**Lesson Proper for Week 10**

**IMPLEMENTING AUTHENTICATION USING EXTERNAL SERVICES**

Due to the scaling of large networks, creating a user account on each router can be an inconvenience. If the account's details are adjusted on one device, the network engineer will need to replicate the changes to all other devices on the network individually. A convenient solution to adjust scaling and ensuring that all of the accounts and privileges are kept synchronized is to use a centralized AAA server such as a Cisco **Access Control Server (ACS)** or a Cisco **Identity Services Engine (ISE**):

The user accounts are created on the ACS or ISE appliance. The routers and switches are configured to query the AAA server if they receive any login requests. The AAA server would also be responsible for providing privileges and getting logs of the activities of each user.

Examples of these security protocols are as follows:

·         RADIUS

·        TACACS+

**TACACS+**

This is a Cisco proprietary third-generation protocol that facilitates the use of AAA services. This protocol is derived from TACACS and XTACACS, and supports authentication, authorization, and accounting. Multiple servers can be used to handle different services. For example, one server can be used to handle authentication and another server can be used to handle authorization for a router.

TACACS+ provides additional layers of security by encrypting the messages between the client and the AAA server.

Here are the some of the special features of TACACS+:

·         TACACS+ supports authorization commands with some advanced authentication mechanisms like Data Encryption Standard and one-time password (OTP) keys

·         TACACS+ supports all 16 privilege levels (0-15)

·         TACACS+ allows the blocking of specific port services such as a TTY or VTY

·         The TACACS+ AAA server can contain an internal database size up to 5,000 users

·        A TACACS+ server acts as a proxy server which authenticates, authorizes, and accounts access details

**CONFIGURING TACACS+**

**USING AAA WITH TACACS+**

Let's consider the example of a user connected to the router, and the TACACS+ server is requesting access to the router. The following are the steps involved in authenticating the user with TACACS+:

1. The **Client**sends a request message to the **Router**

2. The **Router** passes the request to the **TACACS+ Server** and requests for the login text

3. The **TACACS+ Server** prompts for the username and the password, and the**Router** passes the server request to the server

4. The**Client** sends the username and password to the router and the **Router** forwards the same to TACACS+

5. Then, the server replies with an ACCEPT or REJECT code

**RADIUS**

This is an open standard protocol that works in a client and server model. In the implementation of Cisco, the RADIUS client is configured on the Cisco routers and sends authentication or authorization requests to a RADIUS server which is located centrally.

RADIUS can be implemented in various network environments that are in need of high security levels. Some of the environments where RADIUS can be used are as follows:

1. It can be implemented in networks that are built with different vendor products. RADIUS can act as a single server-based database.

2. In networks environments where smart cards are used.

3. It can be used in environments where administrators need to do accounting independently.

4. It can be used in networks where administrators want to set up pre-authentication profiles. Pre-authentication mainly helps ISP's to manage ports and shared resources depending on the agreed upon service agreements.

On the other hand, RADIUS cannot be used for some situations, and they are as follows:

1. RADIUS does not support some of the protocols like AppleTalk Remote Access (ARA), X.25 PAD connections, and NetBIOS

2. RADIUS does not work on the two-way authentication model

3. RADIUS binds the user client to only one service model and does not support a variety of services

**CONFIGURING RADIUS**