**COMPUTER NETWORKS**

**DOCUMENTATION ON HOTEL MANAGEMENT SYSTEM DESIGN USING PACKET TRACER**

**COURSE COORDINATOR: PROFESSOR KHONDEKAR LUTFUL HASAN**

**DEPT. OF CSE, ALIAH UNIVERSITY**

**SUBJECT CODE: CSEUGPC23**

**SEMESTER: 6TH YEAR: 3RD**

**PROGRAM: B. TECH DEPARTMENT: COMPUTER SCIENCE AND**

**ENGINEERING**

**GROUP MEMBERS:**

|  |  |
| --- | --- |
| **NAME** | **ROLL NO** |
| **RAJASREE LAHA** | **CSE214002** |
| **MOUBANI SHEE** | **CSE214019** |

**CONTENTS**

* INTRODUCTION
* THEORY
* NETWORK LAYOUT
* NETWORK CONFIGURATION
* IMPORTANCE OF THIS PROJECT
* CONCLUSION

**Acknowledgment**

We would like to express our sincere gratitude to Mr. Khondekar Lutful Hasan for his invaluable guidance and support throughout this project. Their expertise and insights have been instrumental in successfully completing the Vic Modern Hotel network design and implementation.

This comprehensive documentation provides a detailed overview of the design, implementation, and testing of the Vic Modern Hotel network, serving as a valuable resource for understanding the intricacies of the project.

**Introduction to the Project:**

The entire design of the network proposed for a university is constructed using a Cisco packet tracer which could be used and implemented in real life for better connectivity across a university.

The various devices that are being used in designing the network of **HOTEL MANAGEMENT SYSTEM:**

**1) ROUTER**: A router is a device that forwards data packets along

networks. A router is connected to at least two networks,

commonly two LANs or WANs or a LAN and its ISP's network.

Routers are located at gateways, the places where two or more

networks connect and are the critical device that keeps data

flowing between networks and keeping the networks connected

to the internet. When data is sent between locations on one

network or from one network to a second network the data is

always seen and directed to the correct location by the router.

The router accomplishes this by using headers and forwarding

tables to determine the best path for forwarding the data

packets, and they also use protocols such as ICMP to

communicate with each other and configure the best route

between any two hosts.

Dual WAN 4-Port Gigabit Wireless VPN Router A Linksys Wireless Router DSR-500N.

**2) SWITCH:** A switch is an electrical component that can break an

electrical circuit, interrupting the current or diverting it from

one conductor to another. The most familiar form of switch is a

manually operated electromechanical device with one or more

sets of electric contacts. Each set of contacts can be in one of

two states: either 'closed' meaning the contacts are touching

and electricity can flow between them, or 'open', meaning the

contacts are separated and non conducting. A switch may be

directly manipulated by a human as a control signal to a system,

such as a computer keyboard button, or to control power flow in a circuit, such as a light switch. Automatically-operated

switches can be used to control the motions of machines, for

example, to indicate that a garage door has reached its full

open position or that a machine tool is in a position to accept

another work piece. Switches may be operated by process

variables such as pressure, temperature, flow, current, voltage,

and force, acting as sensors in a process and used to

automatically control a system. For example, a thermostat is

an automatically-operated switch used to control a heating

process. A switch that is operated by another electrical circuit is

called a relay. Large switches may be remotely operated by a motor drive mechanism.

**Network Switches**

**3) MULTILAYER SWITCH:** MLS provides high-performance Layer 3

switching for Cisco routers and switches. MLS switches IP data

packets between subnets using advanced application-specific

integrated circuit (ASIC) switching hardware. Standard routing

protocols, such as Open Shortest Path First (OSPF), Enhanced

Interior Gateway Routing Protocol (Enhanced IGRP), Routing

Information Protocol (RIP), and Intermediate

System-to-Intermediate System (IS-IS), are used for route

determination. MLS enables hardware-based Layer 3 switching

to offload routers from forwarding unicast IP data packets over

shared media networking technologies such as Ethernet. The

packet forwarding function is moved onto Layer 3 Cisco series

switches whenever a partial or complete switched path exists

between two hosts. Packets that do not have a partial or

complete switched path to reach their destinations still use

routers for forwarding packets. MLS also provides traffic

statistics as part of its switching function. These statistics are

used for identifying traffic characteristics for administration,

planning, and troubleshooting. MLS uses NetFlow Data Export

(NDE) to export the flow statistics.

Cisco MDS 9396S 16G Multilayer Fabric Switch

e ROLE OF SWITCHES IN NETWORK - Switches may operate

at one or more layers of the OSI model, including data

link and network. A device that operates simultaneously

at more than one of these layers is known as a multilayer

switch. In switches intended for commercial use, built-in

or modular interfaces make it possible to connect

different types of networks, including Ethernet, Fibre

Channel, ATM, ITU-TG.hn and 802.11.This connectivity

can be at any of the layers mentioned. While layer-2

functionality is adequate for bandwidth-shifting within

one technology, interconnecting technologies such as

Ethernet and token ring is easier at layer 3. Devices that

interconnect at layer 3 are traditionally called routers, so

layer-3 switches can also be regarded as (relatively

primitive) routers. In some service provider and other

environments where there is a need for a great deal of

analysis of network performance and security, switches

may be connected between WAN routers as places for

analytic modules. Some vendors provide firewall,

network intrusion detection, and performance analysis

modules that can plug into switch ports. Some of these

functions may be on combined modules. In other cases,

the switch is used to create a mirror image of data that

can go to an external device. Since most switch port

mirroring provides only one mirrored stream, network

hubs can be useful for fanning out data to several

read-only analyzers, such as intrusion detection systems

and packet sniffers.

**4)SERVER :**

1) In information technology, a server is a computer program that

provides services to other computer programs (and their users) in the same or other computers.

2) The computer that a server. program runs in is also frequently

referred to as a server.

**Theory**

Computer networking is the practice of interfacing two or

more computing devices with each other to share

data. Computer networks are built with a combination of hardware and software.

Note: This page focuses on wireless networking and computer

networks, which is related, but quite different, from social

networking.

**◍Computer Network Classification and Area Networks:**

Computer networks can be categorized in several different ways. One approach defines the type of network according to the geographic area it spans. Local area networks (LANs), for example, typically span a single home, school, or small office building, whereas wide area networks (WANs), reach across cities, states, or even across the world. The Internet is the world's largest public WAN.

**◍Network Design:**

Computer networks also differ in their design approach. The two basic forms of network design are called client/server and peer-to-peer.

Client-server networks feature centralized server computers that

store email, Web pages, files and or applications accessed by client computers and other client devices. On a peer-to-peer network,

conversely, all devices tend to support the same functions.

Client-server networks are much common in business and

peer-to-peer networks more common in homes.

A network topology defines its layout or structure from the point of view of data flow. In so-called bus networks computers share and communicate across one common conduit,

whereas in a star network, all data flows through one centralized

device. Common types of network topologies include bus, star, ring networks and mesh networks.

Computer Network Hardware and Software

Special purpose communication devices including network routers,

access points, and network cables physically glue a network together.

Network operating systems and other software applications generate network traffic and enable users to do useful things.

Home Computer Networking

While other types of networks are built and maintained by

engineers, home networks belong to ordinary homeowners, people often with little or no technical background. Various manufacturers produce broadband router hardware designed to simplify home network setup. A home router enables devices in different rooms to efficiently share a broadband Internet connection, helps people to more easily share their files and printers within the network, and improves overall network security.

Home networks have increased in capability with each generation of new technology. Years ago, people commonly set up their home network just to connect a few PCs, share some documents and perhaps a printer. Now it's common for households to also network game consoles, digital video recorders, and smartphones for streaming sound and video. Home automation systems have also existed for many years, but these too have grown in popularity more recently with practical systems for controlling lights, digital thermostats, and appliances.

Business Computer Networks

Small and home office (SOHO) environments use similar technology as found in home networks. Businesses often have additional communication, data storage, and security requirements that require expanding their networks in different ways, particularly as the business gets larger.

Whereas a home network generally functions as one LAN, a business network tends to contain multiple LANs. Companies with buildings in multiple locations utilize wide-area networking to connect these branch offices together. Though also available and used by some households, voice over IP communication and network storage and backup technologies are prevalent in businesses. Larger companies also maintain their own internal Web sites, called intranets to help with employee business communication.

**◍Project Scope:**

The scope of the project encompasses the design and implementation of network topology, VLAN configuration, DHCP setup, SSH configuration, and port security measures for the Vic Modern Hotel.

Additionally, the project includes testing and verification procedures to ensure the reliability and functionality of the deployed network infrastructure.

**◍Network Topology:**

Physical Layout: The server room is centrally located within the IT department on the third floor to facilitate easy access and maintenance of network equipment.

Logical Layout: A hierarchical network design is adopted, with routers connecting each floor and switches deployed on each floor to connect departmental devices.

Device Specifications: Cisco routers and switches are utilized, with specific models chosen based on performance, scalability, and feature requirements.

A computer screen shot of a computer

Description automatically generated

**◍Technologies Implemented:**

Hierarchical Network Design: The hierarchical design provides scalability and facilitates efficient traffic management by segregating network functions into distinct layers.

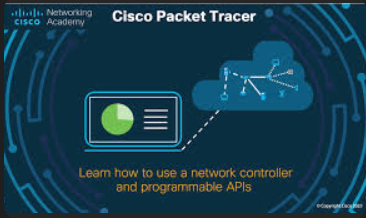
Subnetting and IP Addressing: Subnets are meticulously planned and allocated to accommodate each department's network requirements while minimizing IP address wastage.

Port Security: Port security features are configured on switches to mitigate security risks associated with unauthorized access to network resources.

WLAN Configuration: Wireless networks are configured using Cisco Access Points to provide seamless connectivity for laptops and mobile devices throughout the hotel premises.

**◍Hardware and Software Requirements:**

The hardware requirements include Cisco routers, switches, and access points, pc, printers, while the software requirements comprise the Cisco Packet Tracer for network simulation and configuration.

**◍Physical Setup:**

Here is the detailed documentation of the physical setup, including the placement of routers, switches, and access points within the hotel premises.

Description of cabling infrastructure used to interconnect network devices and ensure reliable data transmission.

**◍VLAN Configuration:**

VLAN Design Considerations: The rationale behind VLAN assignment for each department is explained, emphasizing security, performance, and manageability.

VLAN Implementation: Step-by-step instructions on VLAN configuration, including VLAN creation, port assignment, and VLAN interface configuration.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Inter-VLAN Routing: Explanation of router-on-a-stick configuration for inter-VLAN communication, along with configuration steps and verification procedures.

**◍Inter-VLAN Routing:**

A detailed explanation of how inter-VLAN communication is facilitated using router sub-interfaces, VLAN tagging, and routing protocols such as OSPF.

**◍DHCP Setup:**

Configuration of DHCP pools on routers to dynamically allocate IP addresses to devices within each VLAN.

Explanation of DHCP server role on routers and configuration steps for DHCP pool setup.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen with a white screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**◍SSH Configuration:**

Secure Access Management: The importance of SSH for secure remote access to network devices is emphasized, highlighting its superiority over less secure protocols like Telnet.

SSH Configuration Steps: Detailed instructions on SSH configuration for routers, including key generation, user account creation, and access control settings.

Best Practices: Recommendations for implementing SSH security best practices to safeguard against unauthorized access and ensure secure remote management.

**◍Port Security Configuration:**

Configuration of port security features on switches to prevent unauthorized access to network resources.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Description of sticky MAC address learning method and its implementation to enhance port security.

**◍Total Configuration:**

en

F2-Router#sh start

Using 1789 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname F2-Router

!

!

!

!

!

ip dhcp pool Finance

network 192.168.5.0 255.255.255.0

default-router 192.168.5.1

dns-server 192.168.5.1

ip dhcp pool HR

network 192.168.4.0 255.255.255.0

default-router 192.168.4.1

dns-server 192.168.4.1

ip dhcp pool Sales

network 192.168.3.0 255.255.255.0

default-router 192.168.3.1

dns-server 192.168.3.1

!

!

!

no ip cef

no ipv6 cef

!

!

!

username gtech password 0 gtech

!

!

license udi pid CISCO2911/K9 sn FTX1524W341-

!

!

!

!

!

!

!

!

!

ip domain-name gtech

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface GigabitEthernet0/0

no ip address

duplex auto

speed auto

!

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.3.1 255.255.255.0

!

interface GigabitEthernet0/0.40

encapsulation dot1Q 40

ip address 192.168.4.1 255.255.255.0

!

interface GigabitEthernet0/0.50

encapsulation dot1Q 50

ip address 192.168.5.1 255.255.255.0

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface GigabitEthernet0/2

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/2/0

ip address 10.10.10.1 255.255.255.252

!

interface Serial0/2/1

ip address 10.10.10.10 255.255.255.252

clock rate 64000

!

interface Vlan1

no ip address

shutdown

!

router ospf 10

log-adjacency-changes

network 10.10.10.0 0.0.0.3 area 0

network 10.10.10.8 0.0.0.3 area 0

network 192.168.3.0 0.0.0.255 area 0

network 192.168.4.0 0.0.0.255 area 0

network 192.168.5.0 0.0.0.255 area 0

!

ip classless

!

ip flow-export version 9

!

!

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

!

!

!

end r ata holo total ki ki configured acha seta

**◍Testing and Verification:**

Test Plan: Outline of the test plan used to validate network functionality, including connectivity tests, DHCP lease verification, and inter-department communication tests.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer program

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated

Results Analysis: Analysis of test results, identification of issues encountered, and steps taken to troubleshoot and resolve them.

A computer screen shot of a computer

Description automatically generated

Performance Metrics: Measurement of network performance metrics such as latency, throughput, and packet loss to ensure optimal operation.

**Troubleshooting:**

During implementation, issues like IP conflicts, faulty cables, and misconfigured routers were encountered. Troubleshooting steps included verifying physical connections, using diagnostic tools to ping and trace routes, and resetting network devices. Common network troubleshooting techniques involve checking for IP address conflicts, ensuring correct DNS settings, and examining firewall configurations. Best practices include documenting network changes, keeping firmware updated, and using reliable network monitoring tools. Regularly backing up configurations and implementing robust security measures also help prevent and quickly resolve connectivity issues.

**Future Recommendations:**

**Next-Generation Technologies:**

* **SDN and NFV:** Centralize control and virtualize network services for flexibility and cost reduction.
* **5G and Wi-Fi 6:** Prepare for higher bandwidth and lower latency to support more devices and better performance.

**Security Improvements:**

* **Zero Trust Architecture:** Trust no device by default, enhancing internal and external threat protection.
* **AI-based Threat Detection:** Use AI for proactive threat identification and response.
* **SASE:** Combine network security with WAN capabilities for simplified management and secure access.

**Performance Enhancements:**

* **Network Optimization:** Deploy advanced tools to identify and mitigate bottlenecks.
* **QoS Policies:** Prioritize critical applications to reduce latency.
* **Edge Computing:** Process data closer to its source, reducing latency and bandwidth use.

**Scalability:**

* **Modular Design:** Use modular components for easy expansion.
* **Cloud Integration:** Leverage cloud services for elastic scalability and cost efficiency.
* **Automation:** Implement automation tools for streamlined management and rapid scaling.

**Lessons Learned:**

* **Documentation:** Develop comprehensive network documentation.
* **Continuous Monitoring:** Regularly audit and monitor the network for proactive issue resolution.
* **Training:** Provide ongoing training on new technologies.
* **Feedback Loop:** Integrate user feedback for continuous improvement.

**IMPORTANCE OF THIS PROJECT**

Wide Area Networks are spread over a (very) wide area so

that companies and institutes that are located far from each

other are directly connected via the network. Wide Area

Networks have mostly on more than one location external

connections with other big networks. Internet Service

Providers (ISPs) and multinationals with many offices

frequently own a WAN themselves. Regional education

networks and company networks between several

establishments are also examples of Wide Area Networks.

Two great advantages of WAN are allowing secure and fast

data transmission between the different nodes in the

network. The data transmission is also reliable and

inexpensive. The characteristics of the transmission

facilities lead to an emphasis on efficiency of

communications techniques in the design of WANs.

Controlling the volume of traffic and avoiding excessive

delays is important. Since the topologies of WANs are likely

to be more complex than those of LANs, routing algorithms

also receive more emphasis. Many WANs also implement

sophisticated monitoring procedures to account for which

users consume the network resources.

**Conclusion:**

Project Summary: Summary of key achievements and successful completion of the Vic Modern Hotel network project.

Lessons Learned: Reflection on challenges faced and lessons learned during the project, providing insights for future network design endeavours.

Future Outlook: Discussion of potential future directions for the network, including opportunities for further optimization and expansion.

**References:**

1. "Computer Networks." Pearson.Forouzan, B. A. (2012).

2. "Data Communications and Networking." McGraw-Hill Education.Cisco. (2021).

3. "OSPF Configuration Guide." Retrieved from Cisco OSPF Configuration Guide.Stallings, W. (2013).

4. "NetworK Security Essentials." Pearson.Cisco. (2019).