

Prueba – Seguridad en redes pequeñas y medianas

Nombre: Felipe Oyanedel B

1. Configuración Básica y Direcccionamiento IP

En cada router de la topología se cumplió con la siguiente configuración para obtener administración remota por SSH. Se utilizará nombre del dispositivo de red como username, y password la palabra “test” (sin comillas). También, los equipos deben pertenecer al dominio latam.cl, utilizando una llave RSA de 1024 bits. A su vez, la clave de línea consola será “redes” (sin comillas).

R1

```
login
R1#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R1#show running-config | section line vty
line vty 0 4
 login local
 transport input ssh
R1#show running-config | include username
username R1 privilege 15 password 0 test
R1#show running-config | include domain-name
ip domain-name latam.cl
R1#show crypto key mypubkey rsa
% Key pair was generated at: 0:44:45 UTC julio 18 2025
Key name: R1.latam.cl
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
0000016b 00005be1 00004391 00006f3d 00002c33 00003cce 00005e32 0000435c
00002f11 000074c5 000039dc 000055f0 000075dc 0000570f 00005842 00006f31
00007fff 00001d39 0000254e 000041b2 000012ce 00002017 00005c13 0b88
% Key pair was generated at: 0:44:45 UTC julio 18 2025
Key name: R1.latam.cl.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
0000661a 00002207 00003804 000052ae 00007f02 00000e7a 00004663 000040a8
00002d0d 000052b1 00006bfc 00006167 00005d76 000033c5 00007312 0000496d
000038c7 000045ea 0000359a 00006731 00003ea9 000068f4 000037a7 03c5
R1#show running-config | section line con 0
line con 0
 password redes
 login
R1#
```

Comprobación de funcionamiento de conexión por SSH con usuario y contraseña configurados localmente (username: R1 / password: test).

```
C:\>ssh -l R1 200.200.200.1
Password:
R1#
```

Comprobación de funcionamiento de contraseña establecida en línea consola (redes).

```
User Access Verification
Password:
R1>
```

R2

```
R2#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R2#show running-config | section line vty
line vty 0 4
  login local
  transport input ssh
R2#show running-config | include username
username R2 privilege 15 password 0 test
R2#show running-config | include domain-name
ip domain-name latam.cl
R2#show crypto key mypubkey rsa
% Key pair was generated at: 0:49:12 UTC julio 18 2025
Key name: R2.latam.cl
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00003829 00000c3d 00001eef 0000193e 0000358f 00001790 000002a0 00002c6b
0000538a 0000005b 00002449 0000468b 00004e14 0000633e 00007c5d 00005358
000022cf 000044e2 0000442f 000010e9 0000194a 0000092f 00006058 6083
% Key pair was generated at: 0:49:12 UTC julio 18 2025
Key name: R2.latam.cl.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
0000207f 00006abf 00004a58 000019b3 000025a0 00000692 00003d80 00001399
00004813 00005003 00002b0f 00005887 00000ebb 000000fa 0000399b 000037cb
00000279 00005a64 000053b2 000029c8 000051f2 000048e0 000009c2 3a4c
R2#show running-config | section line con 0
line con 0
  password redes
  login
R2#
```

Comprobación de funcionamiento de conexión por SSH con usuario y contraseña configurados localmente (username: R2 / password: test).

```
C:\>ssh -l R2 200.200.200.2

Password:

R2#
```

Comprobación de funcionamiento de contraseña establecida en línea consola (redes).

```
User Access Verification

Password:

R2>
```

R3

```
R3#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R3#show running-config | section line vty
line vty 0 4
 login local
 transport input ssh
R3#show running-config | include username
username R3 privilege 15 password 0 test
R3#show running-config | include domain-name
ip domain-name latam.cl
R3#show crypto key mypubkey rsa
% Key pair was generated at: 0:52:52 UTC julio 18 2025
Key name: R3.latam.cl
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00000128 00007ea3 00006a79 00006d95 00007618 000035fb 00007d3f 00001918
00001d52 00004344 00004bc2 00004cbd 00001e1b 00000200 00000f86 000037c6
0000173e 00005020 00003fc9 0000014c 00002cfe 00003428 00002f14 3f83
% Key pair was generated at: 0:52:52 UTC julio 18 2025
Key name: R3.latam.cl.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
00003350 00002e8f 00002711 0000743f 00004847 00003a64 0000769c 000032b7
000072d0 00004138 0000261c 00005289 0000199f 00000637 00004614 000053ff
00006669 00004c98 00000bf5 00005991 00006954 00003d38 00003137 5aab
R3#show running-config | section line con 0
line con 0
 password redes
 login
```

Comprobación de funcionamiento de conexión por SSH con usuario y contraseña configurados localmente (username: R3 / password: test).

```
C:\>ssh -l R3 10.1.2.1

Password:

R3#
```

Comprobación de funcionamiento de contraseña establecida en línea consola (redes).

```
User Access Verification

Password:

R3>
```

R4

```
R4#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R4#show running-config | section line vty
line vty 0 4
  login local
  transport input ssh
R4#show running-config | include username
username R4 privilege 15 password 0 test
R4#show running-config | include domain-name
ip domain-name latam.cl
R4#show crypto key mypubkey rsa
% Key pair was generated at: 0:55:11 UTC julio 18 2025
Key name: R4.latam.cl
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00002314 00002210 0000399e 000054e0 00003f05 000067c8 0000271a 00002ec6
00002f8c 00006bcf 00002974 00004ea9 0000644d 00007486 00006d9a 00006d92
000032c5 00003fcc 00003f02 000059ed 00005d38 00003e20 0000663e 2bd5
% Key pair was generated at: 0:55:11 UTC julio 18 2025
Key name: R4.latam.cl.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
000005eb 00000905 000055d1 00000e92 00006294 000018ab 00001941 00004360
0000440f 00007ccb 00003a6d 00004172 00004652 00001cd3 00001121 00001737
00003ca3 00004343 000030e8 000070dc 00002e09 00007857 00006921 6812
R4#show running-config | section line con 0
line con 0
  password redes
  login
R4#
```

Comprobación de funcionamiento de conexión por SSH con usuario y contraseña configurados localmente (username: R4 / password: test).

```
C:\>ssh -l R4 200.200.200.4

Password:

R4#
```

Comprobación de funcionamiento de contraseña establecida en línea consola (redes).

```
User Access Verification

Password:

R4>
```

En cuanto a direccionamiento, fue realizado de la siguiente forma:

LAN R1

Se configuraron subinterfaces dadas las VLANS nombradas en la topología.

```
R1#show running-config | begin interface GigabitEthernet0/0.  
interface GigabitEthernet0/0.10  
  description LAN_VLAN 10  
  encapsulation dot1Q 10  
  ip address 10.1.10.1 255.255.255.0  
!  
interface GigabitEthernet0/0.20  
  description LAN_VLAN 20  
  encapsulation dot1Q 20  
  ip address 10.1.20.1 255.255.255.0
```

Salida del comando: show ip int br

```
R1#show ip int br  
Interface          IP-Address      OK? Method Status        Protocol  
GigabitEthernet0/0 unassigned      YES unset  up            up  
GigabitEthernet0/0.10 10.1.10.1      YES manual  up            up  
GigabitEthernet0/0.20 10.1.20.1      YES manual  up            up  
GigabitEthernet0/1  200.200.200.1  YES manual  up            up  
Vlan1              unassigned      YES unset  administratively down down  
R1#
```

Configuración PC1_VLAN 10

IPv4 Address	10.1.10.30
Subnet Mask	255.255.255.0
Default Gateway	10.1.10.1
DNS Server	192.168.0.50

Configuración SYSLOG – VLAN 20

IPv4 Address	10.1.20.15
Subnet Mask	255.255.255.0
Default Gateway	10.1.20.1
DNS Server	192.168.0.50

LAN R2

Salida del comando: show ip int br

```
R2#show ip int br  
Interface          IP-Address      OK? Method Status        Protocol  
GigabitEthernet0/0 10.1.1.1        YES manual  up            up  
GigabitEthernet0/1 200.200.200.2   YES manual  up            up  
Vlan1              unassigned      YES unset  administratively down down  
R2#
```

Configuración SNMP

IPv4 Address	10.1.1.10
Subnet Mask	255.255.255.240
Default Gateway	10.1.1.1
DNS Server	192.168.0.50

LAN R3

Salida del comando: show ip int br

```
R3#show ip int br
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0       10.1.2.1        YES NVRAM    up          up
GigabitEthernet0/1       200.200.200.3   YES NVRAM    up          up
Vlan1                    unassigned      YES unset   administratively down down
R3#
```

Configuración PC2

IPv4 Address	10.1.2.10
Subnet Mask	255.255.255.224
Default Gateway	10.1.2.1
DNS Server	192.168.0.50

Configuración NTP

IPv4 Address	10.1.2.20
Subnet Mask	255.255.255.224
Default Gateway	10.1.2.1
DNS Server	192.168.0.50

Configuración Laptop Prueba AP

IPv4 Address	10.1.2.11
Subnet Mask	255.255.255.224
Default Gateway	10.1.2.1
DNS Server	192.168.0.50

LAN R4

Salida del comando: show ip int br

```
R4#show ip int br
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0       192.168.0.1     YES NVRAM    up          up
GigabitEthernet0/1       200.200.200.4   YES NVRAM    up          up
Vlan1                    unassigned      YES unset   administratively down down
R4#
```

Configuración HTTP/DNS – No olvidar que se pide NAT para la red a alguna ip del segmento 200.200.200.0/29.

IPv4 Address	192.168.0.50
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server	192.168.0.50

2. Configura SWITCH de topología con VLANS y asignación de puertas de acceso y troncales.

En el caso de la red LAN del Router R1, se nombraron la VLANS dadas en la topología, configurando sus respectivos puertos de acceso y la interfaz en modo troncal para poder realizar la configuración de router on a stick necesaria en este caso.

```
S1#show vlan br
```

VLAN	Name	Status	Ports
1	default	active	Fa0/21, Fa0/22, Fa0/23, Gig0/1 Gig0/2
10	VLAN0010	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10
20	VLAN0020	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
S1#
```

```
S1#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/24	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa0/24	1-1005			
Port	Vlans allowed and active in management domain			
Fa0/24	1,10,20			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa0/24	1,10,20			
S1#				

3. Implementación OSPF

Se tomaron en consideración los siguientes puntos:

- Configurar OSPFv2 con ID 500.
- Utilizar las subredes con su respectiva wildcard a nivel de IPv4.
- Habilitar interfaces pasivas en enlaces correspondiente.

R1

Fue configurado de la siguiente forma, tomando en cuenta los puntos a considerar descritos anteriormente.

```
R1#show running-config | begin router ospf
router ospf 500
  router-id 1.1.1.1
  log-adjacency-changes
  passive-interface GigabitEthernet0/0
  network 200.200.200.0 0.0.0.7 area 0
  network 10.1.10.0 0.0.0.255 area 0
  network 10.1.20.0 0.0.0.255 area 0
```

Se confirma adyacencia con los demás routers.

```
R1#show ip ospf neighbor

Neighbor ID    Pri   State           Dead Time   Address        Interface
3.3.3.3        1     FULL/BDR        00:00:35   200.200.200.3  GigabitEthernet0/1
4.4.4.4        1     FULL/DR         00:00:35   200.200.200.4  GigabitEthernet0/1
2.2.2.2        1     2WAY/DROTHER    00:00:35   200.200.200.2  GigabitEthernet0/1
R1#
```

Se conocen redes remotas en la tabla de enrutamiento del router, gracias a OSPF.

```
R1#show ip route ospf
 10.0.0.0/8 is variably subnetted, 6 subnets, 4 masks
O       10.1.1.0 [110/2] via 200.200.200.2, 00:31:56, GigabitEthernet0/1
O       10.1.2.0 [110/2] via 200.200.200.3, 00:31:56, GigabitEthernet0/1
O      192.168.0.0 [110/2] via 200.200.200.4, 00:31:56, GigabitEthernet0/1
R1#
```

R2

Fue configurado de la siguiente forma, tomando en cuenta los puntos a considerar descritos anteriormente.

```
R2#show running-config | begin router ospf
router ospf 500
  router-id 2.2.2.2
  log-adjacency-changes
  passive-interface GigabitEthernet0/0
  network 200.200.200.0 0.0.0.7 area 0
  network 10.1.1.0 0.0.0.15 area 0
```


Se confirma adyacencia con los demás routers.

```
R2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/BDR	00:00:33	200.200.200.3	GigabitEthernet0/1
4.4.4.4	1	FULL/DR	00:00:33	200.200.200.4	GigabitEthernet0/1
1.1.1.1	1	2WAY/DROTHER	00:00:33	200.200.200.1	GigabitEthernet0/1

```
R2#
```

Se conocen redes remotas en la tabla de enrutamiento del router, gracias a OSPF.

```
R2#show ip route ospf
```

10.0.0.0/8 is variably subnetted, 5 subnets, 4 masks

Destination	Administrative Distance	Next Hop	Interface
10.1.2.0 [110/2]	via 200.200.200.3	00:34:53	GigabitEthernet0/1
10.1.10.0 [110/2]	via 200.200.200.1	00:34:53	GigabitEthernet0/1
10.1.20.0 [110/2]	via 200.200.200.1	00:34:53	GigabitEthernet0/1
192.168.0.0 [110/2]	via 200.200.200.4	00:34:53	GigabitEthernet0/1

```
R2#
```

R3

Fue configurado de la siguiente forma, tomando en cuenta los puntos a considerar descritos anteriormente.

```
R3#show running-config | begin router ospf
router ospf 500
  router-id 3.3.3.3
  log-adjacency-changes
  passive-interface GigabitEthernet0/0
  network 200.200.200.0 0.0.0.7 area 0
  network 10.1.2.0 0.0.0.31 area 0
```

Se confirma adyacencia con los demás routers.

```
R3#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
4.4.4.4	1	FULL/DR	00:00:39	200.200.200.4	GigabitEthernet0/1
1.1.1.1	1	FULL/DROTHER	00:00:39	200.200.200.1	GigabitEthernet0/1
2.2.2.2	1	FULL/DROTHER	00:00:39	200.200.200.2	GigabitEthernet0/1

```
R3#
```

Se conocen redes remotas en la tabla de enrutamiento del router, gracias a OSPF.

```
R3#show ip route ospf
```

10.0.0.0/8 is variably subnetted, 5 subnets, 4 masks

Destination	Administrative Distance	Next Hop	Interface
10.1.1.0 [110/2]	via 200.200.200.2	00:36:26	GigabitEthernet0/1
10.1.10.0 [110/2]	via 200.200.200.1	00:36:26	GigabitEthernet0/1
10.1.20.0 [110/2]	via 200.200.200.1	00:36:26	GigabitEthernet0/1
192.168.0.0 [110/2]	via 200.200.200.4	00:36:36	GigabitEthernet0/1

```
R3#
```

R4

Fue configurado de la siguiente forma, tomando en cuenta los puntos a considerar descritos anteriormente.

```
R4#show running-config | begin router ospf
router ospf 500
  router-id 4.4.4.4
  log-adjacency-changes
  passive-interface GigabitEthernet0/0
  network 200.200.200.0 0.0.0.7 area 0
  network 192.168.0.0 0.0.0.255 area 0
```

Se confirma adyacencia con los demás routers.

```
R4#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/BDR	00:00:33	200.200.200.3	GigabitEthernet0/1
1.1.1.1	1	FULL/DROTHER	00:00:34	200.200.200.1	GigabitEthernet0/1
2.2.2.2	1	FULL/DROTHER	00:00:34	200.200.200.2	GigabitEthernet0/1

```
R4#
```

Se conocen redes remotas en la tabla de enrutamiento del router, gracias a OSPF.

```
R4#show ip route ospf
      10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O       10.1.1.0 [110/2] via 200.200.200.2, 01:04:28, GigabitEthernet0/1
O       10.1.2.0 [110/2] via 200.200.200.3, 01:04:28, GigabitEthernet0/1
O       10.1.10.0 [110/2] via 200.200.200.1, 01:04:28, GigabitEthernet0/1
O       10.1.20.0 [110/2] via 200.200.200.1, 01:04:28, GigabitEthernet0/1
R4#
```

4. Configuración de NAT

En este punto la IP principal del servidor 192.168.0.50 será conocida por la dirección IP 200.200.200.5. Asegura que 192.168.0.50 siempre se vea como 200.200.200.5 para el acceso, lo cual es crucial para aplicaciones que requieren una dirección pública fija, mientras que la red en sí sigue siendo privada.

int g0/0

ip nat inside

exit

int g0/1

ip nat outside

exit

ip nat inside source static 192.168.0.50 200.200.200.5

Se hacen pruebas de ping hacia la dirección IP “pública” declarada para el servidor web, el cual resulta exitoso y la dirección IP es reconocida.

```
C:\>ping 200.200.200.5

Pinging 200.200.200.5 with 32 bytes of data:

Reply from 200.200.200.5: bytes=32 time=35ms TTL=126
Reply from 200.200.200.5: bytes=32 time=17ms TTL=126
Reply from 200.200.200.5: bytes=32 time=39ms TTL=126
Reply from 200.200.200.5: bytes=32 time=10ms TTL=126

Ping statistics for 200.200.200.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 39ms, Average = 25ms

C:\>ipconfig

Wireless0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::20A:F3FF:FE90:CC3E
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 10.1.2.11
    Subnet Mask . . . . .: 255.255.255.224
    Default Gateway . . . . .: ::
                               10.1.2.1
```

Al revisar con el comando show ip nat translations, se ve el detalle del enrutamiento NAT, en el cual se ve la dirección pública y privada del servidor y también la dirección IP desde donde se hizo la consulta, en este caso, la 10.1.2.11.

```
R4#show ip nat translations
Pro Inside global   Inside local   Outside local  Outside global
icmp 200.200.200.5:12 192.168.0.50:12 10.1.2.11:12 10.1.2.11:12
icmp 200.200.200.5:13 192.168.0.50:13 10.1.2.11:13 10.1.2.11:13
icmp 200.200.200.5:14 192.168.0.50:14 10.1.2.11:14 10.1.2.11:14
udp 200.200.200.5:123 192.168.0.50:123 10.1.2.20:123 10.1.2.20:123
--- 200.200.200.5    192.168.0.50    ---          ---
R4#
```

De la misma forma al abrir la dirección URL en el navegador.



Arroja lo siguiente:

```
R4#show ip nat translations
Pro Inside global   Inside local   Outside local  Outside global
udp 200.200.200.5:123 192.168.0.50:123 10.1.2.20:123 10.1.2.20:123
udp 200.200.200.5:53 192.168.0.50:53 10.1.2.11:1026 10.1.2.11:1026
udp 200.200.200.5:53 192.168.0.50:53 10.1.2.11:1027 10.1.2.11:1027
udp 200.200.200.5:53 192.168.0.50:53 10.1.2.11:1028 10.1.2.11:1028
udp 200.200.200.5:53 192.168.0.50:53 10.1.2.11:1029 10.1.2.11:1029
--- 200.200.200.5    192.168.0.50    ---          ---
tcp 200.200.200.5:80 192.168.0.50:80 10.1.2.11:1029 10.1.2.11:1029
tcp 200.200.200.5:80 192.168.0.50:80 10.1.2.11:1030 10.1.2.11:1030
R4#
```

5. Monitoreo Integrado – NTP, SYSLOG y SNMP

NTP

Primeramente, se debe tener en consideración la dirección IP del servidor, en este caso es la 10.1.2.20/27. Ya con la dirección IP conocida, se debe declarar en cada router para sincronizar la hora y fecha dada por el servidor.

Comando utilizado: **(CONFIG)# ntp server 10.1.2.20**

```
R1(config)#ntp server 10.1.2.20
R1(config)#exit
R1#
*Jul 18, 13:36:25.3636: SYS-5-CONFIG_I: Configured from console by
console
R1#show ntp s
R1#show ntp status
Clock is synchronized, stratum 2, reference is 10.1.2.20
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision
is 2**24
reference time is EBFA9C57.00000301 (13:36:23.769 UTC Fri Jul 18
2025)
clock offset is 4.00 msec, root delay is 10.00 msec
root dispersion is 10.17 msec, peer dispersion is 0.00 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -
0.000001193 s/s system poll interval is 4, last update was 6 sec
ago.
R1#
R2#show ntp status
Clock is synchronized, stratum 2, reference is 10.1.2.20
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision
is 2**24
reference time is EBFA9DF7.000001CC (13:43:19.460 UTC Fri Jul 18
2025)
clock offset is 1.00 msec, root delay is 4.00 msec
root dispersion is 10.63 msec, peer dispersion is 0.00 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -
0.000001193 s/s system poll interval is 6, last update was 4 sec
ago.
R3#show ntp status
Clock is synchronized, stratum 2, reference is 10.1.2.20
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision
is 2**24
reference time is EBFAA4F2.00000223 (14:13:6.547 UTC Fri Jul 18
2025)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 13.38 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -
0.000001193 s/s system poll interval is 4, last update was 9 sec
ago.
R3#
R4#show ntp status
Clock is synchronized, stratum 2, reference is 10.1.2.20
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision
is 2**24
reference time is EBFAA4E2.000001F0 (14:12:50.496 UTC Fri Jul 18
2025)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 13.14 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -
0.000001193 s/s system poll interval is 4, last update was 5 sec
ago.
R4#
```

En todos los routers se veía la siguiente salida del comando **show ntp associations**.

```
R3#show ntp associations
address      ref clock    st  when    poll    reach  delay      offset      disp
*~10.1.2.20  127.127.1.1  1   27      32     377    0.00      1.00      0.24
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R3#
```

SYSLOG

El objetivo principal de Syslog es centralizar los logs. En lugar de tener que conectarte a cada dispositivo individualmente para ver sus registros, todos los mensajes se envían a un solo lugar. En este caso, tenemos un servidor dedicado con la dirección IP 10.1.20.15.

La configuración es la siguiente, se debe replicar en todos los routers, según lo indicado.

```
R1#show running-config | begin logging
logging trap debugging
logging 10.1.20.15
```

```
R2#show running-config | begin logging
logging trap debugging
logging 10.1.20.15
```

```
R3#show running-config | begin logging
logging trap debugging
logging 10.1.20.15
```

```
R4#show running-config | begin logging
logging trap debugging
logging 10.1.20.15
```

Confirma que cada router está enviando sus logs al servidor Syslog con la dirección IP 10.1.20.15. Además, se indica que el router está configurado para enviar mensajes con un nivel de severidad de "debugging" (nivel 7) y todos los niveles inferiores (0 al 7) al servidor SYSLOG.

Un ejemplo:

Syslog

Service ☒ On ☐ Off

	Time	HostName	Message
1	07.18.2025 02:30:56.221 PM	10.1.20.1	14:30:56: %OSPF-5-ADJCHG: ...
2	07.18.2025 02:30:56.219 PM	10.1.20.1	14:30:56: %OSPF-5-ADJCHG: ...
3	07.18.2025 02:30:22.472 PM	10.1.20.1	%SYS-5-CONFIG_: Configured from console by console

```
R1(config)#no logging trap debugging
R1(config)#logging
R1(config)#logging tr
R1(config)#logging trap de
R1(config)#logging trap debugging
R1(config)#
*Jul 18, 14:30:56.3030: 14:30:56: %OSPF-5-ADJCHG: Process 500, Nbr
4.4.4.4 on GigabitEthernet0/1 from LOADING to FULL, Loading Done
*Jul 18, 14:30:56.3030: 14:30:56: %OSPF-5-ADJCHG: Process 500, Nbr
3.3.3.3 on GigabitEthernet0/1 from LOADING to FULL, Loading Done
```

Copy Paste

Syslog

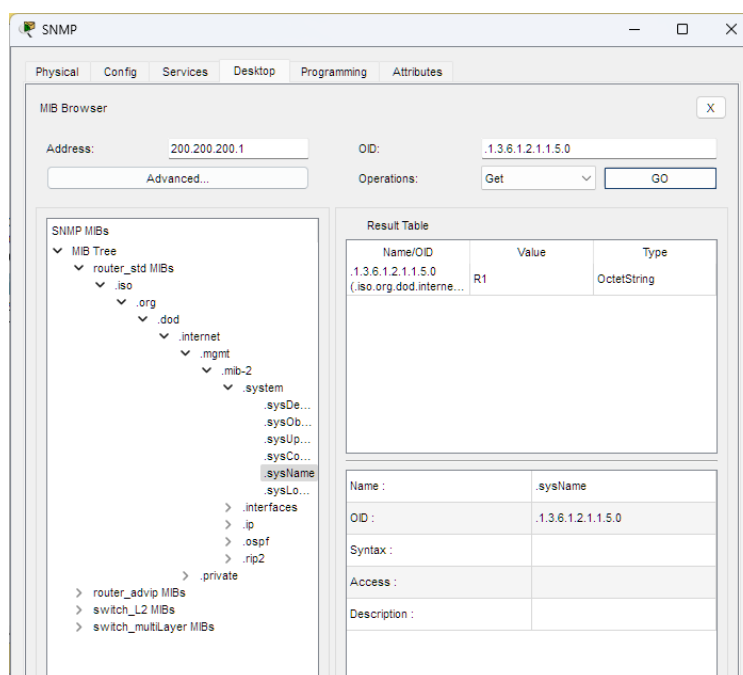
Service ☒ On ☐ Off

	Time	HostName	Message
1	07.18.2025 02:09:56.018 PM	10.1.20.1	14:09:56: %OSPF-5-...
2	07.18.2025 02:13:12.875 PM	200.200.200.3	%SYS-5-CONFIG_: Configured from console b...
3	07.18.2025 02:27:37.879 PM	10.1.20.1	%SYS-5-CONFIG_: Configured from console b...
4	07.18.2025 02:30:22.472 PM	10.1.20.1	%SYS-5-CONFIG_: Configured from console b...
5	07.18.2025 02:30:56.219 PM	10.1.20.1	14:30:56: %OSPF-5-...
6	07.18.2025 02:30:56.221 PM	10.1.20.1	14:30:56: %OSPF-5-...
7	07.18.2025 02:38:34.104 PM	10.1.20.1	%SYS-5-CONFIG_: Configured from console b...
8	07.18.2025 02:38:50.985 PM	200.200.200.4	%SYS-5-CONFIG_: Configured from console b...
9	07.18.2025 02:39:57.681 PM	200.200.200.2	%SYS-5-CONFIG_: Configured from console b...
10	07.18.2025 02:39:57.681 PM	200.200.200.2	: %SYS-6-LOGGINGHOST_STARTST...
11	07.18.2025 02:40:43.988 PM	200.200.200.3	%SYS-5-CONFIG_: Configured from console b...
12	07.18.2025 02:40:43.988 PM	200.200.200.3	: %SYS-6-LOGGINGHOST_STARTST...

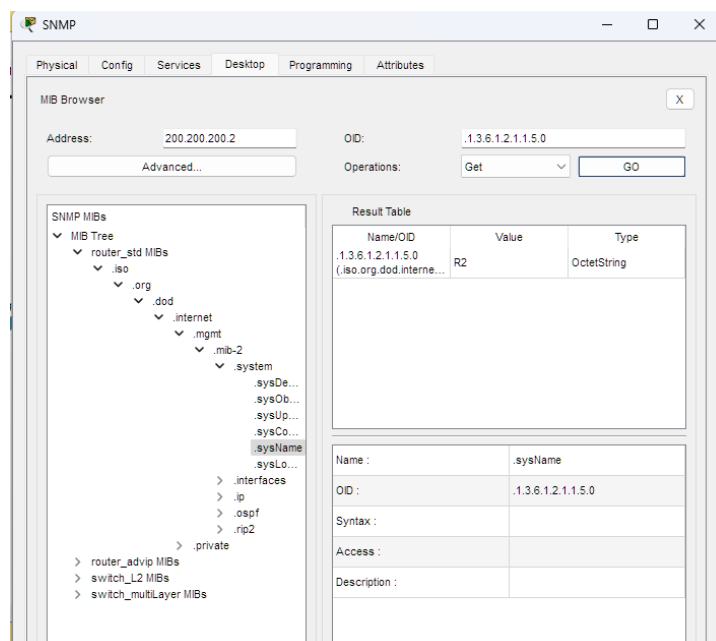
SNMP

Protocolo de capa de aplicación que se utiliza para gestionar y monitorear dispositivos de red de manera centralizada y remota. En este requerimiento vemos que en base a la configuración del nombre de la comunidad y la dirección IP enlazada a alguna interfaz del router (snmp-server **community** **SNMP_[NOMBRE_ROUTER]** rw) podemos obtener el nombre del dispositivo y monitorear diversos parametros.

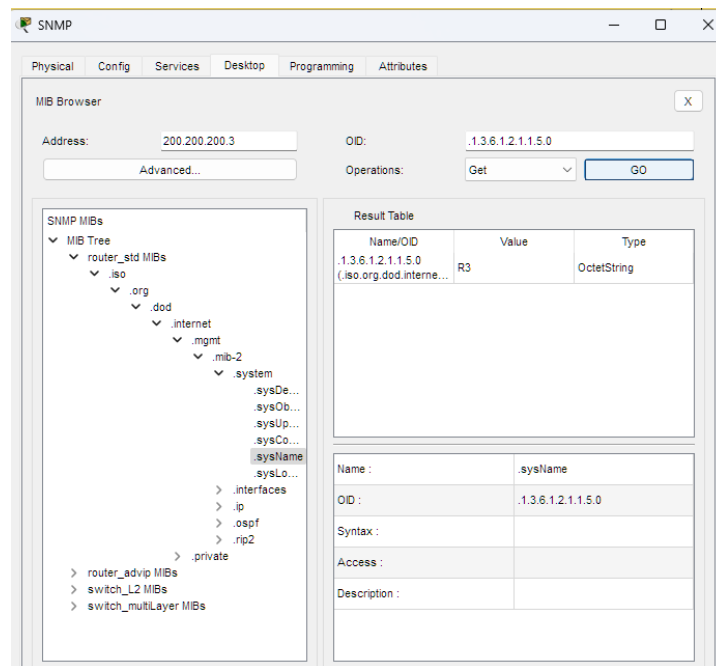
R1



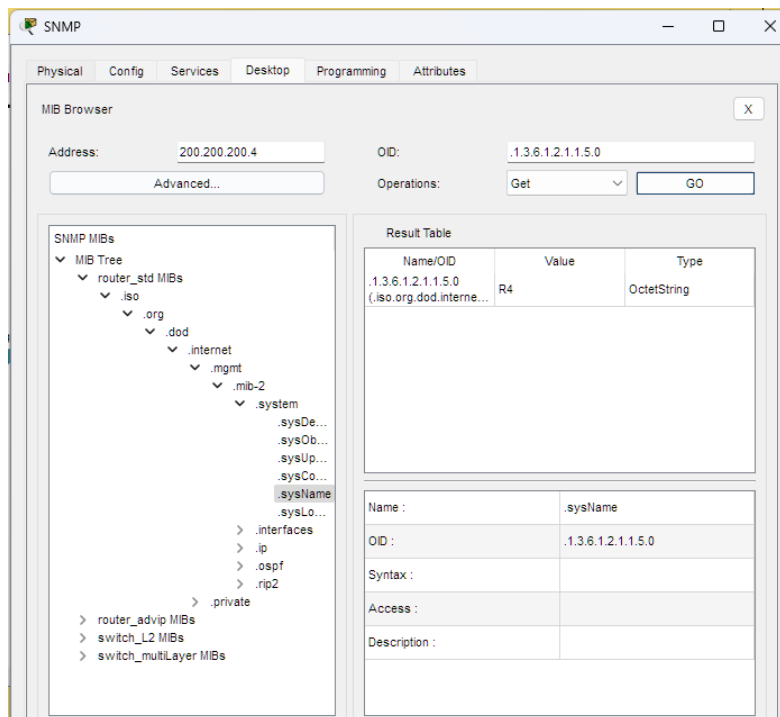
R2



R3



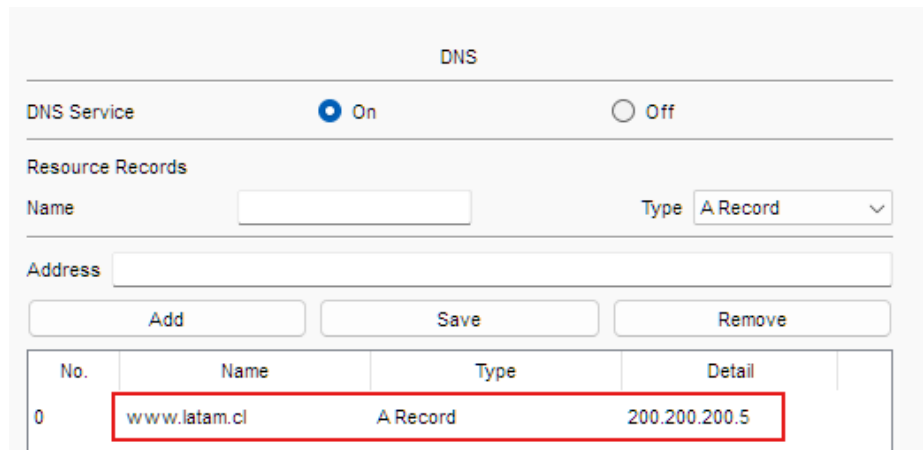
R4



6. Verificación de conectividad y acceso WEB al servidor de la topología.

Servidor WEB : 200.200.200.5 / WWW.LATAM.CL

Se muestra la configuración DNS del servidor, para poder resolver direcciones IP.



DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type A Record

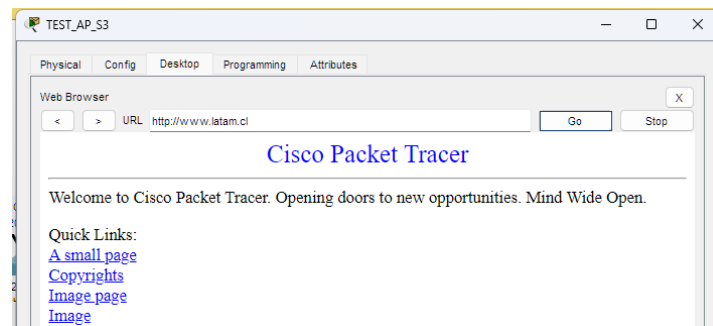
Address

Add Save Remove

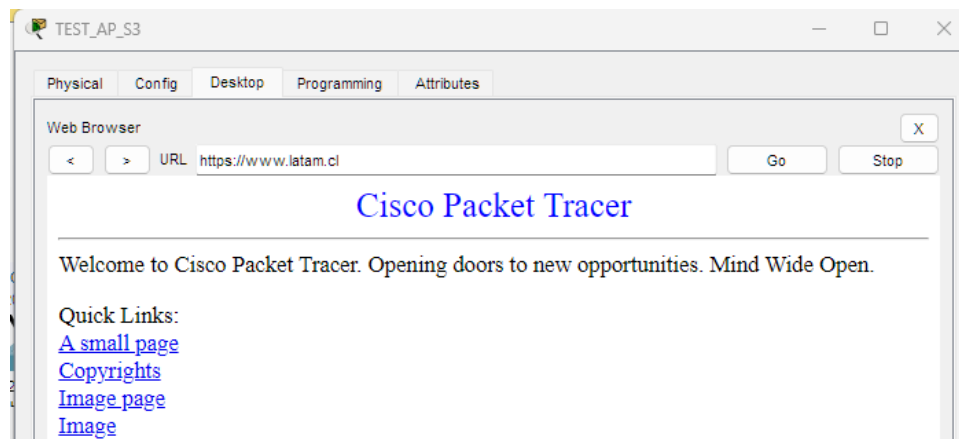
No.	Name	Type	Detail
0	www.latam.cl	A Record	200.200.200.5

Desde una LAPTOP conectada al AP, vemos que la navegación no presenta problemas:

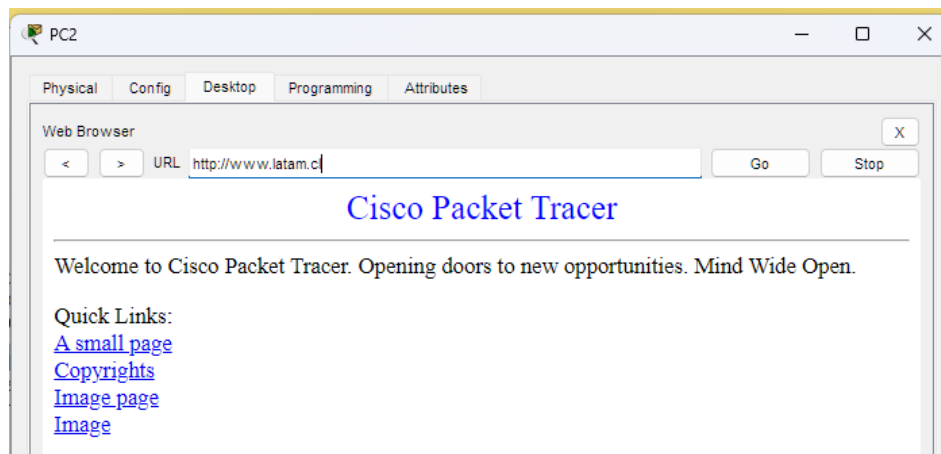
HTTP : Puerto 80



HTTPS : Puerto 443



Desde PC2 hacia el servidor web, antes de implementar ACL:



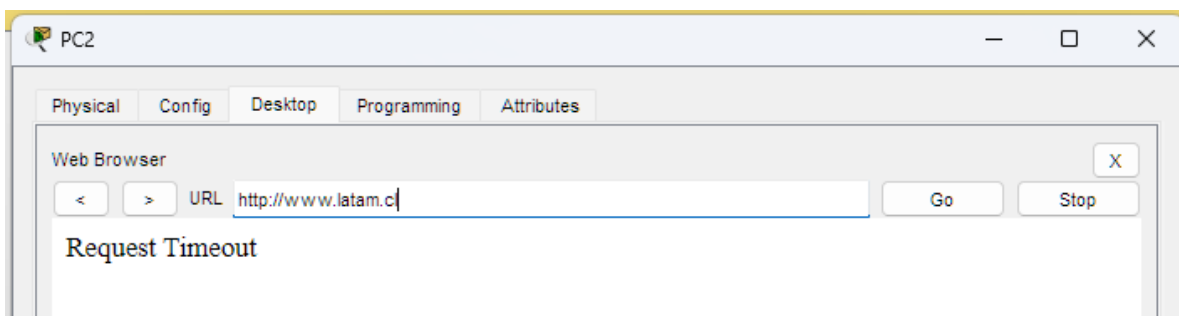
7. Implementación ACL para restringir el acceso al servidor WEB

La configuración de la ACL fue realizada en el R3, puerta de acceso del PC2 en este caso y se declaró en la interfaz G0/0 para filtrar el tráfico entrante en la interfaz y proveniente de este dispositivo.

```
R3#show access-lists
Extended IP access list 101
 10 deny tcp host 10.1.2.10 host 200.200.200.5 eq www
 20 deny tcp host 10.1.2.10 host 200.200.200.5 eq 443
 30 permit ip any any (20 match(es))
```

La ACL nos dice que deniega todo tráfico HTTP/HTTPS hacia el servidor, pero permite el demás tráfico, más que nada para no perder conectividad con la demás red.

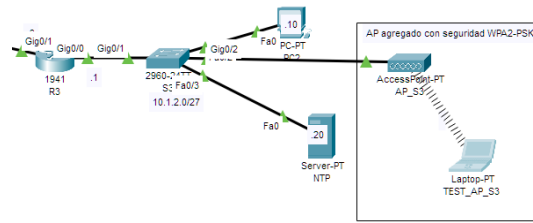
Verificación de ACL:



Concordó con la regla declarada y la ACL se mostró así:

```
R3#show access-lists
Extended IP access list 101
 10 deny tcp host 10.1.2.10 host 200.200.200.5 eq www (9 match(es))
 20 deny tcp host 10.1.2.10 host 200.200.200.5 eq 443
 30 permit ip any any (31 match(es))
```

8. Implementación de equipamiento inalámbrico con seguridad WPA2



Port 1

Port Status ☒ On

SSID AP_S3

2.4 GHz Channel 6

Coverage Range (meters) 140,00

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

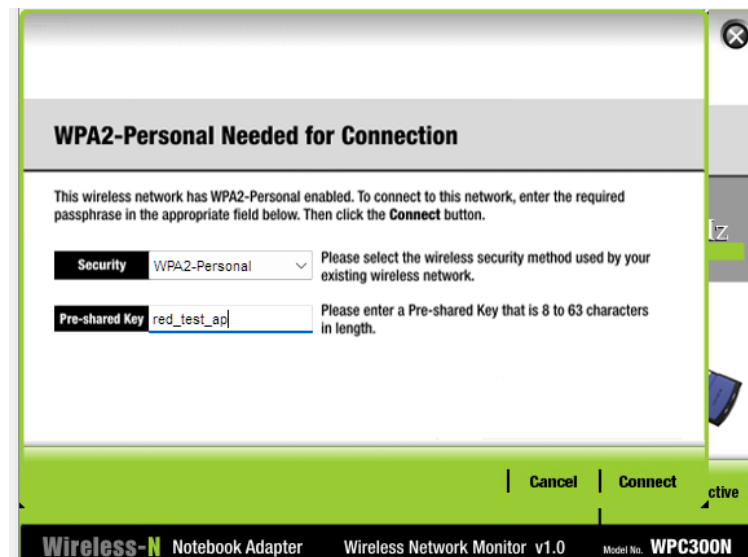
WEP Key

PSK Pass Phrase red_test_ap

User ID

Password

Encryption Type AES



Funcionando OK

