ABSTRACT

This project is totally dedicated to the Network Engineer for new and smart learning of the Network Structure. In this concept it is possible for the networker to check the incoming & the outgoing traffic and to maintain some security concepts as well. In this logic we use the Multi-Layer Switch to act as a DHCP Server for every Department in Network Bulls Organization.

The Multi-Layer Switch along with providing IP Addresses to all the Hosts in Network Bulls also acts as a Back-Bone to the whole Network Scenario. Multi-Layer Switch makes it possible to route and monitor all the Traffic Flow in an MNC – Network Bulls. It provides IP Addresses to the hosts through DHCP Process on time lease. Every Router in each & every Department has been provided with the dedicated PC to be controlled by the Local Administrator of the Department Manually along with the fact that the Network of Network Bulls is also centrally Manage through a Multi-Layer Switch.

The different Departments can communicate with each other to act as a transparent Network Terminology, being an MNC – Network Bulls. The Accounting & Sales Department, Quality Analysis Department, Finance Department, IT Security Department, HR Department & Production Floor are shown as some of the Departments of Network Bulls.

INTRODUCTION

Here are some ideas of projects in the Networking area. Some of these are new, and some are ideas that have run before but could be run again. Note that, unlike the normal project ideas, these ideas do not have a contact listed against them. They are there to give you ideas of the sort of things that could be done. If a project idea seems interesting, and you would like to pursue it further, then you should discuss it with one of the lecturers who are experienced in the Networking area: Bill Buchanan, Gordon Russell, Ahmed Al-Dubai, Imed Romdhani, Jim Jackson, Robert Ludwiniak or Neil Urquhart. They may not be able to help you directly, but will at least be able to point you to somebody better placed, perhaps because their specialist knowledge is in the area of the project.

This introduces the underlying concepts behind networking using the Internet and its protocols as examples. There are two goals:

(1) to give you an understanding of how networks, especially the Internet, work

(2) to teach you network programming.

We will cover the first five chapters of Kurose in detail, working our way down the network stack from the application layer to the data-link layer. Concurrent with the lectures, you (in groups of two) will be building a functional TCP/IP stack and a small web server that will run on it. What you build will be "real" – your code will interoperate with other TCP/IP stacks and you'll be able to talk to your web server using any browser on any TCP/IP stack.

This is a learn-by-doing kind of class. You will get your hands dirty by examining parts of our Internet infrastructure and building other parts. It will be a lot of work, but it will also be a lot of fun, provided you enjoy this sort of thing. We will assume that you do and that you will make a good faith effort. We don't want to have to spend too much time measuring your performance.

If you care about what we're teaching, you'll do a better job of that yourself, and if you don't care, then you should take some course that you do care about.

The goal of the networking project is to enable you to do the following:

1. 1.Build implementations of the Internet protocols
2. 2.Generalize this knowledge to other networking protocols.
3. 3.Be a competent network and systems programmer.
4. Think like a networking practitioner
5. Read and judge articles on networking in trade magazines
6. Begin to read and judge research and technical articles on networking
7. Create simplicity and reliability out of complexity and unreliability
8. Structure and design software systems to achieve that simplicity and Reliability

Project Specification

Hardware Specification

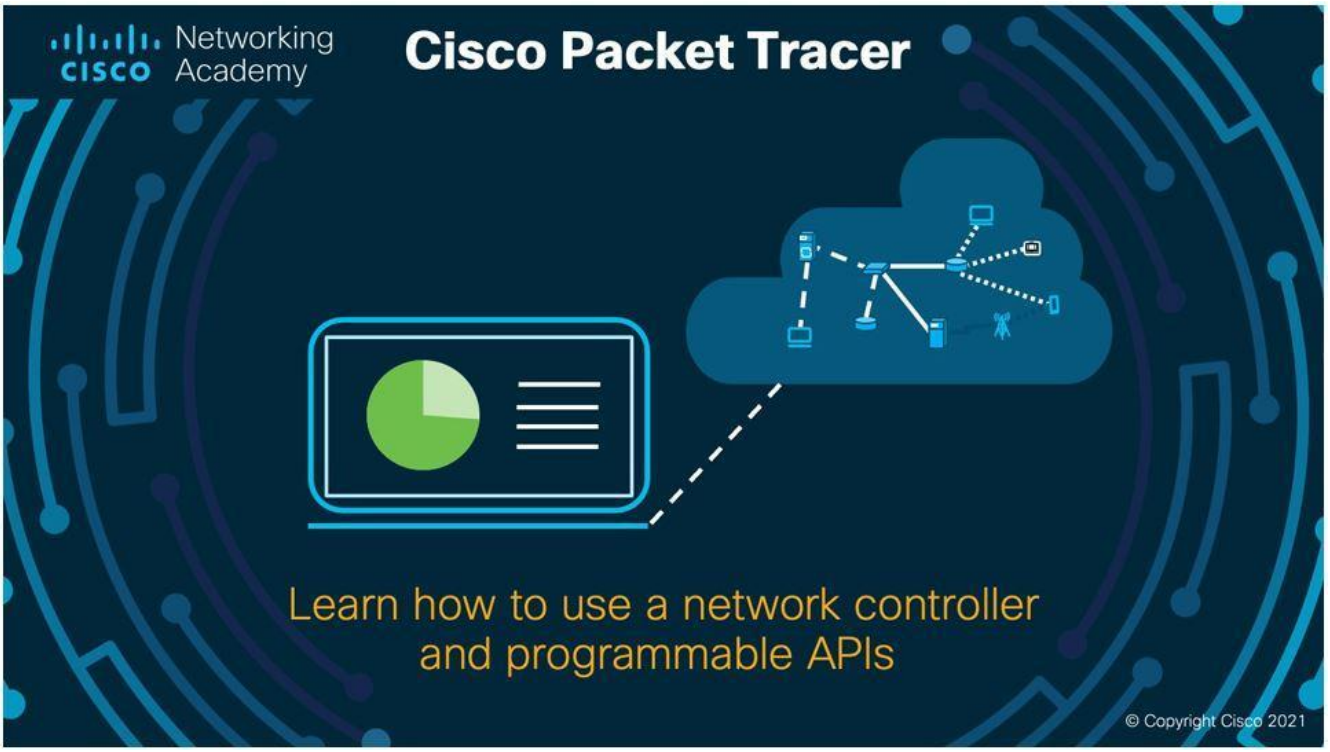
CPU Speed :2GHz recommended or higher
Processor: Pentium Processor or above
Memory/RAM: 1GB minimum,2GB recommended or higher
Display Properties: Greater than 256 color depth
Size of Hard Disk:60 GB minimum
NIC Card

Software Specification

Software Used: Packet Tracer 5.3.2
Operating System: Microsoft Windows XP, Vista,7

Packet Tracer

Packet Tracer is a Cisco router simulator that can be utilized in training and education, but also in research for simple computer network simulations. The tool is created by Cisco Systems and provided for free distribution to faculty, students, and alumni who are or have participated in the Cisco Networking Academy. The purpose of Packet Tracer is to offer students and teachers a tool to learn the principles of networking as well as develop Cisco technology specific skills.



Features

The current version of Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, and EIGRP, to the extent required by the current CCNA curriculum. While Packet Tracer aims to provide a realistic simulation of functional networks, the application itself utilizes only a small number of features found within the actual hardware running a current Cisco IOS version. Thus, Packet Tracer is unsuitable for modeling production networks. With the introduction of version 5.3, several new features were added, including BGP. BGP is not part of the CCNA curriculum, but part of the CCNP curriculum.

PROJECT DETAIL

Description:

Here we have 8 branches of a company in a Campus Network design, they are accessing internet through ISP.

DEVICES USED

8 SERIAL CABLES
28 COPPER CROSS OVER
8 COPPER STRAIGHTS THROUGH
8 ROUTERS
16 SWITCHES (LAYER 2)
1 MULTY LAYER SWITCH
28 PCs
16 CONSOLE CABLES

PROTOCOLS USED

EIGRP 100
VTP (VLAN TRUNKING PROTOCOL) at all SWITCHES
INTER VLAN SWITCHING
DHCP on MULTI-LAYER SWITCH
SUBNET MASKING
WILD CARD MASKING
STP (SPANNING TREE PROTOCOL)
NAT (NETWORK ADDRESS TRANSLATION)

SYSTEM DESIGN

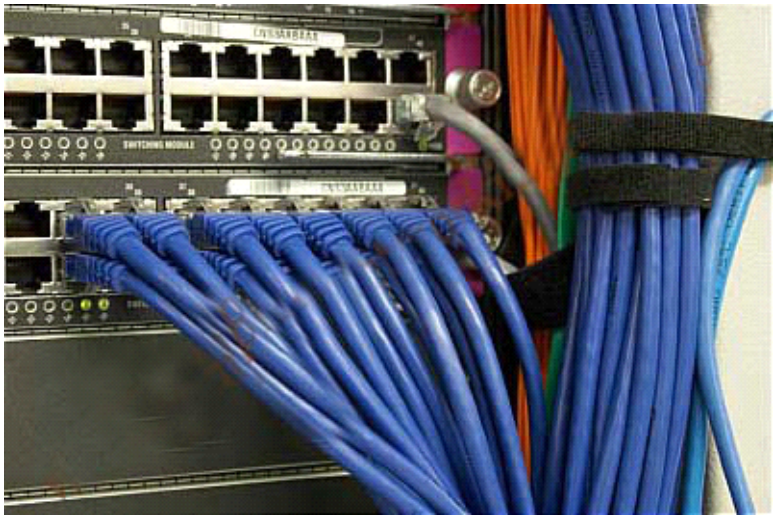
(TECHNOLOGY AND TOOLS USED)

Networking Technologies

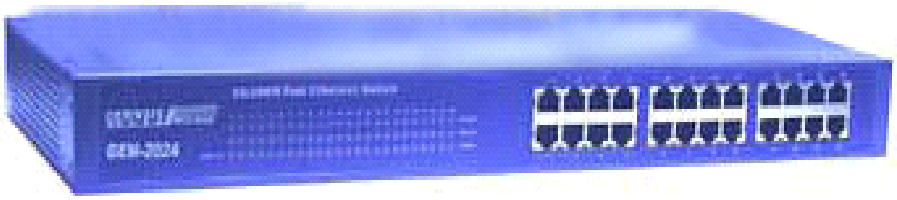
Networks using a Star topology require a central point for the devices to connect. Originally this device was called a concentrator since it consolidated the cable runs from all network devices. The basic form of concentrator is the hub.

As shown in Figure; the hub is a hardware device that contains multiple, independent ports that match the cable type of the network. Most common hubs interconnect Category 3 or 5 twisted-pair cable with RJ-45 ends, although Coax BNC and Fiber Optic BNC hubs also exist. The hub is considered the least common denominator in device concentrators. Hubs offer an inexpensive option for transporting data between devices, but hubs don't offer any form of intelligence. Hubs can be active or passive.

SWITCHES



Switches are a special type of hub that offers an additional layer of intelligence to basic, physical-layer repeater hubs. A switch must be able to read the MAC address of each frame it receives. This information allows switches to repeat incoming data frames only to the computer or computers to which a frame is addressed. This speeds up the network and reduces congestion.



Switches operate at both the physical layer and the data link layer of the OSI Model.
ROUTERS

Routers Are networking devices used to extend or segment networks by forwarding packets

from one logical network to another. Routers are most often used in large inter-networks that use the TCP/IP protocol suite and for connecting TCP/IP hosts and local area networks (LAN s) to the Internet using dedicated leased lines.

Routers work at the network layer (layer 3) of the Open Systems Interconnection (OSI) reference model for networking to move packets between networks using their logical addresses (which, in the case of TCP/IP, are the IP addresses of destination hosts on the network). Because routers operate at a higher OSI level than bridges do, they have better packet-routing and filtering capabilities and greater processing power, which results in routers costing more than bridges.

Routing tables

Routers contain internal tables of information called routing tables that keep track of all known network addresses and possible paths throughout the inter-network, along with cost of reaching each network. Routers route packets based on the available paths and their costs, thus taking advantage of redundant paths that can exist in a mesh topology network.
Because routers use destination network addresses of packets, they work only if the configured network protocol is a routable protocol such as TCP/IP or IPX/SPX. This is different from bridges, which are protocol independent. The routing tables are the heart of a router; without them, there's no way for the router to know where to send the packets it receives.

Unlike bridges and switches, routers cannot compile routing tables from the information in the data packets they process. This is because the routing table contains more detailed information than is found in a data packet, and also because the router needs the information in the table to process the first packets it receives after being activated. A router can't forward a packet to all possible destinations in the way that a bridge can.

Static routers: These must have their routing tables configured manually with all network addresses and paths in the inter-network.

Dynamic routers: These automatically create their routing tables by listening to network traffic.

Routing tables are the means by which a router selects the fastest or nearest path to the next "hop" on the way to a data packet's final destination. This process is done through the use of routing metrics.

Routing metrics which are the means of determining how much distance or time a packet will require to reach the final destination. Routing metrics are provided in different forms.
hop is simply a router that the packet must travel through.

Ticks measure the time it takes to traverse a link. Each tick is 1/18 of a second. When the router selects a route based on tick and hop metrics, it chooses the one with the lowest number of ticks first.

You can use routers, to segment a large network, and to connect local area segments to a single network backbone that uses a different physical layer and data link layer standard. They can also be used to connect LANs to a WAN's.

GATEWAYS

A gateway is a device used to connect networks using different protocols. Gateways operate at the network layer of the OSI model. In order to communicate with a host on another network, an IP host must be configured with a route to the destination network. If a configuration route is not found, the host uses the gateway (default IP router) to transmit the traffic to the destination host. The default t gateway is where the IP sends packets that are destined for remote networks. If no default gateway is specified, communication is limited to the local network. Gateways receive data from a network using one type of protocol stack, removes that protocol stack and repackages it with the protocol stack that the other network can use.

Examples

E-mail gateways-for example, a gateway that receives Simple Mail Transfer Protocol (SMTP) e-mail, translates it into a standard X.400 format, and forwards it to its destination

Gateway Service for NetWare (GSNW), which enables a machine running Microsoft Windows NT Server or Windows Server to be a gateway for Windows clients so that they can access file and print resources on a NetWare server

Gateways between a Systems Network Architecture (SNA) host and computers on a TCP/IP network, such as the one provided by Microsoft SNA Server

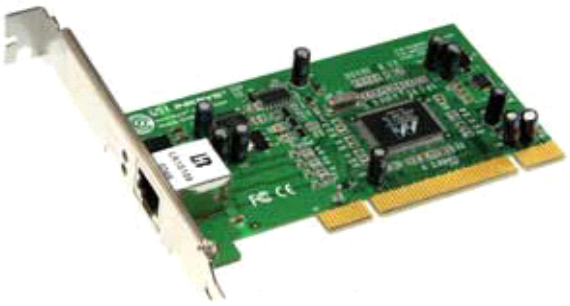
A packet assembler/disassembler (PAD) that provides connectivity between a local area network (LAN) and an X.25 packet-switching network

NICs (Network Interface Card)

Network Interface Card, or NIC is a hardware card installed in a computer so it can communicate on a network. The network adapter provides one or more ports for the network cable to connect to, and it transmits and receives data onto the network cable.
Wireless Lan card

Every networked computer must also have a network adapter driver, which controls the network adapter. Each network adapter driver is configured to run with a certain type of network adapter.

Network Card



Adapter Functions Network Interface

Network interface adapters perform a variety of functions that are crucial to getting data to and from the computer over the network.
These functions are as follows:

Data encapsulation

The network interface adapter and its driver are responsible for building the frame around the data generated by the network layer protocol, in preparation for transmission. The network interface adapter also reads the contents of incoming frames and passes the data to the appropriate network layer protocol.

Signal encoding and decoding

The network interface adapter implements the physical layer encoding scheme that converts the binary data generated by the network layer-now encapsulated in the frame-into electrical voltages, light pulses, or whatever other signal type the network medium uses, and converts received signals to binary data for use by the network layer.

Transmission and reception

The primary function of the network interface adapter is to generate and transmit signals of the appropriate type over the network and to receive incoming signals. The nature of the signals depends on the network medium and the data-link layer protocol. On a typical LAN, every computer receives all of the packets transmitted over the network, and the network interface adapter examines the destination address in each packet, to see if it is intended for that computer.

Data buffering

Network interface adapters transmit and receive data one frame at a time, so they have built-in buffers that enable them to store data arriving either from the computer or from the network until a frame is complete and ready for processing.

Serial/parallel conversion

The communication between the computer and the network interface adapter runs in parallel, that is, either 16 or 32 bits at a time, depending on the bus the adapter uses. Network communications, however, are serial (running one bit at a time), so the network interface adapter is responsible for performing the conversion between the two types of transmissions.

Media access control

The network interface adapter also implements the MAC mechanism that the data-link layer protocol uses to regulate access to the network medium. The nature of the MAC mechanism depends on the protocol used.

Network protocols

A networked computer must also have one or more protocol drivers (sometimes called a transport protocol or just a protocol). The protocol driver works between the upper-level network software and the network adapter to package data to be sent on the network.

In most cases, for two computers to communicate on a network, they must use identical protocols. Sometimes, a computer is configured to use multiple protocols. In this case, two computers need only one protocol in common to communicate. For example, a computer running File and Printer Sharing for Microsoft Networks that uses both NetBEUI and TCP/IP can communicate with computers using only NetBEUI or TCP/IP.

In this project we are using three protocols: -

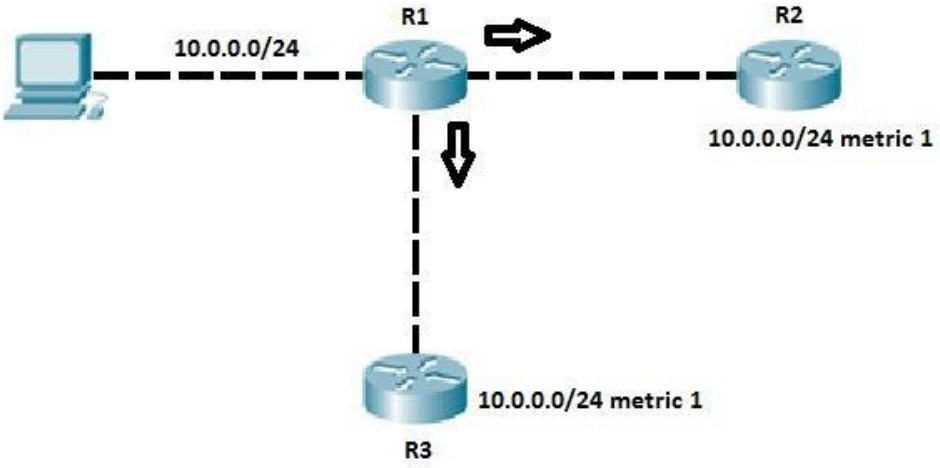
- RIPV2
- OSPF
- EIGRP

RIP (Routing Information Protocol) is one of the oldest distance vector routing protocols. It is usually used on small networks because it is very simple to configure and maintain, but lacks some advanced features of routing protocols like OSPF or EIGRP. Two versions of the protocol exist: version 1 and version 2. Both versions use hop count as a metric and have the administrative distance of 120. RIP version 2 is capable of advertising subnet masks and uses multicast to send routing updates, while version 1 doesn't advertise subnet masks and uses broadcast for updates. Version 2 is backwards compatible with version 1.

RIPv2 sends the entire routing table every 30 seconds, which can consume a lot of bandwidth.

RIPv2 uses multicast address of 224.0.0.9 to send routing updates, supports authentication and triggered updates (updates that are sent when a change in the network occurs).

For example, of how RIP works, consider the following figure.



Router R1 directly connects to the subnet 10.0.0.0/24. Network engineer has configured RIP on R1 to advertise the route to this subnet. R1 sends routing updates to R2 and R3. The routing updates list the subnet, subnet mask and metric for this route. Each router, R2 and R3, receives this update and adds the route to their respective routing tables. Both routers list the metric of 1 because the network is only one hop away.

OSPF

OSPF (Open Shortest Path First) is a link state routing protocol. Because it is an open standard, it is implemented by a variety of network vendors. OSPF will run on most routers that doesn't necessarily have to be Cisco routers (unlike EIGRP which can be run only on Cisco routers).

Here are the most important features of OSPF:

- a classless routing protocols
- supports VLSM, CIDR, manual route summarization, equal cost load balancing
- incremental updates are supported
- uses only one parameter as the metric – the interface cost.
- the administrative distance of OSPF routes is, by default, 110.
- uses multicast addresses 224.0.0.5 and 224.0.0.6 for routing updates.

Routers running OSPF have to establish neighbour relationships before exchanging routes. Because OSPF is a link state routing protocol, neighbours don't exchange routing tables. Instead, they exchange information about network topology. Each OSFP router then runs SFP algorithm to calculate the best routes and adds those to the routing table. Because each router knows the entire topology of a network, the chance for a routing loop to occur is minimal.

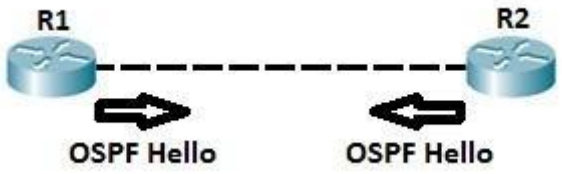
Each OSPF router stores routing and topology information in three tables:

- **Neighbour table** – stores information about OSPF neighbours
- **Topology table** – stores the topology structure of a network
- **Routing table** – stores the best routes

OSPF neighbours

OSPF routers need to establish a neighbour relationship before exchanging routing updates. OSPF neighbours are dynamically discovered by sending Hello packets out each OSPF-enabled interface on a router. Hello packets are sent to the multicast IP address of 224.0.0.5.

The process is explained in the following figure:



Routers R1 and R2 are directly connected. After OSFP is enabled both routers send Hellos to each other to establish a neighbour relationship. You can verify that the neighbour relationship has indeed been established by typing the ***show ip ospf neighbour's*** command.

```
R1#show ip ospf neig

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:30    192.168.0.2     FastEthernet0/0
```

In the example above, you can see that the router-id of R2 is 2.2.2.2. Each OSPF router is assigned a router ID. A router ID is determined by using one of the following:

1. using the router-id command under the OSPF process.
2. using the highest IP address of the router's loopback interfaces.
3. using the highest IP address of the router's physical interfaces.

The following fields in the Hello packets must be the same on both routers in order for routers to become neighbours:

- subnet
- area id
- hello and dead interval timers
- authentication
- area stub flag
- MTU

By default, OSPF sends hello packets every 10 second on an Ethernet network (Hello interval). A dead timer is four times the value of the hello interval, so if a routers on an Ethernet network doesn't receive at least one Hello packet from an OSFP neighbour for 40 seconds, the routers declares that neighbour to be down.

OSPF neighbour states

Before establishing a neighbor relationship, OSPF routers need to go through several state changes. These states are explained below.

1. **Init state** – a router has received a Hello message from the other OSFP router

2. 2-way state – the neighbor has received the Hello message and replied with a Hello message of his own

3. Exstart state – beginning of the LSDB exchange between both routers. Routers are starting to exchange link state information.

4. Exchange state – DBD (Database Descriptor) packets are exchanged. DBDs contain LSAs headers. Routers will use this information to see what LSAs need to be exchanged.

5. Loading state – one neighbor sends LSRs (Link State Requests) for every network it

doesn’t know about. The other neighbor replies with the LSUs (Link State Updates) which contain information about requested networks. After all the requested information have been received, other neighbor goes through the same process

6. Full state – both routers have the synchronized database and are fully adjacent with each other.

OSPF areas

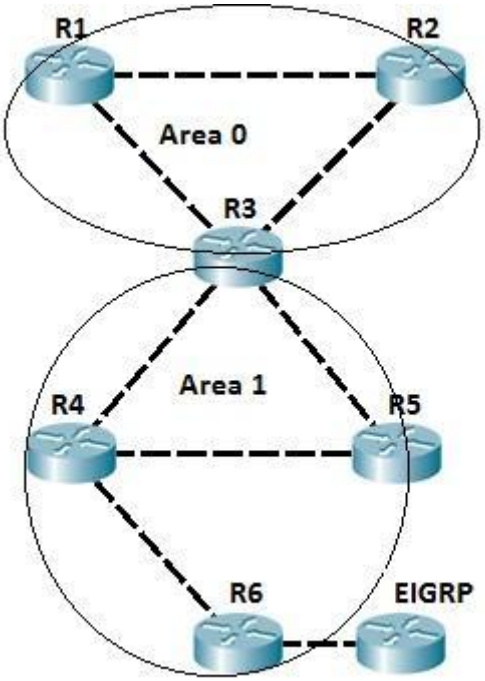
OSPF uses the concept of areas. An area is a logical grouping of contiguous networks and routers. All routers in the same area have the same topology table, but they don’t know about routers in the other areas. The main benefits of creating areas is that the size of the topology and the routing table on a router is reduced, less time is required to run the SFP algorithm and routing updates are also reduced.

Each area in the OSPF network has to connect to the backbone area (area 0). All router inside an area must have the same area ID to become OSPF neighbors. A router that has interfaces in more than one area (area 0 and area 1, for example) is called **Area Border Router (ABR)**. A router that connects an OSPF network to other routing domains (EIGRP network, for example) is called **Autonomous System Border Router (ASBR)**.

NOTE

In OSPF, manual route summarization is possible only on ABRs and ASBRs.

To better understand the concept of areas, consider the following example.

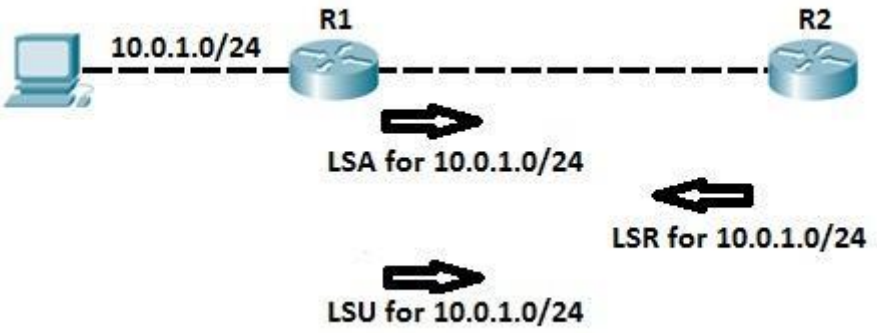


All routers are running OSPF. Routers R1 and R2 are inside the backbone area (area 0). Router R3 is an ABR, because it has interfaces in two areas, namely area 0 and area 1. Router R4 and R5 are inside area 1. Router R6 is an ASBR, because it connects OSFP network to another routing domain (an EIGRP domain in this case). If the R1's directly connected subnet fails, router R1 sends the routing update only to R2 and R3, because all routing updates all localized inside the area.

LSA, LSU and LSR

The **LSAs (Link-State Advertisements)** are used by OSPF routers to exchange topology information. Each LSA contains routing and topology information to describe a part of an OSPF network. When two neighbours decide to exchange routes, they send each other a list of all LSAa in their respective topology database. Each router then checks its topology database and sends a Link State Request (LSR) message requesting all LSAs not found in its topology table. Other router responds with the Link State Update (LSU) that contains all LSAs requested by the other neighbour.

The concept is explained in the following example:



After configuring OSPF on both routers, routers exchange LSAs to describe their respective topology database. Router R1 sends an LSA header for its directly connected network 10.0.1.0/24. Router R2 check its topology database and determines that it doesn't have information about that network. Router R2 then sends Link State Request message requesting further information about that network. Router R1 responds with Link State Update which contains information about subnet 10.0.1.0/24 (next hop address, cost…).

EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) is an advanced distance vector routing protocol. This protocol is an evolution of an earlier Cisco protocol called IGRP, which is now considered obsolete. EIGRP supports classless routing and VLSM, route summarization, incremental updates, load balancing and many other useful features. It is a Cisco proprietary protocol, so all routers in a network that is running EIGRP must be Cisco routers.

Routers running EIGRP must become neighbours before exchanging routing information. To dynamically discover neighbours, EIGRP routers use the multicast address of 224.0.0.10. Each EIGRP router stores routing and topology information in three tables:

Neighbour table – stores information about EIGRP neighbours

Topology table – stores routing information learned from neighbouring routers

Routing table – stores the best routes

Administrative distance of EIGRP is 90, which is less than both the administrative distance of RIP and the administrative distance of OSPF, so EIGRP routes will be preferred over these routes. EIGRP uses Reliable Transport Protocol (RTP) for sending messages.

EIGRP calculates its metric by using bandwidth, delay, reliability and load. By default, only bandwidth and delay are used when calculating metric, while reliability and load are set to zero.

EIGPR uses the concept of autonomous systems. An autonomous system is a set of EIGRP enabled routers that should become EIGRP neighbours. Each router inside an autonomous system must have the same autonomous system number configured, otherwise routers will not become neighbours.

EIGRP Neighbours

EIGRP must establish neighbour relationships with other EIGRP neighbouring routers before exchanging routing information. To establish a neighbour relationship, routers send hello packets every couple of seconds. Hello packets are sent to the multicast address of 224.0.0.10.

The following fields in a hello packet must be the identical in order for routers to become neighbours:

- ASN (autonomous system number)
- subnet number
- K values (components of metric)

Routers send hello packets every couple of seconds to ensure that the neighbour relationship is still active. By default, routers considers the neighbour to be down after a hold-down timer has expired. Hold-down timer is, by default, three times the hello interval. On LAN network the hold-down timer is 15 seconds.

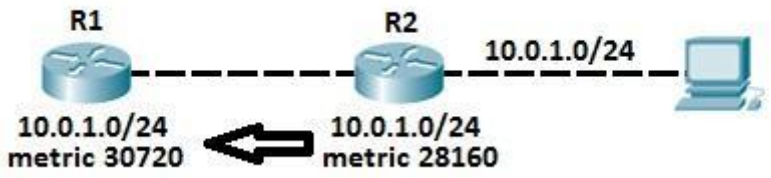
Feasible and reported distance

Two terms that you will often encounter when working with EIGRP are feasible and reported distance. Let's clarify these terms:

Feasible distance (FD) – the metric of the best route to reach a network. That route will be listed in the routing table.

Reported distance (RD) – the metric advertised by a neighbouring router for a specific route. It other words, it is the metric of the route used by the neighbouring router to reach the network.

To better understand the concept, consider the following example.



EIGRP has been configured on R1 and R2. R2 is directly connected to the subnet 10.0.1.0/24 and advertises that subnet into EIGRP. Let's say that R2's metric to reach that subnet is 28160. When the subnet is advertised to R1, R2 informs R1 that its metric to reach 10.0.1.0/24 is 28160. From the R1's perspective that metric is considered to be the **reported distance** for that route. R1 receives the update and adds the metric to the neighbour to the reported distance. That metric is called the **feasible distance** and is stored in R1's routing table (30720 in our case).

The feasible and reported distance are displayed in R1's EIGRP topology table:

```
R1#show ip eigrp topology

IP-EIGRP Topology Table for AS 1/ID(192.168.0.1)



Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
```

```
       r - Reply status


P 10.0.1.0/24, 1 successor, FD is 30720

         via 192.168.0.2 (30720/28160), FastEthernet0/0

P 192.168.0.0/24, 1 successor, FD is 28160

         via Connected, FastEthernet0/0
```

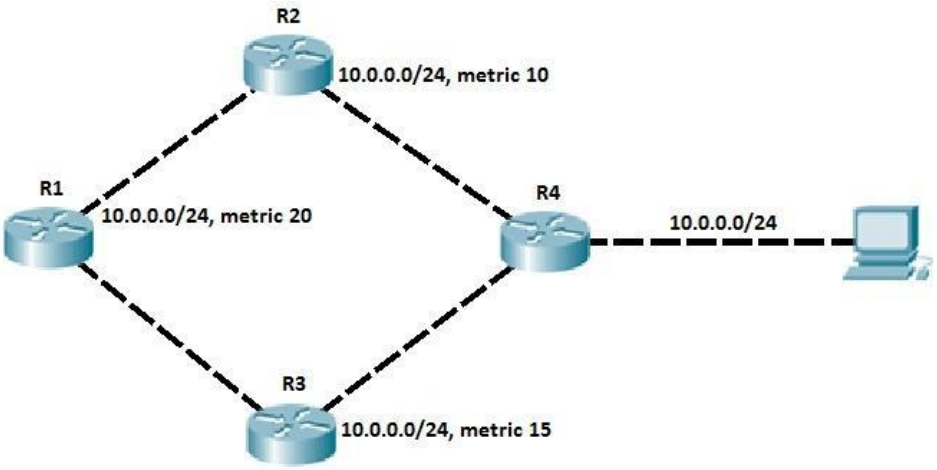
Successor and feasible successor

Another two terms that appear often in the EIGRP world are **successor** and **feasible successor**. A successor is the route with the best metric to reach a destination. That route is stored in the routing table. A feasible successor is a backup path to reach that same destination that can be used immediately if the successor route fails. These backup routes are stored in the topology table.

For a route to be chosen as a feasible successor, one condition must be met:

- the neighbour's advertised distance (AD) for the route must be less than the successor's feasible distance (FD).

The following example explains the concept of a successor and a feasible successor.



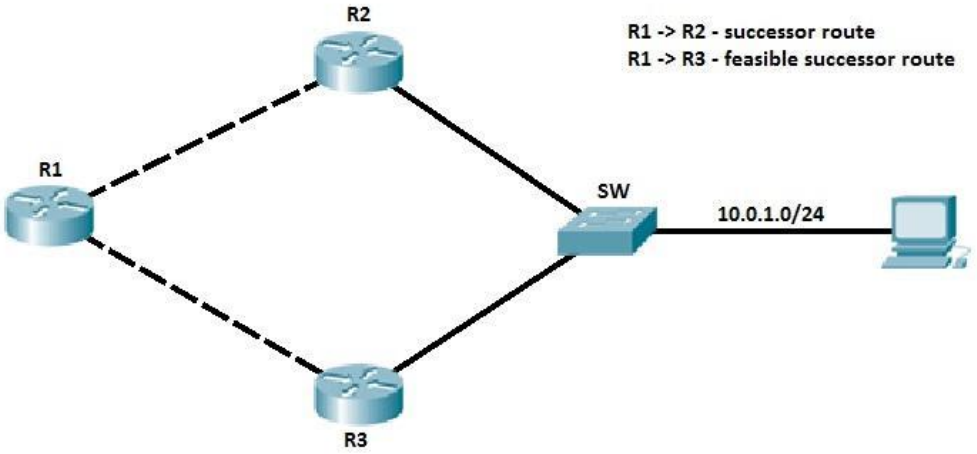
R1 has two paths to reach the subnet 10.0.0.0/24. The path through R2 has the best metric (20) and it is stored in the R1's routing table. The other route, through R3, is a feasible successor route, because the feasibility condition has been met (R3's advertised distance of 15 is less than R1's feasible distance of 20). R1 stores that route in the topology table. This route can be immediately used if the primary route fails.

EIGRP topology table

EIGRP topology table contains all learned routes to a destination. The table holds all routes received from a neighbour, successors and feasible successors for every route, and interfaces on which updates were received. The table also holds all locally connected subnets included in an EIGRP process.

Best routes (the successors) from the topology table are stored in the routing table. Feasible successors are only stored in the topology table and can be used immediately if the primary route fails.

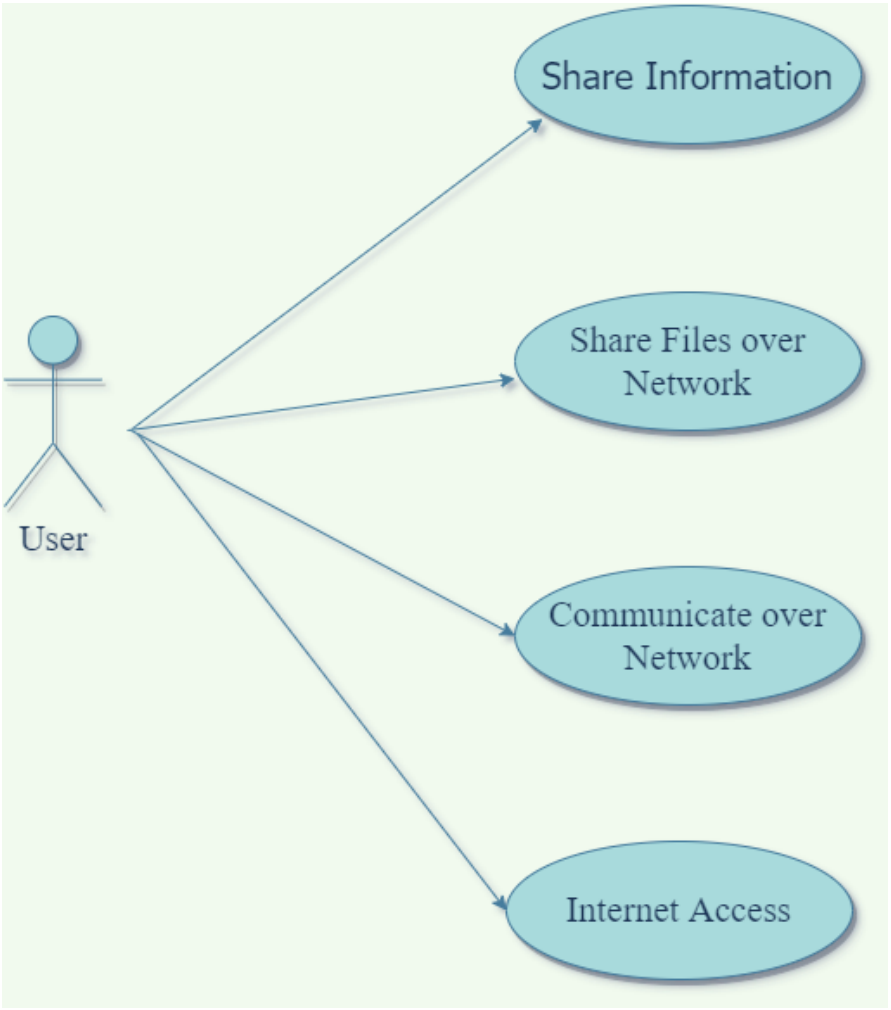
Consider the following network topology.



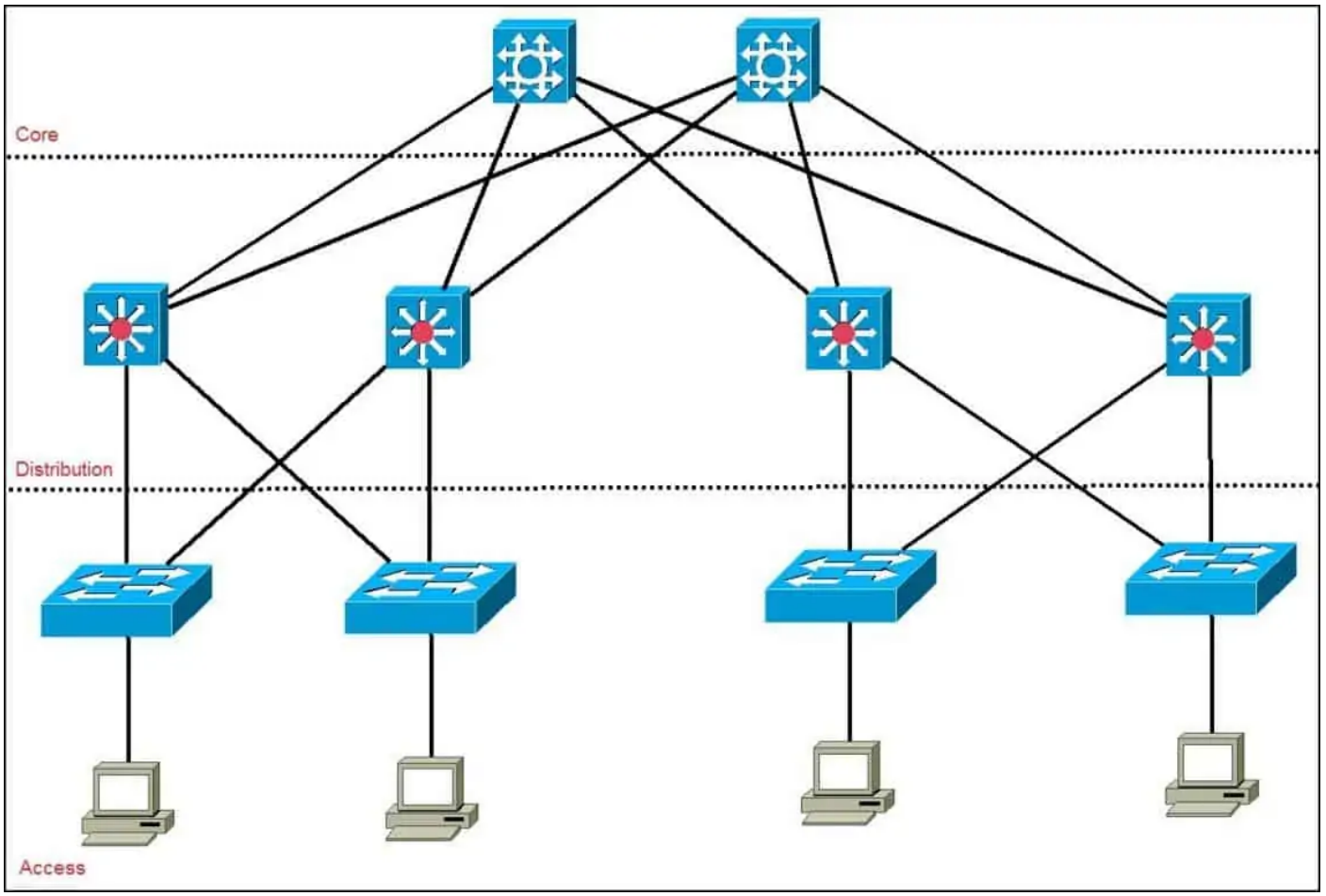
EIGRP is running on all three routers. Routers R2 and R3 both connect to the subnet 10.0.1.0/24 and advertise that subnet to R1. R1 receives both updates and calculates the best route. The best path goes through R2, so R1 stores that route in the routing table. Router R1 also calculates the metric of the route through R3. Let's say that advertised distance of that route is less then feasible

distance of the best route. The feasibility condition is met and router R1 stores that route in the topology table as a feasible successor route. The route can be used immediately if the primary route fails.

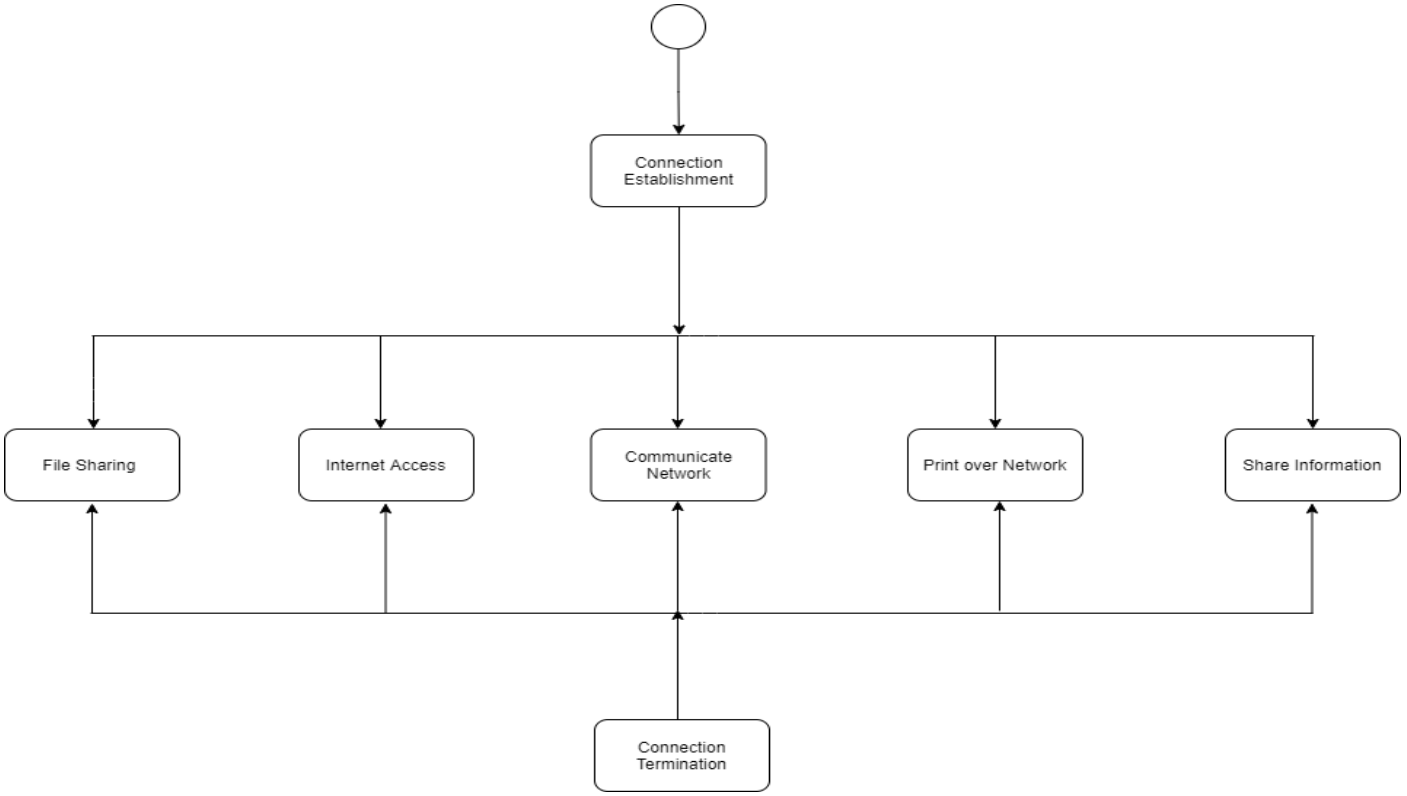
User Case Diagram



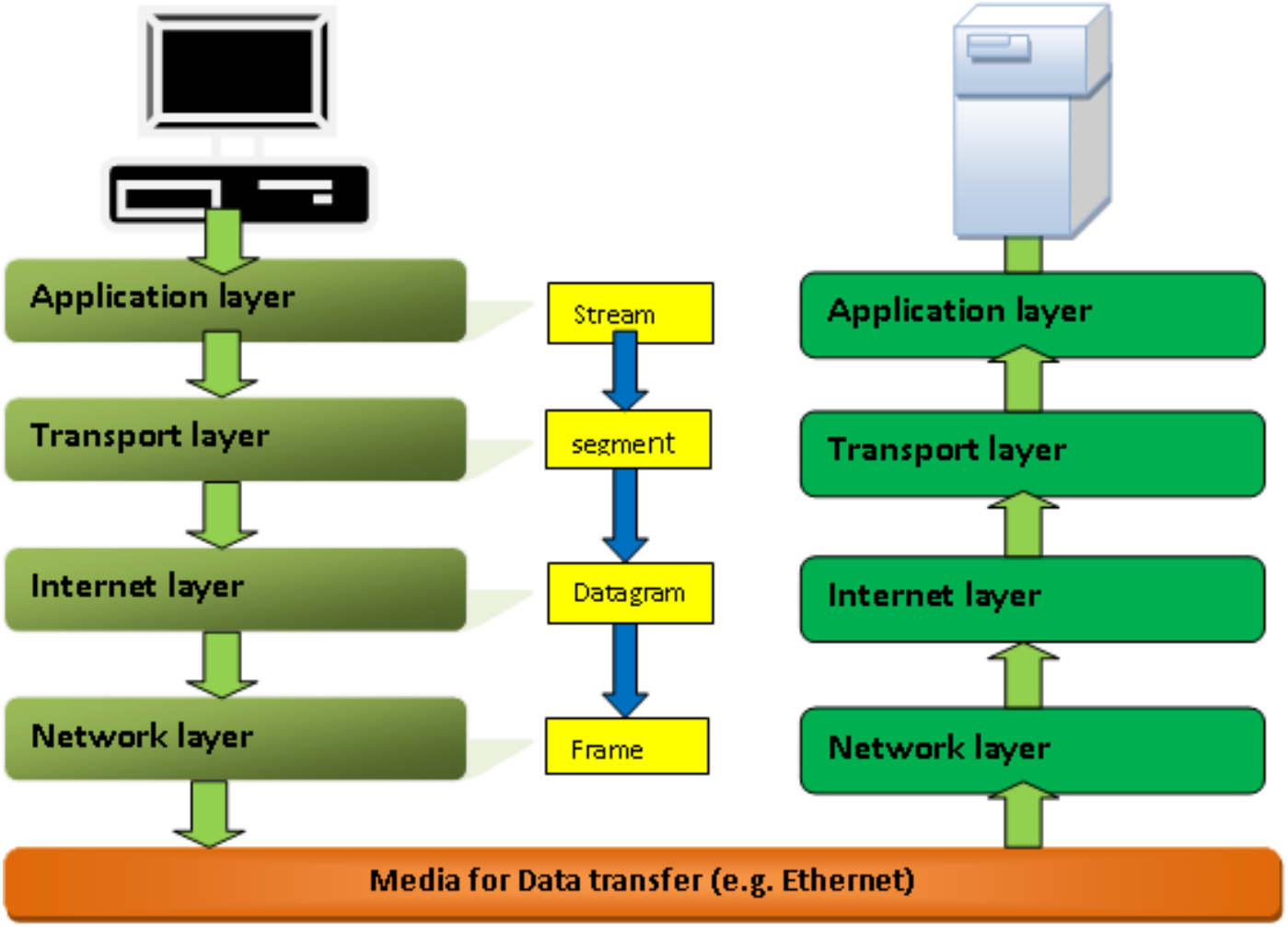
3 Layer Architecture


Core
Distribution
Access

Activity Diagram

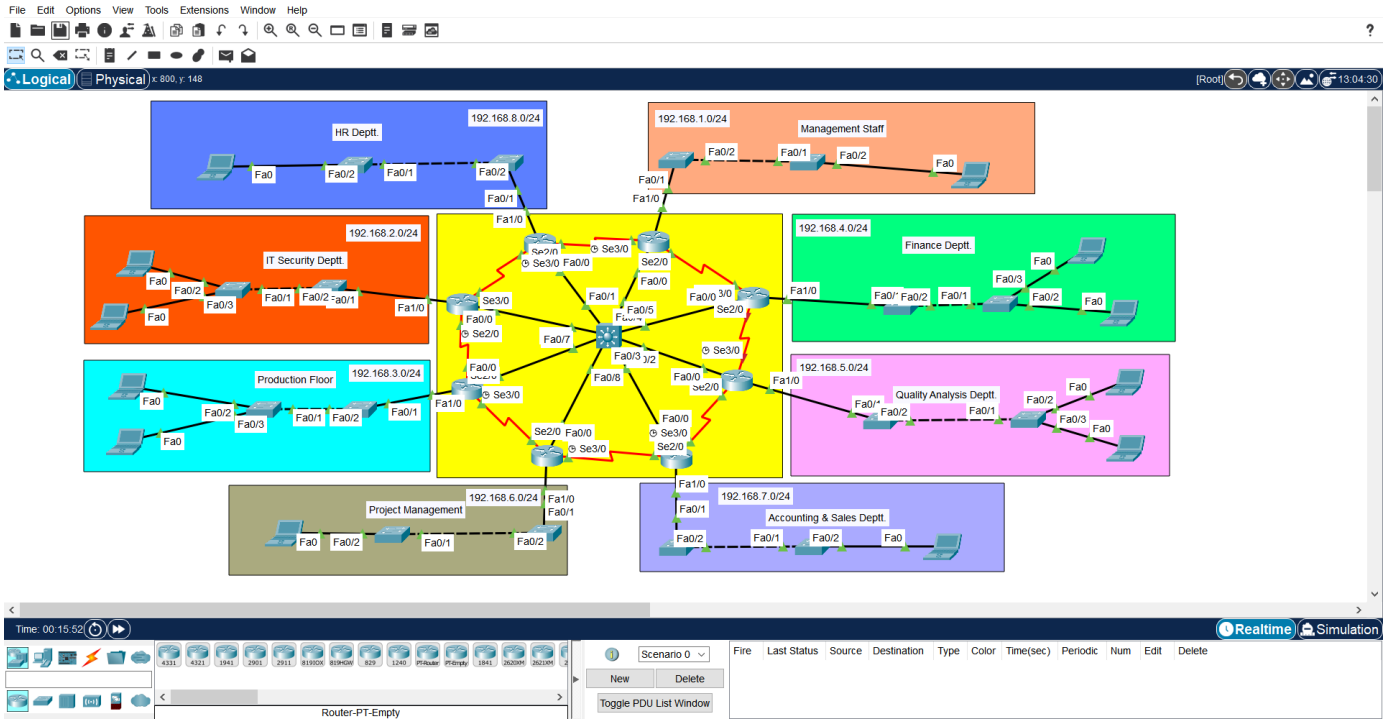


TCP/IP Model


Application layer
Transport layer
Internet layer
Network layer
Stream
segment
Datagram
Frame
Application layer
Transport layer
Internet layer
Network layer
Media for Data transfer (e.g. Ethernet)

SNAPSHOTS

PROJECT SCENARIO



COMMANDS USED

BASIC COMMANDS

- **ENABLE:** To go in privilege mode
- **CONFIGURE TERMINAL:** To go in global configuration mode.
- **ENABLE PASSWORD <VALUE>:** To give password(cisco)
- **ENABLE SECRET <VALUE>:** To give secret password.
- **LINE CONSOLE 0:** To go in line console mode.
- **EXECUTION TIMEOUT 0:** To make console never go to sleep in line console mode.
- **LOGGING SYNCHRONOUS:** To avoid the messages it also run-in line console mode.
- **SHOW RUNNING CONFIGURATION:** To check Configuration.
- **SHOW IP INTERFACE BRIEF:** To show the IP configuration.
- **INTERFACE FASTETHERNET0/0:** To give the IP configuration of fast ethernet.
- **INTERFACE SERIAL0/0:** To give the IP configuration of serial interface.
- **NO SHUTDOWN:** To make interface up.
- **CLOCKRATE 64000:** To provide clock rate to DCE end of serial cable.

ROUTING COMMANDS

STATIC ROUTING COMMANDS:

IN global config mode) # ip route <destination network ip> <subnet mask> <exit interface> <permanent>
For ex.) # ip route 10.1.1.0 255.255.255.0 20.1.1.2

DEFAULT ROUTING COMMANDS:

In global config mode) # ip route <destination network ip> <subnet mask> <exit interface> <permanent>
For ex.) # ip route 0.0.0.0 0.0.0.0 20.1.1.2

DYNAMIC ROUTING COMMANDS

RIP COMMANDS:

In global config mode) # router rip

Router) # network <directly connected n/w ip>
For ex.) # network 10.0.0.0
) # network 20.0.0.0

TO CHANGE RIP VERSION:

In global config mode) # router rip
Router) # version 2
Router) # do show ip route(to check version)
Router) # debug ip rip(shows all updates of multicasting & broadcasting)

EIGRP COMMANDS:
In global config mode) # router eigrp <AD value>
-config) # router eigrp 100
-router) # network < n/w id of directly connected> <wild card mask>
-router) # network 10.1.1.0 0.0.0.255

OSPF COMMANDS:
IN global config mode) # router ospf <process id>
-config) # router ospf 100
-router) # network <network id of directly connected> <subnet mask> <area 0>
-router) # network 192.168.1.0 0.0.0.255 area 0
-router) # do show ip ospf neighbour (to check the neighborship)
-router) # do show ip ospf database (to check the database of the events)

TO CREATE VLANs

1. **To give name to vlan:**

-config) # vlan 2
-config) # name xyz

2. **To add interfaces to VLAN**

-config) # int fa0/0
-int) # switchport mode access
-int) # switchport access vlan2

3. **To do trunking**

-config) # int fa0/0
-int) # switchport mode trunk
-int) # switchport mode dynamic desirable

4. **TO APPLY VTP:**

-config) # vtp mode server
-config) # vtp domain cisco.com
-config) # vtp cisco123
-config) # do show vtp status
-config) # debug SW-vlan vtp events
-config) # do show cdp neighbours

5. **To make VLAN native:**
6.

-config) # switchport trunk native vlan 2

Running Config:

R1

```
Current configuration: 1199 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R8
!
!
!
enable password cisco
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username Admin password 0 cisco
username Admin1 password 0 cisco
!
!
!
!
!
!
!
!
!
ip ssh version 1
ip domain-name cisco
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 88.0.0.1 255.0.0.0
```

```
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.8.1 255.255.255.0
ip helper-address 88.0.0.2
duplex auto
speed auto
!
interface Serial2/0
ip address 18.0.0.8 255.0.0.0
!
interface Serial3/0
ip address 28.0.0.8 255.0.0.0
clock rate 64000
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
interface Serial6/0
no ip address
clock rate 2000000
shutdown
!
interface Serial7/0
no ip address
clock rate 2000000
shutdown
!
router eigrp 100
network 88.0.0.0
network 192.168.8.0
network 18.0.0.0
network 28.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
```

```
!
no cdp run
!
!
!
!
!
!
line con 0
password cisco
login
!
line aux 0
!
line vty 0 4
login local
line vty 5
login local
!
!
!
end
```

R2:

```
Current configuration: 1199 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R8
!
!
!
enable password cisco
!
!
!
!
!
!
!
ip cef
```

```
no ipv6 cef
!
!
!
username Admin password 0 cisco
username Admin1 password 0 cisco
!
!
!
!
!
!
!
!
ip ssh version 1
ip domain-name cisco
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 88.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.8.1 255.255.255.0
ip helper-address 88.0.0.2
duplex auto
speed auto
!
interface Serial2/0
ip address 18.0.0.8 255.0.0.0
!
interface Serial3/0
ip address 28.0.0.8 255.0.0.0
clock rate 64000
!
interface FastEthernet4/0
no ip address
shutdown
!
```

```
interface FastEthernet5/0
no ip address
shutdown
!
interface Serial6/0
no ip address
clock rate 2000000
shutdown
!
interface Serial7/0
no ip address
clock rate 2000000
shutdown
!
router eigrp 100
network 88.0.0.0
network 192.168.8.0
network 18.0.0.0
network 28.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
!
line con 0
password cisco
login
!
line aux 0
!
line vty 0 4
login local
line vty 5
login local
!
!
```

```
!
end
```

R3:

```
Current configuration : 1199 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R8
!
!
!
enable password cisco
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username Admin password 0 cisco
username Admin1 password 0 cisco
!
!
!
!
!
!
!
!
!
ip ssh version 1
ip domain-name cisco
!
!
!
!
!
```

```
!
!
!
interface FastEthernet0/0
ip address 88.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.8.1 255.255.255.0
ip helper-address 88.0.0.2
duplex auto
speed auto
!
interface Serial2/0
ip address 18.0.0.8 255.0.0.0
!
interface Serial3/0
ip address 28.0.0.8 255.0.0.0
clock rate 64000
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
interface Serial6/0
no ip address
clock rate 2000000
shutdown
!
interface Serial7/0
no ip address
clock rate 2000000
shutdown
!
router eigrp 100
network 88.0.0.0
network 192.168.8.0
network 18.0.0.0
network 28.0.0.0
no auto-summary
!
```

```
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
!
line con 0
password cisco
login
!
line aux 0
!
line vty 0 4
login local
line vty 5
login local
!
!
!
end
```

R4:

```
Current configuration : 1199 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R8
!
!
!
enable password cisco
```

```
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username Admin password 0 cisco
username Admin1 password 0 cisco
!
!
!
!
!
!
!
!
!
ip ssh version 1
ip domain-name cisco
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 88.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.8.1 255.255.255.0
ip helper-address 88.0.0.2
duplex auto
speed auto
!
interface Serial2/0
ip address 18.0.0.8 255.0.0.0
!
interface Serial3/0
```

```
ip address 28.0.0.8 255.0.0.0
clock rate 64000
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
interface Serial6/0
no ip address
clock rate 2000000
shutdown
!
interface Serial7/0
no ip address
clock rate 2000000
shutdown
!
router eigrp 100
network 88.0.0.0
network 192.168.8.0
network 18.0.0.0
network 28.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
!
line con 0
password cisco
login
!
line aux 0
```

```
!
line vty 0 4
login local
line vty 5
login local
!
!
!
end
```

R5:

```
Current configuration : 1199 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R8
!
!
!
enable password cisco
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username Admin password 0 cisco
username Admin1 password 0 cisco
!
!
!
!
!
!
!
!
```

```
ip ssh version 1
ip domain-name cisco
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 88.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.8.1 255.255.255.0
ip helper-address 88.0.0.2
duplex auto
speed auto
!
interface Serial2/0
ip address 18.0.0.8 255.0.0.0
!
interface Serial3/0
ip address 28.0.0.8 255.0.0.0
clock rate 64000
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
interface Serial6/0
no ip address
clock rate 2000000
shutdown
!
interface Serial7/0
no ip address
clock rate 2000000
shutdown
!
```

```
router eigrp 100
network 88.0.0.0
network 192.168.8.0
network 18.0.0.0
network 28.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
!
line con 0
password cisco
login
!
line aux 0
!
line vty 0 4
login local
line vty 5
login local
!
!
!
end
```

R6:

```
Current configuration : 1199 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R8
```

```
!
!
!
enable password cisco
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username Admin password 0 cisco
username Admin1 password 0 cisco
!
!
!
!
!
!
!
!
!
ip ssh version 1
ip domain-name cisco
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 88.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.8.1 255.255.255.0
ip helper-address 88.0.0.2
duplex auto
speed auto
!
```

```
interface Serial2/0
ip address 18.0.0.8 255.0.0.0
!
interface Serial3/0
ip address 28.0.0.8 255.0.0.0
clock rate 64000
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
interface Serial6/0
no ip address
clock rate 2000000
shutdown
!
interface Serial7/0
no ip address
clock rate 2000000
shutdown
!
router eigrp 100
network 88.0.0.0
network 192.168.8.0
network 18.0.0.0
network 28.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
!
line con 0
```

```
password cisco
login
!
line aux 0
!
line vty 0 4
login local
line vty 5
login local
!
!
!
end
```

R7:

```
Current configuration: 1199 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R8
!
!
!
enable password cisco
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username Admin password 0 cisco
username Admin1 password 0 cisco
!
```

```
!
!
!
!
!
!
!
ip ssh version 1
ip domain-name cisco
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 88.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.8.1 255.255.255.0
ip helper-address 88.0.0.2
duplex auto
speed auto
!
interface Serial2/0
ip address 18.0.0.8 255.0.0.0
!
interface Serial3/0
ip address 28.0.0.8 255.0.0.0
clock rate 64000
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
interface Serial6/0
no ip address
clock rate 2000000
```

```
shutdown
!
interface Serial7/0
no ip address
clock rate 2000000
shutdown
!
router eigrp 100
network 88.0.0.0
network 192.168.8.0
network 18.0.0.0
network 28.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
!
line con 0
password cisco
login
!
line aux 0
!
line vty 0 4
login local
line vty 5
login local
!
!
!
end

Current configuration : 1199 bytes
!
version 12.2
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
no service password-encryption
!
hostname R8
!
!
!
enable password cisco
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username Admin password 0 cisco
username Admin1 password 0 cisco
!
!
!
!
!
!
!
!
!
ip ssh version 1
ip domain-name cisco
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 88.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.8.1 255.255.255.0
```

```
ip helper-address 88.0.0.2
duplex auto
speed auto
!
interface Serial2/0
ip address 18.0.0.8 255.0.0.0
!
interface Serial3/0
ip address 28.0.0.8 255.0.0.0
clock rate 64000
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
interface Serial6/0
no ip address
clock rate 2000000
shutdown
!
interface Serial7/0
no ip address
clock rate 2000000
shutdown
!
router eigrp 100
network 88.0.0.0
network 192.168.8.0
network 18.0.0.0
network 28.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
```

!
!
!
line con 0
password cisco
login
!
line aux 0
!
line vty 0 4
login local
line vty 5
login local
!
!
!
end

Routing Protocol is "eigrp 100 "
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hop count 100
EIGRP maximum metric variance 1
Redistributing: eigrp 100
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
57.0.0.0
76.0.0.0
77.0.0.0
192.168.7.0
Routing Information Sources:
Gateway Distance Last Update
77.0.0.2 90 0
76.0.0.6 90 6237
57.0.0.1 90 7046
Distance: internal 90 external 170

R8:

Current configuration: 1199 bytes

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R8
!
!
!
enable password cisco
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username Admin password 0 cisco
username Admin1 password 0 cisco
!
!
!
!
!
!
!
!
ip ssh version 1
ip domain-name cisco
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 88.0.0.1 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.8.1 255.255.255.0
ip helper-address 88.0.0.2
duplex auto
speed auto
```

```
!
interface Serial2/0
ip address 18.0.0.8 255.0.0.0
!
interface Serial3/0
ip address 28.0.0.8 255.0.0.0
clock rate 64000
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
interface Serial6/0
no ip address
clock rate 2000000
shutdown
!
interface Serial7/0
no ip address
clock rate 2000000
shutdown
!
router eigrp 100
network 88.0.0.0
network 192.168.8.0
network 18.0.0.0
network 28.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
!
line con 0
password cisco
login
!
line aux 0
!
```

line vty 0 4
login local
line vty 5
login local
!
!
!
end

Routing Protocol is "eigrp 100 "
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hop count 100
EIGRP maximum metric variance 1
Redistributing: eigrp 100
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
88.0.0.0
192.168.8.0
18.0.0.0
28.0.0.0
Routing Information Sources:
Gateway Distance Last Update
88.0.0.2 90 4699570
18.0.0.1 90 4700613
28.0.0.2 90 4700577
Distance: internal 90 external 170

Layer 3 Switch

Current configuration : 2679 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!

```
hostname MLS
!
!
!
!
ip dhcp pool R8
network 192.168.8.0 255.255.255.0
default-router 192.168.8.1
dns-server 1.2.3.4
ip dhcp pool R2
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 1.2.3.4
ip dhcp pool R3
network 192.168.3.0 255.255.255.0
default-router 192.168.3.1
dns-server 1.2.3.4
ip dhcp pool R6
network 192.168.6.0 255.255.255.0
default-router 192.168.6.1
dns-server 1.2.3.4
ip dhcp pool R7
network 192.168.7.0 255.255.255.0
default-router 192.168.7.1
dns-server 1.2.3.4
ip dhcp pool R5
network 192.168.5.0 255.255.255.0
default-router 192.168.5.1
dns-server 1.2.3.4
ip dhcp pool R4
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
dns-server 1.2.3.4
ip dhcp pool R1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 1.2.3.4
!
!
ip routing
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/1
no switchport
ip address 88.0.0.2 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet0/2
no switchport
ip address 77.0.0.2 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet0/3
no switchport
ip address 55.0.0.2 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet0/4
no switchport
ip address 44.0.0.2 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet0/5
no switchport
ip address 11.0.0.2 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet0/6
no switchport
ip address 22.0.0.2 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet0/7
no switchport
ip address 33.0.0.2 255.0.0.0
duplex auto
speed auto
!
```

```
interface FastEthernet0/8
no switchport
ip address 66.0.0.2 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
network 11.0.0.0
network 22.0.0.0
network 33.0.0.0
network 44.0.0.0
network 55.0.0.0
```

```
network 66.0.0.0
network 77.0.0.0
network 88.0.0.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
!
end
```

RESULT AND FUTURE SCORE

6.1RESULT

All the branches communicating with each other and access the internet via ISP using internet and network protocols.

6.2FUTURE SCOPE

Perhaps the greatest concern companies have in doing business over the Internet is the security risk. Hackers, denial-of-service (DoS) attacks, identity theft, and even
cyber-terrorism are very real dangers. In addition, you may wonder how to guarantee the performance and reliability of your Internet-based services. Or, you may not be certain that you have the resources and support needed to deploy and manage e-commerce services and processes.

The good news is that a sound network infrastructure can address all these issues. At the foundation of a robust e-commerce infrastructure are the routers and switches.

An integrated approach to routing and switching lets all workers—even those at different sites—have the same access to business applications, unified communications, and videoconferencing as their colleagues at headquarters.
Cisco lets you grow your network over time, adding features and functionality as you need them while ensuring complete investment protection. An added benefit of this integrated approach is that your IT personnel can centrally
manage the network from headquarters, which keeps staffing counts low.

REFERENCES
www.google.com
www.cbtnuggets.com