Catalyst 3550/3560 Series Switches Using Port−Based Traffic Control Configuration Example

Document ID: 113359

Contents

Introduction

This document provides a sample configuration and verification for the port−based traffic control features on your Catalyst 3550/3560 Series Switches. Specifically, this document shows you how to configure the port−based traffic control features on a Catalyst 3550 switch.

Prerequisites

Requirements

Make sure that you meet these requirements before you attempt this configuration:

- Have basic knowledge of configuration on Cisco Catalyst 3550/3560 Series Switches.
- Have a basic understanding of port−based traffic control features.

Components Used

The information in this document is based on the Cisco Catalyst 3550 Series Switches.

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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Port−Based Traffic Control Overview

The Catalyst 3550/3560 switch offers port−based traffic control that can be implemented in various ways:

- Storm Control
- Protected Ports
- Port Blocking
- Port Security

Storm Control prevents traffic such as a broadcast, a multicast, or a unicast storm on one of the physical interfaces of the switch. Excessive traffic in the LAN, referred to as a LAN storm, will lead to a degradation of network performance. Use storm control in order to avoid the degradation of network performance.

Storm Control observes the packets passing through an interface and determines whether the packets are unicast, multicast, or broadcast. Set the threshold level for incoming traffic. The switch counts the number of packets according to the type of packet received. If broadcast and unicast traffic exceed the threshold level on an interface, then only the traffic of a particular type is blocked. If the multicast traffic exceeds the threshold level on an interface, then all incoming traffic is blocked until the traffic level drops below the threshold level. Use the **storm−control** interface configuration command to configure the traffic specified storm control on the interface.

Configure Protected Ports on a switch used in a case when one neighbor should not see the traffic generated by another neighbor, so that some application traffic will not be forwarded between ports on the same switch. In a switch, Protected Ports does not forward any traffic (unicast, multicast, or broadcast) to any other protected ports, but a Protected Port can forward any traffic to non−protected ports. Use the **switchport protected** interface configuration command on an interface to isolate the traffic at Layer 2 from other protected ports.

Security issues can occur when unknown destination MAC addresses traffic (unicast and multicast) are flooded to all ports in the switch. In order to prevent unknown traffic being forwarded from one port to another port, configure Port Blocking, which will block unknown unicast or multicast packets. Use the **switchport block** interface configuration command to prevent unknown traffic being forwarded.

Use Port Security in order to restrict the input to an interface by identifying MAC addresses of the stations allowed to access the port. Assign secure MAC addresses to a secure port, so that the port does not forward packets with source addresses outside the group of defined addresses. Use sticky learning feature on an interface to convert the dynamic MAC addresses to sticky secure MAC addresses. Use the **switchport port−security** interface configuration command to configure the port security settings on the interface.

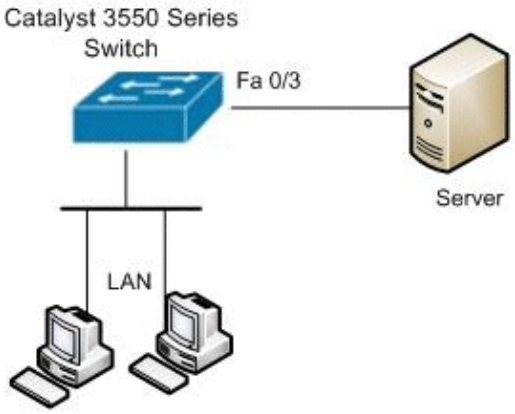
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configuration

This document uses this configuration:

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
```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT in order to view an analysis of **show** command output.

Use the **show interfaces [interface−id] switchport** command in order to verify your entries:

For example:

```
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 the **show storm−control [interface−id] [broadcast | multicast | unicast]** command in order to verify storm control suppression levels set on the interface for specified traffic type.

For example:

```
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 the **show port−security [interface interface−id]** command in order to verify port security settings for the specified interface.

For example:

```
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 the **show port-security [interface interface-id] address** command in order to verify all secure MAC addresses configured on a specified interface.

For example:

```
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
```

Related Information

- **Cisco Catalyst 3550 Series Switches Support Page**
- **Cisco Catalyst 3650 Series Switches Support Page**
- **Switches Product Support**
- **LAN Switching Technology Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Dec 21, 2011 Document ID: 113359