**COMPUTER NETWORKS**

**Case Study**

**Hotel Management Network System**

**Why Networking is required for the application:**

**[1] Communication Between Departments:**

Hotels have various departments such as Admin, Sales, and Reception. Networking enables these departments to communicate and coordinate effectively.

**[2]** **Internet Access:**

Hotel networks provide internet connectivity for hotel management systems as well as for users to access the internet using WiFi.

**[3] Security and Access Control:**

Networking enables the implementation of security measures, such as user authentication and access control, to protect sensitive information within the hotel management system.

**Problem Statement:**

The hotel has three floors; in the first floor there three departments (Reception, store and Logistics), in the second floor there are three departments (Finance, HR and Sales/Marketing), while the third floor hosts the IT and Admin. Therefore, the following are part of the considerations during the design and implementation.

* There should be three routers connecting each floor.
* All routers should be connected to each other using serial DCE cable.
* The network between the routers should be 10.10.10.0/30,10.10.10.4/30 and 10.10.10.8/30.
* Each floor is expected to have one switch (placed in the respective floor).
* Each floor is expected to have WIFI networks connected to some devices
* Each department is expected to be in different VLAN with the following details -

**1st Floor:**

* Reception- VLAN 80, Network of 192.168.8.0/24
* Store- VLAN 70, Network of 192.168.7.0/24
* Logistics- VLAN 60, Network of 192.168.6.0/24

**2nd Floor:**

* Finance- VLAN 50, Network of 192.168.5.0/24
* HR- VLAN 40, Network of 192.168.4.0/24
* Sales- VLAN 30, Network of 192.168.3.0/24

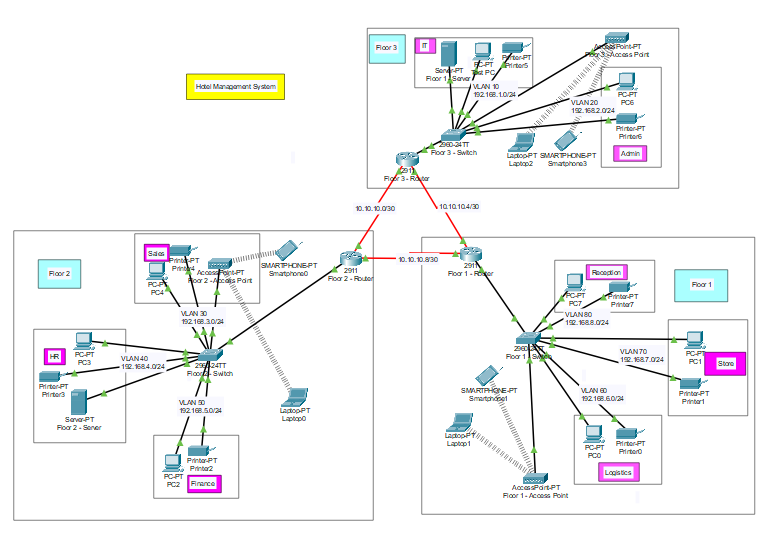
**3rd Floor:**

* Admin- VLAN 20, Network of 192.168.2.0/24
* IT- VLAN 10, Network of 192.168.1.0/24.
* Use OSPF as the routing protocol to advertise routes.
* All devices in the network are expected to obtain IP address dynamically with their respective router configured as the DHCP server.
* All the devices in the network are expected to communicate with each other.
* Configure SSH in all the routers for remote login.
* In IT department, add PC called Test-PC to port fa0/1 and use it to test remote login.
* Configure port security to IT-dept switch to allow only Test-PC to access port fa0/1 (use sticky method to obtain mac-address with violation mode of shutdown.)

**Technologies Implemented:**

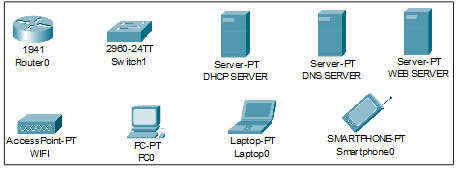
1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Creating VLANs and assigning ports VLAN numbers.
5. /5Subnetting and IP Addressing.
6. Configuring Inter-VLAN Routing (Router on a stick).
7. Configuring DHCP Server (Router as the DHCP Server).
8. Configuring SSH for secure Remote access.
9. Configuring switchport security or Port-Security on the switches.
10. Configuring WLAN or wireless network (Cisco Access Point).
11. Host Device Configurations.
12. Test and Verifying Network Communication.

**Architecture diagram:**



**Networking devices used in Hotel Management System:**

* Routers - communication between various departments
* Switches - manage and direct data traffic
* Servers - centralize and manage data
* Access Points - provide reliable and widespread wireless connectivity
* Personal Computers
* Printers
* Smart Phones
* Laptops



|  |  |
| --- | --- |
| **Devices** | **Quantity** |
| 1) Router (2911) | 3 |
| 2) Switches (2960-24TT) | 3 |
| 3) DHCP Server | 2 |
| 4) Wireless Device (Access Point) | 3 |
| 5) PCs | 8 |
| 6) Printers | 8 |

**Important Terminologies:**

**Packet Tracer:**

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command-line interface. Packet Tracer makes use of a drag-and-drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused on Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.

**Router:**

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divides broadcast domains of hosts connected through it.

**Switch:**

A network switch (also called switching hub, bridging hub, officially MAC bridge is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

**Network Packet:**

A network packet is a formatted unit of data carried by a packet-switched network. A packet consists of control information and user data, which is also known as the payload.

**Server:**

A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines, they are considered servers. There are many types of servers, including web servers, mail servers, and virtual servers.

* **DNS Server:**

DNS stands for Domain Name System servers which are application servers that provide a human-friendly naming method to the user computers in order to make IP addresses readable by users. The DNS system is a widely distributed database of names and other DNS servers, each of which can be used to request an otherwise unknown computer name. When a user needs the address of a system, it sends a DNS request with the name of the desired resource to a DNS server. The DNS server responds with the necessary IP address from its table of names.

* **EMAIL Server:**

An e-mail server is a server that handles and delivers e-mail over a network, using standard email protocols. For example, the SMTP protocol sends messages and handles outgoing mail requests. The POP3 protocol receives messages and is used to process incoming mail. When you log on to a mail server using a webmail interface or email client, these protocols handle all the connections behind the scenes.

**Wireless Network:**

A wireless network broadcasts an access signal to the workstations or PCs. This enables mobility among laptops, tablets, and PCs from room to room while maintaining a firm network connection continuously. A wireless network also presents additional security requirements.

**Computing Device:**

Computing devices are the electronic devices that take user inputs, process the inputs, and then provide us with the end results. These devices may be Smartphones, PC Desktops, Laptops, printer, and many more.

**Internet Protocol:**

Internet Protocol (IP) is one of the fundamental protocols that allow the internet to work. IP addresses are a unique set of numbers on each network and they allow machines to address each other across a network. It is implemented on the internet layer in the IP/TCP model.

**SSH Protocol:**

Secure Shell enables a user to access a remote device and manage it remotely. However, with SSH, all data transmitted over a network (including usernames and passwords) is encrypted and secure from eavesdropping.

SSH is a client-server protocol, with an SSH client and an SSH server. The client machine (such as a PC) establishes a connection to an SSH server running on a remote device (such as a router). Once the connection has been established, a network admin can execute commands on the remote device.

**Why we need to measure network performance?**

Measuring network performance in a hotel management system with multiple VLANs and departments is crucial for several reasons. Firstly, it allows the IT staff to identify and address any bottlenecks or issues that may arise within the network. This is important for ensuring that all departments can communicate and access the resources they need without delays or interruptions.

Measuring network performance enables the IT team to optimize the network for the specific needs of each department. For example, they can prioritize bandwidth for critical systems such as the reservation system or the point of sale system, ensuring that these systems operate smoothly and efficiently.

It allows for proactive monitoring and troubleshooting, helping to prevent potential problems before they impact the operations of the hotel. This is especially important in a hotel environment where the smooth functioning of various systems is essential for providing a high level of service to guests and maintaining operational efficiency.

In summary, measuring network performance in a hotel management system with multiple VLANs and departments is essential for maintaining a reliable and efficient network infrastructure that supports the diverse operational needs of the hotel.

**Performance parameters:**

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Meaning** | **Formula** |
| **Bandwidth** | Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time | Expressed as [bits](https://web.archive.org/web/20190816003233/https:/whatis.techtarget.com/definition/bit-binary-digit) per second ([bps](https://web.archive.org/web/20190816003233/https:/searchnetworking.techtarget.com/definition/bits-per-second)), modern network links have greater capacity, which is typically measured in millions of bits per second ([megabits per second](https://web.archive.org/web/20190816003233/https:/searchnetworking.techtarget.com/definition/Mbps), or Mbps) or billions of bits per second ([gigabits per second](https://web.archive.org/web/20190816003233/https:/whatis.techtarget.com/definition/Gbps-billions-of-bits-per-second), or Gbps). |
| **Throughput** | Throughput measures the percentage of data packets that are successfully being sent; a low throughput means there are a lot of failed or dropped packets that need to be sent again. |  |
| **Packet Loss** | Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination.Due to network congestion | Efficiency = 100% \* (transferred - retransmitted) / transferred  Network Loss = 100 - Efficiency |
| **Transmission time** | The time required for transmission of a message depends on the size of the message and the bandwidth of the channel. | Transmission time=Message size / Bandwidth |
| **Propagation Time** | Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed. | Propagation time = Distance /Propagation speed |
| **Processing Delay** | Time taken by the processor to process the data packet is called processing delay. |  |
| **Queuing Delay** | Time spent by the data packet waiting in the queue before it is taken for execution is called queuing delay. |  |
| **Jitter** | Jitter is defined as the variation in time delay for the data packets sent over a network. This variable represents an identified disruption in the normal sequencing of data packets. Jitter is related to latency, since the jitter manifests itself in increased or uneven latency between data packets, which can disrupt network performance and lead to packet loss and network congestion. Although some level of jitter is to be expected and can usually be tolerated, quantifying network jitter is an important aspect of comprehensive network | Latency=sum of all delays    To measure Jitter, we take the difference between samples, then divide by the number of samples (minus 1). |

**Routing algorithm:**

**Open Shortest Path First (OSPF):**

In a hotel management network system, the Open Shortest Path First (OSPF) routing algorithm plays a crucial role in ensuring efficient and reliable communication between network devices. OSPF is a link-state routing protocol that is well-suited for complex and scalable networks, making it an ideal choice for the diverse and interconnected infrastructure found in hotel environments.

OSPF is designed to scale effectively, making it suitable for hotel networks with numerous interconnected devices, multiple VLANs, and various departments. As the hotel network expands, OSPF can adapt to the changes and efficiently calculate the shortest path to each destination, ensuring optimal routing.

OSPF is well-suited for the complex and dynamic nature of a hotel management network system. Its scalability, fast convergence, support for traffic engineering, redundancy, and QoS capabilities make it an effective routing algorithm for ensuring efficient and reliable communication within the diverse and interconnected infrastructure of a hotel environment.

**Benefits of wireless networking over wired networking**

To better understand the wide usage of wireless networking in today’s world, is to start with the benefits it has over traditional wired networking is crucial for our project implementation. Some major aspects have been stated below that show the various advantages of a wireless network over wired ones.

* **Mobility:**

One of the major advantages of wireless is mobility. Users have the freedom to move within the area of the network with their computing devices staying connected to a network without being concerned about the cable connection.

* **Less Hassle:**

The wireless network helps in the reduction of large amounts of cables or wires which becomes chaotic and difficult to maintain, it makes the connection hassle-free.

* **Accessibility:**

Provide network access across your organization, even in areas that have been challenging to reach with the wired network, so your entire team can stay in touch.

* **Expandability:**

The wireless network helps in the expansion of the network to a wide range by adding multiple new users and locations without additional need to run cables and wires.

* **Guest Access:**

Offer secure network access to guest users, including customers and business partners, while keeping your network resources protected.

With lots of advantages, there come disadvantages as well, like security issues which can be resolved using strict protection passwords. Also, the Speed of wireless networks is slow and having low bandwidth when compared to the direct cable connection networks.

* **Simulation Environment**

The simulations of our network topology can be easily achieved using cisco packet tracer. Using a simulation mode, you can see packets flowing from one node to another and can also click on a packet to see detailed information about the OSI layers of the networking. Packet Tracer offers a huge platform to combine realistic simulation and visualize them simultaneously. Cisco Packet Tracer makes learning and teaching significantly easier by supporting multi-user collaboration and by providing a realistic simulation environment for experimenting with projects.

In order to make our project understandable, we have divided the content into steps. They are as follows:

* **Software & Hardware Requirements**

Before heading towards the implementation, we need to make sure of the following requirements.

* + - A proper workstation (any mid-high range laptop will suffice).
    - Packet Tracer by Cisco
    - 8 GB RAM.
    - Any 10,000+ Average CPU Mark scored processor.
    - 16 GB of dedicated hard disk space.
    - USB 3.0+ port.
* **Brief Knowledge about our approach**

* **Network Requirements**

Our university outline is considered for this wireless university network.

The network is divided into 3 Floors:

1. **Floor 1:**

This floor is divided into accessing points like Reception, Store and Logistics.

1. **Floor 2:**

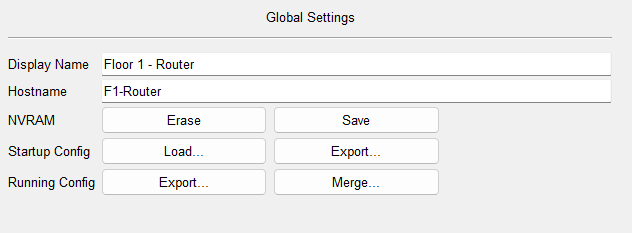
This floor is divided into accessing points like Sales, HR and Finance.

1. **Floor 3:**

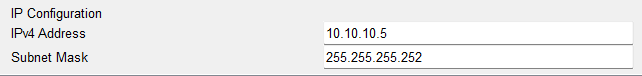
This floor is divided into accessing points like IT and Admin.

**Configuring IP Address:**

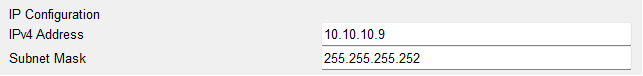
**Floor – 1 Router Configuration:**

****

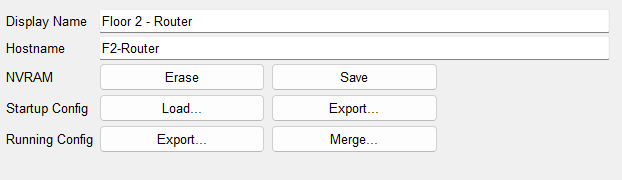
Serial0/3/0



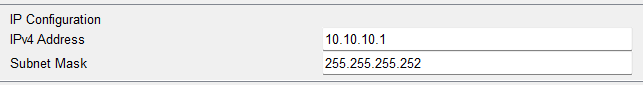
Serial0/3/1



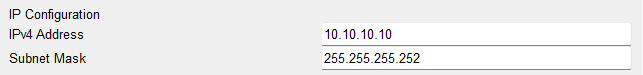
**Floor – 2 Router Configuration:**

****

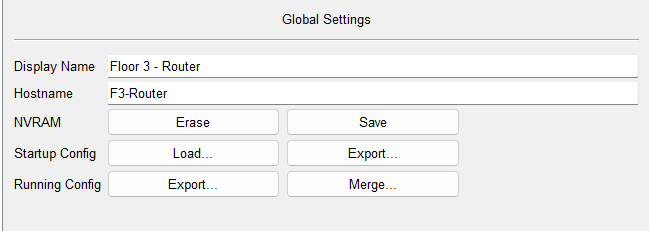
Serial0/3/0



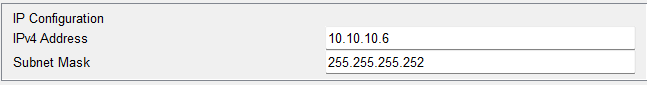
Serial0/3/1



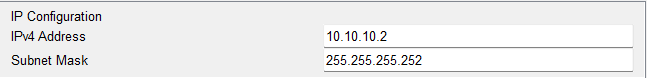
**Floor – 3 Router Configuration:**



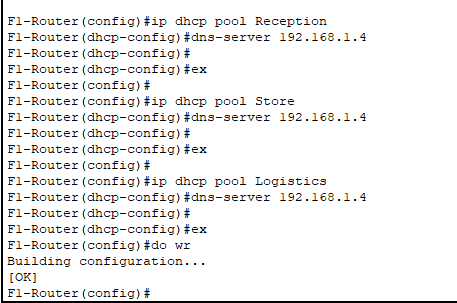
Serial0/3/0

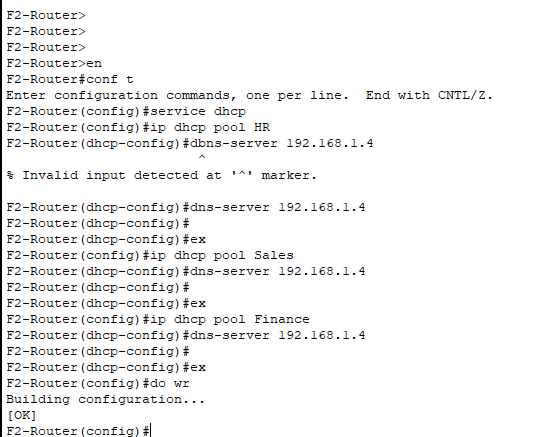


Serial0/3/1

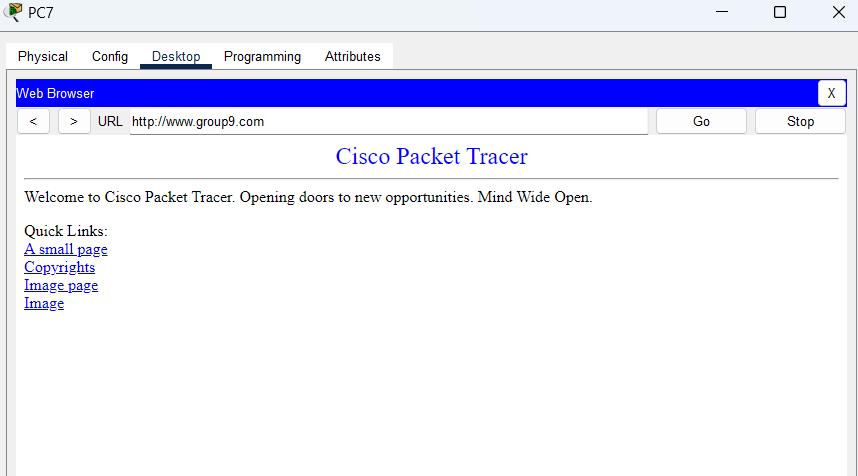


**DNS Server Configuration:**

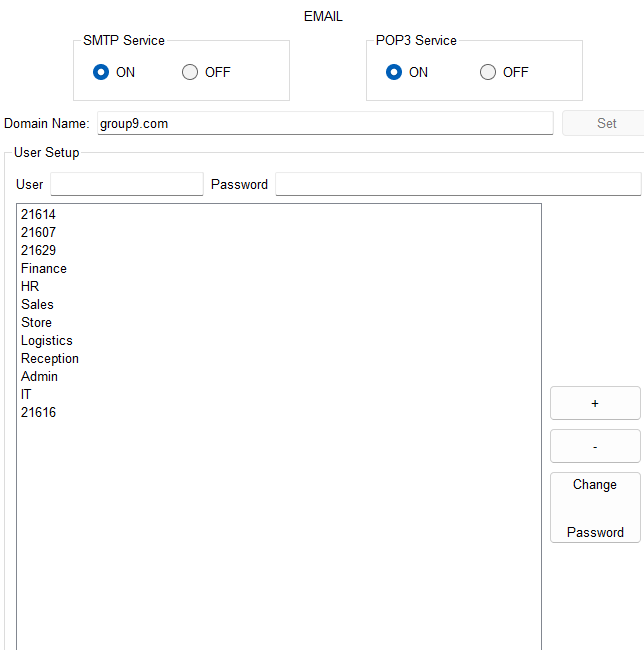




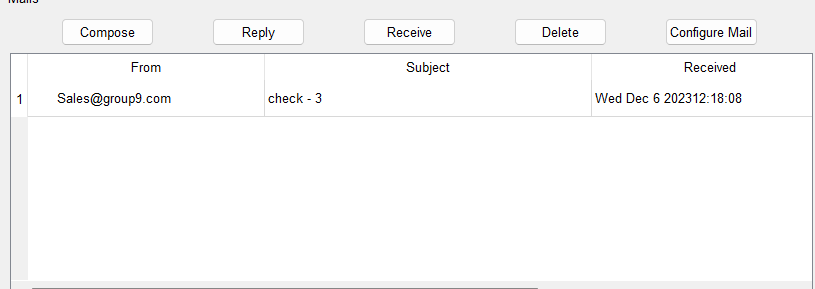
**Working of DNS Server:**

****

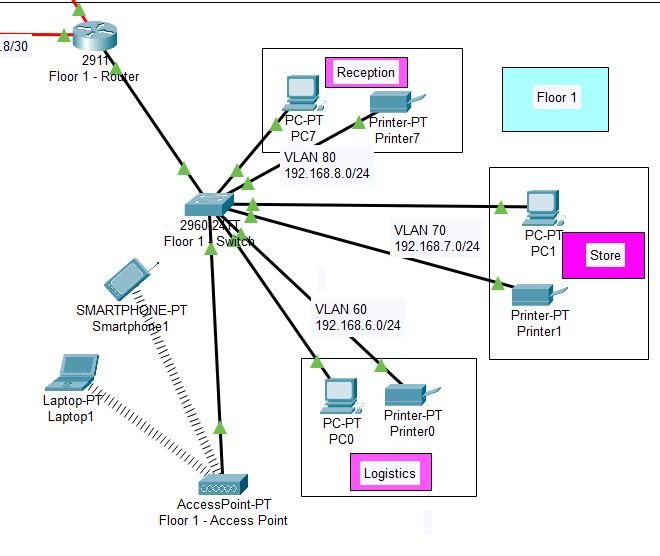
**EMAIL Server Configuration:**



**Working of EMAIL Server:**



* **Floor - 1**



**Assigned IP Addresses:**

192.168.7.2- PC

192.168.7.3 - Printer

192.168.8.2- PC

192.168.8.3 – Printer

192.168.6.2- PC

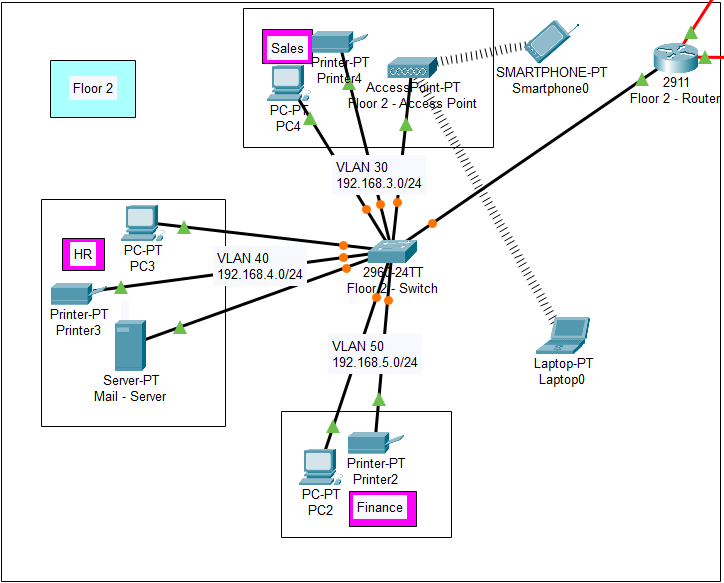
192.168.6.3 – Printer

192.168.6.3 – Access Point

Subnet Mask- 255.255.255.0

DNS Server- 192.168.1.4

* **Floor - 2**



**Assigned IP Addresses:**

192.168.5.2- PC

192.168.5.3 - Printer

192.168.4.2- PC

192.168.4.3 – Printer

192.168.4.4 – EMAIL Server

192.168.3.2- PC

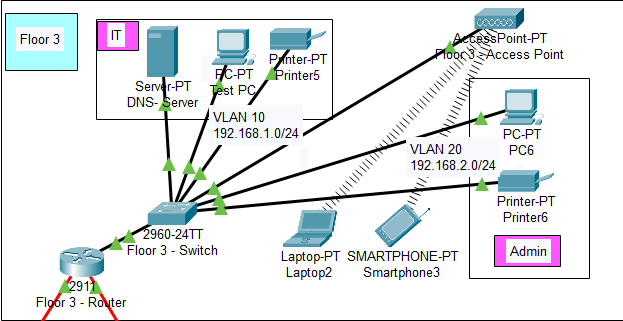
192.168.3.3 – Printer

192.168.3.3 – Access Point

Subnet Mask- 255.255.255.0

DNS Server- 192.168.1.4

* **Floor - 3**



**Assigned IP Addresses:**

192.168.1.2- PC

192.168.1.3 - Printer

192.168.1.4 – DNS Server

192.168.2.2- PC

192.168.2.3 – Printer

192.168.2.3 – Access Point

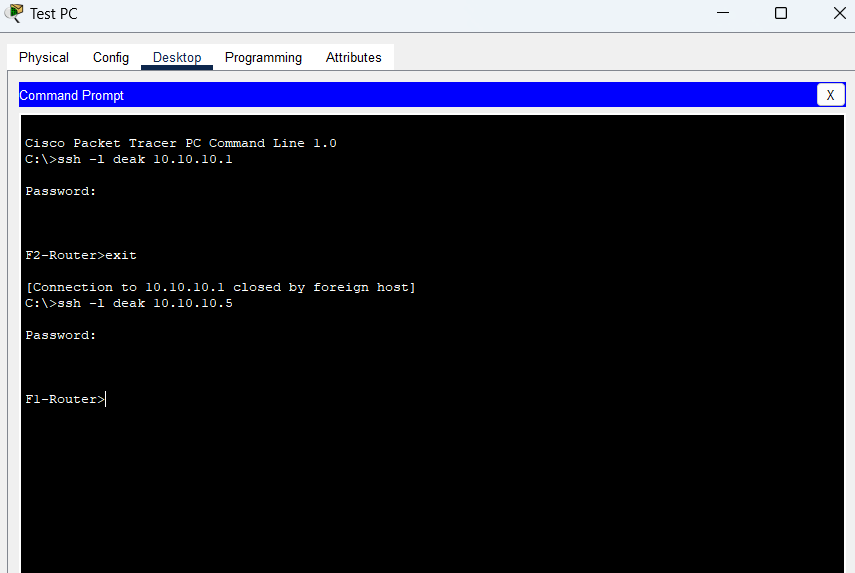
Subnet Mask- 255.255.255.0

DNS Server- 192.168.1.4

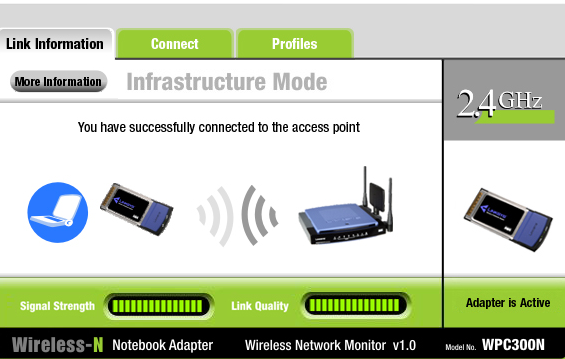
* **Securing the Network**

Routers are secured with SSH (Secure Shell). Routers and their assigned passwords are mentioned below:

|  |  |
| --- | --- |
| **Router Name** | **Passwords** |
| 1. Floor – 1 Router | Console password: deak  ssh password: deak |
| 1. Floor – 2 Router | Console password: deak  ssh password: deak |
| 1. Floor – 3 Router | Console password: deak  ssh password: deak |

****

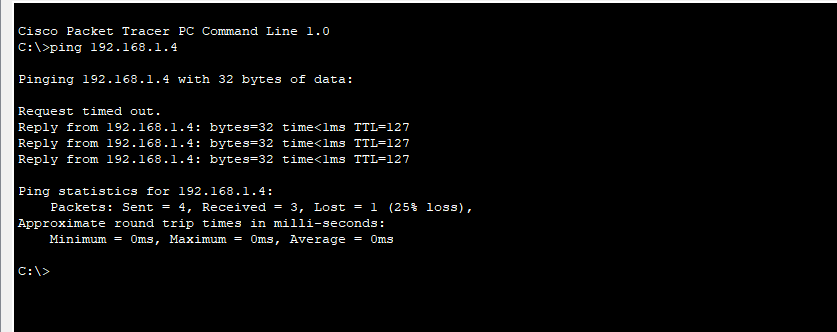
**Connectivity of Wireless Network on Computing Devices:**

****

* **Ping Test:**

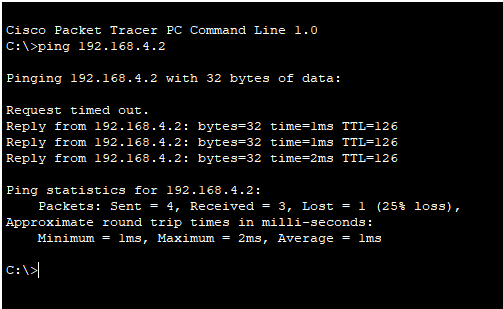
Network connectivity and communication can be tested using the ping command, followed by the domain name or the IP address of the device (equipment) whose connectivity one wishes to verify.

**Ping Test for DNS Server:**

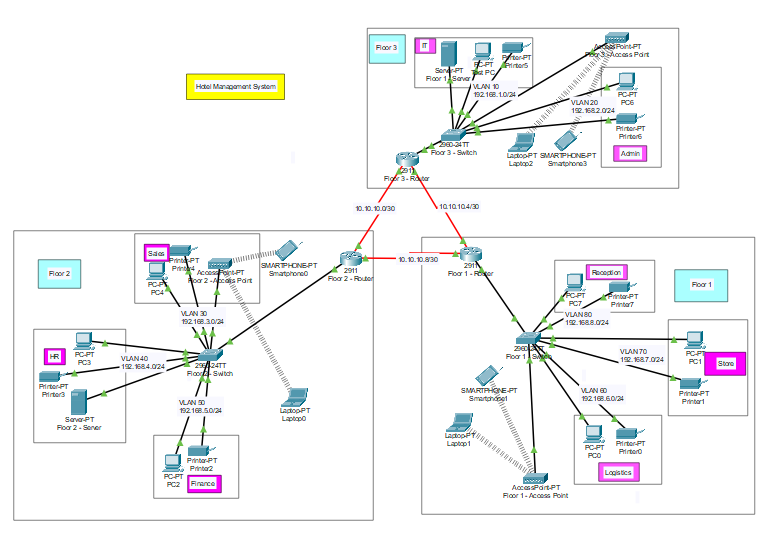
IP Address: 192.168.1.4 ****

**Ping Test for EMAIL Server:**

IP Address: 192.168.4.2

****

**CONCLUSION:**



**Architecture of the Hotel management Network Scenario Designed in Cisco Packet Tracer environment**

In conclusion, a well-designed and efficiently managed network system is indispensable for the seamless operation of a hotel management system. The integration of multiple VLANs and departments necessitates careful attention to network performance, ensuring that communication and data transfer remain smooth and uninterrupted. By proactively measuring and optimizing network performance, hotel IT staff can address potential issues, allocate resources effectively, and maintain a reliable infrastructure that supports the diverse operational needs of the hotel. Ultimately, a robust network system is fundamental to providing exceptional service to both staff and guests, and it underpins the successful functioning of modern hotel management systems.

In conclusion, a well-designed and efficiently managed network system is indispensable for the seamless operation of a hotel management system. The integration of multiple VLANs and departments necessitates careful attention to network performance, ensuring that communication and data transfer remain smooth and uninterrupted. By proactively measuring and optimizing network performance, hotel IT staff can address potential issues, allocate resources effectively, and maintain a reliable infrastructure that supports the diverse operational needs of the hotel. Ultimately, a robust network system is fundamental to providing exceptional service to both staff and guests, and it underpins the successful functioning of modern hotel management systems.