PRACTICAL NO. 1 (A)

The OSPF MD5 authentication is more secure than the plain text authentication. This method uses the MD5 algorithm to compute a hash value from the contents of the OSPF packet and a password. This hash value is transmitted in the packet. The receiver, which knows the same password, calculates its own hash value. If the message is unchanged, the hash value of the receiver should match the hash value of the sender which is transmitted with the message.
Configuring OSPF MD5 authentication is very similar to configuring clear-text authentication. Two commands are required:

- Configure the MD5 value on an interface using the ip ospf message-digest-key 1 md5 VALUE interface command.

- To configure the interface to use MD5 authentication by using the ip ospf authentication message-digest interface command.

PRACTICAL NO. 1 (B)

NTP stands for Network Time Protocol, and it is an Internet protocol used to synchronize the clocks of computers to sometime reference.
There exist several protocols to synchronize computer clocks, each having distinguished features. Here is a list of NTP's features:

- NTP needs some reference clock that defines the true time to operate. All clocks are set towards that true time.
- NTP uses UTC as reference time.
- NTP is a fault-tolerant protocol that will automatically select the best of several available time sources to synchronize to.
- NTP is highly scalable: A synchronization network may consist of several reference clocks. Each node of such a network can exchange time information either bidirectional or unidirectional.
- Even when a network connection is temporarily unavailable, NTP can use measurements from the past to estimate current time and error.
- For formal reasons NTP will also maintain estimates for the accuracy of the local time.

PRACTICAL NO. 1 (C)

System Logging Protocol (Syslog) is a way network devices can use a standard message format to communicate with a logging server. It was designed specifically to make it easy to monitor network devices. Devices can use a Syslog agent to send out notification messages under a wide range of specific conditions.

A big advantage of syslog is that the log server can monitor a vast number of syslog events via log files. Routers, switches, firewalls, and servers can generate log messages, as well as many printers and other devices.

The syslog server receives, categorizes, and stores log messages for analysis, maintaining a comprehensive view of what is going on everywhere on the network. Without this view, devices can malfunction unexpectedly, and outages can be hard to trace.

PRACTICAL NO. 1 (D)

Secure Shell, just like Telnet, enables a user to access a remote device and manage it remotely. However, with SSH, all data transmitted over a network (including usernames and passwords) is encrypted and secure from eavesdropping.

SSH is a client-server protocol, with a SSH client and a SSH server. The client machine (such as a PC) establishes a connection to a SSH server running on a remote device (such as a router). Once the connection has been established, a network admin can execute commands on the remote device.

Configuring SSH requires commands such as:

- **"line vty 0 4" :** this command will set only line 0 to 4 Virtual Teminal Lines can access SSH.

- **"crypto key generate rsa"** : command, when ask you "How many bits in the modulus [512]:" just type "1024″ and press enter. The system will generate 1024 bits keys to secure session lines. You can choose modulus in the range of 360 to 2048.

PRACTICAL NO. 2 (A)

The authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you can set up access control on your router or access server. Authentication is a way of identifying a user before permitting access to the network and network services.

Configuring AAA Authentication for Console Lines requires commands such as:

- **aaa new-model :** Enables authentication, authorization, and accounting (AAA) globally.

- **aaa authentication login default local :** Creates the default local authentication list.

- **line [aux | console | tty | vty] line-number [ending-line-number] :** Enters line configuration mode for the lines to which you want to apply the authentication list.

- **login authentication default :** Applies the authentication list to a line or set of lines.

PRACTICAL NO. 2 (B)

IOS supports the Authentication, Authorization, and Accounting (AAA) model, using the RADIUS or TACACS+ protocols to centralize these functions on dedicated AAA servers. The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service. RADIUS is a distributed client/server system that secures networks against unauthorized access.

All users logging into the router must authenticate with a username and password to one of two redundant TACACS+ servers. Users must be able to log in using a backup local user account stored on the router only if neither TACACS+ server is reachable.

PRACTICAL NO. 3

Access control lists (ACLs) perform packet filtering to control the movement of packets through a network. Packet filtering provides security by limiting the access of traffic into a network, restricting user and device access to a network, and preventing traffic from leaving a network. IP access lists reduce the chance of spoofing and denial-of-service attacks, and allow dynamic, temporary user-access through a firewall.

An Extended IP ACL can filter a packet based on its source and destination IP address, protocol information, port number, message type for ICMP and TCP/IP protocol such as FTP, HTTP, SSH, Telnet etc.

- To create an Extended numbered ACL following global configuration mode command is used:-

1. **Router(config)#** : This command prompt indicates that we are in global configuration mode.

2. **access-list** : Through this parameter we tell router that we are creating or accessing an access list.

3. **ACL_Identifier_number** : With this parameter we specify the type of access list. We have two types of access list; standard and extended. Both lists have their own unique identifier numbers. Extended ACL uses numbers range 100 to 199. We can pick any number from this range to tell the router that we are working with Extended ACL. This number is used in groping the conditions under a single ACL. This number is also a unique identifier for this ACL in router.

4. **permit/deny** : As we know an ACL condition has two actions; permit and deny. If we use **permit** keyword, ACL will allow all packets that match with parameters specified next in command. If we use **deny** keyword, ACL will drop all packets which match with following specified parameters.

5. **IP_protocol** : This parameter tells router that what kind of filtering we want. We have two choices here, host level filtering and application level filtering. Host level filtering is used for generic filtering while application level filtering is used for more specific filtering. In easy language Host level filtering checks "Whether host A is allowed to access host B or not" while application level filtering checks "**How much host A is allowed to access host B**".

PRACTICAL NO. 5

You can filter IP Version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create and apply IP Version 4 (IPv4) named ACLs.

Filter ID IPv6 ACL

For the filter-Id ACL, the full ACEs and the acl name(filter-id) is configured on the switch and only the filter-id is configured on the ACS. The filter-id is sent to the switch in the ACCESS-Accept attribute, and the switch looks up the filter-id for the ACEs, and then applies the ACEs to the client. The foreign switch has to configure the filter-id and ACEs beforehand.

Configuring IPv6 ACLs:-

To filter IPv6 traffic, you perform these steps:-

1. Create an IPv6 ACL, and enter IPv6 access list configuration mode.
2. Configure the IPv6 ACL to block (deny) or pass (permit) traffic.
3. Apply the IPv6 ACL to the interface where the traffic needs to be filtered.
4. Apply the IPv6 ACL to an interface.

PRACTICAL NO. 6

Zone-based firewall is an advanced method of stateful firewall. In stateful firewall, an entry containing source IP address, destination IP address, source Port number and destination Port number, is maintained for the traffic generated by the trusted (private) network in the stateful database. This will only the traffic including the replies for the private (trusted) network using the stateful database.

Zone-based Firewall procedure:

1. **Create zones and assign an interface to it –** In Zone-based firewall, logical zones are created. A zone is assigned to an interface. By default, traffic from one zone to another is not allowed.

2. **Create class-map –** After creating a zone, a class-map policy is made which will identify the type of traffic, like ICMP, on which the policies will be applied.

3. **Create policy-map and assign class-map to the policy-map –** After identifying the type of traffic in class-map, we have to define what action must be taken on the traffic. The action can be:
   - **Inspect:** It is same as inspection of CBAC i.e only that traffic will be allowed from the outside network which will be inspected (return traffic of inside (trusted) network.
   - **Drop:** This is the default action for all traffic. The class-map configured in a policy map can be configured to drop unwanted traffic.
   - **Pass:** This will allow the traffic from one zone to another. Unlike inspect action, it will not create a session state for a traffic. If we want to allow traffic from the opposite direction, corresponding policy should be created.

4. **Configure a zone-pair and assign the policy –** A zone-pair is configured for one direction only. Policies are defined in which traffic is identified (what type of traffic) then what action should be taken (Inspect Denied, permit). Then we have to apply these policies to a zone-pair.

PRACTICAL NO. 9

Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g offices or branches). The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.

The network topology shows three routers. Your task is to configure R1 and R3 to support a site-to-site IPsec VPN when traffic flows between their respective LANs. The IPsec VPN tunnel is from R1 to R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks, such as the Internet. IPsec operates at the network layer and protects and authenticates IP packets between participating IPsec devices.

PRACTICAL NO. 10

The Cisco Adaptive Security Appliance (ASA) is an advanced network security device that integrates a stateful firewall, VPN, and other capabilities. This lab employs an ASA 5505 to create a firewall and protect an internal corporate network from external intruders while allowing internal host's access to the Internet. The ASA creates three security interfaces: Outside, Inside, and DMZ. It provides outside users limited access to the DMZ and no access to inside resources. Inside users can access the DMZ and outside resources.

This lab's focus is the configuration of the ASA as a basic firewall. Other devices will receive minimal configuration to support the ASA portion of this lab. This lab uses the ASA CLI, which is similar to the IOS CLI, to configure basic device and security settings.