

# Configure los parámetros básicos para formar conexiones de control en el router de borde de Cisco

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Verificación de modo](#)

[Configuración](#)

[Configuración de interfaz física](#)

[Configuración de subinterfaz](#)

[Configuración del sistema](#)

[Activación de CSR1000V y C8000V](#)

[Verificación de conexiones de control](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe la configuración básica y el orden de confirmación para incorporar un router de borde de Cisco a una superposición de red de área extensa definida por software.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software (SD-WAN) de Cisco
- Interfaz de línea de comandos (CLI) básica de Cisco IOS® XE

### Componentes Utilizados


Este documento se basa en las siguientes versiones de software y hardware:

- Cisco Edge Router versión 17.6.3
- vManage versión 20.6.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

---

 Nota: En esta guía se da por hecho que, para los routers físicos, el número de serie del router de extremo de Cisco ya se encuentra en el portal Cisco Network Plug & Play (PnP) y se ha sincronizado con la lista de dispositivos vManage; y, para los routers de extremo virtuales, que se ha agregado una instancia virtual al portal PnP y se ha sincronizado con vManage.

---

## Verificación de modo

Paso 1. Verifique que el router esté en el modo administrado por el controlador.

```
<#root>
```

```
show platform software device-mode
```

```
show version | in mode
```

Ejemplo:

```
<#root>
```

```
Router#
```

```
show platform software device-mode
```

```
Device Operating-mode:
```

```
Controller-Managed
```

```
Device-mode bootup status:
```

```
8/03 00:44:16 System is green
```

```
Bootup Success
```


```
<#root>
```

```
Router#
```

```
show version | in mode
```

```
Router operating mode:
```

---

 Nota: Si el modo operativo resulta en Autonomous, mueva el router a Controller-Managed con el `controller-mode enable` comando.

---

Paso 2. Realice un reinicio del software.

En el caso de una nueva tarjeta integrada, se recomienda limpiar el dispositivo con un reinicio de software, lo que garantiza que se eliminen todas las configuraciones anteriores de la base de datos de configuración (CBD).

```
<#root>  
Router#  
request platform software sdwan software reset
```

El dispositivo se recarga y arranca con una configuración en blanco.

Paso 3. Detenga el proceso de detección de PNP.

Si no es necesario el aprovisionamiento sin intervención del usuario (ZTP), detenga el proceso de detección de PNP.

```
<#root>  
Router#  
pnpa service discovery stop
```

---

 Nota: el proceso PNP se detiene en 5-10 minutos.

---

## Configuración

Se tratan dos escenarios:

- Interfaces físicas
- Subinterfaces

Ambos escenarios necesitan un túnel Cisco IOS XE y un túnel SD-WAN asociados con una interfaz para funcionar y una configuración básica del sistema SD-WAN.

## Configuración de interfaz física

La configuración de la interfaz y el túnel para VPN 0 o Global VRF requiere un orden específico; de lo contrario, hay errores en las asociaciones de la interfaz del túnel.

Orden de configuración:

1. Interfaz física
2. Ruta predeterminada
3. Registrar cambios
4. Túnel XE con una interfaz física como origen
5. Túnel SD-WAN XE
6. Registrar cambios

Ejemplo:

```
<#root>

!IOS-XE Portion

!
config-transaction
interface GigabitEthernet0/0/0
ip address 192.168.10.2 255.255.255.0
negotiation auto
no shutdown
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!

commit <<<<<<<<<< Commit changes here

!
interface Tunnel0
no shutdown
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
exit
!

! SD-WAN portion

!
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
encapsulation ipsec
color default
allow-service all
!

commit <<<<<<<<<< Commit changes here
```

```
!  
end
```

Si los cambios se confirman en un orden diferente, puede generar un error porque la interfaz de túnel IOS XE de Cisco no está asociada con la interfaz de túnel SD-WAN.

```
<#root>
```

```
cEdge(config-if)#
```

```
commit
```

```
Aborted: 'interface Tunnel 0 ios-tun:tunnel': Tunnel interface doesn't have corresponding sdwan GigabitEthernet interface
```

En la dirección opuesta, si se intenta remover un túnel SD-WAN sin el túnel Cisco IOS XE simultáneamente, puede conducir a un error de referencia.

```
<#root>
```

```
cEdge(config)#
```

```
commit
```

```
Aborted: 'sdwan interface GigabitEthernet0/0/0 tunnel-interface' : No Tunnel interface found with tunnel-id
```

## Configuración de subinterfaz

La interfaz física, la subinterfaz y la configuración de túnel para VPN 0 o Global VRF requieren un orden específico; de lo contrario, hay errores en las asociaciones de interfaz de túnel.

Orden de configuración:

1. Interfaz física
2. Subinterfaz
3. Ruta predeterminada
4. Registrar cambios
5. Túnel XE con una subinterfaz como origen
6. Túnel SD-WAN XE
7. Registrar cambios

Ejemplo:

```
<#root>
```

```

!IOS-XE Portion

!
config-transaction
interface GigabitEthernet0/0/0
no shutdown
no ip address
ip mtu 1500
mtu 1500
!
interface GigabitEthernet0/0/0.100
no shutdown
encapsulation dot1Q 100
ip address 192.168.10.2 255.255.255.0
ip mtu 1496
mtu 1496
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!

commit          <<<<<<<<<< Commit changes here

!
interface Tunnel0
no shutdown
ip unnumbered GigabitEthernet0/0/0.100
tunnel source GigabitEthernet0/0/0.100
tunnel mode sdwan
exit
!

! SD-WAN portion


!
sdwan
interface GigabitEthernet0/0/0.100
tunnel-interface
encapsulation ipsec
color default
allow-service all
!

commit          <<<<<<<<<< Commit changes here

!
end

```

---

 Nota: Para acomodar el campo de 32 bits agregado a los paquetes por el protocolo 802.1Q, la MTU para las subinterfaces debe ser al menos 4 bytes menor que la MTU de la interfaz física. Esto se configura con el `mtu` comando. La MTU predeterminada en una interfaz física es de 1500 bytes, por lo tanto, la MTU de la subinterfaz no debe ser mayor que 1496 bytes. Además, si la subinterfaz requiere una MTU de 1500 bytes, la MTU de la interfaz física se puede ajustar a 1504 bytes.

---

Si los cambios se confirman en un orden diferente, puede generar un error porque la interfaz de túnel IOS XE de Cisco no está asociada con la interfaz de túnel SD-WAN.

```
<#root>
```

```
cEdge(config)#
```

```
commit
```

```
Aborted: 'sdwan interface GigabitEthernet0/0/0.100 tunnel-interface' : No Tunnel interface found with t
```

## Configuración del sistema

Para unirse al fabric SD-WAN, el router de extremo de Cisco necesita información superpuesta básica en el sistema para poder iniciar la autenticación con vBond.

1. System IP: Identificador único del router de borde, viene en formato de puntos octales. No es una IP enrutable.
2. ID del sitio: identificador único del sitio.
3. Nombre de la organización: Identificador único de la superposición de SD-WAN.
4. IP y puerto vBond: IP y puerto vBond. Se puede obtener del propio vBond con el `show sdwan running-config system` comando.

Ejemplo:

```
<#root>
```

```
config-transaction
```

```
system
```

```
system-ip 10.10.10.1
```

```
site-id 10
```

```
organization-name SDWAN-OVERLAY
```

```
vbond 172.16.120.20 port 12346
```

```
!
```

```
commit
```

Inmediatamente después de confirmar la configuración del sistema, el router de extremo de Cisco se pone en contacto con vBond para la autenticación y comienza a crear conexiones de control con vManage y vsmarts.

## Activación de CSR1000V y C8000V

Los routers virtuales Cisco Edge requieren un paso adicional para asociar un chasis y un token, ya que no son hardware real y el identificador de dispositivo único universal (UUDI) es virtual.

En la GUI de vManage, vaya a: **Configuration > Devices** y localice una entrada CSR1000v o C8000v disponible:

State	Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Certificate Expiration Date	Subject SUDI serial #
	CSR1000v	CSR-7AD5C8CE-301E-4DA8-A74E- <span style="background-color: #00aaff; color: black;">XXXXXXXXXX</span>	Token - 23ffdf400cb14e489- <span style="background-color: #00aaff; color: black;">XXXXXXXXXX</span>	NA	NA	CSR-7AD5C8CE-301E-4DA8- <span style="background-color: #00aaff; color: black;">XXXXXXXXXX</span> ***

Ejecute la activación y sustituya los números de serie y chasis en el comando.

```
<#root>
```

```
request platform software sdwan vedge_cloud activate chassis-number CHASSIS_NUMBER token TOKEN_ID
```

Ejemplo:

```
<#root>
```

```
Router#
```

```
request platform software sdwan vedge_cloud activate chassis-number 7AD5C8CE-301E-4DA8-A74E-90A316XXXXXXXXXX token
```

## Verificación de conexiones de control

Verifique el estado de las conexiones de control con los comandos de verificación.

```
<#root>
```

```
show sdwan control connections
```

```
show sdwan control connection-history
```

## Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)
- [Solucionar problemas de conexiones de control SD-WAN](#)



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).