

Настройка Rapid PVST+, PortFast и BPDU Guard

Топология

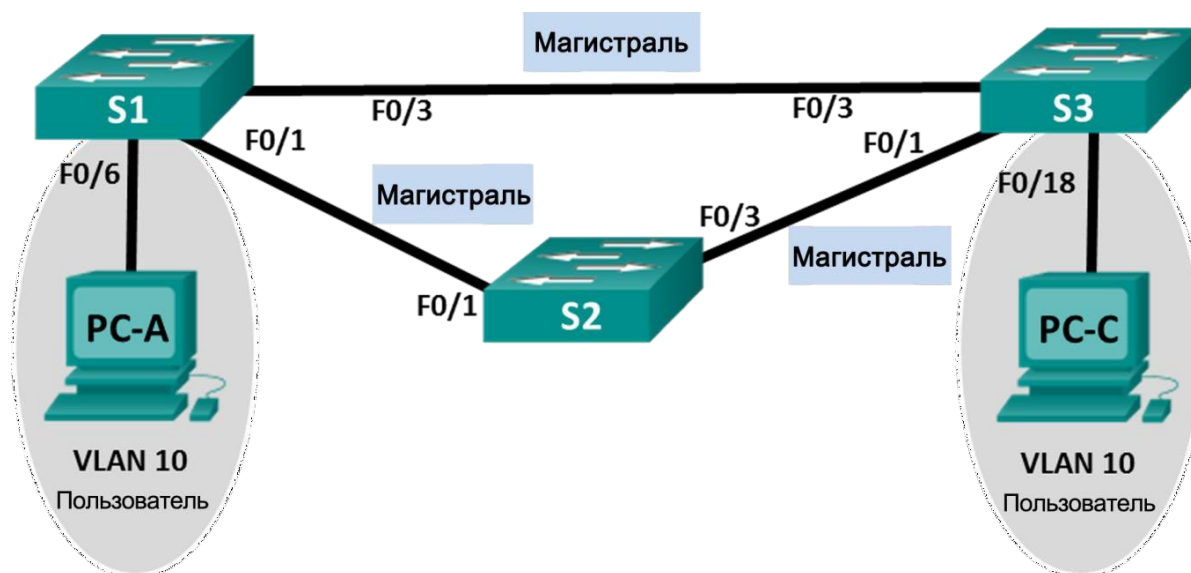


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1_ФАМИЛИЯ	VLAN 99	192.168.X+1.11	255.255.255.0
S2	VLAN 99	192.168.X+1.12	255.255.255.0
S3	VLAN 99	192.168.X+1.13	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_ФАМИЛИЯ
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

Необходимые ресурсы

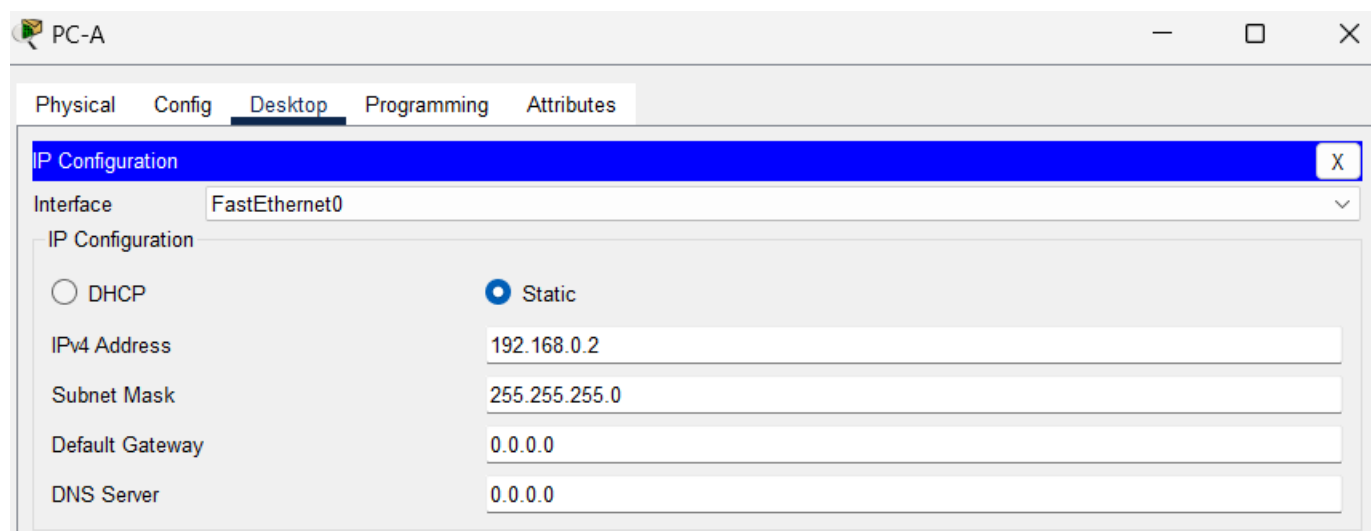
- 3 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (ОС Windows с программой эмуляции терминала, например, Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии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

Часть 1: Создание сети и настройка основных параметров устройства

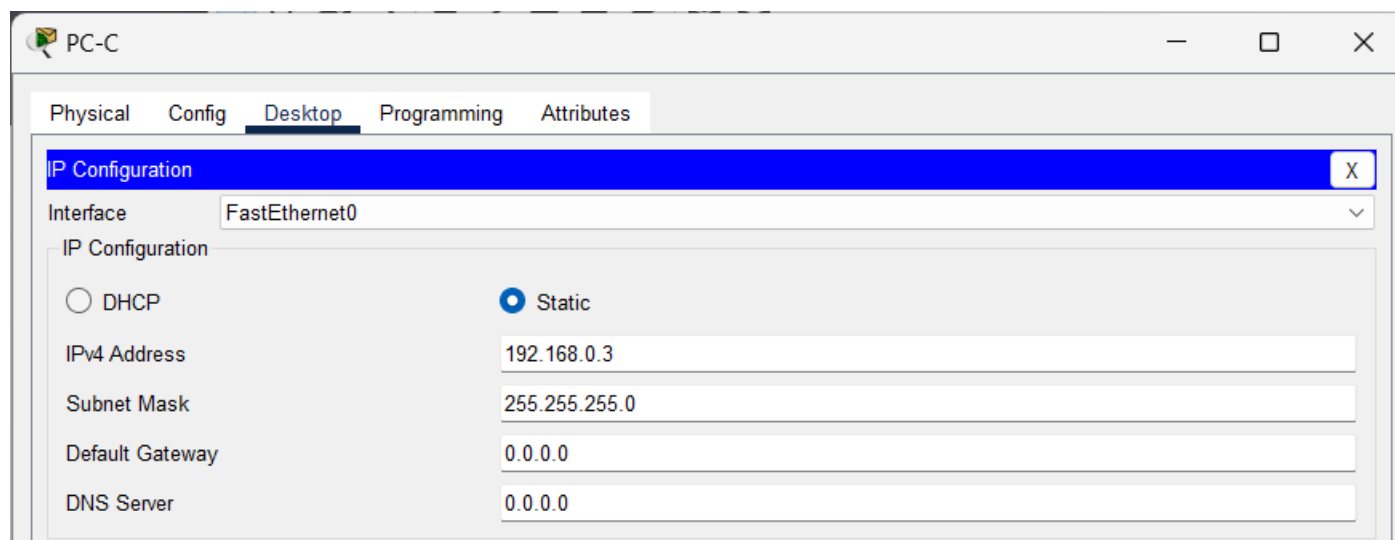
В части 1 вы настроите топологию сети и такие базовые параметры, как IP-адреса интерфейсов, доступ к устройствам и пароли.

Шаг 1: Создайте сеть согласно топологии.

Шаг 2: Настройте узлы ПК.



The screenshot shows the configuration window for PC-A. The 'Desktop' tab is selected. Under 'IP Configuration', the 'Interface' is set to 'FastEthernet0'. The 'Static' radio button is selected. The 'IPv4 Address' is 192.168.0.2, 'Subnet Mask' is 255.255.255.0, 'Default Gateway' is 0.0.0.0, and 'DNS Server' is 0.0.0.0.



The screenshot shows the configuration window for PC-C. The 'Desktop' tab is selected. Under 'IP Configuration', the 'Interface' is set to 'FastEthernet0'. The 'Static' radio button is selected. The 'IPv4 Address' is 192.168.0.3, 'Subnet Mask' is 255.255.255.0, 'Default Gateway' is 0.0.0.0, and 'DNS Server' is 0.0.0.0.

Шаг 3: Выполните инициализацию и перезагрузку коммутаторов.

```
Switch>en
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 00E0.8F2C.669E
Xmodem file svstem is available.
```

Шаг 4: Настройте базовые параметры каждого коммутатора.

- Отключите поиск DNS.
- Присвойте имена устройствам в соответствии с топологией.
- Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTY и включите запрос пароля при подключении.
- Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
- Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
- Отключите все порты коммутатора.
- Сохраните текущую конфигурацию в загрузочную конфигурацию.

Настройка коммутатора S1:

```
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)#enable secret class
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login

S1(config-line)#logging sync
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#interface range f0/1-24, g0/1-2
S1(config-if-range)#shutdown

S1(config-if-range)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy run
S1#copy running-config start
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Настройка коммутатора S2:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#enable secret class
S2(config)#no ip domain-lookup
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#logging sy
S2(config-line)#logging synchronous
S2(config-line)#exit
S2(config)#interface range f0/1-24, g0/1-2
S2(config-if-range)#shutdown

S2(config-if-range)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy run
S2#copy running-config star
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

Настройка коммутатора S3:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#no ip domain-lookup
S3(config)#enable secret class
S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#logging sy
S3(config-line)#logging synchronous
S3(config-line)#exit

S3(config)#interface range f0/1-24, g0/1-2
S3(config-if-range)#shutdown

S3#copy run
S3#copy running-config sta
S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S3#
```

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**.

Настройка коммутатора S1:

```
S1(config)#vlan 10
S1(config-vlan)#name User_Belosludtsev
S1(config-vlan)#vlan 99
S1(config-vlan)#name Management
S1(config-vlan)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy run
S1#copy running-config sta
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Настройка коммутатора S2:

```
S2(config)#vlan 10
S2(config-vlan)#name User_Belosludtsev
S2(config-vlan)#vlan 99
S2(config-vlan)#name Management
S2(config-vlan)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy run
S2#copy running-config st
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

Настройка коммутатора S3:

```
S3(config)#vlan 10
S3(config-vlan)#name User_Belosludtsev
S3(config-vlan)#vlan 99
S3(config-vlan)#name Management
S3(config-vlan)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S3#
```

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.

Настройка коммутатора S1:

```
S1(config)#interface f0/6
S1(config-if)#no shutdown

S1(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

S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
```

Настройка коммутатора S3:

```
S3(config)#interface f0/18
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)#switchport mode access
S3(config-if)#switchport access vlan 10
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 коммутатора S1:

```
S1(config)#int range f0/1, f0/3
S1(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
S1(config-if-range)#switchport mode trunk
^
% Invalid input detected at '^' marker.

S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#end
```

Настройка коммутатора S2:

```
S2(config)#int range f0/1, f0/3
S2(config-if-range)#no shutdown

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

Настройка коммутатора S3:

```
S3(config)#int range f0/1, f0/3
S3(config-if-range)#no shutdown

S3(config-if-range)#switchport mode trunk
S3(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.

Настройка коммутатора S1:

```
S1(config)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.3.11 255.255.255.0
S1(config-if)#end
```

Настройка коммутатора S2:

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S2(config-if)#ip address 192.168.3.12 255.255.255.0
S2(config-if)#
```

Настройка коммутатора S3:

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.3.13 255.255.255.0
```

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.

Коммутатор S1:

```
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, 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_Belosludtsev	active	Fa0/6
99	Management	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
S1#
```

Коммутатор S2:

```
S2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, 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_Belosludtsev	active	
99	Management	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
S2#
```

Коммутатор S3:

```
S3#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, 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_Belosludtsev	active	Fa0/18
99	Management	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
S3#
```

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

Коммутатор S1:

```
S1#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.lq	trunking	99
Fa0/3	on	802.lq	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

```
S1#
```


Коммутатор S2:

```
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     none
Fa0/3     1,10,99

S2#
```

Коммутатор S3:

```
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

S3#
```

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

Коммутатор S1:

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!

:
interface Vlan99
 ip address 192.168.3.11 255.255.255.0
!
```

Коммутатор S2:

```
spanning-tree mode pvst
spanning-tree extend system-id
!

interface Vlan99
 ip address 192.168.3.12 255.255.255.0
!
```

Коммутатор S3:

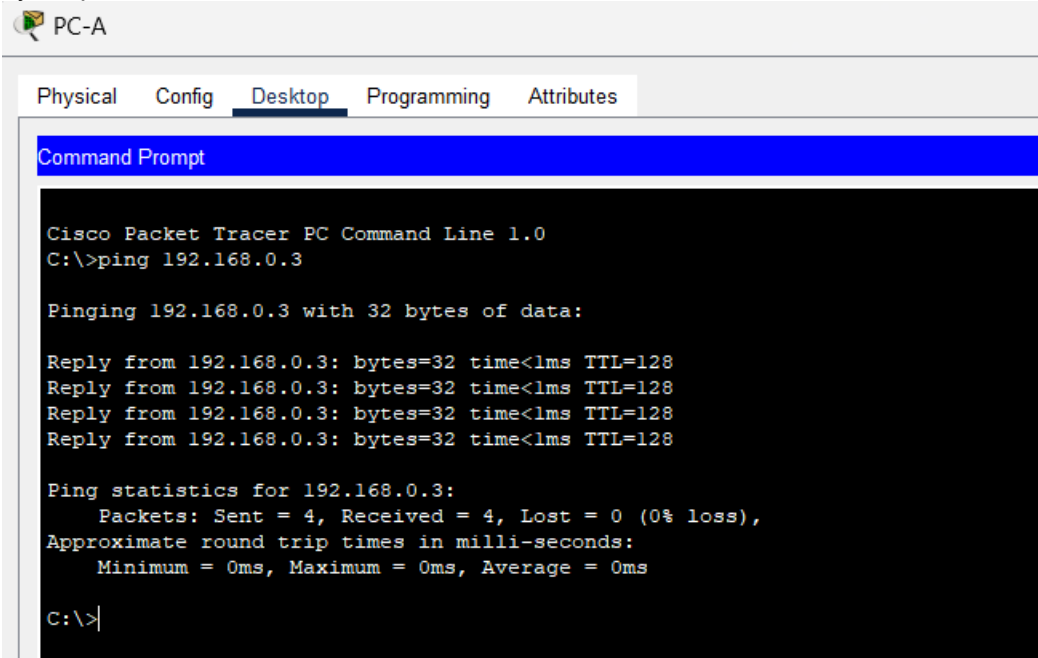
```
spanning-tree mode pvst
spanning-tree extend system-id
!

interface Vlan99
 ip address 192.168.3.13 255.255.255.0
!
```

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?

Если эхо-запрос выполнить не удалось, следует выполнять отладку до тех пор, пока проблема не будет решена.



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.

show spanning-tree vlan 1

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

Коммутатор S1:

```
S1#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0005.5E43.070A
             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     0060.3EDD.AB6A
             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                    Root FWD 19       128.3   P2p
```

Коммутатор S2:

```
S2#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0005.5E43.070A
             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     0060.470C.C153
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

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

Коммутатор S3:

```
S3#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0005.5E43.070A
             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     0005.5E43.070A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

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

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?

```
Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
```

Каков приоритет моста коммутатора S2 для сети VLAN 1?

```
Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
```

Каков приоритет моста коммутатора S3 для сети VLAN 1?

```
Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
```

Какой коммутатор является корневым мостом?

```
S3#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0005.5E43.070A
             This bridge is the root.
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Почему этот коммутатор выбран в качестве корневого моста?

- Выбор делается на основе самого низкого MAC-адреса

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.

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

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

spanning-tree vlan 1,10,99 root secondary

```
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#spanning-tree vlan 1,10,99 root secondary
S1(config)#
```

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

Какой приоритет моста используется для коммутатора S1_ФАМИЛИЯ в сети VLAN 1?

```
S1#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0060.470C.C153
             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     0060.3EDD.AB6A
             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
```

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

Какой интерфейс в сети находится в состоянии блокировки?

```
S2#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0060.470C.C153
             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     0060.470C.C153
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

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

```
S3#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0060.470C.C153
             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     0005.5E43.070A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

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

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.

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?

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

```
S3#debug spanning-tree events
^
% Invalid input detected at '^' marker.

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

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.

spanning-tree mode rapid-pvst

```
S1(config)#spanning-tree mode rapid-pvst
S1(config)#
```

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

Коммутатор S2:

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

Коммутатор S3:

```
! These configuration commands, one per line
S3(config)#spanning-tree mode rapid-pvst
S3(config)#
```

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

Коммутатор S1:

```
S1#show running-config | include spa
S1#show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
S1#
```

Коммутатор S2:

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

Коммутатор S3:

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

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.

spanning-tree portfast

```
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)#
```

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

spanning-tree bpduguard enable

```
S1(config)#int f0/6
S1(config-if)#spanning-tree bpduguard enable
```

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

spanning-tree portfast default

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

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

spanning-tree portfast bpduguard default

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

Шаг 3: Проверьте сходимость Rapid PVST+.

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

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

Вопросы для защиты теоретической части (глава 12)

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

- Гибкость и мобильность: Позволяет передавать данные без необходимости использования проводов, что обеспечивает свободу перемещения для устройств и пользователей.
- Удобство установки: Не требует сложной установки проводов, что упрощает развертывание сетей в различных местах.
- Экономия ресурсов: Сокращает расходы на проводную инфраструктуру, так как не требуется прокладка кабелей.
- Расширяемость: Позволяет легко добавлять новые устройства в сеть без необходимости расширения проводной инфраструктуры.

Основные типы беспроводной связи включают:

- Wi-Fi (беспроводные локальные сети): Используется для беспроводного подключения устройств к сети Интернет в домах, офисах, общественных местах и т.д.
- Bluetooth: Применяется для краткодистанционной связи между устройствами, такими как смартфоны, наушники, клавиатуры и другие периферийные устройства.
- Cellular (мобильная связь): Обеспечивает подключение к Интернету через мобильные сети с использованием сотовых телефонов, планшетов и других поддерживающих устройств.
- RFID (радиочастотная идентификация): Используется для идентификации и отслеживания объектов с помощью радиочастотных меток.
- NFC (ближняя беспроводная связь): Применяется для обмена данными на короткие дистанции, например, для бесконтактной оплаты или передачи информации между устройствами.
- Zigbee и Z-Wave: Протоколы, используемые для создания сетей умного дома и для управления различными устройствами в домашней автоматизации.

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

Bluetooth используется для подключения периферийных устройств к компьютерам и смартфонам, обмена данными между мобильными устройствами, а также для управления умными устройствами.

Спутниковая широкополосная связь применяется для навигации (GPS) и глобальной коммуникации в удаленных или недоступных для проводной связи местах.

Технология MIMO разработана для увеличения пропускной способности, повышения надежности и улучшения покрытия беспроводных сетей.

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

Домашний беспроводной маршрутизатор может выполнять следующие роли:

- **Маршрутизация:** Он направляет сетевой трафик между устройствами в локальной сети и внешней сетью, такой как Интернет.
- **Беспроводной доступ:** Обеспечивает беспроводное подключение устройств к сети через Wi-Fi.
- **Безопасность:** Может предоставлять функции защиты сети, такие как брандмауэр и шифрование данных.

Беспроводные точки доступа используются для расширения зоны покрытия беспроводной сети. Они позволяют увеличить диапазон действия Wi-Fi и обеспечивают более равномерное распределение сигнала в больших помещениях или на больших территориях.

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

Категории точек доступа:

- **Домашние:** Для домашнего использования с базовыми функциями безопасности и ограниченным диапазоном покрытия.
- **Бизнес:** Для коммерческих помещений с расширенными функциями управления и большим диапазоном покрытия.
- **Облачные:** Управляемые через облачные сервисы для удаленного мониторинга и управления.

Варианты антенн:

- **Омни-антенна:** Равномерное покрытие во всех направлениях.
- **Направленная антенна:** Увеличение дальности сигнала в определенном направлении.
- **Секторная антенна:** Широкий угол покрытия.
- **Панельная антенна:** Узкий, но сильный сигнал в определенном направлении.
- **Дисконаправленная антенна:** Высокое усиление для связи на большие расстояния.

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

Характеристика режимов топологий беспроводной сети:

- **Ad-hoc (IBSS - Independent Basic Service Set):** Устройства соединяются непосредственно

друг с другом без использования центральной точки доступа. Подходит для временных сетей или сетей с небольшим количеством устройств.

- Infrastructure (BSS - Basic Service Set): Сеть, в которой устройства соединены через центральную точку доступа (AP). Это основной способ создания беспроводных сетей, таких как Wi-Fi.

Разница между BSS и ESS:

- BSS (Basic Service Set): Это базовый элемент беспроводной инфраструктуры, состоящий из точки доступа и всех подключенных к ней устройств. BSS обеспечивает соединение между устройствами в пределах одной ячейки покрытия.
- ESS (Extended Service Set): Это объединение нескольких BSS через мосты или проводную сеть. ESS позволяет устройствам перемещаться между разными BSS внутри сети, обеспечивая непрерывное беспроводное соединение при перемещении пользователя.

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

Принцип работы беспроводного клиента с методом CSMA/CA:

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance): Перед отправкой данных беспроводной клиент слушает канал на наличие активности. Если канал свободен, клиент начинает передачу данных. Если канал занят, клиент ждет случайное время и повторяет процесс.

Разница между пассивным и активным обнаружением точек доступа:

- Пассивное обнаружение точек доступа: Беспроводной клиент мониторит эфир на наличие сигналов от точек доступа без активной отправки запросов. Это более скрытый метод обнаружения, но требует длительного времени для поиска доступных сетей.
- Активное обнаружение точек доступа: Беспроводной клиент активно отправляет запросы на поиск сетей, отправляя запросы на частоты Wi-Fi-сетей. Это более быстрый метод обнаружения, но может быть более заметным для других устройств в сети.

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

Протокол CAPWAP (Control and Provisioning of Wireless Access Points) предназначен для управления и настройки беспроводными точками доступа (AP) в распределенных беспроводных сетях. Он обеспечивает следующие функции:

- Конфигурация и управление точками доступа: CAPWAP позволяет централизованно управлять настройками и обновлениями программного обеспечения для всех точек доступа в сети.
- Мониторинг и отладка: Протокол предоставляет возможности для мониторинга состояния и производительности точек доступа, а также для выявления проблем и их устранения.
- Безопасность: CAPWAP обеспечивает механизмы шифрования и аутентификации для защиты передаваемой информации и предотвращения несанкционированного доступа к устройствам.

Основные рекомендации по установке точек доступа включают:

- Выбор оптимального расположения: Разместите точку доступа в центре зоны покрытия, чтобы обеспечить равномерное покрытие всей области.
- Избегайте помех: Установите точку доступа вдалеке от других устройств, которые могут

создавать помехи в беспроводном диапазоне, например, микроволновок или беспроводных телефонов.

- **Настройка безопасности:** Включите шифрование Wi-Fi (например, WPA2) и установите надежные пароли для защиты сети от несанкционированного доступа.
- **Регулярное обновление ПО:** Поддерживайте программное обеспечение точек доступа в актуальном состоянии, чтобы исправлять уязвимости и обеспечивать стабильную работу.
- **Мониторинг производительности:** Регулярно мониторьте производительность сети и точек доступа, чтобы быстро реагировать на проблемы и оптимизировать работу сети.

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

Основные угрозы при использовании беспроводных точек доступа включают:

- **Несанкционированный доступ (Unauthorized Access):** Злоумышленники могут попытаться подключиться к беспроводной сети без разрешения, используя украденные учетные данные или взломанные ключи безопасности.
- **Перехват данных (Data Interception):** Злоумышленники могут пытаться перехватывать передаваемую по беспроводной сети информацию, такую как личные данные, пароли или конфиденциальные документы.
- **Атаки на сервисы (Service Attacks):** К злоумышленникам могут быть направлены атаки, целью которых является нарушение работы беспроводной сети, например, атаки на отказ в обслуживании (DoS) или атаки на переполнение буфера (Buffer Overflow).
- **Фальшивые точки доступа (Rogue Access Points):** Злоумышленники могут размещать фальшивые точки доступа, которые пытаются подменить настоящие сети для перехвата трафика или кражи учетных данных.
- **Атаки на службу аутентификации (Authentication Service Attacks):** Злоумышленники могут атаковать службы аутентификации, чтобы получить несанкционированный доступ к сети или прервать ее работу.

Типы аутентификации в беспроводной связи включают:

- **Открытая система (Open System):** Все устройства могут подключиться к сети без аутентификации.
- **WEP (Wired Equivalent Privacy):** Устаревший протокол шифрования, который использует общий ключ для аутентификации и шифрования данных.
- **WPA (Wi-Fi Protected Access):** Более безопасный протокол, который использует персональные и предварительно распределенные ключи для шифрования данных.
- **WPA2 (Wi-Fi Protected Access 2):** Еще более безопасный протокол, который использует аутентификацию с помощью протокола EAP (Extensible Authentication Protocol) и AES (Advanced Encryption Standard) для шифрования данных.
- **WPA3 (Wi-Fi Protected Access 3):** Последняя версия протокола WPA, которая предлагает более надежную защиту с помощью более сложных методов шифрования и аутентификации.

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

Протокол RADIUS (Remote Authentication Dial-In User Service) используется для централизованной аутентификации, авторизации и учета пользователей, подключающихся к сети. Он часто применяется в корпоративных сетях, интернет-провайдерах и беспроводных сетях для обеспечения безопасного доступа.

Методы аутентификации домашнего пользователя включают:

- Использование пароля (Password-based authentication): Пользователь предоставляет идентификационное имя и пароль для проверки подлинности.
- Ключевые карты (Token-based authentication): Пользователь использует уникальный физический токен (например, смарт-карту или USB-ключ) для подтверждения своей личности.
- Биометрическая аутентификация (Biometric authentication): Пользователь использует биометрические данные (например, отпечаток пальца или распознавание лица) для проверки подлинности.
- Сертификаты (Certificate-based authentication): Пользователь использует цифровой сертификат для аутентификации, который был выдан доверенным центром сертификации.