Ejemplo de Configuración de Catalyst 3550/3560 Series Switches Usando Control de Tráfico Basado en Puerto

Contenido

Introducción

Este documento aporta una configuración y verificación de muestra para las características de control de tráfico de acceso basado en los switches Catalyst Serie 3550/3560. En particular, este documento muestra cómo configurar las características de control de tráfico de acceso basado en un switch Catalyst 3550.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar realizar esta configuración:

- Conocimiento básico de la configuración de los switches Catalyst de Cisco serie 3550/3560.
- Contar con conocimientos básicos de las funciones de control de tráfico basado en puertos.

Componentes Utilizados

La información de este documento se basa en los switches Cisco Catalyst de la serie 3550.

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). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Información general sobre el control de tráfico basado en puertos

El switch Catalyst 3550/3560 ofrece control de tráfico basado en puertos que se puede implementar de varias maneras:

- Control de tormentas
- Puertos protegidos
- Bloqueo de puertos
- Seguridad de Puertos

El control de saturación evita el tráfico como una saturación de difusión, multidifusión o unidifusión en una de las interfaces físicas del switch. Un tráfico excesivo en la LAN, denominado tormenta de la LAN, provocará una degradación del rendimiento de la red. Utilice el control de tormentas para evitar la degradación del rendimiento de la red.

El control de tormentas observa los paquetes que pasan a través de una interfaz y determina si los paquetes son de unidifusión, multidifusión o difusión. Establezca el nivel de umbral para el tráfico entrante. El switch cuenta el número de paquetes según el tipo de paquete recibido. Si el tráfico de difusión y unidifusión excede el nivel de umbral en una interfaz, sólo se bloquea el tráfico de un tipo determinado. Si el tráfico multicast excede el nivel de umbral en una interfaz, entonces todo el tráfico entrante se bloquea hasta que el nivel de tráfico descienda por debajo del nivel de umbral. Utilice el comando de configuración de interfaz storm-control para configurar el control de tormenta especificado de tráfico en la interfaz.

Configure los puertos protegidos en un switch utilizado en un caso en el que un vecino no debería ver el tráfico generado por otro vecino, de modo que parte del tráfico de aplicaciones no se reenvíe entre los puertos del mismo switch. En un switch, los puertos protegidos no reenvían tráfico (unidifusión, multidifusión o difusión) a ningún otro puerto protegido, pero un puerto protegido puede reenviar tráfico a puertos no protegidos. Utilice el comando de configuración de interfaz switchport protected en una interfaz para aislar el tráfico en la Capa 2 de otros puertos protegidos.

Los problemas de seguridad pueden ocurrir cuando el tráfico de direcciones MAC de destino desconocido (unidifusión y multidifusión) se inunda en todos los puertos del switch. Para evitar que el tráfico desconocido se reenvíe de un puerto a otro, configure el bloqueo de puertos, que bloqueará los paquetes de unidifusión o multidifusión desconocidos. Utilice el comando de configuración de interfaz switchport block para evitar que se reenvíe tráfico desconocido.

Utilice Port Security para restringir la entrada a una interfaz identificando las direcciones MAC de las estaciones con permiso para acceder al puerto. Asigne direcciones MAC seguras a un puerto seguro, de modo que el puerto no reenvíe paquetes con direcciones de origen fuera del grupo de direcciones definidas. Utilice la función de aprendizaje persistente en una interfaz para convertir las direcciones MAC dinámicas en direcciones MAC seguras y fijas. Utilice el comando de configuración de interfaz switchport port-security para configurar los parámetros de seguridad del puerto en la interfaz.

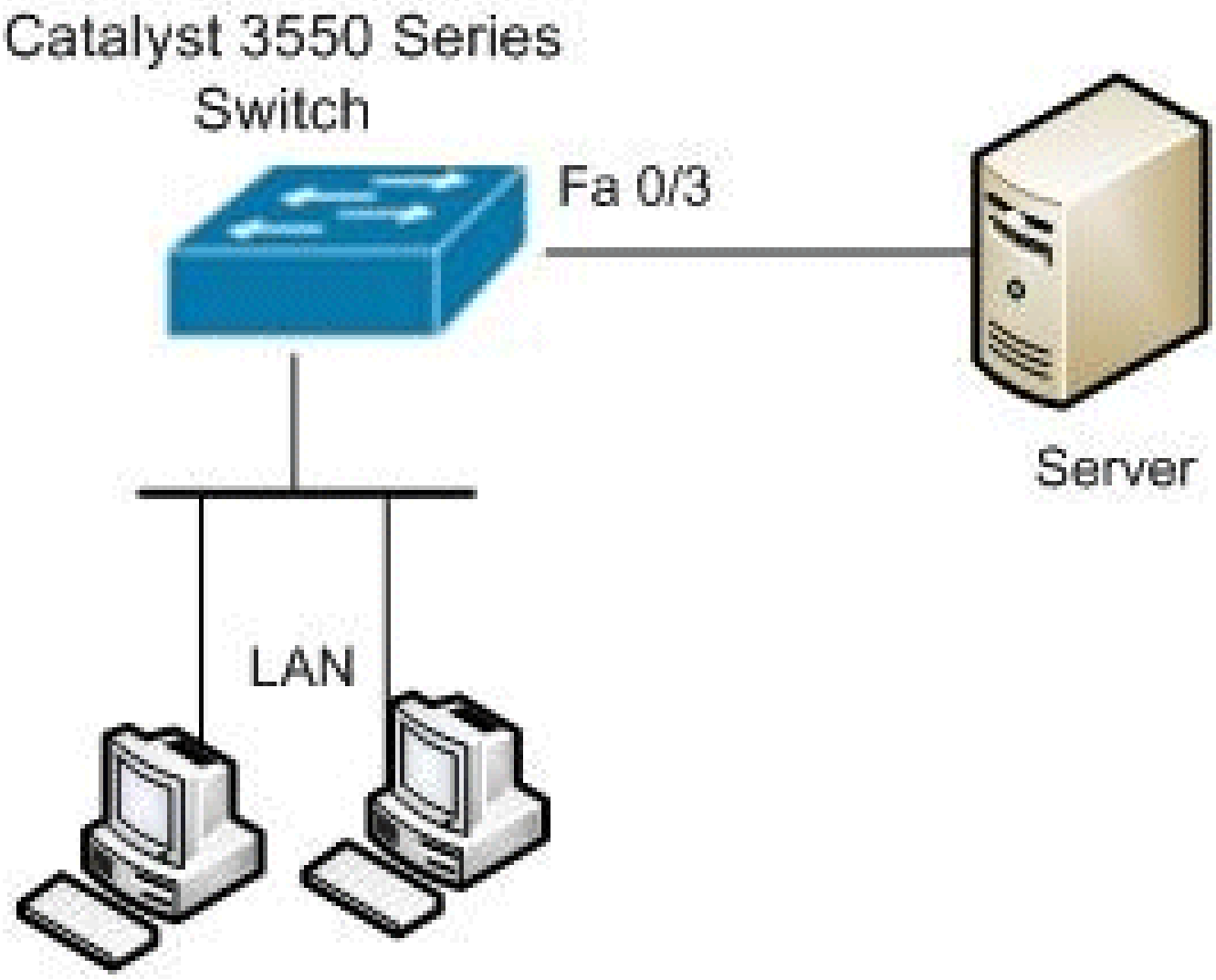
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración

Este documento usa esta configuración:

Catalyst 3550 Switch

```
<#root>
Switch#
configure terminal
Switch(config)#
interface fastethernet0/3


!--- Configure the Storm control with threshold level.

Switch(config-if)#
storm-control unicast level 85 70
Switch(config-if)#
storm-control broadcast level 30



!--- Configure the port as Protected port.

Switch(config-if)#
switchport protected



!--- Configure the port to block the multicast traffic.

Switch(config-if)#
switchport block multicast



!--- Configure the port security.

Switch(config-if)#
switchport mode access
Switch(config-if)#
switchport port-security


!--- set maximum allowed secure MAC addresses.
```

```
Switch(config-if)#
switchport port-security maximum 30


!--- Enable sticky learning on the port.
Switch(config-if)#
switchport port-security mac-address sticky


!--- To save the configurations in the device.
switch(config)#
copy running-config startup-config
Switch(config)#
exit
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilize el OIT para ver una análisis de la salida del comando show.

Utilice el comando show interfaces [interface-id] switchport para verificar sus entradas:

Por ejemplo:

<#root>

```
Switch#
show interfaces fastEthernet 0/3 switchport

Name: Fa0/3
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
```

```
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: enabled
Appliance trust: none
```

Utilice el comando show storm-control [interface-id] [broadcast] | multicast (multidifusión) | unicast] para verificar los niveles de supresión de control de tormentas establecidos en la interfaz para el tipo de tráfico especificado.

Por ejemplo:

<#root>

```
Switch#

show storm-control fastEthernet 0/3 unicast

Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  -----------
Fa0/3      Forwarding       85.00%       70.00%        0.00%

Switch#

show storm-control fastEthernet 0/3 broadcast

Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  -----------
Fa0/3      Forwarding       30.00%       30.00%        0.00%

Switch#

show storm-control fastEthernet 0/3 multicast

Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  -----------
Fa0/3      inactive        100.00%      100.00%       N/A
```

Utilice el comando show port-security [interface interface-id] para verificar la configuración de seguridad de puerto para la interfaz especificada.

Por ejemplo:

```
Switch#show port-security interface fastEthernet 0/3
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
```

```
Maximum MAC Addresses      : 30
Total MAC Addresses        : 4
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 4
Last Source Address        : 0012.0077.2940
Security Violation Count   : 0
```

Utilice el comando show port-security [interface interface-id] address para verificar todas las direcciones MAC seguras configuradas en una interfaz especificada.

Por ejemplo:

```
Switch#show port-security interface fastEthernet 0/3 address
          Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    000d.65c3.0a20    SecureSticky        Fa0/3         -
   1    0011.212c.0e40    SecureSticky        Fa0/3         -
   1    0011.212c.0e41    SecureSticky        Fa0/3         -
   1    0012.0077.2940    SecureSticky        Fa0/3         -
------------------------------------------------------------------------
Total Addresses: 4
```

Información Relacionada

- Página de soporte de switches Cisco Catalyst de la serie 3550
- Página de soporte de switches Cisco Catalyst de la serie 3650
- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems

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).