SMALL BUISNESS NETWORK DESIGN WITH GUEST NETWORK

18CSS202J - COMPUTER COMMUNICATIONS

Mini Project

Submitted by

Rhythm Rohatgi [Reg No: RA2011003010335]

Abhishek Dubey [Reg No: RA2011003010308]

Ritik Gupta [Reg No: RA2011003010324]

Anuj Bansal [Reg No: RA2011003010311]

Under the guidance of

Mr. JAGADEESAN

(Assistant Professor, Department of Computer Science and Engineering)

BACHELOR OF TECHNOLOGY

in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

of

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR- 603 203

MAY 2022

SRM INSTITUTION OF SCIENCE AND

TECHNOLOGY KATTANKULATHUR-603203

BONAFIDE
CERTIFICATE

Certified that this lab report titled **"SMALL BUISNESS NETWORK DESIGN WITH GUEST NETWORK"** is the bonafide work done by **Rhythm Rohatgi [RA2011003010335], Abhishek Dubey [RA2011003010310], Ritik Gupta [RA2011003010324], Anuj Bansal [RA2011003010311]** who carried out the lab exercises under my supervision. Certified further, that tothe best of my knowledge the work reported herein does not form part of any other work.

SIGNATURE

MR. JAGADEESAN

Computer Communications – Course Faculty

Assist

ant Professor Department

of computing technologies

TABLE OF CONTENTS

CHAPTERS

ABSTRACT

This report describes the network design of Health care management or Hospital. In this network topology the nodes (i.e., computers, switches, routers or other devices) are connected to a local area network (LAN) and network via links (twisted pair copper wire cable or optical fiber cable). We have used Cisco Packet Tracer for designing the network topology It's a general design which can be implemented at any higher level to manage network system.

OBJECTIVE

The objective of network design is to satisfy data communication requirements while minimizing expense.

INTRODUCTION

Networking is refered as connecting computers electronically for the purpose of sharing information. Resources such as a file, applications, printers & software are some common information shared in a networking.The advantages of networking can be seen clearly in terms of security, efficiency, manageability & and cost effectiveness as in allows collaboration between users in a wide range. The Switches and Router this device that play an important role in data transfer from one place to another using different technology such as a radio waves & wire.

LAN network is made up of two or more computers connected together in a short distance usually at home, offices buildings or school. WAN is a network that covers wider area than LAN and usually covers cities, countries and the whole world. Several major LAN can be connected together to form a WAN. As a several devices are connected to network, it is important to ensure data collision does not happen when this device attempt to use data channel simultaneously. A set of rules called carrier sense multiple access/collision detection are used to detect and prevent collision in networks.

MODULES

- DHCP

The Dynamic Host Configuration Protocol (DHCP) is a network

management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.

DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

There are many versions of DCHP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

- DNS

The Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

The domain name system (i.e., “DNS”) is responsible for translating domain names into a specific IP address so that the initiating client can load the requested Internet resources. The domain name system works much like a phone book where users can search for a requested person and retrieve their phone number. DNS servers translate requests for specific domains into IP addresses, controlling which server users with access when they enter the domain name into their browser.

- SUBNETTING

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.

Organizations will use a subnet to subdivide large networks into smaller, more efficient subnetworks. One goal of a subnet is to split a large network into a grouping of smaller, interconnected networks to help minimize traffic. This way, traffic doesn't have to flow through unnecessary routs, increasing network speeds.

- HTTPS

Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol. It is used for secure communication over a computer network and is widely used on the Internet. Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol. It is used for secure communication over a computer network and is widely used on the Internet.

- **SSH**

  Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

  SSH enables us to provide a service with encrypted access for the widest range of operating systems (Windows XP-10, Max OS X and Linux); this would not be possible if we provided Windows networked drives (which utilise the SMB/CIFS communication protocol). SSH is reliable and secure and is often used in the High Performance Computing community for this reason.

- **SMTP**

  The Simple Mail Transfer Protocol is a communication protocol for electronic mail transmission.

  The main purpose of SMTP is used to set up communication rules betweenservers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind

- **FTP**

  The File Transfer Protocol is a standard network protocol used for the transfer of computer files between a client and server on a computer network.

  FTP works by opening two connections that link the computers trying to communicate with each other. One connection is designated for the commands and replies that get sent between the two clients, and the other channel handles the transfer of data. During an FTP transmission, there are four commands used by the computers, servers, or proxy servers that are communicating. These are “send,” “get,” “change directory,” and “transfer.”

- **WIFI**

  Wi-Fi is the name of a wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. WiFi is a freedom – freedom from wires. It allows you to connect to the Internet from just about anywhere — a coffee shop, a hospital room, or a conference room at work. What’s more – it is almost 10 times faster than a regular dial-up connection. WiFi networks operate in the unlicensed 2.4 radio bands, with an 11 Mbps (802.11b) or 54 Mbps (802.11a) data rate, respectively.

VLAN and IP Network Design

VLAN's are created and mapped with each department. 1. VLAN 2 – Hospital Authority

2. VLAN 3 – Hospital Service Provider

3. VLAN 4 – Guests

IP networks are created for each VLAN and mapped with the same. The IP address range for users and systems which can be used on the specific department is also included.

VLAN	IP Network Address	IP Address range
VLAN 2	192.168.2.0/24	192.168.2.2- 192.168.2.21
VLAN 3	192.168.3.0/24	192.168.3.2- 192.168.3.41
VLAN 4	192.168.4.0/24	192.168.4.2- 192.168.4.101

PROCEDURE :-

1. The DHCP server is connected to port, which is a member of VLAN 2 The IP address of DHCP server of Hospital server authority is 192.168.3.2 and IP address of hospital authority server is 192.168.2.2

2. Access points are configured with IP address belonging to the VLAN 4 network address range.

3. Switch Configuration

Detailed configuration details on the switches in cicso switch is required. **a.** Create the VLAN's lines namely VLAN 2, VLAN 3, and VLAN 4 with respect to the switch

switch(config)#vlan 2
switch(config-vlan)#name Hospital authority switch(config-vlan)#exit

switch(config)#vlan 3
switch(config-vlan)#name Hospital service providers switch(config-vlan)#exit

switch(config)#vlan 4

switch(config-vlan)#name Guests
switch(config-vlan)#exit

b. Now let's configure appropriate ports on the switch as members of respective VLAN. Only two ports for each vlans are displayed and that can be added based on requirement.

switch(config)#interface fa 0/2
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2

switch(config)#interface fa 0/3
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2

switch(config)#interface fa 0/4
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2

and config the other Fa interface to VLAN 2 as shown above from switch 0 Similarly for Switch 1 and 2 configuration is made with Vlan 3 and 4 respectively

For Switch 1

switch(config)#interface fa 0/2
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 3

For all the Fa interface to VLAN 3 as shown above.

For Switch 2

switch(config)#interface fa 0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 4

For all the Fa interface to VLAN 4 as shown above.

c. Configure the port connected to the router as trunk. This enables in allowing traffic from all the vlans to the router where appropriate routing and access restriction are performed.

switch(config)#interface fa 0/1
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk allowed vlan all
switch(config-if)#exit

4. Router configuration

The below configuration is for the router in the Packet diagram **a.** The interface connected to the internet is configured with the appropriate IP address.

router(config)#interface fa 0/0
router(config-if)#ip address 50.1.1.2 255.0.0.0
router(config-if)#no shutdown

router(config-if)#exit
router(config)#interface fa 0/1
router(config-if)#ip address 8.8.8.1 255.0.0.0
router(config-if)#no shutdown

b. Sub interfaces on the router on physical interface Fa0/0 are mapped with appropriate VLAN and IP address. These configured address on router are default gateway address for users for respective VLAN.

router(config)#interface fa 0/0.1
router (conf ig-subif)#encapsulation dot1Q 2
router(config-subif)#ip address 192.168.2.1 255.255.255.0
router(config-subif)#no shutdown
router(config-subif)#exit
router(config)#interface fa 0/0.2
router(config-subif)#encapsulation dot1Q 3
router(config-subif)#ip address 192.168.3.1
255.255.255.0 router(config-subif)#no shutdown
router(config-subif)#exit
router(config)#interface fa 0/0.3
router(config-subif)#encapsulation dot1Q 4
router(config-subif)#ip address 192.168.4.1
255.255.255.0 router(config-subif)#no shutdown
router(config-subif)#exit

c. The IP helper address is configured on VLAN 3 and 4 interface of router. This is configured for uses in their respective VLANs to reach DHCP server for obtaining dynamic IP address. The configuration is

router(config)#interface fa 0/0.1
router(config-subif)#ip helper-address 192.168.2.2
router(config-subif)#exit
router(config)#interface fa 0/0.7
router(config-subif)#ip helper-address 192.168.3.2
router(config-subif)#exit
router(config)#interface fa 0/0.3
router(config-subif)#ip helper-address 192.168.4.2
router(config-subif)#exit

d. Appropriate access control list is configured on router. This is to deny access from guest network to other 2 networks which are an extended ACL. The first 2 lines deny access from guest network to hospital authority and Hospital server provider networks. Third entry allows all other traffic. This is for internet connection and the access control list is applied in guest vlan interface on router as inbound.

router(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255 192.168.2.0 0.0.0.255

router(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255 192.168.3.0 0.0.0.255

router(config)#access-list 101 permit ip any any
router(config)#interface fa 0/0.2
router(config-subif)#ip access-group 101 inbound

e. Access control list to restrict access from hospital service network to hospital authority network. The first line allows hospital service provider network to access the hospital authority. The second line denies all communication to hospital authority network and third line allows all other communications that is for internet. Access list is applied inbound on VLAN interface corresponding to hospital authority network.

router(config)#access-list 102 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.2
router(config)#access-list 102 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
router(config)#access-list 101 permit ip any any
router(config)#interface fa 0/0.7
router(config-subif)#ip access-group 102 inbound

5. <u>Firewall Configuration</u>

We used ASA1 firewall in this design as it can work as a bridge between Vlan's when configured. Considering the restrictions of access between the Vlans this is best way to config and implement the design

ciscoasa(config)#interface vlan 2
ciscoasa(config)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.2.0 255.255.255.0
ciscoasa(config-if)#exit
ciscoasa(config)#interface vlan 2
ciscoasa(config)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address 192.168.2.0 255.255.255.0
ciscoasa(config-if)#exit

Similarity we restrict the IP address such that no guest can access Hospital service provider or Hospital authority and Hospital service can't access Hospital authority only where as Hospital authority has access to all the Vlans.

6. <u>DHCP Configuration</u>

DHCP configuration are made to assign IP automatically to the end devices. For this process we gave a pool of address encapsulated such that an IP address is assigned to end devices automatically.

Router#sh ip dhcp pool
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool dv2
Router(dhcp-config)#network 192.168.2.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.2.1.
Router(dhcp-config)#ip dhcp pool dv3
Router(dhcp-config)#network 192.168.3.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.3.1
Router(dhcp-config)#ip dhcp pool dv4
Router(dhcp-config)#network 192.168.4.0 255.255.255.0
Router(dhcp-config)#network 192.168.4.0 255.255.255.0
%DHCPD-4-PING_CONFLICT: DHCP address confl Router(dhcp-config)#default router 192.168.4.1 Router(dhcp-config)#ex
Router(config)#ex
Router#%SYS-5-CONFIG_I: Configured from console by console

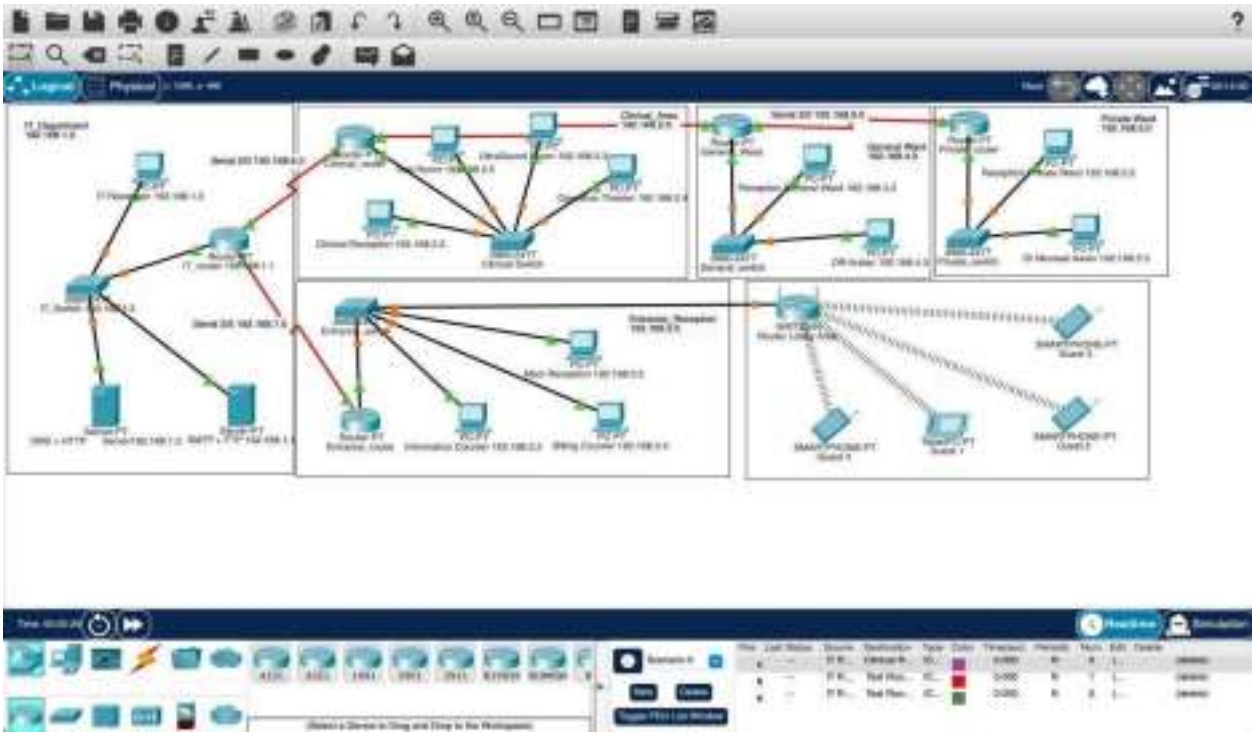
Router#sh run
Building configuration...

Current configuration : 989 bytes
!
version 12.2
no service timestamps log
datetime msec no service
timestamps debug datetime
msec no service password
encryption
!
hostname Router
!
!
!
!
!
ip dhcp pool dv2
network 192.168.2.0 255.255.255.0
default-router
192.168.2.1 ip
dhcp pool dv3
network 192.168.3.0 255.255.255.0
default-router
192.168.3.1 ip
dhcp pool dv4
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1

NETWORK DIAGRAM

INFERENCE

This report describes how we have designed network topology of hospital (Health care Management System). With VLSM for Subnetting, segmented the diagram into 5 segments. This topology can also be implemented on higher level of hospital



REFERENCES

Www.geekforgeeks.com