Switches de las 3550/3560 Series del Catalyst usando el ejemplo de configuración del control de tráfico del acceso basado

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.

prerrequisitos

Requisitos

Aseegurese que usted cumple estos requisitos antes de que usted intente esta configuración:

- Tenga conocimiento básico de la configuración en el Switches de las 3550/3560 Series del Cisco Catalyst.
- Tenga una comprensión básica de las características del control de tráfico del acceso basado.

Componentes Utilizados

La información en este documento se basa en los Cisco Catalyst 3550 Series Switch.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Descripción del control de tráfico del acceso basado

El Switch del Catalyst 3550/3560 ofrece el control de tráfico del acceso basado que se puede implementar de las diversas maneras:

- Control de tormentas
- Puertos protegidos
- Bloqueo del puerto
- Seguridad de Puertos

El control de tormentas previene el tráfico tal como un broadcast, un Multicast, o una tormenta del unicast en una de las interfaces físicas del Switch. El tráfico excesivo en el LAN, designado una tormenta LAN, llevará a 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 el pasar a través de una interfaz y los determina si los paquetes son unicast, Multicast, o broadcast. Fije el límite de umbral para el tráfico entrante. El Switch cuenta el número de paquetes según el tipo de paquete recibido. Si el broadcast y el tráfico de unidifusión exceden el límite de umbral en una interfaz, después solamente el tráfico de un tipo determinado se bloquea. Si el tráfico Multicast excede el límite de umbral en una interfaz, después todo el tráfico entrante se bloquea hasta los descensos del nivel de tráficog debajo del límite de umbral. Utilice el comando interface configuration del control de tormentas de configurar el tráfico especificó el control de tormentas en la interfaz.

Configure los puertos protegidos en un Switch usado en un caso cuando un vecino no debe ver el tráfico generado por otro vecino, de modo que un cierto tráfico de aplicación no sea remitido entre los puertos en el mismo Switch. En un Switch, los puertos protegidos no remiten ningún tráfico (unicast, Multicast, o broadcast) a ninguna otra puertos protegidos, pero un puerto protegido puede remitir cualquier tráfico a los puertos NON-protegidos. Utilice el comando configuration de la interfaz protegida del switchport en una interfaz de aislar el tráfico en la capa 2 de otros puertos protegidos.

Los problemas de seguridad pueden ocurrir cuando el tráfico de las direcciones MAC del destino desconocido (unicast y Multicast) se inunda a todos los puertos en el Switch. Para prevenir el tráfico desconocido que es remitido a partir de un puerto a otro puerto, puerto de la configuración que bloquea, que bloqueará la unidifusión desconocida o los paquetes de multidifusión. Utilice el comando interface configuration del bloque del switchport de prevenir el tráfico desconocido que es remitido.

Utilice la Seguridad de puerto para restringir la entrada a una interfaz identificando las direcciones MAC de las estaciones permitidas acceder el puerto. Asigne los MAC Address seguros a un puerto seguro, de modo que el puerto no remita los paquetes con las direcciones de origen fuera del grupo de direccionamientos definidos. Utilice la característica de aprendizaje Sticky en una

interfaz para convertir las direcciones MAC dinámicas a los MAC Address seguros Stickyes. Utilice el comando interface configuration de la Seguridad de puerto del switchport de configurar las configuraciones de la Seguridad de puerto en la interfaz.

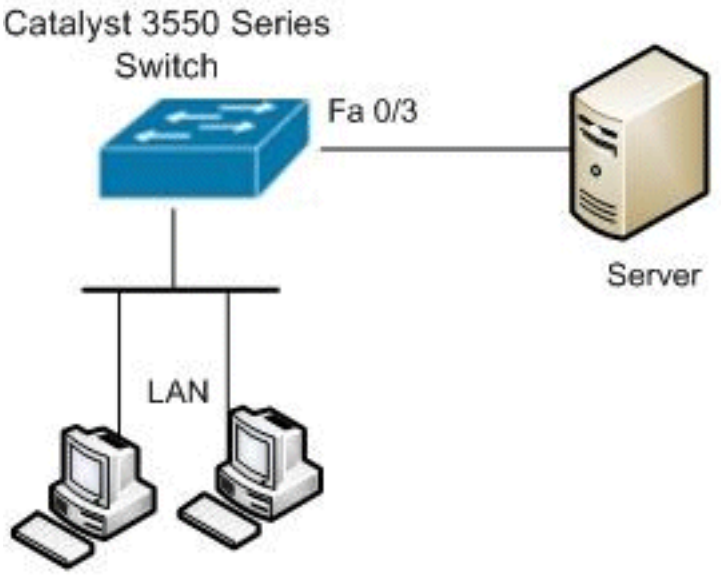
Configurar

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

Note: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados 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

```
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 switchport de las interfaces de la demostración [interface-id] para verificar sus entradas:

Por ejemplo:

```
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 control de tormentas de la demostración [interface-id] [broadcast | Multicast | el comando del unicast] para verificar los niveles de la supresión del control de tormentas fijados en la interfaz para el tráfico especificado teclea.

Por ejemplo:

```
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 del [interface interface-id] de la Seguridad de puerto de la demostración para verificar las configuraciones de la Seguridad de puerto para la interfaz especificada.

Por ejemplo:

```
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 address del [interface interface-id] de la Seguridad de puerto de la demostración para verificar todos los MAC Address seguros configurados en una interfaz especificada.

Por ejemplo:

```
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
```

Información Relacionada

- Página de soporte de los Cisco Catalyst 3550 Series Switch
- Página de soporte de los Cisco Catalyst 3650 Series Switch
- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems