Exemplo de Configuração dos Catalyst 3550/3560 Series Switches Usando Controle de Tráfego Baseado em Porta

Contents

Introduction

Este documento fornece um exemplo de configuração e verificação para os recursos de controle de tráfego baseado em porta nos Catalyst 3550/3560 Series Switches. Especificamente, este documento mostra como configurar os recursos de controle de tráfego baseado em porta em um switch Catalyst 3550.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Ter conhecimento básico da configuração nos switches Cisco Catalyst 3550/3560 Series.
- Ter uma compreensão básica dos recursos de controle de tráfego baseados em porta.

Componentes Utilizados

As informações neste documento têm como referência os switches Cisco Catalyst 3550 Series.

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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Visão geral do controle de tráfego baseado em portas

O switch Catalyst 3550/3560 oferece controle de tráfego baseado em porta que pode ser implementado de várias maneiras:

- Controle de Tempestade de Mensagens
- Portas protegidas
- Bloqueio de portas
- Segurança da porta

O Controle de Tempestade de Mensagens evita o tráfego como um broadcast, um multicast ou uma tempestade unicast em uma das interfaces físicas do switch. O tráfego excessivo na LAN, conhecido como tempestade de LAN, levará a uma degradação do desempenho da rede. Use o controle de tempestade para evitar a degradação do desempenho da rede.

O Controle de Tempestade de Mensagens observa os pacotes que passam por uma interface e determina se os pacotes são unicast, multicast ou broadcast. Defina o nível de limite para o tráfego de entrada. O switch conta o número de pacotes de acordo com o tipo de pacote recebido. Se o tráfego de broadcast e unicast exceder o nível de limite em uma interface, somente o tráfego de um determinado tipo será bloqueado. Se o tráfego multicast exceder o nível de limite em uma interface, todo o tráfego de entrada será bloqueado até que o nível de tráfego caia abaixo do nível de limite. Use o comando de configuração de interface de controle de tempestade para configurar o controle de tempestade especificado de tráfego na interface.

Configurar portas protegidas em um switch usado em um caso em que um vizinho não deve ver o tráfego gerado por outro vizinho, de modo que algum tráfego de aplicativo não seja encaminhado entre portas no mesmo switch. Em um switch, as portas protegidas não encaminham nenhum tráfego (unicast, multicast ou broadcast) para nenhuma outra porta protegida, mas uma porta protegida pode encaminhar qualquer tráfego para portas não protegidas. Use o comando de configuração de interface switchport protected em uma interface para isolar o tráfego na Camada 2 de outras portas protegidas.

Problemas de segurança podem ocorrer quando o tráfego de endereços MAC de destino desconhecido (unicast e multicast) é inundado para todas as portas no switch. Para evitar que o tráfego desconhecido seja encaminhado de uma porta para outra porta, configure o Port Blocking, que bloqueará pacotes unicast ou multicast desconhecidos. Use o comando de configuração de interface switchport block para evitar o encaminhamento de tráfego desconhecido.

Use a segurança de porta para restringir a entrada a uma interface identificando os endereços MAC das estações que têm permissão para acessar a porta. Atribua endereços MAC seguros a uma porta segura, para que a porta não encaminhe pacotes com endereços de origem fora do grupo de endereços definidos. Use o recurso de aprendizado sticky em uma interface para converter os endereços MAC dinâmicos em endereços MAC com segurança sticky. Use o comando de configuração da interface switchport port-security para definir as configurações de segurança de porta na interface.

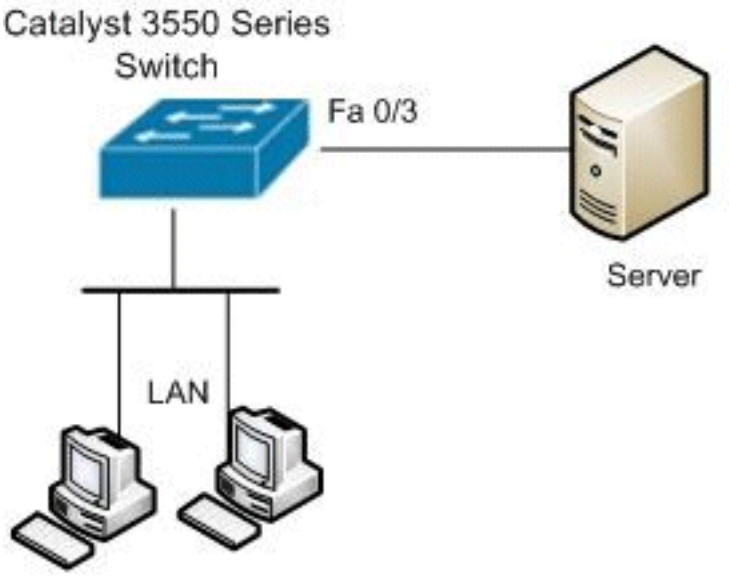
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configuração

Este documento utiliza esta configuração:

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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para visualizar uma análise da saída do comando **show**.

Use o comando **show interfaces [interface-id] switchport** para verificar suas entradas:

Por exemplo:

```
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
```

Use o comando **show storm-control [interface-id] [broadcast | multicast | unicast]** para verificar os níveis de supressão de controle de tempestade definidos na interface para o tipo de tráfego especificado.

Por exemplo:

```
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
```

Use o comando show port-security [interface interface-id] para verificar as configurações de segurança de porta da interface especificada.

Por exemplo:

```
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
```

Use o comando show port-security [interface interface-id] address para verificar todos os endereços MAC seguros configurados em uma interface especificada.

Por exemplo:

```
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
```

Informações Relacionadas

- Página de suporte dos switches Cisco Catalyst 3550 Series
- Página de suporte dos switches Cisco Catalyst 3650 Series
- Suporte ao Produto - Switches
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems