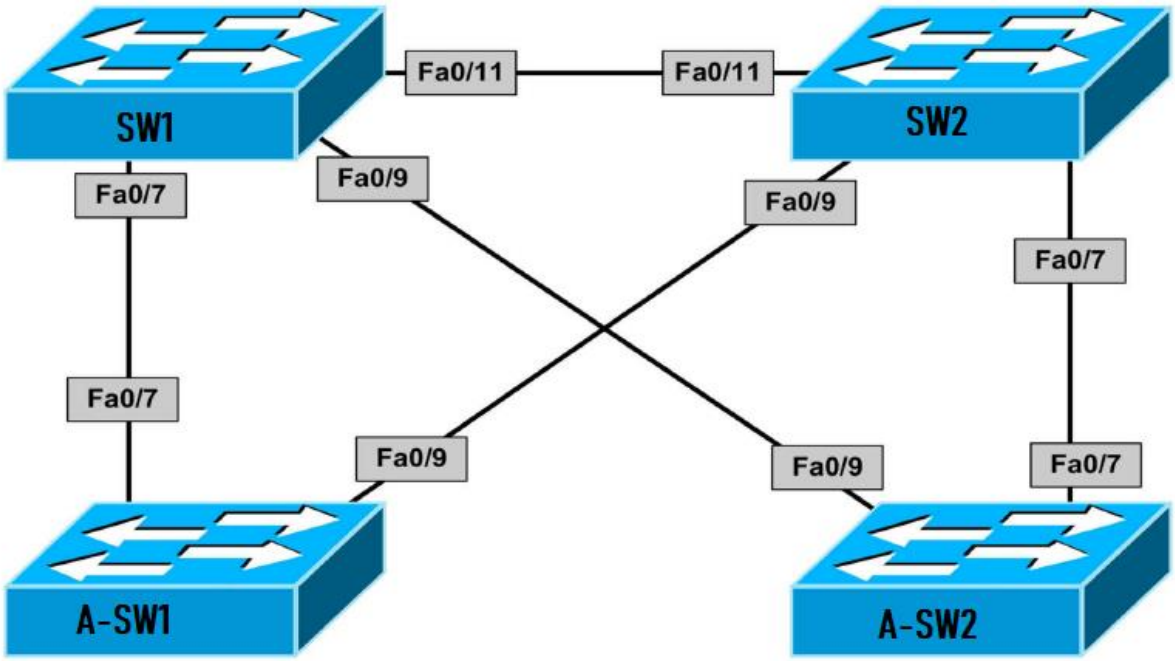
Лабораторная работа № 6 HSRP и безопасность коммутатора
Цель этой лабораторной работы - понять базовый HSRP, общую реализацию и конфигурацию технологий безопасности в коммутаторах Cisco IOS Catalyst.
Топология лабораторной сети показана ниже:



Задание 1
Отключите VTP на всех коммутаторах и создайте следующие VLAN:

SW1: VLAN 100 и VLAN 200
SW2: VLAN 100 и VLAN 200
A-SW1: VLAN 100
A-SW2: VLAN 200

Задание 2
Отключите DTP и 802.1Q настройте транкинг на всех коммутаторах следующим образом:
Магистральные каналы на коммутаторе SW1 должны разрешать только VLAN 1, 100 и 200.
Магистральные каналы на коммутаторе SW2 должны разрешать только VLAN 1, 100 и 200.
Магистральные каналы на коммутаторе A-SW1 должны разрешать только VLAN 1 и 100.
Магистральные каналы на коммутаторе A-SW2 должны разрешать только VLAN 1 и 200.
Задание 3
Настройте следующие SVI и интерфейсы на коммутаторах в топологии:

SW1: Интерфейс VLAN 100: IP-адрес 100.1.1.1/24
SW1: Интерфейс VLAN 200: IP-адрес 200.1.1.1/24
SW2: Интерфейс VLAN 100: IP-адрес 100.1.1.2/24
SW2: Интерфейс VLAN 200: IP-адрес 200.1.1.2/24
A-SW1: Интерфейс VLAN 100: IP-адрес 100.1.1.3/24
A-SW2: Интерфейс VLAN 100: IP-адрес 200.1.1.3/24

Задание 4

Настройте Cisco HSRP версии 1 с приоритетом на коммутаторах SW1 и SW2 следующим образом:
SW1: VLAN 100: IP-адрес HSRP 100.1.1.254, группа 1, приоритет 105, пароль HSRP1
SW1: VLAN 200: IP-адрес HSRP 200.1.1.254, группа 2, приоритет 100, пароль HSRP2
SW2: VLAN 100: IP-адрес HSRP 100.1.1.254, группа 1, приоритет 100, пароль HSRP1
SW2: VLAN 200: IP-адрес HSRP 200.1.1.254, группа 2, приоритет 105, пароль HSRP2

Задание 5

Чтобы обеспечить более быструю сходимость, включите RPVST +. В дополнение к этому, убедитесь, что ваши топологии уровня 2 и уровня 3 согласованы, то есть основной шлюз должен быть корневым для соответствующей VLAN. Наконец, убедитесь, что коммутаторы A-SW1 и A-SW2 также могут пинговать друг друга.

Задание 6

Настройте безопасность портов на всех магистральных каналах на коммутаторах SW1 и SW2. Конфигурация безопасности порта коммутатора должна допускать максимум 10 адресов. По достижении этого предела коммутатор должен отбрасывать пакеты с неизвестными MAC-адресами до тех пор, пока количество MAC-адресов не станет ниже предела. Кроме того, коммутатор должен отправлять SNMP trap и сообщение системного журнала, а счетчик нарушений должен увеличиваться.

Решение

Задание 1

SW1(config)#vtp mode transparent
Перевод устройства в режим VTP TRANSPARENT.
SW1(config)#vlan 100
SW1(config-vlan)#exit
SW1(config)#vlan 200
SW1(config-vlan)#exit
SW2(config)#vtp mode transparent
Перевод устройства в режим VTP TRANSPARENT.
SW2(config)#vlan 100
SW2(config-vlan)#exit
SW2(config)#vlan 200
SW2(config-vlan)#exit
A-SW1(config)#vtp mode transparent
Перевод устройства в режим VTP TRANSPARENT.
A-SW1(config)#vlan 100
A-SW1(config-vlan)#exit
A-SW2(config)#vtp mode transparent
Перевод устройства в режим VTP TRANSPARENT.
A-SW2(config)#vlan 200
A-SW2(config-vlan)#exit

Задание 2
SW1(config)#interface range fasteth 0/7 , fasteth 0/9 , fasteth 0/11
SW1(config-if-range)#switchport
SW1(config-if-range)#switchport trunk encapsulation dot1q
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#switchport trunk allowed vlan 1,100,200
SW1(config-if-range)#switchport nonegotiate
SW1(config-if-range)#exit
SW2(config)#interface range fasteth 0/7 , fasteth 0/9 , fasteth 0/11
SW2(config-if-range)#switchport
SW2(config-if-range)#switchport trunk encapsulation dot1q
SW2(config-if-range)#switchport mode trunk
SW2(config-if-range)#switchport trunk allowed vlan 1,100,200
SW2(config-if-range)#switchport nonegotiate
SW2(config-if-range)#exit
A-SW1(config)#interface range fastethernet 0/7 , fastethernet 0/9
A-SW1(config-if-range)#switchport mode trunk
A-SW1(config-if-range)#switchport trunk allowed vlan 1,100
A-SW1(config-if-range)#exit
A-SW2(config)#interface range fastethernet 0/7 , fastethernet 0/9
A-SW2(config-if-range)#switchport mode trunk

A-SW2(config-if-range)#switchport trunk allowed vlan 1,200
A-SW2(config-if-range)#exit

Проверьте свою конфигурацию с помощью команды show interfaces trunk:

SW1#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/7 on 802.1q trunking 1
Fa0/11 on 802.1q trunking 1
Port Vlans allowed on trunk
Fa0/7 1,100,200
Fa0/11 1,100,200
Port Vlans allowed and active in management domain
Fa0/7 1,100,200
Fa0/11 1,100,200
Port Vlans in spanning tree forwarding state and not pruned
Fa0/7 1,100,200
Fa0/11 200

Задание 3
SW1(config)#**interface vlan 100**
SW1(config-if)#**ip add 100.1.1.1 255.255.255.0**
SW1(config-if)#**exit**
SW1(config)#**interface vlan 200**
SW1(config-if)#**ip add 200.1.1.1 255.255.255.0**
SW1(config-if)#**exit**
SW1(config)#**ip routing**
SW2(config)#**interface vlan 100**
SW2(config-if)#**ip address 100.1.1.2 255.255.255.0**
SW2(config-if)#**exit**
SW2(config)#**interface vlan 200**
SW2(config-if)#**ip address 200.1.1.2 255.255.255.0**
SW2(config-if)#**exit**
SW2(config)#**ip routing**
A-SW1(config)#**interface vlan 100**
A-SW1(config-if)#**ip add 100.1.1.3 255.255.255.0**
A-SW1(config-if)#**exit**
A-SW1(config)#**ip routing**
A-SW2(config)#**interface vlan 200**
A-SW2(config-if)#**ip address 200.1.1.3 255.255.255.0**
A-SW2(config-if)#**exit**
A-SW2(config)#**ip routing**

Задание 4

При выполнении этого задания имейте в виду, что значение приоритета по умолчанию для HSRP равно 100, поэтому для указания этого значения не требуется явной конфигурации. Однако, в отличие от VRRP, приоритетное обслуживание для HSRP по умолчанию отключено и должно быть явно настроено. Кроме того, по умолчанию, когда включен HSRP, включена версия 1. Это задание выполняется следующим образом:

SW1(config)#**interface vlan 100**
SW1(config-if)#**standby 1 ip 100.1.1.254**
SW1(config-if)#**standby 1 priority 105**
SW1(config-if)#**standby 1 preempt**
SW1(config-if)#**standby 1 authentication text HSRP1**
SW1(config-if)#**exit**
SW1(config)#**interface vlan 200**
SW1(config-if)#**standby 2 ip 200.1.1.254**
SW1(config-if)#**standby 2 preempt**
SW1(config-if)#**standby 2 authentication text HSRP2**
SW1(config-if)#**exit**
SW2(config)#**interface vlan 100**
SW2(config-if)#**standby 1 ip 100.1.1.254**
SW2(config-if)#**standby 1 preempt**
SW2(config-if)#**standby 1 authentication text HSRP1**
SW2(config-if)#**exit**
SW2(config)#**interface vlan 200**
SW2(config-if)#**standby 2 ip 200.1.1.254**
SW2(config-if)#**standby 2 priority 105**
SW2(config-if)#**standby 2 preempt**
SW2(config-if)#**standby 2 authentication text HSRP2**
SW2(config-if)#**exit**

Затем, хотя это явно не указано, настройте шлюз по умолчанию для коммутаторов A-SW1 и A-SW2 в качестве виртуального IP-адреса (VIP) HSRP, чтобы они могли связаться с другими.
A-SW1(config)#**ip default-gateway 100.1.1.254**
A-SW2(config)#**ip default-gateway 200.1.1.254**

Проверьте свою конфигурацию с помощью команд show standby на коммутаторах SW1 и SW2:

SW1#**show stand brief**
P indicates configured to preempt.
|
Interface Grp Prio P State Active Standby Virtual IP
Vl100 1 105 P Active local 100.1.1.2 100.1.1.254

Vl200 2 100 P Standby 200.1.1.2 local 200.1.1.254
SW2#**show standby**
Vlan100 - Group 1
State is Standby
9 state changes, last state change 00:01:42
Virtual IP address is 100.1.1.254
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.620 secs
Authentication text “HSRP1”
Preemption enabled
Active router is 100.1.1.1, priority 105 (expires in 8.612 sec)
Standby router is local
Priority 100 (default 100)
IP redundancy name is “hsrp-Vl100-1” (default)
Vlan200 - Group 2
State is Active
5 state changes, last state change 00:14:18
Virtual IP address is 200.1.1.254
Active virtual MAC address is 0000.0c07.ac02
Local virtual MAC address is 0000.0c07.ac02 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.244 secs
Authentication text “HSRP2”
Preemption enabled
Active router is local
Standby router is 200.1.1.1, priority 100 (expires in 9.836 sec)
Priority 105 (configured 105)
IP redundancy name is “hsrp-Vl200-2” (default)
Задание 5
Первая часть этого задания проста. RPVST + включен на всех переключателях следующим образом:

SW1(config)#**spanning-tree mode rapid-pvst**
SW2(config)#**spanning-tree mode rapid-pvst**
A-SW1(config)#**spanning-tree mode rapid-pvst**
A-SW2(config)#**spanning-tree mode rapid-pvst**

Вторая часть этого задания влечет за собой настройку корневых мостов по умолчанию для соответствующих VLAN. Учитывая, что коммутатор SW1 является основным шлюзом для VLAN 100, он должен быть корневым для этой VLAN. Учитывая, что коммутатор SW2 является основным шлюзом для VLAN 200, он должен быть корневым для этой VLAN. Эти два коммутатора

должны быть настроены как вторичный или резервный корневой мост для другой VLAN. Это задание выполняется следующим образом:
SW1(config)#**spanning-tree vlan 100 priority 4096**
SW1(config)#**spanning-tree vlan 200 priority 8192**
SW2(config)#**spanning-tree vlan 100 priority 8192**
SW2(config)#**spanning-tree vlan 200 priority 4096**

После этого проверьте свою конфигурацию с помощью команд show spanning-tree:

SW1#**show spanning-tree summary**
Switch is in rapid-pvst mode
Root bridge for: VLAN0100
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short
Name Blocking Listening Learning Forwarding STP Active
---------- -------- --------- -------- ---------- ----------
VLAN0001 1 0 0 1 2
VLAN0100 0 0 0 2 2
VLAN0200 0 0 0 2 2
---------- -------- --------- -------- ---------- ----------
3 vlans 1 0 0 5 6
SW2#**show spanning-tree summary**
Switch is in rapid-pvst mode
Root bridge for: VLAN0200
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short
Name Blocking Listening Learning Forwarding STP Active
---------- -------- --------- -------- ---------- ----------
VLAN0001 0 0 0 2 2
VLAN0100 0 0 0 2 2

VLAN0200 0 0 0 2 2
---------- -------- --------- -------- ---------- ----------
3 vlans 0 0 0 6 6
Последняя часть задания требует проверки того, что коммутаторы A-SW1 и A-SW2 могут пинговать друг друга:
A-SW1#**ping 200.1.1.3**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
A-SW2#**ping 100.1.1.3**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
Задание 6
SW1(config)#**interface range fasteth 0/7 , fasteth 0/9 , fasteth 0/11**
SW1(config-if-range)#**switchport port-security**
SW1(config-if-range)#**switchport port-security maximum 10**
SW1(config-if-range)#**switchport port-security violation restrict**
SW1(config-if-range)#**switchport port-security mac-address sticky**
SW1(config-if-range)#**exit**
SW2(config)#**interface range fasteth 0/7 , fasteth 0/9 , fasteth 0/11**
SW2(config-if-range)#**switchport port-security**
SW2(config-if-range)#**switchport port-security maximum 10**
SW2(config-if-range)#**switchport port-security violation restrict**
SW2(config-if-range)#**switchport port-security mac-address sticky**
SW2(config-if-range)#**exit**
После этой конфигурации используйте команды show port-security для проверки
SW1#**show port-security**
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)

Fa0/7 10 0 1 Restrict
Fa0/9 10 0 1 Restrict
Fa0/11 10 0 1 Restrict

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 5120
SW2#**show port-security**
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)

Fa0/7 10 1 0 Restrict

Fa0/9 10 1 0 Restrict
Fa0/11 10 0 0 Restrict

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 5120