

# Implementação do Projeto

Informações descritas são concordantes com o modelo OSI (7 camadas).

- ❖ Routers: “c3745-adventerprisek9-mz.124-25d.image”. Incluindo 4 slots com um terminal *ethernet* (NM-1FE-TX).
- ❖ Switches: “c3745-adventerprisek9\_ivs-mz.124-15.T8.image”, é uma imagem de *router*, mas permite uma instalação como ethernet switch, utilizando as funcionalidades da camada *data link* pela inclusão do modulo *switch* com 16 portas (NM-16ESW). No processo de instalação desta *appliance* no GNS3, o processo deve ser realizado com a opção de “Ethernet Switch” selecionada.
- ❖ Supplicant/Cliente: Micro Core Linux 6.4, disponível no GNS3, “linux-microcore-6.4.img”.

## 1. Conectividade entre toda a topologia

Configurações em Routers:

```
interface FastEthernet INT/ID
  ip address IP-ADDR MASK-ID
  no shutdown
!
R1 0/0 - 192.168.10.1 255.255.255.0
    1/0 - dhcp %Public IP
    4/0 - 192.168.100.1 255.255.255.0
```

Configurar NAT para traduções entre IPs público e privados. Apenas rede 192.168.10.0/24 acede à rede publica.

```
ip nat inside source list 10 interface FastEthernet1/0 overload
access-list 10 permit 192.168.10.0 0.0.0.255 %%
%Todos endereços privados são traduzidos para o IP da interface f1/0
!
interface range FastEthernet0/0, f4/0 %interfaces internas
  ip nat inside
interface FastEthernet 1/0 %interface externa
  ip nat outside
```

## 2. RADIUS

Permite autenticação de utilizadores à rede LAN através da estrutura AAA e do protocolo 802.1X. Os serviços AAA (Authentication, Autorization e Accounting) permitem autenticação de utilizadores tanto para a camada *network* (acesso a routers) como acesso à rede física (camada *data link* – 802.1X). O DOT1X foi criado para controlo de acesso port-based através de autenticação a cada utilizador/dispositivo (suplicante) que se conecta à LAN. Através de um mecanismo em cada switch/ponto de acesso (autenticador) pode entregar detalhes da autenticação ao servidor RADIUS (servidor de autenticação).

O serviço de Autenticação e Autorização (AAA) é fornecido por um servidor RADIUS, permitindo um sistema de autenticação centralizado. O GNS3 oferece um *docker* que implementa a funcionalidade do servidor RADIUS, que poupa recursos de *hardware*. A appliance *plug-n-play*, designada de 'AAA'.

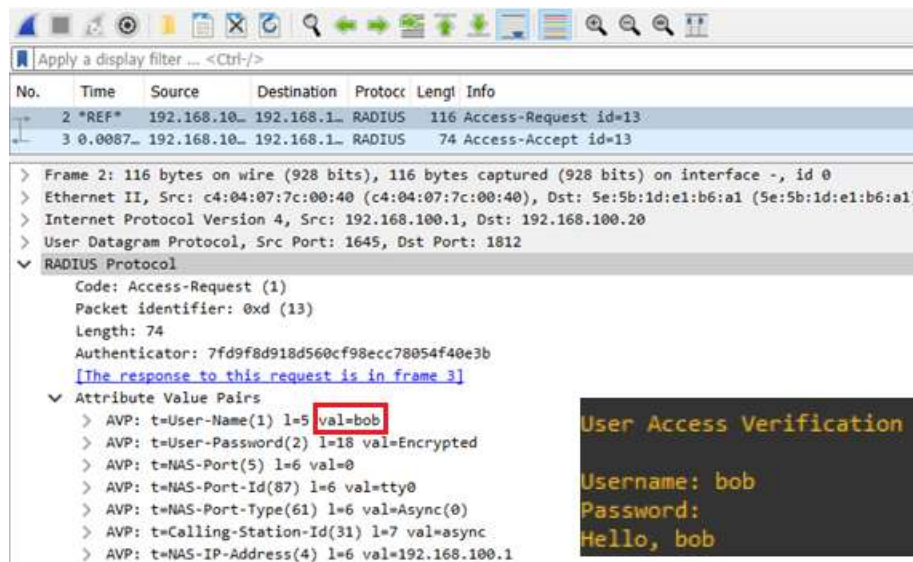
- Configuração: através do terminal, configurar IP `#nano /etc/network/interfaces`

Para routers e switches sempre que acedidos ssh ou console devem ser autenticados pelo servidor RADIUS.

Autenticação: para que sejam acedidos os switches e routers são configurados por:

```
username backup password backup %local_credentials if AAA offline
aaa new-model
aaa authentication login default group radius local %%
%processo login é autenticado pelo servidor radius ou local
radius-server host 192.168.100.20 auth-port 1812 acct-port 1813 key gns3
%endereço servidor, portos de autenticação e registo, chave validação
```

Sempre que for necessário aceder aos dispositivos vai ser solicitado credenciais de acesso e é enviado ao servidor RADIUS um pedido com essas credenciais e o servidor aceita ou recusa consoante essas credenciais. Exemplo para o router CB-GW:



The image displays a Wireshark packet capture of a RADIUS authentication exchange. The packet list shows two frames: Frame 2 (Access-Request) and Frame 3 (Access-Accept). The packet details for Frame 2 show the RADIUS Protocol section expanded, revealing the Attribute Value Pairs (AVPs). The AVPs include t=User-Name(1) with value 'val=bob', t=User-Password(2) with value 'val=Encrypted', t=NAS-Port(5) with value 'val=0', t=NAS-Port-Id(87) with value 'val=tty0', t=NAS-Port-Type(61) with value 'val=Async(0)', t=Calling-Station-Id(31) with value 'val=async', and t=NAS-IP-Address(4) with value 'val=192.168.100.1'. A terminal window on the right shows the login process: 'User Access Verification', 'Username: bob', 'Password:', and 'Hello, bob'.

O controlo de acesso ao meio para os dispositivos que se conectam é configurado nos dispositivos que atuam como autenticadores, como switches. O suplicante 802.1X pode ser uma máquina virtual ou real inserido no ambiente do GNS3, porém máquinas com interface gráfica (GUI) consomem bastantes para recursos. Para “visualizar” funcionalidade a distribuição Micro Core Linux permite testar o funcionamento de suplicante, necessita de algumas configurações:

- I. Instalar *appliance* – disponível no *Marketplace* GNS3;
- II. Interligar com a Internet (seja a nuvem “Cloud” ou “NAT”). Recomendação: NAT.
  - a. (Sugestão) Configurar endereço dinâmico: `$ sudo udhcpc -ieth0;`
  - b. Endereço estático e *gateway*:  
`# ifconfig eth0 IP_ADD netmask MASK up`  
`# route add default gw IP-ADD dev eth0`
- III. Efetuar o download do serviço suplicante e, como sugestão, do serviço *ssh*.
  - a. `$ tce-load -iw wpa_supPLICANT.tcz`
  - b. `$ tce-load -wi openssh`

*Aguardar Instalação. Após termino interligar à topologia.*

- IV. Abrir o terminal do Micro Core Linux e através do editor *vi* criar um documento na pasta *etc* (pasta que guarda ficheiros de configuração). Exemplo:
  - a. Executar: `# vi /etc/ficheiro_dot1x.conf`, abre um ficheiro vazio, as suas linhas são representadas por ‘~’;
  - b. Inserir as seguintes linhas:

```
ctrl_interface=/var/run/wpa_supPLICANT      %executa programa
ap_scan=0                                   %não procura AP, apenas considera file config
network={                                  %Configuração para rede especifica
key_mgmt=IEEE8021X                          %gestão port-based 802.1X
eap=MD5                                      %método de autenticação
identity="bob"                             %credenciais disponíveis no servidor AAA
password="gns3"
eapol_flags=0                              %sem flag especificas
}
```

- c. Guardar ficheiro: *Esc* e inserir `:wq`.  
*‘Esc’* termina a edição, `:wq` guarda alterações e sai do modo edição (*vi*).

- V. Executar modo suplicante. Assim que comando é inserido, *endpoint* envia mensagens ‘EAP Start’ assim que se conecta no *switch*.

```
# wpa_supPLICANT -B -Dwired -ieth0 -c/etc/ficheiro_dot1x.conf.
```

**Nota:** o símbolo cardinal (pound) ‘#’ indica que está em modo privilegiado (root). O símbolo cifrão (dollar) ‘\$’ indica que está em modo execução (utilizador).

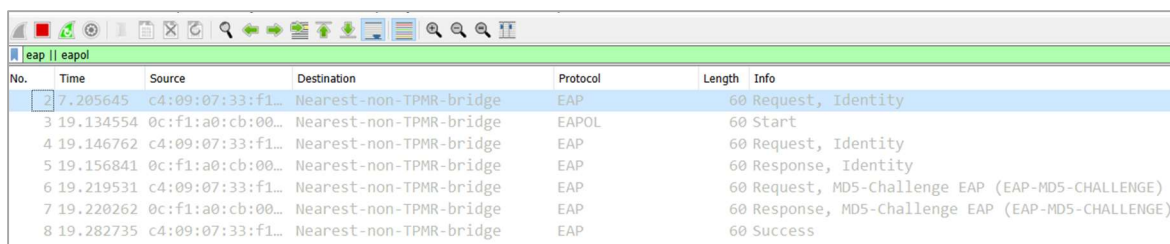
O autenticador é configurado como:

```
aaa new-model %permite autenticação AAA. Se já ativo, não inserir
aaa authentication dot1x default group radius %%%
%define autenticação dot1x pelo servidor RADIUS
aaa authorization network default group radius
%configura método de autorização default p/ serviços na rede, via RADIUS
dot1x system-auth-control %ativa mecanismo 802.1X para autenticar hosts
radius-server host 192.168.100.20 auth-port 1812 acct-port 1813 key gns3
int range FastEthernet1/1 - 9
dot1x port-control auto %configura o controlo da porta
dot1x pae-authenticator %porta é autenticada pelo dispositivo
```

Após todas as configurações, a porta do switch é desativa automaticamente. Contudo após inserir: “# wpa\_supplicant -B -Dwired -ieth0 -c/etc/ficheiro\_dot1x.conf” no suplicante, com servidor operacional, fica ativo novamente. A figura seguinte mostra a confirmação, através da captura de pacotes, do funcionamento 802.1X. Em termos simples, o protocolo funciona:

- 1) Envia “EAPOL Start”: suplicante envia mensagem para a autenticador para iniciar processo de autenticação. O suplicante identifica-se;
- 2) EAP Request/Identity: o autenticador encaminha a identidade do suplicante para o servidor de autenticação para solicitar a respetiva autenticação;
- 3) EAP-Response/Identity: o servidor envia esta mensagem ao autenticador, verificando a identidade do suplicante
- 4) EAP-Request/Method: Autenticador envia mensagem para o suplicante solicitando método de autenticação e chaves de encriptação para uma ligação segura com a rede;
- 5) EAP-Response/Method: suplicante responde utilizando o método de autenticação ( username/password, digital certificate, chaves, etc.);
- 6) EAP-Success: servidor notifica o autenticador se autenticação for sucedida;
- 7) EAPoL-Success: o autenticador cede o acesso ao suplicante;

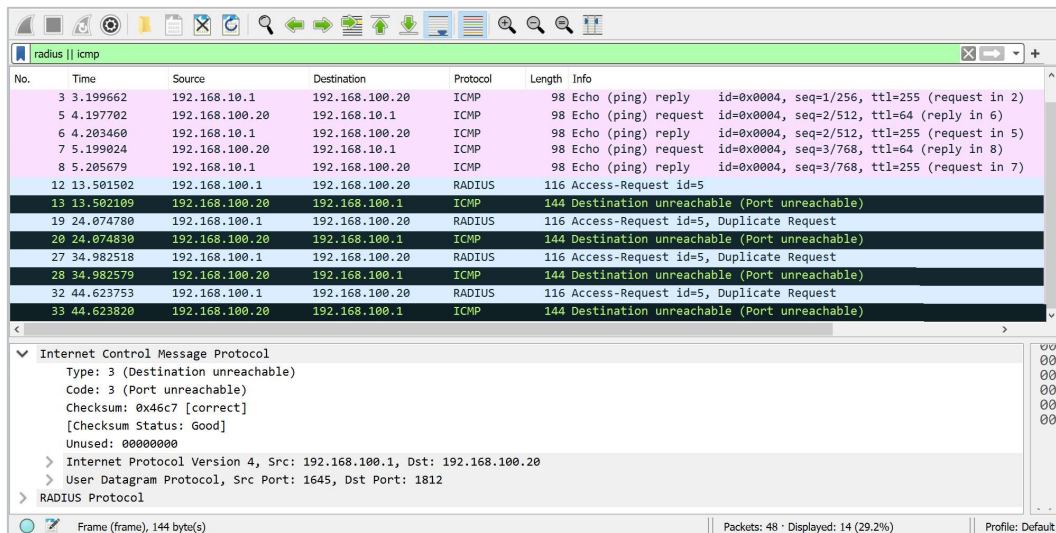
EAP (Extensible Authentication Protocol) e EAPoL (EAP over LAN) são protocolos de comunicação usados no processo 802.1X. EAP é a estrutura que define como suplicante e o servidor de autenticação comunicam e negoceiam, enquanto EAPoL é responsável por encapsular e transportar a mensagens EAP pela LAN (entre suplicante e autenticador).



No.	Time	Source	Destination	Protocol	Length	Info
2	7.205645	c4:09:07:33:f1...	Nearest-non-TPMR-bridge	EAP	60	Request, Identity
3	19.134554	0c:f1:a0:cb:00...	Nearest-non-TPMR-bridge	EAPoL	60	Start
4	19.146762	c4:09:07:33:f1...	Nearest-non-TPMR-bridge	EAP	60	Request, Identity
5	19.156841	0c:f1:a0:cb:00...	Nearest-non-TPMR-bridge	EAP	60	Response, Identity
6	19.219531	c4:09:07:33:f1...	Nearest-non-TPMR-bridge	EAP	60	Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
7	19.220262	0c:f1:a0:cb:00...	Nearest-non-TPMR-bridge	EAP	60	Response, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
8	19.282735	c4:09:07:33:f1...	Nearest-non-TPMR-bridge	EAP	60	Success

**Recomendação:** nestes ISOs as mensagens *dot1x* podem estar desativas, ativar “*debug dot1x {events | packets}*”.

## Troubleshooting:



No.	Time	Source	Destination	Protocol	Length	Info
3	3.199662	192.168.10.1	192.168.100.20	ICMP	98	Echo (ping) reply id=0x0004, seq=1/256, ttl=255 (request in 2)
5	4.197702	192.168.100.20	192.168.10.1	ICMP	98	Echo (ping) request id=0x0004, seq=2/512, ttl=64 (reply in 6)
6	4.203460	192.168.10.1	192.168.100.20	ICMP	98	Echo (ping) reply id=0x0004, seq=2/512, ttl=255 (request in 5)
7	5.199024	192.168.100.20	192.168.10.1	ICMP	98	Echo (ping) request id=0x0004, seq=3/768, ttl=64 (reply in 8)
8	5.205679	192.168.10.1	192.168.100.20	ICMP	98	Echo (ping) reply id=0x0004, seq=3/768, ttl=255 (request in 7)
12	13.501502	192.168.100.1	192.168.100.20	RADIUS	116	Access-Request id=5
13	13.502109	192.168.100.20	192.168.100.1	ICMP	144	Destination unreachable (Port unreachable)
19	24.074780	192.168.100.1	192.168.100.20	RADIUS	116	Access-Request id=5, Duplicate Request
20	24.074830	192.168.100.20	192.168.100.1	ICMP	144	Destination unreachable (Port unreachable)
27	34.982518	192.168.100.1	192.168.100.20	RADIUS	116	Access-Request id=5, Duplicate Request
28	34.982579	192.168.100.20	192.168.100.1	ICMP	144	Destination unreachable (Port unreachable)
32	44.623753	192.168.100.1	192.168.100.20	RADIUS	116	Access-Request id=5, Duplicate Request
33	44.623820	192.168.100.20	192.168.100.1	ICMP	144	Destination unreachable (Port unreachable)

Internet Control Message Protocol  
Type: 3 (Destination unreachable)  
Code: 3 (Port unreachable)  
Checksum: 0x46c7 [correct]  
[Checksum Status: Good]  
Unused: 00000000  
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.20  
> User Datagram Protocol, Src Port: 1645, Dst Port: 1812  
> RADIUS Protocol

Frame (frame), 144 byte(s) | Packets: 48 · Displayed: 14 (29.2%) | Profile: Default

- Sempre que iniciar *appliance*, verifique através da captura de pacotes que pacotes RADIUS são respondidos. Podem existir pedidos RAIDUS e a resposta do porto “unreachable”. **Solução:** executar no *docker* AAA service `freeradius restart`, caso seja apresentada a mensagem:

```
“* Checking FreeRADIUS daemon configuration... [fail]”
```

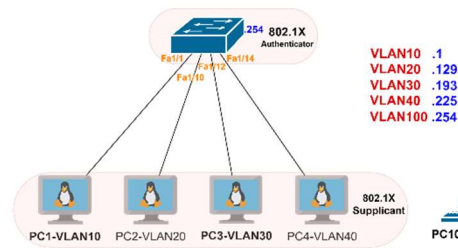
O servidor não está a funcionar corretamente e depois de várias tentativas, é recomendado a reinicialização do GNS3 ou de eliminar e introduzir novamente *appliance*. A mensagem expectável é:

```
“* Checking FreeRADIUS daemon configuration... [ OK ]”
```

```
“* Stopping FreeRADIUS daemon freeradius [ OK ]”
```

```
“* Starting FreeRADIUS daemon freeradius [ OK ]”
```

### 3. VLAN



Testes podem ser executados na VLAN 1. Contudo é uma solução de segurança e VLAN por defeito ou nativa não deve ser VLAN1.

Todas as características incluídas pela VLAN introduzem, principalmente: a segurança, o controlo de tráfego e a divisão dos domínios de *broadcast*. Segurança: dispositivos na camada 2 não podem aceder a outras VLANs, ataques ao protocolo ARP, STP ou DHCP (Discover) não trespassam para outra VLAN, evitando alcance de serviços importantes.

Tráfego e Broadcast: A segmentação melhora a eficiência da rede, segurança, gestão e flexibilidade. Gestão da rede como ARP, CDP, DTP, STP e outros da camada “Ligação” ficam segmentados à sua VLAN, evitando tráfego em toda a extensão da rede física.

Contudo é importante compreender que a separação de VLAN, por exemplo, por departamentos. Existem outros conceitos importantes para que esses departamentos troquem dados.

- Inter-VLAN Routing: consiste em configurar um router para encaminhar tráfegos entre VLANs, portanto a *gateway* de cada VLAN é uma sub-interface do router. Sub-interface é uma interface virtual proveniente da interface física.
- Trunking: aplicado quando o tráfego de múltiplas VLANs segue por um segmento físico, preservando a informação de cada VLAN.
- Layer 3 switch: combina as funções de router e switch, sendo mais eficiente pela sua capacidade de processamento via *hardware*. O processo de inter-vlan routing é realizado internamente a SVI (switc virtual interface) semelhante às sub-interfaces.

No ISO (c3745) do switch utilizada, a criação de VLANs é diferente.

vlan database	
vlan	ID name NAME
10	##VLAN-10##
20	##VLAN-20##
30	##VLAN-30##
40	##VLAN-40##
int vlan ID	
ip	address IP-ADDR
no	shutdown
SW1 10 - 192.168.10.126	
int f1/0	
switchport	mode trunk
sw tr	allowed vlan execpt 1 %evita tráfego na VLAN ativa por defeito
switchport	trunk native vlan 99
sw tr	allowed vlan add 100 %pode ser necessário adicionar VLAN
int range f1/1 - 9	
switchport	mode access
switchport	access vlan 10

<pre> int range f1/10 - 11   switchport mode access   switchport access vlan 20 </pre>
<pre> int range f1/12 - 13   switchport mode access   switchport access vlan 30 </pre>
<pre> int range f1/14 - 15   switchport mode access   switchport access vlan 40 </pre>
<pre> int vlan 10   ip address  IP-ADDR MASK-ID   no shutdown </pre> <p>SW1 - 192.168.10.126 255.255.255.128</p>
<p>Configurar ROAS nos Routers</p>
<pre> interface FastEthernet0/0.VLAN-ID   encapsulation dot1Q VLAN-ID [native] %inserir 'native' p/ VLAN nativa   ip address IP-ADDR MASK-ID </pre> <p> <b>10</b> - 192.168.10.1 255.255.255.128  <b>20</b> - 192.168.10.129 255.255.255.192  <b>30</b> - 192.168.10.193 255.255.255.224  <b>40</b> - 192.168.10.225 255.255.255.224 </p>

## 4. DNS e DHCP

Os endereços podem ser estáticos, contudo automação é importante (DHCP)

Alterar em conformidade pool's DHCP no Router	
<pre>ip dhcp pool <b>IP-VLAN-ID</b>   network <b>IP-ADDR MASK-ID</b>   default-router <b>192.168.10.1</b>   dns-server 8.8.8.8 !</pre>	
<b>R1</b>	
<b>10</b>	<b>192.168.10.0 255.255.255.128 192.168.10.1</b>
<b>20</b>	<b>192.168.10.128 255.255.255.192 192.168.10.129</b>
<b>30</b>	<b>192.168.10.192 255.255.255.224 192.168.10.193</b>
<b>40</b>	<b>192.168.10.224 255.255.255.240 192.168.10.225</b>



## 5. Testar Rede

Após todas as configurações, para executar a rede e testar conectividade são sugeridos os seguintes passos para contornar algumas limitações e garantir um funcionamento efetivo.

1. Iniciar servidor RADIUS. RADIUS para *login* nos equipamentos com **bob** e palavra-chave **gns3** (podem ser criados outros utilizadores);
2. Ligar o Router R1 (CB-GW) e verificar atribuição DHCP. Configurar o relógio para uma hora atual (apenas para NTP atualizar rapidamente), aguardar e verificar sincronização.
3. Aguardar convergência da rede.
4. Se PC (*Micro Core Linux*) já tiver configurações. Executar comando:  

```
# wpa_supplicant -B -Dwired -ieth0 -c/etc/ficheiro_dot1x.conf.
```

Através do Wireshark e/ou *debug dot1x*, é verificado o processo de autenticação.
5. Desligar servidor RADIUS, ou apenas 'eliminar' ligação para testar o recurso da autenticação à base de dados local de cada equipamento, através das credenciais **backup** e **backup123**.