Switch Catalyst serie 3550/3560 Con Esempio Di Configurazione Del Controllo Del Traffico Basato Sulle Porte

Sommario

Introduzione

In questo documento viene fornito un esempio di configurazione e verifica delle funzionalità di controllo del traffico basate sulle porte sugli switch Catalyst serie 3550/3560. In particolare, in questo documento viene spiegato come configurare le funzionalità di controllo del traffico basate sulle porte su uno switch Catalyst 3550.

Prerequisiti

Requisiti

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti requisiti:

- Conoscenze base di configurazione sugli switch Cisco Catalyst serie 3550/3560.
- Conoscere a fondo le funzionalità di controllo del traffico basate sulle porte.

Componenti usati

Per la stesura del documento, sono stati usati switch Cisco Catalyst serie 3550.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Panoramica del controllo del traffico basato sulle porte

Lo switch Catalyst 3550/3560 offre un controllo del traffico basato sulle porte che può essere implementato in diversi modi:

- Controllo temporale
- Porte protette
- Blocco porte
- Sicurezza porta

Il controllo della temporizzazione impedisce il traffico, ad esempio una trasmissione, un multicast o un unicast, su una delle interfacce fisiche dello switch. L'eccesso di traffico sulla LAN, noto come tempesta LAN, causerà una riduzione delle prestazioni della rete. Utilizzare il controllo della temporizzazione per evitare il peggioramento delle prestazioni della rete.

Il controllo Storm osserva i pacchetti che passano attraverso un'interfaccia e determina se sono unicast, multicast o broadcast. Imposta il livello di soglia per il traffico in entrata. Lo switch conta il numero di pacchetti in base al tipo di pacchetto ricevuto. Se il traffico broadcast e unicast supera la soglia su un'interfaccia, viene bloccato solo il traffico di un determinato tipo. Se il traffico multicast supera la soglia su un'interfaccia, tutto il traffico in entrata viene bloccato finché il livello non scende al di sotto della soglia. Usare il comando di configurazione dell'interfaccia **storm-control** per configurare il controllo del traffico specificato sull'interfaccia.

Configurare le porte protette su uno switch nel caso in cui un router adiacente non possa visualizzare il traffico generato da un altro router adiacente, in modo che parte del traffico delle applicazioni non venga inoltrato tra le porte dello stesso switch. In uno switch, le porte protette non inoltrano alcun traffico (unicast, multicast o broadcast) ad altre porte protette, ma una porta protetta può inoltrare qualsiasi traffico a porte non protette. Per isolare il traffico sul layer 2 delle altre porte protette, usare il comando di configurazione dell'interfaccia **switchport protected** su un'interfaccia.

I problemi di sicurezza possono verificarsi quando il traffico di indirizzi MAC di destinazione sconosciuti (unicast e multicast) viene inviato a tutte le porte dello switch. Per evitare che il traffico sconosciuto venga inoltrato da una porta a un'altra, configurare il blocco delle porte, che bloccherà i pacchetti unicast o multicast sconosciuti. Per evitare che il traffico venga inoltrato, usare il comando di configurazione dell'interfaccia di blocco **switchport**.

Usare Port Security per limitare l'input a un'interfaccia identificando gli indirizzi MAC delle stazioni a cui è consentito accedere alla porta. Assegnare indirizzi MAC sicuri a una porta protetta, in modo che la porta non inoltri i pacchetti con indirizzi di origine esterni al gruppo di indirizzi definiti. Usare la funzione di apprendimento permanente su un'interfaccia per convertire gli indirizzi MAC dinamici in indirizzi MAC sicuri. Per configurare le impostazioni di sicurezza delle porte sull'interfaccia, usare il comando di configurazione dell'interfaccia **switchport port-security**.

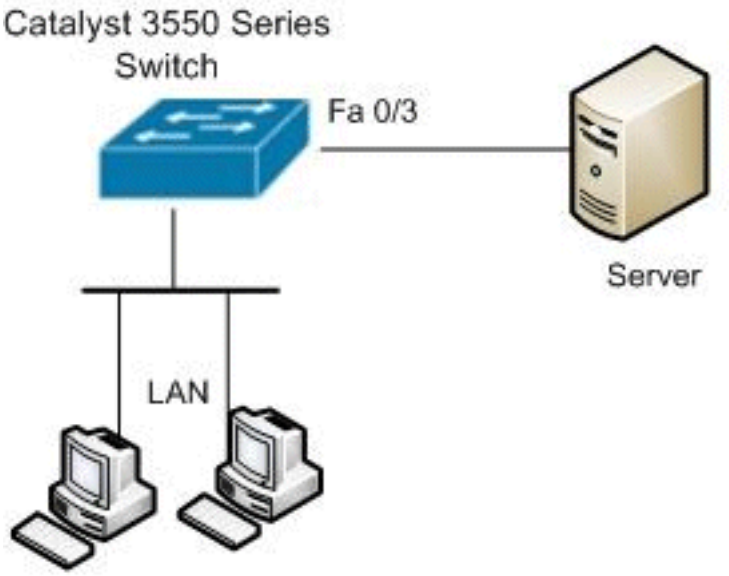
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione

Nel documento viene usata questa configurazione:

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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Utilizzare il comando show interfaces [id-interfaccia] switchport per verificare le voci immesse:

Ad esempio:

```
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
```

Utilizzare il comando show storm-control [interface-id] [broadcast] | multicast | unicast] per verificare i livelli di soppressione del controllo temporale impostati sull'interfaccia per il tipo di traffico specificato.

Ad esempio:

```
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
```

Usare il comando show port-security [interface-id] per verificare le impostazioni di sicurezza delle porte per l'interfaccia specificata.

Ad esempio:

```
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
```

Per verificare tutti gli indirizzi MAC sicuri configurati su un'interfaccia specificata, usare il comando show port-security [interface-id] address.

Ad esempio:

```
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
```

Informazioni correlate

- Pagina di supporto per gli switch Cisco Catalyst serie 3550
- Pagina di supporto per gli switch Cisco Catalyst serie 3650
- Switch - Supporto dei prodotti
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems