Commutateurs de gamme Catalyst 3550/3560 utilisant l'exemple basé sur port de configuration de contrôle du trafic

Contenu

Introduction

Ce document fournit une configuration et une vérification d'échantillon pour les caractéristiques basées sur port de contrôle du trafic sur vos Commutateurs de gamme Catalyst 3550/3560. Spécifiquement, ce document t'affiche comment configurer les caractéristiques basées sur port de contrôle de trafic sur un commutateur du Catalyst 3550.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant que vous tentiez cette configuration :

- Ayez la connaissance de base de la configuration sur des Commutateurs de gamme Cisco Catalyst 3550/3560.
- Ayez une compréhension de base des caractéristiques basées sur port de contrôle de trafic.

Composants utilisés

Les informations dans ce document sont basées sur le Commutateurs de la gamme Cisco Catalyst 3550.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Aperçu basé sur port de contrôle de trafic

Le commutateur du Catalyst 3550/3560 offre le contrôle de trafic basé sur port qui peut être mis en application dans diverses manières :

- Contrôle de tempête
- Ports protégés
- Blocage de port
- Sécurité de port

Le contrôle de tempête empêche le trafic tel qu'une émission, une Multidiffusion, ou une tempête d'unicast sur une des interfaces physiques du commutateur. Le trafic excessif dans le RÉSEAU LOCAL, désigné sous le nom d'une tempête de RÉSEAU LOCAL, mènera à une dégradation des performances du réseau. Employez le contrôle de tempête afin d'éviter la dégradation des performances du réseau.

Le contrôle de tempête observe les paquets traverser une interface et détermine si les paquets sont monodiffusé, Multidiffusion, ou émission. Placez le seuil d'avertissement pour le trafic entrant. Le commutateur compte le nombre de paquets selon le type de paquet reçu. Si l'émission et le trafic unicast dépassent le seuil d'avertissement sur une interface, alors seulement le trafic d'un type particulier est bloqué. Si le trafic de multidiffusion dépasse le seuil d'avertissement sur une interface, alors tout le trafic entrant est bloqué jusqu'aux baisses de niveau du trafic au-dessous du seuil d'avertissement. Utilisez la commande de configuration d'interface de **storm-control** de configurer le contrôle de tempête spécifié par trafic sur l'interface.

Configurez les ports protégés sur un commutateur utilisé dans un cas quand un voisin ne devrait pas voir le trafic généré par un autre voisin, de sorte que du trafic de l'application ne soit pas expédié entre les ports sur le même commutateur. Dans un commutateur, les ports protégés n'expédie aucun trafic (unicast, Multidiffusion, ou émission) à aucun autre port protégé, mais un port protégé peut expédier n'importe quel trafic aux ports non-protégés. Utilisez la commande de configuration d'interface de **switchport protected** sur une interface d'isoler le trafic à la couche 2 d'autres ports protégés.

Les problèmes de sécurité peuvent se produire quand le trafic inconnu d'adresses de MAC de destination (unicast et Multidiffusion) sont inondés à tous les ports dans le commutateur. Afin d'empêcher le trafic inconnu étant expédié d'un port à un autre port, configurez le port bloquant, qui bloquera l'unicast ou les paquets de multidiffusion inconnus. Utilisez la commande de configuration d'interface de **switchport block** d'empêcher le trafic inconnu étant expédié.

Employez la Sécurité de port afin de limiter l'entrée à une interface en identifiant des adresses MAC des stations permises pour accéder au port. Assignez les adresses MAC sécurisées à un port sécurisé, de sorte que le port n'expédie pas des paquets avec des adresses sources en dehors du groupe d'adresses définies. Employez la caractéristique apprenante Rémanente sur

une interface pour convertir les adresses MAC dynamiques aux adresses MAC sécurisées Rémanentes. Utilisez la commande de configuration d'interface de switchport port-security de configurer les configurations de Sécurité de port sur l'interface.

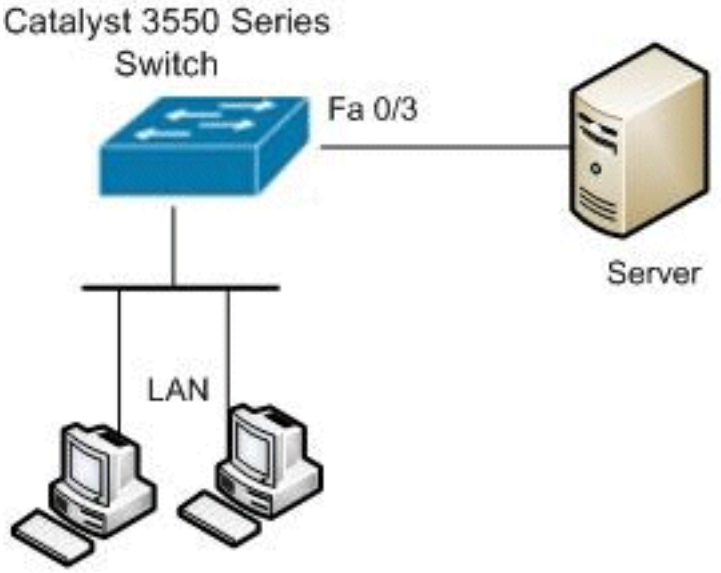
Configurez

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

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour 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 du 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
```

Vérifiez

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.

Employez la commande de switchport d'interfaces d'exposition [interface-id] 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 le show storm-control [interface-id] [émission | Multidiffusion | la commande d'unicast] afin de vérifier des niveaux de suppression de contrôle de tempête réglés sur l'interface pour le trafic indiqué tapent.

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
```

Employez la commande de show port-security [interface-id d'interface] afin de vérifier des configurations de Sécurité de port pour l'interface spécifiée.

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
```

Employez la commande d'adresse de show port-security [interface-id d'interface] afin de vérifier toutes les adresses MAC sécurisées configurées sur une interface spécifiée.

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
```

Informations connexes

- Page de support de Commutateurs de la gamme Cisco Catalyst 3550
- Page de support de Commutateurs de gamme Cisco Catalyst 3650
- Support pour commutateurs
- Prise en charge de la technologie de commutation LAN

- Support et documentation techniques - Cisco Systems