UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

CNO V: SEGURIDAD INFORMATICA

ACTIVIDAD 06 - IMPLEMENTACIÓN IPSEC VPN

Moreno Solís Gisela Geraldine 176522

Introducción

En el presente trabajo se implementó una VPN IPSec Site-to-Site utilizando routers Cisco en un entorno simulado mediante Packet Tracer. El objetivo fue establecer una comunicación segura entre dos redes privadas remotas a través de una red pública, garantizando confidencialidad, integridad y autenticación del tráfico mediante el protocolo IPSec.

La práctica permitió aplicar conceptos de enrutamiento, listas de acceso (ACL), criptografía y configuración de túneles seguros entre dispositivos de red.

Objetivo

Implementar una VPN IPSec Site-to-Site entre dos redes privadas (192.168.1.0/24 y 192.168.3.0/24), permitiendo la comunicación cifrada entre ambas a través de una red pública simulada.

Topología de Red

IPSec (Internet Protocol Security) es un conjunto de protocolos que operan en la Capa 3 del modelo OSI, diseñados para proporcionar seguridad en comunicaciones IP. IPSec garantiza:

- Confidencialidad (mediante cifrado)
- Integridad (mediante algoritmos hash)
- Autenticación (verificación de identidad entre pares)

El establecimiento del túnel se realiza en dos fases:

Fase 1 – IKE / ISAKMP

En esta fase se negocian los parámetros criptográficos y se establece un canal seguro para intercambiar claves. Se define:

- Algoritmo de cifrado
- Algoritmo hash
- Método de autenticación
- Grupo Diffie-Hellman
- Tiempo de vida de la sesión

Fase 2 – IPSec

Se define el tráfico interesante que será cifrado mediante una ACL y se establece el túnel seguro utilizando un transform-set.

Diseño de Red

La topología implementada consta de:

- Router R1 (Sitio A)
- Router ISP (Red pública simulada)
- Router R2 (Sitio B)
- Dos redes LAN privadas

Direccionamiento IP

Sitio A

- R1 G0/1 → 192.168.1.1/24
- R1 G0/0 → 209.165.100.1/30

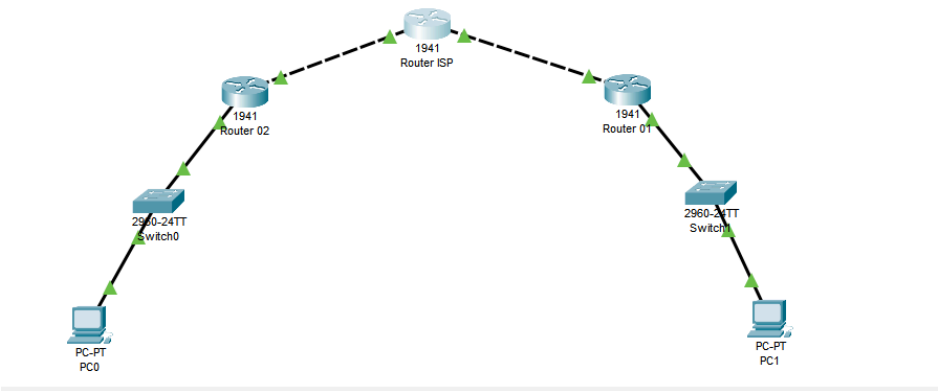
ISP

- G0/0 → 209.165.100.2/30
- G0/1 → 209.165.200.2/30

Sitio B

- R2 G0/0 → 209.165.200.1/30
- R2 G0/1 → 192.168.3.1/24

El diseño permite que ambas redes privadas se comuniquen a través de un enlace WAN simulando Internet.



Implementación Técnica

Configuración de Enrutamiento

Se configuraron rutas estáticas para garantizar conectividad entre routers antes de implementar IPSec.

Router ISP

- enable
- conf t
- hostname ISP
- interface G0/0
- ip address 209.165.100.2 255.255.255.0
- no shut
- interface G0/0
- ip address 209.165.200.2 255.255.255.0
- no shut
- ip route 0.0.0.0 0.0.0.0 209.165.100.2

Router 1 -

- enable
- conf t
- hostname R1
- interface G0/1
- ip address 192.168.1.1 255.255.255.0
- no shut
- interface G0/0
- ip address 209.165.100.1 255.255.255.0
- no shut
- ip route 0.0.0.0 0.0.0.0 209.165.100.2

Router 2

- enable
- configure terminal
- hostname R2
- interface g0/1
- ip address 192.168.3.1 255.255.255.0
- no shutdown
- interface g0/0
- ip address 209.165.200.1 255.255.255.252
- no shutdown
- ip route 0.0.0.0 0.0.0.0 209.165.200.2

Habilitación de Licencia de Seguridad

En cada router se habilitó el paquete de seguridad:

```
license boot module c1900 technology-package securityk9
exit
copy running-config startup-config
reload
```

Posteriormente se verificó con:

```
show version
```

Esto permite habilitar funcionalidades criptográficas necesarias para IPSec.

Implementación de ACL

Las Listas de Control de Acceso (ACL) definen el tráfico interesante que será protegido por IPSec.

En R1

```
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

En R2 (inversa)

```
access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

La ACL debe estar invertida en cada extremo para que el tráfico coincida correctamente durante la negociación.

Phase 1 – ISAKMP Policy

En esta fase se establecen los parámetros criptográficos para la negociación IKE.

En R1

```
crypto isakmp policy 10
 encryption aes 256
 hash sha
 authentication pre-share
 group 5
 lifetime 86400
```

```
exit

crypto isakmp key secretkey address 209.165.200.1
```

En R2

```
crypto isakmp policy 10
 encryption aes 256
 hash sha
 authentication pre-share
 group 5
 lifetime 86400
exit

crypto isakmp key secretkey address 209.165.100.1
```

Esta fase protege únicamente el canal de negociación inicial.

Phase 2 – IPSec Transform-Set

En esta fase se define el método de cifrado del tráfico de datos.

R1

```
crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
```

R2

```
crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
```

Aquí se cifra tanto encabezado como carga útil del paquete IP.

Creación del Crypto Map

En R1

```
crypto map IPSEC-MAP 10 ipsec-isakmp

 set peer 209.165.200.1

 set transform-set VPN-SET

 set pfs group5

 match address 100
```

En R2

```
crypto map IPSEC-MAP 10 ipsec-isakmp
 set peer 209.165.100.1
 set transform-set VPN-SET
 set pfs group5
 set security-association lifetime seconds 86400
 match address 100
```

El crypto map enlaza:

- Peer remoto
- Transform-set
- ACL
- Parámetros adicionales de seguridad

Aplicación del Crypto Map

En R1

```
interface g0/0
 crypto map IPSEC-MAP
```

En R2

```
interface g0/0
 crypto map IPSEC-MAP
```

El mapa debe aplicarse en la interfaz pública (WAN).

Verificación del Túnel

Se verificó el estado con:

```
show crypto isakmp sa
```

Estado esperado:

```
QM_IDLE
```

Se validó el tráfico cifrado con:

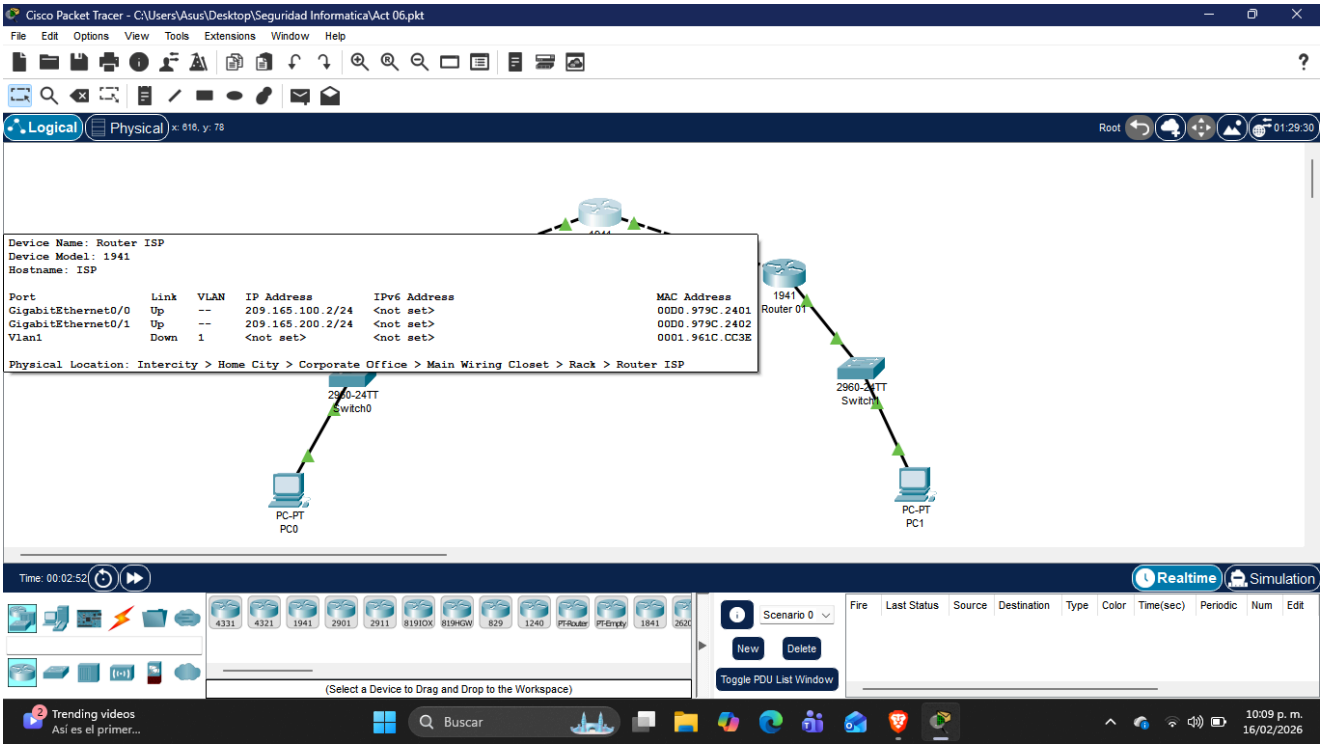
```
show crypto ipsec sa
```

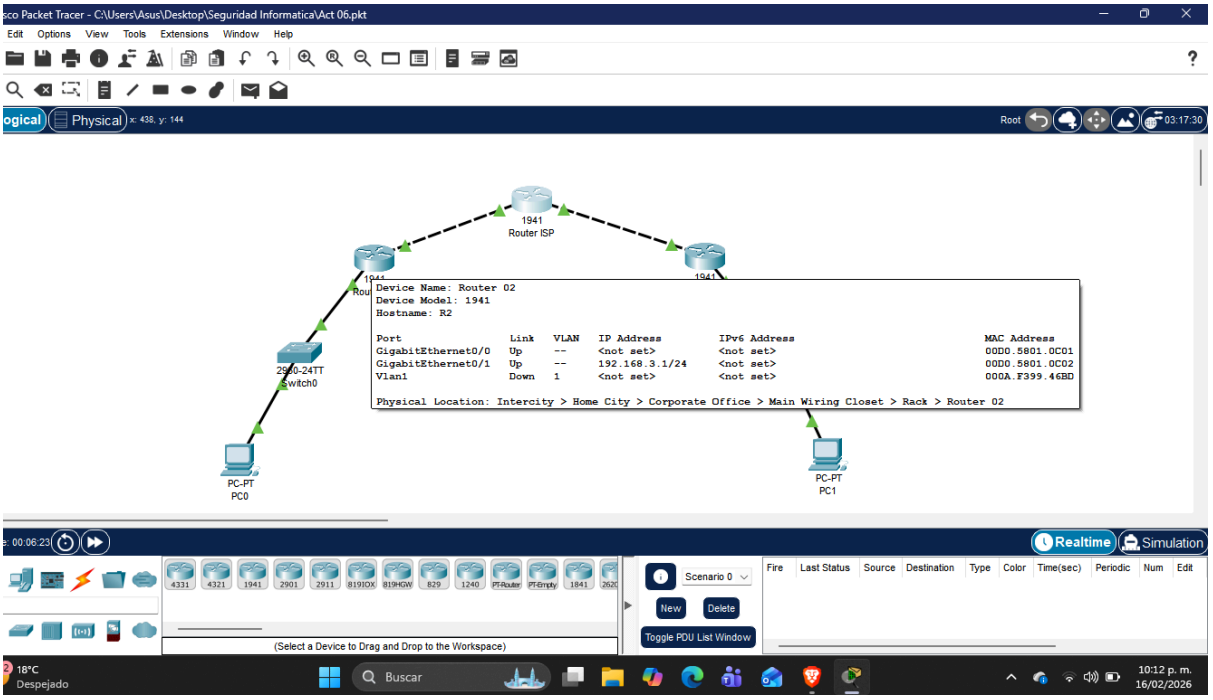
Finalmente se realizó prueba ICMP entre LANs confirmando comunicación segura.

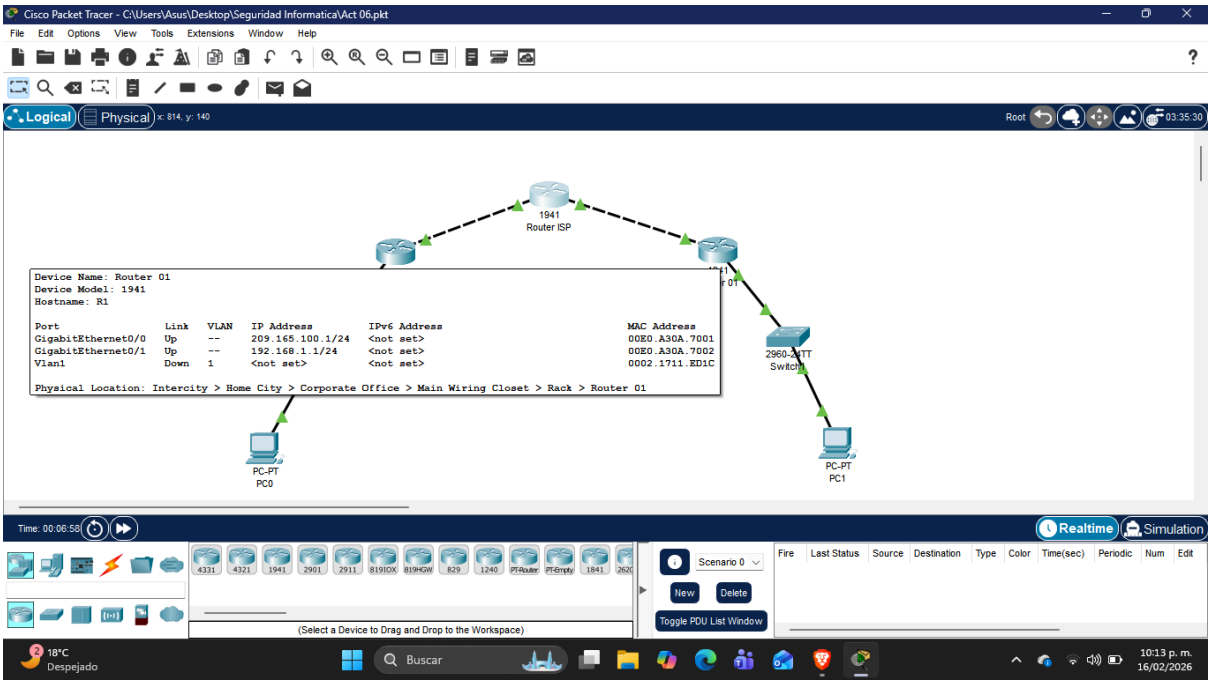
Conclusión Técnica

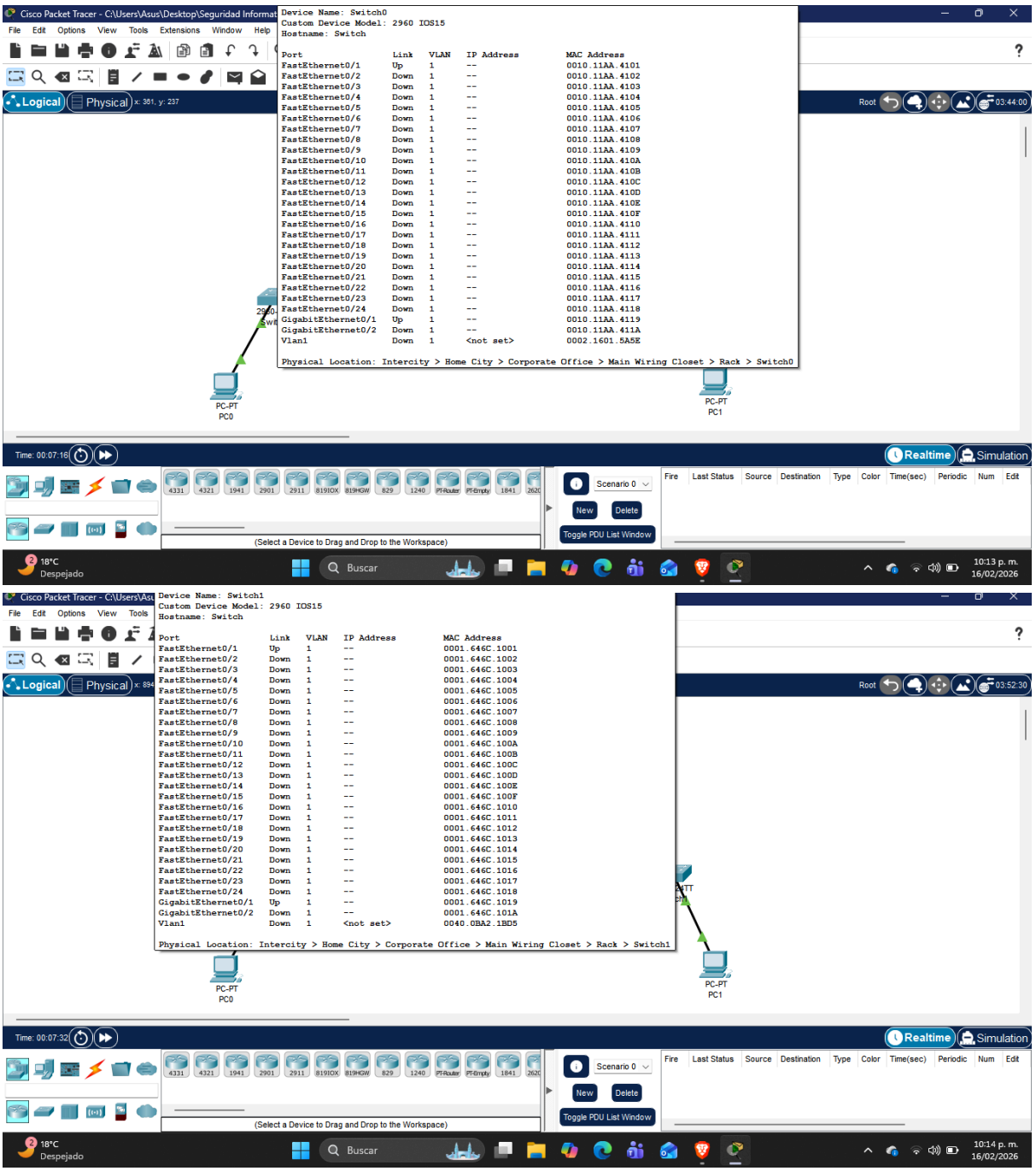
La implementación de la VPN IPSec Site-to-Site fue exitosa, garantizando confidencialidad, integridad y autenticación del tráfico entre redes privadas remotas. Se validó la correcta negociación IKE, establecimiento del túnel IPSec y transmisión cifrada de datos.

La arquitectura implementada es adecuada para entornos empresariales básicos y puede mejorarse mediante IKEv2, autenticación basada en certificados y mecanismos de redundancia.




Cisco Packet Tracer - C:\Users\Asus\Desktop\Seguridad Informatica\Act 06.pkt
Edit Options View Tools Extensions Window Help
Physical
Root
1941
Router ISP
Device Name: Router 02
Device Model: 1941
Hostname: R2
Port Link VLAN IP Address IPv6 Address MAC Address
GigabitEthernet0/0 Up -- <not set> <not set> 00D0.5801.0C01
GigabitEthernet0/1 Up -- 192.168.3.1/24 <not set> 00D0.5801.0C02
Vlan1 Down 1 <not set> <not set> 000A.F399.46BD
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router 02
2960-24TT
Switch0
PC-PT
PC0
PC-PT
PC1
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
(Select a Device to Drag and Drop to the Workspace)
Buscar
10:12 p. m.
16/02/2026


Cisco Packet Tracer - C:\Users\Asus\Desktop\Seguridad Informatica\Act 06.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
Root
1941
Router ISP
Device Name: Router 01
Device Model: 1941
Hostname: R1
Port Link VLAN IP Address IPv6 Address MAC Address
GigabitEthernet0/0 Up -- 209.165.100.1/24 <not set> 00E0.A30A.7001
GigabitEthernet0/1 Up -- 192.168.1.1/24 <not set> 00E0.A30A.7002
Vlan1 Down 1 <not set> <not set> 0002.1711.ED1C
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router 01
2960-24TT
Switch1
PC-PT
PC0
PC-PT
PC1
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
(Select a Device to Drag and Drop to the Workspace)
Buscar
10:13 p. m.
16/02/2026


Cisco Packet Tracer - C:\Users\Asus\Desktop\Seguridad Informat
File Edit Options View Tools Extensions Window Help
Logical Physical
Root
Device Name: Switch0
Custom Device Model: 2960 IOS15
Hostname: Switch
Port Link VLAN IP Address MAC Address
FastEthernet0/1 Up 1 -- 0010.11AA.4101
FastEthernet0/2 Down 1 -- 0010.11AA.4102
FastEthernet0/3 Down 1 -- 0010.11AA.4103
FastEthernet0/4 Down 1 -- 0010.11AA.4104
FastEthernet0/5 Down 1 -- 0010.11AA.4105
FastEthernet0/6 Down 1 -- 0010.11AA.4106
FastEthernet0/7 Down 1 -- 0010.11AA.4107
FastEthernet0/8 Down 1 -- 0010.11AA.4108
FastEthernet0/9 Down 1 -- 0010.11AA.4109
FastEthernet0/10 Down 1 -- 0010.11AA.410A
FastEthernet0/11 Down 1 -- 0010.11AA.410B
FastEthernet0/12 Down 1 -- 0010.11AA.410C
FastEthernet0/13 Down 1 -- 0010.11AA.410D
FastEthernet0/14 Down 1 -- 0010.11AA.410E
FastEthernet0/15 Down 1 -- 0010.11AA.410F
FastEthernet0/16 Down 1 -- 0010.11AA.4110
FastEthernet0/17 Down 1 -- 0010.11AA.4111
FastEthernet0/18 Down 1 -- 0010.11AA.4112
FastEthernet0/19 Down 1 -- 0010.11AA.4113
FastEthernet0/20 Down 1 -- 0010.11AA.4114
FastEthernet0/21 Down 1 -- 0010.11AA.4115
FastEthernet0/22 Down 1 -- 0010.11AA.4116
FastEthernet0/23 Down 1 -- 0010.11AA.4117
FastEthernet0/24 Down 1 -- 0010.11AA.4118
GigabitEthernet0/1 Up 1 -- 0010.11AA.4119
GigabitEthernet0/2 Down 1 -- 0010.11AA.411A
Vlan1 Down 1 <not set> 0002.1601.5A5E
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch0
PC-PT PC0
PC-PT PC1
Time: 00:07:18
Realtime Simulation
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit
18°C Despejado
Buscar
10:13 p. m. 16/02/2026

Cisco Packet Tracer - C:\Users\Asu
File Edit Options View Tools
Logical Physical
Root
Device Name: Switch1
Custom Device Model: 2960 IOS15
Hostname: Switch
Port Link VLAN IP Address MAC Address
FastEthernet0/1 Up 1 -- 0001.646C.1001
FastEthernet0/2 Down 1 -- 0001.646C.1002
FastEthernet0/3 Down 1 -- 0001.646C.1003
FastEthernet0/4 Down 1 -- 0001.646C.1004
FastEthernet0/5 Down 1 -- 0001.646C.1005
FastEthernet0/6 Down 1 -- 0001.646C.1006
FastEthernet0/7 Down 1 -- 0001.646C.1007
FastEthernet0/8 Down 1 -- 0001.646C.1008
FastEthernet0/9 Down 1 -- 0001.646C.1009
FastEthernet0/10 Down 1 -- 0001.646C.100A
FastEthernet0/11 Down 1 -- 0001.646C.100B
FastEthernet0/12 Down 1 -- 0001.646C.100C
FastEthernet0/13 Down 1 -- 0001.646C.100D
FastEthernet0/14 Down 1 -- 0001.646C.100E
FastEthernet0/15 Down 1 -- 0001.646C.100F
FastEthernet0/16 Down 1 -- 0001.646C.1010
FastEthernet0/17 Down 1 -- 0001.646C.1011
FastEthernet0/18 Down 1 -- 0001.646C.1012
FastEthernet0/19 Down 1 -- 0001.646C.1013
FastEthernet0/20 Down 1 -- 0001.646C.1014
FastEthernet0/21 Down 1 -- 0001.646C.1015
FastEthernet0/22 Down 1 -- 0001.646C.1016
FastEthernet0/23 Down 1 -- 0001.646C.1017
FastEthernet0/24 Down 1 -- 0001.646C.1018
GigabitEthernet0/1 Up 1 -- 0001.646C.1019
GigabitEthernet0/2 Down 1 -- 0001.646C.101A
Vlan1 Down 1 <not set> 0040.0BA2.1BD5
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch1
PC-PT PC0
PC-PT PC1
Time: 00:07:32
Realtime Simulation
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit
18°C Despejado
Buscar
10:14 p. m. 16/02/2026