Exemple de configuration de commutateurs de la gamme Catalyst 3550/3560 utilisant le contrôle du trafic basé sur les ports

Contenu

Introduction

Ce document fournit un exemple de configuration et de vérification pour les fonctionnalités de contrôle du trafic basées sur les ports de vos commutateurs de la gamme Catalyst 3550/3560. Ce document vous montre tout particulièrement comment configurer, sur un commutateur Catalyst 3550, les fonctionnalités de contrôle du trafic basé sur le port.

Conditions préalables

Conditions requises

Assurez-vous de respecter ces conditions avant de tenter cette configuration :

- Connaître de base la configuration des commutateurs Cisco Catalyst 3550/3560.
- Comprendre de base les fonctionnalités de contrôle du trafic basées sur les ports.

Components Used

Les informations contenues dans ce document sont basées sur les commutateurs de la gamme Cisco Catalyst 3550.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Vue d'ensemble du contrôle du trafic basé sur les ports

Le commutateur Catalyst 3550/3560 offre un contrôle du trafic basé sur les ports qui peut être mis en oeuvre de différentes manières :

- Contrôle des tempêtes
- Ports protégés
- Blocage de port
- Sécurité de port

Le contrôle des tempêtes empêche le trafic, tel qu'une diffusion, une multidiffusion ou une tempête de monodiffusion sur l'une des interfaces physiques du commutateur. Un trafic excessif dans le réseau local, appelé tempête de réseau local, entraîne une dégradation des performances du réseau. Utilisez le contrôle des tempêtes afin d'éviter la dégradation des performances du réseau.

Storm Control observe les paquets passant par une interface et détermine si les paquets sont de monodiffusion, de multidiffusion ou de diffusion. Définissez le niveau de seuil pour le trafic entrant. Le commutateur compte le nombre de paquets en fonction du type de paquet reçu. Si le trafic de diffusion et de monodiffusion dépasse le niveau de seuil sur une interface, seul le trafic d'un type particulier est bloqué. Si le trafic de multidiffusion dépasse le niveau de seuil sur une interface, tout le trafic entrant est bloqué jusqu'à ce que le niveau de trafic tombe en dessous du niveau de seuil. Utilisez la commande de configuration d'interface de contrôle de tempête pour configurer le contrôle de tempête spécifié du trafic sur l'interface.

Configurez les ports protégés sur un commutateur utilisé dans un cas où un voisin ne doit pas voir le trafic généré par un autre voisin, de sorte qu'un certain trafic d'application ne soit pas transféré entre les ports du même commutateur. Dans un commutateur, les ports protégés ne transmettent aucun trafic (monodiffusion, multidiffusion ou diffusion) vers d'autres ports protégés, mais un port protégé peut transférer tout trafic vers des ports non protégés. Utilisez la commande de configuration d'interface switchport protected sur une interface pour isoler le trafic de couche 2 des autres ports protégés.

Des problèmes de sécurité peuvent survenir lorsque le trafic des adresses MAC de destination inconnues (monodiffusion et multidiffusion) est diffusé sur tous les ports du commutateur. Afin d'empêcher le trafic inconnu d'un port à un autre, configurez le blocage des ports, qui bloquera les paquets de monodiffusion ou de multidiffusion inconnus. Utilisez la commande de configuration d'interface switchport block pour empêcher le transfert de trafic inconnu.

Utilisez la sécurité des ports afin de limiter l'entrée à une interface en identifiant les adresses MAC des stations autorisées à accéder au port. Attribuez des adresses MAC sécurisées à un port sécurisé, afin que le port ne transfère pas les paquets avec des adresses source en dehors du groupe d'adresses définies. Utilisez la fonction d'apprentissage rémanent sur une interface pour convertir les adresses MAC dynamiques en adresses MAC sécurisées rémanentes. Utilisez la commande de configuration d'interface switchport port-security pour configurer les paramètres de sécurité des ports sur l'interface.

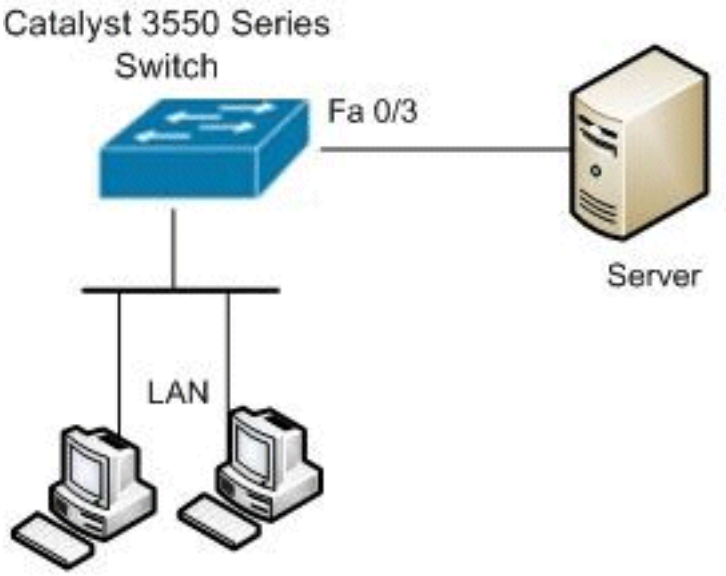
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration

Ce document utilise la configuration suivante :

Commutateur Catalyst 3550

```
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
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

Utilisez la commande show interfaces [interface-id] switchport afin de vérifier vos entrées :

Exemple :

```
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
```

Utilisez la commande show storm-control [id-interface] [broadcast | multidiffusion | unicast] afin de vérifier les niveaux de suppression de contrôle de tempête définis sur l'interface pour le type de trafic spécifié.

Exemple :

```
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
```

Utilisez la commande show port-security [interface id-interface] afin de vérifier les paramètres de sécurité des ports pour l'interface spécifiée.

Exemple :

```
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
```

Utilisez la commande show port-security [interface id-interface] address afin de vérifier toutes les adresses MAC sécurisées configurées sur une interface spécifiée.

Exemple :

```
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
```

Informations connexes

- Page d'assistance des commutateurs de la gamme Cisco Catalyst 3550
- Page d'assistance des commutateurs de la gamme Cisco Catalyst 3650
- Support pour commutateurs
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems