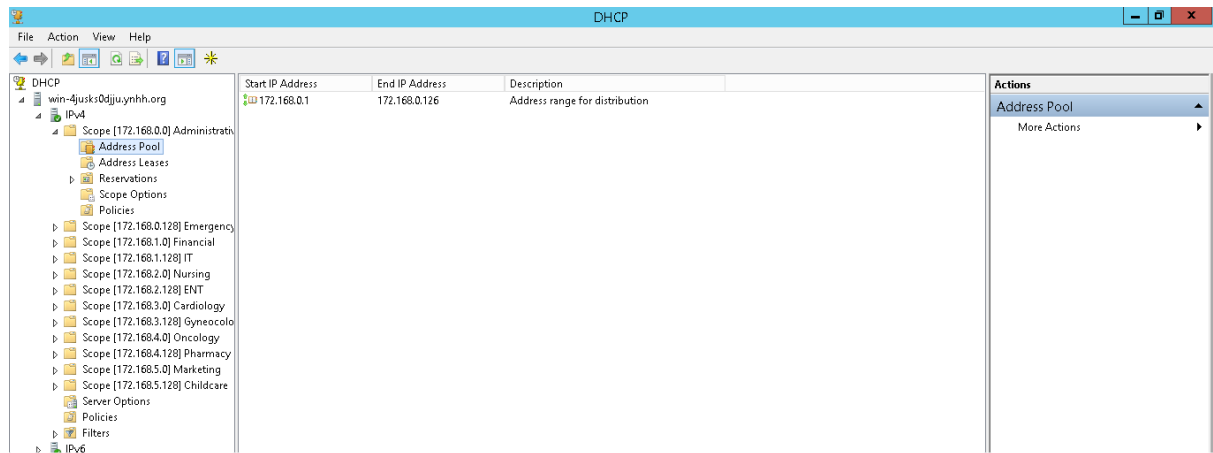




## Adding DHCP Scopes







Adding DNS service:







Adding DNS forward Zones:







Reverse lookup Zone

Adding ADDS Service:







Adding Users and Groups:



Adding Web service





Adding SMTP Service:













**Configuration ISP:**  
ISP#show run  
Building configuration...

Current configuration: 947 bytes

```
!  
version 12.2  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname ISP  
!  
no ip cef  
no ipv6 cef  
!!  
interface FastEthernet0/0  
ip address 6.6.6.5 255.0.0.0  
duplex auto  
speed auto  
!  
interface FastEthernet0/0.1  
no ip address  
!  
interface FastEthernet0/1  
ip address 8.8.8.8 255.0.0.0  
duplex auto  
speed auto  
!  
interface Ethernet1/0  
ip address 7.7.7.7 255.0.0.0  
duplex auto  
speed auto  
!  
interface Ethernet1/1  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Ethernet1/2  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Ethernet1/3  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
router rip  
network 6.0.0.0
```

```
network 7.0.0.0
network 8.0.0.0
network 169.11.0.0
network 172.169.0.0
!
```

### **Newhaven Main Building:**

Newhaven Main Building #show run  
Building configuration...

```
Current configuration: 4470 bytes
!
version 12.2(37) SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Newhaven Main Building
!
!
ip dhcp pool vlan11
network 172.168.0.0 255.255.255.128
default-router 172.168.0.1
ip dhcp pool vlan12
network 172.168.0.128 255.255.255.128
default-router 172.168.0.129
ip dhcp pool vlan13
network 172.168.1.0 255.255.255.128
default-router 172.168.1.1
ip dhcp pool vlan14
network 172.168.1.128 255.255.255.128
default-router 172.168.1.129
ip dhcp pool vlan15
network 172.168.2.0 255.255.255.128
default-router 172.168.2.1
ip dhcp pool vlan16
network 172.168.2.128 255.255.255.128
default-router 172.168.2.129
ip dhcp pool vlan17
network 172.168.3.0 255.255.255.128
default-router 172.168.3.1
ip dhcp pool vlan18
network 172.168.3.128 255.255.255.128
default-router 172.168.3.129
ip dhcp pool vlan19
network 172.168.4.0 255.255.255.128
default-router 172.168.4.1
ip dhcp pool vlan20
network 172.168.4.128 255.255.255.128
```

```

default-router 172.168.4.129
ip dhcp pool vlan21
network 172.168.5.0 255.255.255.128
default-router 172.168.5.1
ip dhcp pool vlan22
network 172.168.5.128 255.255.255.128
default-router 172.168.5.129
ip dhcp pool vlan23
network 169.10.0.0 255.255.240.0
default-router 169.10.0.1
!
!
interface FastEthernet0/1
switchport access vlan 11
!
interface FastEthernet0/2
switchport access vlan 12
!
interface FastEthernet0/3
switchport access vlan 13
!
interface FastEthernet0/4
switchport access vlan 14
!
interface FastEthernet0/5
switchport access vlan 15
!
interface FastEthernet0/6
switchport access vlan 16
!
interface FastEthernet0/7
switchport access vlan 17
!
interface FastEthernet0/8
switchport access vlan 18
!
interface FastEthernet0/9
switchport access vlan 19
!
interface FastEthernet0/10
switchport access vlan 20
!
interface FastEthernet0/11
switchport access vlan 21
!
interface FastEthernet0/12
switchport access vlan 22
!
interface FastEthernet0/13
switchport access vlan 23
!

```

```
interface FastEthernet0/14
switchport access vlan 100
!
interface FastEthernet0/15
switchport access vlan 200
!
interface FastEthernet0/16
switchport access vlan 300
!
```

```
interface FastEthernet0/17
no switchport
ip address 6.6.6.6 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet0/18
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/19
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/20
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
```

```
interface Vlan1
no ip address
shutdown
!
interface Vlan11
mac-address 00d0.ff80.6d01
ip address 172.168.0.1 255.255.255.128
!
interface Vlan12
```



```

mac-address 00d0.ff80.6d02
ip address 172.168.0.129 255.255.255.128
!
interface Vlan13
mac-address 00d0.ff80.6d03
ip address 172.168.1.1 255.255.255.128
!
interface Vlan14
mac-address 00d0.ff80.6d04
ip address 172.168.1.129 255.255.255.128
!
interface Vlan15
mac-address 00d0.ff80.6d05
ip address 172.168.2.1 255.255.255.128
!
interface Vlan16
mac-address 00d0.ff80.6d06
ip address 172.168.2.129 255.255.255.128
!
interface Vlan17
mac-address 00d0.ff80.6d07
ip address 172.168.3.1 255.255.255.128
!
interface Vlan18
mac-address 00d0.ff80.6d08
ip address 172.168.3.129 255.255.255.128
!
interface Vlan19
mac-address 00d0.ff80.6d09
ip address 172.168.4.1 255.255.255.128
!
interface Vlan20
mac-address 00d0.ff80.6d0a
ip address 172.168.4.129 255.255.255.128
!
interface Vlan21
mac-address 00d0.ff80.6d0b
ip address 172.168.5.1 255.255.255.128
!
interface Vlan22
mac-address 00d0.ff80.6d0c
ip address 172.168.5.129 255.255.255.128
!
interface Vlan23
mac-address 00d0.ff80.6d0d
ip address 169.10.0.1 255.255.240.0
!
interface Vlan100
mac-address 00d0.ff80.6d0e
ip address 1.1.1.1 255.0.0.0
!

```

```
interface Vlan200
mac-address 00d0.ff80.6d0f
ip address 2.2.2.1 255.0.0.0
!
interface Vlan300
mac-address 00d0.ff80.6d10
ip address 3.3.3.1 255.0.0.0
!
router rip
network 1.0.0.0
network 2.0.0.0
network 3.0.0.0
network 6.0.0.0
network 169.10.0.0
network 172.168.0.0
!
```

**References:**

1. Top-Down Network Design (3rd Edition) 3rd Edition  
Oppenheimer

Book by Priscilla