Comunidad de Soporte de Cisco en Español Webcast en vivo:

Introducción a la seguridad a nivel de capa 2 y su implementación.

Julio Carvajal Segura

CEO i-Networks.us

CCIE Routing & Switching # 42930

24 de Marzo del 2015

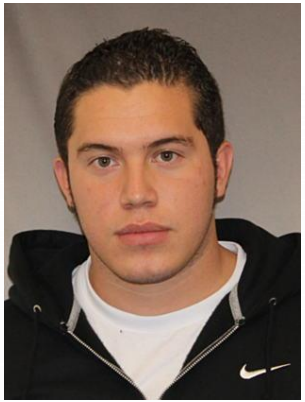
Comunidad de Soporte de Cisco – Webcast en vivo

- El experto del día de hoy es: Julio Carvajal Segura

CCIE Routing & Switching # 42930

Tema: Introducción a la seguridad a nivel de capa 2 y su implementación.

Panel de Expertos

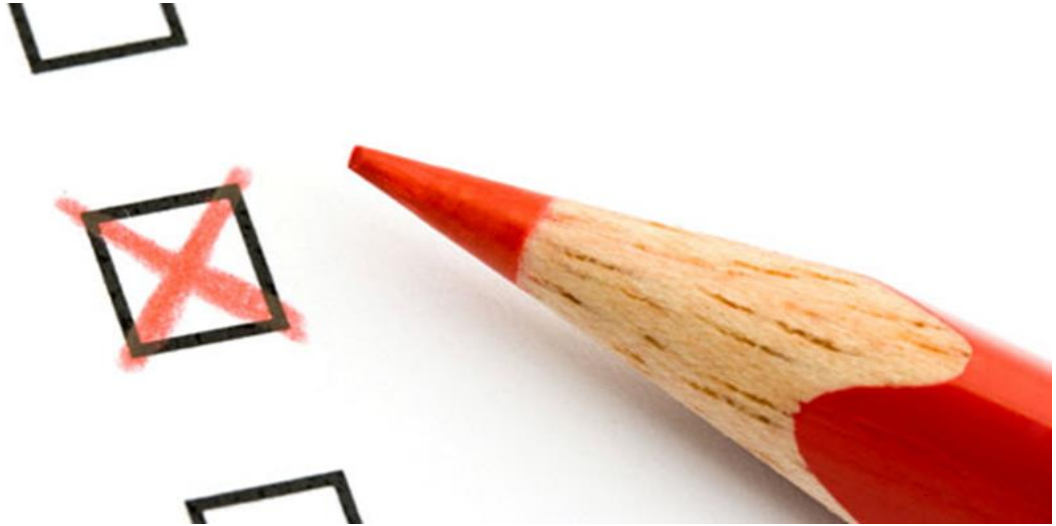


Gustavo Medina
Support Engineer

Gracias por su asistencia el día de hoy

La presentación incluirá algunas preguntas a la audiencia.

Le invitamos cordialmente a participar activamente en las preguntas que le haremos durante la sesión



Webcasts de la comunidad:

Puede encontrar los Webcast de la Comunidad de Soporte de Cisco en español en:

https://supportforums.cisco.com/es/community/5591

¡ Ahora puede realizar sus preguntas al panel de expertos!

Use el panel de preguntas y respuestas (Q&A) para preguntar a los expertos ahora. Ellos empezarán a responder.

Comunidad de Soporte de Cisco en Español Webcast en vivo:

Introducción a la seguridad a nivel de capa 2 y su implementación.

Julio Carvajal Segura

CEO i-Networks.us

24 de Marzo del 2015

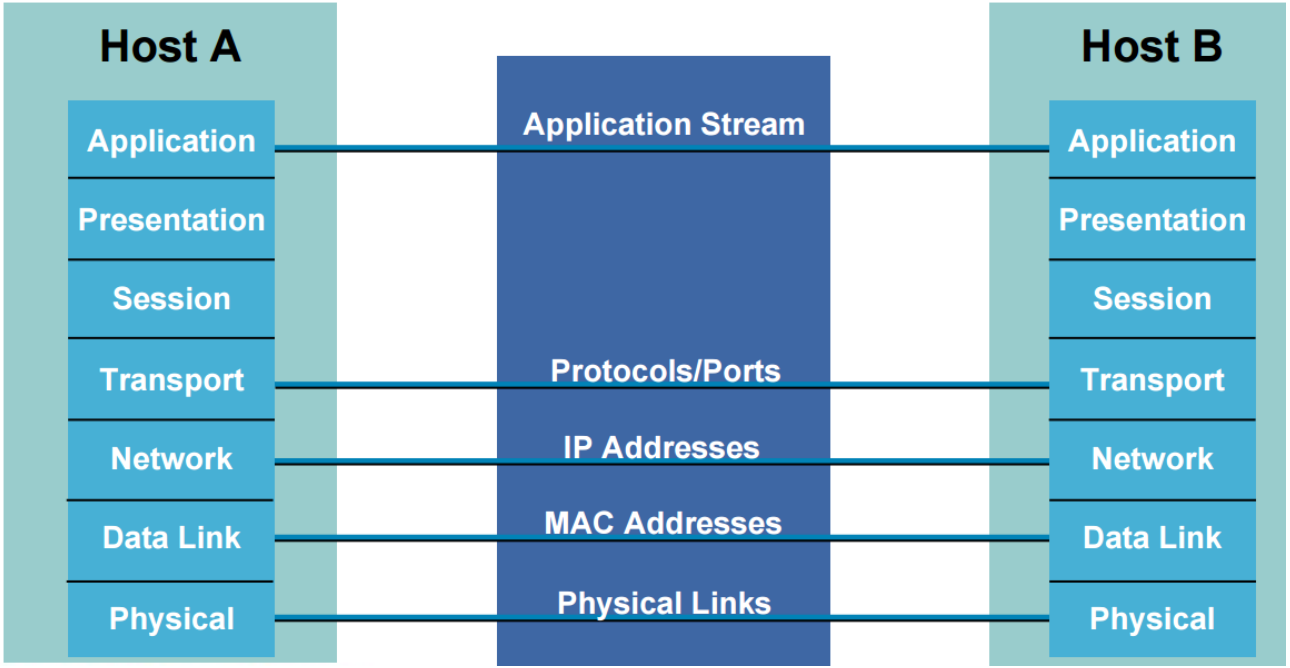
Agenda

- Introducción a la seguridad de redes de telecomunicaciones a nivel de capa 2
- Seguridad a nivel de puertos
- Private-VLAN
- Protección al protocolo de spanning-tree
- Mejores Prácticas para la seguridad a nivel de capa 2

Introducción a la seguridad de capa 2

¿Porqué necesitamos seguridad en la capa 2 del modelo OSI?

- El Modelo OSI es tan seguro como lo es cada una de sus capas, lo que significa que una sola debilidad afectaría todas las otras capas.



Seguridad a nivel de puertos

- Este tipo de protección nos va a permitir proveer seguridad a nivel de cada una de las interfaces, existen diferentes mecanismos para realizar esto.

Por ejemplo:

- Port-Security
- Storm-Control
- Protected Ports

A continuación vamos a discutir cada uno de ellos para luego implementarlos en un mini-lab y ver su funcionamiento.

1ra pregunta a la audiencia

¿Qué mecanismo de control a nivel de puerto tienen corriendo actualmente en su red de telecomunicaciones?

a. Port-Security

b. Storm-Control

c. Protected Ports

Port-Security

- Este mecanismo de seguridad es utilizado en los switches para limitar e identificar las direcciones MAC de los dispositivos que tienen permitido unirse a la red mediante un puerto en específico.

- Esto quiere decir que si yo configuro un puerto GigabitEthernet por ejemplo para que solo permita tráfico de una dirección MAC y recibo tráfico de una MAC diferente a ésta, el puerto no va a permitir este tráfico.

- Cuando una dirección MAC desconocida es identificada en un puerto configurado con Port-Security ocurre lo que se conoce como violación de seguridad

Port-Security con Direccion MAC Estatica

- **Esta opción es comunmente utilizada cuándo el administrador de red tiene claro la dirección MAC del equipo que va a conectar a un puerto específico.**

- **Configuración**

iNetworks(config)#int fa 0/13

iNetworks(config-if)#switchport port-security

iNetworks(config-if)#switchport port-security mac-address 24e9.b3ff.20b1

Port-Security con MAC Address Dinamica

- Esta opción se utiliza cuando no se conoce de antemano la direccion MAC que va a conectarse a un puerto específico.

- Importante recalcar que luego de que la dirección es guardada en la tabla de direcciones MAC de el switch no se va a respaldar en el startup-config por lo que luego que el switch se reinicie, la MAC no estara en la tabla de direcciones MAC.

Port-Security con MAC Address Dinamica

- **Configuración**

iNetworks(config)# int fa 0/13
iNetworks(config-if)#switchport port-security
iNetworks(config-if)# switchport port-security maximum 1

Port-Security con MAC Address Dinamica Sticky

- **El porque de esta opción es exactamente el mismo al anterior, lo único que va a variar en el comportamiento es el hecho de que la direccion MAC se va a guardar en el startup-config por lo que va a sobrevivir el proceso de reinicio del switch.**

Port-Security con MAC Address Sticky

- **Configuración**

iNetworks(config)# int fa 0/13

iNetworks(config-if)# switchport port-security mac-address sticky
iNetworks(config-if)# switchport port-security maximum 1

Datos Importantes acerca de Port-Security

- **Port-Security y VoIP:**

La recomendación en este caso es configurar un máximo de 3 direcciones MAC.

- **Comportamiento de Violación a la Política de Seguridad**

-Protect: El puerto va a descartar todo el tráfico de direcciones MAC no validadas hasta que el número de direcciones MAC lo permita.

-Restrict: El puerto va a descartar todo el tráfico de direcciones MAC no validadas hasta que el número de direcciones MAC lo permita, genera un log e incrementa el conteo de violaciones de seguridad.

-Shutdown (Por Defecto): Deshabilita el puerto de manera total(Error-Disabled), genera un log e incrementa el conteo de violaciones de seguridad.

Comandos Troubleshooting Port-Security

INetworks#show port-security

Nos muestra la configuracíón de manera general acerca de esta funcionalidad en nuestro Switch.

INetworks#show port-security interface fastEthernet 0/13

Nos muestra en detalle la configuración de un puerto en específico acerca de Port-Security y su estado.

Demo en vivo
Port-Security

Storm-Control

Storm-Control

- Funcionalidad que nos permite controlar que tanto trafico unicast, multicast o broadcast es recibido en un puerto en específico para que este realice una acción si la cantidad de tráfico no es aceptable.

- Cuando hablamos de la palabra acción, nos referimos al hecho de que Storm-Control puede descartar el tráfico que no es aceptable o deshabilitar el puerto.

- Su funcionalidad se asemeja con la de Traffic Policing donde un dispositivo limita la cantidad de tráfico que recibe basado en valores configurables. A diferencia de Traffic Policing Storm-Control cuenta con un intervalo de tiempo fijo donde se monitorea la cantidad de tráfico recibido, este valor de tiempo es de un segundo.

- Se puede realizar basado en número de paquetes, porcentaje de tráfico con respecto a la interface o por Mbps

Configuración Storm-Control

- Paso 1
  - Determinar el valor (en porcentaje o en paquetes por segundo) que pueden ser utilizados por Broadcast, Multicast o Unicast en un puerto en específico

iNetworks(config-if)#storm-control broadcast level 20 10

- En este caso le dijimos al Switch que Storm-Control debe ser activado cuando se reciba más de un 2% del ancho de banda todal de la interface y que debe ser deshabilitado al llegar al 1% del ancho de banda de la interface.

- Paso 2
  - Determinar la acción a realizar si Storm-Control es activado.

iNetworks(config-if)#storm-control broadcast level 2 1 shutdown

Como lo muestra la configuración al cruzar el limité del 20 % de ancho de banda el puerto será deshabilitado hasta que el nivel de tráfico Broadcast baje al 10 % del ancho de banda.

Demo en vivo
Storm-Control

Protected Ports

Protected Ports

- Esta funcionalidad provee seguridad de manera local (Es funcional únicamente en el Switch en el que se configura) tal como lo hacen las Private VLANs que analizaremos a fondo mas adelante.

- El administrador de red identificará puertos que no deben de tener comunicación a nivel de capa 2 y los configurara como Protected Ports. Estó hara que los puertos queden totalmente aislados uno del otro.

Configuración Protected Ports

- Paso 1
  - Luego de identificar los puertos a configurar en modo aislado introducimos el comando de Port Protected.

```
iNetworks(config)#int range fastethernet 0/1, fastethernet 0/13
iNetworks(config-if-range)#switchport protected
```

Posteriormente con un comando tal como “show interface fastethernet 0/13 status” podremos observar el estado del puerto con respecto a esta funcionalidad.

```
iNetworks#sh interface fastethernet 0/13 switchport
Protected: true
```

Demo en vivo
Port Protected

Private VLAN

Private VLAN

- Esta funcionalidad nos permite segmentar y filtrar el tráfico dentro de una VLAN.

- Básicamente realiza una partición de el dominio de broadcast a nivel de capa 2 creando multiples dominios permitiendo filtrar tráfico entre los puertos que pertenecen a estos dominios.

- Dichos subdominios estan conformados por una VLAN Primaria y una VLAN Secundaria.

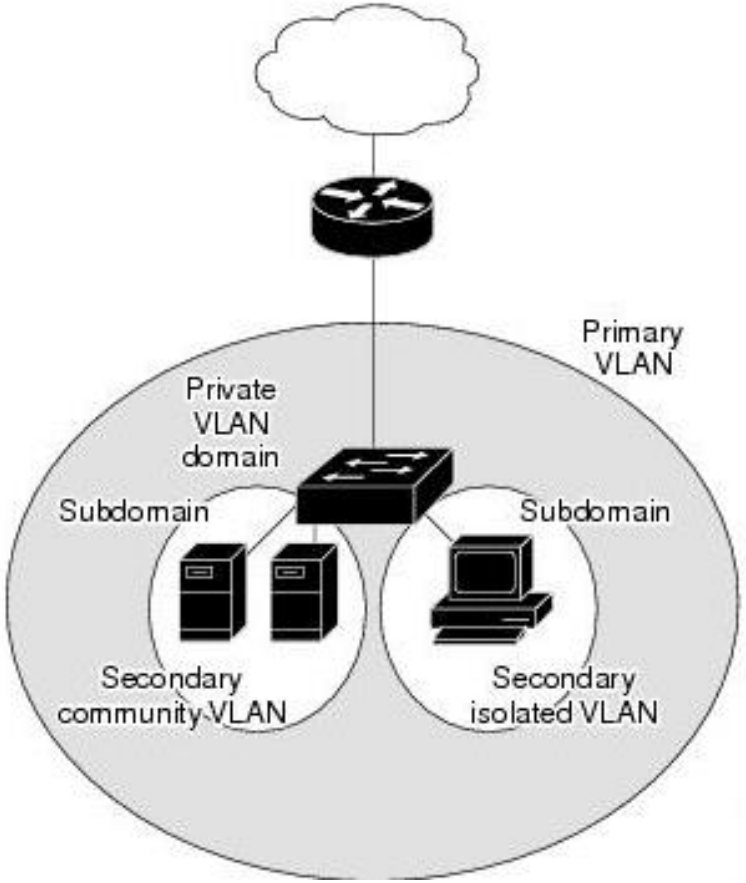
Private VLAN

- Todas las VLANs en un dominio de Private VLAN van a compartir la VLAN primaria. Son las VLANs secundarias las que diferencían un dominio de otro.

- La VLAN Primaria es la VLAN que representa a todo el dominio de capa 2.

- La VLAN secundaria puede ser de tipo Isolated o de tipo Community.

Private VLAN Domain



Tipos de Puertos dentro de una Private VLAN

- **Promiscuo:**
  - Pertenece a la VLAN Primaria
  - Puede comunicarse con todos los puertos de las VLANs Secundarias (Isolated y Community)

- **Isolated:**
  - Un puerto Isolated es un puerto que pertenece a la VLAN secundaria tipo Isolated.
  - No tiene acceso a comunicarse con ningún otro puerto mas que los puertos tipo promiscuo.

- **Community:**
  - Un puerto Community es un puerto que pertenece a la VLAN secundaria tipo community.
  - Puede comunicarse con puertos que se encuentren dentro de la misma VLAN secundaria (Community y con los puertos promiscuos.

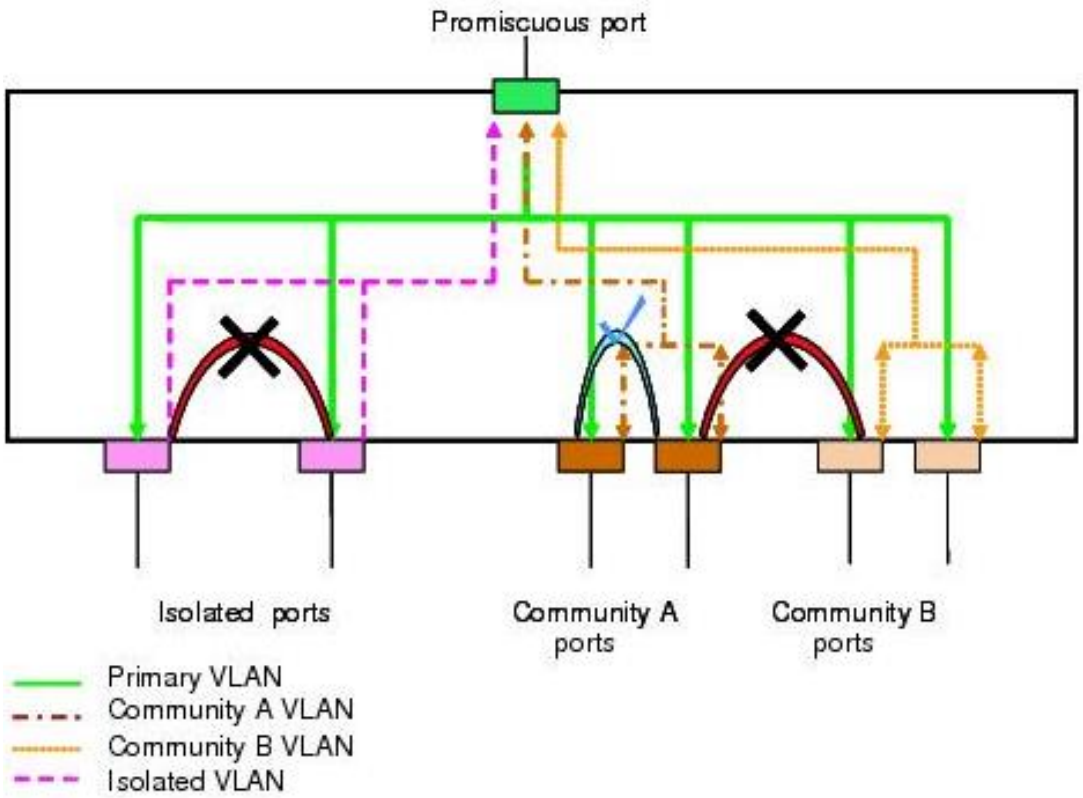
Tráfico en Private VLANs

- Primary VLAN
  - La VLAN Primaria maneja tráfico de los puertos promiscuos hacia los puertos que conectan a los dispositivos finales (Tanto puertos tipo Isolated o Community).

- Isolated VLAN
  - Trabaja con tráfico de manera unidireccional de los dispositivos finales hacia los puertos promiscuos.
  - Cada VLAN Isolated puede tener un o mas puertos en ella y cada uno de ellos estará completamente separado del resto (a nivel de capa 2).

- Community VLAN
  - Maneja tráfico de los puertos de la VLAN Community hacia los puertos promiscuos y los otros puertos en esa misma VLAN Community.

Flujo de Tráfico en una Private VLAN



Configuración Private Vlans

- Paso 1
  - Configurar el Switch en VTP modo Transparente

```
iNetworks(config)#vtp mode  transparent
Setting device to VTP TRANSPARENT mode.
```

- Paso 2
  - Identificar a la VLAN Primaria

```
iNetworks(config)#vlan 60
iNetworks(config-vlan)#private-vlan primary
```

Configuración Private Vlans

Paso 3

- Identificar a las VLANs Secundarias

```
iNetworks(config)#vlan 100
iNetworks(config-vlan)#private-vlan Isolated
iNetworks(config)#vlan 110
iNetworks(config-vlan)#private-vlan Community
iNetworks(config)#vlan 120
iNetworks(config-vlan)#private-vlan Community
```

- Paso 4
  - Asociar las VLANs Secundarias a la VLAN Primaria

```
iNetworks(config)#vlan 60
iNetworks(config-vlan)#private-vlan association 100,110,120
```

Configuración Private Vlans

- Verificando la configuración actual de Private VLANs

iNetworks#show vlan private vlan

Primary	Secondary	Type	Ports
60	100	isolated	
60	110	community	
60	120	community	

Configuración Private Vlans

Paso 5

- Configurar una interface como puerto de capa 2 de una Private VLAN

```
iNetworks(config)# interface gigatibethernet0/17
iNetworks(config)# description Puerto en modo ISOLATED
iNetworks(config-if)# switchport mode private-vlan host
iNetworks(config-if)# switchport private-vlan host-association 60 100
iNetworks(config)# interface gigatibethernet0/18
iNetworks(config)# description Puerto en modo Community-A
iNetworks(config-if)# switchport mode private-vlan host
iNetworks(config-if)# switchport private-vlan host-association 60 110
```

Configuración Private Vlans

```
iNetworks(config)# interface gigatibethernet0/17
iNetworks(config)# description Puerto en modo Community-A
iNetworks(config-if)# switchport mode private-vlan host
iNetworks(config-if)# switchport private-vlan host-association 60 110
iNetworks(config)# interface gigatibethernet0/18
iNetworks(config)# description Puerto en modo Community-B
iNetworks(config-if)# switchport mode private-vlan host
iNetworks(config-if)# switchport private-vlan host-association 60 120
```

Configuración Private Vlans

Paso 6

- Configurar una interface en modo Promiscuo

```
iNetworks(config)# interface gigatibethernet0/1
iNetworks(config)# description Link Hacia el Router
iNetworks(config)#switchport mode trunk
iNetworks(config)#switchport trunk allow vlan 60,100-120
iNetworks(config-if)# switchport mode private-vlan promiscous
iNetworks(config-if)# switchport mode private-vlan mapping 60 add 100,110,120
```

3da pregunta a la audiencia

¿Qué tan familiarizado está usted con el protocolo de Spanning-Tree?

a. He escuchado hablar de el únicamente.
b. Un poco, lo he estudiado brevemente.
c. Mucho, trabajo con el día a día

Protección al Protocolo de Spanning-Tree

Fundamentos de Spanning-Tree

- STP es un protocolo de capa 2 definido por el IEEE 802.ID que se utiliza para proveer caminos alternativos en nuestra red mientras se previenen búcles en redes con múltiples rutas.
- Como podemos ver STP es sumamente importante pero desafortunadamente al momento de ser creado su seguridad no fue tomado en cuenta.
- A continuación vamos a mencionar los mecanismos para superar su vulnerabilidades.

STP BPDU Filter

- BPDUs son los mensajes que se intercambian entre switches para calcular la topología de STP.
- BPDU Filter es la funcionalidad que nos permite filtrar el envío y la recepción de BPDUs en una interface o globalmente.
- Cuando se configura globalmente se aplicará a las interfaces en modo PortFast. Si se recibe un BPDU en una interface, dicha saldra del estado de PortFast y empezara a participar en los cálculos de Spanning-Tree.

Configuración BPDU-Filter

Ejemplo 1

- Configuracíón STP BPDU-Filter por interface

```
iNetworks(config)# interface gigatibethernet0/3
iNetworks(config)# description Link Hacia PC-1
iNetworks(config)#spanning-tree bpdufilter enable
```

Configuración BPDU-Filter

Ejemplo 2

- **Configuracíón STP BPDU-Filter Globalmente**

iNetworks(config)# spanning-tree portfast bpdufilter default

Bridge Protocol Data Unit (BPDU) Guard

- Debido a que STP no realiza ningún tipo de autenticación o encriptación para proteger el intercambio de BPDUs, es vulnerable a ataques por dispositivos no autorizados.
- BPDU Guard nos permite restringir la participación de Switches en STP.
- Esta funcionalidad puede ser configurada por puerto o globalmente (Importante recalcar que se deberá configurar en interfaces que no se esperan recibir BPDUs, esto quiere decir en interfaces que conectan a dispositivos finales).

Configuración BPDU-Guard

Ejemplo 1

- Configuracíón para una interfaz en específico.

```
iNetworks(config)# interface gigatibethernet0/1
iNetworks(config)# description Link Hacia PC-1
iNetworks(config)#spanning-tree portfast
iNetworks(config)#spanning-tree bpduguard enable
```

Configuración BPDU-Guard

Ejemplo 2

- Configuracíón BPDU-Guard Globalmente

iNetworks(config)# spanning-tree portfast bpduguard default

Nota: Cuando es habilitado globalmente, BPDU Guard se aplicá a todas las interfaces que están configuradas en modo Portfast.

STP Root Guard

- Como mencionamos anteriormente, debido al hecho de que nos falta autenticación y encriptación en las tramas de STP somos vulnerables a la participación de un Switch no deseado y que este se haga pasar por el Root Switch o Switch Primario.

- STP Root Guard nos permite configurar puertos determinados en modo designado de tal manera que al otro extremo ningún switch pueda reclamar el rol de Root Switch.

Configuración Root-Guard

Ejemplo 1

- Configuracíón STP Guard

```
iNetworks(config)# interface gigatibethernet0/3
iNetworks(config)# description Link Hacia Switch-3
iNetworks(config)#spanning-tree guard root
```

Prácticas a Seguir
Seguridad en Capa 2

- Administrar los dispositivos de capa 2 de manera segura (por ejemplo SSH en vez de Telnet)

- Restringir acceso a la administración del Switch de tal manera que solamente redes confiables y usuarios autorizados pueden accesarla (por ejemplo utilizar RADIUS para la autenticación de SSH y un access-class en las líneas de SSH para restringir el acceso).

- Evitar usar VLAN 1 ya que todos sabemos de su existencia.

- Deshabilitar DTP en las interfaces no truncales para evitar enlaces truncales no deseados.

- Habilitar Port-Security para evitar acceso no autorizado en nuestros switches.
- Utilizar Private VLAN cuando sea posible para segregar el tráfico a nivel de capa 2.
- Deshabilitar CDP donde sea posible.
- Deshabilitar servicios innecesarios y protocolos no deseados para evitar ataques de DoS o DDoS.

- Deshabilitar los puertos que no estan siendo utilizados en nuestro Switch y asegurarnos que estan en una VLAN que no se utilizar normalmente.

- Habilitar seguridad en el protocolo de STP.

- Utilizar protocolos de control de acceso avanzados como 802.1x

- Reforzar la red mediante el uso de MAC Security

Template de configuración Switches

```
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
enable secret xxxx
username xxxx secret xxxx
aaa new-model
aaa authentication login default local
line con 0
login authentication default
exec-timeout 30 0
logging synchronous
line vty 0 15
transport input ssh
login authentication default
login block-for 5 attempts 3 within 5
```

Haga sus preguntas ahora

Utilize el panel de Q & A para realizar sus preguntas

Nos interesa su opinión!!!

Para completar la evaluación espere un momento y aparecerá automáticamente al cerrar el browser de la sesión.

Pregunte al Experto con:
Julio Carvajal y Gustavo Medina

SI tiene dudas adicionales pregunte en: https://supportforums.cisco.com/es/discussion/12424776 a partir de hoy hasta el próximo viernes 3 de Abril del 2015.

Podrá ver la grabación de este evento, y leer las preguntas y respuestas en 5 días hábiles.

Sesiones de Webcast
Español
Tema: *Telepresencia*

Martes 28 de Abril:

10:00 a.m. Ciudad de México
11:30 a.m. Caracas
1:00 p.m. Buenos Aires
5:00 p.m. Madrid

Estará presentando el experto de Cisco: **Said Portillo**

Durante esta sesión se explicara

Sesiones de Webcast (Portugués)

Tema:

Miércoles de :

8:00 a.m. Ciudad de México

11:00 a.m. Brasilia

Estará presentando el experto de Cisco:

En este webcast se describirán

Reconocimientos en la Comunidad

El reconocimiento al **“Partcipante Destacado de la Comunidad”** se otorga a los miembros que demuestran liderazgo y colaboración con la Comunidad, está diseñado para reconocer y agradecer a aquellas personas que colaboran con contenido técnico de calidad y ayudan a posicionar nuestra comunidad como el destino número uno para las personas interesadas en tecnología Cisco.

Califique el contenido de la Comunidad de Soporte de Cisco en Español.

Ahora puede calificar discusiones, documentos, blogs y videos!!...

Esto es con el fin de que nos ayude a distinguir contenido de calidad y también para reconocer los esfuerzos de los integrantes de la Comunidad de Soporte de Cisco en español.

Soporte Técnico Móvil, tenga acceso a las Comunidades de Soporte Globales.

La Comunidad de Soporte de Cisco cuenta con una aplicación de Acceso Móvil hacia la Comunidades Globales > Español, Portugués, Japonés, Ruso, y Polaco.

Lo invitamos a colaborar activamente en CSC en español y en nuestras redes sociales

https://supportforums.cisco.com/community/spanish

CiscoLatinoamerica	Cisco Cono Sur
Cisco Mexico	Comunidad Cisco Cansac
Cisco España	CiscoSupportCommunity
@Cisco_LA	@ciscocansacsm
@CiscoMexico	@ciscoconosur
@cisco_spain	@cisco_support

Más redes sociales:

CiscoLatam

ciscosupportchannel

Cisco Technical Support

CSC-Cisco-Support-Community

¡Únete a la Comunidad de Soporte de Cisco!

Aquí puedes resolver dudas técnicas, encontrar información en documentos, blogs y videos con contenidos técnicos totalmente en español, además de poder colaborar e interactuar en tiempo real con los expertos en tecnología.


Documentos


Discusiones


Blogs


Móvil


Video


Pregunte al Experto

Gracias por su tiempo

Por favor tome un momento para llenar su evaluación


CISCO