



ИНСТИТУТ
УПРАВЛЕНИЯ
И ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ



РОССИЙСКИЙ УНИВЕРСИТЕТ
ТРАНСПОРТА (МИИТ)



Анализ особенностей взаимодействия на канальном уровне оборудования Cisco и Huawei.

Выполнил: студент группы УВН-411 Коротков Дмитрий

Руководитель: Желенков Б.В

Нормоконтроль: Давыдовский М.А

Цель бакалаврской работы

Целью бакалаврской работы является анализ особенностей взаимодействия сетевого оборудования Cisco и Huawei на канальном уровне, с разработкой рекомендаций по настройке и обеспечению взаимодействия.

В соответствии с поставленной целью необходимо решить задачи:

- анализ возможностей оборудования на канальном уровне;
- анализ и настройка протоколов поддерживаемых обоими производителями;
- обеспечение взаимодействия Cisco и Huawei на канальном уровне;
- разработка рекомендаций по настройке оборудования;

Актуальность проблемы

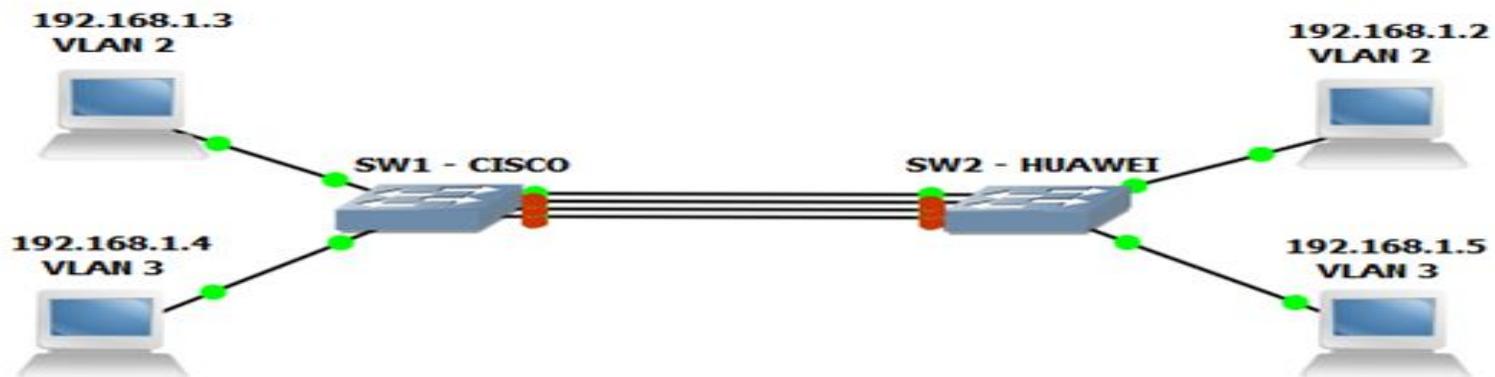
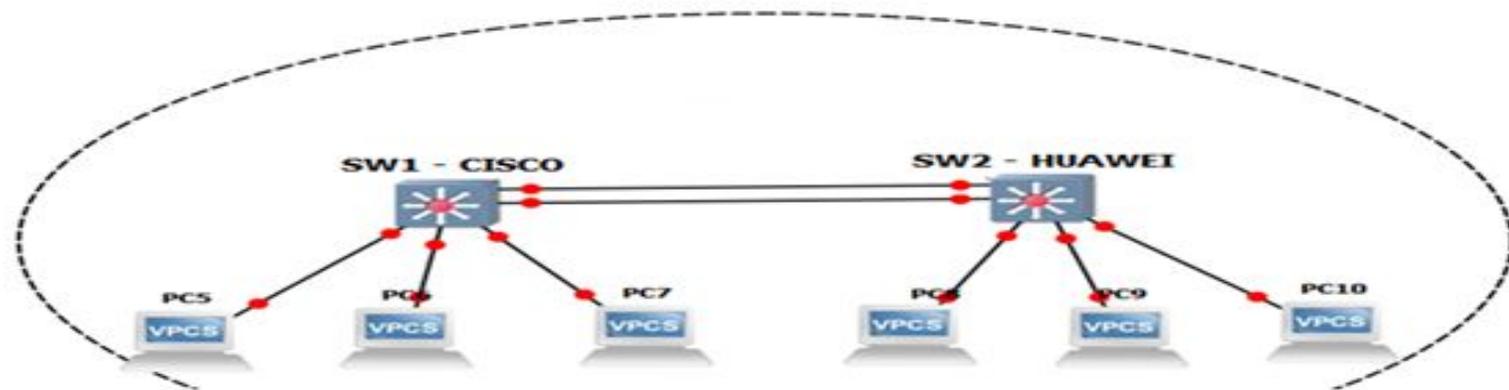
Согласно постановлению в соответствии с которым государственным структурам запрещено закупать иностранное ПО при наличии российского аналога. В Российской Федерации происходит замещение многих товаров, ввоз которых прекратился из – за санкций наложенных на Российскую Федерацию странами Евросоюза и США. Санкции не позволяют странам экспортировать в Российскую Федерацию оборудование двойного назначения.

Товарами двойного назначения называются товары, которые используются в мирных целях, но являющимся угрозой национальных интересов государства

Сравнение линеек Cisco Catalyst 3560 и Huawei s5720

Линейка	Cisco Catalyst 3560	Huawei s5720
Количество встроенных портов	24 – FastEthernet 4 – GigabitEthernet	28 - GigabitEthernet
Тип управления	Уровень 3	Уровень 3
Размер таблицы MAC адресов	8192	65536
Маршрутизация	Статическая маршрутизация, RIPv1, RIPv2, OSPF, IGRP, EIGRP	Статическая маршрутизация, RIP v1, RIP 2, RIPng, OSPF, OSPFv3, BGP, BGP4+, ECMP
Поддержка стандартов	VLAN, STP, RSTP, MSTP, ACL, Portsecurity, GVRP, PVST, VTP, AAA, SSH, EtherChannel , TACACS+ RADIUS	VLAN, STP, RSTP, MSTP, ACL, Portsecurity, GVRP, PVST, VTP, AAA, SSH, EtherChannel , TACACS+ RADIUS
Flash /Встроенная память	128 мб /512 мб	512 мб / 3 гб
Вес, кг	5, 8	4

Схема сети



Безопасность

Задача обеспечение несанкционированного доступа к сегменту сети и настройкам коммутатора. К выполнению представлены протоколы и технологий как:

- Базовый функционал безопасности на коммутаторах Cisco и Huawei
- Access Control List
- Authentication, Authorization, Accounting
- SSH соединение
- Port Security

Безопасность - настройка

При подключение к коммутатору необходимо установить: пароль на авторизацию по консольному порту, пароль в привилегированный режим, баннер авторизации.

№	Cisco	Huawei
1	<code><conf t></code>	<code><system-view></code>
2	<code><line con 0></code>	<code><user-interface console 0></code>
3	<code><password password></code>	<code><set authentication password cipher password></code>
4	<code><login></code>	<code><authentication-mode password></code>
5	<code><banner motd #text# ></code>	<code><header motd information ^text></code>
6	<code><enable secret password></code>	<code><super password simple password></code>

Таблица 1.1

Безопасность - настройка

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

```
diplom_cisco(config)#enable secret cisco
diplom_cisco(config)#^Z
diplom_cisco#
%SYS-5-CONFIG_I: Configured from console by console
```

```
diplom_cisco(config)#line con 0
diplom_cisco(config-line)#password cisco
diplom_cisco(config-line)#login
diplom_cisco(config-line)#^Z
diplom_cisco#
%SYS-5-CONFIG_I: Configured from console by console
```

```
!
line con 0
  password cisco
  login
User Access Verification

Password:
```

```
Switch(config)#banner motd #This system is part IT_TRAIN lab environment#
Switch(config)#^Z
```

```
This system is part IT TRAIN lab environment:

User Access Verification

Password: |
```

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]
```

```
[Huawei-ui-console0]set authentication password cipher huawei
[Huawei-ui-console0]
May 27 2017 23:25:45-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.25.191.3.1 configurations have been changed. The current change number is 4, change loop count is 0, and the maximum number of records is 4095.
```

```
[Huawei-ui-console0]authentication-mode password
[Huawei-ui-console0]
May 27 2017 23:27:06-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.25.191.3.1 configurations have been changed. The current change number is 4, change loop count is 0, and the maximum number of records is 4095.
```

```
user-interface con 0
  authentication-mode password
  set authentication password cipher mK7c11a4x:`S/0Rb{DzN|[F#
```

```
[Huawei]header shell information ^This system is part of IT-TRAIN lab environment This
[Huawei]
May 28 2017 01:26:44-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.191.3.1 configurations have been changed. The current change number is 11, the change loop count is 0, and the maximum number of records is 4095.
[Huawei]
[Huawei]
```

```
Password:
This system is part of IT-TRAIN lab environment
```

Безопасность AAA / SSH / ACL - настройка

Немаловажным моментом в безопасности является авторизация удаленного пользователя. Используем удаленное SSH соединение, локальную авторизацию по протоколу AAA и списки доступа на удаленное соединение

№	Cisco	Huawei
1	<code><conf t></code>	<code><system-view></code>
2	<code><aaa new model></code>	<code><aaa></code>
3	<code><username name privilege number secret password></code>	<code><local – user user_name privilege level number password cipher password></code>
4	<code><aaa authentication login name local enable></code>	<code><local – user huawei service type ssh></code>
5	<code><crypto key generate rsa></code> <code><service password-encryption></code>	<code><rsa local – key – pair create></code>
6	<code><line vty 0 4></code>	<code><user – interface vty 0 4></code>
7	<code><login authentication name></code>	<code><authentication – mode aaa></code>
8	<code><transport input ssh></code>	<code><protocol inbound ssh></code>

	Cisco	Huawei
9	<code><line vty 0 4></code> <code><access-list number permit ip mask></code>	<code><acl number number></code> <code><rule permit source ip mask></code>
10	<code><access-class number in></code>	<code><user-interface vty 0 4></code> <code><acl number inbound></code>
11	<code><interface vlan number></code> <code><ip address ip mask></code> <code><no shutdown></code>	<code><interface vlanif number></code> <code><ip address ip mask></code>

Таблица 1.3

Безопасность AAA / SSH / ACL - настройка

```
Switch(config)#username cisco pri
Switch(config)#username cisco privilege 15 secret cisco
Switch(config)#aaa new-model
Switch(config)#aaa authentication login ciscovty local enable
Switch(config)#line vty 0 4
Switch(config-line)#login authe
Switch(config-line)#login authentication ciscovty
```

```
Switch(config)#clock set 18:00:00 23 May 2018
Switch(config)#ip domain name cisco.com
Switch(config)#crypto key generate rsa
The name for the keys will be: diplom_cisco.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
```

```
How many bits in the modulus [512]: 400
% Generating 400 bit RSA keys, keys will be non-exportable...[OK]
Switch(config)#service password-encryption
Switch(config)#access-list 2 permit 172.16.0.0 255.240.0.0
Switch(config)#line vty 0 4
Switch(config-line)#tr
Switch(config-line)#transport inpu
Switch(config-line)#transport input ssh
Switch(config-line)#logging synchronous
Switch(config-line)#exec-tim
Switch(config-line)#exec-timeout 30 0
Switch(config-line)#acc
Switch(config-line)#access-class 2 in
Switch(config-line)#exit
```

```
[Huawei-aaa]local-user huawei privilege level 15
[Huawei-aaa]
May 28 2017 01:44:41-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.
25.191.3.1 configurations have been changed. The current change number is 13, the
change loop count is 0, and the maximum number of records is 4095.
```

```
[Huawei-aaa]rsa local-key-pair create
The key name will be: Huawei_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       it will take a few minutes.
Input the bits in the modulus[default = 512]:|
```

```
[Huawei]user-interface vty 0 4
[Huawei-ui-vty0-4]authentication-mode aaa
[Huawei-ui-vty0-4]protocol inbound ssh
[Huawei-ui-vty0-4]
May 28 2017 02:17:31-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.
25.191.3.1 configurations have been changed. The current change number is 20, the
change loop count is 0, and the maximum number of records is 4095.|
```

```
<Huawei>display ssh server status
SSH version                :1.99
SSH connection timeout     :60 seconds
SSH server key generating interval :0 hours
SSH authentication retries :3 times
SFTP server                 :Disable
Stelnet server              :Disable
Scp server                  :Disable
<Huawei>|
```

Безопасность Port Security - настройка

Отладка инструмента PortSecurity. Данная функция фильтрует трафик на основе анализа MAC-адреса рабочей станции подключенной к порту коммутатора.

Таблица 1.4

№	Cisco	Huawei
1	<code><conf t></code>	<code><system-view></code>
2	<code><interface GigabitEthernet number></code>	<code><interface GigabitEthernet number ></code>
3	<code><switchport mode access></code> <code><switchport port-security mac-address></code>	<code><port-security enable ></code> <code><port – security max – mac – num number></code>
4	<code><switchport port-security violation shutdown></code>	<code><port –security protect-action shutdown></code>
5	<code><interface GigabitEthernet number></code>	<code><interface GigabitEthernet number></code>
6	<code><switchport mode access></code>	<code><port – security enable></code>
7	<code><switchport port-security mac-address sticky></code> <code><switchport port-security violation restrickt></code> <code><switchport port-security maximum number></code>	<code><port-security-action protect></code> <code><port – security mac-address sticky></code>

Безопасность Port Security - настройка

```
diplom_cisco(config)#interface gi
diplom_cisco(config)#interface gigabitEthernet 0/3
diplom_cisco(config-if)#switchport mode access
diplom_cisco(config-if)#switchport port-secu
diplom_cisco(config-if)#switchport port-security mac-address sticky
diplom_cisco(config-if)#switchport port-security violation restrict
```

```
diplom_cisco#show port-security interface GigabitEthernet 0/1
Port Security           : Disabled
Port Status             : Secure-down
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
```

```
diplom_cisco#show port-security interface gigabitEthernet 0/3
Port Security           : Disabled
Port Status             : Secure-down
Violation Mode         : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 3
```

```
[Huawei]interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]port-security enable
[Huawei-GigabitEthernet0/0/1]port-security max-mac-num 5
[Huawei-GigabitEthernet0/0/1]port-security protect-action shutdown
```

```
interface GigabitEthernet0/0/1
port-security enable
port-security protect-action shutdown
port-security max-mac-num 5
#
```

```
Huawei]interface GigabitEthernet 0/0/3
Huawei-GigabitEthernet0/0/3]port-security mac-address sticky
Huawei-GigabitEthernet0/0/3]port-security protect-action protect
```

```
interface GigabitEthernet0/0/3
port-security enable
port-security protect-action protect
port-security mac-address sticky
```

Взаимодействия коммутаторов

Задача обеспечение стабильности взаимодействия между коммутаторами, балансировка нагрузки и отказоустойчивой связи. К рассмотрению представлены протоколы :

- VLAN
- 802.1Q
- Семейство протоколов STP / MSTP / RSTP
- Протоколы группового вещания - GVRP

Взаимодействия коммутаторов VLAN / 802.1Q

Таблица 1.5

№	Cisco	Huawei
1	<conf t>	<system – view>
2	<interface vlan number> <ip address ip mask> <no shutdown >	<vlan number> <description Management>
3	<interface GigabitEthernet 0/1> <switchport mode access>	<interface Gigabit Ethernet 0/0/1> <description access_port>
4	<switchport access vlan 10>	<port link-type-access> <port default vlan 20 >
5	<interface GigabitEthernet 0/2> <switchport access vlan 20>	<interface GigabitEthernet 0/0/3> <port default vlan 30>
6	<interface GigabitEthernet 0/3> <switchport access vlan 10>	<interface GigabitEthernet 0/0/2> <port default vlan 20>



Cisco	Huawei	№
<interface GigabitEthernet 0/4>	<interface Eth-Trunk 1>	8
<switchport mode trunk>	<port link-type trunk>	9
<switchport trunk allowed vlan 10,20>	<port trunk allow-pass vlan 20> <port trunk allow-pass vlan 30>	10
<switchport trunk native vlan 50>	<port trunk pvid vlan 50>	11
<gvrp global>	<gvrp>	12
< gvrp registration type>	<gvrp> <gvrp registration status>	13
<gvrp timer join number>	<gvrp timer number>	14

Таблица 1.6

Взаимодействия коммутаторов VLAN / 802.1Q

```
diplom_cisco(config)#interface vlan 100
diplom_cisco(config-if)#ip address 172.16.1.2 255.240.0.0
diplom_cisco(config-if)#no shutdown
!
interface Vlan100
 ip address 172.16.1.2 255.240.0.0
```

```
diplom_cisco(config)#interface GigabitEthernet 0/2
diplom_cisco(config-if)#switchport mode access
diplom_cisco(config-if)#switchport access vlan 20
!
interface GigabitEthernet 0/2
 switchport access vlan 20
 switchport mode access
```

```
diplom_cisco(config)#interface GigabitEthernet 0/4
diplom_cisco(config-if)#swi
diplom_cisco(config-if)#switchport mode trunk
diplom_cisco(config-if)#switchport trunk allowed vlan 10,20
diplom_cisco(config-if)#switchport trunk native vlan 50
!
interface GigabitEthernet0/4
 switchport trunk native vlan 50
 switchport trunk allowed vlan 10,20
 switchport mode trunk
```

```
[Huawei]vlan 10
[Huawei-vlan10]description Managment
```

VID	Status	Property	MAC-LRN	Statistics	Description
1	enable	default	enable	disable	VLAN 0001
10	enable	default	enable	disable	Managment

```
[Huawei]interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1]description Access_port
[Huawei-GigabitEthernet0/0/1]port link-type access
[Huawei-GigabitEthernet0/0/1]port default vlan 20
```

```
[Huawei]interface GigabitEthernet 0/0/3
Huawei-GigabitEthernet0/0/3]port link-type access
[Huawei-GigabitEthernet0/0/3]port default vlan 30
```

```
[Huawei]vlan 50
50 enable default enable disable VLAN 0050
interface Eth-Trunk1
port link-type trunk
port trunk pvid vlan 50
port trunk allow-pass vlan 20 30
```

Взаимодействия коммутаторов STP



<show -spanning-tree>

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
            Address    0060.5CC3.2A35
            This bridge is the root
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768 (priority 32768 sys-id-ext 1)
            Address    0060.5CC3.2A35
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface          Role Sts Cost          Prio.Nbr Type
-----
GE0/3              Desg FWD 19            128.3    P2p
GE0/2              Desg FWD 19            128.2    P2p
GE0/1              Desg FWD 19            128.1    P2p
```

<display stp brief>

```
-----[CIST Global Info][Mode MSTP]-----
CIST Bridge           :32769.4c1f-ccc0-33bd
Config Times          :Hello 2s MaxAge 20s FwdDly 15s MaxHop 20
Active Times          :Hello 2s MaxAge 20s FwdDly 15s MaxHop 20
CIST Root/ERPC        :32768
CIST RegRoot/IRPC     :32768
CIST RootPortId       :128.1
BPDU-Protection       :Disabled
TC or TCN received    :6
TC count per hello    :0
STP Converge Mode     :Normal
Time since last TC    :0 days 0h:9m:36s
Number of TC          :4
Last TC occurred      :GigabitEthernet0/0/1
----[Port1(GigabitEthernet0/0/1)] [FORWARDING]----
Port Protocol         :Enabled
Port Role              :Root Port

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]display stp brief
MSTID  Port              Role  STP State  Protection
0      GigabitEthernet0/0/1  ROOT  FORWARDING  NONE
0      GigabitEthernet0/0/2  ALTE  DISCARDING  NONE
0      GigabitEthernet0/0/3  ALTE  DISCARDING  NONE
[Huawei]
```

Взаимодействия коммутаторов STP

Рисунок 1.2

```
switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4096
            Address    4C1F.CC0E.665C
            This bridge is the root
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    32768
            Address    0060.5CC3.2A35
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time 20

Interface    Role Sts Cost      Prio.Nbr Type
-----
GE0/3       Altn BLK 19        128.3   P2p
GE0/2       Altn BLK 19        128.2   P2p
GE0/1       Root FWD 19        128.1   P2p
```

Рисунок 1.1

```
[Huawei]stp priority 4096
[Huawei]
[Huawei]system-view
May 18 2018 23:52:58-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
25.191.3.1 configurations have been changed. The current change number is 4, the
change loop count is 0, and the maximum number of record
[Huawei]disp stp brief
MSTID Port          Role STP State      Protection
0     GigabitEthernet0/0/1  DESI FORWARDING  NONE
0     GigabitEthernet0/0/2  DESI LEARNING    NONE
0     GigabitEthernet0/0/3  DESI LEARNING    NONE
[Huawei]
```

```
switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4096
            Address    4C1F.CC0E.665C
            Cost        10
            Port        GigabitEthernet0/3
            This bridge is the root
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    32768
            Address    0060.5CC3.2A35
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time 20

Interface    Role Sts Cost      Prio.Nbr Type
-----
GE0/3       Root FWD 10        128.3   P2p
GE0/2       Altn BLK 19        128.2   P2p
GE0/1       Altn BLK 19        128.1   P2p
```

Рисунок 1.1	Изменение приоритета коммутатора Huawei / <stp priority number>
Рисунок 1.2	Изменение приоритета коммутатора Cisco / spanning-tree vlan vlan-id priority value
Рисунок 1.3	Изменение приоритета интерфейса Cisco / spanning-tree port-priority

Рисунок 1.3

Взаимодействия коммутаторов RSTP / MSTP

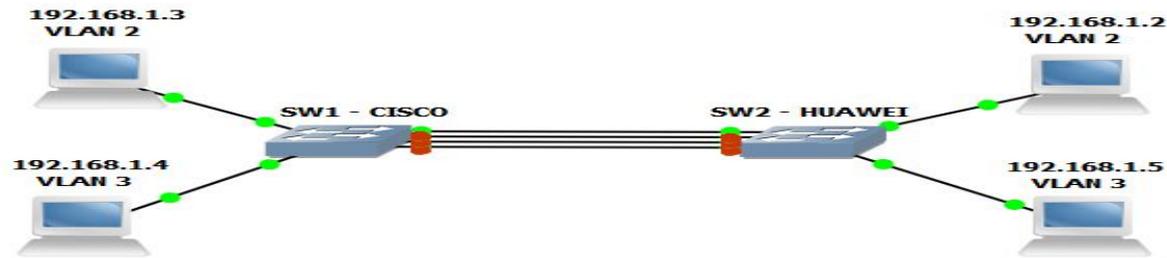


Таблица 1.8

№	Cisco	Huawei
1	<code><spanning-tree mode rapid-pvst></code>	<code><stp mode rstp></code>
2	<code><spanning-tree mode mst></code>	<code><stp mode mstp></code>
3	<code><name nameregion></code>	<code><stp region-configuration></code> <code><region-name></code>
4	<code><instance number vlan number></code>	<code><instance number vlan number></code>
5		<code><active region-configuration></code> <code><stp instance number priority number></code>
6	<code><revision number></code>	<code><number revision></code>

```
Huawei>display stp region-configuration
Oper configuration
Format selector      :0
Region name         :CiscoHuawei
Revision level      :1

Instance  VLANs Mapped
 0         1, 4 to 4094
 2         2
 3         3
```

```
Name      [CiscoHuawei]
Revision  1      Instances configured 3

Instance  Vlans mapped
-----
0         1,4-4094
2         2
3         3
```

Заключение

Целью выпускной квалификационной работы являлся анализ особенностей взаимодействия сетевого оборудования Cisco и Huawei на канальном уровне с разработкой рекомендаций по настройке.

- В процессе были рассмотрены как технические так и программные параметры обоих производителей.
- Произведены настройки и анализ протоколов канального уровня на устройствах Huawei и Cisco
- Установлены и проанализированы взаимодействия по различным протоколам, между коммутаторами
- Разработаны рекомендации по настройке оборудования Cisco и Huawei на канальном уровне.

Полученные результаты выпускной квалификационной работы можно использовать в качестве учебно-методического материала по настройке сетевого оборудования Cisco и Huawei на канальном уровне.

Спасибо за внимание!