使用基于端口的流量控制配置示例的Catalyst 3550/3560系列交换机

目录

简介
先决条件
要求
使用的组件
规则
基于端口的流量控制概述
配置
网络图
配置
验证
相关信息

简介

本文档为Catalyst 3550/3560系列交换机上基于端口的流量控制功能提供配置和验证示例。具体而言，本文档介绍如何在 Catalyst 3550 交换机上配置基于端口的流量控制功能。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解Cisco Catalyst 3550/3560系列交换机的基本配置知识。
- 基本了解基于端口的流量控制功能。

使用的组件

本文档中的信息基于 Cisco Catalyst 3550 系列交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

基于端口的流量控制概述

Catalyst 3550/3560交换机提供基于端口的流量控制，可通过多种方式实施：

- 风暴控制
- 受保护端口
- 端口阻塞
- 端口安全性

风暴控制可防止交换机物理接口上的广播、组播或单播风暴等流量。LAN中的过多流量（称为LAN风暴）将导致网络性能下降。使用风暴控制来避免网络性能下降。

风暴控制观察通过接口的数据包并确定数据包是单播、组播还是广播。设置传入流量的阈值级别。交换机根据收到的数据包类型计算数据包数。如果广播和单播流量超过接口上的阈值级别，则仅阻止特定类型的流量。如果组播流量超过接口上的阈值级别，则所有传入流量都会被阻止，直到流量级别降至阈值级别以下。使用storm-control接口配置命令配置接口上指定的风暴控制流量。

在交换机上配置受保护端口，以防一个邻居看不到另一个邻居生成的流量时使用，这样，某些应用流量就不会在同一交换机的端口之间转发。在交换机中，受保护端口不会将任何流量（单播、组播或广播）转发到任何其他受保护端口，但受保护端口可以将任何流量转发到非受保护端口。在接口上使用switchport protected接口配置命令，将第2层的流量与其他受保护端口隔离。

当未知目的MAC地址流量（单播和组播）泛洪到交换机中的所有端口时，可能会出现安全问题。为防止未知流量从一个端口转发到另一个端口，请配置端口阻止(Port Blocking)，这将阻止未知单播或组播数据包。使用switchport block接口配置命令防止转发未知流量。

使用端口安全(Port Security)，通过识别允许访问端口的站点的MAC地址来限制接口的输入。将安全MAC地址分配给安全端口，以便端口不会转发源地址位于定义地址组外的数据包。在接口上使用粘滞学习功能将动态MAC地址转换为粘滞安全MAC地址。使用switchport port-security接口配置命令在接口上配置端口安全设置。

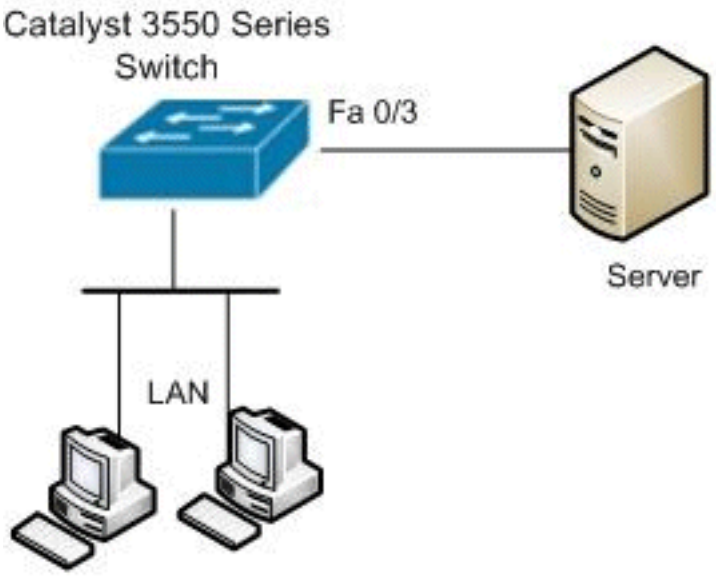
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：要获取有关本部分中所使用命令的更多信息，可使用命令查找工具（仅限已注册客户）。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

Catalyst 3550 交换机

```
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
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

请使用show interfaces [interface-id] switchport命令验证您的条目：

例如：

```
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
```

使用show storm-control [interface-id] [broadcast |组播 | unicast]命令，以验证接口上为指定流量类型设置的风暴控制抑制级别。

例如：

```
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
```

使用show port-security [interface interface-id]命令验证指定接口的端口安全设置。

例如：

```
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
```

使用show port-security [interface interface-id] address命令验证在指定接口上配置的所有安全MAC地址。

例如：

```
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
```

相关信息

- Cisco Catalyst 3550 系列交换机支持页面
- Cisco Catalyst 3650 系列交换机支持页面
- 交换机产品支持
- LAN 交换技术支持
- 技术支持和文档 - Cisco Systems