**AAA (Authentication, Authorization, and Accounting) Lab Day 8&9**

Objective:

The aim of this lab is to implement and configure AAA (Authentication, Authorization, and Accounting) services using both local and centralised methods. The focus of the lab is on how to secure network devices by way of configuring AAA on routers and employing TACACS+ in addition to RADIUS protocols.

Introduction:

It is through AAA services that user access can be managed, as well as ensuring network security. This means that administrators have the ability to authenticate users who would like to pass through the portal. To go further these officials can also authorize such individuals’ access to specific resources they need at any time. This laboratory exercise will provide an opportunity for students to gain hands-on experience with centralized as well as some local AAA configurations which will help them understand just where these two methods work best or not?

Materials and Tools:

GNS3 (Graphical Network Simulator)

Cisco Router (R1)

Generic PC nodes

AAA Server (e.g., TACACS+ and RADIUS)

Kali Linux (for testing & verification) Centralized AAA Implementation:

Introduction to Centralized AAA:

Understand when distributed authentication fails in larger networks.

Setting Up TACACS+ or RADIUS Server:

Add the TACACS+ and RADIUS appliance for GNS3 by downloading its Docker image.

Configure a unique IP address for your AAA server plus set up proper authentication protocols.

Configuring AAA on Router (R1):

Enabling AAA on router: aaa new-model

Router Configuration

Test the configuration by attempting to log in using the credentials stored on the AAA server.

**Verification and Testing:**

Use various show commands on R1 to verify the configuration:

**show privilege**

**show user**

**show logging**

Attempt login attempts from both local and remote (AAA server) configurations and observe the differences.

Observations:

**Local AAA:** Easy to configure but lacks scalability. User credentials and access policies need to be managed on each device, which can become cumbersome in larger networks.

**Centralized AAA:** Provides centralized management, making it easier to enforce consistent access control policies across the network. The use of TACACS+ and RADIUS enhances security but requires additional setup and resources.

**Conclusion**:

On our lab day 8 &9 we tried to demonstrate the implementation of AAA in a network environment, highlighting the differences between local and centralized approaches. While local AAA is suitable for smaller networks, centralized AAA is more efficient and secure for larger deployments. The use of TACACS+ and RADIUS protocols provides enhanced security and manageability, making it the preferred choice for enterprise networks.