Catalyst 3550/3560 Серия Переключает Использование Примера конфигурации Управления трафиком На основе порта

Содержание

Введение

Этот документ предоставляет пример конфигурации и проверку для функций управления трафиком на основе порта на вашем Catalyst 3550/3560 Коммутаторы Серии. В частности этот документ показывает вам, как настроить функции управления трафиком на основе порта на Коммутаторе Catalyst 3550.

Предварительные условия

Требования

Удостоверьтесь в соответствии этим требованиям перед попыткой применения этой конфигурации:

- Имейте базовые знания о конфигурации на Cisco Catalyst 3550/3560 Коммутаторы Серии.
- Имейте основное понимание функций управления трафиком на основе порта.

Используемые компоненты

Сведения в этом документе основываются на коммутаторах Cisco Catalyst серии 3550.

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Обзор управления трафиком на основе порта

Catalyst 3550/3560 коммутатор предлагает управление трафиком на основе порта, которое может быть внедрено в различных способах:

- Контроль шторма
- Защищенные порты
- Блокирование порта
- Безопасность портов

Управление штормом предотвращает трафик, такой как широковещание, групповая адресация или шторм индивидуальной рассылки на одном из физических интерфейсов коммутатора. Избыточный трафик в LAN, называемой штормом LAN, приведет к ухудшению производительности сети. Используйте управление штормом во избежание ухудшения производительности сети.

Управление штормом наблюдает пакеты, проходящие через интерфейс, и определяет, одноадресно переданы ли пакеты, переданы в многоадресном режиме или переданы. Установите пороговый уровень для входящего трафика. Коммутатор считает количество пакетов согласно типу пакета полученным. Если передано и трафик с конкретным адресом превышают пороговый уровень на интерфейсе, то только трафик определенного типа заблокирован. Если многоадресный трафик превышает пороговый уровень на интерфейсе, то весь входящий трафик заблокирован, пока уровень трафика не опускается ниже порогового уровня. Используйте команду настройки интерфейса storm-control для настройки заданного управления штормом трафика на интерфейсе.

Настройте Защищенные порты на коммутаторе, используемом в случае, когда один соседний узел не должен видеть трафик, генерируемый другим соседним узлом, так, чтобы некоторый трафик приложения не был передан между портами на том же коммутаторе. В коммутаторе Защищенные порты не передают трафика (одноадресно передайте, передайте в многоадресном режиме, или широковещание) к любым другим защищенным портам, но Защищенному порту может передать любой трафик к незащищенным портам. Используйте команду настройки интерфейса switchport protected на интерфейсе для изоляции трафика на Уровне 2 от других защищенных портов.

Проблемы безопасности могут произойти, когда трафик MAC-адресов неизвестного назначения (одноадресно передавал и передавал в многоадресном режиме), лавинно рассылается ко всем портам в коммутаторе. Для предотвращения неизвестного трафика, передаваемого от одного порта до другого порта, настройте Блокирование порта, которое заблокирует одноадресного одноадресного или пакеты групповой адресации. Используйте команду настройки интерфейса switchport block для предотвращения передаваемого неизвестного трафика.

Используйте Защиту на уровне порта для ограничения ввода интерфейсом путем определения MAC-адресов станций, позволенных обратиться к порту. Назначьте безопасные MAC-адреса на защищенный порт, так, чтобы порт не делал передач пакетов с адресами источника вне группы определенных адресов. Используйте функцию обучения sticky на интерфейсе для преобразования динамических MAC-адресов в sticky безопасные MAC-адреса. Используйте команду настройки интерфейса switchport port-security для настройки параметров настройки защиты на уровне порта на интерфейсе.

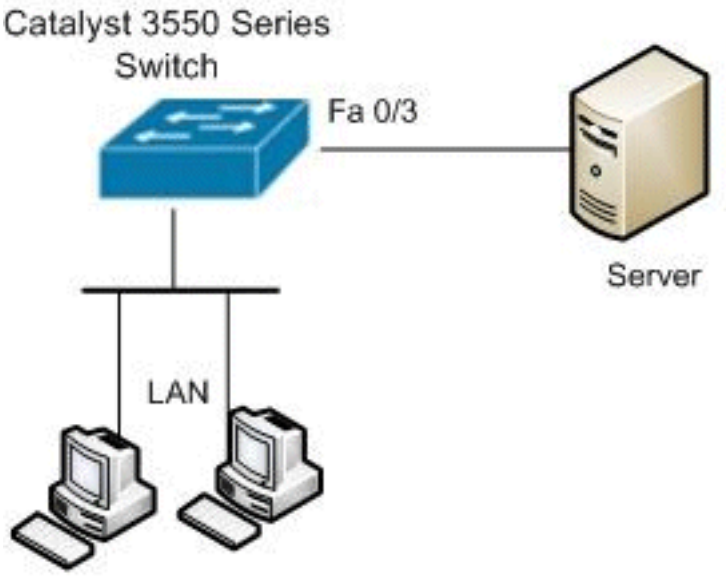
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



!--- конфигурацию

В данном документе используется следующая конфигурация:

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
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Используйте OIT для просмотра анализа выходных данных команды show.**

Используйте **show interfaces [interface-id] команда switchport** для проверки записей:

Пример:

```
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
```

Используйте **show storm-control [interface-id] [широковещание | групповая адресация | индивидуальная рассылка]** команда для проверки набора уровней подавления управления штормом на интерфейсе для типа указанного потока данных.

Пример:

```
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
```

Используйте show port-security [интерфейсный interface-id] команда для проверки параметров настройки защиты на уровне порта для заданного интерфейса.

Пример:

```
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
```

Используйте show port-security [интерфейсный interface-id] команда адреса для проверки всех безопасных MAC-адресов, настроенных на заданном интерфейсе.

Пример:

```
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
```

Дополнительные сведения

- Страница технической поддержки коммутаторов Cisco Catalyst серии 3550
- Cisco Catalyst страница технической поддержки коммутаторов серии 3650

- Поддержка коммутаторов
- Поддержка технологии коммутации локальных сетей
- Cisco Systems – техническая поддержка и документация