COMPUTER NETWORKS MINI PROJECT
Review - 1

COMPANY NETWORK DESIGN Using WAN

—

Rusali Saha(RA1911026010095)
Sandra Animon(RA1911026010097)
Vemula Venkata Reshmi(RA1911026010118)

PROBLEM STATEMENT

- **Companies usually operate in different offices, locations, countries - need for a proper interconnected network communication system**

- **Working on singular, local systems can result in huge traffic and time wastage - reductions in productivity and efficiency for the enterprise**

- **Local Area Networks are not useful for communications over large geographical locations - security, traffic**

- **Old methods for local networks — like on-site installations and manual maintenance**

OBJECTIVE:

- To build a networking model to initiate the inter process communication mechanisms while controlling expenses using a **wide area network**
- Model with high reliability and enhanced security
- Sharing and relaying of information to other users instantly between devices around the world
- Editing of remote sites and access to database like financial records
- Build a largely virtualized, cloud-based, and less-expensive solution than the hardware-intensive scenarios of the past

Functionalities and Computing Resources

We will try to implement our network model using the following protocols:

- TELNET and SSH
- SMTP and POP3
- DNS
- DHCP
- FTP and TFTP
- HTTP

We will use the Cisco Packet Tracer and the following devices as resources:

- Routers
- Switches
- Cables
- Servers
- PCs
- Laptops

Alternative Solutions/Methods

1. The current idea of the network system will be implemented using IPv4 protocol. Alternatively, it can also be configured using IPv6.
    a. IPv6 is a new network protocol - improved scalability and routing, security ease-of-configuration and higher performance
    b. IPv6 is incompatible with IPv4, will require changes to the software in every networked device

2. We can use RADIUS SERVER - central server authentication and TELNET configuration.

3. We can implement different router layer security aspects - OSPF, EIGRP, networks and authentication

IPv4 (Internet Protocol Version 4)

1. Encryption and authentication is not provided in IPv4 (Internet Protocol Version 4).

2. Header of IPv4 is 20 – 60 bytes.

3. Packet flow identification is not available in IPv4 (Internet Protocol Version 4).

4. Sender and forwarding routers performs fragmentation in IPv4

5. In IPv4, security features relies on application

6. IPv4 supports DHCP and Manual address configuration

IPv6 (Internet Protocol Version 6)

1. Encryption and authentication is provided in IPv6 (Internet Protocol Version 6).

2. Header of IPV6 is fixed at 40 bytes

3. Packet flow identification is available in IPv6. Flow label field is available in the header.

4. Fragmentation is performed only by the sender in IPv6

5. In IPv6 there is an inbuilt security feature named IPSEC

6. IPv6 supports renumbering and auto address configuration

Design constraints for required performance criteria.

- Expensive to install - setting up a WAN requires extensive purchasing of routers, switches and security solutions.
- Disconnection problems in remote locations
- Maintenance - data center must operate 24/7 requiring a full time job assistance from network administrators and technicians.

PERFORMANCE CRITERIA

- Bandwidth - how rapidly the web server is able to upload the requested information, measure of data or information that can be transmitted in a fixed measure of time.
- Throughput - number of messages successfully transmitted per unit time
- Latency - total time taken for a complete message to arrive at the destination,
- Jitter - interference in the normal order of sending data packets, packets with different delays result in jitter at receiver end

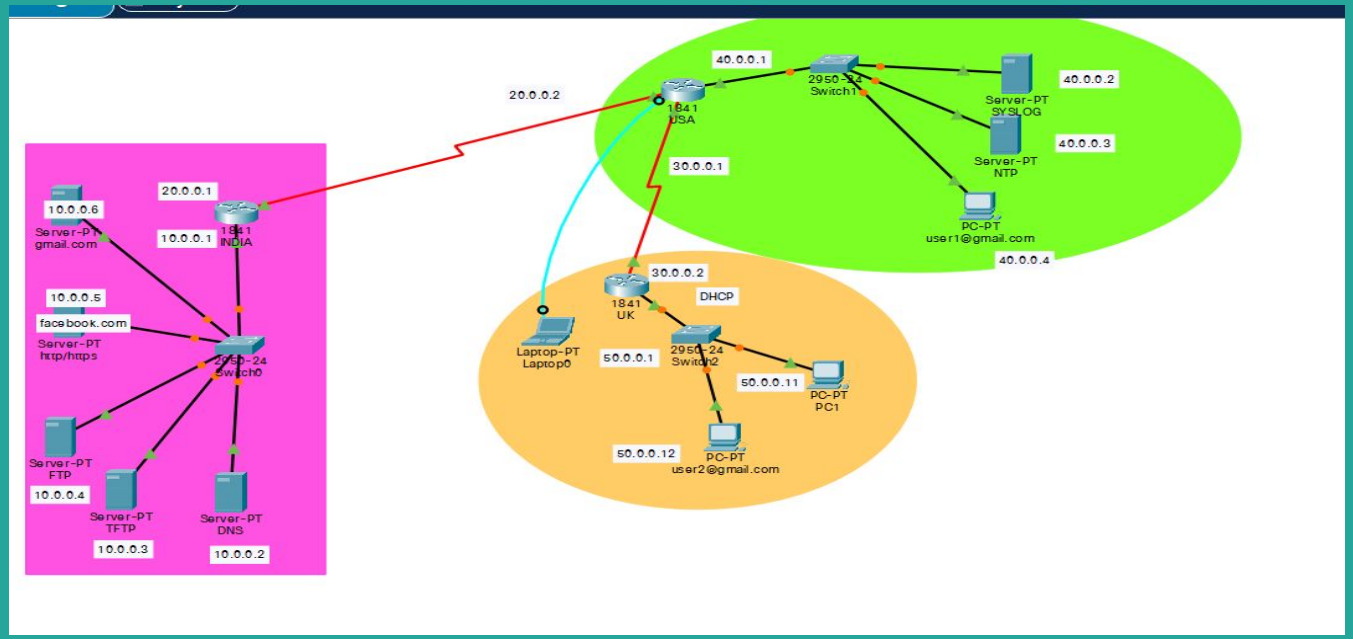
PROTOCOLS SUCCESSFULLY IMPLEMENTED

- **DNS - Domain Name System** is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network
- **TFTP - Trivial File Transfer Protocol** - a simple protocol that provides basic file transfer function with no user authentication, intended for applications that do not need the sophisticated interactions.
- **FTP - The File Transfer Protocol** is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network.
- **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.
- **SYSLOG -System Logging Protocol** (Syslog) is a way network devices can use a standard message format to communicate with a logging server. It was designed specifically to make it easy to monitor network devices. Devices can use a Syslog agent to send out notification messages under a wide range of specific conditions.
- **NTP - Network Time Protocol** (NTP) is a protocol used to synchronize computer clock times in a network. It belongs to and is one of the oldest parts of the TCP/IP protocol suite. The term *NTP* applies to both the protocol and the client-server programs that run on computers.

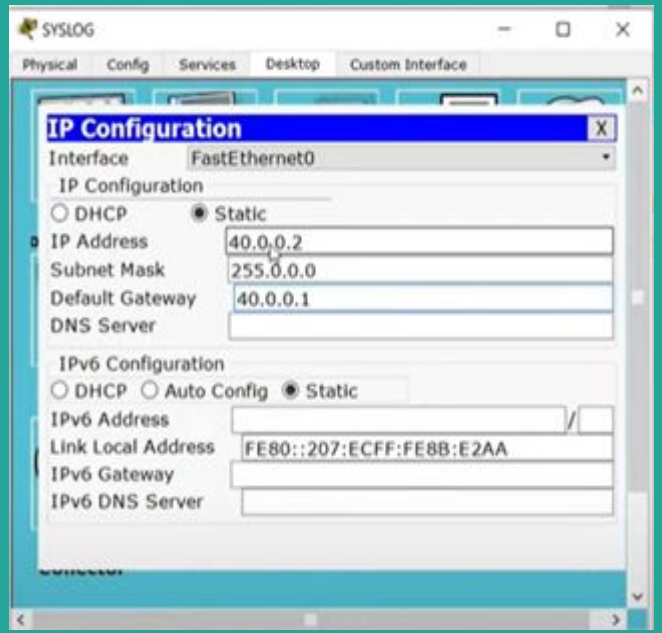
OUR WORKING MODEL DEMO

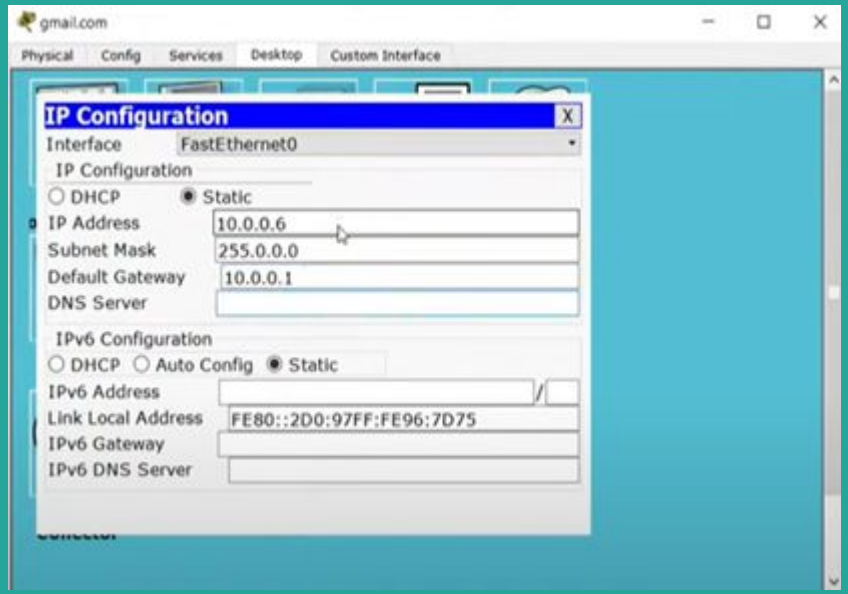
Making of the model

STEP 1 : make the configuration for company branches with different devices

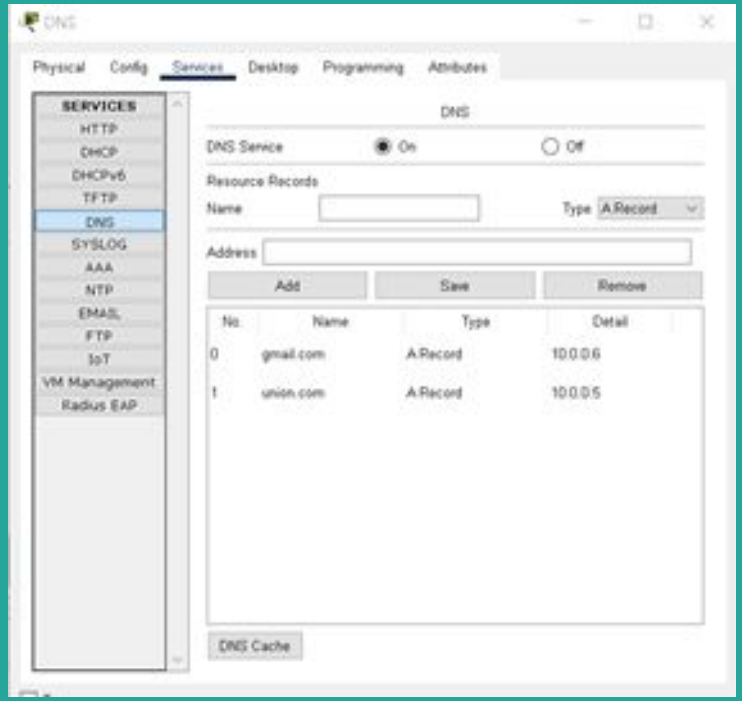


Step2: do IP CONFIGURATION for all devices all devices

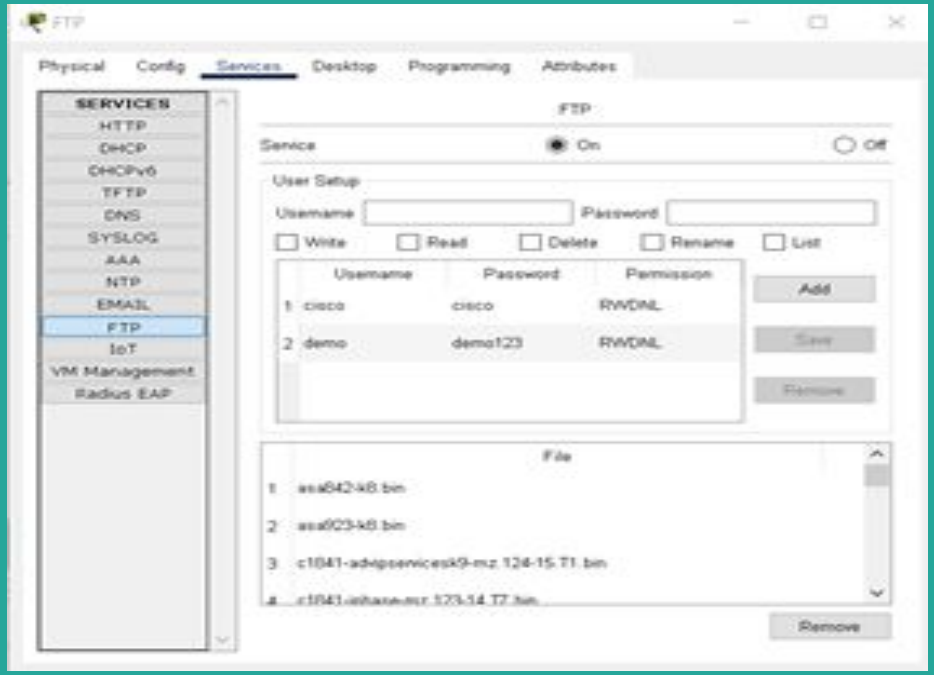




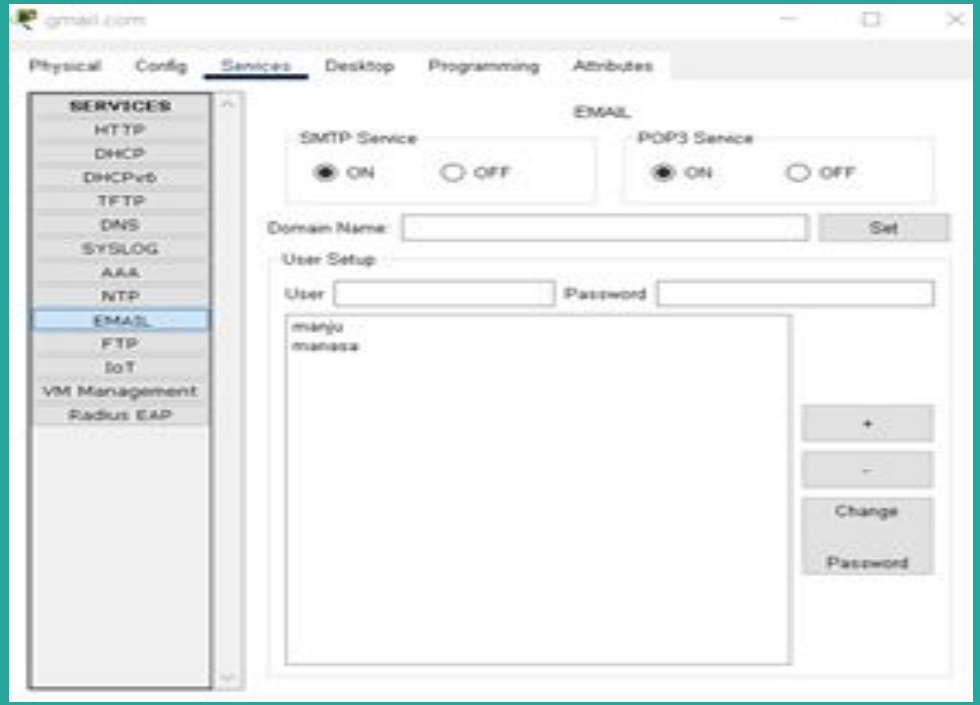
Step3: make DNS for company website and gmail for sending mails



Step4: create a user using FTP SERVER name called demo

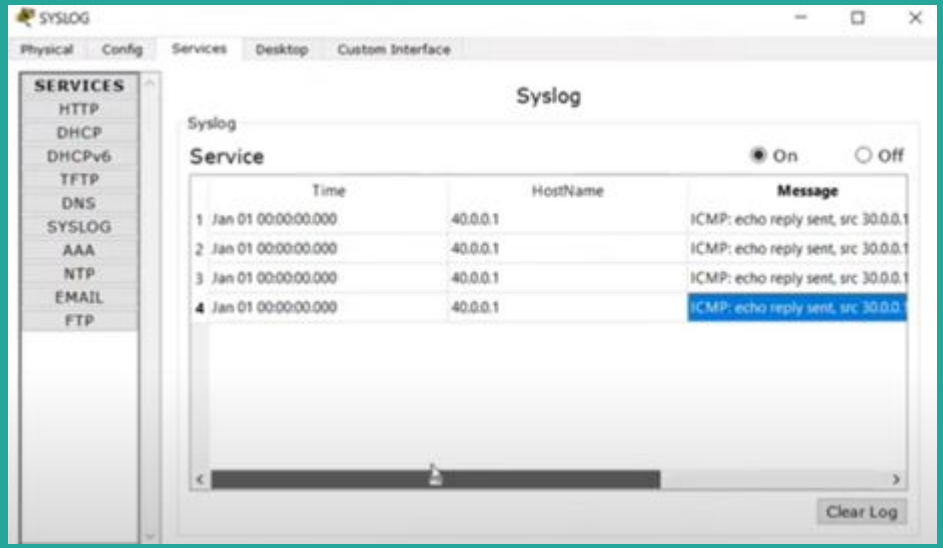


Step5: make users for sending mails between company branches GMAIL SERVER

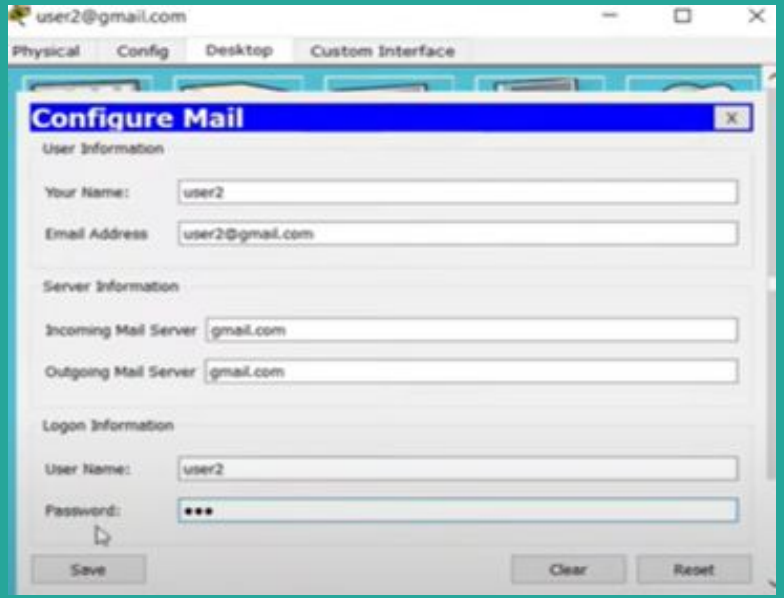


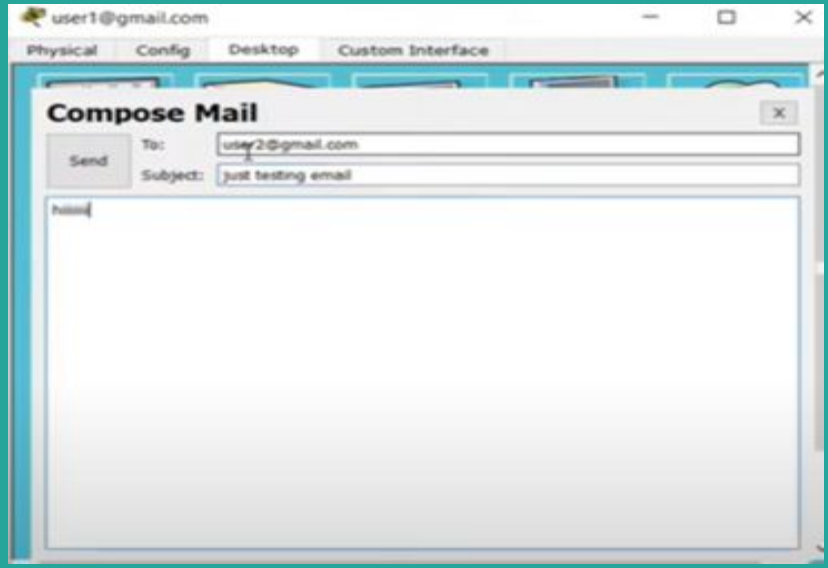
Step6: apply DHCP on one of the branch

Step7: Make SYSLOG server for seeing the log of connection between different branches

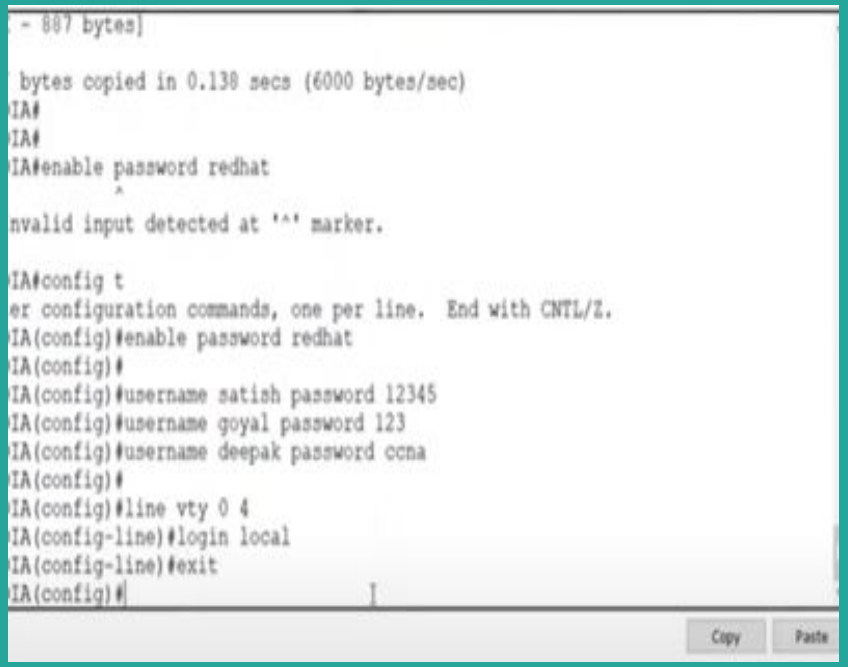


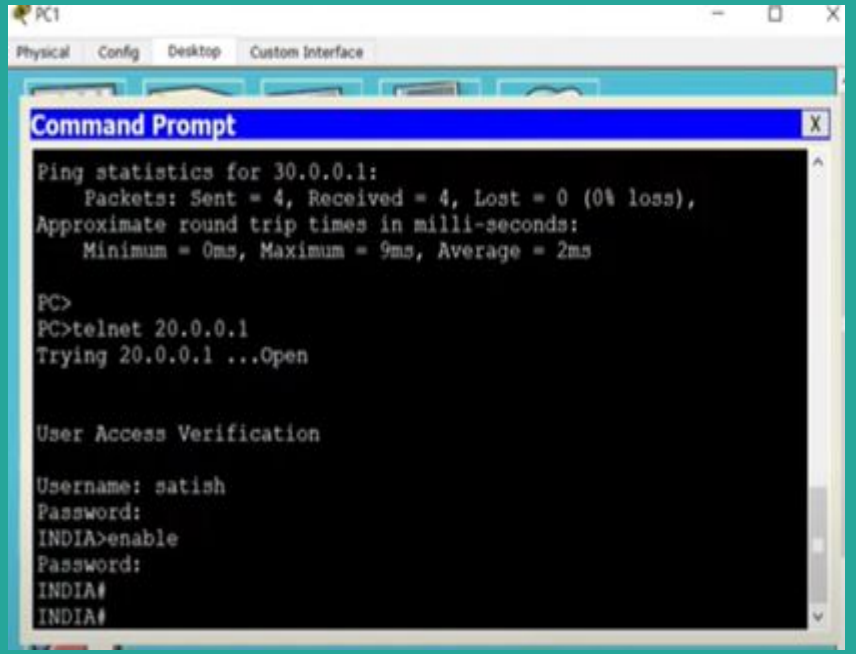
STEP8: CONFIGURE MAIL so that we can send information from one branch to another using gmail





Step9: make password for ENABLE so that outside user cannot login only local users have the access





ADVANTAGES

1. Area Coverage

WAN generally covers geographical areas of large proportions (1000 kms or more than that). Probably if your business offices are located at different locations, then without an effort all the branches can be communicated through WAN. For this purpose Internet Service Providers (ISPs) can provide leased lines.

2. Centralized Data

Using WAN means that you can share the data connected to all the devices in the respective network. For an example you can setup head office server and share the data among all the office branches. Hence, there is no need to purchase separate emails, files and backup servers. Instead you can get all the backup and support from the head office server.

3. Updated Files

From WAN users can get updated files and data from the servers. Companies can work to update files from the servers so that all the connected devices can receive them. That too in a fraction of seconds.

4. Message Exchange

With the advancement of Internet of Things (IoT) and LAN, a sudden growth of WAN based devices can be seen. From this communication through messages can be done fast with the help of popular applications such as messenger and whatsapp.

REQUIREMENTS

- All routers are provided with the security of radius server - different usernames and passwords for each
- Login system will prevent unauthorised access to unknown users
- Minimum connection speed of 100 Mbps
- Average required throughput - 5 Mbps
- Peak traffic load can increase it to 10-15 Mbps

THANK YOU!