Catalyst Switches der Serien 3550/3560 mit portbasierter Datenverkehrssteuerung - Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration und Verifizierung für die portbasierten Datenverkehrskontrollfunktionen der Catalyst Switches der Serien 3550/3560. In diesem Dokument wird insbesondere die Konfiguration der portbasierten Datenverkehrskontrollfunktionen auf einem Catalyst 3550-Switch erläutert.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Grundkenntnisse der Konfiguration von Cisco Catalyst Switches der Serien 3550/3560
- Grundlegende Kenntnisse der portbasierten Datenverkehrskontrollfunktionen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Cisco Catalyst Switches der Serie 3550.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Portbasierte Datenverkehrskontrolle - Übersicht

Der Catalyst 3550/3560 Switch bietet eine portbasierte Datenverkehrskontrolle, die auf verschiedene Weise implementiert werden kann:

- Storm Control
- Geschützte Ports
- Portblockierung
- Port-Sicherheit

Storm Control verhindert Datenverkehr wie Broadcast, Multicast oder Unicast-Stürme an einer der physischen Schnittstellen des Switches. Übermäßiger Datenverkehr im LAN, der als LAN-Sturm bezeichnet wird, führt zu einer Beeinträchtigung der Netzwerkleistung. Verwenden Sie die Sturmkontrolle, um eine Beeinträchtigung der Netzwerkleistung zu vermeiden.

Die Storm Control überwacht die Pakete, die über eine Schnittstelle übertragen werden, und bestimmt, ob es sich um Unicast-, Multicast- oder Broadcast-Pakete handelt. Legen Sie den Schwellenwert für eingehenden Datenverkehr fest. Der Switch errechnet die Anzahl der Pakete nach dem empfangenen Pakettyp. Wenn der Broadcast- und Unicast-Datenverkehr den Schwellenwert für eine Schnittstelle überschreitet, wird nur der Datenverkehr eines bestimmten Typs blockiert. Wenn der Multicast-Datenverkehr den Grenzwert einer Schnittstelle überschreitet, wird der gesamte eingehende Datenverkehr blockiert, bis der Datenverkehr unter den Schwellenwert fällt. Verwenden Sie den Befehl Storm Control **Interface Configuration (Sturmkontrolle**-Schnittstellenkonfiguration), um die angegebene Sturmkontrolle für den Datenverkehr auf der Schnittstelle zu konfigurieren.

Konfigurieren Sie geschützte Ports auf einem Switch, der in einem Fall verwendet wird, in dem ein Nachbar den von einem anderen Nachbar generierten Datenverkehr nicht sehen sollte, sodass ein Teil des Anwendungsdatenverkehrs nicht zwischen Ports auf demselben Switch weitergeleitet wird. In einem Switch leiten Protected Ports keinen Datenverkehr (Unicast, Multicast oder Broadcast) an andere geschützte Ports weiter. Ein geschützter Port kann jedoch jeglichen Datenverkehr an ungeschützte Ports weiterleiten. Verwenden Sie den Befehl **switchport protected interface configuration auf einer Schnittstelle, um den Datenverkehr auf Layer 2 von anderen geschützten Ports zu isolieren.**

Sicherheitsprobleme können auftreten, wenn unbekannte MAC-Adressen-Adressen (Unicast und Multicast) an alle Ports im Switch geleitet werden. Um zu verhindern, dass unbekannter Datenverkehr von einem Port an einen anderen weitergeleitet wird, konfigurieren Sie die Portblockierung, die unbekannte Unicast- oder Multicast-Pakete blockiert. Verwenden Sie den Befehl **switchport block interface configuration, um die Weiterleitung von unbekanntem Datenverkehr zu verhindern.**

Verwenden Sie Port Security, um die Eingabe auf eine Schnittstelle zu beschränken, indem Sie die MAC-Adressen der Stationen identifizieren, die auf den Port zugreifen dürfen. Weisen Sie

einem sicheren Port sichere MAC-Adressen zu, sodass der Port keine Pakete mit Quelladressen außerhalb der Gruppe definierter Adressen weiterleitet. Verwenden Sie die Sticky-Learning-Funktion auf einer Schnittstelle, um die dynamischen MAC-Adressen in sichere MAC-Adressen umzuwandeln. Verwenden Sie den **Befehl switchport port-security interface configuration, um die Portsicherheitseinstellungen für die Schnittstelle zu konfigurieren.**

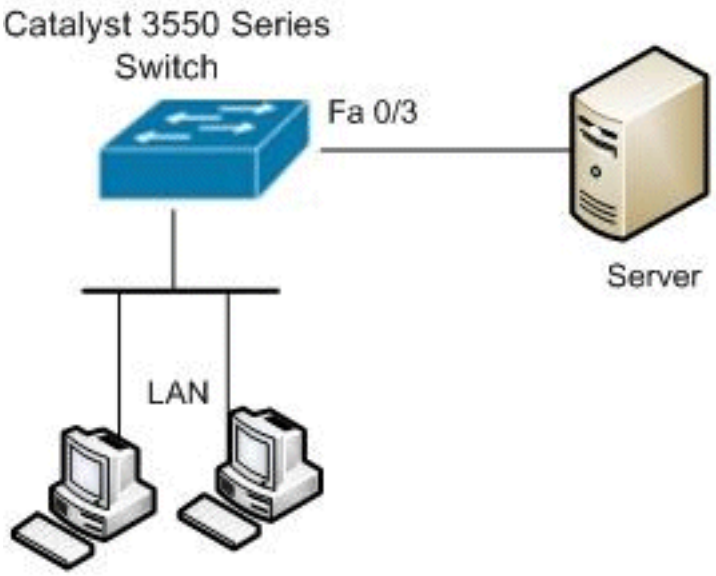
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfiguration

In diesem Dokument wird diese Konfiguration verwendet:

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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Mit dem Befehl **show interfaces [interface-id] switchport können Sie** Ihre Einträge überprüfen:

Beispiel:

```
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
```

Verwenden Sie die **Show Storm Control [Interface-ID] [Broadcast | Multicast | unicast]**-Befehl **zur** Überprüfung der auf der Schnittstelle für den angegebenen Datenverkehrstyp festgelegten Unterdrückungsstufen der Sturmkontrolle.

Beispiel:

```
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
```

Mit dem Befehl **show port-security [interface-id] können Sie die Portsicherheitseinstellungen für die angegebene Schnittstelle überprüfen.**

Beispiel:

```
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
```

Verwenden Sie den **Befehl** show port-security [interface interface-id] address**, um** alle sicheren MAC-Adressen zu überprüfen, die auf einer angegebenen Schnittstelle konfiguriert wurden.

Beispiel:

```
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
```

Zugehörige Informationen

- Support-Seite für Cisco Catalyst Switches der Serie 3550

- Support-Seite für Cisco Catalyst Switches der Serie 3650
- Produktsupport für Switches
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems