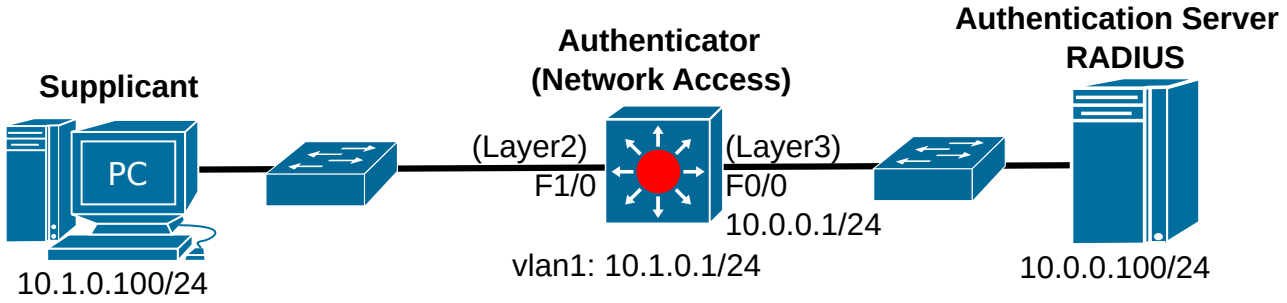
SEGURANÇA EM REDES DE COMUNICAÇÕES

LAYER 2 ACCESS CONTROL

802.1X & RADIUS

1. Start a Virtual Machine with a Linux Server, connect it to the Internet and install the RADIUS server (freeradius): `sudo apt-get install freeradius`.
Verify the status of the RADIUS service with: `systemctl status freeradius`
To start and stop the RADIUS service use: `sudo systemctl stop freeradius` and `sudo systemctl start freeradius`

2. Set up a network in GNS3 with a client PC (Linux VM), a Layer3 switch, and an authentication RADIUS server (VM Linux). The client PC will be the an AAA supplicant and the Layer3 switch will be the AAA network authenticator. The PC is connected to a Layer2 port (VLAN 1) on the Layer3 Switch and the Layer3 Switch connects to the RADIUS server using a Layer3 port. Test the connectivity between all network devices.



3. Configure the RADIUS service: edit the file /etc/freeradius/3.0/clients.conf and add the access credentials for the Authenticator/Layer3 switch (10.0.0.1):

```
client 10.0.0.1 {
        secret  = radiuskey
}
```

Define the user/supplicant credentials by editing the file /etc/freeradius/3.0/users and adding the line

```
"labredes"      Cleartext-Password := "labcom"
```

Note: confirm that this is not the last line of the configuration file.
Restart and check the status of the radius server.

4. Configure the Authenticator by enabling 802.1X in Layer2 ports using the RADIUS server:

```
ESW1(config)# aaa new-model
ESW1(config)# aaa authentication dot1x default group radius
ESW1(config)# dot1x system-auth-control
ESW1(config)# radius-server host 10.0.0.100 auth-port 1812 key radiuskey
ESW1(config)# interface FastEthernet1/0
ESW1(config-if)# dot1x port-control auto
```

Use the command `show dot1x` to verify the status of 802.1X authentication.
Start a packet capture between the PC and Layer3 switch. Test the connectivity between the PC and Layer3 switch.
>> What can you conclude?

5. Disable the PC's Ethernet interface, configure the 802.1X authentication (using the respective network manager) with the credentials labredes/labcom. Start one packet capture between the Layer3 switch and RADIUS server, and another between the PC and layer3 switch. Re-enable the PC's Ethernet interface. Test the connectivity between the PC and Layer3 switch. Re-verify the status of 802.1X authentication at the Layer3 switch.
>> Analyze and explain the purpose of the EAP and TLSv1 packets exchanged between the PC and Layer3 switch.
>> Analyze and explain the purpose and content of the RADIUS packets exchanged between the Layer3 switch and the RADIUS server.

6. Activate the RADIUS log functionality to include the logging of authentication requests. Edit the file /etc/freeradius/3.0/radiusd.conf and change the following value inside the log section:

```
auth = yes
```

Restart the RADIUS server: `sudo systemctl restart freeradius`. Test multiple accesses with correct and wrong usernames and passwords (disable and enable the network interface upon the changes).

>> Analyze the latest RADIUS log file in /var/log/freeradius and identify the successful and unsuccessful authentication (Auth) entries.

>> How, in a centralized manner, detect failed access attempts and identifying the switch/port were it occurred?

Note: if the authentication process freezes on the switch, perform a `shutdown/no shutdown` on that port.