PROJECT REPORT

ON

IMPLEMENTATION OF EIGRP ROUTING PROTOCOLS, DHCP POOLS, PORT’S SECURITIES and Vlans

TABLE OF CONTENTS

Chapter No. **Title** **Page No**

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

This project is based on the implementation of routing EIGRP and vlan. Building network for an organization, who wants to establish his network in Pakistan for better communication with markets in Pakistan. So, they have offices in four different cities Islamabad and Karachi, Lahore, and Peshawar (Khyber Pakhtunkhwa).

EIGRP Routing Protocol is implemented in the project. Router eigrp is used across all the cities. To enable communication between four different offices around the country. EIGRP is an advanced distance-vector routing protocol that uses features from both distance-vector and link-state routing protocols. EIGRP is very efficient in its use of network resources because it sends only incremental updates to neighboring routers when there is a change to the network. VLAN divide the actual broadcast domain into small logical domain. It actually a logically grouping of network users and resources connected to administratively defined ports on a switch. Implementation and configuration of vlan make possible to reduce the broadcast, that concern and specific group nodes broadcast restrict to its own VLAN. Host in same vlan can communicate freely, but the communication of different VLAN hosts requires a layer 3 device. Different VLANs host can communicate with the technique called inter-vlan routing, inter-vlan routing can be achieved with help of router on a stick and switch virtual interface methodologies. Our Project is done in Packet Tracer, which is virtual simulator, for networking students.

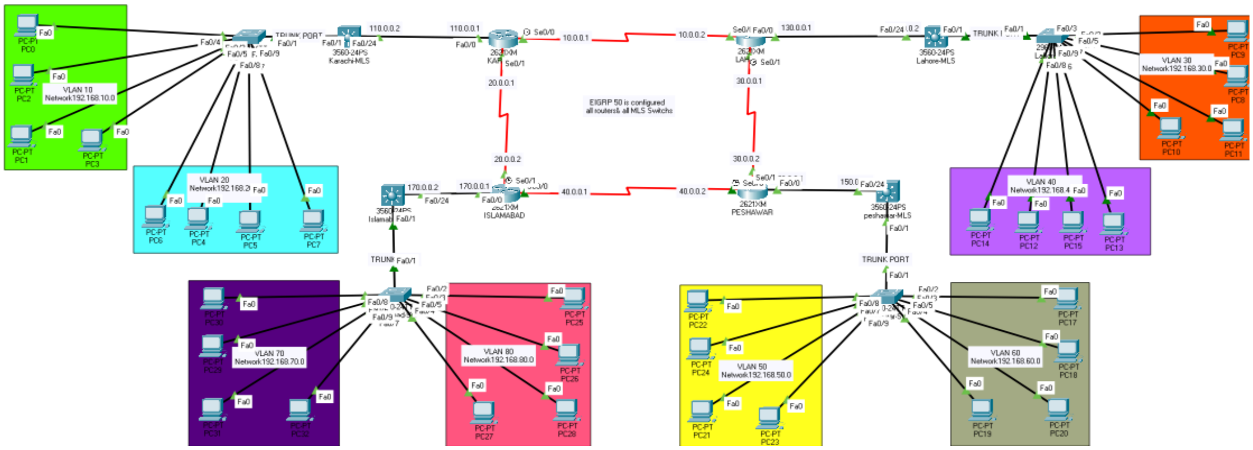


Figure 1.1 Network topology

1.1 Distance vector protocols

These types of routing protocols are a mixture of link state and distance vector. The Enhanced Interior Gateway Routing Protocol (EIGRP) is a very good example of an ADV; it acts like a link state because it sends periodic hello messages to discover their neighbors and because it only sends partial updates when changes occur. Full updates only occur at the beginning when the routers are trying to converge.

They are still a distance vector routing protocol, because they rely on their neighbors to learn about the network. But EIGRP is a very good protocol to use in a medium or even an enterprise network, due to all the features and tables they create as well.

1.2 The Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP (Enhanced Interior Gateway Routing Protocol) is an advanced distance vector routing protocol that incorporates features from both distance-vector and link-state routing. It is sometimes referred to as a hybrid routing protocol because it has characteristics of both distance-vector and link-state routing protocols. EIGRP replaced Interior Gateway Routing Protocol (IGRP)**,** an older proprietary Cisco routing protocol. EIGRP was also a proprietary protocol, but Cisco decided in 2013 to convert it to an open standard. This routing protocol is mostly used on Cisco devices and all routers in the network must support it. EIGRP is a popular choice for routing within campus networks both big and small. Many network engineers believe that EIGRP is the best choice for a routing protocol on private networks because it offers the best balance between speed, scalability and ease of management.

1.2.1 EIGRP features

EIGRP is sometimes referred to as a hybrid routing protocol because it has characteristics of both distance-vector and link-state protocols. For example, EIGRP doesn't send link-state packets as OSPF does; instead, it sends traditional distance-vector updates containing information about networks plus the cost of reaching them from the perspective of the advertising router. And EIGRP has link-state characteristics as well-it synchronizes routing tables between neighbors at startup, and then sends specific updates only when topology changes occur. This makes EIGRP suitable for very large networks. EIGRP has a maximum hop count of 255. There are a number of powerful features that make EIGRP a real standout from IGRP and other protocols. The main ones are listed here:

- Support for IP, IPX, and AppleTalk via protocol-dependent modules
- Considered classless (same as RIPv2 and OSPF)
- Support for VLSM/CIDR
- Support for summaries and discontiguous networks
- Efficient neighbor discovery
- Communication via Reliable Transport Protocol (RTP
- Best path selection via Diffusing Update Algorithm (DUAL)

1.2.2 Hop Counts

EIGRP supports a variety of network protocols. It can provide routing support for IPv4, IPv6, Internetwork packet exchange (IPX), and AppleTalk. Similar to its predecessor IGRP, EIGRP has a maximum hop count of 224 and a default maximum hop count of 100. EIGRP has administrative distance of 90. This means its routes are slightly more trusted than IRGP routes and a lot more trusted than RIP routes that have an administrative distance of 120.

1.2.3 Metric

One of EIGRP's main benefits is being able to consider many different attributes when calculating a route's cost, or metric. Namely, EIGRP is one of the only routing protocols that can consider any combination **of** Bandwidth**,** Load**,** Delay, and Reliability into its cost calculation.

Each of these attributes are controlled by what is known as a *K-value*. These K-values each enable the consideration of one of the aforementioned attributes, as well as the scale to which the attribute is considered.

K1 = Bandwidth

K2 = Load

K3 = Delay

K4 & K5 = Reliability

Each of these values are used in what EIGRP calls a Composite Metric formula. That formula is as follows:

EIGRP metric:

256 * { K1*BW + [(K2*BW)/(256-load)] + (K3*delay) } * { K5/(reliability+K4) }

The K-values themselves are a number between 0 and 255. You can set each value independently based upon what you want considered in the cost calculation for each route. If in your routing domain you wish to *not* consider one of the attributes above, you can set the appropriate K-value to Zero. If you wish to consider an attribute, you can set the appropriate K-value to one.

Since the K-values can be any value up to 255, you also have the ability to scale how heavily a particular value is considered. For example, if you wish for Bandwidth to be considered twice as important as Delay, you can set the K1 value to 2, and the K3 value to 1. If you wish to consider Bandwidth and Delay in a 2:3 ratio, you can set K1 to 2, and K3 to 3. This is what gives EIGRP such flexibility in its cost comparison, you can choose which attributes and how important each attribute is to your routing domain.

It should be noted, however, that before two routers will become EIGRP neighbors, they must have matching K-values. Which makes sense, because if one router considers Delay as the utmost important, and the other considers Bandwidth as the utmost important, then they might disagree as to which path to a destination network is best.

1.2.4 Bandwidth Calculation

Bandwidth: The bandwidth value used in the EIGRP metric calculation is determined by dividing 10,000,000 by the bandwidth (in kbps) of the slowest link along the path to the destination network.

1.2.5 Delay Calculation

Unlike bandwidth, which represents the “weakest link,” the delay value is cumulative. Specifically, it’s the sum of all delays associated with all of the interfaces that must be exited in order to get to the destination network. The output of the show interfaces command shows an interface’s delay in microseconds. However, the value used in EIGRP’s metric calculation is in tens of microseconds. This means you would add up all of the egress interface delays as seen in the show interfaces output for each egress interface, and then divide by 10 to get the tens of microsecond’s unit of measure.

1.2.6 Reliability

The reliability is a value used in the numerator of a fraction, with 255 as its denominator. The value of the fraction indicates the reliability of a link. For example, a reliability value of 255 indicates the link is 100 percent reliable (that is, 255/255 = 1 = 100 percent).

1.2.7 LOAD

Similar to reliability, load is a value used in the numerator of a fraction, with 255 as its denominator. The value of the fraction indicates how busy a link is. For example, a load value of 1 indicates the link is minimally loaded (that is, 1/255 = 0.004 < 1 percent).

1.3 EIGRP Packet Types

EIGRP (Enhanced Interior Gateway Routing Protocol) uses EIGRP Messages to establish and maintain the EIGRP Neighbor ship. In other words, it uses different EIGRP Packet Types for its operations.

EIGRP uses Five Packet Types for as EIGRP Messages. These EIGRP Packet Types are given below:

1.3.1 Hello Packet

Hello Packets are used to establish and maintain EIGRP Neighbourship. It is a keep alive message also. This Hello messages are sent as Multicast messages to Multicast Address 224.0.0.10.

1.3.2 Update Packet

EIGRP Update Packets are used to send routing updates. With these Update messages, Topology Tables and Routing Tables are built. Update Messages are sent both Unicast and Multicast. If an update is sent to a new neighbor, it is sent as unicast. If this update is related to any route change, then it is sent as Multicast to 224.0.0.10 address.

1.3.3 Query Packet

EIGRP Query Packets are used to ask for any routing update, requests an update. If a Successor fails, Query messages, a backup route is asked. EIGRP Query Messages are sent as Multicast to 224.0.0.10 address.

1.3.4 Reply Packet

EIGRP Reply Packets are used as a response to the Query Packets. They include the alternate routes to the requested destination. Reply Messages are unicast messages.

1.3.5 ACK Packet

Ack Packets are used as a feedback to the Update, Query or Reply packets as a feedback mechanism. It is not used for Hello Packets and Ack Packets. Ack messages are empty hello messages without any data and they are sent as unicast.

1.4 EIGRP tables

So speaking of tables, EIGRP relies on three tables. And these tables are really, really important. These are the fundamentals of EIGRP. And we'll see relationship between all these tables here. Each EIGRP router uses three to store routing information:

1.4.1 Neighbor table

It is the first step of EIGRP operation to discover the neighbors. A router running EIGRP multicasts Hello packets to discover the neighbors. An adjacency is created with these neighbors so that it can exchange route updates as a second step. Only the adjacent routers exchange routing information. Each router builds a neighbor table from the Hello packets it receives from adjacent EIGRP routers. To check the neighbor table, you can run "show ip eigrp neighbors" command.

1.4.2 Topology Table

The topology table is used to store information about all known routes received from all neighbors. If a neighbor is advertising a possible route, it must be using that route to forward packets to the destination network. The PDMs are responsible for putting information into the topology table.

The topology table is a database of possible routes. It provides the information that is used to select the best possible route, which is copied into the routing table. The best metric along all possible paths to the remote network is called the *feasible distance* (FD). The FD is the metric (reported or advertised distance) reported by the neighbor plus the metric to the neighbor reporting the route. The best route, called the *successor,* is the route with the lowest metric to the destination network. This is the route that is copied into the routing table.

If the successor route goes away, DUAL will search the topology table for a backup route. The topology table is where EIGRP stores the information for up to six alternate routes to a particular network. The backup routes are called *feasible successors*. The feasible successors stored in the topology table are what makes it possible for EIGRP to converge rapidly or even instantly. If there is no feasible successor in the table, a multicast is sent out to find a new route. Changes are made to the topology table if another router provides information about an alternate route.

Topology tables are stored in RAM and are re-created whenever a router starts up. Routing tables obtain all their information from the topology table. The *show ip eigrp topology* command shows us the topology table: HQ# show ip eigrp topology.

1.4.3 Routing Table

This is the table that has the best possible route to a destination. The command “show ip route” shows all routes. To specifically see the EIGRP route in routing table “show ip route eigrp” comes routing table holds the best routes to each destination and is used for forwarding packets. Successor routes are offered to the routing table. If a router learns more than one route to exactly the same destination from different routing sources, it uses the administrative distance to determine which route to keep in the routing table. By default, up to 4 routes to the same destination with the same metric can be added to the routing table (recall that the router can be configured to accept up to 16 per destination). The router maintains one routing table for each network protocol configured.

1.5 EIGRP Router ID

Each EIGRP-speaking router has an associated EIGRP router ID (RID). The RID is a 32-bit value written in dotted decimal format, like an IPv4 address. A router’s EIGRP RID is determined when the EIGRP process starts. Interestingly, EIGRP uses the same steps to RID calculation as does OSPF. The following list identifies these step, in sequential order:

Interestingly, while EIGRP requires a router to have a RID, the RID value plays a very trivial role in an EIGRP process. EIGRP neighbors can even have duplicate RIDs and still establish an EIGRP Neighbourship between them, although it’s a best practice to assign unique RIDs to EIGRP neighbors. However, before we overly minimize the RID, there is one very important time a router needs a unique router RID. Specifically, if we’re injecting external routes into an EIGRP routing process, the router performing that redistribution needs a unique RID.

1.6 EIGRP Configuration Modes

Two methods of EIGRP configuration: classic mode and named mode.

1.6.1 Classic Configuration Mode

With classic EIGRP configuration mode, most of the configuration takes place in the EIGRP process, but some settings are configured under the interface configuration sub mode. This can add complexity for deployment and troubleshooting as users must scroll back and forth between the EIGRP process and individual network interfaces. Some of the settings set individually are hello advertisement interval, split-horizon, authentication, and summary route advertisements.

Classic configuration requires the initialization of the routing process with the global configuration command router eigrp *as-number* to identify the ASN and initialize the EIGRP process. The second step is to identify the network interfaces with the command network *ip-address* [*mask*]. The network statement is explained in the following sections.

1.6.2 EIGRP Name mode

EIGRP named mode configuration was released to overcome some of the difficulties network engineers have with classic EIGRP autonomous system configuration, including scattered configurations and unclear scope of commands.

EIGRP named configuration provides the following benefits:

- All the EIGRP configuration occurs in one location.
- It supports current EIGRP features and future developments.
- It supports multiple address families (including Virtual Routing and Forwarding [VRF] instances). EIGRP named configuration is also known as multi-address family configuration mode.
- Commands are clear in terms of the scope of their configuration.

EIGRP named mode provides a hierarchical configuration and stores settings in three subsections:

Address Family: This sub mode contains settings that are relevant to the global EIGRP AS operations, such as selection of network interfaces, EIGRP K values, logging settings, and stub settings.

Interface: This sub mode contains settings that are relevant to the interface, such as hello advertisement interval, split-horizon, authentication, and summary route advertisements. In actuality, there are two methods of the EIGRP interface section's configuration. Commands can be assigned to a specific interface or to a *default* interface, in which case those settings are placed on all EIGRP-enabled interfaces. If there is a conflict between the default interface and a specific interface, the specific interface takes priority over the default interface.

Topology**:** This sub mode contains settings regarding the EIGRP topology database and how routes are presented to the router's RIB. This section also contains route redistribution and administrative distance settings.

EIGRP named configuration makes it possible to run multiple instances under the same EIGRP process.

1.7 Advantages and Disadvantages of EIGRP

Eigrp Routing Protocols have their own pros and cons but most of large business organization uses this protocol.

1.7.1 Advantages

- EIGRP uses AS (Autonomous system) number ranging from 1-65535 to identify collection of routers that share same information.
- EIGRP have less convergent time and is more efficient
- EIGRP supports both auto and manual route summarization
- Supports multiple routed protocols like IP ,IPX and apple talks
- EIGRP converges rapidly in the event of link failure
- EIGRP can load balance equal and unequal cost path. By default
- EIGRP supports 4 load balancing path. It can be extended to 6 paths

1.7.2 Disadvantages

- EIGRP routing protocol can be used only on Cisco network devices so if the company has multiple vendors networking equipment, it will not work. Cisco has opened EIGRP standard to other vendors in March 2013. Now all vendors can implement and use EIGRP on their networking equipment but advanced features are still maintained and controlled by Cisco.
- EIGRP is still distance vector routing protocol and only relies on routed provided by directly connected neighbor.
- EIGRP is not extensible and does not support future application through ''opaque'' LSA, e.g. MPLS Traffic Engineering. Opaque LSAs provide a generalized mechanism to allow for the future extensibility of OSPF.

CHAPTER 2

CONCEPTUAL STUDY OF VLAN

2.1 Understanding VLAN

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch module port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN.

Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router, as shown below. Because a VLAN is considered a separate logical network, it contains its own bridge MIB information and can support its own implementation of spanning tree.

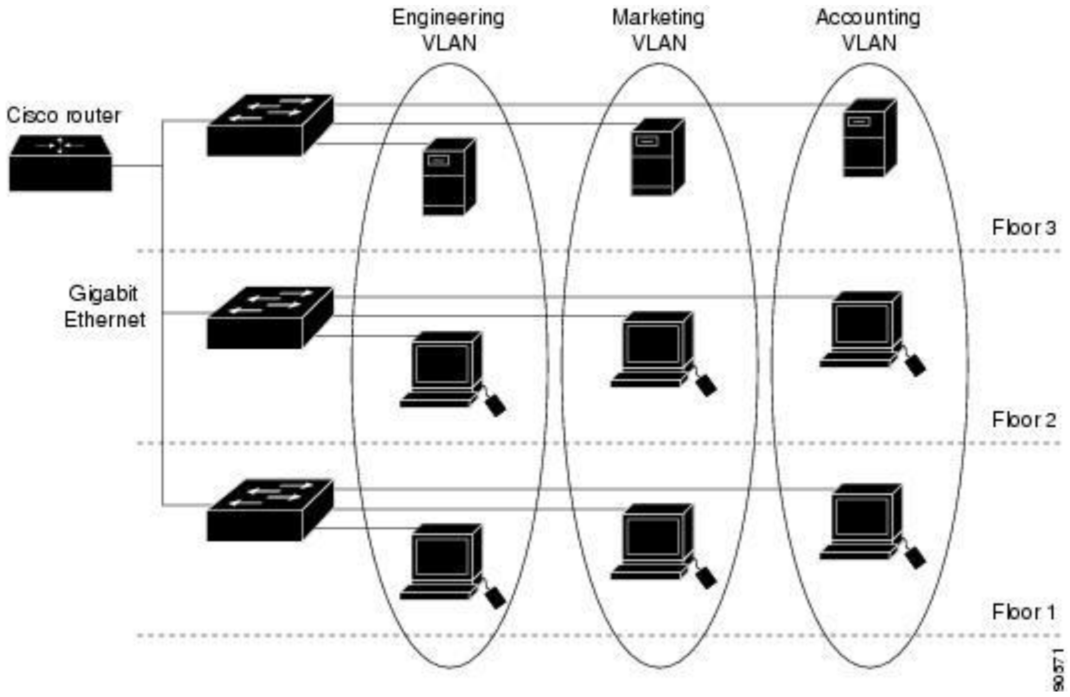


Figure 2.1 VLAN

VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch module is assigned manually on an interface-by-interface basis. When you assign switch module interfaces to VLANs by using this method, it is known as interface-based,

2.2 Supported VLAN

VLANs are identified with a number from 1 to 4094. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database.

Although the switch module supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch module hardware.

The switch module supports per-VLAN spanning-tree plus (PVST+) or rapid PVST+ with a maximum of 128 spanning-tree instances. One spanning-tree instance is allowed per VLAN.

2.3 Normal VLAN range

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. You can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)

Configurations for VLAN IDs 1 to 1005 are written to the file vlan.dat (VLAN database), and you can display them by entering the show VLAN privileged EXEC command. The vlan.dat file is stored in flash memory.

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

VLAN ID

VLAN name

VLAN type (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)

2.4 Extended VLAN Range

You can create extended-range VLANs (in the range 1006 to 4094) to enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any switchport commands that allow VLAN IDs. Extended-range VLAN configurations are not stored in the VLAN database, but they are stored in the switch module running configuration file, and you can save the configuration in the startup configuration file by using the copy running-config startup-config privileged EXEC command.

2.5 How VLAN Work

A VLAN is a set of end stations and the switch ports that connect them. You can have different reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Adding virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast. Like a router, it partitions the network into logical segments, which provides better administration, security, and management of multicast traffic.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station might omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet can either reject it or insert a tag using its default VLAN ID. A given port can handle traffic for more than one VLAN, but it can support only one default VLAN ID.

The Private Edge VLAN feature lets you set protection between ports located on the switch. This means that a protected port cannot forward traffic to another protected port on the same switch. The feature does not provide protection between ports located on different switches.

The diagram in this article shows a switch with four ports configured to handle the traffic for two VLANs. Port 1/0/2 handles traffic for both VLANs, while port 1/0/1 is a member of VLAN 2 only, and ports 1/0/3 and 1/0/4 are members of VLAN 3 only. The script following the diagram shows the commands you would use to configure the switch as shown in the diagram.

2.6 Internal study of VLAN

The magic of how virtual local area networks (VLANs) work is found in the Ethernet headers. When a switch receives an Ethernet frame, the frame will either already have a VLAN tag or the switch will insert a VLAN tag into the Ethernet header. If the frame was received from another switch, that switch will have already inserted the VLAN tag; while frames come from network devices, such as computers, the frame will not have a VLAN tag.

If you are using the switch defaults for VLANs, the VLAN tag that will be placed on the frame is VLAN1. When placing a VLAN tag (also known as an IEEE 802.1Q tag) on the Ethernet frame, the four bytes of data, which make up the VLAN tag, are inserted before the Type field, as shown in the following figure. This 4-byte header includes several pieces of information:

A 2-byte Tag Protocol Identifier (TPID), which will be set to a value of 0x8100 to denote that this frame carries 802.1Q or 802.1p tag information.

A 2-byte Tag Control Information (TCI), which is made of the following:

A 3-bit user Priority Code Point (PCP) that sets a priority value between 0 and 7, which can be used for Quality of Service (QoS) priority traffic delivery.

A 1-bit Canonical Format Indicator (CFI) that is a compatibility bit between Ethernet and other network structures, such as Token Ring. For Ethernet networks, this value will also be set to zero.

A 12-bit VLAN Identifier (VID) that identifies the VLAN the frame belongs to.

2.7 VLAN Frame

Now you know how to move VLAN traffic from one switch to another by using IEEE 802.1Q tags or ISL frames across ISL links, but how does VLAN information get onto the frames in the first place? There are both manual and automatic methods for doing this, but the most common method is the manual method of configuring a port-based VLAN.

With a port-based VLAN, your switch examines data that comes in on a port, and if the data is not already tagged with a VLAN, the switch then places a VLAN tag on the data.

When implementing VLANs on your network, you use trunk ports for your inter-switch links, but for your client access ports, you use Access mode instead of Trunk mode.

When you unbox your new switch, all ports are in Access mode by default; that means that they expect to have computing devices connected to them, and they will automatically insert IEEE 802.1Q tags into any Ethernet frames that do not already have tags. Typically, ports in Access mode expect to see untagged traffic because computers and other devices do not know how to pre-tag Ethernet frames.

If you have implemented IP telephony, IP phones are capable of tagging their own traffic through an integrated two-port switch.

A switch does not expect to see traffic with VLAN tags on ports in Access mode because most devices on those ports do not tag their own traffic; traffic on Trunk mode ports automatically allow traffic tagged for any VLANs to be sent to connected switches. Because Trunk mode ports send traffic tagged for any VLAN, they expect to see traffic arriving from connected switches tagged for any VLAN.

2.8 Passing traffic from VLAN to VLAN

VLANs allow you to isolate users from each other by placing them in different VLANs, but now how do you pass traffic from one VLAN to another VLAN? Doing so involves the use of a Layer 3 device to route the traffic from one VLAN to another; yes, that would be router. Therefore, if your router does not support VLANs or VLAN tagging, this process will require an interface configured on each VLAN, which can be an expensive proposition.

The best solution is to purchase a router that supports VLANs, which means you can connect a single interface on your router to a Trunk mode port on your switch, which allows the router to internally route between virtual VLAN interfaces.

The other option you have available to you is to purchase a Layer 3 switch, which is a switch with routing functions built into it. That is, they are capable of providing all the inter-VLAN routing functionality, without leaving the switching device.

CHAPTER 3

ROUTER AND SWITCH SECURITY

3.1 Router Security

Router Security is an activity designed to protect the integrity and usability of the network and the data. It includes both hardware and software technologies to protect your network form the threads. Now days, Security is most essential part of every organization, they want to protect their data as well as their router from intruders and harmful thread and activities. For this purpose, they implement the router security methods to remove harmful threads.

The method that is used for securities are

- Authentications
- VLANS
- Port Security

3.1.1 Authentications

To enhance the security of your network you have to set passwords to routers and switches so that unauthorized person can't have access them. For this purpose, the routers and switches have their own authentication services like password or encrypted password. You can set the password to the console, and auxiliary port as well as the router user mode and privilege mode too so no unauthorized person can even telnet your router or switch. The password must be given by the person who has the responsibility to maintain the network devices say, Network Administrator of an organization.

3.1.2 Virtual Local Area Network

It was hard to establish the communication between the LAN's network before 1980's. You used to define separate networks for different LAN. For this, you would have to define different IP address for each LAN network using multiple switches for each LAN. After the VLAN technology it overcame this scenario using one switch having different LAN network on the same switch.

The VLAN technology has an important role in the networking and an important topic in networking. Let us tell you about a scenario before VLAN.

For example, a company having finance department and a client so they are totally different physical networks. In order to communicate with the finance department, you would have to make two different physical network for them using separate switches. So VLANs were introduced to logical separate or segment the networks using one switch.

We take a single switch and chop it up in multiple networks where the traffic is actually separate between these network means that multiple networks on the same physical hardware say, switch and still we can keep their traffic completely different. Also, the VLANs that are created for the separate networks are also logically separate for each other inside the switch. It reduces the cost of an organization to purchase multiple switches.

VLANs make it easy for the network administrator to partition a single switched network to match the functional and security requirements of their system without having to run new cables or make major changes in their current network infrastructure. VLANs are often set up by larger businesses to re-partition device for better traffic managements.

It also provides higher degree of security on the network by allowing control over device like which devices have access to each other.

3.1.3 Port Security

Port security limits the number of valid MAC addresses allowed on a port. The MAC addresses of the device that is permitted are allowed to have access, while other host with different MAC addresses are denied. If any other MAC address is connected, then it violates the port security rules, and that port is automatically shut down.

You would have to define how many MAC addresses you allow to the particular port but once it is violated by undefined MAC address it denies it and the port is being shut down.

CHAPTER 4
NETWORK DEVICES AND PROTOCOLS

4.1 Routers

A router is a layer 3 network device of the OSI Model that forwards data packets between the computer and networks. It directly performs traffic over the network. A packet is forwarded form one router to another router, according to some rules and regulations called Protocols. The router acknowledges the packet source and destination IP address. Router works on IP address. Router builds up a routing table listing the preferred routes between any two computer or routers between the network.

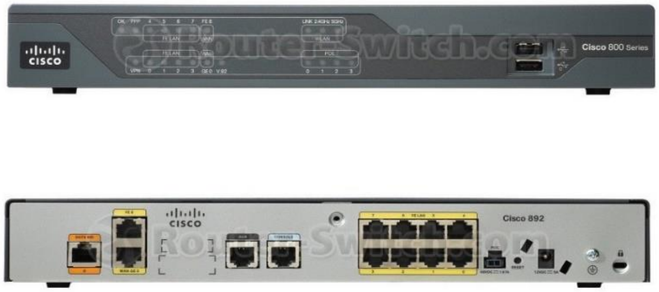


Figure 4.1 Cisco Router

It accepts two types of IP address that are

I. Static
II. Dynamic

Static routes are fed manually in router, while dynamic router are advertised, and every router that uses the same routing protocol feeds it in its routing table automatically.

It has interface through it connects to other router, switches and computers. It has Fast Ethernet interface, Serial interface, Auxiliary and console ports.

Console port is used for the configuration of routers. Router is an intelligent device and has the following components defined

i. Processor
ii. RAM
iii. NVRAM

iv. Flash Memory
v. ROM

4.1.1 Processor

Router makes the decision making solution through processor. Processor processes all the operations of the routers i.e. Data sending/Receiving, Packet identifying, Possible routes of the destination network.

4.1.2 Random Access Memory

It stores the run-time configuration of the router. It is a volatile memory that temporary stores the router configuration which is call running-configurations. When router is switched off all the data is flashed.

4.1.3 Non-Volatile Random Access Memory (NVRAM)

It is a build-in chip with in the routers. It permanently stores the router configuration and all the saved configuration are stored on NVRAM. The configuration stored on NVRAM are called start-up configuration. RAM can be changed but NVRAM is fixed and can't be changed.

4.1.4 Flash Memory

The flash memory stores the operating system of the router. The operating system of the router is called IOS (Internetwork Operating System).

If the router operating system crashes, then you have to reinstall it through flash memory.

4.1.5 Read Only Memory

ROM is read-only memory available on a router's processor board. The initial bootstrap software that runs on a Cisco router is usually stored in ROM. ROM also maintains instructions for Power-on Self-Test (POST) diagnostics. For ROM Software upgrades, the pluggable chips on the motherboard should be replaced.

4.2 Switches

Switch is a layer 2 network device of the OSI Model that connects devices on computer network by using packet switching of receiving and sending packet with in a network. It is also call Switching hub, Bridging Hub, MAC Bridge. Switch is an intelligent device which save the MAC address of the computer attached to it. It doesn't broadcast the packet send by source device. It's a LAN (Local Area Network) device. It also performs error checking before sending the data. It has multiple ports for node-to-node communications. The difference between Router and Switch is that router can connect other network too but switch can only able to set communication within same network.

Figure 4.2 D-Link Switch

4.3 Dynamic Host Configuration Protocol (DHCP)

It is a network protocol used on IP network, that automatically assign an IP address and other information to each host connected to it. In addition to the IP address, the DHCP also assigns the subnet mask, default gateway address, Domain Name Server address.

No two host over the same network has same IP address means that every host in a network must have different IP address. In a network, where a huge amount of hosts is present, so giving an IP address to a host is difficult and can produce error, because we cannot remember the IP address, that are assign to host or the remaining address, Therefore, DHCP is very useful for the assigning of the IP addresses to the host automatically.

4.4 MLS (MULTI-LAYER SWITHCH)

Multi-layer switch is also known is Layer 3 switch. It is also used for forwarding traffic between different Vlan. In MLS we make SVI to each Vlan and assign IP address to each SVI.

CHAPTER 5

ROUTERS & SWITCHES CONFIGURATIONS

5.1 Configuration of Islamabad Router

5.1.1 Hostname and password configuration

```
Router>
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host
Router(config)#hostname isb-router
isb-router(config)#
isb-router(config)#enable secret isb12345
isb-router(config)#exit
isb-router#
```

5.1.2 Interface configuration

```
Isb-router>
isb-router>enable
Password:
isb-router#
Isb-router#config t
Enter configuration commands, one per line. End with CNTL/Z.
isb-router (config)#
isb-router (config)#
isb-router (config)#interface serial 0/0
isb-router (config-if)#ip address 40.0.0.1 255.0.0.0
isb-router (config-if)#encapsulation hdlc
isb-router (config-if)#clock rate 64000
isb-router (config-if)#keepalive 10
isb-router (config-if)#no shutdown
```

```
Isb-router>
isb-router>enable
Password:
isb-router#
isb-router#config t
Enter configuration commands, one per line. End with CNTL/Z.
isb-router (config)#
isb-router (config)#
isb-router (config)#interface serial 0/1
isb-router (config-if)#ip address 20.0.0.2 255.0.0.0
isb-router (config-if)#encapsulation hdlc
isb-router (config-if)#clock rate 64000
isb-router (config-if)#keepalive 10
isb-router (config-if)#no shutdown
```

```
Isb-router>
isb-router>enable
Password:
isb-router#
isb-router#config t
Enter configuration commands, one per line. End with CNTL/Z.
isb-router (config)#interface fastEthernet 0/0
isb-router (config-if)#no shutdown
isb-router (config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
```

5.1.3 EIGRP configuration

```
Isb-router>
Isb-router>enable
Password:
Isb-router#
```

Isb-router#config t

Enter configuration commands, one per line. End with CNTL/Z.

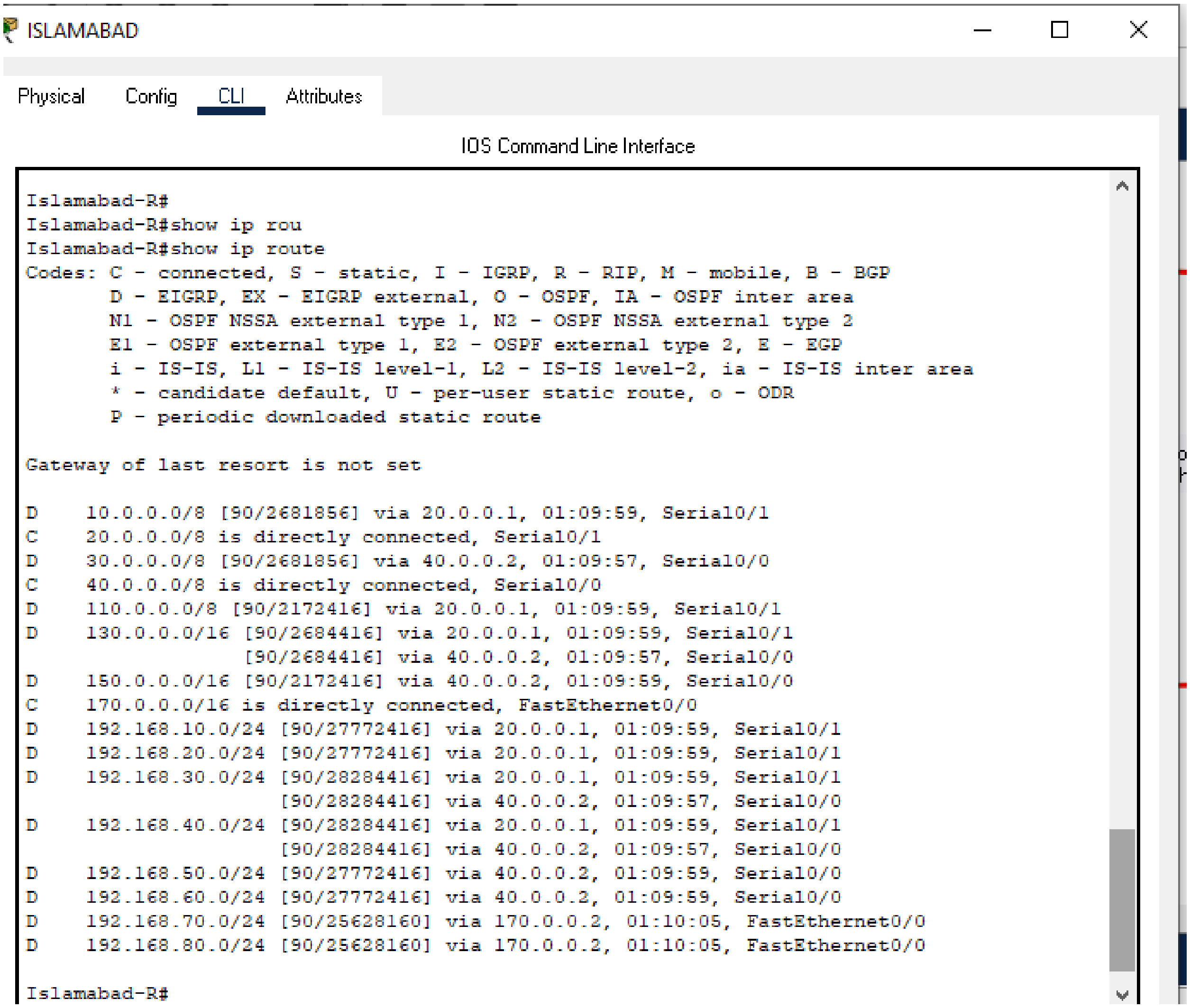
isb-router (config)#router eigrp 50

isb-router (config-router)#network 20.0.0.0

isb-router (config-router)#network 40.0.0.0

isb-router (config-router)#network 170.0.0.0

isb-router (config-router)#exit



```
Islamabad-R#
Islamabad-R#show ip rou
Islamabad-R#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    10.0.0.0/8 [90/2681856] via 20.0.0.1, 01:09:59, Serial0/1
C    20.0.0.0/8 is directly connected, Serial0/1
D    30.0.0.0/8 [90/2681856] via 40.0.0.2, 01:09:57, Serial0/0
C    40.0.0.0/8 is directly connected, Serial0/0
D    110.0.0.0/8 [90/2172416] via 20.0.0.1, 01:09:59, Serial0/1
D    130.0.0.0/16 [90/2684416] via 20.0.0.1, 01:09:59, Serial0/1
                  [90/2684416] via 40.0.0.2, 01:09:57, Serial0/0
D    150.0.0.0/16 [90/2172416] via 40.0.0.2, 01:09:59, Serial0/0
C    170.0.0.0/16 is directly connected, FastEthernet0/0
D    192.168.10.0/24 [90/27772416] via 20.0.0.1, 01:09:59, Serial0/1
D    192.168.20.0/24 [90/27772416] via 20.0.0.1, 01:09:59, Serial0/1
D    192.168.30.0/24 [90/28284416] via 20.0.0.1, 01:09:59, Serial0/1
                     [90/28284416] via 40.0.0.2, 01:09:57, Serial0/0
D    192.168.40.0/24 [90/28284416] via 20.0.0.1, 01:09:59, Serial0/1
                     [90/28284416] via 40.0.0.2, 01:09:57, Serial0/0
D    192.168.50.0/24 [90/27772416] via 40.0.0.2, 01:09:59, Serial0/0
D    192.168.60.0/24 [90/27772416] via 40.0.0.2, 01:09:59, Serial0/0
D    192.168.70.0/24 [90/25628160] via 170.0.0.2, 01:10:05, FastEthernet0/0
D    192.168.80.0/24 [90/25628160] via 170.0.0.2, 01:10:05, FastEthernet0/0

Islamabad-R#
```

Figure 5.1 routing table Of ISB-router

5.2 Configuration of Peshawar Router

5.2.1 Hostname and password configuration

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname PEW-router
PEW-router(config)#enable secret pew12345
PEW-router(config)#
PEW-router(config)#exit
PEW-router#
```

5.2.2 Interface configuration

```
PEW-router(config)#interface serial 0/1
PEW-router(config-if)#ip address 30.0.0.2 255.0.0.0
PEW-router(config-if)#encapsulation hdlc
PEW-router(config-if)#keepalive 10
PEW-router(config-if)#clock rate 64000
PEW-router(config-if)no shutdown
PEW-router(config-if)#exit

PEW-router(config)#interface serial 0/0
PEW-router(config-if)#ip address 40.0.0.2 255.0.0.0
PEW-router(config-if)#encapsulation hdlc
PEW-router(config-if)#keepalive 10
PEW-router(config-if)#clock rate 64000
PEW-router(config-if)no shutdown
PEW-router(config-if)#exit

PEW-router#
PEW-router#config t
Enter configuration commands, one per line. End with CNTL/Z.
PEW-router(config)#interface fastEthernet 0/0
PEW-router(config-if)#ip address 150.0.0.1 255.255.0.0
```

PEW-router(config-if)#no shutdown

PEW-router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

PEW-router(config-if)#exit

PEW-router(config)#

5.2.3 EIGRP configuration

PEW-Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

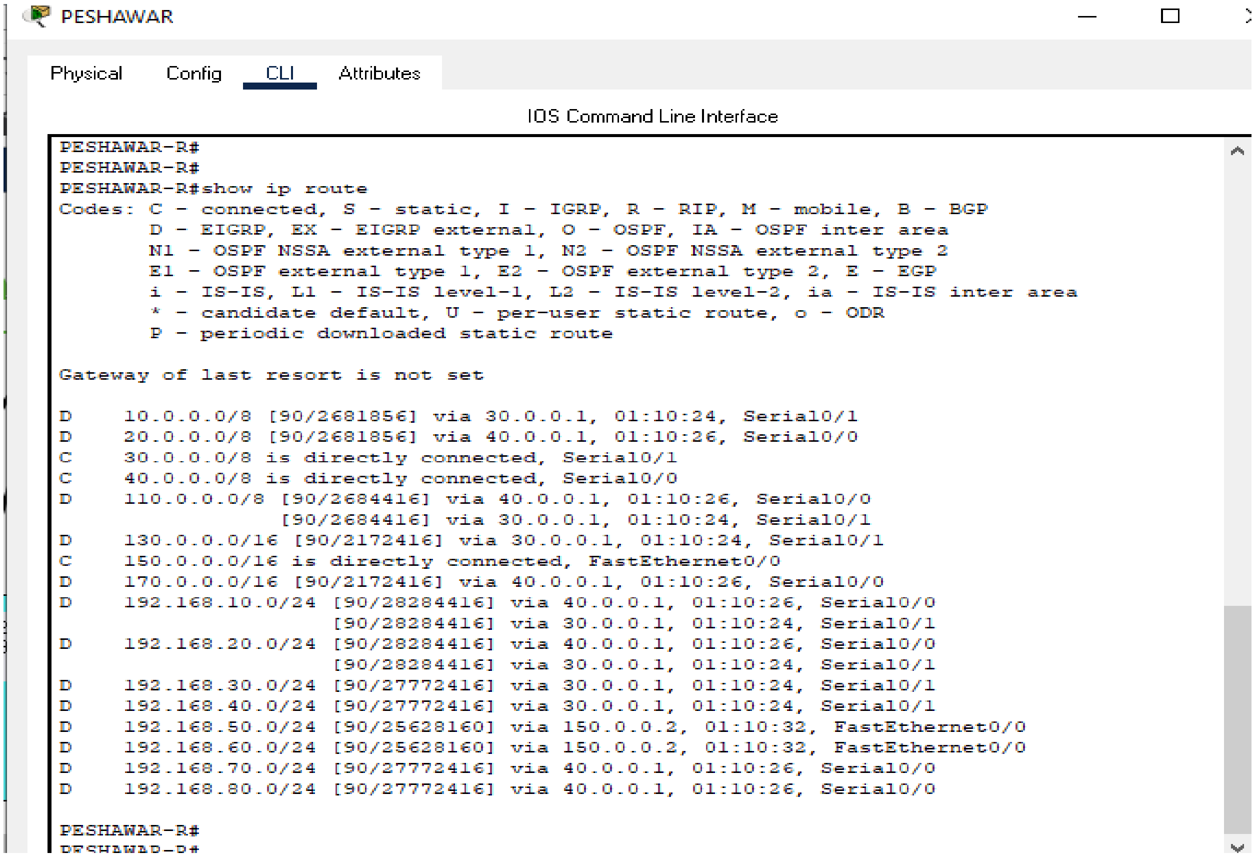
PEW-router(config)#router eigrp 50

PEW-router(config-router)#network 30.0.0.0

PEW-router(config-router)#network 150.0.0.0

PEW-router(config-router)#network 40.0.0.0

PEW-router(config-router)#exit



```
PESHAWAR-R#
PESHAWAR-R#
PESHAWAR-R#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    10.0.0.0/8 [90/2681856] via 30.0.0.1, 01:10:24, Serial0/1
D    20.0.0.0/8 [90/2681856] via 40.0.0.1, 01:10:26, Serial0/0
C    30.0.0.0/8 is directly connected, Serial0/1
C    40.0.0.0/8 is directly connected, Serial0/0
D    110.0.0.0/8 [90/2684416] via 40.0.0.1, 01:10:26, Serial0/0
                 [90/2684416] via 30.0.0.1, 01:10:24, Serial0/1
D    130.0.0.0/16 [90/2172416] via 30.0.0.1, 01:10:24, Serial0/1
C    150.0.0.0/16 is directly connected, FastEthernet0/0
D    170.0.0.0/16 [90/2172416] via 40.0.0.1, 01:10:26, Serial0/0
D    192.168.10.0/24 [90/28284416] via 40.0.0.1, 01:10:26, Serial0/0
                     [90/28284416] via 30.0.0.1, 01:10:24, Serial0/1
D    192.168.20.0/24 [90/28284416] via 40.0.0.1, 01:10:26, Serial0/0
                     [90/28284416] via 30.0.0.1, 01:10:24, Serial0/1
D    192.168.30.0/24 [90/27772416] via 30.0.0.1, 01:10:24, Serial0/1
D    192.168.40.0/24 [90/27772416] via 30.0.0.1, 01:10:24, Serial0/1
D    192.168.50.0/24 [90/25628160] via 150.0.0.2, 01:10:32, FastEthernet0/0
D    192.168.60.0/24 [90/25628160] via 150.0.0.2, 01:10:32, FastEthernet0/0
D    192.168.70.0/24 [90/27772416] via 40.0.0.1, 01:10:26, Serial0/0
D    192.168.80.0/24 [90/27772416] via 40.0.0.1, 01:10:26, Serial0/0

PESHAWAR-R#
PESHAWAR-R#
```

Figure 5.2 routing table Of PEW-router

5.3 Configuration of Lahore Router

5.3.1 Hostname and password configuration

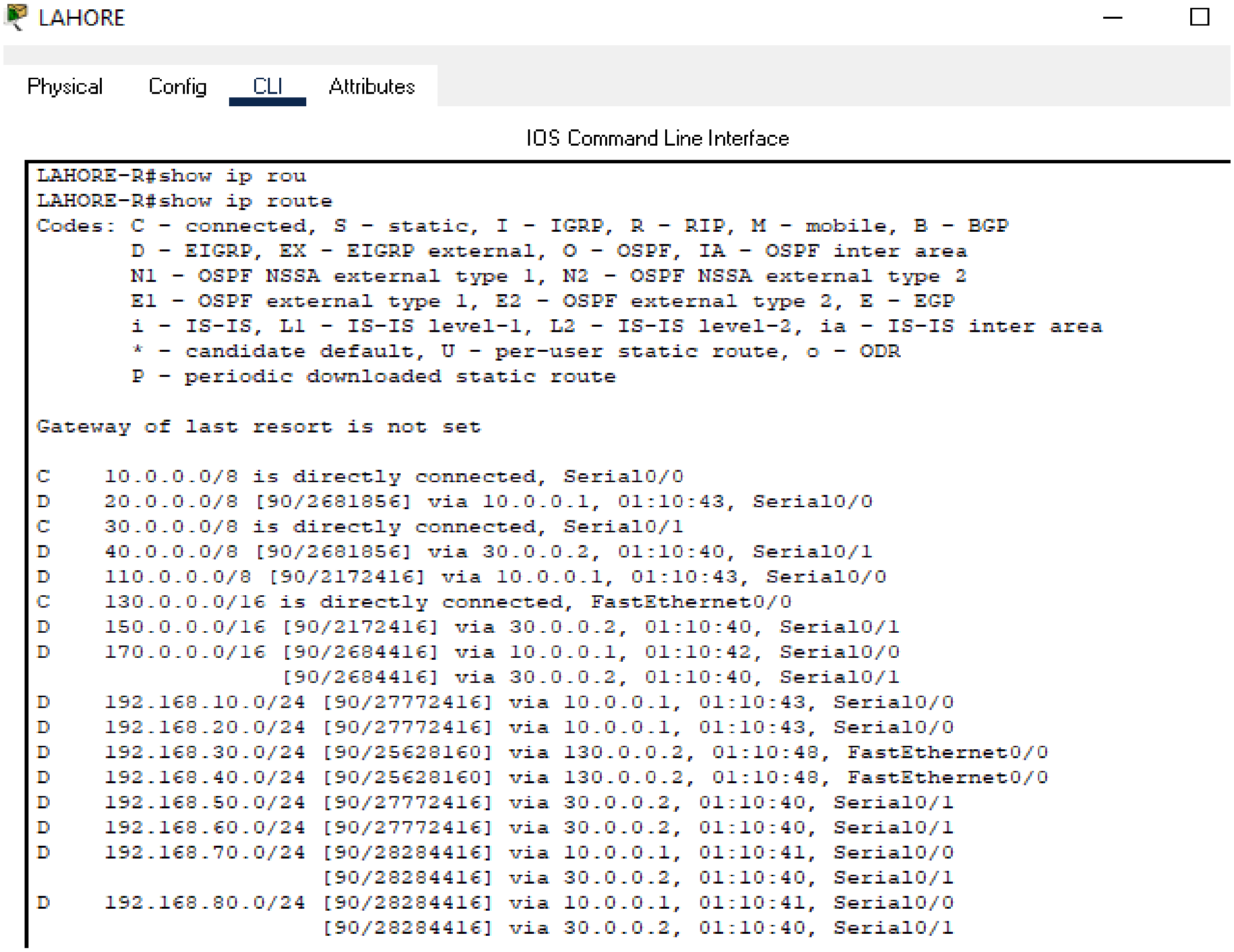
```
Router>enable

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname LHR-router

LHR-router(config)#enable secret lhr12345

LHR -router(config)#

LHR -router(config)#exit

LHR -router#
```

5.3.2 Interface configuration

```
LHR-Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

LHR-router(config)#interface serial 0/0

LHR-router(config-if)#ip address 10.0.0.2 255.0.0.0

LHR-router(config-if)#encapsulation hdlc

LHR-router(config-if)#clock rate 64000

LHR-router(config-if)#keepalive 10

LHR-router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0, changed state to up

LHR-router(config-if)#

LHR-router(config-if)#exit
```

```
LHR-Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

LHR-router(config)#interface serial 0/1

LHR-router(config-if)#ip address 30.0.0.1 255.0.0.0

LHR-router(config-if)#encapsulation hdlc

LHR-router(config-if)#clock rate 64000

LHR-router(config-if)#keepalive 10
```

```
LHR-router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
LHR-router(config-if)#
LHR-router(config-if)#exit

LHR-Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
LHR-router(config)#interface fastEthernet 0/0
LHR-router(config-if)#ip address 130.0.0.1 255.255.0.0
LHR-router(config-if)#no shutdown
LHR-router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
LHR-router(config-if)#exit
```



```
LAHORE-R#show ip rou
LAHORE-R#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0
D    20.0.0.0/8 [90/2681856] via 10.0.0.1, 01:10:43, Serial0/0
C    30.0.0.0/8 is directly connected, Serial0/1
D    40.0.0.0/8 [90/2681856] via 30.0.0.2, 01:10:40, Serial0/1
D    110.0.0.0/8 [90/2172416] via 10.0.0.1, 01:10:43, Serial0/0
C    130.0.0.0/16 is directly connected, FastEthernet0/0
D    150.0.0.0/16 [90/2172416] via 30.0.0.2, 01:10:40, Serial0/1
D    170.0.0.0/16 [90/2684416] via 10.0.0.1, 01:10:42, Serial0/0
                  [90/2684416] via 30.0.0.2, 01:10:40, Serial0/1
D    192.168.10.0/24 [90/27772416] via 10.0.0.1, 01:10:43, Serial0/0
D    192.168.20.0/24 [90/27772416] via 10.0.0.1, 01:10:43, Serial0/0
D    192.168.30.0/24 [90/25628160] via 130.0.0.2, 01:10:48, FastEthernet0/0
D    192.168.40.0/24 [90/25628160] via 130.0.0.2, 01:10:48, FastEthernet0/0
D    192.168.50.0/24 [90/27772416] via 30.0.0.2, 01:10:40, Serial0/1
D    192.168.60.0/24 [90/27772416] via 30.0.0.2, 01:10:40, Serial0/1
D    192.168.70.0/24 [90/28284416] via 10.0.0.1, 01:10:41, Serial0/0
                     [90/28284416] via 30.0.0.2, 01:10:40, Serial0/1
D    192.168.80.0/24 [90/28284416] via 10.0.0.1, 01:10:41, Serial0/0
                     [90/28284416] via 30.0.0.2, 01:10:40, Serial0/1
```

Figure 5.3 routing table Of LHR-router

5.3.3 EIGRP configuration

```
LHR-Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
LHR-router(config)#router eigrp 50
LHR-router(config-router)#network 130.0.0.0
LHR-router(config-router)#network 10.0.0.0
LHR-router(config-router)#network 30.0.0.0
LHR-router(config-router)#exit
```

5.4 Configuration of Karachi Router

5.4.1 Hostname and password configuration

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname KHI-router
KHI-router(config)#enable secret khi12345
KHI-router(config)#exit
KHI-router#
%SYS-5-CONFIG_I: Configured from console by console
```

5.4.2 Interface configuration

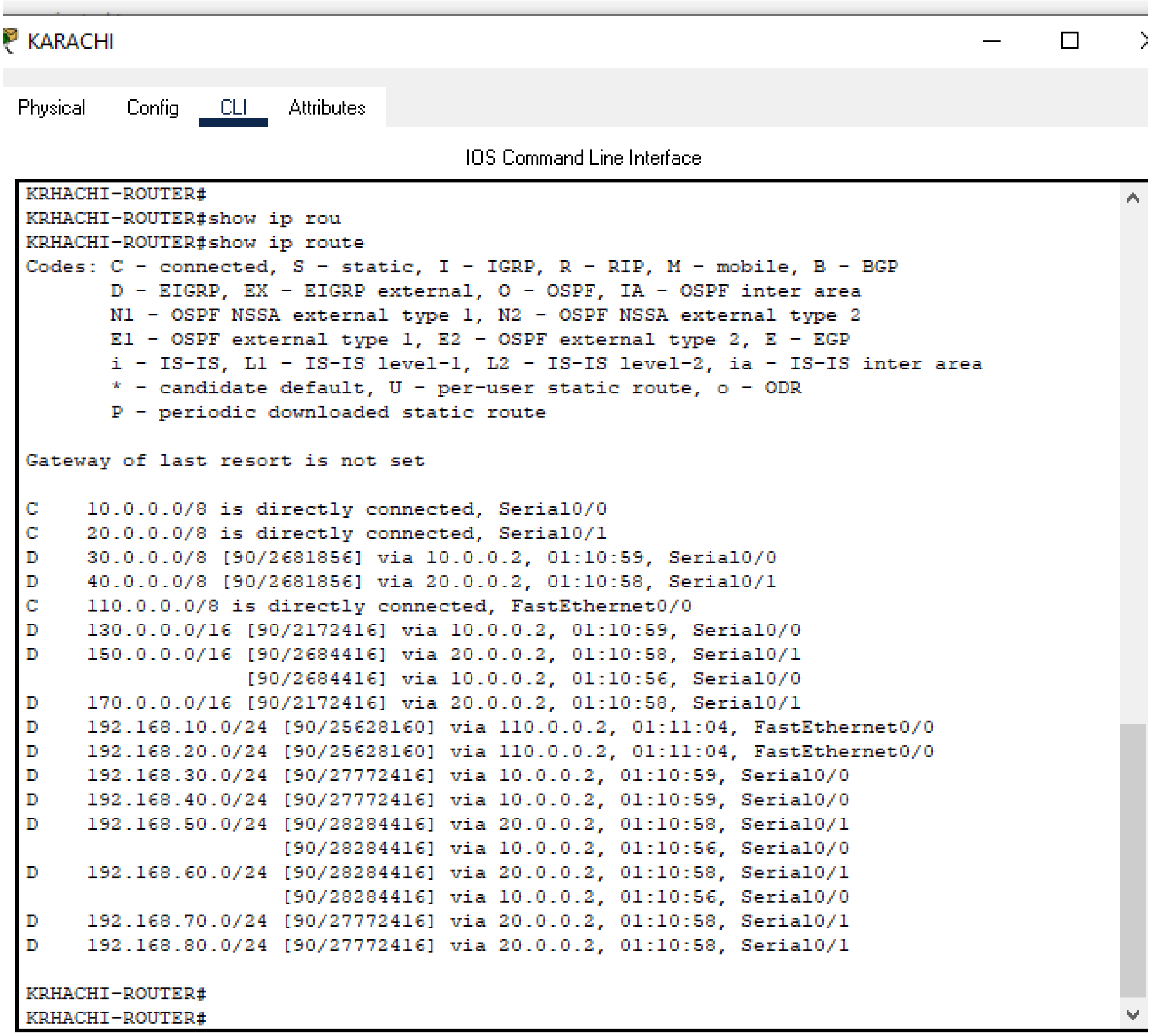
```
KHI-Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
KHI-router(config)#interface fastEthernet 0/0
KHI-router(config-if)#ip address 110.0.0.1 255.0.0.0
KHI-router(config-if)#no shutdown
KHI-router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
KHI-router(config-if)#exit

KHI-Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
KHI-router(config)#interface serial 0/0
KHI-router(config-if)#ip address 10.0.0.1 255.0.0.0
KHI-router(config-if)#encapsulation hdlc
KHI-router(config-if)#clock rate 64000
KHI-router(config-if)#keepalive 10
KHI-router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
KHI-router(config-if)#
KHI-router(config-if)#exit
```

```
KHI-Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
KHI-router(config)#interface serial 0/1
KHI-router(config-if)#ip address 20.0.0.1 255.0.0.0
KHI-router(config-if)#encapsulation hdlc
KHI-router(config-if)#clock rate 64000
KHI-router(config-if)#keepalive 10
KHI-router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to up
KHI-router(config-if)#
KHI-router(config-if)#exit
```

5.4.3 EIGRP configuration

```
KHI-Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
KHI-router(config)#router eigrp 50
KHI-router(config-router)#network 10.0.0.0
KHI-router(config-router)#network 20.0.0.0
KHI-router(config-router)#network 110.0.0.0
KHI-router(config-router)#exit
KHI-router(config)#
```



```
KRHACHI-ROUTER#
KRHACHI-ROUTER#show ip rou
KRHACHI-ROUTER#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0
C    20.0.0.0/8 is directly connected, Serial0/1
D    30.0.0.0/8 [90/2681856] via 10.0.0.2, 01:10:59, Serial0/0
D    40.0.0.0/8 [90/2681856] via 20.0.0.2, 01:10:58, Serial0/1
C    110.0.0.0/8 is directly connected, FastEthernet0/0
D    130.0.0.0/16 [90/2172416] via 10.0.0.2, 01:10:59, Serial0/0
D    150.0.0.0/16 [90/2684416] via 20.0.0.2, 01:10:58, Serial0/1
                  [90/2684416] via 10.0.0.2, 01:10:56, Serial0/0
D    170.0.0.0/16 [90/2172416] via 20.0.0.2, 01:10:58, Serial0/1
D    192.168.10.0/24 [90/25628160] via 110.0.0.2, 01:11:04, FastEthernet0/0
D    192.168.20.0/24 [90/25628160] via 110.0.0.2, 01:11:04, FastEthernet0/0
D    192.168.30.0/24 [90/27772416] via 10.0.0.2, 01:10:59, Serial0/0
D    192.168.40.0/24 [90/27772416] via 10.0.0.2, 01:10:59, Serial0/0
D    192.168.50.0/24 [90/28284416] via 20.0.0.2, 01:10:58, Serial0/1
                     [90/28284416] via 10.0.0.2, 01:10:56, Serial0/0
D    192.168.60.0/24 [90/28284416] via 20.0.0.2, 01:10:58, Serial0/1
                     [90/28284416] via 10.0.0.2, 01:10:56, Serial0/0
D    192.168.70.0/24 [90/27772416] via 20.0.0.2, 01:10:58, Serial0/1
D    192.168.80.0/24 [90/27772416] via 20.0.0.2, 01:10:58, Serial0/1

KRHACHI-ROUTER#
KRHACHI-ROUTER#
```

Figure 5.4 routing table Of KHI-router

5.5 Configuration of Islamabad MLS switch

5.5.1 Hostname and password configuration

Switch>

Switch>enable

Switch#

Switch#config t

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#hostname ISB-MLS
Islamabad-MLS (config)#ENABLE SECRET isb12345
Islamabad-MLS (config)#
Islamabad-MLS (config)#exit
```

5.5.2 Interface configuration

```
Islamabad-MLS#config t
Enter configuration commands, one per line. End with CNTL/Z.
Islamabad-MLS(config)#
Islamabad-MLS(config)#interface fastEthernet 0/24
Islamabad-MLS(config-if)#ip address 170.0.0.2 255.255.0.0
Islamabad-MLS(config-if)#no shutdown
Islamabad-MLS(config-if)#
Islamabad-MLS(config-if)#exit
```

5.5.3 SVI configuration

```
Islamabad-MLS#config t
Enter configuration commands, one per line. End with CNTL/Z.
Islamabad-MLS(config)#interface vlan 70
Islamabad-MLS(config-if)#ip address 192.168.70.100 255.255.255.0
Islamabad-MLS(config-if)#no shutdown
Islamabad-MLS(config-if)#
Islamabad-MLS(config-if)#exit
```

```
Islamabad-MLS#config t
Enter configuration commands, one per line. End with CNTL/Z.
Islamabad-MLS(config)#interface vlan 80
Islamabad-MLS(config-if)#ip address 192.168.80.100 255.255.255.0
Islamabad-MLS(config-if)#no shutdown
Islamabad-MLS(config-if)#
Islamabad-MLS(config-if)#exit
```

5.5.4 Trunk port configuration

Islamabad-MLS#config t

Enter configuration commands, one per line. End with CNTL/Z.

Islamabad-MLS(config)#interface fastEthernet 0/1

Islamabad-MLS(config-if)#switchport mode trunk

Islamabad-MLS(config-if)#exit

5.5.5 Dhcp configuration

Ip dhcp pool vlan70
Network 192.168.70.0 255.255.255.0
Default-router 192.168.70.100
Dns-server 8.8.8.8

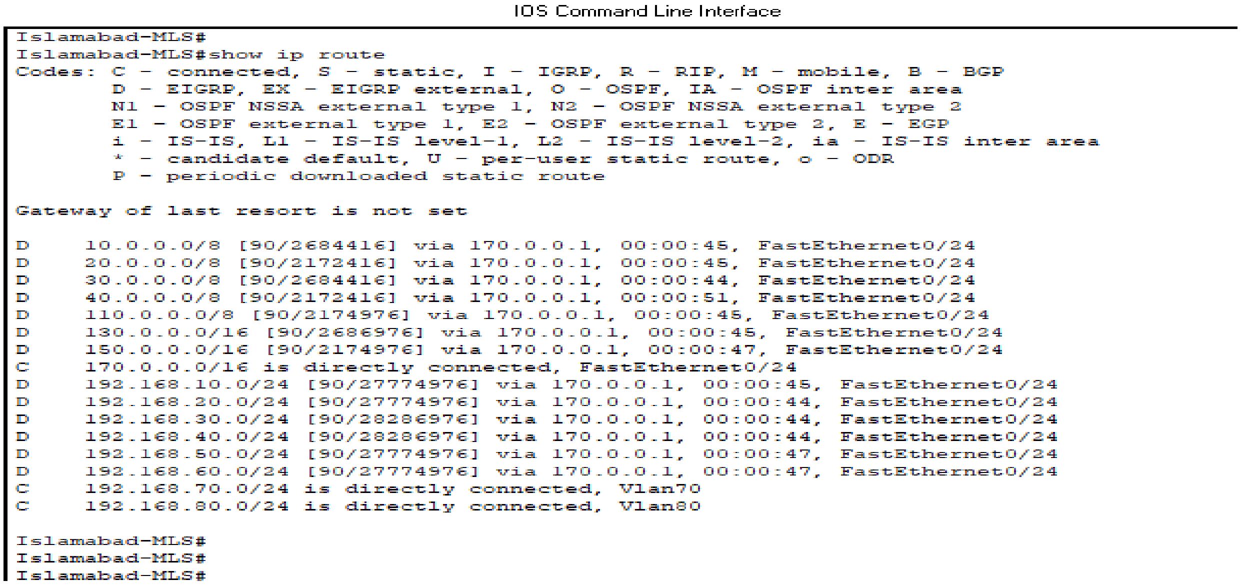
Ip dhcp pool vlan80
Network 192.168.80.0 255.255.255.0
Default-router 192.168.80.100
Dns-server 8.8.8.8

5.5.6 EIGRP configuration

Router eigrp 50

Network 170.0.0.0

Network 192.0.0.0 0.255.255.255



```
Islamabad-MLS#
Islamabad-MLS#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    10.0.0.0/8 [90/2684416] via 170.0.0.1, 00:00:45, FastEthernet0/24
D    20.0.0.0/8 [90/2172416] via 170.0.0.1, 00:00:45, FastEthernet0/24
D    30.0.0.0/8 [90/2684416] via 170.0.0.1, 00:00:44, FastEthernet0/24
D    40.0.0.0/8 [90/2172416] via 170.0.0.1, 00:00:51, FastEthernet0/24
D    110.0.0.0/8 [90/2174976] via 170.0.0.1, 00:00:45, FastEthernet0/24
D    130.0.0.0/16 [90/2686976] via 170.0.0.1, 00:00:45, FastEthernet0/24
D    150.0.0.0/16 [90/2174976] via 170.0.0.1, 00:00:47, FastEthernet0/24
C    170.0.0.0/16 is directly connected, FastEthernet0/24
D    192.168.10.0/24 [90/27774976] via 170.0.0.1, 00:00:45, FastEthernet0/24
D    192.168.20.0/24 [90/27774976] via 170.0.0.1, 00:00:44, FastEthernet0/24
D    192.168.30.0/24 [90/28286976] via 170.0.0.1, 00:00:44, FastEthernet0/24
D    192.168.40.0/24 [90/28286976] via 170.0.0.1, 00:00:44, FastEthernet0/24
D    192.168.50.0/24 [90/27774976] via 170.0.0.1, 00:00:47, FastEthernet0/24
D    192.168.60.0/24 [90/27774976] via 170.0.0.1, 00:00:47, FastEthernet0/24
C    192.168.70.0/24 is directly connected, Vlan70
C    192.168.80.0/24 is directly connected, Vlan80

Islamabad-MLS#
Islamabad-MLS#
Islamabad-MLS#
```

Figure 5.5 **routing table Of ISB-MLS**

5.6 Configuration of Peshawar MLS switch

5.6.1 Hostname and password configuration

```
Sw#config t
Enter configuration commands, one per line. End with CNTL/Z.
Sw (config)#
sw (config)#hostname PESHAWAR-MLS
Peshawar-MLS (config)#enable secret pew12345
Peshawar-MLS (config)#
Peshawar-MLS (config)#exit
Peshawar-MLS#
```

5.6.2 Interface configuration

```
Islamabad-MLS#config t
Enter configuration commands, one per line. End with CNTL/Z.
Peshawar -MLS(config)#
Peshawar-MLS(config)#interface fastEthernet 0/24
Peshawar-MLS(config-if)#ip address 150.0.0.2 255.255.0.0
Peshawar-MLS(config-if)#no shutdown
Peshawar-MLS(config-if)#
Peshawar-MLS(config-if)#exit
```

5.6.3 SVI configuration

```
PESHAWAR-MLS#config t
Enter configuration commands, one per line. End with CNTL/Z.
PESHAWAR-MLS(config)#interface vlan 50
PESHAWAR-MLS(config-if)#ip address 192.168.50.100 255.255.255.0
PESHAWAR-MLS(config-if)#no shutdown
PESHAWAR-MLS(config-if)#exit
PESHAWAR-MLS(config)#interface vlan 60
PESHAWAR-MLS(config-if)#ip address 192.168.60.100 255.255.255.0
PESHAWAR-MLS(config-if)#no shutdown
PESHAWAR-MLS(config-if)#exit
```

5.6.4 Trunk port configuration

```
PESHAWAR -Sw#config t
Enter configuration commands, one per line. End with CNTL/Z.
```

PESHAWAR-MLS(config)#interface fastEthernet 0/1

PESHAWAR-MLS(config-if)#switchport mode trunk

PESHAWAR-MLS(config-if)#exit

5.6.5 Dhcp configuration

Ip dhcp pool vlan50
Network 192.168.50.0 255.255.255.0
Default-router 192.168.50.100
Dns-server 8.8.8.8
Ip dhcp pool vlan60
Network 192.168.60.0 255.255.255.0
Default-router 192.168.60.100
Dns-server 8.8.8.8

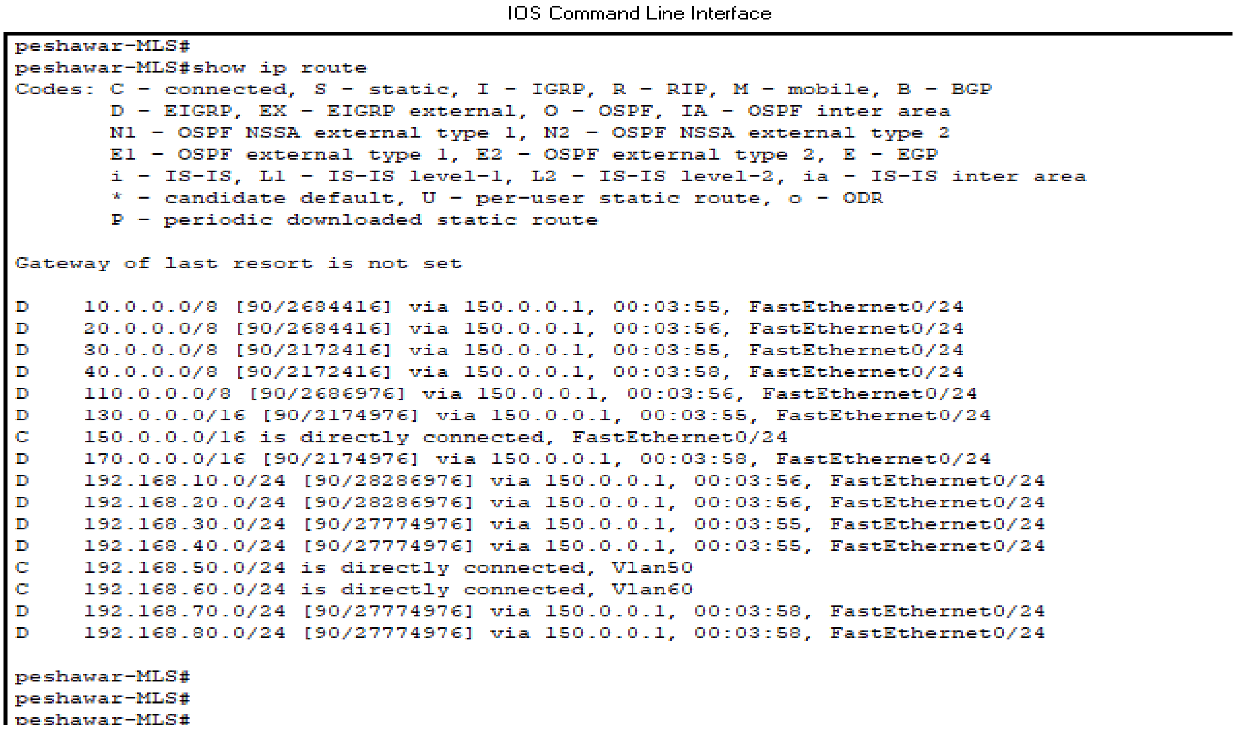
5.6.6 EIGRP configuration

Router eigrp 50

Network 150.0.0.0

Network 192.168.50.0

Network 192.168.60.0



```
peshawar-MLS#
peshawar-MLS#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    10.0.0.0/8 [90/2684416] via 150.0.0.1, 00:03:55, FastEthernet0/24
D    20.0.0.0/8 [90/2684416] via 150.0.0.1, 00:03:56, FastEthernet0/24
D    30.0.0.0/8 [90/2172416] via 150.0.0.1, 00:03:55, FastEthernet0/24
D    40.0.0.0/8 [90/2172416] via 150.0.0.1, 00:03:58, FastEthernet0/24
D    110.0.0.0/8 [90/2686976] via 150.0.0.1, 00:03:56, FastEthernet0/24
D    130.0.0.0/16 [90/2174976] via 150.0.0.1, 00:03:55, FastEthernet0/24
C    150.0.0.0/16 is directly connected, FastEthernet0/24
D    170.0.0.0/16 [90/2174976] via 150.0.0.1, 00:03:58, FastEthernet0/24
D    192.168.10.0/24 [90/2828976] via 150.0.0.1, 00:03:56, FastEthernet0/24
D    192.168.20.0/24 [90/2828976] via 150.0.0.1, 00:03:56, FastEthernet0/24
D    192.168.30.0/24 [90/2774976] via 150.0.0.1, 00:03:55, FastEthernet0/24
D    192.168.40.0/24 [90/2774976] via 150.0.0.1, 00:03:55, FastEthernet0/24
C    192.168.50.0/24 is directly connected, Vlan50
C    192.168.60.0/24 is directly connected, Vlan60
D    192.168.70.0/24 [90/2774976] via 150.0.0.1, 00:03:58, FastEthernet0/24
D    192.168.80.0/24 [90/2774976] via 150.0.0.1, 00:03:58, FastEthernet0/24

peshawar-MLS#
peshawar-MLS#
peshawar-MLS#
```

Figure 5.6 routing table Of PEW-MLS

5.7 Configuration of Lahore MLS switch

5.7.1 Hostname and password configuration

```
Lahore-MLS>

Lahore-MLS>enable

Lahore-MLS#config t

Enter configuration commands, one per line. End with CNTL/Z.

Lahore-MLS(config)#host

Lahore-MLS(config)#hostname lahore-MLS

lahore-MLS(config)#enable secret lhr12345

lahore-MLS(config)#exit

lahore-MLS#

%SYS-5-CONFIG_I: Configured from console by console
```

5.7.2 Interface configuration

```
Lahore-MLS#config t

Enter configuration commands, one per line. End with CNTL/Z.

Lahore-MLS (config-if)#interface fastethernet 0/24

Lahore-MLS (config-if)#ip address 130.0.0.2 255.255.0.0

Lahore-MLS (config-if)#no shutdown

Lahore-MLS (config-if)#

Lahore-MLS (config-if)#exit
```

5.7.3 SVI configuration

```
Lahore-MLS#config t

Enter configuration commands, one per line. End with CNTL/Z.

lahore-MLS(config)#interface vlan 30

lahore-MLS(config-if)#ip address 192.168.30.100 255.255.255.0

lahore-MLS(config-if)#no shutdown

lahore-MLS(config-if)#exit

lahore-MLS(config)#interface vlan 40

lahore-MLS(config-if)#ip address 192.168.40.100 255.255.255.0

lahore-MLS(config-if)#no shutdown

lahore-MLS(config-if)#exit
```

5.7.4 Trunk port configuration

lahore-MLS-Sw#config t

Enter configuration commands, one per line. End with CNTL/Z.

lahore-MLS(config)#interface fastEthernet 0/1

lahore-MLS(config-if)#switchport mode trunk

lahore-MLS(config-if)#exit

5.7.5 Dhcp configuration

Ip dhcp pool vlan30

Network 192.168.30.0 255.255.255.0

Default-router 192.168.30.100

Dns-server 8.8.8.8

Ip dhcp pool vlan40

Network 192.168.40.0 255.255.255.0

Default-router 192.168.40.100

Dns-server 8.8.8.8

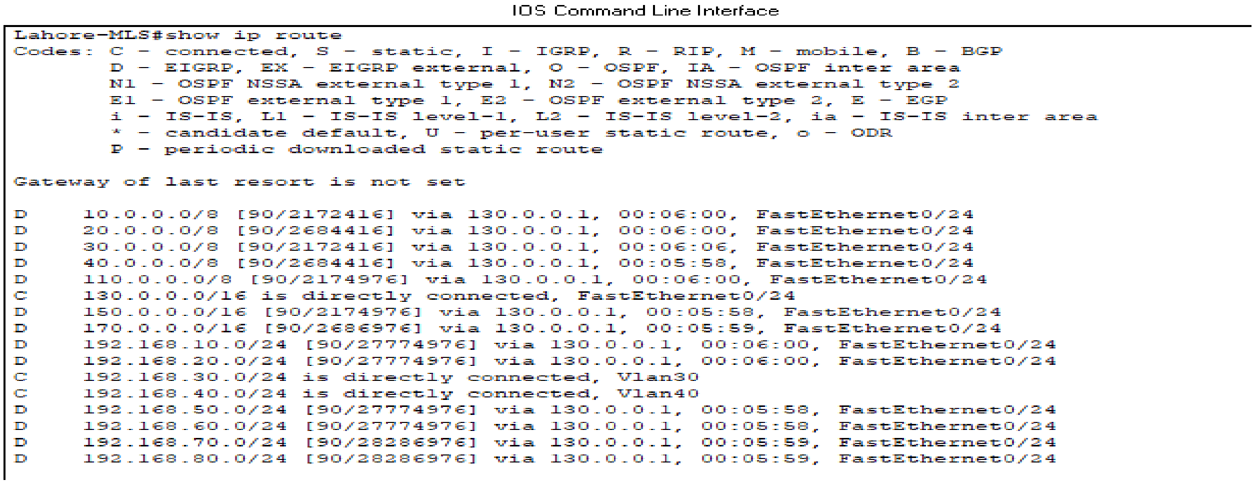
5.7.6 EIGRP configuration

Router eigrp 50

Network 130.0.0.0

Network 192.168.40.0

Network 192.168.30.0



```
Lahore-MLS#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    10.0.0.0/8 [90/2172416] via 130.0.0.1, 00:06:00, FastEthernet0/24
D    20.0.0.0/8 [90/2684416] via 130.0.0.1, 00:06:00, FastEthernet0/24
D    30.0.0.0/8 [90/2172416] via 130.0.0.1, 00:06:06, FastEthernet0/24
D    40.0.0.0/8 [90/2684416] via 130.0.0.1, 00:05:58, FastEthernet0/24
D    110.0.0.0/8 [90/2174976] via 130.0.0.1, 00:06:00, FastEthernet0/24
C    130.0.0.0/16 is directly connected, FastEthernet0/24
D    150.0.0.0/16 [90/2174976] via 130.0.0.1, 00:05:58, FastEthernet0/24
D    170.0.0.0/16 [90/2686976] via 130.0.0.1, 00:05:59, FastEthernet0/24
D    192.168.10.0/24 [90/27774976] via 130.0.0.1, 00:06:00, FastEthernet0/24
D    192.168.20.0/24 [90/27774976] via 130.0.0.1, 00:06:00, FastEthernet0/24
C    192.168.30.0/24 is directly connected, Vlan30
C    192.168.40.0/24 is directly connected, Vlan40
D    192.168.50.0/24 [90/27774976] via 130.0.0.1, 00:05:58, FastEthernet0/24
D    192.168.60.0/24 [90/27774976] via 130.0.0.1, 00:05:58, FastEthernet0/24
D    192.168.70.0/24 [90/28286976] via 130.0.0.1, 00:05:59, FastEthernet0/24
D    192.168.80.0/24 [90/28286976] via 130.0.0.1, 00:05:59, FastEthernet0/24
```

Figure 5.7 routing table Of LHR-MLS

5.8 Configuration of Karachi MLS switch

5.8.1 Hostname and password configuration

```
KARACHI-MLS>
KARACHI-MLS>enable
KARACHI-MLS#config t
Enter configuration commands, one per line. End with CNTL/Z.
KARACHI-MLS(config)#hostname Karachi-MLS
Karachi-MLS(config)#enable secret khi12345
Karachi-MLS(config)#exit
Karachi-MLS#
%SYS-5-CONFIG_I: Configured from console by console
```

5.8.2 Interface configuration

```
Karachi-MLS#config t
Enter configuration commands, one per line. End with CNTL/Z.
Karachi-MLS(config)#interface fastEthernet 0/24
Karachi-MLS(config-if)#ip address 110.0.0.2 255.0.0.0
Karachi-MLS(config-if)#no shutdown
Karachi-MLS(config-if)#exit
```

5.8.3 SVI configuration

```
Karachi-MLS#
Karachi-MLS#config t
Enter configuration commands, one per line. End with CNTL/Z.
Karachi-MLS(config)#interface vlan 10
Karachi-MLS(config-if)#ip address 192.168.10.100 255.255.255.0
Karachi-MLS(config-if)#no shutdown
Karachi-MLS(config-if)#
Karachi-MLS(config-if)#exit
Karachi-MLS(config)#
Karachi-MLS(config)#interface vlan 20
Karachi-MLS(config-if)#ip address 192.168.20.100 255.255.255.0
Karachi-MLS(config-if)#no shutdown
```

```
Karachi-MLS(config-if)#exit
Karachi-MLS(config)#
```

5.8.4 Trunk port configuration

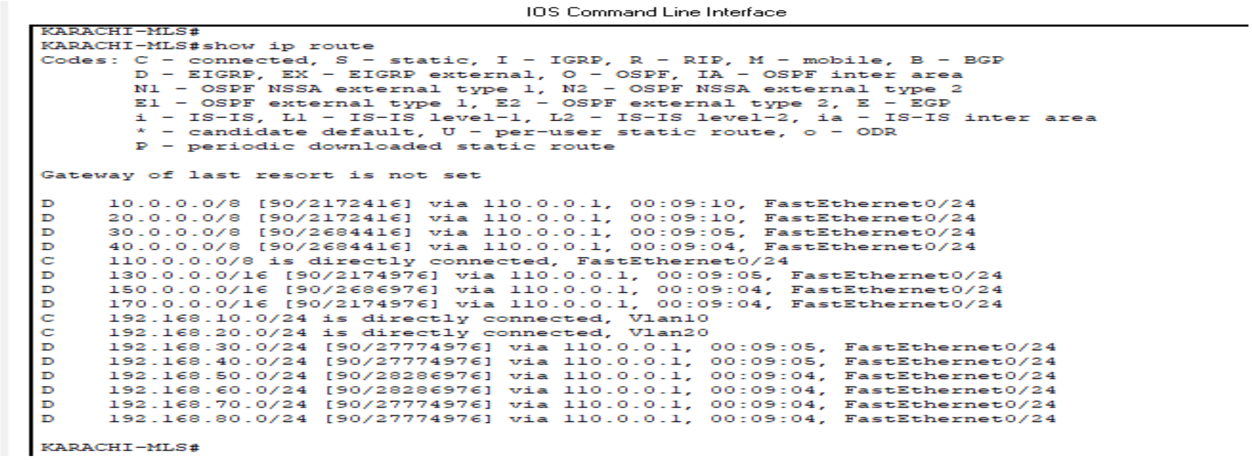
```
Karachi-MLS#config t
Enter configuration commands, one per line. End with CNTL/Z.
Karachi-MLS(config)#interface fastEthernet 0/1
Karachi-MLS(config-if)#switchport mode trunk
Karachi-MLS(config-if)#exit
```

5.7.5 Dhcp configuration

```
Ip dhcp pool vlan10
Network 192.168.10.0 255.255.255.0
Default-router 192.168.10.100
Dns-server 8.8.8.8
Ip dhcp pool vlan20
Network 192.168.20.0 255.255.255.0
Default-router 192.168.20.100
Dns-server 8.8.8.8
```

5.8.6 EIGRP configuration

```
Router eigrp 50
Network 110.0.0.0
Network 192.0.0.0
```



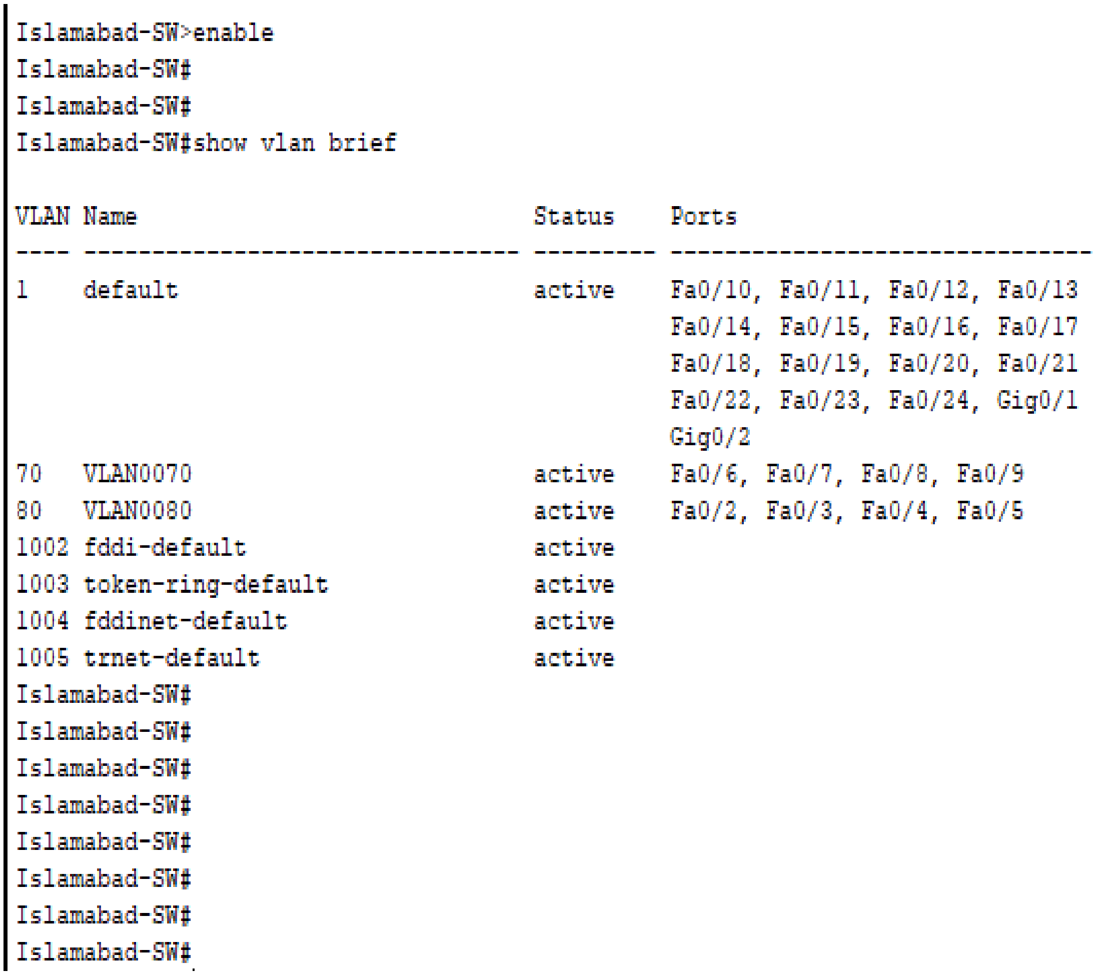
```
KARACHI-MLS#
KARACHI-MLS#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    10.0.0.0/8 [90/2172416] via 110.0.0.1, 00:09:10, FastEthernet0/24
D    20.0.0.0/8 [90/2172416] via 110.0.0.1, 00:09:10, FastEthernet0/24
D    30.0.0.0/8 [90/2684416] via 110.0.0.1, 00:09:05, FastEthernet0/24
D    40.0.0.0/8 [90/2684416] via 110.0.0.1, 00:09:04, FastEthernet0/24
C    110.0.0.0/8 is directly connected, FastEthernet0/24
D    130.0.0.0/16 [90/2174976] via 110.0.0.1, 00:09:05, FastEthernet0/24
D    150.0.0.0/16 [90/2686976] via 110.0.0.1, 00:09:04, FastEthernet0/24
D    170.0.0.0/16 [90/2174976] via 110.0.0.1, 00:09:04, FastEthernet0/24
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
D    192.168.30.0/24 [90/27774976] via 110.0.0.1, 00:09:05, FastEthernet0/24
D    192.168.40.0/24 [90/27774976] via 110.0.0.1, 00:09:05, FastEthernet0/24
D    192.168.50.0/24 [90/28286976] via 110.0.0.1, 00:09:04, FastEthernet0/24
D    192.168.60.0/24 [90/28286976] via 110.0.0.1, 00:09:04, FastEthernet0/24
D    192.168.70.0/24 [90/27774976] via 110.0.0.1, 00:09:04, FastEthernet0/24
D    192.168.80.0/24 [90/27774976] via 110.0.0.1, 00:09:04, FastEthernet0/24

KARACHI-MLS#
```

Figure 5.8 routing table Of KHI-MLS

5.9 Vlan and ports assessment on layer 2 switch

5.9.1 Islamabad switch

```
Islamabad-Sw#config t

Enter configuration commands, one per line. End with CNTL/Z.

Islamabad-SW(config)#

Islamabad-SW(config)#vlan 70

Islamabad-SW(config-vlan)#name

Islamabad-SW(config-vlan)#exit

Islamabad-SW(config)#

Islamabad-SW(config)#vlan 80

Islamabad-SW(config-vlan)#name

Islamabad-SW(config-vlan)#

Islamabad-SW(config-vlan)#exit
```

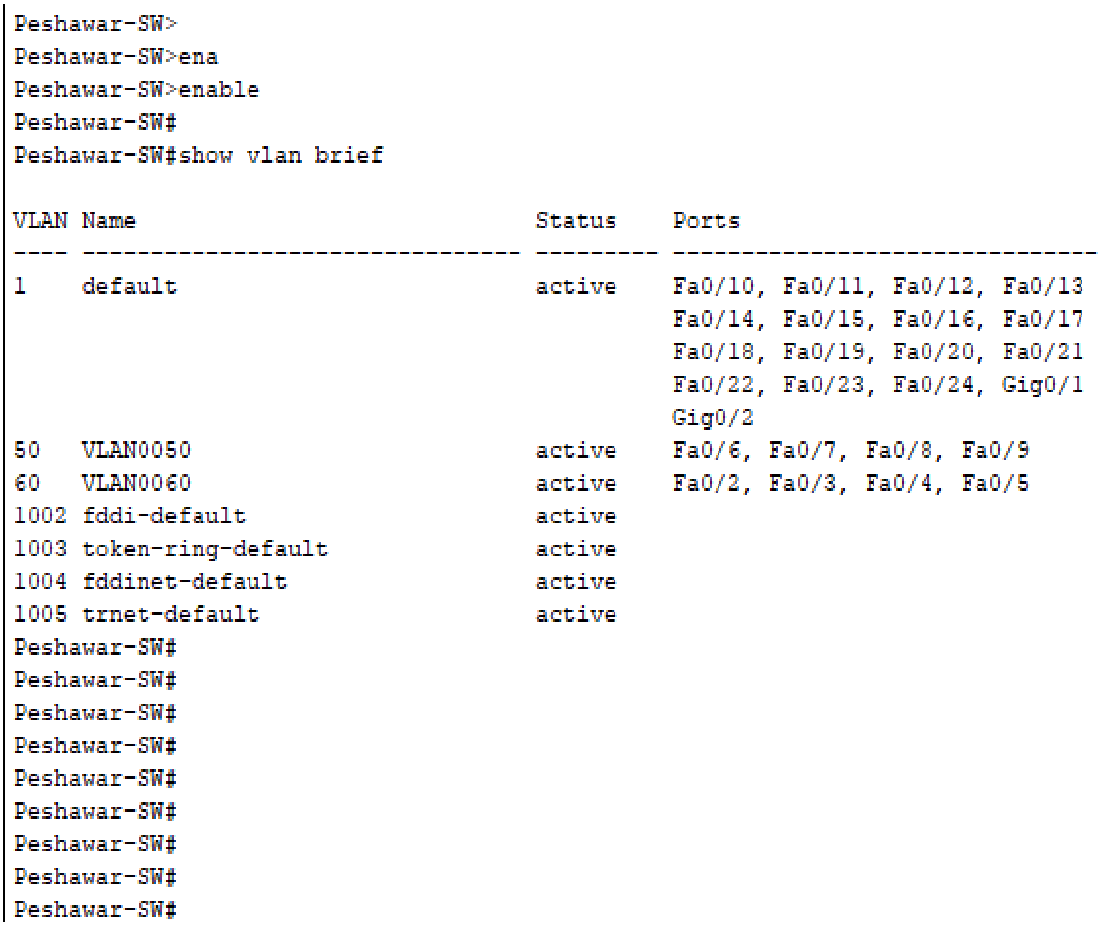


```
Islamabad-SW>enable
Islamabad-SW#
Islamabad-SW#
Islamabad-SW#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
70   VLAN0070                         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
80   VLAN0080                         active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Islamabad-SW#
Islamabad-SW#
Islamabad-SW#
Islamabad-SW#
Islamabad-SW#
Islamabad-SW#
Islamabad-SW#
Islamabad-SW#
```

Figure 5.9 vlan database of Islamabad switch

5.9.2 Peshawar switch

```
Peshawar-Sw#config t
Enter configuration commands, one per line. End with CNTL/Z.
Peshawar-SW(config)#
Peshawar-SW(config)#
Peshawar-SW(config)#vlan 50
Peshawar-SW(config-vlan)#name
Peshawar-SW(config-vlan)#exit
Peshawar-SW(config)#
Peshawar-SW(config)#vlan 60
Peshawar-SW(config-vlan)#name
Peshawar-SW(config-vlan)#
Peshawar-SW(config-vlan)#exit
```

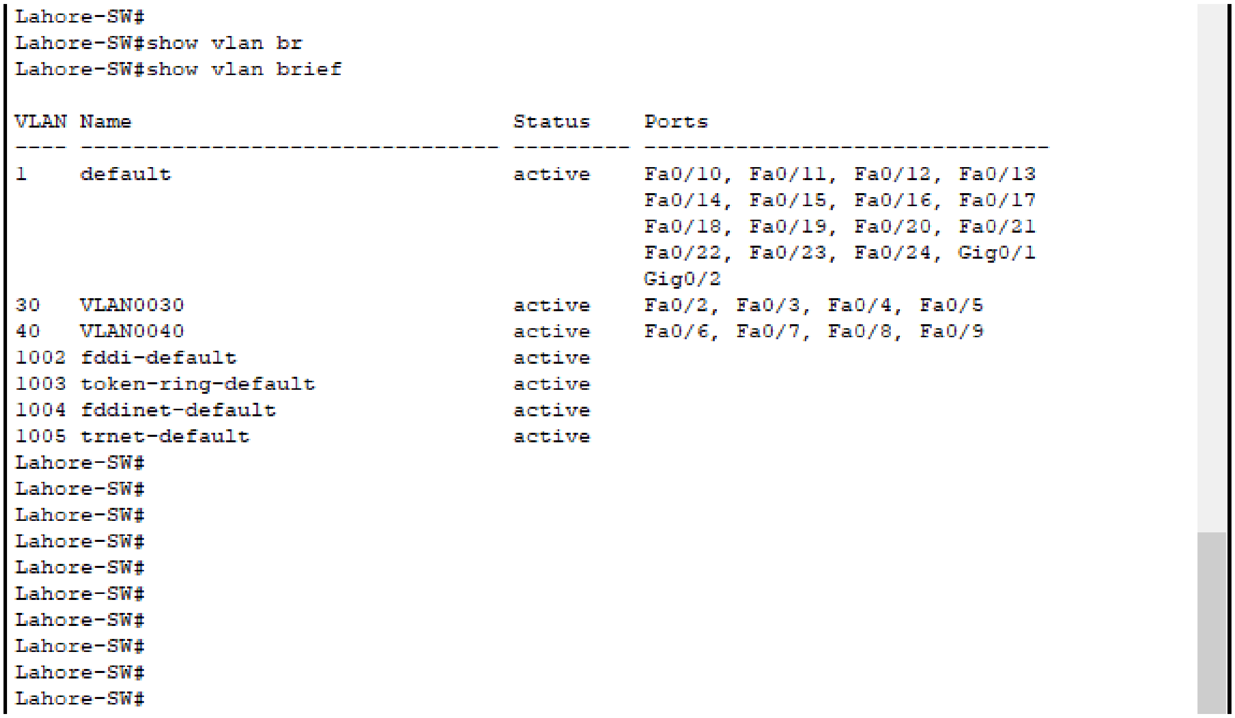


```
Peshawar-SW>
Peshawar-SW>ena
Peshawar-SW>enable
Peshawar-SW#
Peshawar-SW#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
50   VLAN0050                         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
60   VLAN0060                         active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
```

Figure 5.10 vlan database of Peshawar switch

5.9.3 Lahore switch

```
Lahore-Sw#config t

Enter configuration commands, one per line. End with CNTL/Z.

Lahore-SW(config)#

Lahore-SW(config)#vlan 30

Lahore-SW(config-vlan)#name

Lahore-SW(config-vlan)#

Lahore-SW(config-vlan)#exit

Lahore-SW(config)#

Lahore-SW(config)#vlan 40

Lahore-SW(config-vlan)#name

Lahore-SW(config-vlan)#

Lahore-SW(config-vlan)#exit

Lahore-SW(config)#
```

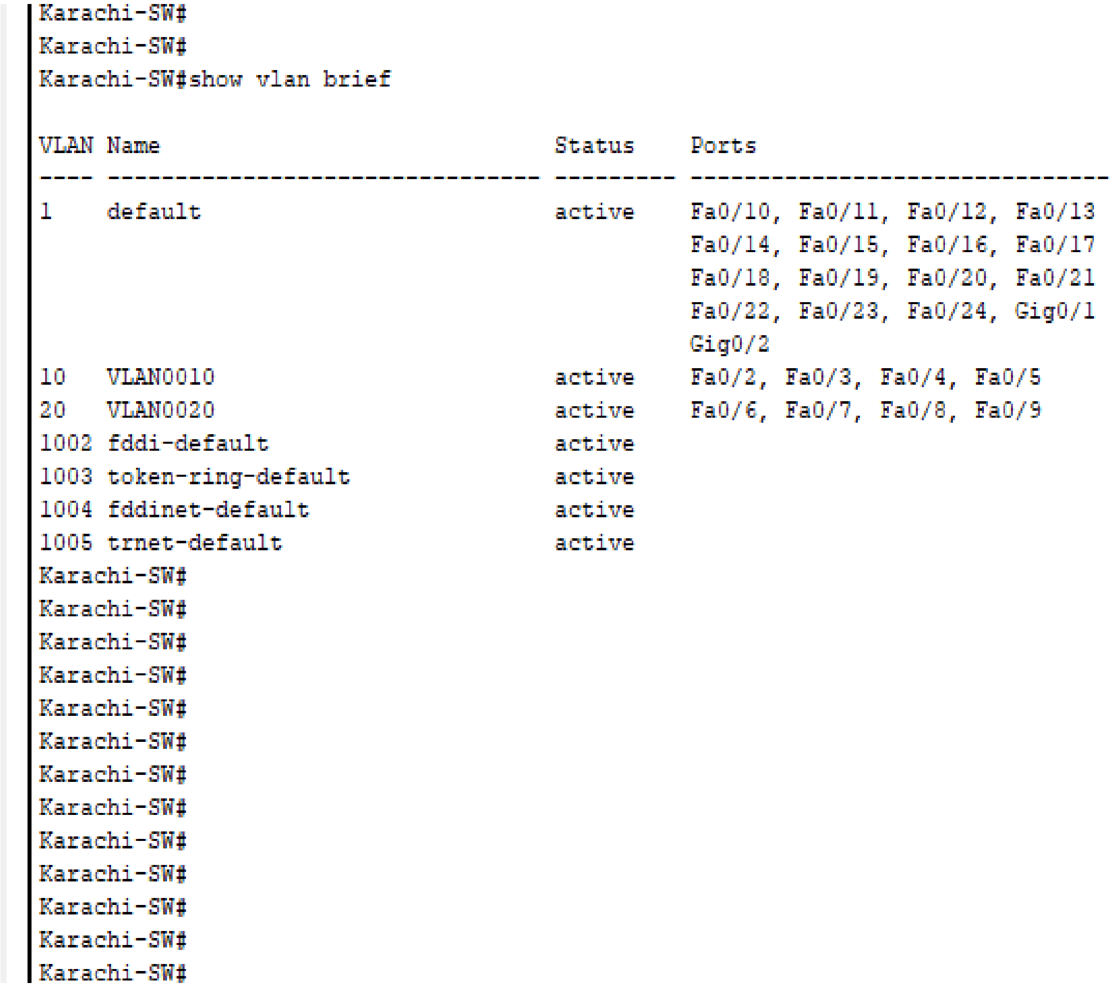


```
Lahore-SW#
Lahore-SW#show vlan br
Lahore-SW#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
30   VLAN0030                         active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
40   VLAN0040                         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
```

Figure 5.11 vlan database of Lahore switch

5.9.4 Karachi switch

```
Karachi-Sw#config t
Enter configuration commands, one per line. End with CNTL/Z.
Karachi-SW(config)#
Karachi-SW(config)#vlan 10
Karachi-SW(config-vlan)#name
Karachi-SW(config-vlan)#
Karachi-SW(config-vlan)#exit
Karachi-SW(config)#
Karachi-SW(config)#
Karachi-SW(config)#vlan 20
Karachi-SW(config-vlan)#
Karachi-SW(config-vlan)#name
Karachi-SW(config-vlan)#exit
```



```
Karachi-SW#
Karachi-SW#
Karachi-SW#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   VLAN0010                         active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
20   VLAN0020                         active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Karachi-SW#
Karachi-SW#
Karachi-SW#
Karachi-SW#
Karachi-SW#
Karachi-SW#
Karachi-SW#
Karachi-SW#
Karachi-SW#
Karachi-SW#
Karachi-SW#
Karachi-SW#
Karachi-SW#
```

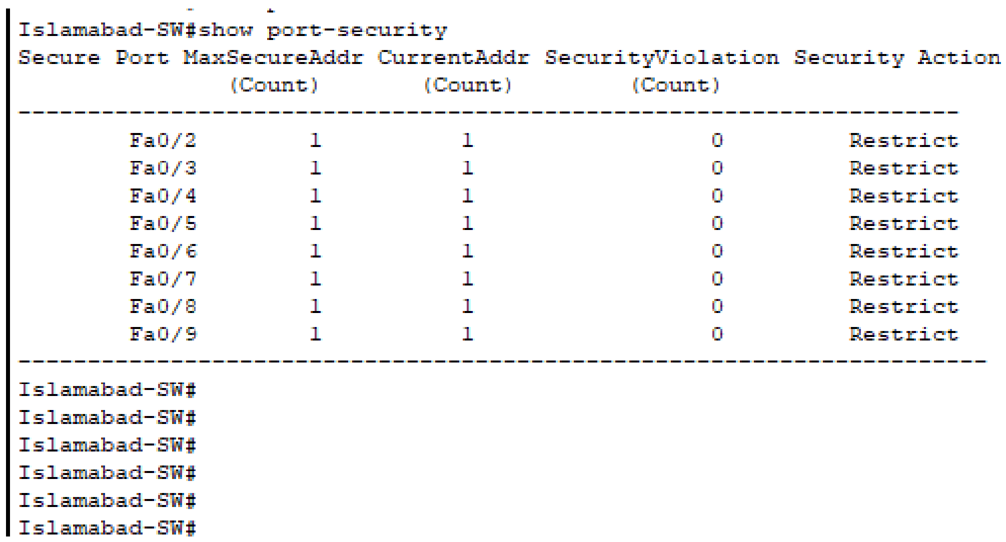
Figure 5.12 vlan database of Karachi switch

5.10 PORT SECURITY CONFIGURATION

5.10.1 PORT SECURITY CONFIGURATION ISLAMABAD SWITCH

```
Interface fastethernet0/2
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 000A.F3A6.A327
!
Interface fastethernet0/3
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0050.0F64.8A4A
!
Interface fastethernet0/4
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0060.47C7.165D
!
Interface fastethernet0/5
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0007.EC6E.9E41
!
```

```
Interface fastethernet0/6
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0060.3E12.8417
!
Interface fastethernet0/7
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 00D0.D335.B6D4
!
Interface fastethernet0/8
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 000A.418B.C14A
!
Interface fastethernet0/9
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 00D0.BC2E.A59D
```



```
Islamabad-SW#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/2        1           1                 0         Restrict
        Fa0/3        1           1                 0         Restrict
        Fa0/4        1           1                 0         Restrict
        Fa0/5        1           1                 0         Restrict
        Fa0/6        1           1                 0         Restrict
        Fa0/7        1           1                 0         Restrict
        Fa0/8        1           1                 0         Restrict
        Fa0/9        1           1                 0         Restrict
----------------------------------------------------------------------
Islamabad-SW#
Islamabad-SW#
Islamabad-SW#
Islamabad-SW#
Islamabad-SW#
Islamabad-SW#
```

Figure 5.13 port security database of Islamabad switch

5.10.2 Port security configuration Peshawar switch

```
Interface fastethernet0/2
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0090.215B.D4D0
!
Interface fastethernet0/3
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 00E0.8FD4.2361
!
Interface fastethernet0/4
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0030.A318.808B
!
Interface fastethernet0/5
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0001.63BE.9811
!
Interface fastethernet0/6
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0060.5CD2.A8A8
!
Interface fastethernet0/7
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 00D0.D39A.AB19
!
Interface fastethernet0/8
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0004.9A5A.8202
!
```

Interface fastethernet0/9

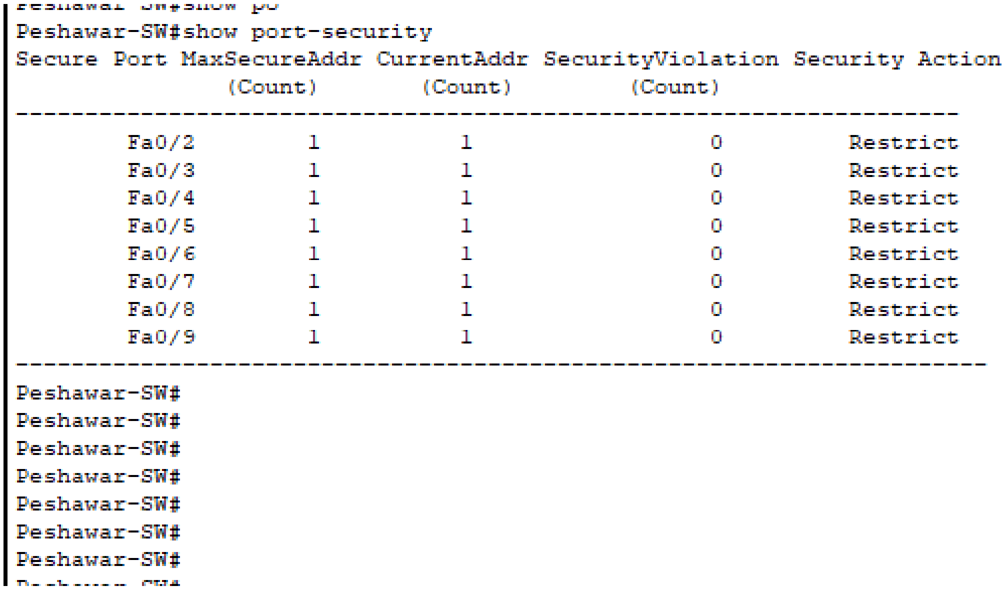
Switchport mode access

Switchport port-security

Switchport port-security mac-address sticky

Switchport port-security violation restrict

Switchport port-security mac-address sticky 0030.A38C.51E2



```
Peshawar-SW#show po
Peshawar-SW#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/2        1           1                 0         Restrict
        Fa0/3        1           1                 0         Restrict
        Fa0/4        1           1                 0         Restrict
        Fa0/5        1           1                 0         Restrict
        Fa0/6        1           1                 0         Restrict
        Fa0/7        1           1                 0         Restrict
        Fa0/8        1           1                 0         Restrict
        Fa0/9        1           1                 0         Restrict
----------------------------------------------------------------------
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
Peshawar-SW#
```

Figure 5.14 port security database of Peshawar switch

5.10.3 Port security configuration Lahore switch

Interface fastethernet0/2

Switchport mode access

Switchport port-security

Switchport port-security mac-address sticky

Switchport port-security violation restrict

Switchport port-security mac-address sticky 0090.2138.0C75

!

Interface fastethernet0/3

Switchport mode access

Switchport port-security

Switchport port-security mac-address sticky

Switchport port-security violation restrict

```
Switchport port-security mac-address sticky 00D0.BC49.2E5C
!
Interface fastethernet0/4
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0060.2FA4.734D
!
Interface fastethernet0/5
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0060.2FC1.9D46
!
Interface fastethernet0/6
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 00D0.D34D.3EEB
!
Interface fastethernet0/7
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0001.C737.ACAE
!
Interface fastethernet0/8
```

Switchport mode access

Switchport port-security

Switchport port-security mac-address sticky

Switchport port-security violation restrict

Switchport port-security mac-address sticky 0006.2A52.7E68

!

Interface fastethernet0/9

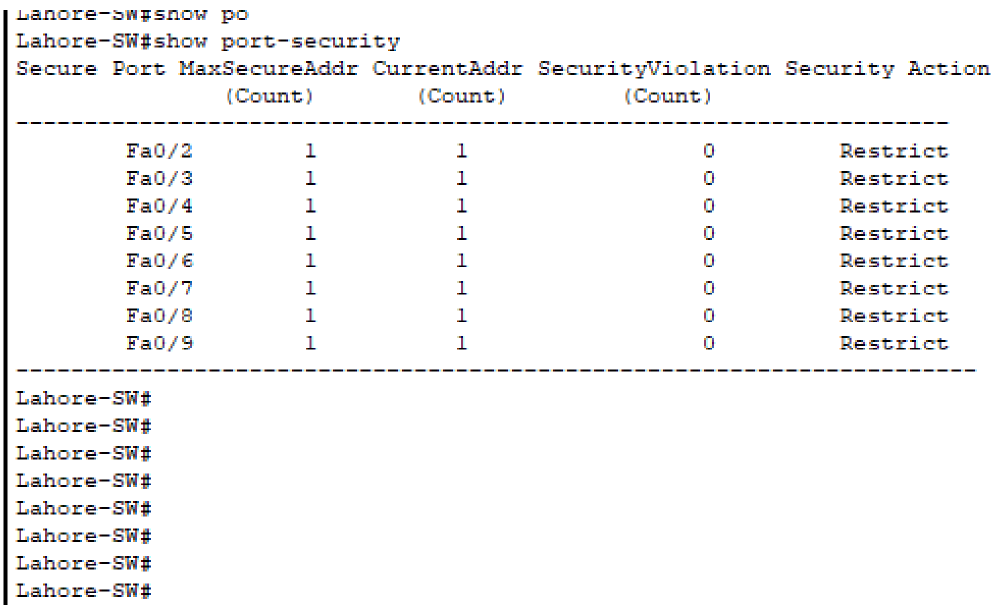
Switchport mode access

Switchport port-security

Switchport port-security mac-address sticky

Switchport port-security violation restrict

Switchport port-security mac-address sticky 000C.85AE.A45E



```
Lahore-SW#show po
Lahore-SW#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/2        1           1                 0          Restrict
        Fa0/3        1           1                 0          Restrict
        Fa0/4        1           1                 0          Restrict
        Fa0/5        1           1                 0          Restrict
        Fa0/6        1           1                 0          Restrict
        Fa0/7        1           1                 0          Restrict
        Fa0/8        1           1                 0          Restrict
        Fa0/9        1           1                 0          Restrict
----------------------------------------------------------------------
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
Lahore-SW#
```

Figure 5.15 port security database of Lahore switch

5.10.4 PORT SECURITY CONFIGURATION KARACHI SWITCH

Interface FastEthernet0/2

Switchport mode access

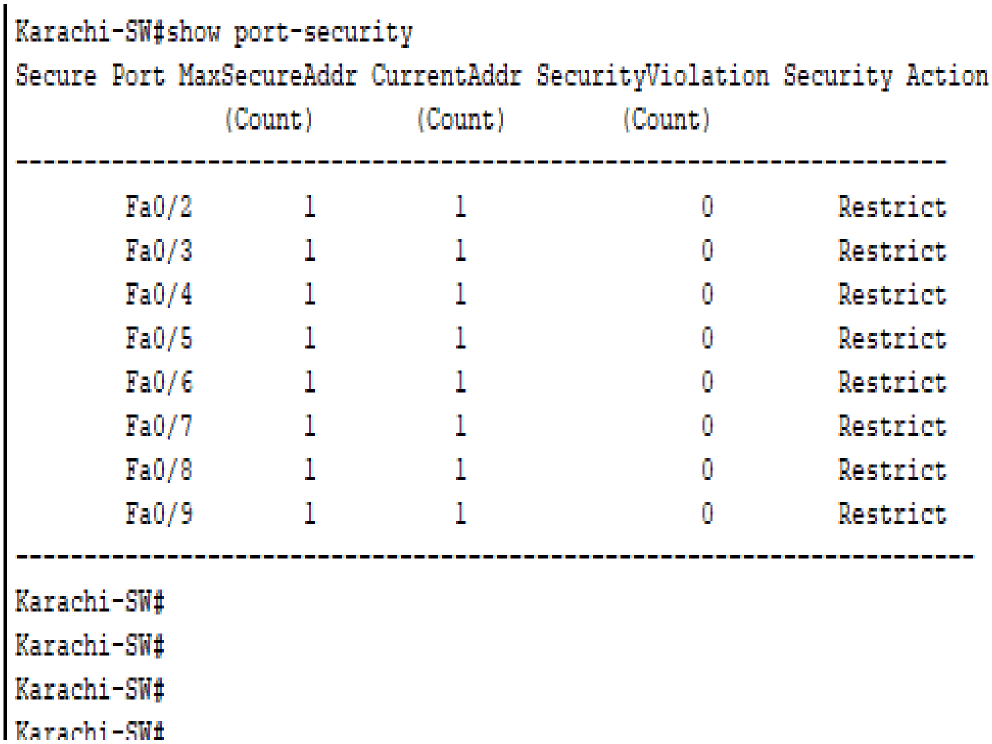
Switchport port-security

Switchport port-security mac-address sticky

Switchport port-security violation restrict

```
Switchport port-security mac-address sticky 0090.0CA1.A607
!
Interface fastethernet0/3
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0010.11DC.8107
!
Interface fastethernet0/4
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0001.4347.9C34
!
Interface fastethernet0/5
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0004.9A33.EB0C
!
Interface fastethernet0/6
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0002.4A04.AB08
!
Interface fastethernet0/7
```

```
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0002.4AD6.CC66
!
Interface fastethernet0/8
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0009.7C86.BC94
!
Interface fastethernet0/9
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security violation restrict
Switchport port-security mac-address sticky 0006.2A60.5A9C
```



```
Karachi-SW#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/2        1          1                 0         Restrict
        Fa0/3        1          1                 0         Restrict
        Fa0/4        1          1                 0         Restrict
        Fa0/5        1          1                 0         Restrict
        Fa0/6        1          1                 0         Restrict
        Fa0/7        1          1                 0         Restrict
        Fa0/8        1          1                 0         Restrict
        Fa0/9        1          1                 0         Restrict
----------------------------------------------------------------------
Karachi-SW#
Karachi-SW#
Karachi-SW#
Karachi-SW#
```

Figure 5.16 port security database of Karachi switch

CHAPTER 6

Discussion and Conclusion

6.1 Discussion and Conclusion

After all the configuration and information, we got the following achievements

- We understood what dynamic routing protocol are, how the routers route the IP Addresses, and how to configure EIGRP into router.
- What is an IP Address,
- How securities are provided to the router and switches like port security provided by the switches and authentication of router too.
- We are quite familiar with router and all the routing protocol that are Interior Gateway Protocols (IGP). Despite of this, we also learn how to configure a router, and maintain it and also DHCP protocols and how they are implemented.

6.2 Conclusion

Overall the report the conclusion of EIGRP is, this is hybrid routing protocol (distance vector that has link-state protocol characteristics) is very useful and better routing protocol. It is Faster and smarter that other routing protocol. Classless protocol (supports VLSMS). Default com- posite metric applies bandwidth and delay. We can factor load and de pend ability into the metric sends partial route updates only when there are changes. Support for authentication. Uses DUAL for loop prevention. By default, equal-cost load balancing. Unequal-cost charge equilibrating with the variability command Administrative length is 90 for EIGRP inner routes, 170 for EIGRP external routes, and 5 for EIGRP summary routes. Possible routing protocol for the burden of a network, applied in big networks. Cables that are used in the project are packet tracer based in reality it may be different like now a day, Optical fiber cables are mostly used in networking, due to higher bandwidth and faster speed.

References

1. https://searchnetworking.techtarget.com/definition/EIGRP
2. https://www.geeksforgeeks.org/features-of-enhanced-interior-gateway-routing-protocol-eigrp/
3. https://www.sciencedirect.com/topics/computer-science/topology-table
4. https://en.wikipedia.org/wiki/IPv4
5. https://www.computernetworkingnotes.com/ccna-study-guide/eigrp-configuration-step-by-step-guide.html
6. https://en.wikipedia.org/wiki/Packet_Tracer
7. https://networklessons.com/switching/intervlan-routing
8. https://searchnetworking.techtarget.com/definition/virtual-LAN
9. https://www.comptia.org/content/guides/what-is-a-wide-area-network
10. https://www.networkworld.com/article/2297171/network-security-mpls-explained.html
11. https://www.networkworld.com/article/3299438/dhcp-defined-and-how-it-works.html
12. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/44sg/configuration/guide/Wrapper-44SG/port_sec.pdf