ПОЯСНЕНИЕ, ПОЧЕМУ МАЛО БАЛЛОВ В pkt ФАЙЛЕ:

Не засчитывает добавление интерфейсов в vlan BlackHole (скорее всего ошибка в названии)

Packet Tracer - Конфигурация безопасности коммутатора

Таблица VLAN

Коммутатор	Номер VLAN	Имя VLAN	Членство в порту	Сеть
SW-1	10	Администратор	F0/1, F0/2	192.168.10.0/24
	20	Продажи	F0/10	192.168.20.0/24
	99	Управление	F0/24	192.168.99.0/24
	100	Собственный	G0/1, G0/2	Нет
	999	BlackHole	Все неиспользуемые	Нет
SW-2	10	Администратор	F0/1, F0/22	192.168.10.0/24
	20	Продажи	F0/10	192.168.20.0/24
	99	Управление	F0/24	192.168.99.0/24
	100	Собственный	Нет	Нет
	999	BlackHole	Все неиспользуемые	None

Задачи

Часть 1. Создание защищенного магистрального соединения

Часть 2: Безопасность неиспользуемых портов коммутатора

Часть 3: Обеспечение безопасности портов

Часть 4: Включение отслеживание DHCP

Часть 5: Настройка Rapid PVST, PortFast и BPDU Guard

Общая информация

Вы повышаете безопасность на двух коммутаторах доступа в частично настроенной сети. Вы реализуете ряд мер безопасности, описанных в этом модуле, в соответствии с приведенными ниже требованиями. Обратите внимание, что в этой сети настроена маршрутизация, поэтому соединение между узлами в разных VLAN должно функционировать после завершения.

Инструкция

Шаг 1:Создание защищенного магистрального соединения

а. Соедините порты G0/2 двух коммутаторов уровня доступа.

б. Настройте порты G0/1 и G0/2 как статическое магистральное соединение на обоих коммутаторах.

в. Отключите согласование DTP на обеих сторонах канала.

г. Создайте VLAN 100 и присвойте ей имя Native на обоих коммутаторах.

д. Настройте все магистральные порты на обоих коммутаторах для использования VLAN 100 в качестве native VLAN.

```
SW-1(config)#int range g0/1-2
SW-1(config-if-range)#switchport mode trunk
```

```
SW-1(config-if-range)#switchport nonegotiate
SW-1(config-if-range)#exit
SW-1(config)#vlan 100
SW-1(config-vlan)#name Na
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (1), with DLS1
GigabitEthernet1/0/1 exit
SW-1(config)#vlan 100
SW-1(config-vlan)#name Native
SW-1(config-vlan)#exit
SW-1(config)#int range g0/1-2
```

```
SW-1(config-if-range)#switchport trunk native vlan 100
```

```
SW-2(config)#int range g0/1-2
SW-2(config-if-range)#switchport mode trunk

SW-2(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 100 on GigabitEthernet
VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet0/1 on VLAN0001. Inconsistent local vlan


SW-2(config-if-range)#switchport nonegotiate
SW-2(config-if-range)#exit
SW-2(config)#vlan 100
SW-2(config-vlan)#name Native
SW-2(config-vlan)#exit
SW-2(config)#int range g0/1-2
SW-2(config-if-range)#switchport trunk native vla
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (1), with D
Gswitchport trunk native vlan 100
SW-2(config-if-range)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking GigabitEthernet0/1 on VLAN0
Port consistency restored.
```

Шаг 2: Безопасность неиспользуемых портов коммутатора

а. Отключите все неиспользуемые порты на коммутаторе SW-1.

```
SW-1(config)#int range f0/3-9, f0/11-24
SW-1(config-if-range)#shutdown
```

б. На коммутаторе S1 создайте сеть VLAN 86 и присвойте ей имя BlackHole. Настроенное имя должно точно соответствовать требованию.

в. Переместите все неиспользуемые порты коммутатора во VLAN BlackHole.

```
SW-1(config)#vlan 86
SW-1(config-vlan)#name BlackHole
SW-1(config-vlan)#exit
SW-1(config)#int range f0/3-9, f0/11-24
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 86
SW-1(config-if-range)#int range f0/3-9, f0/11-23
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 86
SW-1(config-if-range)#exit
```

Шаг 3: Настройте параметры безопасности портов.

а. Активируйте защиту портов на всех активных портах доступа на коммутаторе SW-1.

б. Сконфигурируйте активные порты, чтобы разрешить изучение максимум 4 MAC-адресов на портах.

в. Для портов F0/1 на SW-1 статически сконфигурируйте MAC-адрес компьютера с использованием защиты порта.

г. Настройте каждый активный порт доступа таким образом, чтобы он автоматически добавлял адреса MAC, изученные на этом порту, в текущую конфигурацию.

д. Настройте режим нарушения безопасности порта, чтобы отбрасывать пакеты с MAC-адресов, которые превышают максимум, генерировать запись системного журнала, но не отключать порты.

```
SW-1(config)#int range f0/24, f0/1-2, g0/1-2
SW-1(config-if-range)# switchport port-security
SW-1(config-if-range)# switchport port-security
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/
SW-1(config-if-range)# switchport port-security maximum 4
SW-1(config-if-range)# switchport port-security mac-address sticky
SW-1(config-if-range)# switchport port-security violation restrict
```

Шаг 4: Настройте анализ DHCP-трафика.

а. Настройте магистральные порты на SW-1 как доверенные порты.

```
SW-1(config)#int range g0/1-2
SW-1(config-if-range)#ip dhcp snooping trust
```

б. Ограничьте ненадежные порты на SW-1 пятью DHCP-пакетами в секунду.

```
SW-1(config-if-range)#ip dhcp snooping trust
SW-1(config-if-range)#exit
SW-1(config)#int range f0/3-9, f0/11-23
SW-1(config-if-range)#ip dhcp snooping limit rate 5
SW-1(config-if-range)#
```

в. На SW-2 включите DHCP snooping глобально и для VLAN 10, 20 и 99.

```
SW-2>enable
SW-2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-2(config)#ip dhcp snooping
SW-2(config)#ip dhcp snooping vlan 10,20,99
SW-2(config)#
```

Примечание. Конфигурация отслеживания DHCP может не работать должным образом в Packet Tracer.

Часть 5. Настройка PortFast и BPDU Guard

а. Включите PortFast на всех портах доступа, которые используются на SW-1.

б. Включите BPDU Guard на всех портах доступа, которые используются на SW-1.

```
SW-1(config)#int range g0/1-2
SW-1(config-if-range)#ip dhcp snooping trust
SW-1(config-if-range)#exit
SW-1(config)#int range f0/3-9, f0/11-23
SW-1(config-if-range)#ip dhcp snooping limit rate 5
SW-1(config-if-range)#int range f0/1-2, f0/10, f0/24
SW-1(config-if-range)#spanning-tree portfast
```

в. Настройте SW-2, чтобы все порты доступа использовали PortFast по умолчанию.

```
SW-2>enable
SW-2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-2(config)#ip dhcp snooping
SW-2(config)#ip dhcp snooping vlan 10,20,99
SW-2(config)#spanning-tree portfast default
SW-2(config)#
```