

포트 기반 트래픽 제어 컨피그레이션을 사용하는 Catalyst 3550/3560 Series 스위치 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[포트 기반 트래픽 제어 개요](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[다음을 확인합니다.](#)

[관련 정보](#)

[소개](#)

이 문서에서는 Catalyst 3550/3560 Series 스위치의 포트 기반 트래픽 제어 기능에 대한 샘플 컨피그레이션 및 검증을 제공합니다. 특히 이 문서에서는 Catalyst 3550 스위치에서 포트 기반 트래픽 제어 기능을 구성하는 방법을 보여줍니다.

[사전 요구 사항](#)

[요구 사항](#)

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- Cisco Catalyst 3550/3560 Series Switch에 대한 컨피그레이션에 대한 기본적인 지식을 보유하고 있습니다.
- 포트 기반 트래픽 제어 기능에 대한 기본적인 이해가 있어야 합니다.

[사용되는 구성 요소](#)

이 문서의 정보는 Cisco Catalyst 3550 Series 스위치를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

[표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

[포트 기반 트래픽 제어 개요](#)

Catalyst 3550/3560 스위치는 다양한 방식으로 구현할 수 있는 포트 기반 트래픽 제어를 제공합니다.

- 스톱 컨트롤
- 보호된 포트
- 포트 차단
- 포트 보안

Storm Control은 스위치의 물리적 인터페이스 중 하나에서 브로드캐스트, 멀티캐스트 또는 유니캐스트 스톱과 같은 트래픽을 방지합니다. LAN의 과도한 트래픽(LAN 스톱)은 네트워크 성능 저하를 초래할 수 있습니다. 네트워크 성능 저하를 방지하려면 스톱 제어를 사용합니다.

Storm Control은 인터페이스를 통과하는 패킷을 관찰하고 패킷이 유니캐스트, 멀티캐스트 또는 브로드캐스트인지 결정합니다. 수신 트래픽의 임계값 레벨을 설정합니다. 스위치는 수신된 패킷 유형에 따라 패킷 수를 계산합니다. 브로드캐스트 및 유니캐스트 트래픽이 인터페이스의 임계값 수준을 초과할 경우 특정 유형의 트래픽만 차단됩니다. 멀티캐스트 트래픽이 인터페이스의 임계값 수준을 초과하면 트래픽 수준이 임계값 수준 아래로 떨어질 때까지 모든 수신 트래픽이 차단됩니다. 인터페이스에서 [지정된 트래픽](#)을 구성하려면 storm-control interface configuration 명령을 사용합니다.

한 인접 디바이스가 다른 인접 디바이스에서 생성한 트래픽을 볼 수 없는 경우에 사용되는 스위치에서 Protected Ports를 구성하여 일부 애플리케이션 트래픽이 동일한 스위치의 포트 간에 전달되지 않도록 합니다. 스위치에서 Protected Ports는 어떤 트래픽(유니캐스트, 멀티캐스트 또는 브로드캐스트)도 다른 보호된 포트에 전달하지 않지만, Protected Port는 모든 트래픽을 보호되지 않는 포트에 전달할 수 있습니다. 인터페이스에서 switchport **protected interface configuration 명령**을 사용하여 레이어 2의 트래픽을 다른 보호된 포트와 격리합니다.

알 수 없는 대상 MAC 주소 트래픽(유니캐스트 및 멀티캐스트)이 스위치의 모든 포트에 플러딩될 때 보안 문제가 발생할 수 있습니다. 알 수 없는 트래픽이 한 포트에서 다른 포트에 전달되지 않도록 하려면 알 수 없는 유니캐스트 또는 멀티캐스트 패킷을 차단하는 포트 차단을 구성합니다. [switchport block interface](#) 컨피그레이션 명령을 사용하여 알 수 없는 트래픽이 전달되지 않도록 합니다.

포트에 액세스할 수 있는 스테이션의 MAC 주소를 식별하여 인터페이스에 대한 입력을 제한하려면 포트 보안을 사용합니다. 보안 MAC 주소를 보안 포트에 할당하여 포트가 정의된 주소 그룹 외부의 소스 주소로 패킷을 전달하지 않도록 합니다. 인터페이스에서 스티커 학습 기능을 사용하여 동적 MAC 주소를 스티커 보안 MAC 주소로 변환합니다. 인터페이스에서 [포트 보안 설정](#)을 구성하려면 switchport port-security interface configuration 명령을 사용합니다.

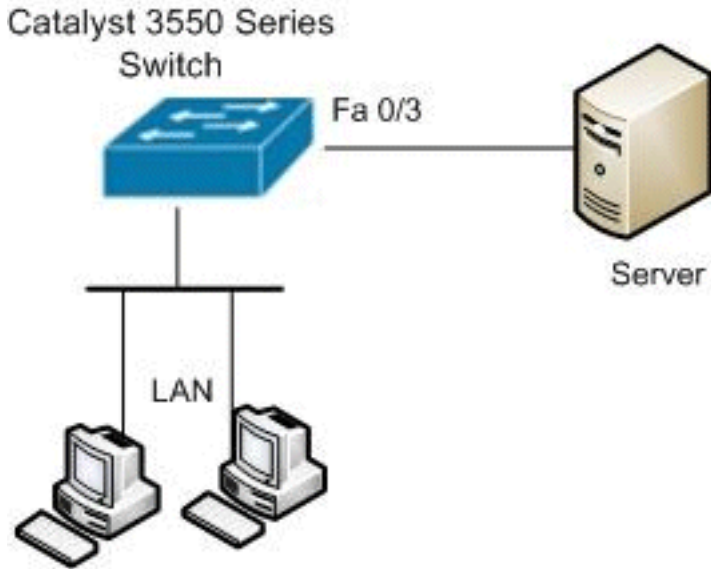
[구성](#)

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 [명령 조회 도구](#)([등록된 고객만 해당](#))를 사용하십시오.

[네트워크 다이어그램](#)

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output [Interpreter 도구\(등록된 고객만 해당\)](#)(OIT)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 OIT를 사용합니다.

항목을 확인하려면 [show interfaces \[interface-id\] switchport](#) 명령을 사용합니다.

예를 들면 다음과 같습니다.

```
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
```

[show storm-control \[interface-id\] \[broadcast\]](#) 사용 | [멀티캐스트 | unicast](#) 지정된 트래픽 유형에 대해 인터페이스에 설정된 스톱 제어 억제 레벨을 확인하기 위한 명령입니다.

예를 들면 다음과 같습니다.

```
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
```

지정된 인터페이스에 대한 포트 보안 설정을 확인하려면 [show port-security \[interface interface-id\]](#) 명령을 사용합니다.

예를 들면 다음과 같습니다.

```
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
```

지정된 인터페이스에 구성된 모든 보안 MAC 주소를 확인하려면 [show port-security \[interface interface-id\] address](#) 명령을 사용합니다.

예를 들면 다음과 같습니다.

```
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
```

[관련 정보](#)

- [Cisco Catalyst 3550 Series 스위치 지원 페이지](#)
- [Cisco Catalyst 3650 Series 스위치 지원 페이지](#)
- [스위치 제품 지원](#)
- [LAN 스위칭 기술 지원](#)
- [기술 지원 및 문서 - Cisco Systems](#)