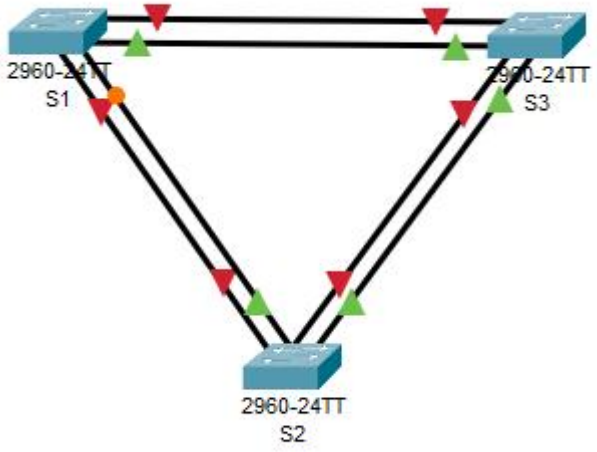
Часть 2

Создана сеть согласно топологии



Шаг 1. Отключение всех портов на коммутаторах

Коммутатор S1_Sidorov

```
S1_Sidorov#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1_Sidorov(config)#interface range fa0/1 - 24
S1_Sidorov(config-if-range)#shutdown



%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
```

Коммутатор S2

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface range fa0/1 -24
S2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
```

Коммутатор S3

```
S3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#interface range f0/1 - 24
S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
```

Шаг 2. Настройка подключённых портов в качестве транковых

Коммутатор S1_Sidorov

```
S1_Sidorov(config)# interface range f0/1 - 4
S1_Sidorov(config-if-range)#switchport mode trunk
S1_Sidorov(config-if-range)#switchport mode trunk
S1_Sidorov(config-if-range)#exit
```

Коммутатор S2

```
S2(config)#interface range f0/1-4
S2(config-if-range)#swi
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#exit
```

Коммутатор S3

```
S3(config)#interface range f0/1-4
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#exit
```

Шаг 3. Включение портов на всех комутаторах

Коммутатор S1_Sidorov

```
S1_Sidorov(config)# interface range f0/2, f0/4
S1_Sidorov(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to down
S1_Sidorov(config-if-range)#ex
S1_Sidorov(config-if-range)#exit
```

Коммутатор S2

```
S2(config)#interface range fa0/2, fa0/4
S2(config-if-range)#no shutdown


%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to down
S2(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if-range)#exit
```

Коммутатор S3

```
S3(config)#interface range f0/2, f0/4
S3(config-if-range)#no shutdown


S3(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

S3(config-if-range)#exit
```

Шаг 4. Данные протокола spanning tree

Коммутатор S1_Sidorov

```
S1_Sidorov#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000C.CF9A.2335
             Cost        19
             Port        4(FastEthernet0/4)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.FFE8.1948
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/4            Root FWD 19        128.4    P2p
```

Коммутатор S2

```
S2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000C.CF9A.2335
             Cost        19
             Port        4(FastEthernet0/4)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0030.F2CE.D07D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Root FWD 19        128.4    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

Коммутатор S3

```
S3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000C.CF9A.2335
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000C.CF9A.2335
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p
```

Часть 3

Шаг 2. Изменение стоимости порта

Коммутатор S1_Sidorov - с заблокированным портом

```
S1_Sidorov(config)#interface f0/4
S1_Sidorov(config-if)#spann
S1_Sidorov(config-if)#spanning-tree cost 18
S1_Sidorov(config-if)#exit
```

Шаг 3. Изменения протокола spanning-tree

Коммутатор S1_Sidorov Fa0/2 - сменил роль на назначенный

```
S1_Sidorov#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000C.CF9A.2335
             Cost        18
             Port        4(FastEthernet0/4)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.FFE8.1948
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/4            Root FWD 18        128.4    P2p
```

Коммутатор S2 Fa0/2 - сменил роль на альтернативный

```
S2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000C.CF9A.2335
             Cost        19
             Port        4(FastEthernet0/4)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0030.F2CE.D07D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Root FWD 19        128.4    P2p
Fa0/2            Altn BLK 19        128.2    P2p
```

Шаг 4. Удаление изменения стоимости порта на коммутаторе S1

```
S1_Sidorov(config)#interface f0/4
S1_Sidorov(config-if)#no span
S1_Sidorov(config-if)#no spanning-tree cost 18
```

```
S1_Sidorov#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000C.CF9A.2335
             Cost        19
             Port        4(FastEthernet0/4)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.FFE8.1948
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/4            Root FWD 19        128.4    P2p
```

Часть 4

Включение всех портов

Коммутатор S1_Sidorov

```
S1_Sidorov(config)#interface range f0/1, f0/3
S1_Sidorov(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to down
```

Коммутатор S2

```
S2(config)#interface range fa0/1, fa0/3
S2(config-if-range)#no shutdown


%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to down
S2(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S2(config-if-range)#exit
```

Коммутатор S3

```
S3(config)#interface range fa0/1, fa0/3
S3(config-if-range)#no shutdown


S3(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

S3(config-if-range)#exit
```

Изменения протокола spanning-tree

Коммутатор S1_Sidorov

```
S1_Sidorov#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000C.CF9A.2335
             Cost        19
             Port        3(FastEthernet0/3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00D0.FFE8.1948
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ---------------------------
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Root FWD 19        128.3    P2p
Fa0/1            Altn BLK 19        128.1    P2p
Fa0/4            Altn BLK 19        128.4    P2p
```

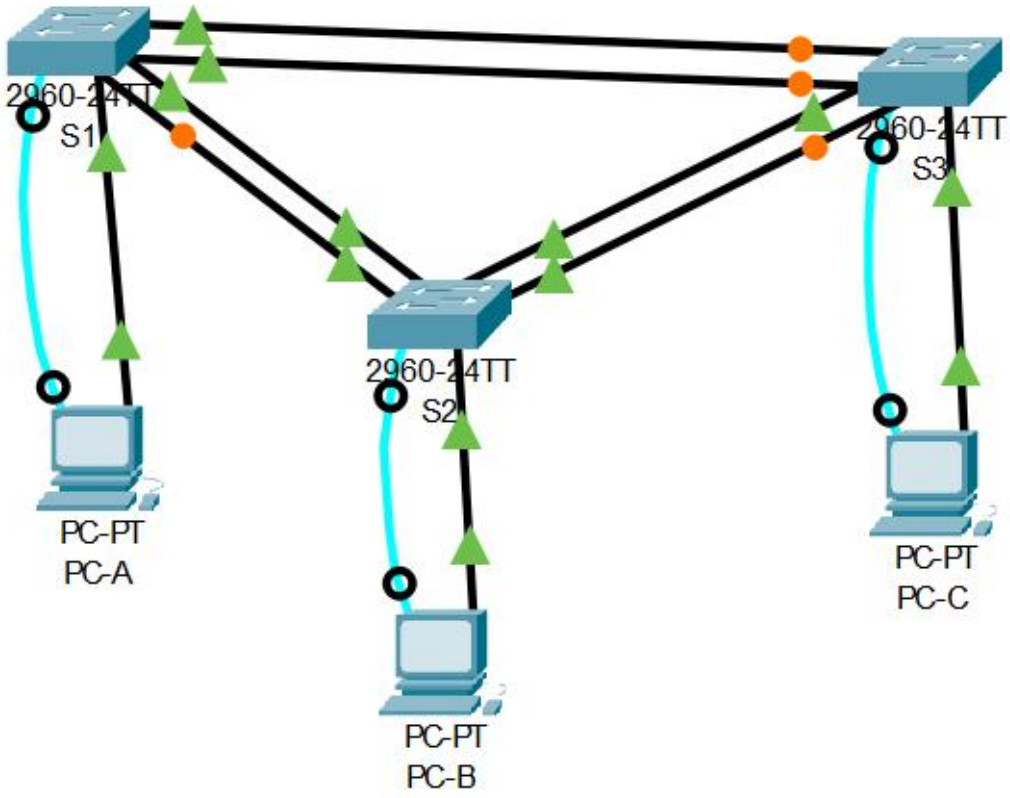
Коммутатор S2

```
S2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     000C.CF9A.2335
             Cost        19
             Port        3(FastEthernet0/3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0030.F2CE.D07D
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Root FWD 19        128.3    P2p
```

Практическая работа №5

Часть 1: Настройка основных параметров коммутатора

Была создана сеть согласно топологии



Настройка коммутаторов

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1_Sidorov
S1_Sidorov(config)#service password-encryption
S1_Sidorov(config)#banner motd #Unauthorized access is prohibited.#
S1_Sidorov(config)#enable secret class
S1_Sidorov(config)#line console 0
S1_Sidorov(config-line)#password cisco
S1_Sidorov(config-line)#login
S1_Sidorov(config-line)#logging synchronous
S1_Sidorov(config-line)#exit
S1_Sidorov(config)#line vty 0 15
S1_Sidorov(config-line)#password cisco
S1_Sidorov(config-line)#login
S1_Sidorov(config-line)#exit
```

Настройка базовых параметров коммутатора 1

Аналогично для коммутаторов S2 и S3

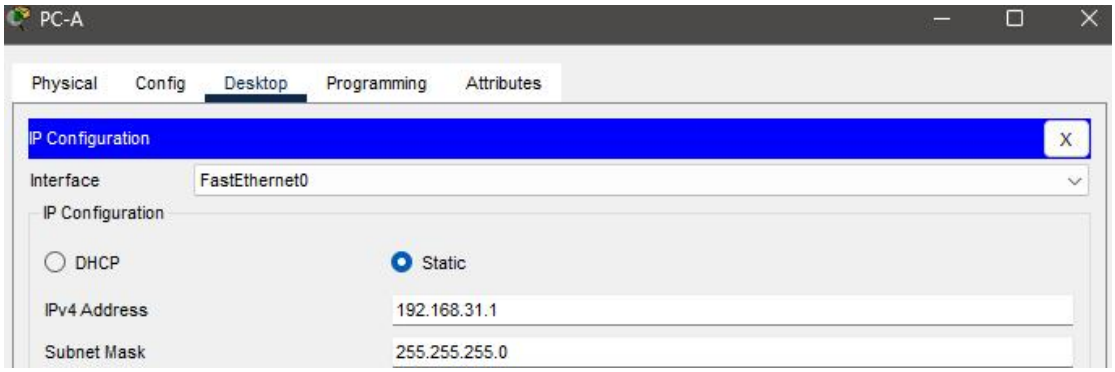
```
S1_Sidorov(config-vlan)#exit
S1_Sidorov(config)#vlan 99
S1_Sidorov(config-vlan)#name Management
S1_Sidorov(config-vlan)#exit
S1_Sidorov(config)#vlan 31
S1_Sidorov(config-vlan)#name Staff
S1_Sidorov(config-vlan)#exit
S1_Sidorov(config)#interface f0/6
S1_Sidorov(config-if)#switchport mode access
S1_Sidorov(config-if)#switchport access vlan 31
S1_Sidorov(config-if)#exit
S1_Sidorov(config)#interface vlan 99
S1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1_Sidorov(config-if)#ip address 192.168.99.11 255.255.255.0
S1_Sidorov(config-if)#exit
S1_Sidorov(config)#exit
S1_Sidorov#
%SYS-5-CONFIG_I: Configured from console by console

S1_Sidorov#write memory
Building configuration...
[OK]
```

```
S1_Sidorov(config)#interface range f0/1-f0/4
S1_Sidorov(config-if-range)#switchport mode access
S1_Sidorov(config-if-range)#switchport access vlan 31
S1_Sidorov(config-if-range)#exit
S1_Sidorov(config)#exit
S1_Sidorov#
%SYS-5-CONFIG_I: Configured from console by console

S1_Sidorov#write memory
Building configuration...
[OK]
```

Настройка портов коммутатора 1

Аналогично для S2 и S3 с подстановкой ip адресов 192.168.99.12 и 192.168.99.13 соответственно.

Настройка компьютеров



Настройка компьютера PC-A

Аналогично для PC-B и PC-C с подстановкой ip адресов 192.168.31.2 и 192.168.31.3 соответственно

Часть 2 : Настройка протокола PAgP

Настройка протокола PAgP

```
S1_Sidorov(config)#interface range f0/3-4
S1_Sidorov(config-if-range)#channel-group 1 mode desirable
S1_Sidorov(config-if-range)#
Creating a port-channel interface Port-channel 1

S1_Sidorov(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to down
```

Настройка PAgP на коммутаторе S1_Sidorov, аналогично для S3 с mode auto

Проверка объедененности портов

```
S1_Sidorov#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           PAgP   Fa0/3(P) Fa0/4(P)
```

Коммутатор S1_Sidorov

```
S3(config)#do show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           PAgP   Fa0/3(P) Fa0/4(P)
```

Коммутатор S3

Настройка транковых портов

```
S1_Sidorov(config)#interface po1
S1_Sidorov(config-if)#switchport mode trunk

S1_Sidorov(config-if)#switchport trunk native vlan 99
```

Коммутатор S1_Sidorov

```
S3(config)#interface po1
S3(config-if)#switchport mode trunk

S3(config-if)#switchport trunk native vlan 99
```

Коммутатор S3

Проверка

```
S3#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      99

Port        Vlans allowed on trunk
Po1         1-1005

Port        Vlans allowed and active in management domain
Po1         1,31,99

Port        Vlans in spanning tree forwarding state and not pruned
Po1         none

S3#show spanning-tree
VLAN0031
  Spanning tree enabled protocol ieee
  Root ID    Priority    32799
             Address     0060.2F59.268C
             Cost        12
             Port        28(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32799  (priority 32768 sys-id-ext 31)
             Address     00D0.FFE6.E732
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/18           Desg FWD 19        128.18   P2p
Po1              Root BKN*12        128.28   Shr *TYPE_Inc
```

Коммутатор S3

```
S1_Sidorov#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      99

Port        Vlans allowed on trunk
Po1         1-1005

Port        Vlans allowed and active in management domain
Po1         1,31,99

Port        Vlans in spanning tree forwarding state and not pruned
Po1         31

S1_Sidorov#show spanning-tree
VLAN0031
  Spanning tree enabled protocol ieee
  Root ID    Priority    32799
             Address     0060.2F59.268C
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32799  (priority 32768 sys-id-ext 31)
             Address     0060.2F59.268C
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 19        128.6    P2p
Po1              Desg FWD 12        128.28   Shr
```

Коммутатор S1_Sidorov

Часть 3: Настройка протокола LACP

Настройка LACP между S1_Sidorov и S2

```
S1_Sidorov(config)#interface range f0/1 - 2
S1_Sidorov(config-if-range)#channel-group 2 mode active
S1_Sidorov(config-if-range)#
Creating a port-channel interface Port-channel 2

S1_Sidorov(config-if-range)#exit
S1_Sidorov(config)#interface port-channel 2
S1_Sidorov(config-if)#switchport mode trunk
S1_Sidorov(config-if)#switchport native vlan 99
                                ^
% Invalid input detected at '^' marker.

S1_Sidorov(config-if)#switchport trunk native vlan 99
S1_Sidorov(config-if)#exit
```

Настройка LACP на коммутаторе S1_Sidorov

```
S2(config)#interface range F0/1-2
S2(config-if-range)#channel-group 2 mode passive
S2(config-if-range)#
Creating a port-channel interface Port-channel 2

S2(config-if-range)#exit
S2(config)#interface port-channel 2
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#exit
```

Настройка LACP на коммутаторе S2

```
S1_Sidorov#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           PAgP   Fa0/3(P) Fa0/4(P)
2      Po2(SU)           LACP   Fa0/1(P) Fa0/2(P)
```

Проверка на коммутаторе S1_Sidorov

```
S2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------

2      Po2(SU)          LACP   Fa0/1(P) Fa0/2(P)
```

Проверка на коммутаторе S2

Настройка LACP для S2 и S3

```
S3(config)#interface range f0/1-2
S3(config-if-range)#channel-group 3 mode active
S3(config-if-range)#
Creating a port-channel interface Port-channel 3

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

S3(config-if-range)#exit
S3(config)#interface port-channel 3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
```

Настройка на коммутаторе S3

```
S2(config)#interface range f0/3-f0/4
S2(config-if-range)#channel-group 3 mode passive
S2(config-if-range)#
Creating a port-channel interface Port-channel 3

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
```

```
S2(config-if-range)#exit
S2(config)#interface port-channel 3
S2(config-if)#switchport mode trunk
```

```
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#exit
```

Настройка коммутатора S2

```
S2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------

2      Po2(SU)           LACP   Fa0/1(P) Fa0/2(P)
3      Po3(SU)           LACP   Fa0/3(P) Fa0/4(P)
```

Проверка на коммутаторе S2

```
S3#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+-----------------------------------------------

1      Po1(SU)           PAgP   Fa0/3(P) Fa0/4(P)
3      Po3(SU)           LACP   Fa0/1(P) Fa0/2(P)
```

Проверка на коммутаторе S3

Проверка наличия сквозного соединения

```
C:\>ping 192.168.31.2

Pinging 192.168.31.2 with 32 bytes of data:

Reply from 192.168.31.2: bytes=32 time=1ms TTL=128
Reply from 192.168.31.2: bytes=32 time<1ms TTL=128
Reply from 192.168.31.2: bytes=32 time<1ms TTL=128
Reply from 192.168.31.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.31.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.31.3

Pinging 192.168.31.3 with 32 bytes of data:

Reply from 192.168.31.3: bytes=32 time<1ms TTL=128
Reply from 192.168.31.3: bytes=32 time<1ms TTL=128
Reply from 192.168.31.3: bytes=32 time<1ms TTL=128
Reply from 192.168.31.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.31.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping с PC-A на PC-B и PC-C

```
S1_Sidorov#ping
Protocol [ip]:
Target IP address: 192.168.99.12
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.12, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

S1_Sidorov#ping 192.168.99.13

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.13, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/3/10 ms
```

Ping с S1_Sidorov на S2 и S3

Реализация DHCPv4

Топология

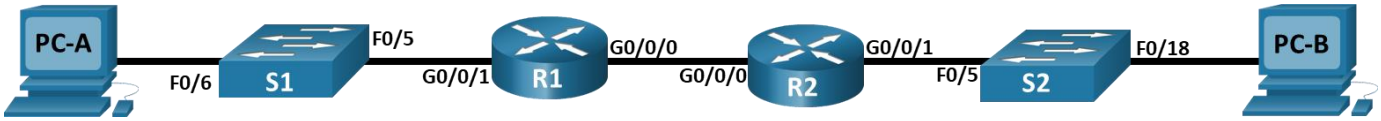


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1_Sidorov	G0/0/0	10.0.0.1	255.255.255.252	—
	G0/0/1	—	—	
	G0/0/1.100	192.168.1.1	255.255.255.192	
	G0/0/1.221	192.168.1.65	255.255.255.224	
	G0/0/1.1000	—	—	
R2	G0/0/0	10.0.0.2	255.255.255.252	—
	G0/0/1	192.168.1.97	255.255.255.240	
S1	VLAN 221	192.168.1.66	255.255.255.224	192.168.1.65
S2	VLAN 1	192.168.1.98	255.255.255.240	192.168.1.97
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Таблица VLAN

VLAN	Имя	Назначенный интерфейс
1	Нет	S2: F0/18
100	Clients	S1: F0/6
221	Management	S1: VLAN 221
999	Parking_Lot	S1: F0/1-4, F0/7-24, G0/1-2
1000	Native	—

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

www.netacad.com

Часть 2. Настройка и проверка двух серверов DHCPv4 на R1_ФАМИЛИЯ

Часть 3. Настройка и проверка DHCP-ретрансляции на R2

Необходимые ресурсы

- 2 маршрутизатора (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.4 или аналогичным)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.2(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (ОС Windows с программой эмуляции терминалов, такой как Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты.
- Кабели Ethernet, расположенные в соответствии с топологией

Инструкции

Часть 1. Создание сети и настройка основных параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовые параметры для узлов ПК и коммутаторов.

Шаг 1. Создание схемы адресации

Подсеть сети 192.168.1.0/24 в соответствии со следующими требованиями:

a. Одна подсеть «Подсеть A», поддерживающая 58 хостов (клиентская VLAN на R1_ФАМИЛИЯ).

   Подсеть A

   Запишите первый IP-адрес в таблице адресации для R1_ФАМИЛИЯ G0/0/1.100.

b. Одна подсеть «Подсеть B», поддерживающая 28 хостов (управляющая VLAN на R1_ФАМИЛИЯ).

   Подсеть B:

   Запишите первый IP-адрес в таблице адресации для R1_ФАМИЛИЯ G0/0/1.X+200. Запишите второй IP-адрес в таблице адресов для S1 VLAN X+200 и введите соответствующий шлюз по умолчанию.

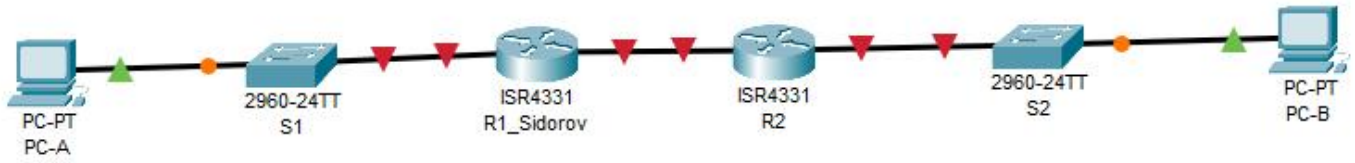
c. Одна подсеть «Подсеть C», поддерживающая 12 узлов (клиентская сеть на R2).

   Подсеть C:

   Запишите первый IP-адрес в таблице адресации для R2 G0/0/1. Запишите второй IP-адрес в таблице адресов для S2 VLAN 1 и введите соответствующий шлюз по умолчанию.

Шаг 2. Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.



© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

www.netacad.com

Шаг 3. Произведите базовую настройку маршрутизаторов.

a. Назначьте маршрутизатору имя устройства.

b. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

c. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

d. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.

e. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.

f. Зашифруйте открытые пароли.

g. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

h. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

i. Установите часы на маршрутизаторе на сегодняшнее время и дату.

Примечание. Вопросительный знак (**?**) позволяет открыть справку с правильной последовательностью параметров, необходимых для выполнения этой команды.

Настройка первого маршрутизатора:

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with
Router(config)#hostname R1_Sidorov
R1_Sidorov(config)#no ip domain lookup
R1_Sidorov(config)#enable secret class
R1_Sidorov(config)#line con 0
R1_Sidorov(config-line)#password cisco
R1_Sidorov(config-line)#login
R1_Sidorov(config-line)#exit
R1_Sidorov(config)#line vty 0 15
R1_Sidorov(config-line)#password cisco
R1_Sidorov(config-line)#login
R1_Sidorov(config-line)#exit
R1_Sidorov(config)#service password-enc
R1_Sidorov(config)#service password-encryption
R1_Sidorov(config)#banner motd #Unautorized banned#
R1_Sidorov(config)#exit
R1_Sidorov#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
R1 Sidorov#
```

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Настройка второго маршрутизатора:

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with
Router(config)#hostname R2
R2(config)#no ip domain lookup
R2(config)#enable secret class
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service pass
R2(config)#service password-enc
R2(config)#service password-encryption
R2(config)#banner motd #Unauthorized banned#
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
R2#
```

Шаг 4. Настройка маршрутизации между сетями VLAN на маршрутизаторе R1_ФАМИЛИЯ

a. Активируйте интерфейс G0/0/1 на маршрутизаторе.

```
R1_Sidorov(config)#int g0/0/1
R1_Sidorov(config-if)#no shutdown

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
```

b. Настройте подинтерфейсы для каждой VLAN в соответствии с требованиями таблицы IP-адресации. Все субинтерфейсы используют инкапсуляцию 802.1Q и назначаются первый полезный адрес из вычисленного пула IP-адресов. Убедитесь, что подинтерфейсу для native VLAN не назначен IP-адрес. Включите описание для каждого подинтерфейса.

```
R1_Sidorov(config)#int g0/0/1.100
R1_Sidorov(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.100, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.100, changed state
to up

R1_Sidorov(config-subif)#encapsulation dot1
R1_Sidorov(config-subif)#encapsulation dot1Q 100
R1_Sidorov(config-subif)#ip address 192.168.1.1 255.255.255.255.192
                                            ^
% Invalid input detected at '^' marker.

R1_Sidorov(config-subif)#ip address 192.168.1.1 255.255.255.192
R1_Sidorov(config-subif)#description Client_network
R1_Sidorov(config-subif)#exit
```

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

```
R1_Sidorov(config)#int g0/0/1.221
R1_Sidorov(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.221, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.221, changed state
to up

R1_Sidorov(config-subif)#encapsulation dot1q 221
R1_Sidorov(config-subif)#ip address 192.168.1.65 255.255.255.224
R1_Sidorov(config-subif)#description Management
R1_Sidorov(config-subif)#exit
```

```
R1_Sidorov(config)#int g0/0/1.1000
R1_Sidorov(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.1000, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.1000, changed state
to up

R1_Sidorov(config-subif)#encapsulation dot1q 1000 native
R1_Sidorov(config-subif)#description Native
R1_Sidorov(config-subif)#exit
```

c. Убедитесь, что вспомогательные интерфейсы работают.

```
R1_Sidorov(config)#do show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   unassigned      YES unset  up                    up
GigabitEthernet0/0/1.100192.168.1.1     YES manual up                    up
GigabitEthernet0/0/1.221192.168.1.65    YES manual up                    up
GigabitEthernet0/0/1.1000unassigned      YES unset  up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Шаг 5. Настройте G0/1 на R2, затем G0/0/0 и статическую маршрутизацию для обоих маршрутизаторов

a. Настройте G0/0/1 на R2 с первым IP-адресом подсети C, рассчитанным ранее.

```
R2(config)#int g0/0/1
R2(config-if)#ip address 192.168.1.97 255.255.255.240
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
```

b. Настройте интерфейс G0/0/0 для каждого маршрутизатора на основе приведенной выше таблицы IP-адресации.

```
R2(config-if)#int g0/0/0
R2(config-if)#ip address 10.0.0.2 255.255.255.252
R2(config-if)#no shutdowns
                         ^
% Invalid input detected at '^' marker.

R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
```

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

```
R1_Sidorov(config)#int g0/0/0
R1_Sidorov(config-if)#ip address 10.0.0.1 255.255.255.252
R1_Sidorov(config-if)#no shutdown

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
```

c. Настройте маршрут по умолчанию на каждом маршрутизаторе, указываемом на IP-адрес G0/0/0 на другом маршрутизаторе.

```
R1_Sidorov(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

```
R2(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.1
R2(config)#
```

d. Убедитесь, что статическая маршрутизация работает с помощью отправки эхо-запроса до адреса G0/0/1 R2 от R1_ФАМИЛИЯ.

```
R1_Sidorov#
%SYS-5-CONFIG_I: Configured from console by console
ping
Protocol [ip]:
Target IP address: 192.168.1.97
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.97, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

e. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

```
R1_Sidorov#write memory
Building configuration...
[OK]
```

```
R2#write memory
Building configuration...
[OK]
```

Шаг 6. Настройте базовые параметры каждого коммутатора.

a. Присвойте коммутатору имя устройства.

b. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

c. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

d. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.

e. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.

f. Зашифруйте открытые пароли.

g. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

h. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

i. Установите часы на маршрутизаторе на сегодняшнее время и дату.

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

www.netacad.com

Примечание. Вопросительный знак (**?**) позволяет открыть справку с правильной последовательностью параметров, необходимых для выполнения этой команды.

j. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with
Switch(config)#hostname S1
S1(config)#no ip domain lookup
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#vty 0 15
             ^
% Invalid input detected at '^' marker.

S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service pass
S1(config)#service password-encryption
S1(config)#banner motd #Unauthorized banned#
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
clock set 11:53:00 17 march 2024
S1#write memory
Building configuration...
[OK]
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End wit
Switch(config)#hostname S2
S2(config)#no ip domain lookup
S2(config)#enable secret class
S2(config)#line con 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd #Unauthorized banned#
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
```

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Шаг 7. Создайте сети VLAN на коммутаторе S1.

Примечание. S2 настроен только с базовыми настройками.

a. Создайте необходимые VLAN на коммутаторе 1 и присвойте им имена из приведенной выше таблицы.

```
Enter configuration commands, one
S1(config)#vlan 100
S1(config-vlan)#name Clients
S1(config-vlan)#exit
S1(config)#vlan 221
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#vlan 999
S1(config-vlan)#name Parking_lot
S1(config-vlan)#exi
S1(config)#vlan 1000
S1(config-vlan)#name Native
S1(config-vlan)#exit
```

b. Настройте и активируйте интерфейс управления на S1 (VLAN X+200), используя второй IP-адрес из подсети, рассчитанный ранее. Кроме того установите шлюз по умолчанию на S1.

```
S1(config)#int vlan 221
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan221, changed state to up

S1(config-if)#ip address 192.168.1.66 255.255.255.224
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.1.65
```

c. Настройте и активируйте интерфейс управления на S2 (VLAN 1), используя второй IP-адрес из подсети, рассчитанный ранее. Кроме того, установите шлюз по умолчанию на S2

```
S2(config)#int vlan 1
S2(config-if)#ip address 192.168.1.98 255.255.255.240
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
exit
S2(config)#ip default-gateway 192.168.1.97
```

d. Назначьте все неиспользуемые порты S1 VLAN Parking_Lot, настройте их для статического режима доступа и административно деактивируйте их. На S2 административно деактивируйте все неиспользуемые порты.

```
S1(config)#int range f0/1-4, f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#shut
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
```

```
S2(config)#int range f0/1-4, f0/6-17, f0/19-24, g0/1-2
S2(config-if-range)#shut

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
```

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

www.netacad.com

Примечание. Команда interface range полезна для выполнения этой задачи с минимальным количеством команд.

Шаг 8. Назначьте сети VLAN соответствующим интерфейсам коммутатора.

a. Назначьте используемые порты соответствующей VLAN (указанной в таблице VLAN выше) и настройте их для режима статического доступа.

```
S1(config)#int f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 100
S1(config-if)#no shut
S1(config-if)#exit
```

b. Убедитесь, что VLAN назначены на правильные интерфейсы.

```
S1(config)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5
100  Clients                          active    Fa0/6
221  Management                       active
999  Parking_lot                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
1000 Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1(config)#
```

c. Почему интерфейс F0/5 указан в VLAN 1? Потому что

данный интерфейс не был назначен ни одному из созданных

VLAN => он указан VLAN 1

Шаг 9. Вручную настройте интерфейс S1 F0/5 в качестве транка 802.1Q.

a. Измените режим порта коммутатора, чтобы принудительно создать магистральный канал.

b. В рамках конфигурации транкового канала установите для native VLAN значение 1000.

c. В качестве другой части конфигурации магистрали укажите, что VLAN 100, X+200 и 1000 могут проходить по транковому каналу.

d. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

```
S1(config)#int f0/5
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan221, changed state to up

S1(config-if)#switchport trunk native vlan 1000
S1(config-if)#switchport trunk allowed vlan 100,221,1000
S1(config-if)#exit
S1(config)#do write memory
Building configuration...
[OK]
```

e. Проверьте состояние транкового канала.

```
S1(config)#do show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/5       on           802.1q         trunking      1000

Port        Vlans allowed on trunk
Fa0/5       100,221,1000

Port        Vlans allowed and active in management domain
Fa0/5       100,221,1000

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/5       100,221,1000
```

Какой IP-адрес был бы у ПК, если бы он был подключен к сети с помощью DHCP? Один из указанных в подсети A

Часть 2. Настройка и проверка двух серверов DHCPv4 на R1_ФАМИЛИЯ

В части 2 необходимо настроить и проверить сервер DHCPv4 на R1_ФАМИЛИЯ. Сервер DHCPv4 будет обслуживать две подсети, подсеть A и подсеть C.

Шаг 1. Настройте R1_ФАМИЛИЯ с пулами DHCPv4 для двух поддерживаемых подсетей. Ниже приведен только пул DHCP для подсети A

a. Исключите первые пять используемых адресов из каждого пула адресов.

```
R1_Sidorov(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.5
R1_Sidorov(config)#ip dhcp excluded-address 192.168.1.97 192.168.1.101
```

b. Создайте пул DHCP (используйте уникальное имя для каждого пула).

c. Укажите сеть, поддерживающую этот DHCP-сервер.

d. В качестве имени домена укажите CCNA-lab.com.

e. Настройте соответствующий шлюз по умолчанию для каждого пула DHCP.

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

f. Затем настройте второй пул DHCPv4, используя имя пула R2_Client_LAN и вычислите сеть, шлюз по умолчанию, и используйте то же имя домена и время аренды, что и предыдущий пул DHCP.

```
R1_Sidorov(config)#ip dhcp pool VLAN100
R1_Sidorov(dhcp-config)#network 192.168.1.0 255.255.255.192
R1_Sidorov(dhcp-config)#default-router 192.168.1.1
R1_Sidorov(dhcp-config)#domain-name CCNA-lab.com
R1_Sidorov(dhcp-config)#exit
R1_Sidorov(config)#ip dhcp pool R2_Client_LAN
R1_Sidorov(dhcp-config)#network 192.168.1.96 255.255.255.240
R1_Sidorov(dhcp-config)#default-router 192.168.1.97
R1_Sidorov(dhcp-config)#domain-name CCNA-lab.com
R1_Sidorov(dhcp-config)#exit
R1_Sidorov(config)#do write memory
Building configuration...
[OK]
```

Шаг 2. Сохраните конфигурацию.

Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 3. Проверка конфигурации сервера DHCPv4

a. Чтобы просмотреть сведения о пуле, выполните команду **show ip dhcp pool** .

```
R1_Sidorov(config)#do show ip dhcp pool

Pool VLAN100 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 0
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.1          192.168.1.1      - 192.168.1.62      0    / 2     / 62

Pool R2_Client_LAN :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 14
 Leased addresses               : 0
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.97         192.168.1.97     - 192.168.1.110     0    / 2     / 14
```

b. Выполните команду **show ip dhcp bindings** для проверки установленных назначений адресов DHCP.

```
R1_Sidorov#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
```

c. Выполните команду **show ip dhcp server statistics** для проверки сообщений DHCP.

Шаг 4. Попытка получить IP-адрес от DHCP на PC-A

a. Из командной строки компьютера PC-A выполните команду **ipconfig /all**.

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

www.netacad.com

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0050.0FA2.2075
   Link-local IPv6 Address.........: FE80::250:FFF:FEA2:2075
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-9B-87-3B-42-00-50-0F-A2-20-75
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 00D0.BA63.DC05
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-9B-87-3B-42-00-50-0F-A2-20-75
   DNS Servers.....................: ::
                                     0.0.0.0
```

b. После завершения процесса обновления выполните команду **ipconfig** для просмотра новой информации об IP-адресе.

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

```
C:\>ipconfig /renew

   IP Address.......................: 192.168.1.6
   Subnet Mask......................: 255.255.255.192
   Default Gateway..................: 192.168.1.1
   DNS Server.......................: 0.0.0.0

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: CCNA-lab.com
   Link-local IPv6 Address.........: FE80::250:FFF:FEA2:2075
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.6
   Subnet Mask.....................: 255.255.255.192
   Default Gateway.................: ::
                                     192.168.1.1

Bluetooth Connection:

   Connection-specific DNS Suffix..: CCNA-lab.com
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```

c. Проверьте подключение с помощью эхо-запроса на IP-адрес интерфейса R1_ФАМИЛИЯ G0/0/1.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Часть 3. Настройка и проверка DHCP-ретрансляции на R2

В части 3 настраивается R2 для ретрансляции DHCP-запросов из локальной сети на интерфейсе G0/0/1 на DHCP-сервер (R1_ФАМИЛИЯ).

Шаг 1. Настройка R2 в качестве агента DHCP-ретрансляции для локальной сети на G0/0/1

a. Настройте команду **ip helper-address** на G0/0/1, указав IP-адрес G0/0/0 R1_ФАМИЛИЯ.

b. Сохраните конфигурацию.

```
R2(config)#int g0/0/1
R2(config-if)#ip helper-address 10.0.0.1
R2(config-if)#exit
R2(config)#do write memory
Building configuration...
[OK]
```

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

www.netacad.com

Шаг 2. Попытка получить IP-адрес от DHCP на PC-B

a. Из командной строки компьютера PC-B выполните команду **ipconfig /all**.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0060.3E06.9899
   Link-local IPv6 Address.........: FE80::260:3EFF:FE06:9899
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-34-B1-1E-41-00-60-3E-06-98-99
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 00D0.97E7.B1E3
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-34-B1-1E-41-00-60-3E-06-98-99
   DNS Servers.....................: ::
                                     0.0.0.0
```

b. После завершения процесса обновления выполните команду **ipconfig** для просмотра новой информации об IP-адресе.

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

www.netacad.com

```
C:\>ipconfig /renew

   IP Address.......................: 192.168.1.102
   Subnet Mask......................: 255.255.255.240
   Default Gateway..................: 192.168.1.97
   DNS Server.......................: 0.0.0.0

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: CCNA-lab.com
   Link-local IPv6 Address.........: FE80::260:3EFF:FE06:9899
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.102
   Subnet Mask.....................: 255.255.255.240
   Default Gateway.................: ::
                                     192.168.1.97

Bluetooth Connection:

   Connection-specific DNS Suffix..: CCNA-lab.com
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
```

c. Проверьте подключение с помощью эхо-запроса на IP-адрес интерфейса R1_ФАМИЛИЯ G0/0/1.

```
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time<1ms TTL=126
Reply from 192.168.1.6: bytes=32 time<1ms TTL=126
Reply from 192.168.1.6: bytes=32 time<1ms TTL=126
Reply from 192.168.1.6: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

d. Выполните **show ip dhcp binding** для R1_ФАМИЛИЯ для проверки назначений адресов в DHCP.

```
R1_Sidorov#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.6      0050.0FA2.2075           --                     Automatic
192.168.1.102    0060.3E06.9899           --                     Automatic
```

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Вопросы для защиты теоретической части (главы 7, 8)

1. **Опишите назначение протокола DHCP. Назовите основные преимущества протокола DHCP**

Протокол динамической конфигурации узла v4 (DHCPv4) динамически назначает адреса IPv4 и другую информацию о конфигурации сети. Поскольку стационарные ПК обычно составляют основную часть сетевых узлов, протокол DHCPv4 является крайне полезным инструментом, позволяющим сетевым администраторам значительно экономить время.

2. **Опишите принцип работы протокола DHCP. Какой тип рассылки используется в сообщении DHCP Discover и почему?**

DHCPv4 работает по модели «клиент-сервер». Когда клиент подключается к серверу DHCPv4, сервер присваивает или сдает ему в аренду IPv4-адрес. . Поскольку клиент не может знать, к какой подсети он относится, сообщение DHCPDISCOVER представляет собой широковещательную рассылку IPv4 (IPv4-адрес назначения 255.255.255.255)

3. **Укажите основные шаги для получения IP-адреса при использовании протокола DHCPv4. Какие основные действия необходимо предпринять для настройки сервера DHCPv4?**

1. Обнаружение DHCP (DHCPDISCOVER)

2. Предложение DHCP (DHCPOFFER)

3. Запрос DHCP (DHCPREQUEST)

4. Подтверждение DHCP (DHCPACK)

Шаг 1. Исключение IPv4-адресов. Можно исключить один адрес или диапазон адресов, задав адреса нижнего и верхнего пределов диапазона. В число исключенных адресов должны входить адреса, присвоенные маршрутизаторам, серверам, принтерам и другим устройствам, которые были или будут настроены вручную. Можно также ввести команду несколько раз. Команда ip dhcp excluded-address low-address [top-address]

Шаг 2. Определите имя пула DHCPv4. Команда ip dhcp pool pool-name (имя пула) создает пул с заданным именем и переводит маршрутизатор в режим конфигурации протокола DHCPv4

Шаг 3. Создайте пул DHCPv4. Пул адресов и основной шлюз маршрутизатора должны быть настроены. Используйте команду network для определения диапазона доступных адресов. Используйте команду default-router, чтобы задать основной шлюз маршрутизатора

4. **Какой тип рассылки используется в сообщении DHCP Request и почему? Какие шаги используются для продления аренды IP-адреса при использовании протокола DHCPv4?**

Применение широковещательной рассылки обусловлено тем, что на момент отправки DHCP Request клиент ещё не имеет присвоенного IP-адреса, и ему неизвестен адрес DHCP-сервера. Поэтому клиент отправляет свой запрос широковещательно на весь локальный сегмент сети, чтобы обеспечить получение ответа от доступного DHCP-сервера.

1. Запрос DHCP (DHCPREQUEST). Перед окончанием аренды клиент отправляет сообщение DHCPREQUEST непосредственно DHCPv4-серверу, который первоначально предложил IPv4-адрес. Если сообщение DHCPACK не получено за определенный период времени, клиент отправляет другое сообщение DHCPREQUEST широковещательной рассылкой, чтобы другой DHCPv4- сервер мог продлить срок аренды.

2. Подтверждение DHCP (DHCPACK). При получении сообщения DHCPREQUEST сервер подтверждает информацию об аренде ответным сообщением DHCPACK.

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

5. **Для чего необходимо использовать DHCPv4-ретрансляцию? Перечислите варианты назначения GUA для IPv6.**

DHCPv4-ретрансляция используется в сетях, где клиенты DHCP находятся в другом сегменте сети, отличном от сегмента, на котором находится DHCP-сервер. Варианты назначения глобальных уникальных адресов (GUA) для IPv6 включают: статическое назначение, автоматическое назначение с использованием DHCPv6 и назначение с помощью Stateless Address Autoconfiguration (SLAAC).

6. **Охарактеризуйте работу метода SLAAC. Какие флаги используются в сообщении RA и что они означают?**

SLAAC - это служба без определения состояния, которая означает, что нет сервера, который поддерживает информацию о сетевых адресах, чтобы знать, какие IPv6-адреса используются и какие из них доступны. SLAAC отправляет периодические ICMPv6 RA-сообщения (то есть каждые 200 секунд), предоставляя адресацию и другую информацию о конфигурации для узлов для автонастройки их IPv6 адреса на основе информации в RA.

Сообщение ICMPv6 RA содержит следующие три флага:

Флаг A. Флаг автонастройки адреса означает использование автоматической настройки адресов без состояния (SLAAC) для создания GUA IPv6

Значение флага O, равное 1, используется для информирования клиента о том, что на DHCPv6-сервере без отслеживания состояния доступна дополнительная информация о конфигурации.

Флаг M. Флаг конфигурации управляемого адреса означает использование сервера DHCPv6 с сохранением состояния для получения GUA IPv6.

7. **Охарактеризуйте работу метода DHCPv6 без сохранения состояния. Опишите методы, используемые для генерации идентификатора интерфейса при использовании SLAAC.**

Если RA указывает метод DHCPv6 без учета состояния, узел использует информацию из сообщения RA для адресации и связывается с сервером DHCPv6 для получения дополнительной информации

8. **Охарактеризуйте работу метода DHCPv6 с сохранением состояния. Опишите основные шаги работы DHCPv6.**

DHCPv6 с сохранением состояния (stateful DHCPv6) используется для назначения IP-адресов и других настроек. Основные шаги работы DHCPv6 включают в себя передачу сообщения DHCPv6 Solicit, получение DHCPv6 Advertisement от сервера и назначение IP-адреса.

9.**Как клиент IPv6 может убедиться в уникальности своего IPv6-адреса, полученного с помощью метода SLAAC? Какие основные действия необходимо предпринять для настройки сервера DHCPv6?**

Когда клиент IPv6 использует метод SLAAC (Stateless Address Autoconfiguration) для получения своего IPv6-адреса, он формирует свой адрес на основе префикса, который объявлен в сети, и своего MAC-адреса. Уникальность адреса обеспечивается за счет уникальности MAC-адреса клиента. Однако, чтобы убедиться в уникальности своего адреса, клиент может выполнить следующие действия:

Произвести проверку на конфликт адресов: Клиент может отправить сообщение Neighbor Solicitation (NS) с целью проверить, используется ли его IPv6-адрес уже другим устройством в сети. Если клиент не получит ответ на такое сообщение, это означает, что

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

его адрес уникален в сети.

Проверить локальные таблицы ассоциации адресов: Клиент может проверить свои локальные таблицы ассоциации адресов (ARP для IPv4, NDP для IPv6) на наличие конфликтов. Если клиент обнаружит, что его IPv6-адрес уже ассоциирован с другим устройством, он должен запросить новый адрес.

Для настройки сервера DHCPv6 (Dynamic Host Configuration Protocol version 6) основные действия включают в себя следующее:

Настройка интерфейса для работы с DHCPv6: Настройте интерфейс на сервере DHCPv6, чтобы он был способен слушать DHCPv6 запросы. Например:

Router(config)# interface gigabitethernet0/0

Router(config-if)# ipv6 dhcp server <пул_адресов>

Создание DHCPv6 пула: Создайте пул DHCPv6, в котором будет указан диапазон IPv6-адресов, которые сервер DHCPv6 будет выдавать клиентам. Например:

Router(config)# ipv6 dhcp pool <имя_пула>

Router(config-dhcp)# address prefix <префикс_сети> <длина_префикса>

Router(config-dhcp)# dns-server <IPv6_DNS_сервер>

Настройка параметров DHCPv6: Укажите другие параметры DHCPv6, такие как DNS-серверы, адрес шлюза и дополнительные параметры, если необходимо.

Активация DHCPv6 на интерфейсе: Активируйте DHCPv6 на интерфейсе, чтобы сервер DHCPv6 начал обрабатывать DHCPv6 запросы от клиентов. Например:

Router(config-if)# ipv6 nd other-config-flag

© © 2017 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Конфигурация безопасности коммутатора

Топология

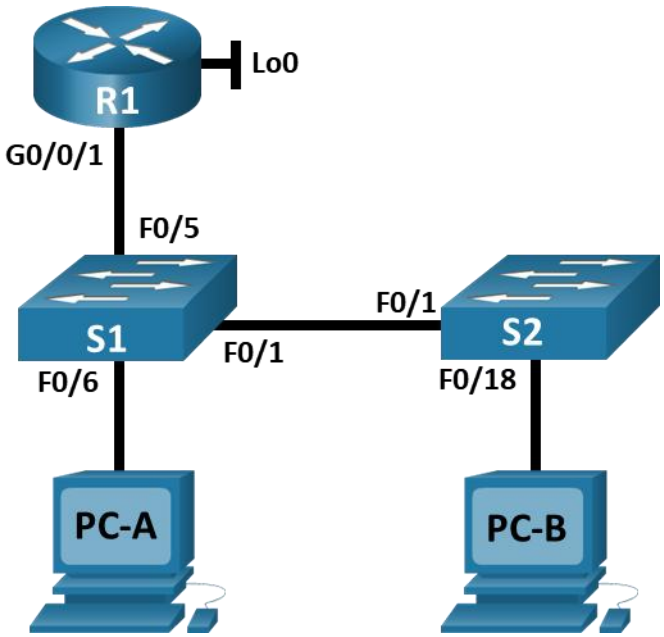


Таблица адресации

Устройство	interface/vlan	IP-адрес	Маска подсети
R1_ФАМИЛИЯ	G0/0/1	192.168.31.1	255.255.255.0
	Loopback 0	10.10.1.1	255.255.255.0
S1	VLAN 31	192.168.31.201	255.255.255.0
S2	VLAN 31	192.168.31.202	255.255.255.0
PC A	NIC	DHCP	255.255.255.0
PC B	NIC	DHCP	255.255.255.0

Цели

Часть 1. Настройка основного сетевого устройства

- Создайте сеть.
- Настройте маршрутизатор R1_ФАМИЛИЯ.

Конфигурация безопасности коммутатора

- Настройка и проверка основных параметров коммутатора

Часть 2. Настройка сетей VLAN

- Сконфигруриуйте VLAN X+10.
- Сконфигруриуйте SVI для VLAN X+10.
- Настройте VLAN 333 с именем Native на S1 и S2.
- Настройте VLAN 999 с именем ParkingLot на S1 и S2.

Часть 3: Настройки безопасности коммутатора.

- Реализация магистральных соединений 802.1Q.
- Настройка портов доступа
- Безопасность неиспользуемых портов коммутатора
- Документирование и реализация функций безопасности порта.
- Реализовать безопасность DHCP snooping .
- Реализация PortFast и BPDU Guard
- Проверка сквозной связанности.

Необходимые ресурсы

- 1 Маршрутизатор (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.3 или аналогичным)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (ОС Windows с программой эмуляции терминалов, такой как Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты.
- Кабели Ethernet, расположенные в соответствии с топологией

Инструкции

Часть 1. Настройка основного сетевого устройства

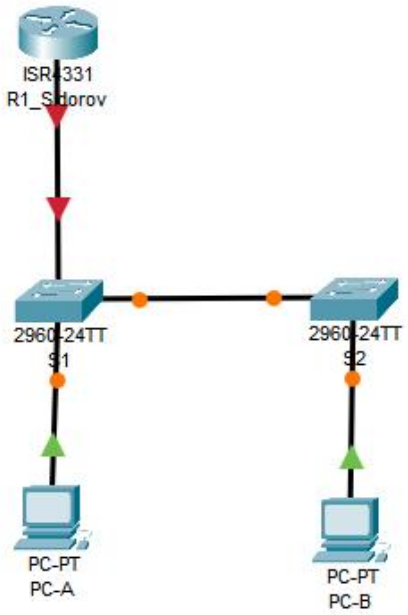
Шаг 1. Создайте сеть.

a. Создайте сеть согласно топологии.

b. Инициализация устройств

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Конфигурация безопасности коммутатора



Шаг 2. Настройте маршрутизатор R1_ФАМИЛИЯ.

a. Загрузите следующий конфигурационный скрипт на R1_ФАМИЛИЯ.

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1_Sidorov
R1_Sidorov(config)#no ip domain-lookup
R1_Sidorov(config)#ip dhcp excluded-address 192.168.31.1 192.168.31.9
R1_Sidorov(config)#ip dhcp excluded-address 192.168.31.201 192.168.31.202
R1_Sidorov(config)#ip dhcp pool Students
R1_Sidorov(dhcp-config)#network 192.168.31.0 255.255.255.0
R1_Sidorov(dhcp-config)#default-router 192.168.31.1
R1_Sidorov(dhcp-config)#domain-name CCNA2.Lab-7
R1_Sidorov(dhcp-config)#exit
R1_Sidorov(config)#interface Loopback0

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1_Sidorov(config-if)#ip address 10.10.1.1 255.255.255.0
R1_Sidorov(config-if)#exit
R1_Sidorov(config)#interface g0/0/1
R1_Sidorov(config-if)#description Link to S1
R1_Sidorov(config-if)#no shutdown

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1_Sidorov(config-if)#line con 0
R1_Sidorov(config-line)#logging sync
R1_Sidorov(config-line)#logging synchronous
R1_Sidorov(config-line)#exec-timeout 0 0
R1_Sidorov(config-line)#exit
R1_Sidorov(config)#
R1_Sidorov(config)#ip dhcp relay information trust-all
```

b. Проверьте конфигурацию сетевых интерфейсов на R1_ФАМИЛИЯ.

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

Конфигурация безопасности коммутатора

```
R1_Sidorov(config)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   192.168.31.1    YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Loopback0              10.10.1.1       YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

c. Убедитесь, что IP-адресация и интерфейсы находятся в состоянии up / up (при необходимости устраните неполадки).

Шаг 3. Настройка и проверка основных параметров коммутатора

a. Настройте имя хоста для коммутаторов S1 и S2.
b. Запретите нежелательный поиск в DNS.

c. Настройте описания интерфейса для портов, которые используются в S1 и S2.

d. Установите для шлюза по умолчанию для VLAN управления значение 192.168.X+10.1 на обоих коммутаторах.

```
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#int F0/5
S1(config-if)#description Connection to Router
S1(config-if)#exit
S1(config)#int F0/1
S1(config-if)#description Connection to S2
S1(config-if)#exit
S1(config)#int F0/6
S1(config-if)#description Connection to PCA
S1(config-if)#exit
```

```
S1(config)#ip default-gateway 192.168.31.1
S1(config)#do write memory
Building configuration...
[OK]
```

```
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#int f0/1
S2(config-if)#description Connection to S1
S2(config-if)#exit
S2(config)#int f0/18
S2(config-if)#description Connection to PCB
S2(config-if)#exit
```

```
S2(config)#ip default-gateway 192.168.31.1
S2(config)#do write memory
Building configuration...
[OK]
```

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Часть 2. Настройка сетей VLAN на коммутаторах.

Шаг 1. Сконфигруриуйте VLAN X+10.

Добавьте VLAN X+10 на S1 и S2 и назовите VLAN - **Management.**

Шаг 2. Сконфигруриуйте SVI для VLAN X+10. Настройте IP-адрес в соответствии с таблицей адресации для SVI для VLAN X+10 на S1 и S2. Включите интерфейсы SVI и предоставьте описание для интерфейса.

Шаг 3. Настройте VLAN 333 с именем Native на S1 и S2.

Шаг 4. Настройте VLAN 999 с именем ParkingLot на S1 и S2.

```
S1(config)#vlan 31
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#interface vlan 31
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan31, changed state to up

S1(config-if)#ip address 192.168.31.201 255.255.255.0
S1(config-if)#description Management Vlan
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#exit
S1(config)#do write memory
Building configuration...
[OK]
```

```
S2(config)#vlan 31
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#int vlan 31
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan31, changed state to up

S2(config-if)#ip address 192.168.31.202 255.255.255.0
S2(config-if)#description Management Vlan
S2(config-if)#no shut
S2(config-if)#exit
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#exit
S2(config)#do write memory
Building configuration...
[OK]
```

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Конфигурация безопасности коммутатора

Часть 3. Настройки безопасности коммутатора.

Шаг 1. Релизация магистральных соединений 802.1Q.

a. Настройте все магистральные порты Fa0/1 на обоих коммутаторах для использования VLAN 333 в качестве native VLAN.

```
S1(config)#interface f0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan31, changed state to up
switchport trunk native vlan 333
S1(config-if)#exit
```

```
S2(config)#int f0/1
S2(config-if)#switchport mode trunk

S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan31, changed state to up
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 333 on
FastEthernet0/1 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent local
vlan.


S2(config-if)#switchport trunk native vlan 333
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0333.
Port consistency restored.
```

b. Убедитесь, что режим транкинга успешно настроен на всех коммутаторах с помощью команды **show interface trunk** на обоих коммутаторах.

```
S1(config)#do show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      333

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,31,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       31,999
```

```
S2(config)#do show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      333

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,31,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,31,333,999
```

c. Отключить согласование DTP F0/1 на S1 и S2.

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

Конфигурация безопасности коммутатора

```
S1(config)#int f0/1
S1(config-if)#switchport none
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1(config)#

S2(config)#int f0/1
S2(config-if)#switchport non
S2(config-if)#switchport nonegotiate
S2(config-if)#exit
S2(config)#
```

d. Проверьте с помощью команды **show interfaces**. Пример:

```
S1(config)#do show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off

S2(config)#do show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
```

Шаг 2. Настройка портов доступа

a. На S1 настройте F0/5 и F0/6 в качестве портов доступа и свяжите их с VLAN X+10.

```
S1(config)#int range f0/5-6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 31
S1(config-if-range)#exit
```

b. На S2 настройте порт доступа Fa0/18 и свяжите его с VLAN X+10.

```
S2(config)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 31
S2(config-if)#exit
```

Шаг 3. Безопасность неиспользуемых портов коммутатора

a. На S1 и S2 переместите неиспользуемые порты из VLAN 1 в VLAN 999 и отключите неиспользуемые порты.

```
interface range not validated - command rejecte
S1(config)#int range f0/2-4, f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#shutdown
```

```
S1(config)#int range g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#shutdown
```

```
S2(config)#int range f0/2-17, f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#shutdown
```

b. Убедитесь, что неиспользуемые порты отключены и связаны с VLAN 999, введя команду **show interfaces status**.

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

Конфигурация безопасности коммутатора

```
S1(config)#do show interfaces status
Port      Name                Status       Vlan       Duplex  Speed Type
Fa0/1     Connection to S2    connected    trunk      auto    auto  10/100BaseTX
Fa0/2                         disabled 999        auto    auto  10/100BaseTX
Fa0/3                         disabled 999        auto    auto  10/100BaseTX
Fa0/4                         disabled 999        auto    auto  10/100BaseTX
Fa0/5     Connection to Rout  connected    31         auto    auto  10/100BaseTX
Fa0/6     Connection to PCA   connected    31         auto    auto  10/100BaseTX
Fa0/7                         disabled 999        auto    auto  10/100BaseTX
Fa0/8                         disabled 999        auto    auto  10/100BaseTX
Fa0/9                         disabled 999        auto    auto  10/100BaseTX
Fa0/10                        disabled 999        auto    auto  10/100BaseTX
Fa0/11                        disabled 999        auto    auto  10/100BaseTX
Fa0/12                        disabled 999        auto    auto  10/100BaseTX
Fa0/13                        disabled 999        auto    auto  10/100BaseTX
Fa0/14                        disabled 999        auto    auto  10/100BaseTX
Fa0/15                        disabled 999        auto    auto  10/100BaseTX
Fa0/16                        disabled 999        auto    auto  10/100BaseTX
Fa0/17                        disabled 999        auto    auto  10/100BaseTX
Fa0/18                        disabled 999        auto    auto  10/100BaseTX
Fa0/19                        disabled 999        auto    auto  10/100BaseTX
Fa0/20                        disabled 999        auto    auto  10/100BaseTX
Fa0/21                        disabled 999        auto    auto  10/100BaseTX
Fa0/22                        disabled 999        auto    auto  10/100BaseTX
Fa0/23                        disabled 999        auto    auto  10/100BaseTX
Fa0/24                        disabled 999        auto    auto  10/100BaseTX
Gig0/1                        disabled 999        auto    auto  10/100BaseTX
Gig0/2                        disabled 999        auto    auto  10/100BaseTX
```

```
S2(config)#do show interfaces status
Port      Name                Status       Vlan       Duplex  Speed Type
Fa0/1     Connection to S1    connected    trunk      auto    auto  10/100BaseTX
Fa0/2                         disabled 999        auto    auto  10/100BaseTX
Fa0/3                         disabled 999        auto    auto  10/100BaseTX
Fa0/4                         disabled 999        auto    auto  10/100BaseTX
Fa0/5                         disabled 999        auto    auto  10/100BaseTX
Fa0/6                         disabled 999        auto    auto  10/100BaseTX
Fa0/7                         disabled 999        auto    auto  10/100BaseTX
Fa0/8                         disabled 999        auto    auto  10/100BaseTX
Fa0/9                         disabled 999        auto    auto  10/100BaseTX
Fa0/10                        disabled 999        auto    auto  10/100BaseTX
Fa0/11                        disabled 999        auto    auto  10/100BaseTX
Fa0/12                        disabled 999        auto    auto  10/100BaseTX
Fa0/13                        disabled 999        auto    auto  10/100BaseTX
Fa0/14                        disabled 999        auto    auto  10/100BaseTX
Fa0/15                        disabled 999        auto    auto  10/100BaseTX
Fa0/16                        disabled 999        auto    auto  10/100BaseTX
Fa0/17                        disabled 999        auto    auto  10/100BaseTX
Fa0/18    Connection to PCB   connected    31         auto    auto  10/100BaseTX
Fa0/19                        disabled 999        auto    auto  10/100BaseTX
Fa0/20                        disabled 999        auto    auto  10/100BaseTX
Fa0/21                        disabled 999        auto    auto  10/100BaseTX
Fa0/22                        disabled 999        auto    auto  10/100BaseTX
Fa0/23                        disabled 999        auto    auto  10/100BaseTX
Fa0/24                        disabled 999        auto    auto  10/100BaseTX
Gig0/1                        disabled 999        auto    auto  10/100BaseTX
Gig0/2                        disabled 999        auto    auto  10/100BaseTX
```

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

Конфигурация безопасности коммутатора

Шаг 4. Документирование и реализация функций безопасности порта.

Интерфейсы F0/6 на S1 и F0/18 на S2 настроены как порты доступа. На этом шаге вы также настроите безопасность портов на этих двух портах доступа.

a. На S1 введите команду **show port-security interface f0/6** для отображения настроек по умолчанию безопасности порта для интерфейса F0/6. Запишите свои ответы ниже.

```
S1(config)#do show port-security interface f0/6
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
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

b. На S1 включите защиту порта на F0/6 со следующими настройками:

- Максимальное количество записей MAC-адресов: **3**
- Режим безопасности: **restrict**
- Aging time: **60 мин.**

```
S1(config)#int f0/6
S1(config-if)#switchport-security maximum
                          ^
% Invalid input detected at '^' marker.

S1(config-if)#switchport port-security maximum 3
S1(config-if)#switchport port-security violation restrict
S1(config-if)#switchport port-security aging time 60
S1(config-if)#switchport port-security aging type inactivity
```

c. Проверьте настройки защиты порта (**port-security**) на S1 для интерфейса F0/6. Далее просмотрите выходные данные команды **show port-security address**.

```
S1(config)#do show port-security interface f0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 60 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

Конфигурация безопасности коммутатора

```
S1(config)#do show port-security address
                Secure Mac Address Table
----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

d. Включите безопасность порта для F0/18 на S2. Настройте каждый активный порт доступа таким образом, чтобы он автоматически добавлял адреса MAC, изученные на этом порту, в текущую конфигурацию.

```
S2(config)#int f0/18
S2(config-if)#switchport port-security
S2(config-if)#exit
```

e. Настройте следующие параметры безопасности порта на S2 F0/18:

- Максимальное количество записей MAC-адресов: **2**
- Тип безопасности: **Protect**
- Aging time: **60 мин.**

```
S2(config)#int f0/18
S2(config-if)#switchport port-security
S2(config-if)#exit
S2(config)#int f0/18
S2(config-if)#switchport port-secuirty maximum 2
                                 ^
% Invalid input detected at '^' marker.

S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security violation protect
S2(config-if)#switchport aging time 60
                         ^
% Invalid input detected at '^' marker.

S2(config-if)#switchport port-security aging time 60
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#exit
```

f. Проверьте настройки защиты порта (**port-security**) на S2 для интерфейса F0/18. Далее просмотрите выходные данные команды **show port-security address**.

```
S2(config)#do show port-security interface f0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 60 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Конфигурация безопасности коммутатора

```
S2(config)#do show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Шаг 5. Реализовать безопасность DHCP snooping.

a. На S2 включите DHCP snooping и настройте DHCP snooping во VLAN X+10.

```
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping vlan 31
```

b. Настройте магистральные порты на S2 как доверенные порты.

```
S2(config)#int f0/1
S2(config-if)#ip dhc
S2(config-if)#ip dhcp snooping trus
S2(config-if)#ip dhcp snooping trust
```

c. Ограничьте ненадежный порт Fa0/18 на S2 пятью DHCP-пакетами в секунду.

```
S2(config)#int f0/18
S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#exit
```

d. Проверьте DHCP Snooping на S2 с помощью команды **show ip dhcp snooping**.

```
S2(config)#do show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
31
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
------------------------   -------    ----------------
FastEthernet0/1            yes        unlimited
FastEthernet0/18           no         5
```

e. В командной строке на PC-B освободите, а затем обновите IP-адрес.

```
C:\>ipconfig /release

   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Server......................: 0.0.0.0

C:\>ipconfig /renew

   IP Address......................: 192.168.31.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.31.1
   DNS Server......................: 0.0.0.0
```

f. Проверьте привязку отслеживания DHCP с помощью команды **show ip dhcp snooping binding**.

Конфигурация безопасности коммутатора

```
S2#sho ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
------------------
00:D0:58:C1:AC:BD   192.168.31.10    0           dhcp-snooping  31    FastEthernet0/18
Total number of bindings: 1
```

Шаг 6. Реализация PortFast и BPDU Guard

a. Настройте PortFast на всех портах доступа, которые используются на обоих коммутаторах.

b. Включите защиту BPDU на портах доступа VLAN X+10 для S1 и S2, подключенных к PC-A и PC-B.

```
S1(config)#int f0/5
S1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)#exit
```

```
S1(config)#int f0/6
S1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#exi
```

```
S2(config)#int f0/18
S2(config-if)#span
S2(config-if)#spanning-tree p
S2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)#spanning-tree bp
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#exit
```

c. Убедитесь, что защита BPDU и PortFast включены на соответствующих портах с помощью команды **show spanning-tree interface f0/6 detail**.

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

```
Port 5 (FastEthernet0/5) of VLAN0031 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.5
  Designated root has priority 32799, address 00D0.5836.79A3
  Designated bridge has priority 32799, address 00D0.5836.79A3
  Designated port id is 128.5, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-point by default


S1#show spanning-tree interface f0/6 detail



Port 6 (FastEthernet0/6) of VLAN0031 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.6
  Designated root has priority 32799, address 00D0.5836.79A3
  Designated bridge has priority 32799, address 00D0.5836.79A3
  Designated port id is 128.6, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-point by default
S2#show spanning-tree interface f0/18 detail



Port 18 (FastEthernet0/18) of VLAN0031 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.18
  Designated root has priority 32799, address 00D0.5836.79A3
  Designated bridge has priority 32799, address 00D0.BC14.2C3A
  Designated port id is 128.18, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-point by default
```

Шаг 7. Проверьте наличие сквозного подключения.

Отправьте эхо-запрос между всеми устройствами в таблице IP-адресации.

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Конфигурация безопасности коммутатора

```
C:\>ping 192.168.31.1

Pinging 192.168.31.1 with 32 bytes of data:

Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.31.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.31.201

Pinging 192.168.31.201 with 32 bytes of data:

Request timed out.
Reply from 192.168.31.201: bytes=32 time=1ms TTL=255
Reply from 192.168.31.201: bytes=32 time<1ms TTL=255
Reply from 192.168.31.201: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.31.201:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.31.202

Pinging 192.168.31.202 with 32 bytes of data:

Request timed out.
Reply from 192.168.31.202: bytes=32 time<1ms TTL=255
Reply from 192.168.31.202: bytes=32 time=1ms TTL=255
Reply from 192.168.31.202: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.31.202:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.10.1.1

Pinging 10.10.1.1 with 32 bytes of data:

Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Отправка ping с PC-B

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

Конфигурация безопасности коммутатора

```
C:\>ping 192.168.31.10

Pinging 192.168.31.10 with 32 bytes of data:

Reply from 192.168.31.10: bytes=32 time<1ms TTL=128
Reply from 192.168.31.10: bytes=32 time<1ms TTL=128
Reply from 192.168.31.10: bytes=32 time<1ms TTL=128
Reply from 192.168.31.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.31.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.31.1

Pinging 192.168.31.1 with 32 bytes of data:

Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.31.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.31.201

Pinging 192.168.31.201 with 32 bytes of data:

Request timed out.
Reply from 192.168.31.201: bytes=32 time<1ms TTL=255
Reply from 192.168.31.201: bytes=32 time<1ms TTL=255
Reply from 192.168.31.201: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.31.201:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.31.202

Pinging 192.168.31.202 with 32 bytes of data:

Request timed out.
Reply from 192.168.31.202: bytes=32 time<1ms TTL=255
Reply from 192.168.31.202: bytes=32 time<1ms TTL=255
Reply from 192.168.31.202: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.31.202:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Отправка ping с PC-A

Конфигурация безопасности коммутатора

```
R1_Sidorov#ping
Protocol [ip]:
Target IP address: 192.168.31.201
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.31.201, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

R1_Sidorov#ping
Protocol [ip]:
Target IP address: 192.168.31.202
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.31.202, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
```

Отправка ping с R1_Sidorov

```
S1#ping
Protocol [ip]:
Target IP address: 192.168.31.202
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.31.202, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

S1#ping
Protocol [ip]:
Target IP address: 192.168.31.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.31.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Отправка ping с S1

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Вопросы для защиты теоретической части (глава 11)

1. Вопрос: Для чего необходимо обеспечить безопасность портов коммутатора? Что произойдет, если к порту с включенной безопасностью подключают более одного устройства и почему?

Ответ: Обеспечение безопасности портов коммутатора необходимо для предотвращения несанкционированного доступа к сети и защиты от атак, таких как атаки мак-флуда или атаки переполнения камеры MAC-адресов. Если к порту с включенной безопасностью подключают более одного устройства, то возникает риск возникновения мак-флуда или атаки переполнения камеры MAC-адресов, что может привести к отказу в обслуживании (DoS) или возможности злоумышленнику проникнуть в сеть.

2. Вопрос: Какое минимальное и максимальное количество MAC-адресов может быть разрешено на одном порту коммутатора? Опишите все существующие способы изучения MAC-адресов на коммутаторе.

Ответ: Минимальное количество MAC-адресов, разрешенных на одном порту коммутатора, - один. Максимальное количество зависит от настроек коммутатора, но обычно оно ограничено одним MAC-адресом. Существующие способы изучения MAC-адресов на коммутаторе включают в себя статическое изучение MAC-адресов, динамическое изучение с помощью протокола MAC-адресного изучения (MAC-адреса), а также изучение с использованием механизма статического изучения (sticky learning).

3. Вопрос: Опишите существующие типы устаревания безопасности порта. Каким образом можно активировать отключенный по ошибке порт коммутатора?

Ответ: Существующие типы устаревания безопасности порта включают в себя статическое устаревание, динамическое устаревание и устаревание по неприкосновенности. Чтобы активировать отключенный по ошибке порт коммутатора, вы можете использовать команду no shutdown в режиме конфигурации интерфейса.

4. Вопрос: Дайте характеристику режимам нарушения безопасности порта. В чем заключается опасность включенного протокола согласования DTP?

Ответ: Режимы нарушения безопасности порта включают в себя отклонение, отключение и защиту. Отклонение позволяет записывать нарушения в системный журнал без принятия каких-либо мер. Отключение отключает порт, если нарушение безопасности обнаружено. Защита автоматически закрывает порт и предотвращает дальнейшие нарушения. Опасность включенного протокола согласования DTP заключается в том, что злоумышленник может использовать этот протокол для внедрения в сеть с целью выполнения атак вроде атаки мак-флуда или атаки переполнения камеры MAC-адресов.

5. Вопрос: Опишите суть технологии DHCP Snooping. Для чего может понадобиться динамическая проверка ARP?

Ответ: DHCP Snooping - это технология, которая используется для защиты сети от атак DHCP-отравления или от других атак, связанных с DHCP. Он контролирует передачу DHCP-сообщений на недоверенных портах и регистрирует информацию о DHCP-клиентах. Динамическая проверка ARP может потребоваться для защиты сети от атак перехвата ARP или от других атак, связанных с ARP, путем мониторинга ARP-таблиц и предотвращения подмены MAC-адресов.

6. Вопрос: Перечислите рекомендации по настройке портов с помощью динамической проверки ARP. Почему необходимо включать функции BPDU Guard И PortFast?

Ответ: Рекомендации по настройке портов с использованием динамической проверки ARP включают в себя настройку доверенных портов для устройств, которые отправляют ARP-запросы, и настройку недоверенных портов для всех остальных портов. Включение функций BPDU Guard и PortFast необходимо для обеспечения безопасности сети и предотвращения возможных атак, таких как атаки на мак-адреса и атаки на маршрутизаторы.

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

Конфигурация безопасности коммутатора

7. Вопрос: Какие шаги необходимо предпринять для устранения угрозы VLAN Hopping?
Ответ: Для устранения угрозы VLAN Hopping необходимо настроить протоколы безопасности VLAN, такие как Private VLANs, а также настроить механизмы защиты от атак, такие как DHCP Snooping и Dynamic ARP Inspection.

8. Вопрос: Что рекомендуется сделать при использовании сети native VLAN? Какие два типа портов коммутаторов используются на коммутаторах Cisco в составе средств защиты от атак DHCPспуфинга?
Ответ: При использовании сети native VLAN рекомендуется настроить разрешение безопасности порта для всех портов, находящихся в сети native VLAN. Два типа портов коммутаторов Cisco, используемых в качестве средств защиты от атак DHCP-спуфинга, включают в себя доверенные порты и недоверенные порты.

9. **Вопрос: Почему устройства уровня 2 считаются самым слабым звеном в инфраструктуре безопасности компании? Где хранятся динамически определяемые MAC-адреса, когда включена функция sticky learning?**
Ответ: Устройства уровня 2 считаются самым слабым звеном в инфраструктуре безопасности компании, потому что они имеют ограниченные механизмы защиты и могут быть подвержены различным атакам, таким как атаки мак-адресов и атаки переполнения камеры MAC-адресов. Динамически определяемые MAC-адреса, когда включена функция sticky learning, хранятся во временном кэше коммутатора.

© © 2019 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Настройка Rapid PVST+, PortFast и BPDU Guard

Топология

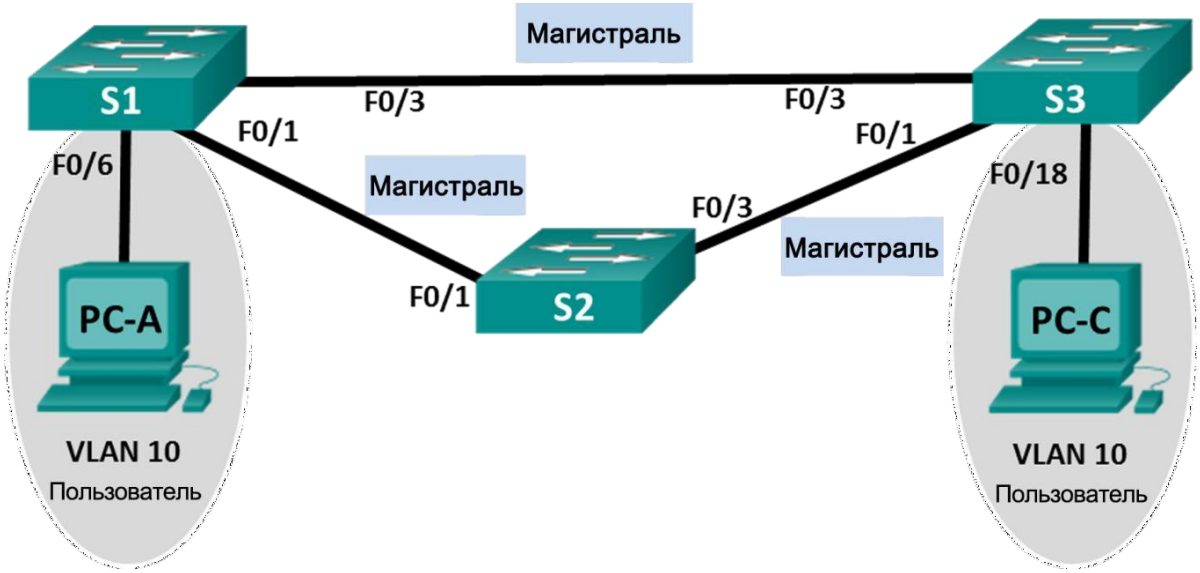


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1_Sidorov	VLAN 99	192.168.22.11	255.255.255.0
S2	VLAN 99	192.168.22.12	255.255.255.0
S3	VLAN 99	192.168.22.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

Назначения сети VLAN

VLAN	Имя
10	User_Sidorov
99	Management

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Настройка сетей VLAN, native VLAN и транковых каналов

Часть 3. Настройка корневого моста и проверка сходимости PVST+

Часть 4. Настройка Rapid PVST+, PortFast, BPDU guard и проверка сходимости

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

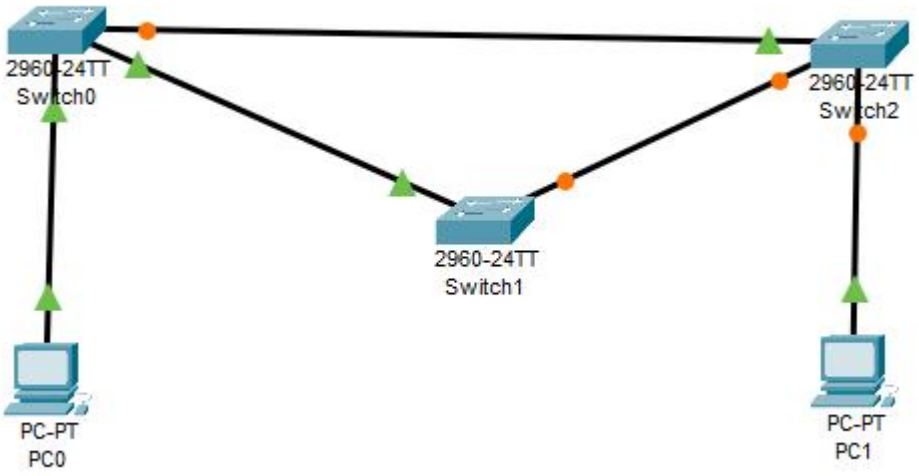
Необходимые ресурсы

- 3 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (ОС Windows с программой эмуляции терминала, например, Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией

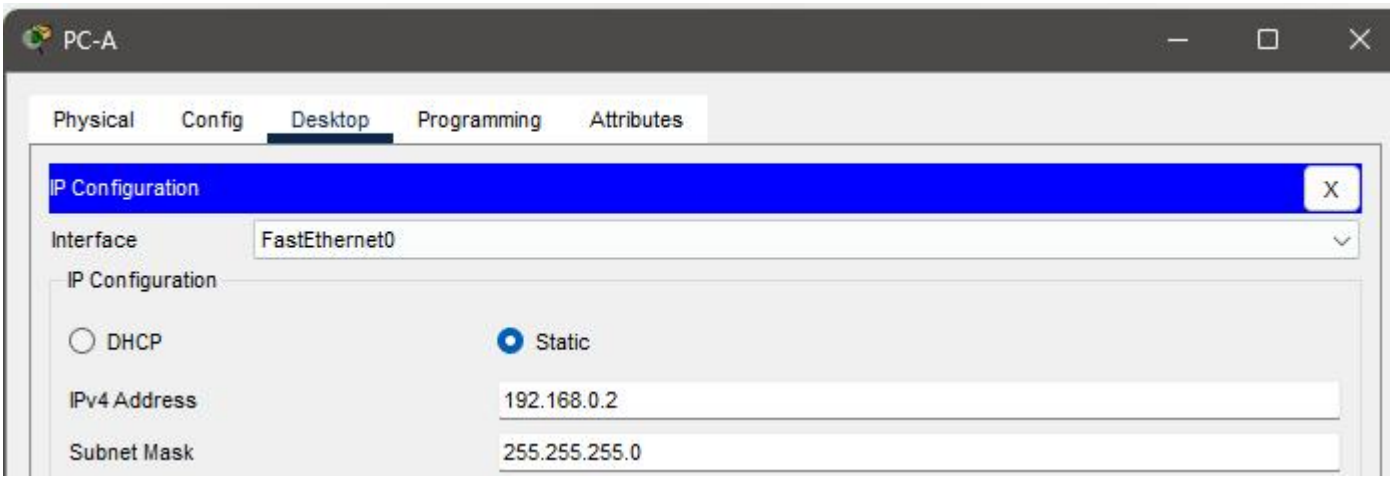
Часть 1: Создание сети и настройка основных параметров устройства

В части 1 вы настроите топологию сети и такие базовые параметры, как IP-адреса интерфейсов, доступ к устройствам и пароли.

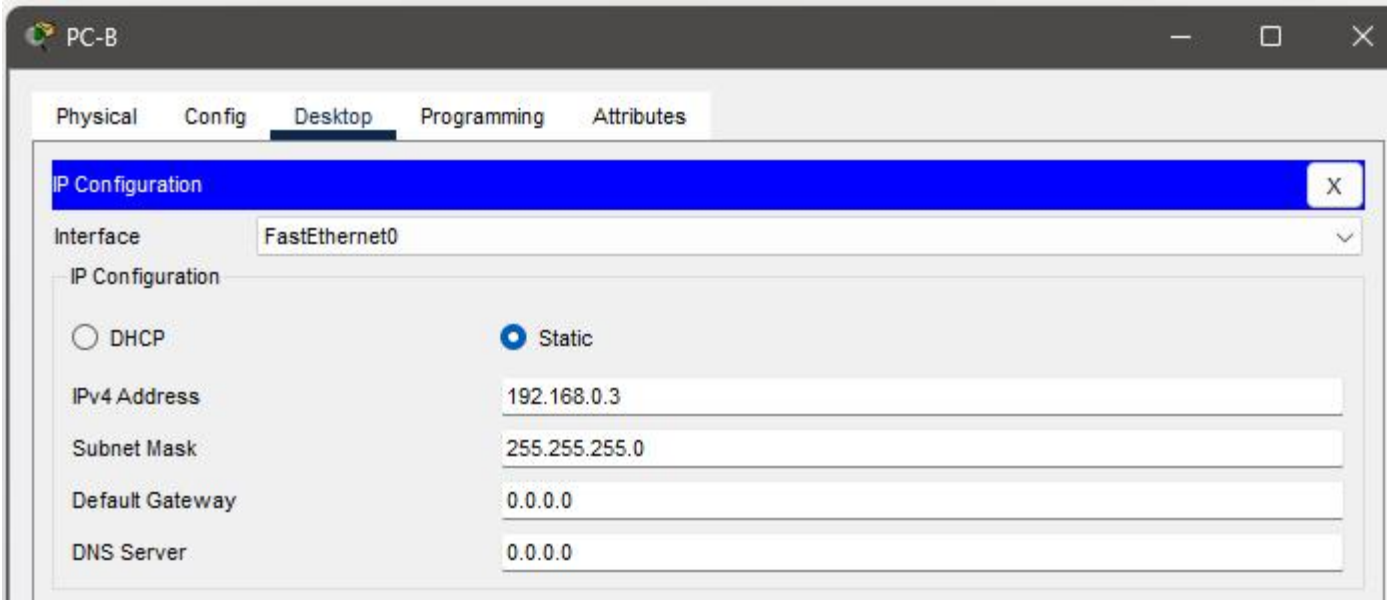
Шаг 1: Создайте сеть согласно топологии.



Шаг 2: Настройте узлы ПК.



Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.



Шаг 3: Выполните инициализацию и перезагрузку коммутаторов.

Шаг 4: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTY и включите запрос пароля при подключении.

d. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

e. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

f. Отключите все порты коммутатора.

g. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Базовые настройки для коммутатора S1_Sidorov, для других коммутаторов параметры идентичны за исключением hostname S2 и S3 для второго и третьего коммутатора соответственно.

```
Switch(config)#hostname S1_Sidorov
S1_Sidorov(config)#no ip domain-lookup
S1_Sidorov(config)#line console 0
S1_Sidorov(config-line)#password cisco
S1_Sidorov(config-line)#login
S1_Sidorov(config-line)#exit
S1_Sidorov(config)#line vty 0 15
S1_Sidorov(config-line)#password cisco
S1_Sidorov(config-line)#login
S1_Sidorov(config-line)#exit
S1_Sidorov(config)#enable secret class
S1_Sidorov(config)#line console 0
S1_Sidorov(config-line)#logging synchronous
S1_Sidorov(config-line)#exit
S1_Sidorov(config)#interface range f0/1-24, g0/1-2
S1_Sidorov(config-if-range)#shutdown
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Часть 2: Настройка сетей VLAN, native VLAN и транковых каналов

В части 2 рассматриваются создание сетей VLAN, назначения сетям VLAN портов коммутатора, настройка транковых портов и изменение native VLAN для всех коммутаторов.

Примечание. Команды, необходимые для работы по части 2, указаны в Приложении А. Проверьте свои знания и попытайтесь настроить сети VLAN, сеть VLAN с нетегированным трафиком и магистрали, не заглядывая в это приложение.

Шаг 1: Создайте сети VLAN.

Используйте соответствующие команды, чтобы создать сети VLAN 10 и 99 на всех коммутаторах. Присвойте сети VLAN 10 имя **User_ФАМИЛИЯ**, а сети VLAN 99 — имя **Management**.

Создание VLAN для коммутатора S1_Sidorov, для оставшихся коммутаторов аналогично.

```
S1_Sidorov#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1_Sidorov(config)#vlan 10
S1_Sidorov(config-vlan)#name User_Sidorov
S1_Sidorov(config-vlan)#exit
S1_Sidorov(config)#vlan 99
S1_Sidorov(config-vlan)#name Management
S1_Sidorov(config-vlan)#exit
```

Шаг 2: Переведите пользовательские порты в режим доступа и назначьте сети VLAN.

Для интерфейса F0/6 S1_ФАМИЛИЯ и интерфейса F0/18 S3 включите порты, настройте их в качестве портов доступа и назначьте их сети VLAN 10.

```
S1_Sidorov(config)#interface f0/6
S1_Sidorov(config-if)#switchport mode access
S1_Sidorov(config-if)#switchport access vlan 10
S1_Sidorov(config-if)#no shutdown

S1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
```

```
S3(config)#interface f0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 10
S3(config-if)#no shutdown

S3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

S3(config-if)#exit
```

Шаг 3: Настройте транковые порты и назначьте их сети native VLAN 99.

Для портов F0/1 и F0/3 на всех коммутаторах включите порты, настройте их в качестве транковых и назначьте их сети native VLAN 99.

Настройка транковых портов для коммутатора S1_Sidorov, для остальных коммутаторов аналогично.

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
S1_Sidorov(config)#interface range f0/1, f0/3
S1_Sidorov(config-if-range)#switchport mode trunk
S1_Sidorov(config-if-range)#switchport trunk native vlan 99
```

Шаг 4: Настройте административный интерфейс на всех коммутаторах.

Используя таблицу адресации, настройте на всех коммутаторах административный интерфейс с соответствующим IP-адресом.

```
S1_Sidorov(config)#int vlan 99
S1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1_Sidorov(config-if)#ip address 192.168.22.11
% Incomplete command.
S1_Sidorov(config-if)#ip address 192.168.22.11 255.255.255.0
S1_Sidorov(config-if)#no shutdown
```

```
S2(config)#int vlan 99
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S2(config-if)#ip address 192.168.22.12
% Incomplete command.
S2(config-if)#ip address 192.168.22.12 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#exit
```

```
S3(config)#int vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.22.13 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
```

Шаг 5: Проверка конфигураций и возможности подключения.

Используйте команду **show vlan brief** на всех коммутаторах, чтобы убедиться в том, что все сети VLAN внесены в таблицу VLAN и назначены правильные порты.

```
S1_Sidorov#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   User_Sidorov                     active    Fa0/6
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   User_Sidorov                     active
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

```
S3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   User_Sidorov                     active    Fa0/18
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Используйте команду **show interfaces trunk** на всех коммутаторах для проверки магистральных интерфейсов.

```
S1_Sidorov#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/3       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99
Fa0/3       1,10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99
Fa0/3       none
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
S2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/3       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99
Fa0/3       1,10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99
Fa0/3       1,10,99

S3#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/3       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99
Fa0/3       1,10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99
Fa0/3       1,10,99
```

Используйте команду **show running-config** на всех коммутаторах, чтобы проверить все остальные конфигурации.

```
hostname S1_Sidorov
!
enable secret 5 $1$mERr$9cTjUIEqN
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
```

Какие настройки используются для режима протокола spanning-tree на коммутаторах Cisco?

_____

Проверьте подключение между компьютерами PC-A и PC-C. Удалось ли получить ответ на эхо-запрос?

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time=1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Часть 3: Настройка корневого моста и проверка сходимости PVST+

В части 3 вам предстоит определить корневой мост по умолчанию в сети, назначить основной и вспомогательный корневые мосты и использовать команду **debug** для проверки сходимости PVST+.

Шаг 1: Определите текущий корневой мост.

С помощью какой команды пользователи определяют состояние протокола spanning-tree коммутатора Cisco Catalyst для всех сетей VLAN? Запишите команду в строке ниже.

_____

Выполните команду на всех трех коммутаторах, чтобы ответить на следующие вопросы:

Примечание. На каждом коммутаторе доступно три экземпляра протокола spanning-tree. По умолчанию на коммутаторах Cisco используется конфигурация STP PVST+, которая позволяет создавать отдельный экземпляр протокола spanning-tree для каждой сети VLAN (VLAN 1 и все остальные настроенные пользователем сети VLAN).

Каков приоритет моста коммутатора S1_ФАМИЛИЯ для

сети VLAN 1?

Каков приоритет моста коммутатора S2 для сети VLAN 1?

Каков приоритет моста коммутатора S3 для сети VLAN 1?

Какой коммутатор является корневым мостом?

Почему этот коммутатор выбран в качестве корневого моста?

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
S1_Sidorov#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.9681.6097
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0060.2FAC.860A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/3            Altn BLK 19        128.3    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0001.9681.6097
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0060.2FAC.860A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/6            Desg FWD 19        128.6    P2p

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0001.9681.6097
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32867  (priority 32768 sys-id-ext 99)
             Address     0060.2FAC.860A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/3            Altn BLK 19        128.3    P2p
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
S2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.9681.6097
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0001.9681.6097
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0001.9681.6097
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0001.9681.6097
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0001.9681.6097
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32867  (priority 32768 sys-id-ext 99)
             Address     0001.9681.6097
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
S3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.9681.6097
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0030.F258.E37E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0001.9681.6097
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0030.F258.E37E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/18           Desg FWD 19        128.18   P2p

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    32867
             Address     0001.9681.6097
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32867  (priority 32768 sys-id-ext 99)
             Address     0030.F258.E37E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Шаг 2: Настройте основной и вспомогательный корневые мосты для всех существующих сетей VLAN.

При выборе корневого моста (коммутатора) по MAC-адресу может образоваться условно оптимальная конфигурация. В этой лабораторной работе вам необходимо настроить коммутатор S2 в качестве корневого моста и коммутатор S1_ФАМИЛИЯ — в качестве вспомогательного корневого моста.

a. Настройте коммутатор S2 в качестве основного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже.

spanning-tree vlan 1,10,99 root primary

```
S2(config)#spanning-
S2(config)#spanning-tree vlan 1,10,99 root primary
```

b. Настройте коммутатор S1_ФАМИЛИЯ в качестве вспомогательного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже.

```
S1_Sidorov(config)#span
S1_Sidorov(config)#spanning-tree vlan 1,10,99 root secondary
```

Используйте команду **show spanning-tree** для ответа на следующие вопросы:

Какой приоритет моста используется для коммутатора S1_ФАМИЛИЯ в сети

VLAN 1?

Какой приоритет моста используется для коммутатора S2 в сети VLAN 1?

Какой интерфейс в сети находится в состоянии блокировки? (Fa0/3 коммутатора S3)

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
S1_Sidorov#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0001.9681.6097
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28673  (priority 28672 sys-id-ext 1)
             Address     0060.2FAC.860A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0001.9681.6097
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28682  (priority 28672 sys-id-ext 10)
             Address     0060.2FAC.860A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/6            Desg FWD 19        128.6    P2p

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    24675
             Address     0001.9681.6097
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28771  (priority 28672 sys-id-ext 99)
             Address     0060.2FAC.860A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
S2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0001.9681.6097
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     0001.9681.6097
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0001.9681.6097
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     0001.9681.6097
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p

VLAN0099
  Spanning tree enabled protocol ieee
  Root ID    Priority    24675
             Address     0001.9681.6097
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24675  (priority 24576 sys-id-ext 99)
             Address     0001.9681.6097
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Шаг 3: Измените топологию 2-го уровня и проверьте сходимость.

Чтобы проверить сходимость PVST+, необходимо создать изменение топологии 2-го уровня, используя команду **debug** для отслеживания событий протокола spanning-tree.

a. Выполните команду **debug spanning-tree events** в привилегированном режиме на коммутаторе S3.

```
S3#debug ?
  ip       IP information
  sw-vlan  vlan manager
```

Примечание. Прежде чем продолжить, исходя из выходных данных команды **debug** убедитесь, что все сети VLAN на интерфейсе F0/3 перешли в состояние пересылки, после чего используйте команду **no debug spanning-tree events**, чтобы остановить вывод данных командой **debug**.

Через какие состояния портов проходит каждая сеть VLAN на интерфейсе F0/3 в процессе схождения сети?

Listenenig, learning и forwarding

Используя временную метку из первого и последнего сообщений отладки STP, рассчитайте время (округляя до секунды), которое потребовалось для схождения сети. **Рекомендация**. Формат временной метки сообщений отладки: чч.мм.сс.мс

Время, которое потребовалось для схождения сети: ~30с.

Часть 4: Настройка Rapid PVST+, PortFast, BPDU Guard и проверка сходимости

В части 4 вам предстоит настроить Rapid PVST+ на всех коммутаторах. Вам необходимо будет настроить функции PortFast и BPDU guard на всех портах доступа, а затем использовать команду **debug** для проверки сходимости Rapid PVST+.

Шаг 1: Настройте Rapid PVST+.

a. Настройте S1 для использования Rapid PVST+. Запишите команду в строке ниже.

```
S1_Sidorov(config)#spanning-tree mode rapid
S1_Sidorov(config)#spanning-tree mode rapid-pvst
```

b. Настройте коммутаторы S2 и S3 для Rapid PVST+.

```
S2(config)#spanning-tree mode rapid-pvst
S3(config)#spanning-tree mode rapid-pvst
```

c. Проверьте конфигурации с помощью команды **show running-config | include spanning-tree mode**.

```
S1_Sidorov#show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

```
S2#show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

```
S3#show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Шаг 2: Настройте PortFast и BPDU Guard на портах доступа.

PortFast является функцией протокола spanning-tree, которая переводит порт в состояние пересылки сразу после его включения. Эту функцию рекомендуется использовать при подключении узлов, чтобы они могли начать обмен данными по сети VLAN немедленно, не дожидаясь протокола spanning-tree. Чтобы запретить портам, настроенным с использованием PortFast, пересылать кадры BPDU, которые могут изменить топологию протокола spanning-tree, можно включить функцию BPDU guard. После получения BPDU функция BPDU Guard отключает порт, настроенный с помощью функции PortFast.

a. Настройте F0/6 на S1_ФАМИЛИЯ с помощью функции PortFast. Запишите команду в строке ниже.

b. Настройте F0/6 на S1_ФАМИЛИЯ с помощью функции BPDU Guard. Запишите команду в строке ниже.

```
S1_Sidorov(config)#int fa0/6
S1_Sidorov(config-if)#spann
S1_Sidorov(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
S1_Sidorov(config-if)#spanning-tree bpduguard enable
S1_Sidorov(config-if)#exit
```

c. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции PortFast. Запишите команду в строке ниже.

d. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции BPDU. Запишите команду в строке ниже.

```
S3(config)#spanning-tree portfast default
S3(config)#spanning-tree portfast bpduguard default
```

Шаг 3: Проверьте сходимость Rapid PVST+.

a. Выполните команду **debug spanning-tree events** в привилегированном режиме на коммутаторе S3.

b. Измените топологию, отключив интерфейс F0/1 на коммутаторе S3.

Используя временную метку из первого и последнего сообщений отладки RSTP, рассчитайте время, которое потребовалось для схождения сети.

Время потребовавшееся для схождения сети ~1с

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Вопросы для защиты теоретической части (глава 12)

1. Опишите преимущества беспроводной связи. Кратко охарактеризуйте основные типы беспроводной связи.

2. В каких случаях используются технологии Bluetooth и спутниковая широкополосная связь? Для чего была разработана технология MIMO?

3. Какие роли может выполнять домашний беспроводной маршрутизатор? Для чего нужны беспроводные точки доступа?

4. Назовите и охарактеризуйте категории точек доступа. Перечислите и опишите варианты антенн для беспроводных устройств.

5. Дайте характеристику режимам топологий беспроводной сети. В чем заключается разница между BSS и ESS?

6. Опишите принцип работы беспроводного клиента при использовании метода CSMA/CA. В чем разница между пассивным и активным обнаружением точек доступа?

7. Опишите назначение протокола CAPWAP. Назовите основные рекомендации по установке точек доступа.

8. Опишите основные угрозы при использовании беспроводных точек доступа. Какие бывают типы аутентификации в беспроводной связи?

9. Для чего используется протокол RADIUS? Опишите методы аутентификации домашнего пользователя.

Преимущества беспроводной связи:

Мобильность: Позволяет пользователям подключаться к сети в любом месте, где есть сигнал.

Гибкость: Упрощает процесс развертывания сети и добавления новых устройств.

Удобство: Позволяет избежать проводов и кабелей, что делает сеть более аккуратной и удобной в использовании.

Основные типы беспроводной связи:

Wi-Fi: Стандарт для локальных беспроводных сетей на основе технологий IEEE 802.11.

Bluetooth: Технология для краткодистанционной связи между устройствами.

Спутниковая связь: Использует спутники для передачи данных на большие расстояния.

Использование технологий Bluetooth и спутниковой широкополосной связи:

Bluetooth: Используется для подключения устройств на короткие расстояния, например, между смартфоном и гарнитурой.

Спутниковая широкополосная связь: Применяется в случаях, когда требуется обеспечить связь в удаленных или труднодоступных местах, где отсутствует инфраструктура земных сетей.

Технология MIMO (Multiple Input Multiple Output): Разработана для увеличения пропускной способности и устойчивости беспроводных сетей путем использования нескольких антенн для передачи и приема данных одновременно.

Роли домашнего беспроводного маршрутизатора:

Обеспечение доступа к интернету для домашних устройств.

Создание локальной беспроводной сети для обмена данными между устройствами в домашней сети.

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Беспроводные точки доступа: Необходимы для расширения покрытия сети и увеличения числа подключаемых устройств.

Категории точек доступа:

Домашние (SOHO) точки доступа: Предназначены для использования в домашних и небольших офисных сетях.

Промышленные точки доступа: Обладают более высокой производительностью и надежностью для использования в предприятиях и крупных организациях.

Варианты антенн:

Омни-антенны: Обеспечивают равномерное распределение сигнала во всех направлениях.

Направленные антенны: Направлены на конкретное направление для увеличения дальности и скорости передачи данных.

Характеристика режимов топологий беспроводной сети:

BSS (Basic Service Set): Одна базовая станция и все подключенные к ней клиенты.

ESS (Extended Service Set): Несколько базовых станций, объединенных в одну беспроводную сеть.

Принцип работы беспроводного клиента с использованием CSMA/CA:

Клиент прослушивает канал на предмет активности.

Если канал свободен, клиент передает данные.

Если канал занят, клиент ждет случайное время и повторяет попытку передачи.

Разница между пассивным и активным обнаружением точек доступа:

Пассивное обнаружение: Клиенты прослушивают канал на предмет наличия сигналов от точек доступа.

Активное обнаружение: Клиенты отправляют запросы на поиск точек доступа и ожидают ответов.

Назначение протокола CAPWAP (Control and Provisioning of Wireless Access Points):

Используется для управления и настройки беспроводными точками доступа.

Обеспечивает передачу данных между контроллером и точками доступа.

Основные рекомендации по установке точек доступа:

Размещение точек доступа таким образом, чтобы обеспечить равномерное покрытие всей области.

Избегать помех от других беспроводных устройств и стен.

Основные угрозы при использовании беспроводных точек доступа:

Неавторизованный доступ: Злоумышленники могут попытаться получить доступ к сети.

Перехват данных: Возможность перехвата и подмены передаваемых данных.

Типы аутентификации в беспроводной связи:

WPA/WPA2-PSK: Предварительно распределенный ключ для аутентификации устройств.

802.1X/EAP: Используется централизованный сервер аутент

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Протокол RADIUS (Remote Authentication Dial-In User Service):

Протокол RADIUS используется для централизованной аутентификации, авторизации и учета (AAA) пользователей, обычно в сетях доступа. Он позволяет централизованно управлять доступом пользователей к сети, обеспечивая безопасность и удобство учета использования ресурсов сети. Основное применение протокола RADIUS - это обеспечение безопасного доступа к сети для удаленных пользователей, использующих услуги, такие как VPN (Virtual Private Network), дисковые службы и т. д.

Методы аутентификации домашнего пользователя:

PSK (Pre-Shared Key):

PSK используется для предварительно согласованной аутентификации, где устройства и точки доступа предварительно договариваются о секретном ключе (пароле), который используется для аутентификации. Этот метод прост в установке, но менее безопасен по сравнению с другими методами аутентификации.

802.1X (EAP - Extensible Authentication Protocol):

Этот метод использует протокол 802.1X для аутентификации пользователей на сети. Он требует сервера аутентификации (например, RADIUS), который взаимодействует с клиентом через аутентификационный сервер. После установки связи точка доступа запрашивает у пользователя учетные данные, а затем отправляет их на сервер аутентификации для проверки.

MAC-адрес (MAC Address Filtering):

Этот метод базируется на фильтрации MAC-адресов устройств. Точка доступа разрешает доступ только устройствам, чьи MAC-адреса находятся в списке разрешенных. Это предоставляет дополнительный уровень безопасности, но может быть неэффективным в среде, где могут происходить поддельные атаки на MAC-адреса.

Captive Portal (Захватывающий портал):

Этот метод требует от пользователей прохождения аутентификации через специальную веб-страницу (портал), прежде чем они получат доступ к сети. Пользователям могут предложить ввести учетные данные или пройти другие формы аутентификации, такие как SMS-коды или социальная аутентификация.

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Настройка базовых параметров маршрутизатора с помощью интерфейса командной строки (CLI) системы Cisco IOS

Топология

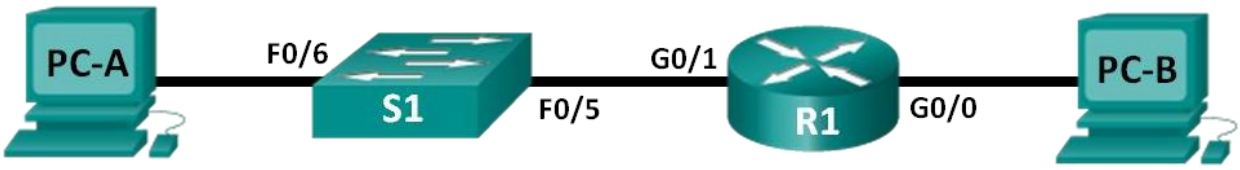


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1_Sidorov	G0/0	192.168.0.1	255.255.255.0	—
	G0/1	192.168.1.1	255.255.255.0	—
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Задачи

Часть 1. Настройка топологии и инициализация устройств

- Подключите кабели к оборудованию в соответствии с топологией сети.
- Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Часть 2. Настройка устройств и проверка подключения

- Настройте статическую информацию IPv4 на интерфейсах ПК.
- Настройте базовые параметры маршрутизатора.
- Проверьте подключение к сети.
- Настройте на маршрутизаторе протокол SSH.

Часть 3. Отображение сведений о маршрутизаторе

- Загрузите из маршрутизатора данные об аппаратном и программном обеспечении.
- Интерпретируйте выходные данные загрузочной конфигурации.
- Интерпретируйте выходные данные таблицы маршрутизации.
- Проверьте состояние интерфейсов.

Часть 4. Конфигурация протокола IPv6 и проверка подключения

Необходимые ресурсы

- 1 маршрутизатор Cisco
- 1 коммутатор Cisco

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

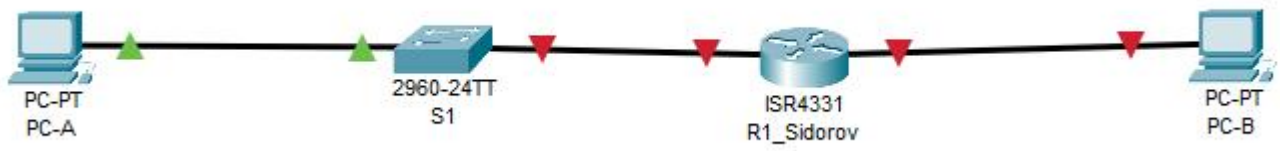
- 2 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала Tera Term или Putty)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты.
- Кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка топологии и инициализация устройств

Шаг 1: Создайте сеть согласно топологии.

a. Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

b. Включите все устройства в топологии.

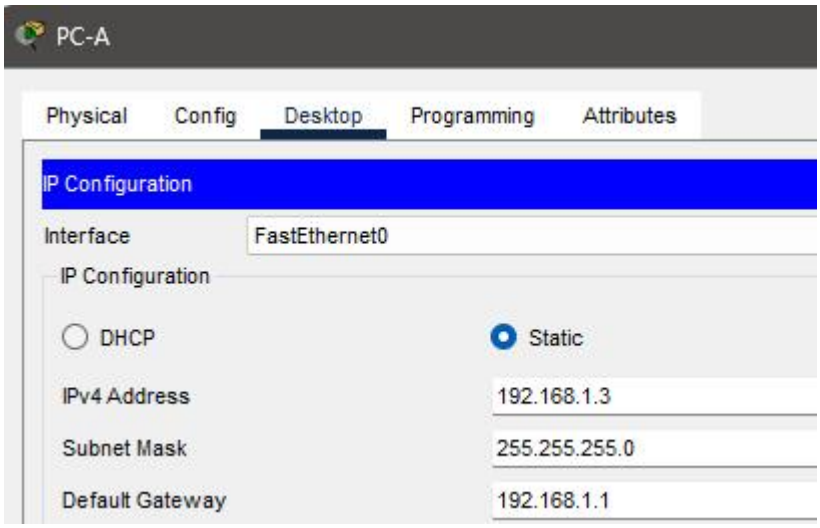


Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Часть 2: Настройка устройств и проверка подключения

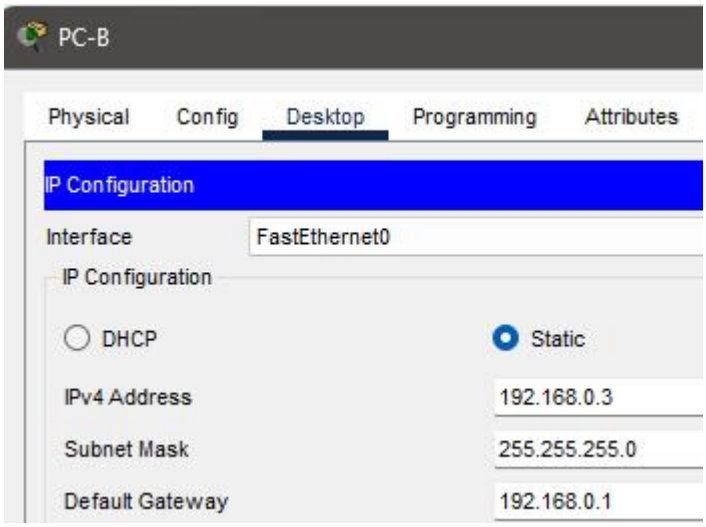
Шаг 1: Настройте интерфейсы ПК.

a. Настройте на компьютере PC-A IP-адрес, маску подсети и параметры основного шлюза.



b. Настройте на компьютере PC-B IP-адрес, маску подсети и параметры основного шлюза.

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.



Шаг 2: Настройте маршрутизатор.

a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.

b. Войдите в режим глобальной конфигурации маршрутизатора.

c. Назначьте маршрутизатору имя устройства **R1_ ФАМИЛИЯ**. Укажите свою фамилию на английском языке.

d. Введите команду для того, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

e. Установите минимальную длину 10 символов для всех паролей.

   Укажите способы усиления защиты паролей, кроме установки минимальной длины.

f. Назначьте **cisco12345** в качестве зашифрованного пароля привилегированного режима.

g. В качестве пароля консоли назначьте **ciscoconpass**. Установите лимит времени для консольного подключения (5 минут), активируйте вход в систему (запрашивание пароля) и добавьте команду **logging synchronous**. Команда **logging synchronous** позволяет синхронизировать выходные данные отладки и программного обеспечения Cisco IOS, а также запрещает этим сообщениям прерывать ввод команд с клавиатуры.

h. В качестве пароля линий vty назначьте **ciscovtypass**, установите лимит времени для удаленного подключения (5 минут), активируйте вход в систему (запрашивание пароля) и добавьте команду **logging synchronous**.

i. Зашифруйте открытые пароли.

j. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1_Sidorov
R1_Sidorov(config)#no ip domain-lookup
R1_Sidorov(config)#security passwords min-length 10
R1_Sidorov(config)#enable secret cisco12345
R1_Sidorov(config)#line con 0
R1_Sidorov(config-line)#password ciscoconpass
R1_Sidorov(config-line)#exec-timeout 5 0
R1_Sidorov(config-line)#login
R1_Sidorov(config-line)#logging synchronous
R1_Sidorov(config-line)#exit
R1_Sidorov(config)#line vty 0 15
R1_Sidorov(config-line)#password ciscovtypass
R1_Sidorov(config-line)#exec-timeout 5 0
R1_Sidorov(config-line)#login
R1_Sidorov(config-line)#logging synchronous
R1_Sidorov(config-line)#exit
R1_Sidorov(config)#service password-encryption
R1_Sidorov(config)#banner motd #Unauthroized access banned#
```

k. Настройте IP-адрес и описание интерфейса. Активируйте оба интерфейса на маршрутизаторе.

```
R1_Sidorov(config)#int g0/0/0
R1_Sidorov(config-if)#description Connection to PCB
R1_Sidorov(config-if)#ip address 192.168.0.1 255.255.255.0
R1_Sidorov(config-if)#no shutdown

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

R1_Sidorov(config-if)#int g0/0/1
R1_Sidorov(config-if)#description connection to s1
R1_Sidorov(config-if)#ip address 192.168.1.1 255.255.255.0
R1_Sidorov(config-if)#no shutdown

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1_Sidorov(config-if)#exit
```

l. Настройте часы на маршрутизаторе.

m. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Что произойдет, если перезагрузить маршрутизатор до того, как будет выполнена команда **copy running-config startup-config**?

```
R1_Sidorov#clock set 12:00:00 24 march 2024
R1_Sidorov#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1_Sidorov#
```

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

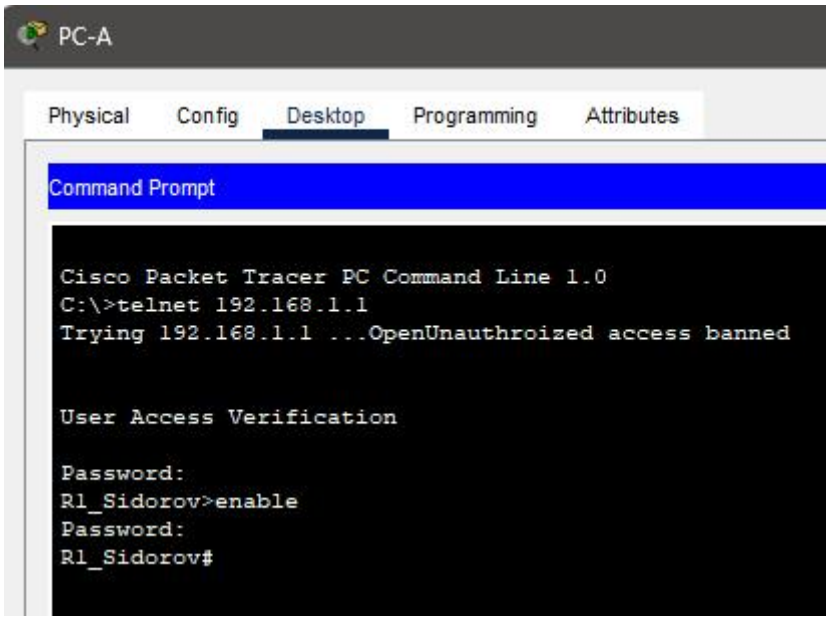
Шаг 3: Проверьте подключение к сети.

a. Из командной строки компьютера PC-B отправьте эхо-запрос на компьютер PC-A.

Примечание. Может потребоваться отключение межсетевого экрана на компьютерах.

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

b. Подключитесь к маршрутизатору R1_ФАМИЛИЯ от компьютера PC-A с помощью службы Telnet.



Шаг 4: Настройте маршрутизатор для доступа по протоколу SSH.

a. Активируйте подключения SSH и создайте пользователя (username - ваша фамилия на английском языке, доменное имя маршрутизатора - CCNA-lab.com) в локальной базе данных маршрутизатора. Длина ключа шифрования - 1024 бит. Не забудьте записать пароль, чтобы не забыть его при повторном подключении.

```
R1_Sidorov#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1_Sidorov(config)#ip domain-name CCNA-lab.com
R1_Sidorov(config)#username sidorov
R1_Sidorov(config)#username sidorov privilege 15 secret 1
% Password too short - must be at least 10 characters. Password not configured.
R1_Sidorov(config)#username sidorov privilege 15 secret sidorov
% Password too short - must be at least 10 characters. Password not configured.
R1_Sidorov(config)#username sidorov privilege 15 secret sidorovpass
```

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
R1_Sidorov(config)#line vty 0 15
R1_Sidorov(config-line)#transport input ssh
R1_Sidorov(config-line)#login local
R1_Sidorov(config-line)#exit
R1_Sidorov(config)#crypto key generate rsa
The name for the keys will be: R1_Sidorov.CCNA-lab.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1_Sidorov(config)#
*Mar 24 12:27:1.776: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

b. Подключитесь к маршрутизатору R1_ФАМИЛИЯ от компьютера PC-A по протоколу SSH.

```
C:\>ssh -l sidorov 192.168.1.1

Password:

Unauthroized access banned

R1_Sidorov#
```

Часть 3: Отображение сведений о маршрутизаторе

В третьей части вам предстоит использовать команду **show** в сеансе SSH, чтобы получить информацию из маршрутизатора.

Шаг 1: Установите SSH-подключение к R1_ФАМИЛИЯ.

На компьютере PC-B создайте сеанс SSH с маршрутизатором R1_ФАМИЛИЯ по IP-адресу 192.168.0.1 и войдите в систему, используя имя пользователя (ваша фамилия на английском языке) и пароль, который вы придумали самостоятельно.

```
C:\>ssh -l sidorov 192.168.0.1

Password:

Unauthroized access banned

R1_Sidorov#
```

Шаг 2: Получите основные данные об аппаратном и программном обеспечении.

a. Используйте команду **show version**, чтобы ответить на вопросы о маршрутизаторе.

Как называется образ IOS, под управлением которой работает маршрутизатор?

```
R1_Sidorov#show version
Cisco IOS Software [Everest], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version
16.6.4,RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Sun 08-Jul-18 04:33 by mcpre
```

Какой объем энергонезависимого ОЗУ (NVRAM) имеет маршрутизатор?

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Каким объемом флеш-памяти обладает маршрутизатор?

```
cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
```

b. Зачастую команды **show** могут выводить несколько экранов данных. Фильтрация выходных данных позволяет пользователю отображать лишь нужные разделы выходных данных. Чтобы включить команду фильтрации, после команды **show** введите прямую черту (**|**), после которой следует ввести параметр и выражение фильтрации. Чтобы отобразить все строки выходных данных, которые содержат выражение фильтрации, можно согласовать выходные данные с оператором фильтрации с помощью ключевого слова **include**. Настройте фильтрацию для команды **show version** и используйте команду **show version | include register**, чтобы ответить на следующий вопрос.

Какому процессу загрузки последует маршрутизатор при следующей перезагрузке?

```
R1_Sidorov#show version | include register
Configuration register is 0x2102
```

Возможны различные ответы. В большинстве случаев (0x2102) маршрутизатор последует процессу обычной загрузки, загрузит IOS из флеш-памяти, а загрузочную конфигурацию — из NVRAM (если она содержится). Если регистр конфигурации (config register) равен 0x2142, на маршрутизаторе будет пропущена загрузка конфигурации и будет открыта командная строка пользовательского режима. При сбое начальной загрузки маршрутизатор переходит в режим ROMMON.

Шаг 3: Отобразите загрузочную конфигурацию.

Выведите загрузочную конфигурацию на маршрутизаторе, чтобы ответить на следующие вопросы.

Как пароли представлены в выходных данных?

```
line con 0
 exec-timeout 5 0
 password 7 0822455D0A1606181C1B0D1739
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 5 0
 password 7 0822455D0A1613030B1B0D1739
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 exec-timeout 5 0
 password 7 0822455D0A1613030B1B0D1739
 logging synchronous
 login local
 transport input ssh
```

```
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUU1.
```

```
username sidorov privilege 15 secret 5 $1$mERr$4wtXesyLPKONTUdwTJxUF0
```

Теперь попробуйте ввести эту команду таким образом, чтобы вывод **начинался** с конфигурации

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

линий vty. См. пункт b шага 2.

Что происходит в результате выполнения этой команды?

```
R1_Sidorov#show running-config | begin vty
line vty 0 4
 exec-timeout 5 0
 password 7 0822455D0A1613030B1B0D1739
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 exec-timeout 5 0
 password 7 0822455D0A1613030B1B0D1739
 logging synchronous
 login local
 transport input ssh
!
!
!
end
```

Шаг 4: Отобразите таблицу маршрутизации на маршрутизаторе.

Отобразите таблицу маршрутизации, чтобы ответить на следующие вопросы.

Какой код используется в таблице маршрутизации для обозначения сети с прямым подключением?

Сколько записей маршрутов закодированы с символом «C» в таблице маршрутизации?

```
R1_Sidorov#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.0.1/32 is directly connected, GigabitEthernet0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
```

Шаг 5: Отобразите на маршрутизаторе сводный список интерфейсов.

Отобразите сводный список интерфейсов на маршрутизаторе, чтобы ответить на следующий вопрос.

Какая команда позволяет изменить состояние портов Gigabit Ethernet с DOWN на UP?

```
R1_Sidorov#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.0.1     YES manual up                    up
GigabitEthernet0/0/1   192.168.1.1     YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Часть 4: Настройка протокола IPv6 и проверка подключения

Шаг 1: Назначьте IPv6-адреса интерфейсу G0/0 маршрутизатора R1_ФАМИЛИЯ и включите IPv6-маршрутизацию.

Примечание. Назначение IPv6-адрес в дополнение к IPv4-адресам на интерфейсе называют двойным стеком, поскольку активным является как протокол IPv4, так и протокол IPv6. Благодаря включению IPv6-маршрутизации одноадресной передачи на маршрутизаторе R1_ФАМИЛИЯ компьютер PC-B получает сетевой IPv6-префикс для интерфейса G0/0 маршрутизатора R1_ФАМИЛИЯ и может автоматически настраивать свой IPv6-адрес и шлюз по умолчанию.

a. Назначьте интерфейсу G0/0 глобальный индивидуальный IPv6-адрес - 2001:db8:acad:a::1/64, в дополнение к индивидуальному адресу на интерфейсе назначьте локальный адрес канала (**link-local**) – fe80::1. **Включите** IPv6-маршрутизацию.

```
R1_Sidorov(config)#int g0/0/0
R1_Sidorov(config-if)#ipv6 address 2001:db8:acad:a::1/64
R1_Sidorov(config-if)#ipv6 address FE80::1 link-local
R1_Sidorov(config-if)#no shutdown
R1_Sidorov(config-if)#exit
R1_Sidorov(config)#ipv6 uni
R1_Sidorov(config)#ipv6 unicast-routing
R1_Sidorov(config)#exit
```

Проверьте параметры IPv6 на маршрутизаторе R1_ФАМИЛИЯ.

```
R1_Sidorov#show ipv6 int brief
GigabitEthernet0/0/0       [up/up]
    FE80::1
    2001:DB8:ACAD:A::1
GigabitEthernet0/0/1       [up/up]
    unassigned
GigabitEthernet0/0/2       [administratively down/down]
    unassigned
Vlan1                      [administratively down/down]
    unassigned
```

b. На компьютере PC-B выполните команду для отображения настроек IPv6.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::201:42FF:FE0E:3C20
   IPv6 Address....................: 2001:DB8:ACAD:A:201:42FF:FE0E:3C20
   IPv4 Address....................: 192.168.1.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: FE80::1
                                     192.168.0.1
```

Какой IPv6-адрес назначен компьютеру PC-B?

Какой шлюз по умолчанию назначен компьютеру PC-B? _____

От компьютера PC-B отправьте эхо-запрос на локальный адрес канала шлюза по умолчанию маршрутизатора R1_ФАМИЛИЯ. Была ли проверка успешной? _____

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
C:\>ping FE80::1

Pinging FE80::1 with 32 bytes of data:

Reply from FE80::1: bytes=32 time<1ms TTL=255
Reply from FE80::1: bytes=32 time<1ms TTL=255
Reply from FE80::1: bytes=32 time<1ms TTL=255
Reply from FE80::1: bytes=32 time<1ms TTL=255

Ping statistics for FE80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

От компьютера PC-B отправьте эхо-запрос на индивидуальный IPv6-адрес маршрутизатора R1_ФАМИЛИЯ 2001:db8:acad:a::1. Была ли проверка успешной? _____

```
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Вопросы для защиты теоретической части (глава 14)

1. Дайте определение понятию “маршрутизация”. Какими способами маршрутизатор получает сведения об удаленных сетях?

2. Что означает понятие “поиск наилучшего совпадения” относительно маршрутизатора? Для чего служат статические маршруты?

3. Опишите процесс пересылки пакетов маршрутизатором. Что произойдет, если в таблице маршрутизации нет соответствия между IP-адресом назначения и префиксом?

4. Дайте характеристику механизмам пересылки пакетов. Опишите все возможные источники получения маршрутов в таблице маршрутизации.

5. В каких случаях целесообразно настроить статический маршрут? Дайте определение понятию “административное расстояние”.

6. В каких случаях целесообразно настроить динамическую маршрутизацию? Дайте определение понятию “метрика маршрута”.

7. Проведите краткую сравнительную характеристику статической и динамической маршрутизации на основе нескольких критериев. Какие бывают протоколы динамической маршрутизации (опишите категории и приведите примеры)?

8. Для чего нужны протоколы динамической маршрутизации? Какие компоненты включают в себя протоколы динамической маршрутизации?

9. Как вычисляется метрика для протоколов RIP, OSPF и EIGRP? Как работает распределение нагрузки при использовании динамической маршрутизации?

10. Опишите назначение кодов C, L и S в таблице маршрутизации. В каких случаях используется протокол BGP?

Что такое маршрутизация и как маршрутизатор получает информацию о удалённых сетях?

Маршрутизация - это процесс направления сетевых пакетов от отправителя к получателю в сети компьютеров. Маршрутизаторы получают информацию о удалённых сетях двумя основными способами: статическая маршрутизация (вручную настраиваемые маршруты) и динамическая маршрутизация (использование протоколов маршрутизации для автоматического обновления таблиц маршрутизации).

Что такое поиск наилучшего совпадения и зачем нужны статические маршруты?

Поиск наилучшего совпадения - это процесс выбора наилучшего маршрута для доставки пакета на основе IP-адреса назначения. Статические маршруты используются для задания постоянных маршрутов к определённым сетям, обычно используемым в случаях, когда путь до сети известен и не меняется часто.

Как происходит пересылка пакетов маршрутизатором и что случится, если нет соответствия в таблице маршрутизации?

Маршрутизатор выбирает маршрут из своей таблицы маршрутизации и отправляет пакет в соответствии с выбранным маршрутом. Если нет соответствия в таблице маршрутизации, маршрутизатор не сможет определить путь для доставки пакета и, вероятно, отбросит его или отправит на узел по умолчанию.

Каковы механизмы пересылки пакетов и откуда маршрутизатор получает маршруты?

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Механизмы пересылки пакетов включают в себя коммутацию (как например, пересылка пакетов на основе MAC-адресов в локальной сети) и маршрутизацию (пересылка пакетов на основе IP-адресов в сети). Маршруты могут быть получены как статически (вручную заданные администратором), так и динамически (автоматически обновляемые с помощью протоколов маршрутизации).

Когда целесообразно использовать статический маршрут и что такое административное расстояние?

Статический маршрут целесообразен, когда путь до сети известен заранее и не меняется часто. Административное расстояние - это метрика, используемая для определения приоритета выбора маршрута: чем меньше административное расстояние, тем выше приоритет маршрута.

Когда целесообразно использовать динамическую маршрутизацию и что такое метрика маршрута?

Динамическая маршрутизация целесообразна в сетях, где топология часто меняется или когда требуется автоматическое обновление маршрутов. Метрика маршрута - это числовое значение, используемое для оценки качества маршрута, чем меньше метрика, тем лучше маршрут.

Сравнение статической и динамической маршрутизации и примеры протоколов динамической маршрутизации.

Статическая маршрутизация требует ручной настройки маршрутов, в то время как динамическая маршрутизация позволяет автоматически обновлять маршруты. Протоколы динамической маршрутизации включают RIP, OSPF, EIGRP, BGP и др.

Назначение протоколов динамической маршрутизации и их компоненты.

Протоколы динамической маршрутизации используются для автоматического обновления таблиц маршрутизации. Они включают в себя алгоритмы выбора маршрута и механизмы обмена информацией о маршрутах между маршрутизаторами.

Как вычисляются метрики для протоколов RIP, OSPF и EIGRP и как работает распределение нагрузки при динамической маршрутизации?

В протоколе RIP метрика основана на числе прыжков до сети, в OSPF - на стоимости пути, а в EIGRP - на комбинации различных параметров. Распределение нагрузки при динамической маршрутизации обычно осуществляется с помощью балансировки нагрузки между нескольким

© Корпорация Cisco и/или ее дочерние компании, 2022. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Настройка статических маршрутов и маршрутов IPv4 и IPv6 по умолчанию

Топология

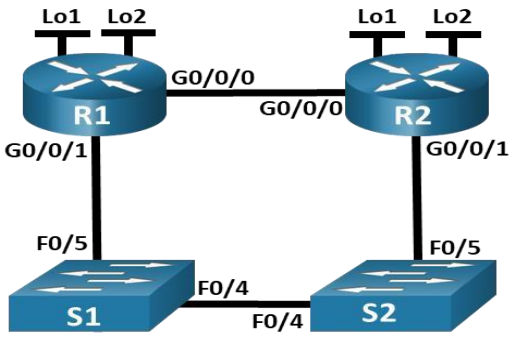


Таблица адресации

Устройство	Интерфейс	IP адрес/префикс
R1_ФАМИЛИЯ	G0/0/0	172.16.X+1.1 /24
		2001:db8:acad:2::1/64
R1_ФАМИЛИЯ		fe80::1
	G0/0/1	192.168.1.1 /24
		2001:db8:acad:1::1 /64
		fe80::1
	Loopback1	10.1.0.1 /24
		2001:db8:acad:10::1 /64
		fe80::1
	Loopback2	209.165.200.225 /27
		2001:db8:acad:209::1 /64
		fe80::1
R2	G0/0/0	172.16.X+1.2 /24
		2001:db8:acad:2::2 /64

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Устройство	Интерфейс	IP адрес/префикс
		fe80::2
	G0/0/1	192.168.1.2 /24
		2001:db8:acad:1::2 /64
		fe80::2
	Loopback1	10.2.0.1 /24
		2001:db8:acad:11::2 /64
		fe80::2
	Loopback2	209.165.200.193 /27
		2001:db8:acad:210::1 /64
		fe80::2

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Настройка и проверка IP-адресации и IPv6 на R1_ФАМИЛИЯ и R2

Часть 3. Настройка и проверка статической маршрутизации и маршрутизации по умолчанию для IPv4 на R1_ФАМИЛИЯ и R2

Часть 4. Настройка и проверка статической маршрутизации и маршрутизации по умолчанию для IPv6 на R1_ФАМИЛИЯ и R2

Необходимые ресурсы

- 2 маршрутизатора (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.4 или аналогичным)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.2(2) (образ lanbasek9) или аналогичная модель)
- 1 ПК (под управлением Windows с программой эмуляции терминала, например, Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты.
- Кабели Ethernet, расположенные в соответствии с топологией

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

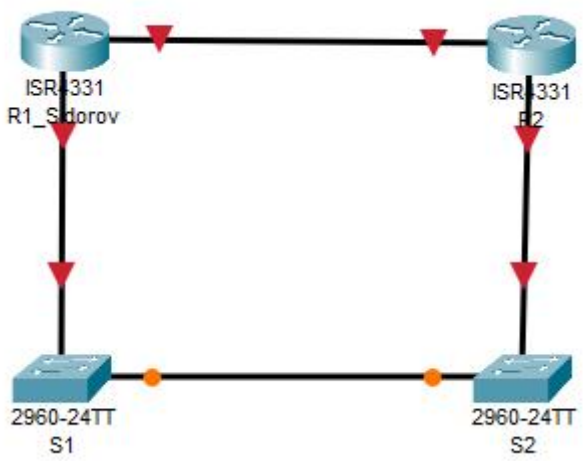
Инструкции

Часть 1. Создание сети и настройка основных параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовые параметры для узлов ПК и коммутаторов.

Шаг 1. Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.



Шаг 2. Произведите базовую настройку маршрутизаторов.

a. Назначьте маршрутизатору имя устройства.
b. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
c. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
d. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
e. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
f. Зашифруйте открытые пароли.
g. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
h. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

```
Router(config)#hostname R1_Sidorov
R1_Sidorov(config)#no ip domain-lookup
R1_Sidorov(config)#enable secret class
R1_Sidorov(config)#line console 0
R1_Sidorov(config-line)#password cisco
R1_Sidorov(config-line)#login
R1_Sidorov(config-line)#exit
R1_Sidorov(config)#line vty 0 4
R1_Sidorov(config-line)#password cisco
R1_Sidorov(config-line)#login
R1_Sidorov(config-line)#exit
R1_Sidorov(config)#service password encryption
                                   ^
% Invalid input detected at '^' marker.

R1_Sidorov(config)#service password-encryption
R1_Sidorov(config)#banner motd #Authorized access only#
R1_Sidorov(config)#exit
R1_Sidorov#
%SYS-5-CONFIG_I: Configured from console by console
copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
Router(config)#hostname R2
R2(config)#no ip domain lookup
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd #authorized access only#
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Шаг 3. Настройте базовые параметры каждого коммутатора.

a. Присвойте коммутатору имя устройства.

b. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

c. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

d. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.

e. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.

f. Зашифруйте открытые пароли.

g. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

h. Выключите все интерфейсы, которые не будут использоваться.

i. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

```
Switch(config)#hostname S1
S1(config)#no ip domain lookup
S1(config)#enable secret class
S1(config)#line console -0
                        ^
% Invalid input detected at '^' marker.

S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #Authorized access only#
S1(config)#interface range f0/1-3, f0/6-24, g0/1-2
S1(config-if-range)#shutdown
```

```
Switch(config)#hostname S2
S2(config)#no ip domain lookup
S2(config)#enable secret class
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd #Authorized access only#
S2(config)#interface range f0/1-3, f0/6-24, g0/1-2
S2(config-if-range)#shutdown
```

Вывод команды **show cdp neighbors** в этот момент на R1_ФАМИЛИЯ или R2 приводит к пустому списку. Дайте пояснение.

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

Часть 2. Настройка и проверка адресации IPv4 и IPv6 на R1_ФАМИЛИЯ и R2

В части 2 необходимо настроить и проверить адреса IPv4 и IPv6 на R1_ФАМИЛИЯ и R2. Для получения информации, необходимой для выполнения этой части, используйте приведенную выше таблицу.

Шаг 1. Настройте IP-адреса для обоих маршрутизаторов.

a. Включите одноадресную маршрутизацию IPv6.

```
R1_Sidorov(config)#ipv6 unicast-routing

R2(config)#ipv6 unicast-routing
```

b. Настройте IP-адрес в соответствии с таблицей адресации.

R1_Sidorov

```
R1_Sidorov(config)#interface g0/0/0
R1_Sidorov(config-if)#iip address 172.16.22.1 255.255.255.0
                      ^
% Invalid input detected at '^' marker.

R1_Sidorov(config-if)#ip address 172.16.22.1 255.255.255.0
R1_Sidorov(config-if)#ipv6 address fe80::1 link-local
R1_Sidorov(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1_Sidorov(config-if)#no shutdown

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
```

```
R1_Sidorov(config)#interface g0/0/1
R1_Sidorov(config-if)#ip address 192.168.1.1 255.255.255.0
R1_Sidorov(config-if)#ipv6 address fe80::1 link-local
R1_Sidorov(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1_Sidorov(config-if)#no shutdown

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
```

```
R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
ip address 10.1.0.1 255.255.255.0
R1_Sidorov(config-if)#ipv6 address fe80::1 link-local
R1_Sidorov(config-if)#ipv6 address 2001:db8:acad:10::1/64
R1_Sidorov(config-if)#no shutdown
R1_Sidorov(config-if)#exit
R1_Sidorov(config)#
```

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

```
R1_Sidorov(config)#interface lo2

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface Loopback2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, chang
ip address 209.165.200.225 255.255.255.224
R1_Sidorov(config-if)#ip address 209.165.200.225 255.255.255.224
R1_Sidorov(config-if)#ipv6 address fe80::1 link-local
R1_Sidorov(config-if)#ipv6 address 2001:db8:acad:209::1/64
R1_Sidorov(config-if)#no shutdown
R1 Sidorov(config-if)#
```

R2

```
R2(config)#interface g0/0/0
R2(config-if)#ip address 172.16.22.2 255.255.255.0
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
```

```
R2(config)#interface g0/0/1
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#ipv6 address 2001:db8:acad:1::2/64
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
```

```
R2(config)#interface lo1

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,

R2(config-if)#ip address 10.2.0.1 255.255.255.0
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#ipv6 address 2001:db8:acad:11::2/64
R2(config-if)#no shutdown
```

```
R2(config)#interface lo2

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2,

R2(config-if)#ip address 209.165.200.193 255.255.255.224
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#ipv6 address 2001:db8:acad:210::1/64
R2(config-if)#no shutdown
R2(config-if)#exit
```

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Шаг 2. Проверьте правильность IP-адресов.

a. Выполните команду, чтобы проверить назначения IPv4 интерфейсам.

```
R1_Sidorov#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   172.16.22.1     YES manual up                    up
GigabitEthernet0/0/1   192.168.1.1     YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Loopback1              10.1.0.1        YES manual up                    up
Loopback2              209.165.200.225 YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   172.16.22.2     YES manual up                    up
GigabitEthernet0/0/1   192.168.1.2     YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Loopback1              10.2.0.1        YES manual up                    up
Loopback2              209.165.200.193 YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

b. Выполните команду, чтобы проверить назначения IPv6 интерфейсам.

```
R1_Sidorov#show ipv6 interface brief
GigabitEthernet0/0/0       [up/up]
    FE80::1
    2001:DB8:ACAD:2::1
GigabitEthernet0/0/1       [up/up]
    FE80::1
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/2       [administ:
    unassigned
Loopback1                  [up/up]
    FE80::1
    2001:DB8:ACAD:10::1
Loopback2                  [up/up]
    FE80::1
    2001:DB8:ACAD:209::1
Vlan1                      [administ:
    unassigned
```

```
R2#show ipv6 interface brief
GigabitEthernet0/0/0       [up/up]
    FE80::2
    2001:DB8:ACAD:2::2
GigabitEthernet0/0/1       [up/up]
    FE80::2
    2001:DB8:ACAD:1::2
GigabitEthernet0/0/2       [administr
    unassigned
Loopback1                  [up/up]
    FE80::2
    2001:DB8:ACAD:11::2
Loopback2                  [up/up]
    FE80::2
    2001:DB8:ACAD:210::1
Vlan1                      [administr
    unassigned
```

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

Часть 3. Настройка и проверка статической маршрутизации и маршрутизации по умолчанию для IPv4 на R1_ФАМИЛИЯ и R2

В части 3 настраивается статическая и стандартная маршрутизация на R1_ФАМИЛИЯ и R2, чтобы обеспечить полное подключение между маршрутизаторами с использованием IPv4. Опять же, статическая маршрутизация, используемая здесь, предназначена не для представления наилучшей практики, а для оценки способности завершить необходимые конфигурации.

Шаг 1. На R1_ФАМИЛИЯ настройте статический маршрут к сети Loopback1 R2, используя адрес G0/0/1 R2 в качестве следующего перехода.

a. Используйте команду **ping**, чтобы убедиться, что интерфейс G0/0/1 R2 доступен.

```
R1_Sidorov#ping
Protocol [ip]:
Target IP address: 192.168.1.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

b. Настройте статический маршрут для сети Loopback1 R2 через адрес G0/0/1 R2.

```
R1_Sidorov(config)#ip route 10.2.0.0 255.255.255.0 192.168.1.2
```

Шаг 2. На R1_ФАМИЛИЯ настройте статический маршрут по умолчанию через адрес G0/0/0 R2.

a. Используйте команду **ping** , чтобы убедиться, что интерфейс G0/0/0 R2 доступен.

```
R1_Sidorov#ping
Protocol [ip]:
Target IP address: 172.16.22.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.22.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

b. Настройте статический маршрут по умолчанию через адрес G0/0/0 R2.

```
R1_Sidorov(config)#ip route 0.0.0.0 0.0.0.0 172.16.22.2
```

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Шаг 3. На R1_ФАМИЛИЯ настройте плавающий статический маршрут по умолчанию через адрес G0/0/1 R2.

Настройте плавающий статический маршрут по умолчанию с AD 80 через адрес G0/1 R2.

```
R1_Sidorov(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2 80
```

Шаг 4. На R2 настройте статический маршрут по умолчанию через адрес G0/0/0

R1_ФАМИЛИЯ

a. Используйте команду **ping**, чтобы убедиться, что интерфейс G0/0/0 R1_ФАМИЛИЯ доступен.

```
R2#ping
Protocol [ip]:
Target IP address: 172.16.22.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.22.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

b. Настройте статический маршрут по умолчанию через адрес G0/0/0 R1_ФАМИЛИЯ.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.22.1
```

Шаг 5. Убедитесь, что маршруты работают.

a. Используйте команду **show ip route**, чтобы убедиться, что в таблице маршрутизации R1_ФАМИЛИЯ отображаются статические маршруты и маршруты по умолчанию.

```
R1_Sidorov#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.22.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.0.0/24 is directly connected, Loopback1
L       10.1.0.1/32 is directly connected, Loopback1
S       10.2.0.0/24 [1/0] via 192.168.1.2
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.22.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.22.1/32 is directly connected, GigabitEthernet0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback2
L       209.165.200.225/32 is directly connected, Loopback2
S*   0.0.0.0/0 [1/0] via 172.16.22.2
```

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

b. На R1_ФАМИЛИЯ выполните команду **traceroute 10.2.0.1**. Выходные данные должны показать, что следующий переход — 192.168.1.2.

```
R1_Sidorov#traceroute 10.2.0.1
Type escape sequence to abort.
Tracing the route to 10.2.0.1

  1   192.168.1.2     7 msec    0 msec    0 msec
```

c. На R1_ФАМИЛИЯ выполните команду **traceroute 209.165.200.193**. Выходные данные должны показать, что следующий переход — 172.16.X+1.2.

```
R1_Sidorov#traceroute 172.16.22.2
Type escape sequence to abort.
Tracing the route to 172.16.22.2

  1   172.16.22.2     0 msec    0 msec    0 msec
```

d. Выполните команду **shutdown** на R1_ФАМИЛИЯ G0/0/0.

```
R1_Sidorov#conf t
Enter configuration commands, one p
R1_Sidorov(config)#interface g0/0/0
R1_Sidorov(config-if)#shutdown

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface GigabitE

%LINEPROTO-5-UPDOWN: Line protocol
down

R1_Sidorov(config-if)#exit
```

e. Покажите, что плавающий статический маршрут работает. Выполните команду **show ip route static**. Вы должны увидеть два статических маршрута. Статический маршрут по умолчанию с AD равным 80 и статическим маршрутом к сети 10.2.0.0/24 с AD равным 1.

```
R1_Sidorov#show ip route static
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S       10.2.0.0/24 [1/0] via 192.168.1.2
S*   0.0.0.0/0 [80/0] via 192.168.1.2
```

f. Демонстрация плавающего статического маршрута работает, введите команду **traceroute 209.165.200.193**. Вывод покажет следующий переход - 192.168.1.2.

```
R1_Sidorov#traceroute 209.165.200.193
Type escape sequence to abort.
Tracing the route to 209.165.200.193

  1   192.168.1.2     0 msec    0 msec    0 msec
```

g. Выполните команду **no shutdown** на R1_ФАМИЛИЯ G0/0/0.

Часть 4. Настройка и проверка статической маршрутизации и маршрутизации по умолчанию для IPv6 на R1_ФАМИЛИЯ и R2

В части 4 необходимо настроить статическую маршрутизацию и маршрутизацию по умолчанию на R1_ФАМИЛИЯ и R2, чтобы обеспечить полное соединение между маршрутизаторами с

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco
www.netacad.com

использованием IPv6. Опять же, статическая маршрутизация, используемая здесь, предназначена не для представления наилучшей практики, а для оценки способности завершить необходимые конфигурации.

Шаг 1. На R2 настройте статический маршрут к сети Loopback1 R1_ФАМИЛИЯ, используя адрес G0/0/1 R1_ФАМИЛИЯ в качестве следующего перехода.

a. Используйте команду **ping**, чтобы убедиться, что интерфейс G0/0/1 R1_ФАМИЛИЯ доступен.

```
R2#ping
Protocol [ip]:
Target IP address: 192.168.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
```

b. Настройте статический маршрут для сети Loopback1 R1_ФАМИЛИЯ через адрес G0/0/1 R1_ФАМИЛИЯ.

```
R2(config)#ipv6 route 2001:db8:acad:10::/64 2001:db8:acad:1::1
```

Шаг 2. На R2 настройте статический маршрут по умолчанию через адрес G0/0/0 R1_ФАМИЛИЯ.

a. Используйте команду **ping**, чтобы убедиться, что интерфейс G0/0/0 R1_ФАМИЛИЯ доступен.

```
R2#ping
Protocol [ip]: ipv6
Target IPv6 address: 2001:db8:acad:2::1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:2::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

b. Настройте статический маршрут по умолчанию через адрес G0/0/0 R1_ФАМИЛИЯ.

```
R2(config)#ipv6 route ::/0 2001:db8:acad:2::1
```

Шаг 3. На R2 настройте плавающий статический маршрут по умолчанию через адрес G0/0/1 R1_ФАМИЛИЯ.

Настройте плавающий статический маршрут по умолчанию с AD 80 через адрес G0/0/1 R2.

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

```
R2(config)#ipv6 route ::/0 2001:db8:acad:1::1 80
```

Шаг 4. На R1_ФАМИЛИЯ настройте статический маршрут по умолчанию через адрес G0/0/0 R1_ФАМИЛИЯ.

a. Используйте команду **ping**, чтобы убедиться, что интерфейс G0/0/0 R2 доступен.

```
R1_Sidorov#ping
Protocol [ip]: ipv6
Target IPv6 address: 2001:db8:acad:2::2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:2::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

b. Настройте статический маршрут по умолчанию через адрес G0/0/0 R2.

```
R1_Sidorov(config)#ipv6 route ::/0 2001:db8:acad:2::2
```

Шаг 5. Убедитесь, что маршруты работают.

a. Используйте команду **show ipv6 route**, чтобы убедиться, что таблица маршрутизации R2 отображает статические маршруты и маршруты по умолчанию.

```
R2#show ipv6 route
IPv6 Routing Table - 11 entries
Codes: C - Connected, L - Local, S - Static, R - R
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS inter
       ND - ND Default, NDp - ND Prefix, DCE - Des
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext
       D - EIGRP, EX - EIGRP external
S   ::/0 [1/0]
     via 2001:DB8:ACAD:2::1
C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:1::2/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:2::2/128 [0/0]
     via GigabitEthernet0/0/0, receive
S   2001:DB8:ACAD:10::/64 [1/0]
     via 2001:DB8:ACAD:1::1
C   2001:DB8:ACAD:11::/64 [0/0]
     via Loopback1, directly connected
L   2001:DB8:ACAD:11::2/128 [0/0]
     via Loopback1, receive
C   2001:DB8:ACAD:210::/64 [0/0]
     via Loopback2, directly connected
L   2001:DB8:ACAD:210::1/128 [0/0]
     via Loopback2, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

b. На R2 выполните команду **traceroute 2001:db8:acad:10: :1**. Выходные данные должны показать, что следующий переход - 2001:db8:acad:1: :1.

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

```
R2#traceroute 2001:db8:acad:10::1
Type escape sequence to abort.
Tracing the route to 2001:db8:acad:10::1

  1   2001:DB8:ACAD:1::1 0 msec    0 msec    0 msec
```

c. На R2 выполните команду **traceroute 2001:db8:acad:209: :1**. Выходные данные должны показать, что следующий переход - 2001:db8:acad:2::1.

```
R2#traceroute 2001:db8:acad:209::1
Type escape sequence to abort.
Tracing the route to 2001:db8:acad:209::1

  1   2001:DB8:ACAD:2::1 0 msec    0 msec    0 msec
R2#
```

d. Выполните команду **shutdown** на R2 G0/0/0.

```
R2(config)#int g0/0/0
R2(config-if)#shutdown
```

e. Покажите, что плавающий статический маршрут работает. Выполните команду **show ip6 route static**. Вы должны увидеть два статических маршрута. Статический маршрут по умолчанию с AD 80 и статическим маршрутом в сеть 2001:db8:acad:10::/64 с AD 1.

```
R2#show ipv6 route ?
  WORD                  IPv6 name or address
  X:X:X:X::X/<0-128>    IPv6 prefix
  ospf                  OSPFv3 routes
  summary               Summary display
  <cr>
R2#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RI
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS intera
       ND - ND Default, NDp - ND Prefix, DCE - Dest
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   ::/0 [80/0]
     via 2001:DB8:ACAD:1::1
C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:1::2/128 [0/0]
     via GigabitEthernet0/0/1, receive
S   2001:DB8:ACAD:10::/64 [1/0]
     via 2001:DB8:ACAD:1::1
C   2001:DB8:ACAD:11::/64 [0/0]
     via Loopback1, directly connected
L   2001:DB8:ACAD:11::2/128 [0/0]
     via Loopback1, receive
C   2001:DB8:ACAD:210::/64 [0/0]
     via Loopback2, directly connected
L   2001:DB8:ACAD:210::1/128 [0/0]
     via Loopback2, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

f. Наконец, продемонстрируйте, что плавающий статический маршрут работает, выполнив команду **traceroute 2001:db8:acad:209::1** . Следующий переход - 2001:db8:acad:1: :1.

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

```
R2#traceroute 2001:db8:acad:209::1
Type escape sequence to abort.
Tracing the route to 2001:db8:acad:209::1

  1   2001:DB8:ACAD:1::1 0 msec    0 msec    0 msec
```

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Вопросы для защиты теоретической части (глава 15)

1. Опишите типы создания статических маршрутов. Каков диапазон значений административного расстояния и для настройки какого типа маршрута оно используется?

1. Стандартный статический маршрут
2. Статический маршрут по умолчанию
3. Плавающий статический маршрут
4. Суммарный статический маршрут

Диапазон значений административного расстояния (AD) обычно составляет от 0 до 255. Оно используется для настройки типа маршрута, чтобы определить приоритет, когда несколько маршрутов доступны для конкретного пакета. Чем ниже значение AD, тем выше приоритет маршрута.

2. Дайте определение статическому маршруту по умолчанию. Как определяется сеть назначения для статического IPv6 маршрута?

Статический маршрут по умолчанию представляет собой маршрут, который используется для направления всех пакетов, не соответствующих другим маршрутам в таблице маршрутизации. Для статического IPv6 маршрута сеть назначения определяется как "::/0", что означает любой адрес IPv6.

3. В каком случае может потребоваться создание полностью заданного статического маршрута и почему? Какие параметры можно использовать для идентификации следующего перехода в статическом маршруте?

Полностью заданный статический маршрут может потребоваться, когда требуется указать явные детали о маршруте, включая IP-адрес следующего перехода и интерфейс. Параметры, такие как IP-адрес следующего перехода, интерфейс и AD, могут использоваться для идентификации следующего перехода в статическом маршруте.

4. Каким образом можно создать статический маршрут с прямым подключением? Почему важно настраивать статический маршрут по умолчанию?

Статический маршрут с прямым подключением создается для сетей, к которым устройство подключено напрямую. Настройка статического маршрута по умолчанию важна для обеспечения возможности маршрутизации пакетов в сети, когда нет других соответствующих маршрутов.

5. Для чего необходимо настраивать плавающий статический маршрут? Что представляет из себя статический маршрут хостов?

Настройка плавающего статического маршрута выполняется для обеспечения резервного пути маршрутизации, который активируется только в случае отказа основного маршрута. Статический маршрут хостов представляет собой маршрут, который направляет пакеты к конкретному хосту.

6. В каком случае в таблице маршрутизации появится плавающий статический маршрут? Для чего нужен суммарный статический маршрут?

Плавающий статический маршрут появится в таблице маршрутизации, когда основной маршрут станет недоступным. Суммарный статический маршрут используется для объединения нескольких подсетей в один маршрут.

7. Что из себя представляет стандартный статический маршрут? Почему для плавающего статического маршрута значение административного расстояния (AD) должно быть больше, чем AD протокола динамической маршрутизации?

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Стандартный статический маршрут это основной маршрут, используемый, если нет других соответствующих маршрутов в таблице маршрутизации. Для плавающего статического маршрута значение AD должно быть больше, чем AD протокола динамической маршрутизации, чтобы обеспечить приоритет плавающего маршрута.

8. Каким образом можно осуществить поиск и устранение неполадок, связанных со статическими маршрутами? Какой адрес и длина префикса используются при настройке статического маршрута IPv4 и IPv6 по умолчанию?

Поиск и устранение неполадок, связанных со статическими маршрутами, обычно осуществляется путем проверки таблицы маршрутизации на наличие правильных маршрутов и следующих переходов. Для статического маршрута IPv4 по умолчанию используется адрес "0.0.0.0" с длиной префикса "/0", а для статического маршрута IPv6 по умолчанию используется "::/0".

© © 2013 г. - гггг Корпорация Cisco и/или ее дочерние компании. Все права защищены. Открытая информация Cisco

Настройка основных параметров протокола RIPv2

Топология

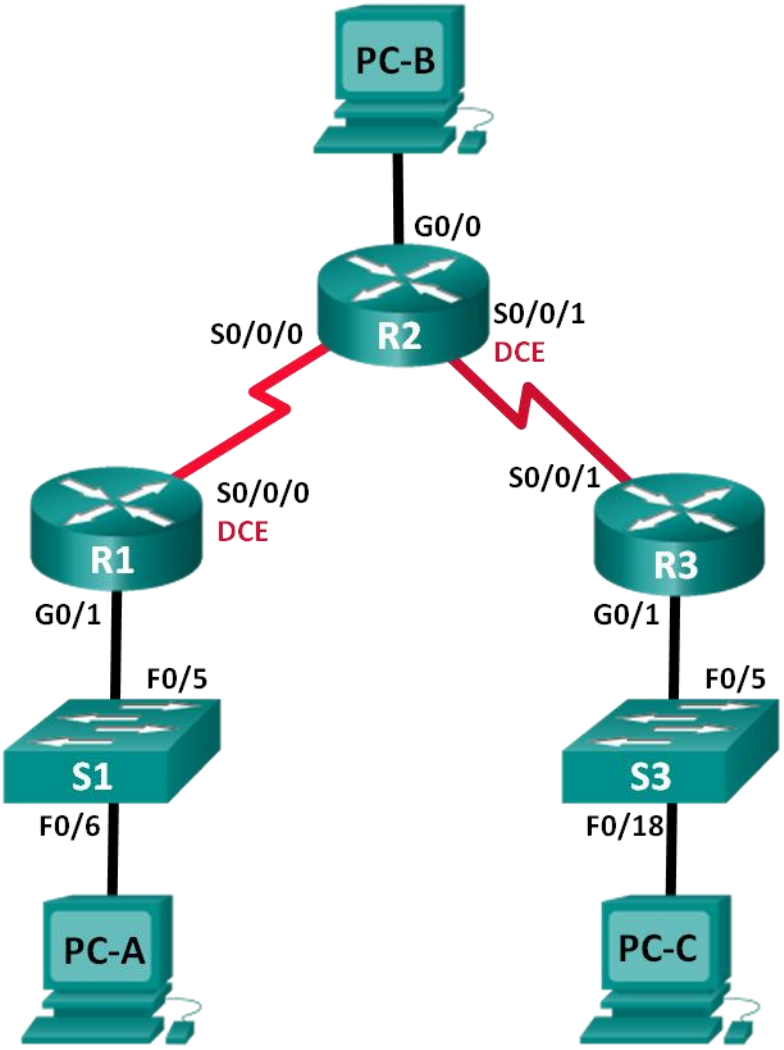


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	172.30.10.1	255.255.255.0	—
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	—
R2_ФАМИЛИЯ	G0/0	209.165.222.1	255.255.255.0	—

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

	S0/0/0	10.1.1.2	255.255.255.252	—
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	—
R3	G0/1	172.30.30.1	255.255.255.0	—
	S0/0/1	10.2.2.1	255.255.255.252	—
S1	—	VLAN 1	—	—
S3	—	VLAN 1	—	—
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.222.2	255.255.255.0	209.165.222.1
PC-C	NIC	172.30.30.3	255.255.255.0	172.30.30.1

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Настройка и проверка маршрутизации RIPv2

- Настройте на маршрутизаторах протокол RIPv2 и проверьте его работоспособность.
- Настройте пассивный интерфейс.
- Изучите таблицы маршрутизации.
- Отключите автоматическое объединение.
- Настройте маршрут по умолчанию. • Проверьте наличие сквозного соединения.

Общие сведения/сценарий

Протокол RIP версии 2 (RIPv2) используется для маршрутизации IPv4-адресов в небольших сетях. RIPv2 — это бесклассовый протокол маршрутизации на базе векторов расстояния, определенный в RFC 1723. Поскольку RIPv2 является бесклассовым протоколом маршрутизации, маски подсетей включены в обновления маршрутизации. По умолчанию протокол RIPv2 автоматически суммирует сети на границах сети. После отключения функции автоматического суммирования протокол RIPv2 прекращает суммирование сетей по их классовому адресу на пограничных маршрутизаторах.

В данной лабораторной работе необходимо настроить топологию сети с использованием маршрутизации RIPv2, отключить автоматическое суммирование, указать маршрут по умолчанию и использовать команды CLI для отображения и проверки сведений о маршрутизации RIP.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. Доступные команды и результаты их выполнения зависят от модели устройства и версии Cisco IOS и могут отличаться от тех, которые приведены в этой лабораторной работе. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

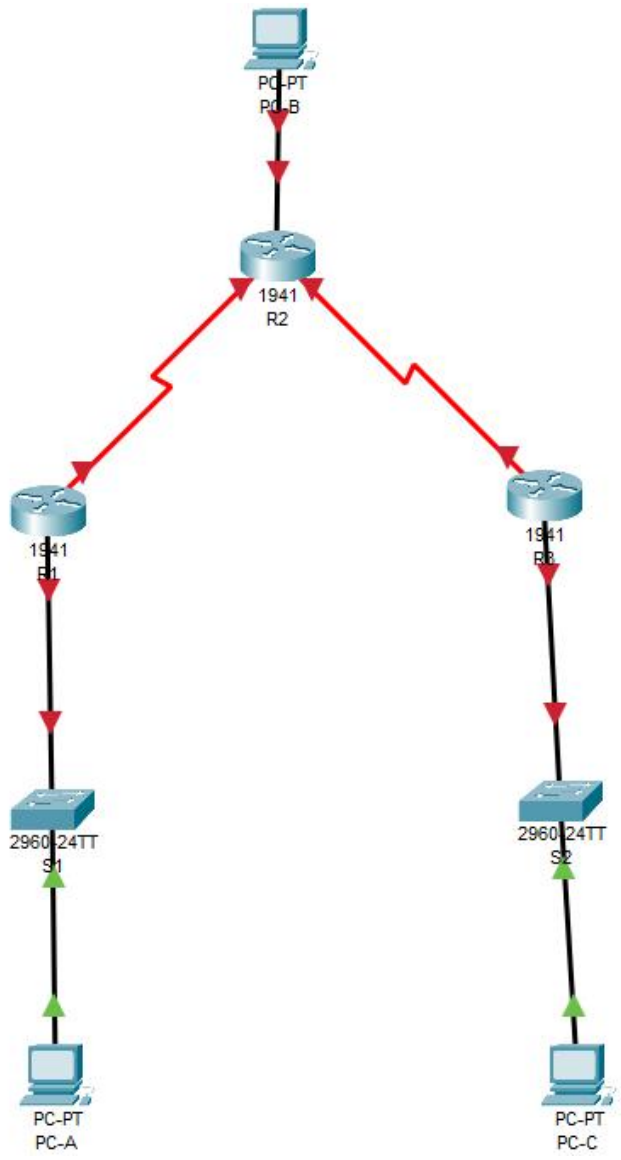
Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель).
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель).
- 3 ПК (ОС Windows с программой эмуляции терминала, например, Tera Term).
- Консольные кабели для настройки устройств Cisco IOS через консольные порты. • Кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Создание сети и настройка основных параметров устройства

В части 1 вам предстоит создать топологию сети и настроить основные параметры.

Шаг 1: Создайте сеть согласно топологии.



© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Настройте основные параметры на каждом маршрутизаторе и коммутаторе. a.

Отключите поиск DNS.

b. Настройте имена устройств в соответствии с топологией.

c. Настройте шифрование пароля.

d. Назначьте **class** в качестве пароля привилегированного режима EXEC.

e. Назначьте **cisco** в качестве паролей консоли и VTY.

f. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

g. Настройте **logging synchronous** на линии консоли.

h. Назначьте IP-адреса всем интерфейсам в соответствии с таблицей адресации.

i. Для каждого интерфейса настройте описание с IP-адресом.

j. Если возможно, установите значение тактовой частоты для последовательного интерфейса DCE.

k. Скопируйте текущую конфигурацию в загрузочную конфигурацию.

S1, S2 настраивался по аналогии

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain lookup
S1(config)#service password-enc
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#logging sync
S1(config-line)#login
S1(config-line)#exit
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#logging sync
S1(config-line)#login
S1(config-line)#exit
S1(config)#banner motd #Unautorized access only
Enter TEXT message.  End with the character '#'.
#

S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Router R2_Sidorov, по аналогии в соответствии с табл. адресации были настроены R1 и R3

```
Router(config)#hostname R2_Sidorov
R2_Sidorov(config)#service password-enc
R2_Sidorov(config)#enable secret class
R2_Sidorov(config)#line console 0
R2_Sidorov(config-line)#password cisco
R2_Sidorov(config-line)#logging sync
R2_Sidorov(config-line)#login
R2_Sidorov(config-line)#exit
R2_Sidorov(config)#line vyt 0 15
                      ^
% Invalid input detected at '^' marker.

R2_Sidorov(config)#line vty 0 15
R2_Sidorov(config-line)#password cisco
R2_Sidorov(config-line)#logging sync
R2_Sidorov(config-line)#login
R2_Sidorov(config-line)#exit
R2_Sidorov(config)#banner motd #unautorized access only#
R2_Sidorov(config)#int g0/0
R2_Sidorov(config-if)#ip address 209.165.222.1 255.255.255.0
R2_Sidorov(config-if)#no shut
```

```
R2_Sidorov(config)#int g0/0
R2_Sidorov(config-if)#description Con to pcb
R2_Sidorov(config-if)#exit
R2_Sidorov(config)#int s0/0/0
R2_Sidorov(config-if)#desc con to r1
R2_Sidorov(config-if)#ip address 10.1.1.2 255.255.255.252
R2_Sidorov(config-if)#exit
R2_Sidorov(config)#int s0/0/1
R2_Sidorov(config-if)#desc con to r3
R2_Sidorov(config-if)#ip address 10.2.2.2 255.255.255.252
R2_Sidorov(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2_Sidorov(config-if)#exit
R2_Sidorov(config)#int s0/0/0
R2_Sidorov(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R2_Sidorov(config-if)#exit
R2_Sidorov(config)#exit
R2_Sidorov#
%SYS-5-CONFIG_I: Configured from console by console

R2_Sidorov#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

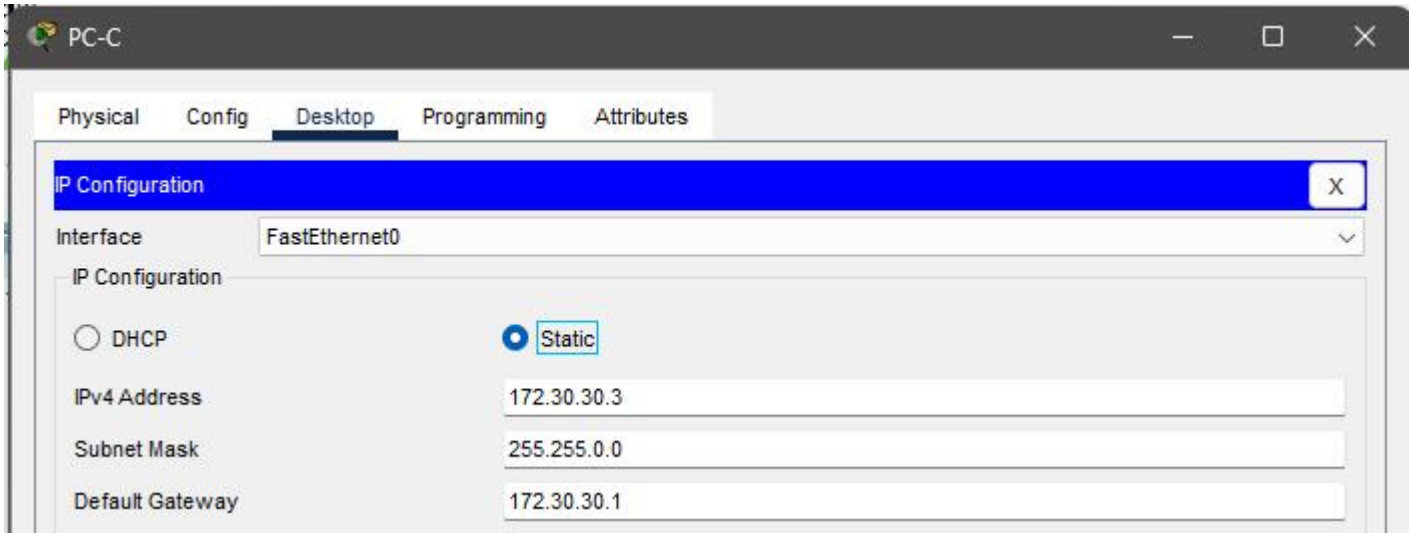
```
R2_Sidorov(config)#int s0/0/1
R2_Sidorov(config-if)#clock rate 128000
R2_Sidorov(config-if)#exit
```

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Шаг 4: Настройте IP-адресацию на компьютере. Сведения об IP-адресах

компьютеров можно посмотреть в таблице адресации.

PC-C, по аналогии для PC-B и PC-A в соотв. с таблицей адресации



Шаг 5: Проверка связи.

На данный момент компьютеры не могут отправлять друг другу эхо-запросы.

a. Каждая рабочая станция должна иметь возможность проводить эхо-тестирование присоединенного маршрутизатора. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

```
C:\> ping 172.30.10.1

Pinging 172.30.10.1 with 32 bytes of data:

Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255
Reply from 172.30.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.30.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 172.30.30.1

Pinging 172.30.30.1 with 32 bytes of data:

Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255
Reply from 172.30.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.30.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
C:\>ping 209.165.222.1

Pinging 209.165.222.1 with 32 bytes of data:

Reply from 209.165.222.1: bytes=32 time<1ms TTL=255
Reply from 209.165.222.1: bytes=32 time<1ms TTL=255
Reply from 209.165.222.1: bytes=32 time<1ms TTL=255
Reply from 209.165.222.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.222.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

b. Маршрутизаторы должны успешно отправлять эхо-запросы друг другу. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

```
R1#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/10 ms
```

```
R3#ping 10.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/9/14 ms
```

Часть 2: Настройка и проверка маршрутизации RIPv2

В части 2 необходимо будет настроить маршрутизацию RIPv2 на всех маршрутизаторах в сети, а затем убедиться, что таблицы маршрутизации обновляются правильно. После проверки RIPv2 вам предстоит отключить автоматическое суммирование, настроить маршрут по умолчанию и проверить сквозное соединение.

Шаг 1: Настройте маршрутизацию по протоколу RIPv2.

a. Настройте протокол RIPv2 на маршрутизаторе R1 в качестве протокола маршрутизации и проинформируйте об этом соответствующие подключённые сети.

```
R1# config t
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# passive-interface g0/1
R1(config-router)# network 172.30.0.0
R1(config-router)# network 10.0.0.0
```

Команда **passive-interface** прекращает отправку обновлений маршрутизации из указанного интерфейса. Данный процесс предотвращает нежелательную отправку маршрутизирующей информации в локальную сеть. Тем не менее, сеть, к которой относится указанный интерфейс, по-прежнему объявляется в обновлениях маршрутизации, которые отправляются из других интерфейсов.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#passive-interface g0/1
R1(config-router)#network 172.30.0.0
R1(config-router)#network 10.0.0.0
```

b. Настройте протокол RIPv2 на маршрутизаторе R3 и воспользуйтесь командой **network**, чтобы добавить соответствующие сети и предотвратить обновления маршрутизации в интерфейсе локальной сети.

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#passive-interface g0/1
R3(config-router)#network 172.30.0.0
R3(config-router)#network 10.0.0.0
```

c. Настройте протокол RIPv2 на маршрутизаторе R2_ФАМИЛИЯ и воспользуйтесь командой network, чтобы добавить соответствующие подключенные сети. Не объявляйте сеть 209.165.X+201.0.

Примечание. Не обязательно делать интерфейс G0/0 на маршрутизаторе R2_ФАМИЛИЯ пассивным, поскольку сеть, связанная с этим интерфейсом, не объявляется.

```
R2_Sidorov(config)#router rip
R2_Sidorov(config-router)#version 2
R2_Sidorov(config-router)#network 10.0.0.0
R2_Sidorov(config-router)#exit
```

Шаг 2: Проверьте текущее состояние сети.

a. Состояние двух последовательных каналов можно легко проверить с помощью команды **show ip interface brief** на маршрутизаторе R2_ФАМИЛИЯ.

```
R2_Sidorov#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     209.165.222.1   YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/0/0            10.1.1.2        YES manual up                    up
Serial0/0/1            10.2.2.2        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

b. Проверьте наличие подключения между компьютерами.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

PC-A

```
C:\>ping 209.165.222.2

Pinging 209.165.222.2 with 32 bytes of data:

Reply from 172.30.10.1: Destination host unreachable.
Request timed out.
Reply from 172.30.10.1: Destination host unreachable.
Reply from 172.30.10.1: Destination host unreachable.

Ping statistics for 209.165.222.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=2ms TTL=125
Reply from 172.30.30.3: bytes=32 time=2ms TTL=125
Reply from 172.30.30.3: bytes=32 time=3ms TTL=125
Reply from 172.30.30.3: bytes=32 time=11ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 11ms, Average = 4ms
```

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

PC-C

```
C:\>ping 209.165.222.2

Pinging 209.165.222.2 with 32 bytes of data:

Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.
Reply from 172.30.30.1: Destination host unreachable.

Ping statistics for 209.165.222.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.30.10.3

Pinging 172.30.10.3 with 32 bytes of data:

Reply from 172.30.10.3: bytes=32 time=15ms TTL=125
Reply from 172.30.10.3: bytes=32 time=12ms TTL=125
Reply from 172.30.10.3: bytes=32 time=11ms TTL=125
Reply from 172.30.10.3: bytes=32 time=10ms TTL=125

Ping statistics for 172.30.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 15ms, Average = 12ms
```

c. Убедитесь в том, что протокол RIPv2 активирован на маршрутизаторах.

Чтобы проверить это, можно воспользоваться командами **debug ip rip**, **show ip protocols** и **show run**. Выходные данные команды **show ip protocols** для маршрутизатора R1 показаны ниже.

```
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 23 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0           22
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
            10.0.0.0
            172.30.0.0
Passive Interface(s):
            GigabitEthernet0/1
Routing Information Sources:
            Gateway         Distance      Last Update
            10.1.1.2             120      00:00:09
Distance: (default is 120)
```

Какие сведения подтверждают работу RIPv2 при выполнении команды **debug ip rip** на маршрутизаторе R2_ФАМИЛИЯ?

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
R2_Sidorov#debug ip rip
RIP protocol debugging is on
R2_Sidorov#RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0

R2_Sidorov#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.0.0/16 via 0.0.0.0 in 1 hops

R2_Sidorov#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.0.0/16 via 0.0.0.0 in 1 hops
```

Какие сведения подтверждают работу RIPv2 при выполнении команды **show run** на маршрутизаторе R3?

```
router rip
 version 2
 passive-interface GigabitEthernet0/1
 network 10.0.0.0
 network 172.30.0.0
```

d. Отключите автоматическое суммирование маршрутов.

Локальные сети, подключенные к маршрутизаторам R1 и R3, состоят из «разорванных» сетей. Маршрутизатор R2_ФАМИЛИЯ отображает в таблице маршрутизации два пути к сети 172.30.0.0/16, имеющие одинаковую стоимость. Маршрутизатор R2_ФАМИЛИЯ отображает только адрес главной классовой сети 172.30.0.0, но не отображает подсети этой сети.

```
R2_Sidorov#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R    172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:14, Serial0/0/1
                   [120/1] via 10.1.1.1, 00:00:11, Serial0/0/0
     209.165.222.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.222.0/24 is directly connected, GigabitEthernet0/0
L       209.165.222.1/32 is directly connected, GigabitEthernet0/0
```

Маршрутизатор R1 отображает только собственную подсеть для сети 172.30.10.0/24. В таблице маршрутизации R1 нет маршрута для подсети 172.30.30.0/24 маршрутизатора R3.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:06, Serial0/0/0
     172.30.0.0/16 is variably subnetted, 3 subnets, 3 masks
R       172.30.0.0/16 is possibly down, routing via 10.1.1.2, Serial0/0/0
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1
```

Маршрутизатор R3 отображает только собственную подсеть для сети 172.30.30.0/24. В таблице маршрутизации R3 нет маршрута для подсетей 172.30.10.0/24 маршрутизатора R1.

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:06, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
     172.30.0.0/16 is variably subnetted, 3 subnets, 3 masks
R       172.30.0.0/16 is possibly down, routing via 10.2.2.2, Serial0/0/1
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1
```

Чтобы определить маршруты, полученные в обновлениях RIP от маршрутизатора R3, используйте команду **debug ip rip** на маршрутизаторе R2_ФАМИЛИЯ. Укажите их далее.

```
R2_Sidorov#debug ip rip
RIP protocol debugging is on
R2_Sidorov#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.0.0/16 via 0.0.0.0 in 1 hops
```

Маршрутизатор R3 не передает какие-либо подсети 172.30.0.0, только суммарный маршрут 172.30.0.0/16, включая маску подсети. Поэтому таблицы маршрутизации на R1 и R2_ФАМИЛИЯ не отображают подсети 172.30.0.0 на R3.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Шаг 3: Отключите автоматическое объединение.

a. Для отключения автоматического суммирования в RIPv2 используется команда **no auto-summary**. Отключите автоматическое суммирование на всех маршрутизаторах. Маршрутизаторы больше не суммируют маршруты на границах главной классовой сети. Маршрутизатор R1 приведен здесь в качестве примера.

```
R2_Sidorov(config)#router rip
R2_Sidorov(config-router)#no auto-sum
```

```
R3(config)#router rip
R3(config-router)#no aut
R3(config-router)#no auto-summary
```

```
R1#conf t
Enter configuration commands,
R1(config)#router rip
R1(config-router)#no auto0sum
```

b. Чтобы очистить таблицу маршрутизации, используйте команду **clear ip route ***.

```
R1#clear ip route *
```

```
R2_Sidorov#clear ip route *
```

```
R3#clear ip route *
```

c. Изучите таблицы маршрутизации. Не забывайте, что после очистки таблиц маршрутизации потребуется некоторое время для выравнивания их содержимого.

Подсети LAN, подключенные к маршрутизаторам R1 и R3, должны быть включены во все три таблицы маршрутизации.

```
R2_Sidorov#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
     172.30.0.0/24 is subnetted, 2 subnets
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:06, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:08, Serial0/0/1
     209.165.222.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.222.0/24 is directly connected, GigabitEthernet0/0
L       209.165.222.1/32 is directly connected, GigabitEthernet0/0
```

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:12, Serial0/0/0
     172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1
R       172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0
```

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:16, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
     172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.30.10.0/24 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1
```

d. Чтобы проверить обновления RIP, на маршрутизаторе R2_ФАМИЛИЯ используйте команду **debug ip rip**.

   R2_ФАМИЛИЯ# **debug ip rip**

   Через 60 секунд выполните команду **no debug ip rip**.

   Какие маршруты содержатся в обновлениях RIP, принятых от R3?

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
R2_Sidorov#debug ip rip
RIP protocol debugging is on
R2_Sidorov#RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.10.0/24 via 0.0.0.0, metric 2, tag 0

R2_Sidorov#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.30.0/24 via 0.0.0.0 in 1 hops

R2_Sidorov#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.10.0/24 via 0.0.0.0 in 1 hops

R2_Sidorov#RIP: sending  v2 update to 224.0.0.9 via Serial0/0/0 (10.1.1.2)
RIP: build update entries
      10.2.2.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.30.0/24 via 0.0.0.0, metric 2, tag 0
RIP: sending  v2 update to 224.0.0.9 via Serial0/0/1 (10.2.2.2)
RIP: build update entries
      10.1.1.0/30 via 0.0.0.0, metric 1, tag 0
      172.30.10.0/24 via 0.0.0.0, metric 2, tag 0

R2_Sidorov#RIP: received v2 update from 10.2.2.1 on Serial0/0/1
      172.30.30.0/24 via 0.0.0.0 in 1 hops

R2_Sidorov#RIP: received v2 update from 10.1.1.1 on Serial0/0/0
      172.30.10.0/24 via 0.0.0.0 in 1 hops
```

Шаг 4: Настройка и перераспределение маршрута по умолчанию для доступа к Интернету

a. На маршрутизаторе R2_ФАМИЛИЯ создайте статический маршрут к сети 0.0.0.0 0.0.0.0 с помощью команды **ip route**. В результате весь трафик с неизвестным адресом назначения будет пересылаться на компьютер PC-B с адресом 209.165.X+201.2, моделируя Интернет путем настройки шлюза «последней надежды» на маршрутизаторе R2_ФАМИЛИЯ.

```
R2_Sidorov(config)#ip route 0.0.0.0 0.0.0.0 209.165.222.2
```

b. Маршрутизатор R2_ФАМИЛИЯ объявит маршрут для других маршрутизаторов, если команда **default- information originate** будет добавлена в его конфигурацию RIP.

```
R2_Sidorov(config)#router rip
R2_Sidorov(config-router)#default-information originate
```

Шаг 5: Проверка конфигурации маршрутизации

a. Просмотрите таблицу маршрутизации маршрутизатора R1.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:23, Serial0/0/0
     172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1
R       172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:23, Serial0/0/0
R*   0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:23, Serial0/0/0
```

b. Просмотрите таблицу маршрутизации на R2_ФАМИЛИЯ. Каким образом путь для интернет-трафика появился в таблице маршрутизации маршрутизатора R2_ФАМИЛИЯ?

```
R2_Sidorov#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.222.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
     172.30.0.0/24 is subnetted, 2 subnets
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:02, Serial0/0/1
     209.165.222.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.222.0/24 is directly connected, GigabitEthernet0/0
L       209.165.222.1/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 209.165.222.2
```

Шаг 6: Проверьте подключение.

a. Смоделируйте отправку трафика в Интернет, отправив эхо-запросы от узла PC-A и PC-C в сеть 209.165.X+201.2.

   Успешно ли выполнена проверка связи? _____

b. Убедитесь в том, что узлы в разбитой на подсети сети могут достичь друг друга. Для этого выполните эхо-запрос между узлами PC-A и PC-C.

   Успешно ли выполнена проверка связи? _____ **Примечание**. Может потребоваться отключение межсетевого экрана на компьютерах.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

PC-A

```
C:\>ping 209.165.222.2

Pinging 209.165.222.2 with 32 bytes of data:

Reply from 209.165.222.2: bytes=32 time=12ms TTL=126
Reply from 209.165.222.2: bytes=32 time=1ms TTL=126
Reply from 209.165.222.2: bytes=32 time=11ms TTL=126
Reply from 209.165.222.2: bytes=32 time=6ms TTL=126

Ping statistics for 209.165.222.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 7ms

C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=14ms TTL=125
Reply from 172.30.30.3: bytes=32 time=10ms TTL=125
Reply from 172.30.30.3: bytes=32 time=11ms TTL=125
Reply from 172.30.30.3: bytes=32 time=2ms TTL=125

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 14ms, Average = 9ms
```

PC-C

```
C:\>ping 209.165.222.2

Pinging 209.165.222.2 with 32 bytes of data:

Reply from 209.165.222.2: bytes=32 time=15ms TTL=126
Reply from 209.165.222.2: bytes=32 time=11ms TTL=126
Reply from 209.165.222.2: bytes=32 time=1ms TTL=126
Reply from 209.165.222.2: bytes=32 time=10ms TTL=126

Ping statistics for 209.165.222.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 9ms

C:\>ping 172.30.30.3

Pinging 172.30.30.3 with 32 bytes of data:

Reply from 172.30.30.3: bytes=32 time=6ms TTL=128
Reply from 172.30.30.3: bytes=32 time=4ms TTL=128
Reply from 172.30.30.3: bytes=32 time=6ms TTL=128
Reply from 172.30.30.3: bytes=32 time=4ms TTL=128

Ping statistics for 172.30.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 6ms, Average = 5ms
```

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Вопросы для защиты теоретической части (самостоятельное изучение + глава 14)

1. Характеристика механизмов пересылки пакетов и источников получения маршрутов:

Механизмы пересылки пакетов включают в себя прямую пересылку (forwarding), которая осуществляется маршрутизатором на основе информации в его таблице маршрутизации. Таблица маршрутизации содержит записи о том, какие пакеты отправлять и через какие интерфейсы и маршруты.

Источники получения маршрутов в таблице маршрутизации могут включать:

Статические маршруты: Настроенные администратором вручную.
Динамические маршруты: Получаемые от протоколов динамической маршрутизации, таких как RIP, OSPF, EIGRP, BGP и др.
По умолчанию (default routes): Маршруты, которые используются для направления всех пакетов, не соответствующих другим маршрутам в таблице маршрутизации.

2. Определение понятия “административное расстояние” (AD) и его использование в RIP:

Административное расстояние (AD) это мера надежности или доверия к источнику маршрута. В протоколе RIP по умолчанию AD равно 120. Его можно посмотреть, используя команду show ip route на маршрутизаторе Cisco.

3. Целесообразность настройки динамической маршрутизации и определение понятия “метрика маршрута”:

Динамическая маршрутизация целесообразна в случаях, когда сеть динамична, подвержена частым изменениям топологии или когда требуется автоматическое обнаружение и восстановление маршрутов. Метрика маршрута это числовая оценка качества или стоимости маршрута, которая используется для выбора наилучшего маршрута к конкретному пункту назначения.

4. Проведите краткую сравнительную характеристику статической и динамической маршрутизации:

Статическая маршрутизация:

Преимущества:

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

- Простота настройки: Статические маршруты настраиваются вручную администратором, что делает процесс простым и прозрачным.
- Предсказуемость: Маршруты остаются неизменными, пока их не изменит администратор, что обеспечивает стабильность сети.

Недостатки:

- Неэффективность в динамических средах: В динамичных сетях изменение топологии может требовать регулярного обновления статических маршрутов.
- Ресурсозатратность: На больших сетях администрирование статических маршрутов может быть трудоёмким и требовать больших ресурсов.

Динамическая маршрутизация:

Преимущества:

- Автоматизация: Маршруты обновляются и подстраиваются автоматически в ответ на изменения топологии сети.
- Эффективность: В динамической среде динамическая маршрутизация может обеспечить более эффективное использование сетевых ресурсов.
- Недостатки:
- Сложность настройки: Настройка и поддержка протоколов динамической маршрутизации требует определённого уровня знаний и опыта.
- Возможность возникновения проблем: Неверная настройка или непредвиденные обстоятельства могут привести к проблемам с маршрутизацией.

Протоколы динамической маршрутизации:

Протоколы динамической маршрутизации делятся на две основные категории: внутренние и внешние.

Внутренние протоколы маршрутизации работают в пределах одной автономной системы (AS) и включают в себя:

RIP (Routing Information Protocol): Простой и распространённый протокол, который измеряет метрику маршрута по количеству прыжков (hops) до целевой сети.

OSPF (Open Shortest Path First): Продвинутый протокол, использующий стоимость маршрута, основанную на пропускной способности (bandwidth).

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

EIGRP (Enhanced Interior Gateway Routing Protocol): Cisco-специфичный протокол, который учитывает несколько факторов, таких как пропускная способность, задержка, надёжность и загрузка канала.

Внешние протоколы маршрутизации используются для обмена маршрутами между различными автономными системами и включают в себя:

BGP (Border Gateway Protocol): Протокол маршрутизации, используемый в Интернете, который обменивается информацией о маршрутах между различными автономными системами.

5. Назначение протоколов динамической маршрутизации и их компоненты:

Протоколы динамической маршрутизации нужны для автоматического обнаружения и обновления маршрутов в сети. Они включают в себя механизмы обмена сообщениями между маршрутизаторами, алгоритмы выбора маршрутов и техники сходимости.

6. Вычисление метрики для протоколов RIP, OSPF и EIGRP и распределение нагрузки:

Для RIP метрика основана на количестве прыжков до целевой сети.
OSPF использует стоимость маршрута, которая зависит от пропускной способности канала.
EIGRP вычисляет метрику, учитывая пропускную способность, задержку, надежность и загрузку канала. Распределение нагрузки при использовании динамической маршрутизации основано на механизмах балансировки нагрузки, таких как равновесие нагрузки на основе маршрутов или потоков данных.

7. Назначение кодов C, L и S в таблице маршрутизации и применение протокола BGP:

C: Код C обозначает, что маршрут является прямым подключением к маршрутизатору.
L: Код L указывает на локальный маршрут, который обозначает маршрут к собственному IP-адресу маршрутизатора.
S: Код S используется для статических маршрутов.
Протокол BGP используется в крупных сетях Интернета и корпоративных сетях для обмена маршрутной информацией между автономными системами.

8. Недостатки динамической маршрутизации и пассивный интерфейс:

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Недостатки динамической маршрутизации:

Сложность настройки: Настройка протоколов динамической маршрутизации требует определённого уровня знаний и опыта. Администратор должен понимать особенности работы каждого протокола и уметь корректно настраивать их параметры.

Возможность возникновения проблем: Неверная настройка или непредвиденные обстоятельства могут привести к проблемам с маршрутизацией. Например, неправильная конфигурация маршрутизаторов или сбой в работе протокола могут привести к недоступности частей сети.

Нагрузка на процессор маршрутизатора: Процессор маршрутизатора должен обрабатывать информацию о маршрутах и обмене сообщениями между маршрутизаторами, что может привести к дополнительной нагрузке и снижению производительности устройства.

Пассивный интерфейс:

Пассивный интерфейс в сетевой терминологии обозначает интерфейс маршрутизатора или коммутатора, который не участвует в обмене информацией о маршрутах с другими устройствами. Он принимает только входящий трафик и не генерирует собственные маршруты. Рассмотрим основные аспекты пассивных интерфейсов:

Предотвращение передачи маршрутов: Пассивные интерфейсы не рассылают обновления маршрутов в сеть, что может быть полезно для уменьшения нагрузки на сеть и защиты от возможных угроз.

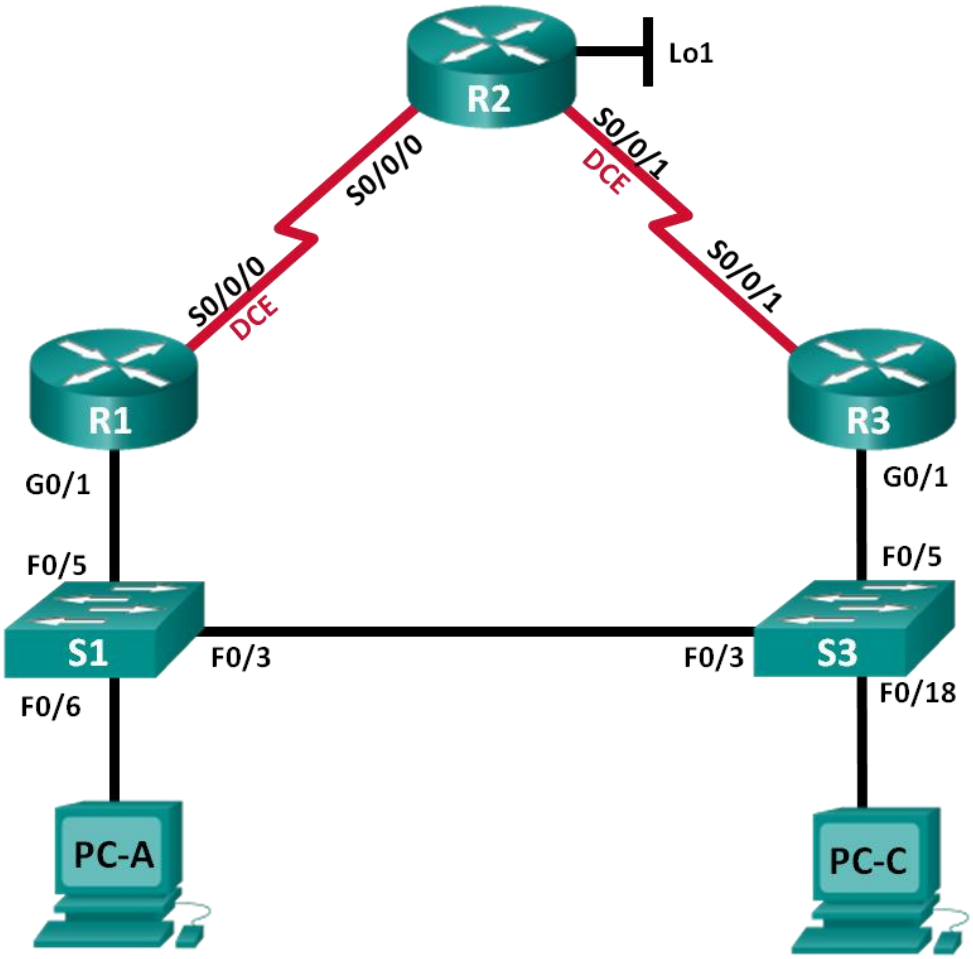
Использование во внешних связях: Пассивные интерфейсы часто используются на внешних граничных устройствах сети, например, на подключениях к Интернету или другим внешним сетям. Это помогает предотвратить нежелательное распространение внутренних маршрутов за пределы сети.

Ограничение нагрузки на маршрутизатор: Поскольку пассивные интерфейсы не участвуют в обмене маршрутной информацией, они могут помочь уменьшить нагрузку на процессор маршрутизатора и повысить его производительность.

© Корпорация Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Настройка HSRP

Топология



Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	—
R2_ФАМИЛИЯ	S0/0/0	10.1.1.2	255.255.255.252	—
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	—
	Lo1	209.165.221.225	255.255.255.224	—
R3	G0/1	192.168.1.3	255.255.255.0	—
	S0/0/1	10.2.2.1	255.255.255.252	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.13	255.255.255.0	192.168.1.3
PC-A	NIC	192.168.1.31	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.33	255.255.255.0	192.168.1.3

Задачи

Часть 1. Построение сети и проверка соединения

Часть 2. Настройка обеспечения избыточности на первом хопе с помощью HSRP

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 компьютера (ОС Windows с программой эмуляции терминала, например, Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet и последовательные кабели согласно топологии

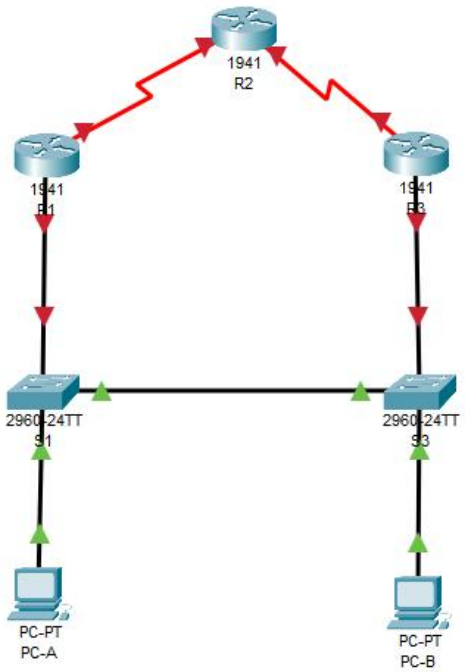
Часть 1: Построение сети и проверка связи

В первой части вам предстоит настроить топологию сети и выполнить базовую настройку, например IP-адреса интерфейсов, статическую маршрутизацию, доступ к устройствам и пароли.

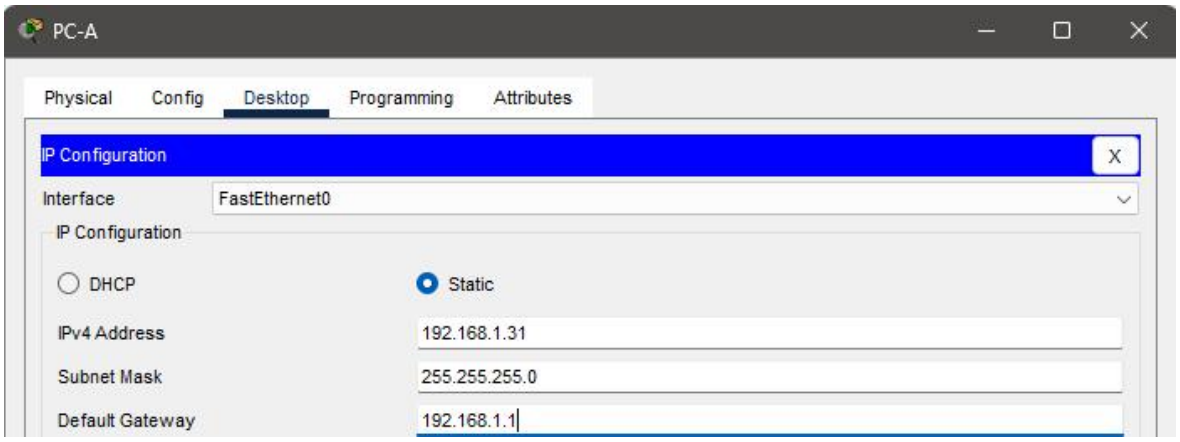
Шаг 1: Создайте сеть согласно топологии.

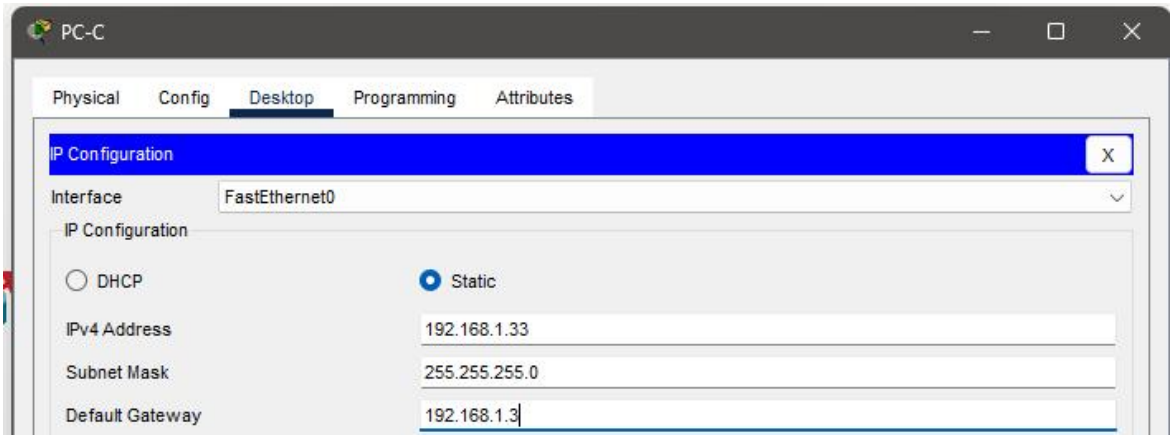
Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.



Шаг 2: Настройте узлы ПК.





Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.

d. Установите тактовую частоту на **128000** для всех последовательных интерфейсов маршрутизатора DCE.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

R2_Sidorov, по аналогии R1 и R3 в соответствии с таблицей адресации

```
Router(config)#hostname R2_Sidorov
R2_Sidorov(config)#no ip domain lookup
R2_Sidorov(config)#int s0/0/0
R2_Sidorov(config-if)#ip address 10.1.1.2 255.255.255.252
R2_Sidorov(config-if)#no shut

R2_Sidorov(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
exit
R2_Sidorov(config)#int s0/0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
                     ^
% Invalid input detected at '^' marker.

R2_Sidorov(config)#int s0/0/1
R2_Sidorov(config-if)#ip address 10.2.2.2 255.255.255.252
R2_Sidorov(config-if)#clock rate 128000
R2_Sidorov(config-if)#no shut

R2_Sidorov(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R2_Sidorov(config-if)#exit
R2_Sidorov(config)#int lo
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
1

R2_Sidorov(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R2_Sidorov(config-if)#ip address 209.165.221.225 255.255.255.224
R2_Sidorov(config-if)#no shut
R2_Sidorov(config-if)#exit
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
R2_Sidorov(config)#line con 0
R2_Sidorov(config-line)#password cisco
R2_Sidorov(config-line)#login
R2_Sidorov(config-line)#logg
R2_Sidorov(config-line)#logging sync
R2_Sidorov(config-line)#exit
R2_Sidorov(config)#enable secret class
R2_Sidorov(config)#line vty 0 15
R2_Sidorov(config-line)#password cisco
R2_Sidorov(config-line)#login
R2_Sidorov(config-line)#logging synchr
R2_Sidorov(config-line)#logging synchronous
R2_Sidorov(config-line)#exit
R2_Sidorov(config)#exit
R2_Sidorov#
%SYS-5-CONFIG_I: Configured from console by console

R2_Sidorov#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Шаг 5: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

d. Настройте IP-адреса для коммутаторов, указанных в таблице адресации.

e. На каждом коммутаторе настройте шлюз по умолчанию.

f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

S1, по аналогии для S3 в соответствии с таблицей адресации

```
Switch(config)#hostname S1
S1(config)#no ip domain lookup
S1(config)#enable secret class
S1(config)#int vlan1
S1(config-if)#ip address 192.168.1.11 255.255.255.0
S1(config-if)#no shut

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#exit
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logg sync
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logg sync
S1(config-line)#exit
S1(config)#ip default-gateway 192.168.1.1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Шаг 6: Проверьте подключение между PC-A и PC-C.

Отправьте ping-запрос с компьютера PC-A на компьютер PC-C. Удалось ли получить ответ?

```
C:\>ping 192.168.1.31

Pinging 192.168.1.31 with 32 bytes of data:

Reply from 192.168.1.31: bytes=32 time=5ms TTL=128
Reply from 192.168.1.31: bytes=32 time=15ms TTL=128
Reply from 192.168.1.31: bytes=32 time<1ms TTL=128
Reply from 192.168.1.31: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 5ms

C:\>
```

Шаг 7: Настройте маршрутизацию.

a. Настройте RIP версии 2 на всех маршрутизаторах. Добавьте в процесс RIP все сети, кроме 209.165.X+200.224/27.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 10.0.0.0
R1(config-router)#network 192.168.1.0
R1(config-router)#exit
R1(config)#exit
```

```
R2_Sidorov(config)#router rip
R2_Sidorov(config-router)#version 2
R2_Sidorov(config-router)#no auto-summary
R2_Sidorov(config-router)#do show ip route connected
 C   10.1.1.0/30  is directly connected, Serial0/0/0
 C   10.2.2.0/30  is directly connected, Serial0/0/1
 C   209.165.221.224/27  is directly connected, Loopback1

R2_Sidorov(config-router)#network 10.0.0.0
R2_Sidorov(config-router)#exit
R2_Sidorov(config)#exit
```

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#no auto-summ
R3(config-router)#no auto-summary
R3(config-router)#do show ip route conn
 C   10.2.2.0/30  is directly connected, Serial0/0/1
 C   192.168.1.0/24  is directly connected, GigabitEthernet0/1

R3(config-router)#network 10.0.0.0
R3(config-router)#network 192.168.1.0
R3(config-router)#exit
R3(config)#exit
```

b. Настройте маршрут по умолчанию на маршрутизаторе R2_ФАМИЛИЯ с использованием Lo1 в качестве интерфейса выхода в сеть 209.165.X+200.224/27.

c. На маршрутизаторе R2_ФАМИЛИЯ используйте следующие команды для перераспределения маршрута по умолчанию в процесс RIP.

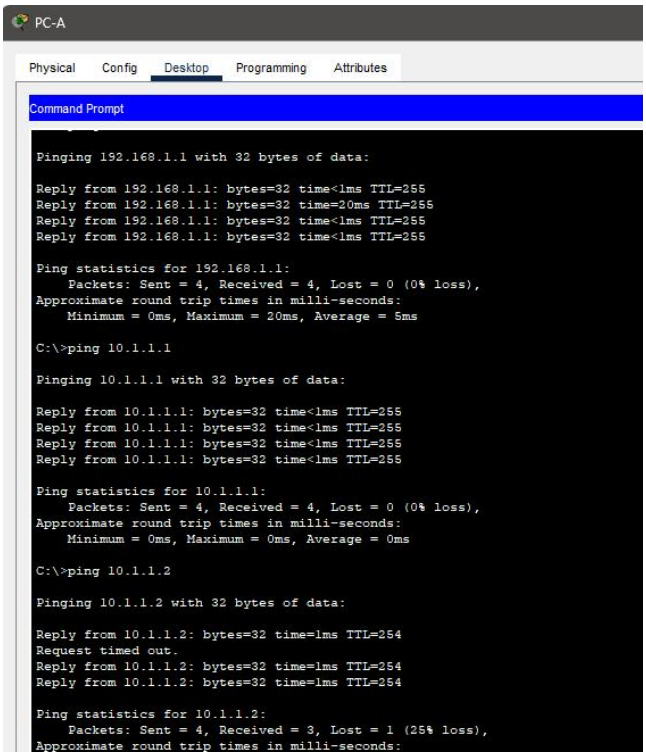
```
R2_ФАМИЛИЯ(config)# router rip
R2_ФАМИЛИЯ(config-router)# default-information originate
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

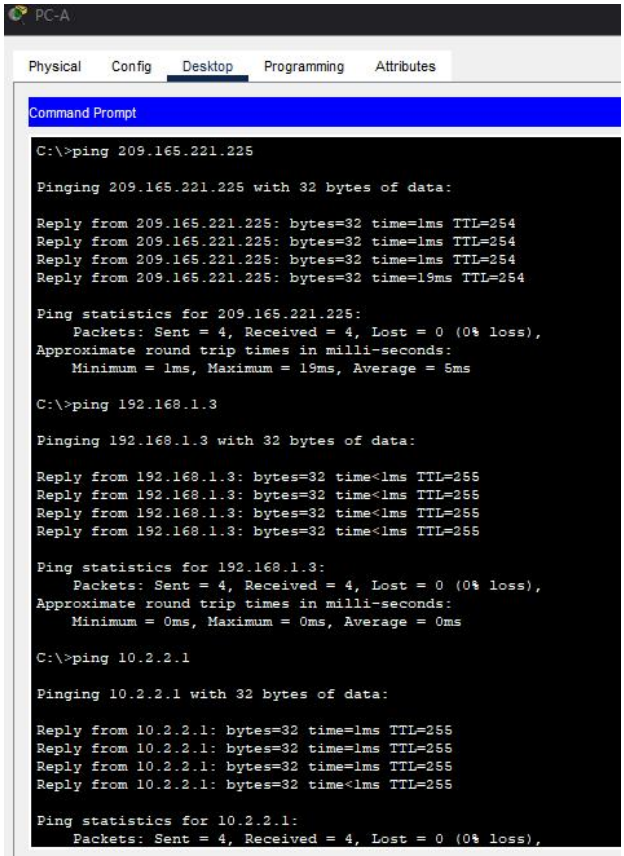
```
R2_Sidorov(config)#ip route 0.0.0.0 0.0.0.0 loopback 1
%Default route without gateway, if not a point-to-point interface, may impact performance
R2_Sidorov(config)#router rip
R2_Sidorov(config-router)#drfault-in
R2_Sidorov(config-router)#drfault-info
R2_Sidorov(config-router)#default-in
R2_Sidorov(config-router)#default-information orig
R2_Sidorov(config-router)#default-information originate
R2_Sidorov(config-router)#exit
R2_Sidorov(config)#exit
```

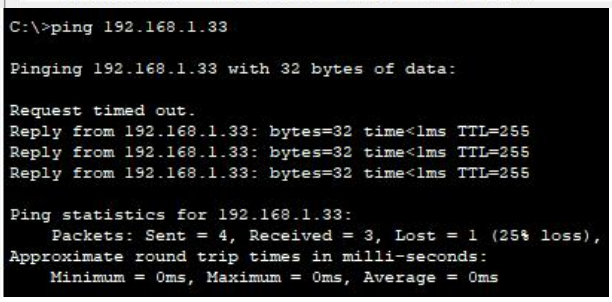
Шаг 8: Проверьте подключение.

a. Необходимо получить ответ на ping-запросы с компьютера PC-A от каждого интерфейса на маршрутизаторах R1, R2_ФАМИЛИЯ и R3, а также от компьютера PC-C. Удалось ли получить все ответы?



Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.





b. Необходимо получить ответ на ping-запросы с компьютера PC-C от каждого интерфейса на маршрутизаторах R1, R2_ФАМИЛИЯ и R3, а также от компьютера PC-A. Удалось ли получить все ответы?

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

PC-C

Physical Config Desktop Programming Attributes

Command Prompt

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=1ms TTL=255
Reply from 10.1.1.1: bytes=32 time<1ms TTL=255
Reply from 10.1.1.1: bytes=32 time=1ms TTL=255
Reply from 10.1.1.1: bytes=32 time=18ms TTL=255

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 5ms

C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=1ms TTL=254
Reply from 10.1.1.2: bytes=32 time=15ms TTL=254
Reply from 10.1.1.2: bytes=32 time=1ms TTL=254
Reply from 10.1.1.2: bytes=32 time=1ms TTL=254

Ping statistics for 10.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 4ms
```

```
Reply from 10.2.2.2: bytes=32 time=33ms TTL=254
Reply from 10.2.2.2: bytes=32 time=19ms TTL=254
Reply from 10.2.2.2: bytes=32 time=1ms TTL=254
Reply from 10.2.2.2: bytes=32 time=1ms TTL=254

Ping statistics for 10.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 33ms, Average = 13ms

C:\>ping 209.165.221.225

Pinging 209.165.221.225 with 32 bytes of data:

Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=20ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.221.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 20ms, Average = 5ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=255
Reply from 192.168.1.3: bytes=32 time<1ms TTL=255
Reply from 192.168.1.3: bytes=32 time<1ms TTL=255
Reply from 192.168.1.3: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
C:\>ping 10.2.2.1

Pinging 10.2.2.1 with 32 bytes of data:

Reply from 10.2.2.1: bytes=32 time<1ms TTL=255
Reply from 10.2.2.1: bytes=32 time<1ms TTL=255
Reply from 10.2.2.1: bytes=32 time=1ms TTL=255
Reply from 10.2.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.31

Pinging 192.168.1.31 with 32 bytes of data:

Reply from 192.168.1.31: bytes=32 time<1ms TTL=128
Reply from 192.168.1.31: bytes=32 time<1ms TTL=128
Reply from 192.168.1.31: bytes=32 time<1ms TTL=128
Reply from 192.168.1.31: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Часть 2: Настройка обеспечения избыточности на первом хопе с помощью HSRP

Даже если топология спроектирована с учетом избыточности (два маршрутизатора и два коммутатора в одной сети LAN), оба компьютера, PC-A и PC-C, необходимо настраивать с одним адресом шлюза. PC-A использует R1, а PC-C — R3. В случае сбоя на одном из этих маршрутизаторов или интерфейсов маршрутизаторов компьютер может потерять подключение к сети Интернет.

В части 2 вам предстоит изучить поведение сети до и после настройки протокола HSRP. Для этого вам понадобится определить путь, по которому проходят пакеты, чтобы достичь loopback-адрес на R2_ФАМИЛИЯ.

Шаг 1: Определите путь интернет-трафика для PC-A и PC-C.

В командной строке на PC-A введите команду **tracert** для loopback-адреса 209.165.X+200.225 на маршрутизаторе R2_ФАМИЛИЯ.

```
C:\>tracert 209.165.221.225

Tracing route to 209.165.221.225 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.1.1
  2   0 ms      1 ms      1 ms      209.165.221.225

Trace complete.
```

В командной строке на PC-C введите команду **tracert** для loopback-адреса 209.165.X+200.225 на маршрутизаторе R2_ФАМИЛИЯ.

```
C:\>tracert 209.165.221.225

Tracing route to 209.165.221.225 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.1.3
  2   1 ms      1 ms      0 ms      209.165.221.225

Trace complete.
```

Шаг 2: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение между S1 и R1.

a. В командной строке на PC-A введите команду **ping –t** для адреса **209.165.X+200.225** на маршрутизаторе R2_ФАМИЛИЯ. Убедитесь, что окно командной строки открыто.

```
C:\>ping -t 209.165.221.225

Pinging 209.165.221.225 with 32 bytes of data:

Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
```

b. В процессе эхо-тестирования отсоедините кабель Ethernet от интерфейса F0/5 на S1. Отключение интерфейса F0/5 на S1 приведет к тому же результату.

```
S1(config-if)#shutdown
S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

c. Какими были бы результате при повторении шагов 2a и 2b на компьютере PC-C и коммутаторе S3?

```
S3(config-if)#shutdown
S3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

d. Повторно подсоедините кабели Ethernet к интерфейсу F0/5 или включите интерфейс F0/5 на S1 и S3, соответственно. Повторно отправьте эхо-запросы на 209.165.X+200.225 с компьютеров PC-A и PC-C, чтобы убедиться в том, что подключение восстановлено.

```
C:\>ping 209.165.221.225

Pinging 209.165.221.225 with 32 bytes of data:

Reply from 209.165.221.225: bytes=32 time=2ms TTL=254
Request timed out.
Reply from 209.165.221.225: bytes=32 time=19ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.221.225:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 19ms, Average = 7ms
```

```
C:\>ping 209.165.221.225

Pinging 209.165.221.225 with 32 bytes of data:

Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=21ms TTL=254

Ping statistics for 209.165.221.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 21ms, Average = 6ms
```

Шаг 3: Настройте HSRP на R1 и R3.

В этом шаге вам предстоит настроить HSRP и изменить адрес шлюза по умолчанию на компьютерах PC-A, PC-C, S1 и коммутаторе S2 на виртуальный IP-адрес для HSRP. R1 назначается активным маршрутизатором с помощью команды приоритета HSRP. a. Настройте протокол HSRP на маршрутизаторе R1.

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
R1(config)#int g0/1
R1(config-if)#standby version 2
R1(config-if)#standby 1 ip 192.168.1.254
R1(config-if)#
%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Init -> Init

R1(config-if)#standby 1 priority 150
R1(config-if)#standby 1 preempt
R1(config-if)#
```

b. Настройте протокол HSRP на маршрутизаторе R3.

```
R3(config)#int g0/1
R3(config-if)#standby version 2
R3(config-if)#standby 1 ip 192.168.1.254
R3(config-if)#
%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Init -> Init
```

c. Проверьте HSRP, выполнив команду **show standby** на R1 и R3.

```
R3#show standby
GigabitEthernet0/1 - Group 1 (version 2)
  State is Standby
    5 state changes, last state change 00:12:24
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.224 secs
  Preemption disabled
  Active router is 192.168.1.1
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Gig0/1-1 (default)
```

```
R1#show standby
GigabitEthernet0/1 - Group 1 (version 2)
  State is Active
    6 state changes, last state change 00:09:10
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.629 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.3
  Priority 150 (configured 150)
  Group name is hsrp-Gig0/1-1 (default)
```

d. Используйте команду **show standby brief** на R1 и R3, чтобы просмотреть сводку состояния HSRP. Выходные данные приведены ниже.

```
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/1      1    150 P Active   local           192.168.1.3     192.168.1.254
```

```
R3#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/1      1    100   Standby  192.168.1.1     local           192.168.1.254
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

e. Измените адрес шлюза по умолчанию для PC-A, PC-C, S1 и S3. Какой адрес следует использовать?

192.168.1.254

f. Проверьте новые настройки. Отправьте эхо-запрос с PC-A и с PC-C на loopback-адрес маршрутизатора R2_ФАМИЛИЯ. Успешно ли выполнены эхо-запросы?

```
C:\>ping 209.165.221.225

Pinging 209.165.221.225 with 32 bytes of data:

Request timed out.
Reply from 209.165.221.225: bytes=32 time=18ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.221.225:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 18ms, Average = 6ms
```

```
C:\>ping 209.165.221.225

Pinging 209.165.221.225 with 32 bytes of data:

Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=15ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.221.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 4ms
```

Шаг 4: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение с коммутатором, подключенным к активному маршрутизатору HSRP (R1).

a. В командной строке на PC-A введите команду **ping –t** для адреса 209.165.X+200.225 на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.

b. Во время отправки эхо-запроса отсоедините кабель Ethernet от интерфейса F0/5 на коммутаторе S1 или выключите интерфейс F0/5.

```
S1(config)#interface FastEthernet0/5
S1(config-if)#shutdown
S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
C:\>ping -t 209.165.221.225

Pinging 209.165.221.225 with 32 bytes of data:

Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=29ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Request timed out.
Request timed out.
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=1ms TTL=254
Reply from 209.165.221.225: bytes=32 time=27ms TTL=254
Reply from 209.165.221.225: bytes=32 time=19ms TTL=254
```

Шаг 5: Проверьте настройки HSRP на маршрутизаторах R1 и R3.

a. Выполните команду **show standby brief** на маршрутизаторах R1 и R3.

До включения

```
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/1      1    150 P Init     unknown         unknown         192.168.1.254
```

```
R3#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/1      1    100   Active   local           unknown         192.168.1.254
```

После включения

```
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/1      1    150 P Active   local           192.168.1.3     192.168.1.254
```

```
R3#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/1      1    100   Standby  192.168.1.1     local           192.168.1.254
```

Шаг 6: Изменение приоритетов HSRP.

a. Измените приоритет HSRP на 200 на маршрутизаторе R3. Какой маршрутизатор является активным?

```
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/1      1    150 P Active   local           192.168.1.3     192.168.1.254
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

```
R3#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/1      1    200   Standby  192.168.1.1     local           192.168.1.254
```

b. Выполните команду, чтобы сделать активным маршрутизатор R3 без изменения приоритета. Какую команду вы использовали?

```
R3(config)#int g0/1
R3(config-if)#sta
R3(config-if)#standby 1 pre?
preempt
R3(config-if)#standby 1 pre
R3(config-if)#standby 1 preempt
R3(config-if)#ex
 %HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Standby -> Active
i
```

c. Используйте команду **show**, чтобы убедиться, что R3 является активным маршрутизатором.

```
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/1      1    150 P Standby  192.168.1.3     local           192.168.1.254
```

```
R3#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/1      1    200 P Active   local           192.168.1.1     192.168.1.254
```

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Вопросы для защиты теоретической части (главы 9, 10, 16)

Для чего необходимо резервирование маршрутизаторов? Опишите преимущества протокола HSRP.

Резервирование маршрутизаторов необходимо для обеспечения непрерывной работы сети в случае отказа одного из маршрутизаторов. Протокол HSRP (Hot Standby Router Protocol) предоставляет механизм резервирования, позволяющий создать виртуальный маршрутизатор, который будет служить как резервный для активного маршрутизатора. Преимущества HSRP включают в себя увеличение надежности сети, улучшение доступности ресурсов, а также возможность балансировки нагрузки.

Какие роли исёполняют активный, резервный и виртуальный маршрутизатор? Каким образом происходит процесс выбора активного маршрутизатора?

Активный маршрутизатор: основной маршрутизатор, обрабатывающий трафик в сети.
Резервный маршрутизатор: запасной маршрутизатор, готовый заменить активный в случае его отказа.
Виртуальный маршрутизатор: абстрактная сущность, создаваемая протоколом HSRP для представления группы активного и резервного маршрутизаторов.
Процесс выбора активного маршрутизатора основан на приоритете, который назначается каждому маршрутизатору. Маршрутизатор с наивысшим приоритетом становится активным. В случае равенства приоритетов используется MAC-адрес маршрутизатора для выбора активного.

Что происходит в случае сбоя активного маршрутизатора? Что произойдет, если в сети появится маршрутизатор с более высоким приоритетом?

При сбое активного маршрутизатора резервный маршрутизатор автоматически принимает роль активного, чтобы обеспечить непрерывность работы сети. Если в сети появится маршрутизатор с более высоким приоритетом, он станет активным, а бывший активный маршрутизатор примет роль резервного.

Что необходимо сделать для возобновления процесса выбора активного маршрутизатора? Опишите состояния протокола HSRP.

Для возобновления процесса выбора активного маршрутизатора необходимо изменить условия приоритета (например, изменить приоритет текущего активного маршрутизатора или добавить новый маршрутизатор с более высоким приоритетом). Состояния протокола HSRP включают в себя:

Initial (Инициализация)
Learn (Обучение)
Listen (Слушание)
Speak (Речь)
Standby (Резервный)
Active (Активный)

В каком случае сработает приоритетное вытеснение маршрутизатора? Опишите принцип работы сетевой атаки DDoS.

Приоритетное вытеснение маршрутизатора сработает, если в сеть войдет маршрутизатор с более высоким приоритетом, чем у текущего активного маршрутизатора, заставив его стать резервным.
Сетевая атака DDoS (Distributed Denial of Service) предполагает насыщение целевой системы или сети трафиком из большого количества источников, что приводит к перегрузке и отказу в обслуживании.

Дайте характеристику компонентам AAA. Как будет вести себя коммутатор в результате успешной атаки на таблицу CAM?

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Компоненты AAA (Authentication, Authorization, Accounting) обеспечивают механизмы аутентификации, авторизации и учета пользователей в сети. Коммутатор в результате успешной атаки на таблицу CAM (Content Addressable Memory) может потерять информацию о соответствии MAC-адресов и портов, что приведет к некорректному пересылке пакетов и возможному отказу в обслуживании.

Опишите принцип работы атаки с двойным тегированием. В чем заключается опасность ARP атак?

Атака с двойным тегированием (Double Tagging) заключается в манипуляции с VLAN тегами в сети, что может позволить злоумышленнику получить доступ к данным в других VLAN. Опасность ARP атак (Address Resolution Protocol) заключается в возможности перехвата и подмены ARP-запросов и ответов, что может привести к перенаправлению трафика на злоумышленный узел.

В чем заключается потенциальная опасность использование протокола CDP? Как поступит маршрутизатор, если на нем не настроен маршрут по умолчанию и пакет должен быть перенаправлен в сеть назначения, которая не указана в его таблице маршрутизации?

Потенциальная опасность использования протокола CDP (Cisco Discovery Protocol) заключается в возможности получения злоумышленником информации о топологии сети и используемых устройствах. Если на маршрутизаторе не настроен маршрут по умолчанию и пакет должен быть перенаправлен в сеть назначения, которая не указана в его таблице маршрутизации, маршрутизатор отклонит пакет и отправит сообщение об ошибке.

Какие данные могут быть получены с помощью протокола CDP? Каким образом можно провести атаку STP протокола?

С помощью протокола CDP можно получить информацию о соседних устройствах, используемых интерфейсах и их параметрах, таких как платформа и версия программного обеспечения. Атаку на протокол STP (Spanning Tree Protocol) можно провести, например, с помощью подмены BPDU-пакетов (Bridge Protocol Data Units), что может привести к созданию петли в сети и нарушению ее работы.

В чем заключается опасность DHCP-спуфинга? Опишите метод сетевой атаки VLAN Hopping.

Опасность DHCP-спуфинга заключается в возможности злоумышленника подменить легитимный DHCP-сервер в сети, предоставив клиентам некорректную конфигурацию сети, например, указав в качестве шлюза злонамеренный маршрутизатор. Метод сетевой атаки VLAN Hopping основан на эксплуатации недостатков конфигурации коммутаторов, позволяющих злоумышленнику получить доступ к данным в других VLAN путем отправки трафика, содержащего двойные VLAN теги.

Авторское право © компании Cisco и (или) ее дочерних компаний, 2017 г. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.