

Requerimiento 1. Realiza la asignación de IPv4/IPv6, fortalecer las contraseña y acceso en routers, y la creación de VLAN a su vez la asignación en interfaces correspondiente.

Instrucciones relacionadas:

- Toda conexión externa se encuentra direccionada con IPv4/IPv6.

En el router BORDE se hizo el direccionamiento usando los segmentos de red dados ara lograr la conectividad de la red interna con la externa

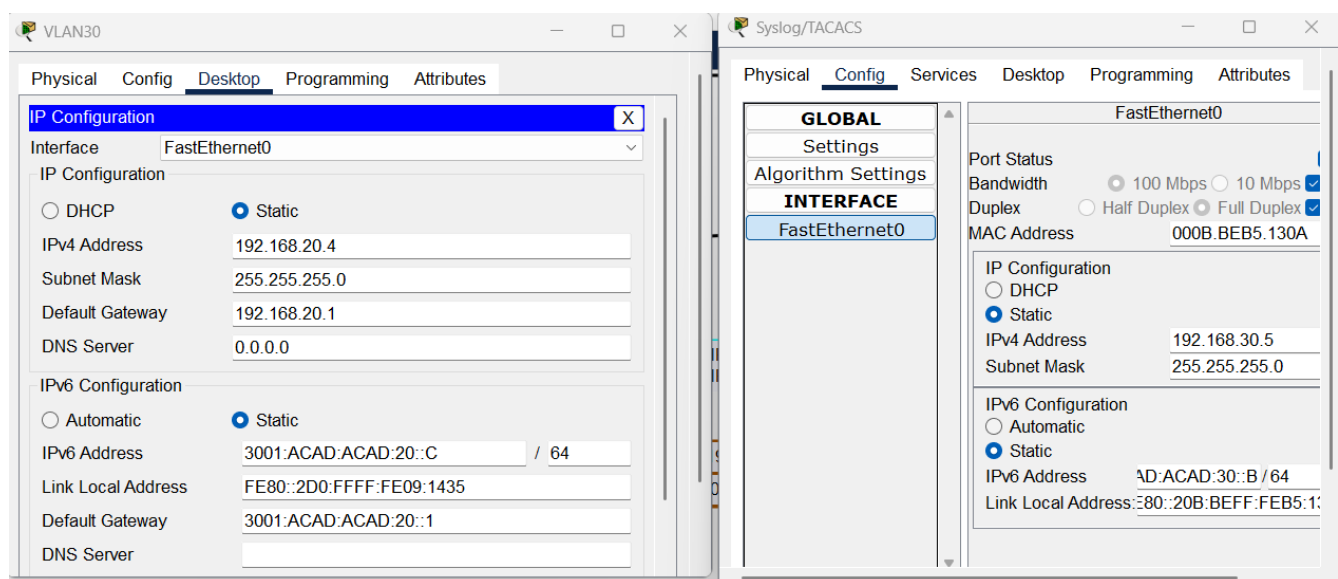
```

BORDE#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0       201.0.0.2       YES manual up          up
GigabitEthernet0/1       205.0.0.1       YES manual up          up
GigabitEthernet0/2       unassigned      YES unset  administratively down down
Vlan1                    unassigned      YES unset  administratively down down
BORDE#show ipv6 interface brief
GigabitEthernet0/0       [up/up]
FE80::210:11FF:FE5D:BC01
3001:ABCD:ABCD:201::2
GigabitEthernet0/1       [up/up]
FE80::210:11FF:FE5D:BC02
3001:ABCD:ABCD:205::1
GigabitEthernet0/2       [administratively down/down]
unassigned
Vlan1                    [administratively down/down]
unassigned
BORDE#

```

- Asignar IPv4/IPv6 en equipos finales.

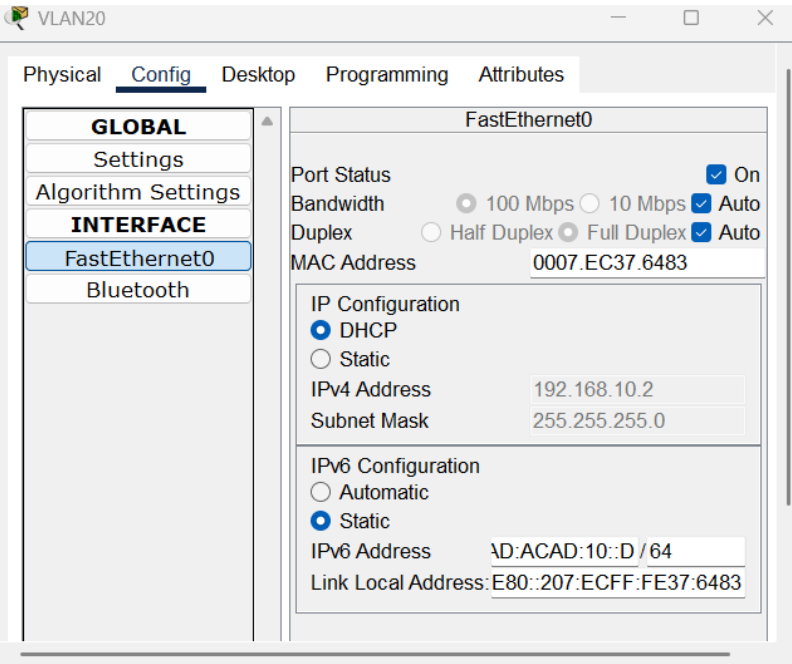
Se asignaron las Ip a los dispositivos finales según la indicación de la topología. Estática para las todas las Vlanes, excepto para la Vlan 20 en ipV4 que se hizo por DHCP creando un pool en el CORE.



Pool en CORE para la asignación del PC Vlan20

```
CORE#show running-config | section dhcp
ip dhcp pool VLAN20_POOL
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
CORE#
```

PC Vlan20 con su Ip por DHCP



•Fortalecer las contraseñas y acceso a routers y switches de la manera más resistente posible.

Para cumplir con este punto se configuraron varias cosas. Se Configuro el “enable secret” para crear y encriptar la contraseña al modo privilegio (contraseña: “ClavePrueba”). Se aseguraron los accesos por consola “line con 0” y SHH “line vty 0 4) ademas de un banner donde se advierte contra uso no autorizado”

Tipo de Acceso	Comando de Configuración	Contraseña
Modo de Privilegio	enable secret	ClavePrueba
(#)Acceso por Consola	line console 0	ClaveConsola
(>)Acceso Remoto (>)	line vty 0 15	Clavevty

Capturas (Para ejemplo solo CORE):

```
service password-encryption
!
hostname CORE
!
!
enable secret 5 $l$mERr$/xJfn2g/dGyRwd0S4YBHg/
!
```

```
banner motd ^CADVERTENCIA! Acceso no autorizado prohibido. Solo
personal autorizado.^C
!
!
!
!
logging trap debugging
logging 192.168.30.5
line con 0
  password 7 0802404F1F1C26181C1803082B
  login
!
line aux 0
!
line vty 0 4
  password 7 0802404F1F1C13030B
  login
line vty 5 15
  password 7 0802404F1F1C13030B
  login
,
```

- Crear las VLAN propuestas en todos los switches.

Se crearon todas las Vlan que nos pedia la prueba.

10	NATIVA	active
20	TI	active
30	RRHH	active
40	SERVIDORES	active

Page 11

- Asignar solo interfaz en uso a VLAN correspondiente.

Solo se asignaron las interfaces realmente conectadas a dispositivos finales por vlan. No se realizo el apagado de todas las interfaces sin uso y enviarlas a una vlan especial como BlackHole por la premura de la prueba.

Captura SWB :

30	RRHH	active	Fa0/14
40	SERVIDORES	active	Fa0/11

Captura SWA: La de Vlan 10 fue para hacer la prueba de conectividad con Vlan 20

10	NATIVA	active	Fa0/24
20	TI	active	Fa0/23

Requerimiento 2. Configura enlaces troncales con los ajustes necesarios, la habilitación de STP y mecanismos de estabilización con sus requerimientos respectivos.

- En los enlaces troncales permitir solo el paso de VLAN de datos.

Se configuraron todos los enlaces troncales para que solo permitan el tráfico de las VLANs de datos que realmente se necesitan

```
SWD#show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Fa0/10    on        802.1q         trunking      10
Fa0/15    on        802.1q         trunking      10
Fa0/20    on        802.1q         trunking      10

Port      Vlans allowed on trunk
Fa0/10    10,20,30,40
Fa0/15    10,20,30,40
Fa0/20    10,20,30,40

Port      Vlans allowed and active in management domain
Fa0/10    10,20,30,40
Fa0/15    10,20,30,40
Fa0/20    10,20,30,40

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/10    10,20,30,40
Fa0/15    10,20,30,40
Fa0/20    10,20,30,40
```

- VLAN Nativa tendrá configuración apropiada.

Se cambio la vlan nativa 1 por la Vlan 10 como nativa

```
SWD#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/10    on        802.1q         trunking    10
Fa0/15    on        802.1q         trunking    10
Fa0/20    on        802.1q         trunking    10
```

- En enlaces troncales deshabilitar protocolo DTP .

Se deshabilitó en todos los enlaces troncales con el comando “switchport nonegotiate”

```
SWA#show interfaces Fa0/5 switchport
Name: Fa0/5
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
```

- Implementar PVST+ Rápido.

Se implementó el protocolo Rapid PVST+ en todos los switches. Se designó al Switch SWD como el puente raíz para todas las VLANs asignándole una prioridad más baja.

```
SWD#show spanning-tree
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    4106
             Address     00E0.F9A9.A1B3
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4106 (priority 4096 sys-id-ext 10)
             Address     00E0.F9A9.A1B3
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/10         Desg FWD 19        128.10   P2p
Fa0/15         Desg FWD 19        128.15   P2p
Fa0/20         Desg FWD 19        128.20   P2p

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    4116
             Address     00E0.F9A9.A1B3
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4116 (priority 4096 sys-id-ext 20)
             Address     00E0.F9A9.A1B3
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 20
```

- Implementar mecanismos de estabilización de STP en interfaces de acceso

Se implementaron los mecanismos de PortFast y BPDU Guard en los puertos de acceso

```

interface FastEthernet0/11
  switchport access vlan 40
  ip dhcp snooping limit rate 2
  switchport mode access
  switchport port-security
  switchport port-security maximum 2
  spanning-tree portfast
  spanning-tree bpduguard enable
!

```

Requerimiento 3. Implementar seguridad de capa 2, control de tormentas, y DHCP con su correspondiente configuración para evitar ataque en este protocolo.

- En el SWA implementar seguridad de puerto dinámica.

```

SWA#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)          (Count)          (Count)
-----
Fa0/23        1                1                0          Restrict
-----
SWA#

```

- En el SWB implementar seguridad de puerto con aprendizaje con un máximo de 2 MAC. En caso de exceder, la interfaz debe desactivarse (shutdown).

```

SWB#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)          (Count)          (Count)
-----
Fa0/11        2                1                0          Shutdown
Fa0/14        2                1                0          Shutdown
-----

```

- Enlaces troncales: habilitar control de tormentas al 20% .

Se configuro con el comando “storm-control broadcast level 20.0” en las interfaces troncales

Por ejemplo en SWB en la interface fa0/20 (troncal hacia SWD)

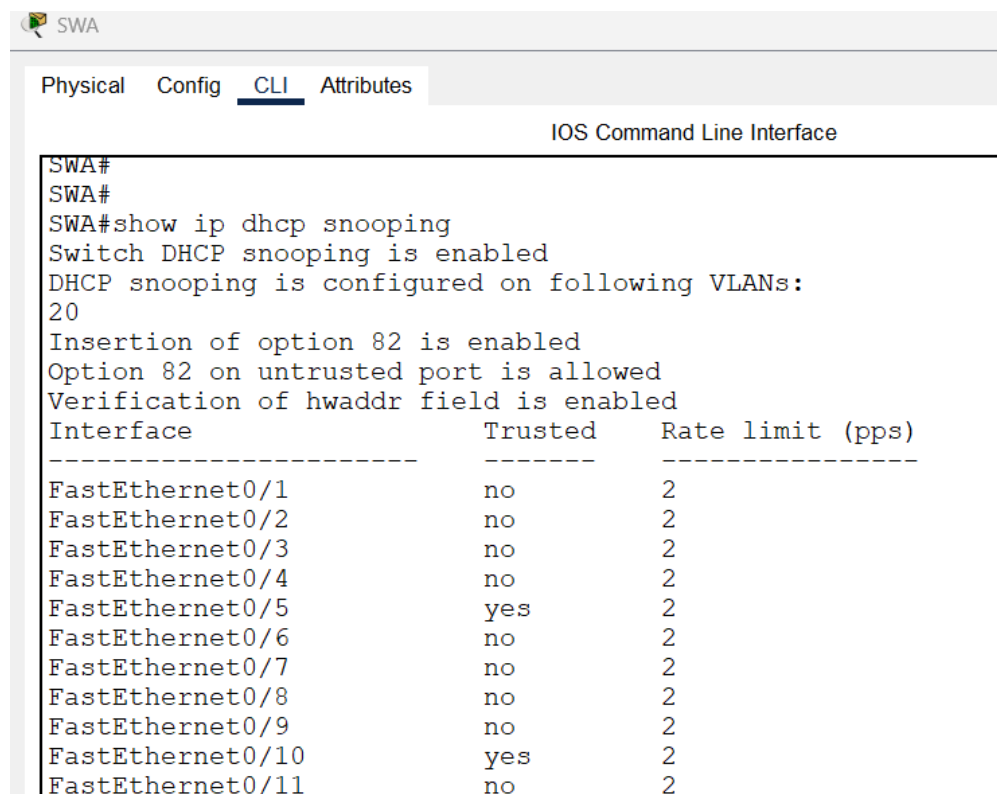
```

interface FastEthernet0/20
description Trunk
switchport trunk native vlan 10
switchport trunk allowed vlan 10,20,30,40
ip dhcp snooping trust
switchport mode trunk
storm-control broadcast level 20

```

- Equipos de VLAN20 deben recibir solo 2 IP por minuto, además de que debe ser solo a través del DHCP legítimo.

Se implementó DHCP Snooping para proteger la VLAN 20 de ataques DHCP. Se configuraron como “Trust” las interfaces troncales y “No Trust” las interfaces a equipos finales (en este caso se lo aplicamos a todas las interfaces que no eran troncales)



The screenshot shows the CLI of a switch named SWA. The 'CLI' tab is selected. The output of the command 'show ip dhcp snooping' is displayed, showing that DHCP snooping is enabled on VLAN 20. Below this, a table lists the status of DHCP snooping on various interfaces.

Interface	Trusted	Rate limit (pps)
FastEthernet0/1	no	2
FastEthernet0/2	no	2
FastEthernet0/3	no	2
FastEthernet0/4	no	2
FastEthernet0/5	yes	2
FastEthernet0/6	no	2
FastEthernet0/7	no	2
FastEthernet0/8	no	2
FastEthernet0/9	no	2
FastEthernet0/10	yes	2
FastEthernet0/11	no	2

Requerimiento 4. Realiza enrutamiento intervlan y confi guraciones para lograr conectividad. Además de todos los mensajes Syslog del router deben llegar al servidor respectivo.

- Realizar enrutamiento intervlan en IPv4/IPv6.

Se configuró el enrutamiento inter-VLAN en el switch CORE para permitir que los equipos de diferentes VLANs se comuniquen entre sí. Esto se logró creando una interfaz virtual (SVI) para cada VLAN y asignándole una dirección IPv4 e IPv6. Cada SVI actúa como el gateway predeterminado para su respectiva VLAN, permitiendo que el switch de Capa 3 enrute el tráfico entre ellas.

Captura de “show ip interface brief” en CORE:

Vlan1	unassigned	YES	unset	administratively down	down
Vlan10	192.168.100.1	YES	manual	up	up
Vlan20	192.168.10.1	YES	manual	up	up
Vlan30	192.168.20.1	YES	manual	up	up
Vlan40	192.168.30.1	YES	manual	up	up

Captura de show ipv6 interface brief en CORE:

```
unassigned
Vlan10 [up/up]
FE80::201:C9FF:FE38:3E04
3001:ACAD:ACAD:100::1
Vlan20 [up/up]
FE80::201:C9FF:FE38:3E01
3001:ACAD:ACAD:10::1
Vlan30 [up/up]
FE80::201:C9FF:FE38:3E02
3001:ACAD:ACAD:20::1
Vlan40 [up/up]
FE80::201:C9FF:FE38:3E03
3001:ACAD:ACAD:30::1
CORE#
```

- Implementar enrutamiento por defecto en IPv6 de ida y vuelta en red externa.

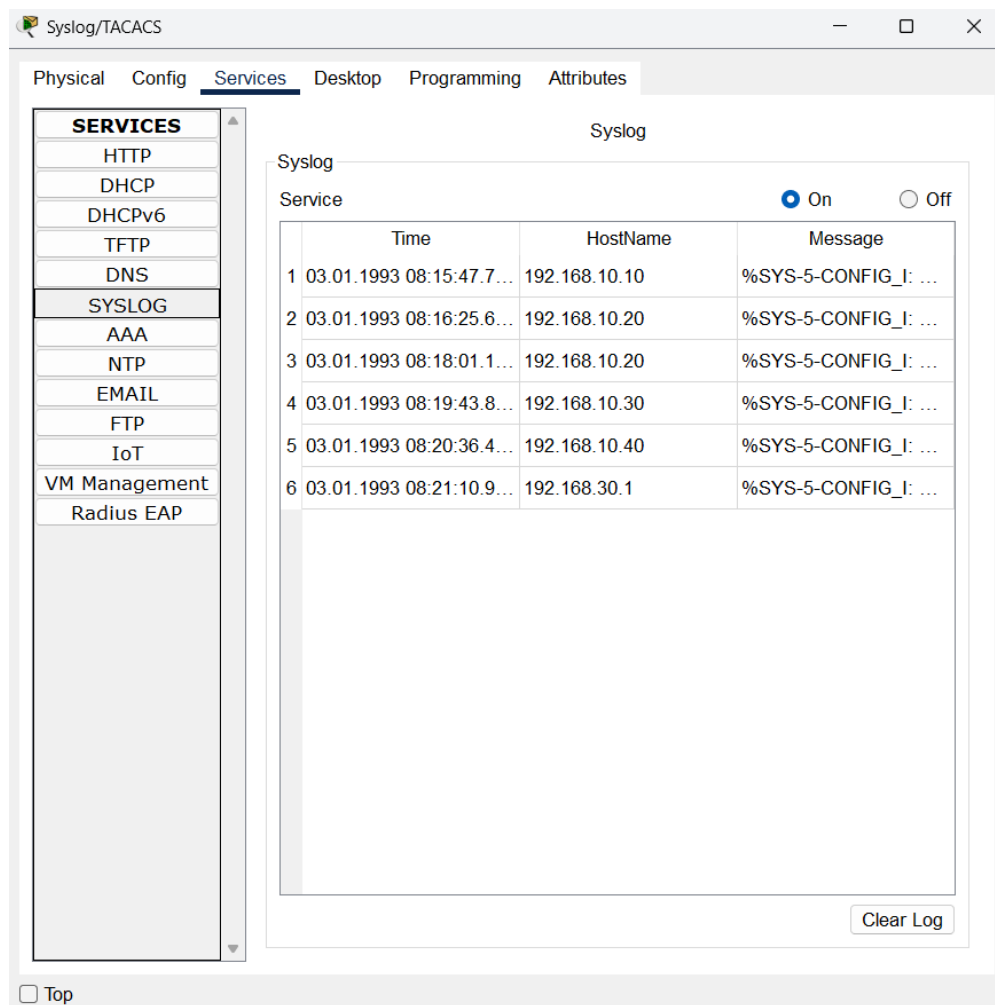
En BORDE:

```
-----
BORDE#show ipv6 static
IPv6 Static routes Table - default
Codes: * - installed in RIB, u/m - Unicast/Multicast only
      U - Per-user Static route
      N - ND Static route
      M - MIP Static route
      P - DHCP-PD Static route
      R - RHI Static route
*   ::/0 via 3001:ABCD:ABCD:205::2, distance 1
*   3001:ACAD:ACAD:10::/64 via 3001:ABCD:ABCD:201::1, distance 1
*   3001:ACAD:ACAD:20::/64 via 3001:ABCD:ABCD:201::1, distance 1
*   3001:ACAD:ACAD:30::/64 via 3001:ABCD:ABCD:201::1, distance 1
BORDE#
```

- Todos los mensajes generados por los switches deben llegar al servidor Syslog.

Se les asigno una IP de la Vlan 20 a cada switch y se le activo el logging y se le configuro la Ip del servidor para que enviaran los log al servidor





- Implementar lista de acceso donde VLAN10 y VLAN20 no se comuniquen en IPv4/IPv6

```
CORE#show access-lists
Extended IP access list NO_VLAN10_TO_VLAN20_IPV4
 10 deny ip 192.168.100.0 0.0.0.255 192.168.10.0 0.0.0.255 (4 match(es))
 20 permit ip any any
Extended IP access list NO_VLAN20_TO_VLAN10_IPV4
 10 deny ip 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 (11 match(es))
 20 permit ip any any (10 match(es))
IPv6 access list NO_VLAN10_TO_VLAN20_IPV6
 deny ipv6 3001:ACAD:ACAD:100::/64 3001:ACAD:ACAD:10::/64 (4 match(es))
 permit ipv6 any any
IPv6 access list NO_VLAN20_TO_VLAN10_IPV6
 deny ipv6 3001:ACAD:ACAD:10::/64 3001:ACAD:ACAD:100::/64 (4 match(es))
 permit ipv6 any any
CORE#
```

```
CORE#show ipv6 access-list
IPv6 access list NO_VLAN10_TO_VLAN20_IPV6
 deny ipv6 3001:ACAD:ACAD:100::/64 3001:ACAD:ACAD:10::/64 (4 match(es))
 permit ipv6 any any
IPv6 access list NO_VLAN20_TO_VLAN10_IPV6
 deny ipv6 3001:ACAD:ACAD:10::/64 3001:ACAD:ACAD:100::/64 (4 match(es))
 permit ipv6 any any
```

Prueba de que había conexión:

En Ipv4:

```
Vlan 10 Prueba
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

En Ipv6:

```
VLAN20
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 3001:ACAD:ACAD:100::1

Pinging 3001:ACAD:ACAD:100::1 with 32 bytes of data:

Reply from 3001:ACAD:ACAD:100::1: bytes=32 time<1ms TTL=255
Reply from 3001:ACAD:ACAD:100::1: bytes=32 time<1ms TTL=255
Reply from 3001:ACAD:ACAD:100::1: bytes=32 time<1ms TTL=255
Reply from 3001:ACAD:ACAD:100::1: bytes=32 time<1ms TTL=255

Ping statistics for 3001:ACAD:ACAD:100::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 3001:ACAD:ACAD:100::2

Pinging 3001:ACAD:ACAD:100::2 with 32 bytes of data:

Reply from 3001:ACAD:ACAD:100::2: bytes=32 time=10ms TTL=127
Reply from 3001:ACAD:ACAD:100::2: bytes=32 time=2ms TTL=127
Reply from 3001:ACAD:ACAD:100::2: bytes=32 time<1ms TTL=127
Reply from 3001:ACAD:ACAD:100::2: bytes=32 time<1ms TTL=127

Ping statistics for 3001:ACAD:ACAD:100::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>
```

Después de implementarla:

```
VLAN20
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 3001:ACAD:ACAD:100::2

Pinging 3001:ACAD:ACAD:100::2 with 32 bytes of data:

Reply from 3001:ACAD:ACAD:10::1: Destination host unreachable.
Reply from 3001:ACAD:ACAD:10::1: Destination host unreachable.
Reply from 3001:ACAD:ACAD:10::1: Destination host unreachable.
Reply from 3001:ACAD:ACAD:10::1: Destination host unreachable.

Ping statistics for 3001:ACAD:ACAD:100::2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

- Crear cuenta a elección en router BORDE el cual debe ser validado por servidor TACACS+

Se configuró el Router **BORDE** para utilizar un servidor **TACACS+** como método de autenticación

```
BORDE#show running-config | section tacacs
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
tacacs-server host 192.168.30.5
tacacs-server key ClaveTacacs
BORDE#show running-config | section line vty
line vty 0 4
password 7 0802404F1F1C13030B
login authentication default
transport input ssh
line vty 5 15
password 7 0802404F1F1C13030B
login authentication default
transport input ssh
BORDE#
```

Configuración del servidor:

The screenshot shows the Syslog/TACACS web interface with the 'Services' tab selected. The 'AAA' service is highlighted in the left sidebar. The main configuration area is titled 'AAA' and includes the following sections:

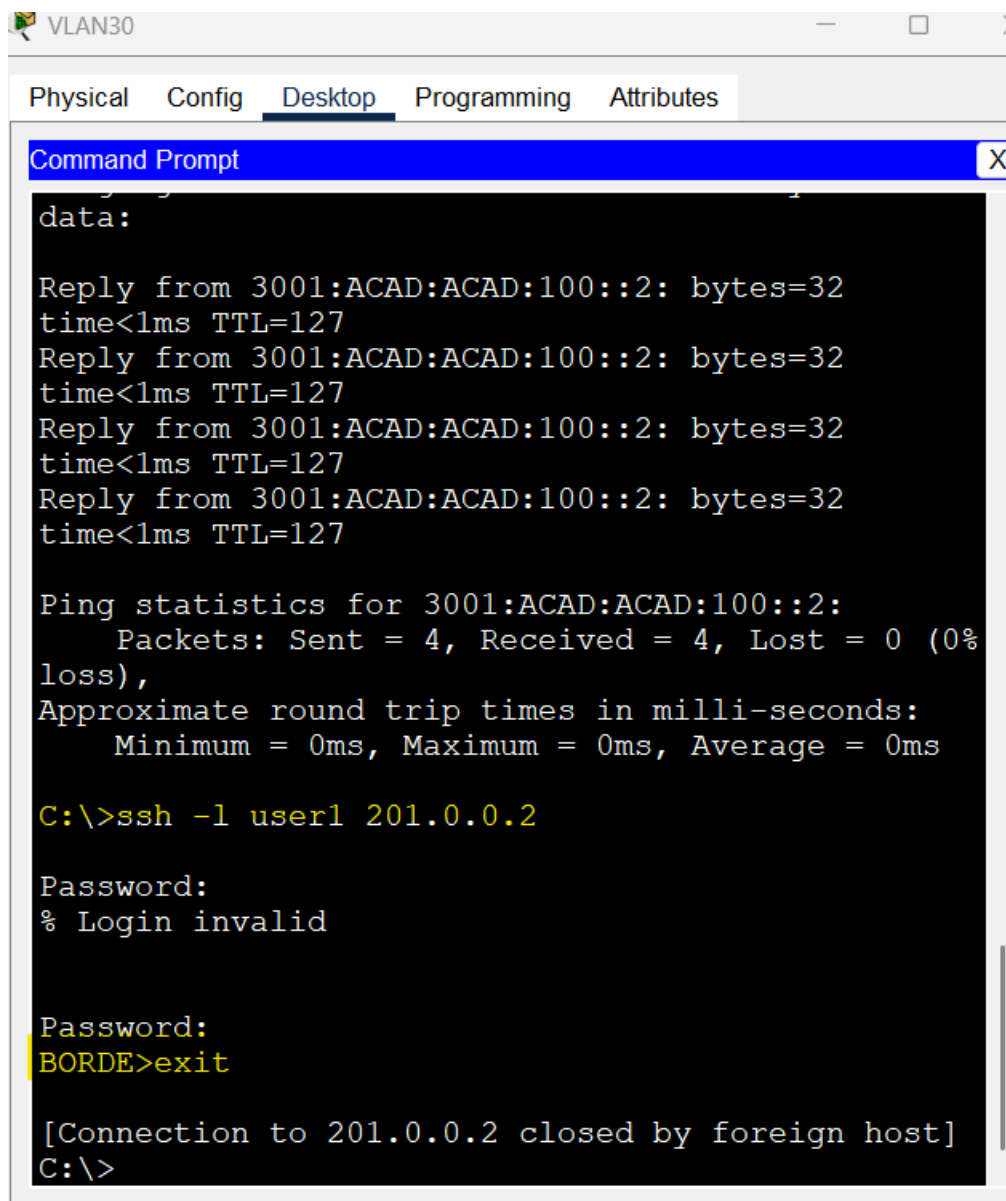
- Service:** A toggle switch is set to 'On'. The 'Radius Port' is set to 49.
- Network Configuration:**
  - Client Name: [Empty field]
  - Client IP: [Empty field]
  - Secret: [Empty field]
  - ServerType: Radius (dropdown menu)
- Table:** A table with 4 columns: Client Name, Client IP, Server Type, and Key. It contains one entry:
 

	Client Name	Client IP	Server Type	Key
1	BORDE	201.0.0.2	Tacacs	ClaveTacacs
- User Setup:**
  - Username: [Empty field]
  - Password: [Empty field]
- Table:** A table with 2 columns: Username and Password. It contains two entries:
 

	Username	Password
1	user1	cisco
2	user2	prueba

Buttons for 'Add', 'Save', and 'Remove' are present next to the table entries.

Prueba de que se puede entrar desde un dispositivo al router Borde:



```
VLAN30
Physical Config Desktop Programming Attributes
Command Prompt X
data:
Reply from 3001:ACAD:ACAD:100::2: bytes=32
time<1ms TTL=127
Reply from 3001:ACAD:ACAD:100::2: bytes=32
time<1ms TTL=127
Reply from 3001:ACAD:ACAD:100::2: bytes=32
time<1ms TTL=127
Reply from 3001:ACAD:ACAD:100::2: bytes=32
time<1ms TTL=127

Ping statistics for 3001:ACAD:ACAD:100::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ssh -l user1 201.0.0.2

Password:
% Login invalid

Password:
BORDE>exit

[Connection to 201.0.0.2 closed by foreign host]
C:\>
```