

Особенности конфигурирования коммутаторов Cisco Catalyst в комплексных системах безопасности

Используя сеть, особенно ресурсы сети общего использования, для функционирования системы безопасности, пользователи должны быть уверены, что конфиденциальная информация попадет именно тому, кому она предназначена. Для этих целей используется гибкая, динамическая архитектура сетевой безопасности и виртуальных частных сетей. Возможности обеспечения безопасности сети должны быть сосредоточены не на отдельных продуктах, а на системном подходе для решения следующих задач:

- Защита информации и ресурсов от несанкционированного доступа.
- Активный динамический контроль за использованием сети пользователями.
- Обнаружение атак на критически важные ресурсы и подсети.

В данном случае мы рассматриваем коммутаторы *Cisco Catalyst* как устройства, обеспечивающие соединение между системами безопасности и пользователями систем безопасности на базе локальной сети. Это позволяет пользователю, находясь в любой точке локальной сети, осуществлять управление всем комплексом системы безопасности.

Конфигурирование коммутаторов *Cisco Catalyst* позволяет обеспечить высокий уровень безопасности соединений между сетевыми устройствами. Это позволяет ограничить доступ пользователей к устройствам, обеспечить непрерывную связь устройств с высоким приоритетом в случае перегрузки сети, а также уменьшить вред, наносимый несанкционированными действиями пользователя.

Пример конфигурирования коммутаторов Cisco Catalyst в системах безопасности, подключенных к локальной компьютерной сети

Конфигурацию функций безопасности на коммутаторах Cisco Catalyst 2950 и Cisco Catalyst 3750 мы рассмотрим на примере локальной компьютерной сети, показанной на рис.1.

Система безопасности представлена следующими подсистемами: система контроля и управления доступом (СКУД) на базе контроллера PW-5000 (Honeywell Security) и система телевизионного наблюдения (СТН) на базе цифрового видеорегистратора Fusion (Honeywell Video Systems).

Для подключения контроллера PW-5000 к коммутатору сети требуется сетевой модуль PW5K1EN (Honeywell Security). Выход модуля подключается через коннектор RJ-45 к коммутатору. Далее требуется установить сетевой адрес контроллера (принадлежащий адресному пространству сети), в рассмотренном случае задан адрес 10.0.0.201. Для подключения видеорегистратора Fusion используется встроенная сетевая карта Ethernet, которая подключается к коммутатору сети через RJ-45 коннектор. Далее также устанавливается сетевой адрес, в рассмотренном случае - это 10.0.0.200.

Если контроллеров или видеорегистраторов в сети несколько, то на каждое устройство устанавливается свой индивидуальный сетевой адрес. Пользователи системы безопасности осуществляют работу в сети со своих рабочих мест, используя стандартные процедуры подключения.

Локальная сеть 10.0.0.0

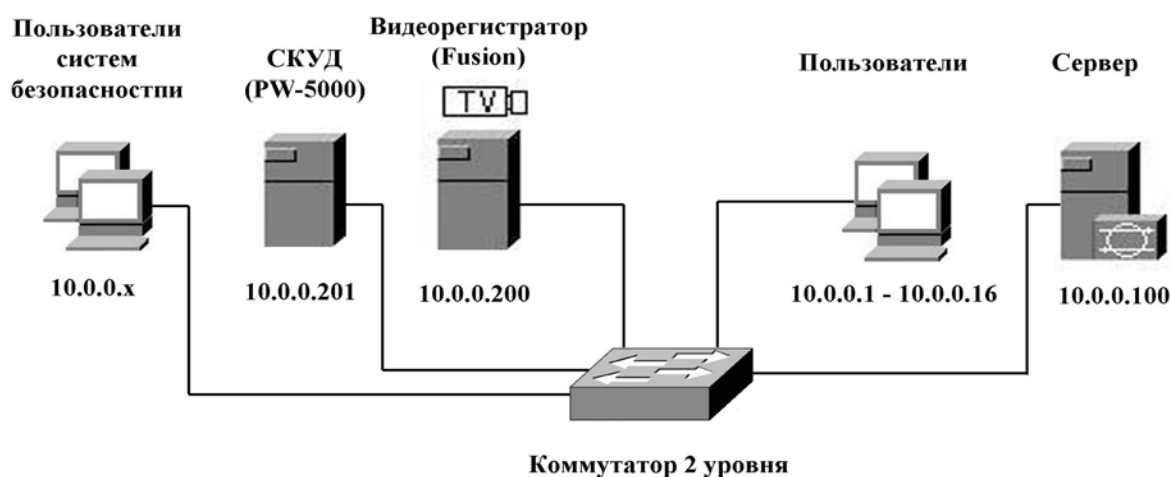


Рис.1. Локальная сеть.

Для обеспечения информационной безопасности сети будут реализованы следующие задачи:

1. Разделить сеть на сеть систем безопасности и пользовательскую сеть.
2. Ограничить доступ к системам безопасности и установить фильтрацию трафика.
3. Обеспечить безопасность портов коммутатора.
4. Определить качество обслуживания, которое заключается в определении алгоритмов, согласно которым коммутаторы осуществляют доставку различных видов трафика.

Разделение сети на сеть систем безопасности и пользовательскую сеть

Разделим всю сеть на сеть систем безопасности и пользовательскую сеть с помощью технологии сетей VLAN. Сети VLAN (Virtual Local Area Network) - это определенные внутри коммутатора широковещательные домены, позволяющие внутри устройства второго уровня управлять широковещательными, многоадресными, одноадресными рассылками, а также одноадресными рассылками с неизвестным получателем.

Разделение на сети VLAN позволит избежать случайного соединения пользователей с системами безопасности. Создадим две сети VLAN и назначим им порты, к которым подключены пользователи (для пользовательской VLAN), и порты, к которым подключены системы безопасности, а также пользователи систем безопасности (VLAN систем безопасности).

Так же возможно создание узлов, доступных для любого пользователя **частной** VLAN (возможно на коммутаторах Catalyst 3750 enhanced version).

После конфигурирования VLAN в целях безопасности следует отключить default VLAN (VLAN, установленная по умолчанию).

Данная конфигурация позволяет широковещательным запросам распространяться только в своей VLAN, что повышает производительность сети.

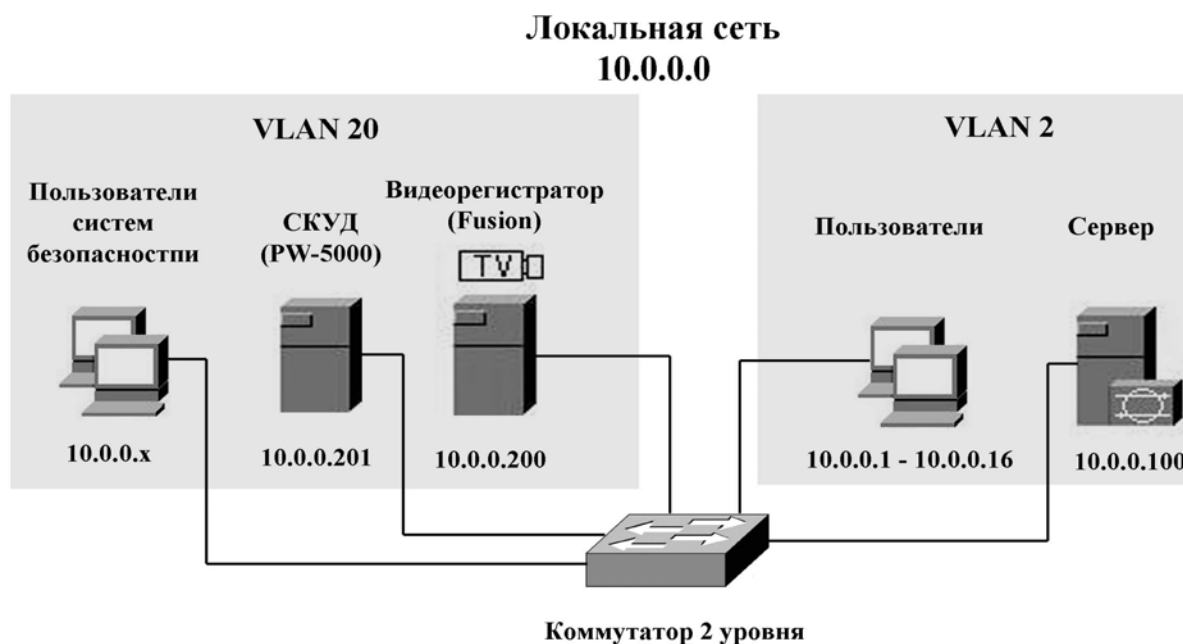


Рис.2. Разбиение локальной сети на VLAN.

Например:

```
#vlan database
(vlan)#vlan 2
(vlan)#end
#conf t
(config)#vlan 2
(config-vlan)#name VLAN 2 (Задается имя выбранной VLAN)
(config-vlan)#interface type/mode
(config-if)#switchport access vlan 2
(config-if)#end
```

Ограничение доступа к системам безопасности и установка фильтрации трафика

Списки контроля доступа (Access Control List-ACL) определяют то, каким образом трафик обрабатывается при прохождении через сетевое устройство. В ACL для управления обменом данными используется адресная информация и сведения о портах.

В рассматриваемом случае, наиболее эффективным методом будет запрещение передачи информации на те устройства, которым не понадобится эта информация или она будет вредоносной.

Например:

- Запретить IP трафик между сервером 10.0.0.100 и системами безопасности 10.0.0.200 и 10.0.0.201.
- Запретить IP трафик между системами безопасности 10.0.0.200 и 10.0.0.201 и адресами с 10.0.0.1 по 10.0.0.16.
- Запретить UDP трафик.

```

#conf t
(config)#access-list 101 deny ip host 10.0.0.100 host 10.0.0.200
(config)#access-list 101 deny ip host 10.0.0.100 host 10.0.0.201
(config)#access-list 101 deny udp any any
(config)#access-list 101 permit ip any any (эта команда разрешает остальной трафик)
(config)#interface vlan 20
(config-if)#ip access-group 101 in (входящий трафик)
(config)#access-list 102 deny ip host 10.0.0.200 10.0.0.0 0.0.0.15
(config)#access-list 102 deny ip host 10.0.0.201 10.0.0.0 0.0.0.15
(config)#access-list 102 deny ip host 10.0.0.200 host 10.0.0.16
(config)#access-list 102 deny ip host 10.0.0.201 host 10.0.0.16
(config)#access-list 102 permit ip any any
(config)#interface vlan 20
(config-if)#ip access-group 102 out (исходящий трафик)

```

В результате трафик, неподходящий к установленным условиям, будет отброшен. Следует учитывать, что ACL по умолчанию заканчивается строкой **access-list access-list-number deny ip any any**, которая запрещает трафик, не удовлетворяющий ни одному поставленному условию.

Обеспечение безопасности портов коммутатора

Функция безопасности портов коммутатора позволяет настроить какой-либо порт коммутатора так, так чтобы доступ к коммутатору через этот порт предоставлялся только заданному устройству или группе устройств. При обращении к порту с неавторизованного MAC-адреса коммутатор может приостановить работу порта или отключить его.

В рассматриваемом случае на каждый порт следует привязать один разрешенный MAC-адрес, и отключение порта в случае подключения устройства с другим MAC-адресом.

Например:

```

(config)#interface type/mode
(config-if)#switchport mode access
(config-if)#switchport port-security
(config-if)#switchport port-security maximum 1 (число разрешенных подключений)
(config-if)#switchport port-security mac-address Н.Н.Н (Н.Н.Н - MAC-адрес подключаемого устройства)
(config-if)#switchport port-security violation shutdown
(config-if)#end

```

Следует учитывать, что коммутаторы имеют ограниченное число адресов, для которых можно обеспечить безопасность портов, поэтому для обеспечения безопасности для большого числа адресов, следует ознакомиться со специальной документацией на используемое аппаратное обеспечение.

Определение качества обслуживания коммутатора

Качество обслуживания (Quality of Service-QoS) коммутаторов определяет алгоритмы, согласно которым коммутаторы осуществляют доставку различных типов трафика. Для этого требуется классифицировать трафик, то есть выбрать определенный трафик, к которому будет применяться QoS-стратегия. Классификация трафика может осуществляться на входных портах коммутатора.

В рассмотренном ниже примере будет заданна конфигурация для исходящего трафика, а так же буферизация его в памяти коммутатора в зависимости от приоритета. В данном примере будет

привилегирован трафик от видеорегистратора Fusion, сконфигурированы исходящие очереди на рабочие станции.

Например:

```
(config-if)#mls qos cos cos-id (установка приоритета от 0 до 7 на порту подключенного к видеорегистратору Fusion, в данном случае 7)
```

```
(config)#mls qos (включение режима QoS)
```

```
(config)#mls qos queue-set output qset-id buffers 20 20 20 40 (устанавливается процентное значение для каждой очереди выделенное в буфере)
```

```
(config)#mls qos queue-set output qset-id threshold queue-id 50 80 50 400 (первое значение это нижний порог отбрасывания фреймов, второе - верхний, третье - зарезервированное место в памяти, четвертое - максимальное доступное место в общей памяти)
```

```
(config)#interface interface-id (порт к которому подключена рабочая станция)
```

```
(conng-if)#srr-queue bandwidth shape 0 0 0 8 (устанавливается полоса пропускания для каждой очереди)
```

```
(config-if)#srr-queue bandwidth share 200 100 150 255 (устанавливается вес обслуживания для каждой очереди передачи)
```

```
(config-if)#queue-set qset-id (установка шаблона на порт)
```

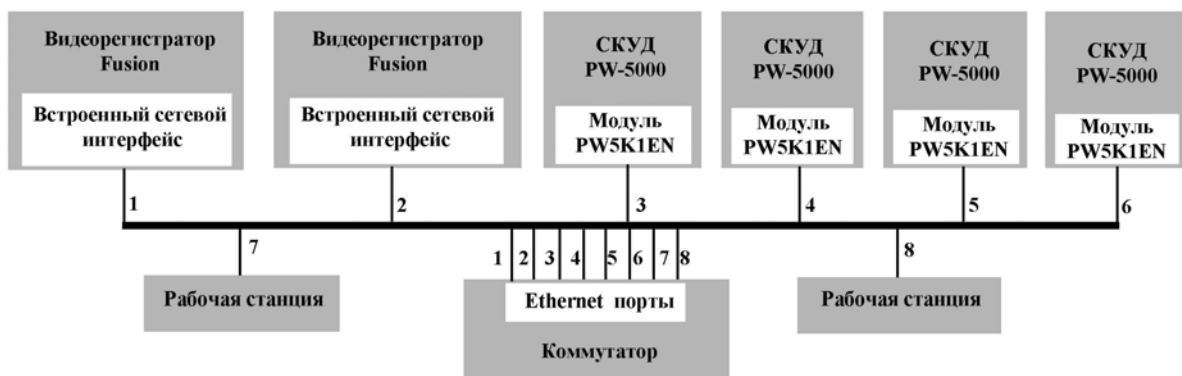
При конфигурировании буфера и порогов следует заметить, что значение *qset-id* является шаблоном настроек, которые применяются к данному порту, а значение *queue-id* определяет очередь. В данном случае была сконфигурирована исходящая очередь для приоритетов 6 и 7. После установки на порту значения *cos-id*, приоритет входящей информации преобразовывается в соответствующее значение.

При программировании буфера следует учитывать, что сумма значений для всех очередей не должна превышать 100%. Следует так же внимательно устанавливать пороги отбрасывания фреймов. Если для очереди размер буфера достигает своего порогового значения (первое значение устанавливается от 1 до 400%), то фреймы начинают отбрасываться, при достижении второго порогового (устанавливаются от 1 до 400%) значения отбрасываются все фреймы данной очереди. Третье значение определяет место в резервной памяти (значения от 1 до 100%), а четвертое - выделенное место для очереди в общей памяти (значения от 1 до 400%).

Конфигурация полосы пропускания выполняется командой **srr-queue bandwidth shape**, далее указываются весовые коэффициенты. Следует учесть, что они вводятся как 1/коэффициент.

В показанном примере мы установили полосу пропускания для четвертой очереди 12,5% = 1/8 (значения от 1 до 65535). Регулировка веса обслуживания выполняется командой **srr-queue bandwidth share**, после чего устанавливается вес обслуживания очереди (от 1 до 255). В примере показано, что четвертая очередь имеет самый большой вес, соответственно эта очередь будет обслужена первой.

Пример структурной схемы системы безопасности



Спецификация оборудования.

| № | Наименование | Обозначение | Кол-во |
|----------|--|--------------------|---------------|
| 1. | Система контроля и управления доступом PW-5000 | PW-5000 | 4 |
| 2. | Видеорегистратор Fusion | Fusion | 2 |
| 3. | Коммутатор Cisco Catalyst 2950 | Коммутатор | 1 |
| 4. | Рабочая станция | Рабочая станция | 2 |