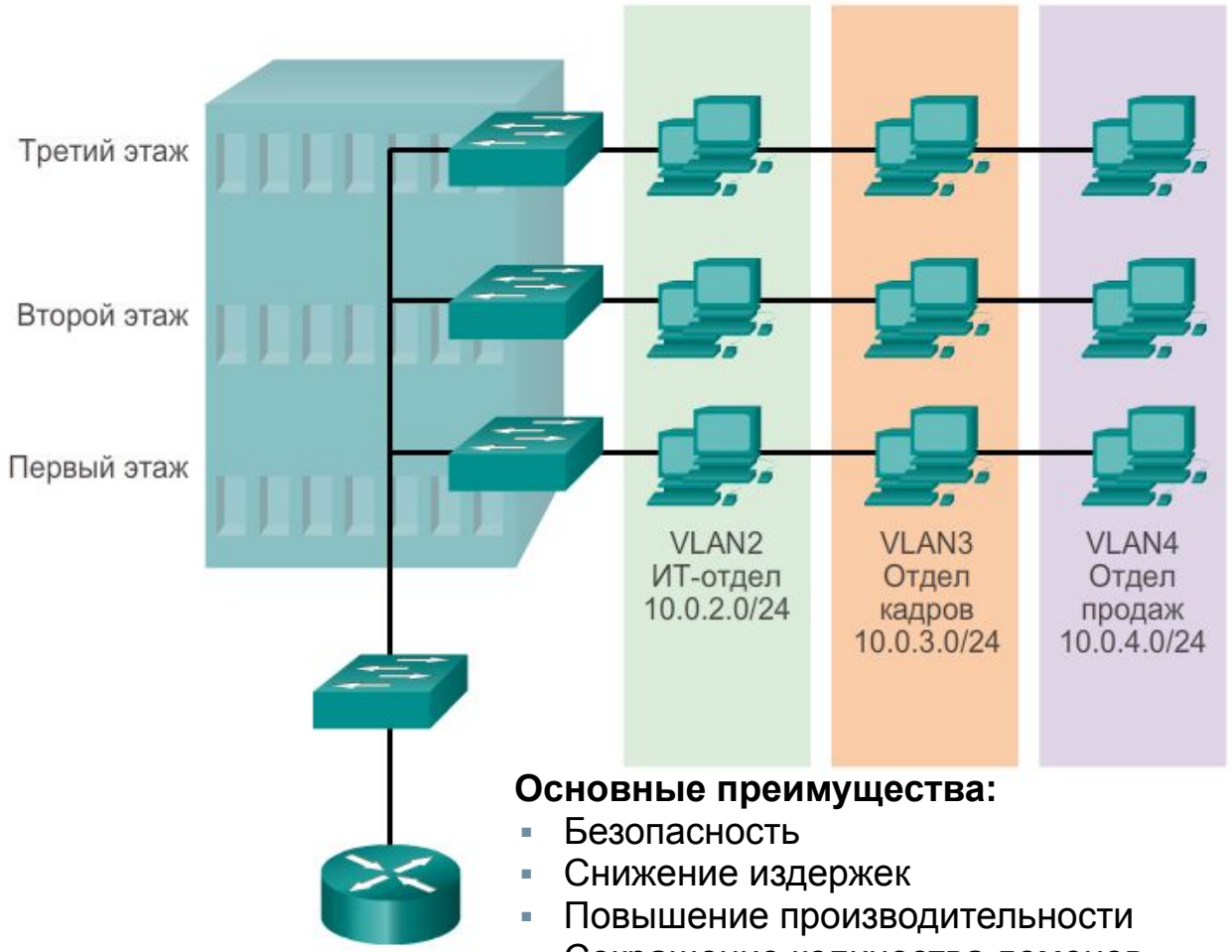
Виртуальные локальные сети (VLAN)

Маршрутизация и коммутация

Cisco | Networking Academy®
Mind Wide Open™

Определение VLAN



Основные преимущества:

- Безопасность
- Снижение издержек
- Повышение производительности
- Сокращение количества доменов широковещательной рассылки
- Упрощенная форма управления проектами и приложениями

Основные понятия:

- VLAN (виртуальная LAN) — это результат логического разделения сети уровня 2.
- Можно создать несколько разделов, позволяющих сосуществовать нескольким VLAN.
- Каждая VLAN является широковещательным доменом и в большинстве случаев имеет собственную IP-сеть.
- Сети VLAN взаимно изолированы, и пакеты между ними могут передаваться только через маршрутизатор.
- Группы узлов внутри VLAN не знают о существовании VLAN.
- Процедура разделения сети уровня 2 также задействует устройство уровня 2, чаще всего коммутатор.

Типы сетей VLAN

- VLAN передачи данных настроена специально для передачи трафика, генерируемого пользователем.
- VLAN по умолчанию. Все порты коммутатора становятся частью VLAN по умолчанию после первоначальной загрузки коммутатора. Порты коммутатора, находящиеся в сети VLAN по умолчанию, являются частью одного широковещательного домена. Сетью VLAN по умолчанию для коммутаторов Cisco установлена VLAN 1.
- Native VLAN назначена транковому порту 802.1Q. Транковые порты — это каналы между коммутаторами, которые поддерживают передачу трафика, связанного с более чем одной сетью VLAN. Рекомендуется настроить native VLAN как неиспользуемую VLAN, отличающуюся от сети VLAN 1 и других VLAN.
- VLAN управления настроена для доступа к функциям управления коммутатора. Сеть VLAN 1 по умолчанию является управляющей VLAN. Для создания управляющей VLAN интерфейсу SVI коммутатора данной VLAN назначаются IP-адрес и маска подсети.

Краткий обзор сетей VLAN

Типы сетей VLAN

VLAN 1

```
Switch# 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
                                   Gi0/1,  Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

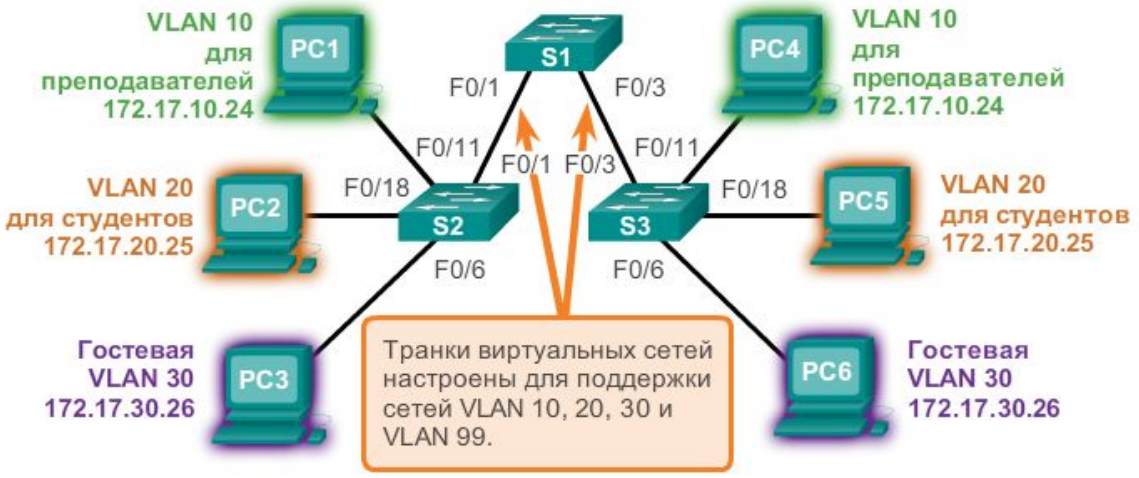
- Все порты назначены сети VLAN 1 для пересылки данных по умолчанию.
- Сетью native VLAN по умолчанию является сеть VLAN 1.
- Сетью управления VLAN по умолчанию является сеть VLAN 1.
- VLAN 1 нельзя переименовывать или удалять.

VLAN в среде со множеством коммутаторов

Транковые каналы VLAN

VLAN 10 для преподавателей и сотрудников — 172.17.10.0/24
VLAN 20 для учащихся — 172.17.20.0/24
Гостевая VLAN 30 — 172.17.30.0/24
VLAN 99 сеть native и управляющая сеть— 172.17.99.0/24.

Порты F0/1-5 — это транковые интерфейсы 802.1Q, настроенные с сетью native VLAN 99.
Порты F0/11-17 принадлежат сети VLAN 10.
Порты F0/18-24 принадлежат сети VLAN 20.
Порты F0/6-10 принадлежат сети VLAN 30.

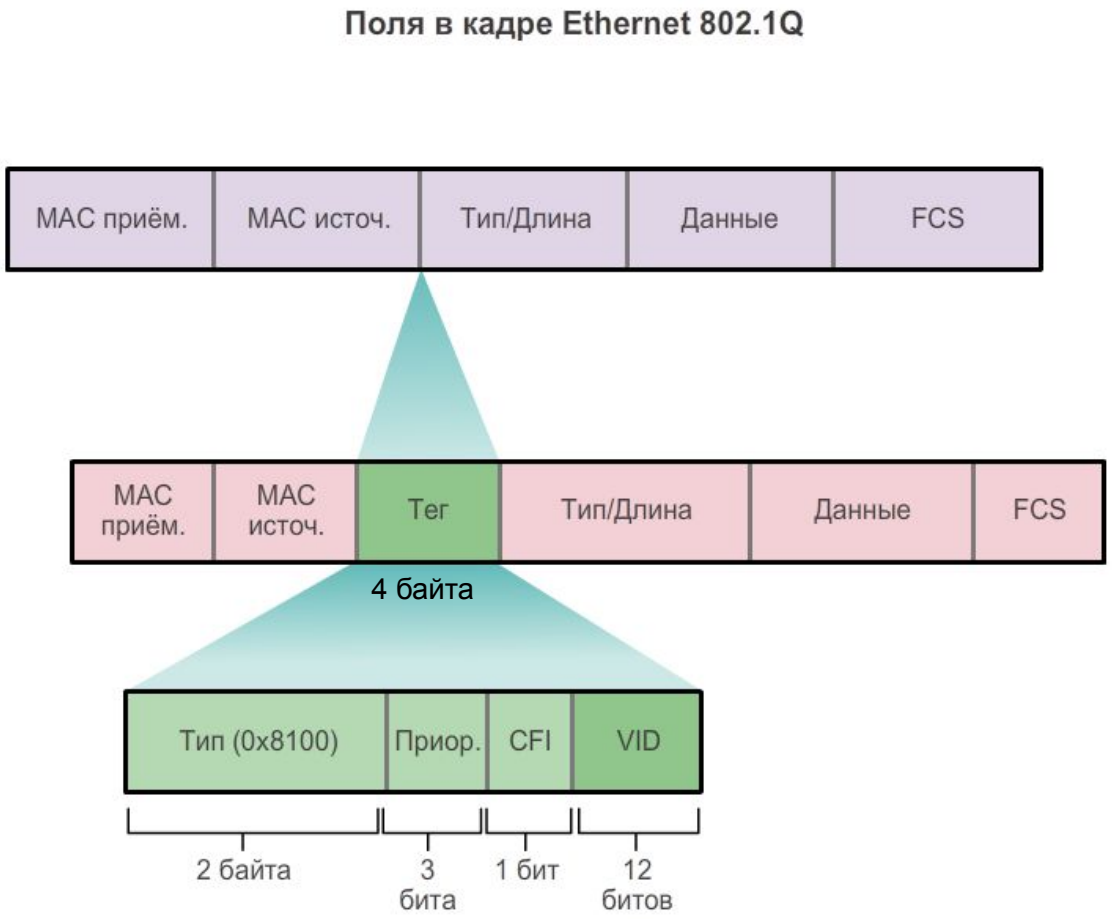


- Транковый канал VLAN поддерживает работу более одной VLAN.
- Обычно транковый канал устанавливается **между коммутаторами** для возможности связи между устройствами одной VLAN, даже если физически они подключены к разным коммутаторам.
- Транковый канал VLAN не принадлежит ни одной VLAN.
- ОС Cisco IOS поддерживает известный транковый протокол VLAN — стандарт IEEE802.1q.

Присвоение меток кадрам Ethernet для идентификации VLAN

- Присвоение **меток кадрам** используется в целях правильной **передачи множества кадров VLAN через транковый канал**.
- Метки присваиваются кадрам **коммутаторами** для определения той VLAN, которой эти кадры принадлежат. Существуют различные протоколы распределения меток (или тегирования), среди которых одним из наиболее распространённых протоколов является стандарт IEEE 802.1q.
- Метка VLAN **присваивается** кадру коммутатором **до перемещения кадра по транковому каналу** и **удаляется до пересылки кадра через нетранковый порт**.
- Кадры с соответствующей меткой могут пересекать **любое количество коммутаторов через транковый канал**, и всё равно будут направлены в правильную VLAN назначения.
- Кадру, принадлежащему **native VLAN**, не присваивается метка. Если нет связанных с native VLAN портов и никаких других транковых каналов, не отмеченный меткой кадр отбрасывается.

Присвоение меток кадрам Ethernet для идентификации VLAN



Тип — это 2-байтовое значение, которое называется значением идентификатора протокола тегирования (TPID). Значение для Ethernet имеет вид шестнадцатеричного числа ***0x8100***.

Приоритет пользователя — это 3-битовое значение, которое поддерживает реализацию уровня или сервиса.

Идентификатор канонического формата (CFI) — это 1-битовый идентификатор, который обеспечивает передачу кадров Token Ring по каналам Ethernet.

VLAN-идентификатор (VID) — это 12-битный идентификационный **номер VLAN**, который поддерживает до ***4096*** идентификаторов VLAN.

Диапазоны VLAN на коммутаторах Catalyst

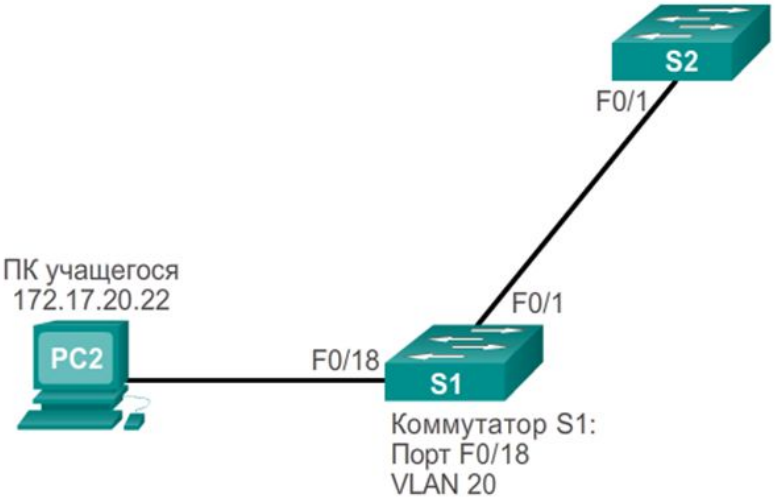
- Коммутаторы Catalyst серий 2960 и 3560 способны поддерживать более 4 000 сетей VLAN.
- Данные сети VLAN можно разделить на две категории.
- К первой категории относятся сети VLAN стандартного диапазона.
  - Сюда относятся сети VLAN с номерами от 1 до 1 005.
  - Конфигурации хранятся в файле флеш-памяти vlan.dat.
  - Протокол VTP, служащий для обмена информацией о VLAN, имеющихся на выбранном транковом порту, может узнавать и хранить только сети VLAN стандартного диапазона.
- Вторая категория — это сети VLAN расширенного диапазона.
  - К данным сетям VLAN относятся сети с номерами от 1 006 до 4 096.
  - Конфигурации хранятся в энергонезависимом ОЗУ (NVRAM) в файле текущей конфигурации.
  - Протокол VTP не распознаёт сети VLAN расширенного диапазона.

Назначение VLAN

Создание VLAN

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	`S1# configure terminal`
Создайте сеть VLAN с допустимым номером идентификатора.	`S1(config)# vlan vlan-id`
Укажите уникальное имя для идентификации сети VLAN.	`S1(config-vlan)# name vlan-name`
Вернитесь в привилегированный режим.	`S1(config-vlan)# end`

```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```



Назначение VLAN

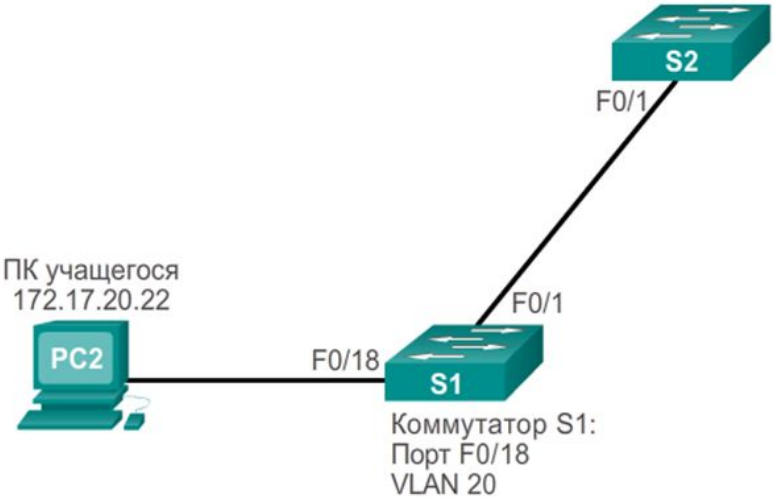
Назначение портов сетям VLAN

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	`S1# configure terminal`
Войдите в режим конфигурации интерфейса для SVI.	`S1(config)# interface` *interface_id*
Переведите порт в режим доступа.	`S1(config-if)# switchport mode access`
Назначьте порт сети VLAN.	`S1(config-if)# switchport access vlan` *vlan_id*
Вернитесь в привилегированный режим.	`S1(config-if)# end`

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```

```
S1# 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
                                 Gi0/1, Gi0/2
20   student             active    Fa0/18
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
S1#
```



Назначение VLAN

Изменение принадлежности портов VLAN

```
S1(config)# int fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# 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
                                 Gi0/1, Gi0/2
20   student             active
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
S1#
```

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh 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, Fa0/12, Fa0/13
                                    Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                    Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                    Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
```

```
S1# config t
S1(config)# int fa0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# 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, Fa0/12, Fa0/1
                                     Fa0/14, Fa0/15, Fa0/16, Fa0/
                                     Fa0/18, Fa0/19, Fa0/20, Fa0/
                                     Fa0/22, Fa0/23, Fa0/24, Gi0/
                                     Gi0/2
20   student              active     Fa0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Назначение VLAN

Проверка информации о VLAN

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0

S1#
```

```
S1#show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia
001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Настройка транковых каналов по стандарту IEEE 802.1q

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	`S1# configure terminal`
Войдите в режим конфигурации интерфейса для SVI.	`S1(config)# interface` *interface_id*
Настройте канал в качестве транкового.	`S1(config-if)# switchport mode trunk`
Укажите сеть native VLAN для транков 802.1Q без меток.	`S1(config-if)# switchport trunk native vlan` *vlan_id*
Укажите список сетей VLAN, которым разрешён доступ в транковый канал.	`S1(config-if)# switchport trunk allowed vlan` *vlan-list*
Вернитесь в привилегированный режим.	`S1(config-if)# end`

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

Сброс настроек транкового канала до состояния по умолчанию

```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<выходные данные опущены>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<выходные данные опущены>
```

Возвращение порта в режим доступа

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<выходные данные опущены>
```

Проверка конфигурации транкового канала

Проверка конфигурации транкового канала

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<выходные данные опущены>
```

Динамический протокол транковых каналов

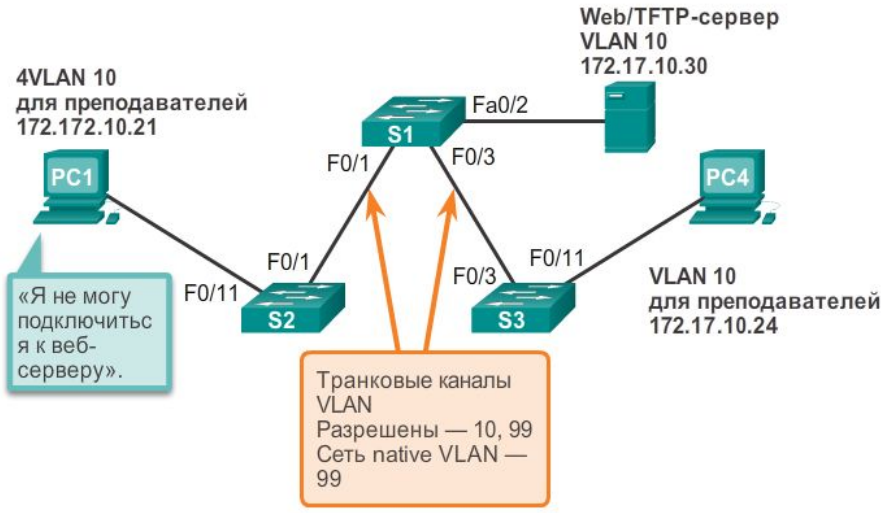
Режимы интерфейса для согласования

- Порты коммутатора можно настроить вручную для создания транковых каналов.
- Порты коммутатора также можно настроить для согласования и установления транкового канала с подключённым узлом.
- **Динамический протокол транковых каналов** (DTP) — это протокол **для управления согласованием транковых каналов**.
- DTP является собственным протоколом Cisco. Он по умолчанию доступен на коммутаторах Cisco Catalyst серии 2960 и серии 3560.
- Если порт на соседнем коммутаторе настроен в транковом режиме, поддерживающем протокол DTP, то согласованием управляет этот порт.
- По умолчанию протокол DTP на коммутаторах Cisco Catalyst 2960 и 3560 настроен с конфигурацией **dynamic auto**.
- На коммутаторах Cisco Catalyst 2960 и 3560 поддерживаются следующие транковые режимы:
  - dynamic auto (динамический автоматический)
  - dynamic desirable (динамический рекомендуемый)
  - Trunk (транк)
  - Nonegotiate (доступ)

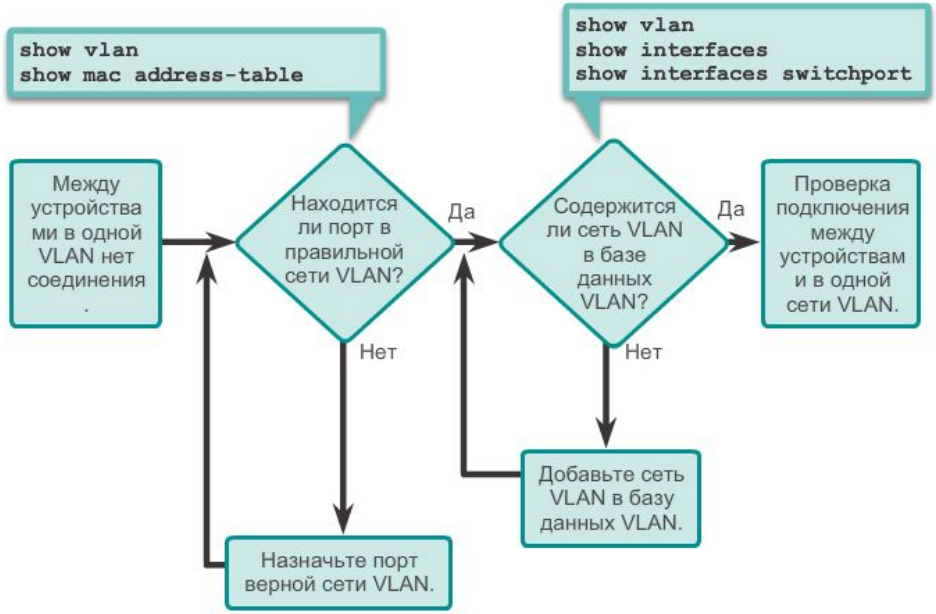
	Динамический автоматический	Динамический рекомендуемый	Транк	Доступ
Динамический автоматический	Доступ	Транк	Транк	Доступ
Динамический рекомендуемый	Транк	Транк	Транк	Доступ
Транк	Транк	Транк	Транк	Ограниченные возможности подключения
Доступ	Доступ	Доступ	Ограниченные возможности подключения	Доступ

Проблемы адресации VLAN

- Настоятельно рекомендуется связывать VLAN с IP-сетью.
- Поскольку разные IP-сети поддерживают связь только через маршрутизатор, **все устройства внутри VLAN должны быть частью такой же IP-сети**, чтобы иметь возможность обмениваться информацией.
- На рисунке *PC1* не может связаться с сервером, поскольку у него *неверно настроен IP-адрес*.



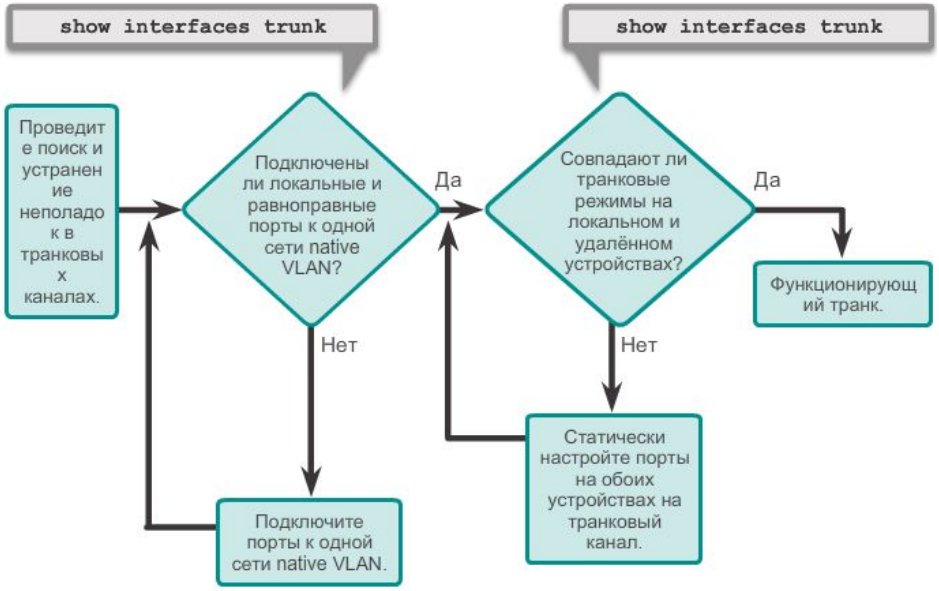
Отсутствующие VLAN



- Если все причины, по которым не совпадают IP-адреса, были устранены, а устройства до сих пор не могут установить связь, проверьте, **настроена ли VLAN на коммутаторе**.
- Примените команду **switchport trunk allowed vlan** для определения, каким VLAN разрешено отправлять кадры через транковый канал.

- **Наиболее распространённые ошибки конфигурации транковых каналов**:
  1. Несовпадение native VLAN;
  2. Несовпадение транковых режимов;
  3. Разрешённые VLAN на транковых каналах.

- Проверьте состояние транковых портов на коммутаторах при помощи команды **show interfaces trunk**.

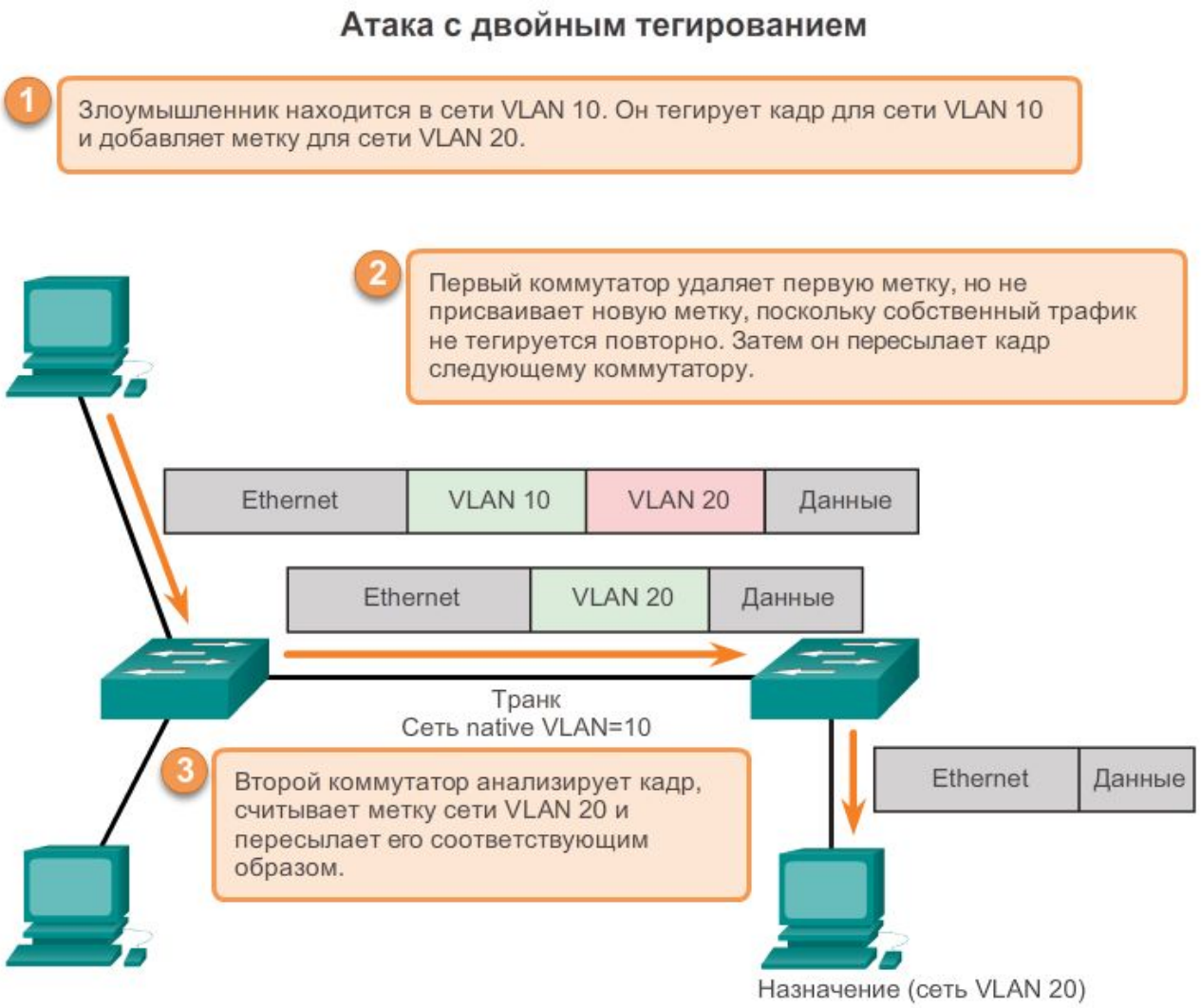


Атаки на сети VLAN

Спуфинг-атака на коммутатор

- В современных коммутируемых сетях существует несколько типов атак. Одной из них является атака **VLAN hopping**.
- **По умолчанию** порт коммутатора настроен с конфигурацией **dynamic auto**.
- ***Путём настройки узла в качестве коммутатора и создания транкового канала злоумышленник может получить доступ к любой VLAN в сети***. Злоумышленник теперь может получить доступ к другим VLAN.
- Для предотвращения основной спуфинг-атаки на коммутатор необходимо **отключить транковую связь на всех портах, за исключением тех, на которых транковая связь необходима**.

Атака с использованием дважды тегированного трафика



- Большинство коммутаторов выполняют только один уровень деинкапсуляции 802.1Q, что позволяет взломщику внедрить второй, не авторизованный, атакующий заголовок в кадр.
- После удаления первого, легального заголовка 802.1Q коммутатор пересылает кадр в VLAN, заданную неавторизованным заголовком 802.1Q.
- Лучший способ сдержать атаку с применением дважды тегированного трафика — **гарантированное отличие native VLAN транкового порта от VLAN любого пользовательского порта**.

Периметр частной VLAN (PVLAN)

- Функция периметра частной VLAN (PVLAN), также известная как **функция защищённых портов**, ***гарантирует отсутствие трафика одноадресной передачи, широковещательной или многоадресной рассылок между защищёнными портами коммутатора***.
- PVLAN имеет только локальную значимость.
- Обмен трафиком через защищённый порт может производиться только с незащищёнными портами.
- Обмен трафиком между защищёнными портами не осуществляется.


```
S1(config)# interface g0/1
S1(config-if)# switchport protected
S1(config-if)# end
S1# show interfaces g0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<выходные данные опущены>

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

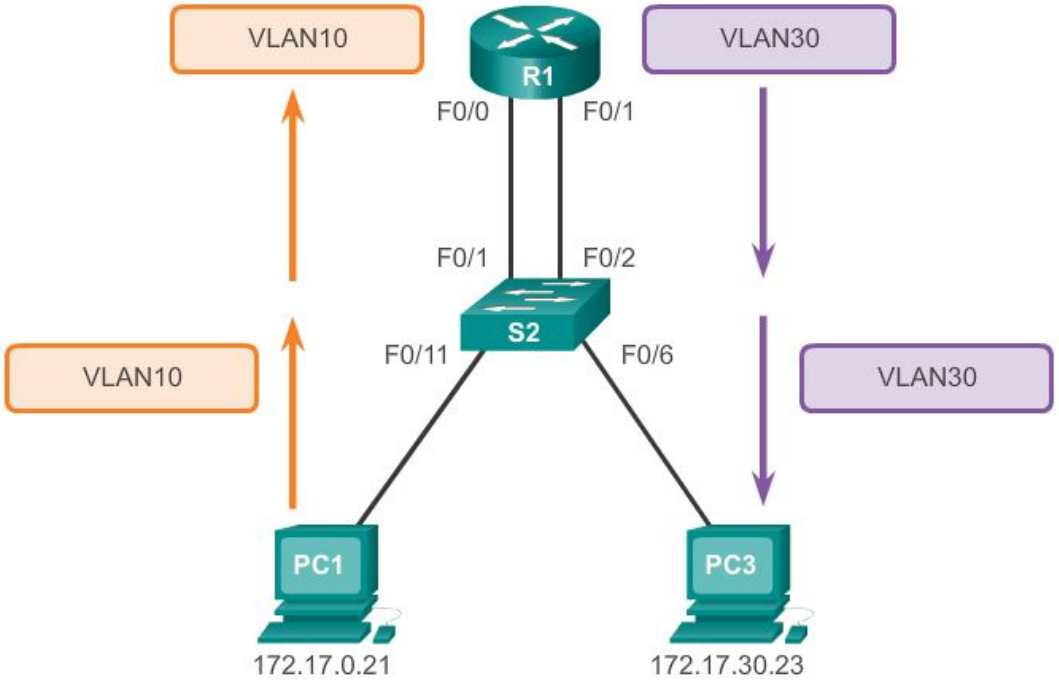
Практические рекомендации по проектированию VLAN

Указания по проектированию VLAN

- Переместите все порты из VLAN1 и назначьте их неиспользуемой VLAN.
- Отключите все неиспользуемые порты коммутатора.
- Разделите трафик управления и трафик пользовательских данных.
- Измените VLAN управления на VLAN, отличную от VLAN1. Сделайте то же самое для native VLAN.
- Убедитесь, что к коммутатору могут подключаться для конфигурирования только устройства из VLAN управления.
- На коммутаторе должны быть разрешены только SSH-подключения.
- Отключите функцию автосогласования на транковых портах.
- Не используйте режимы **switchport mode dynamic auto** и **switchport mode dynamic desirable**.

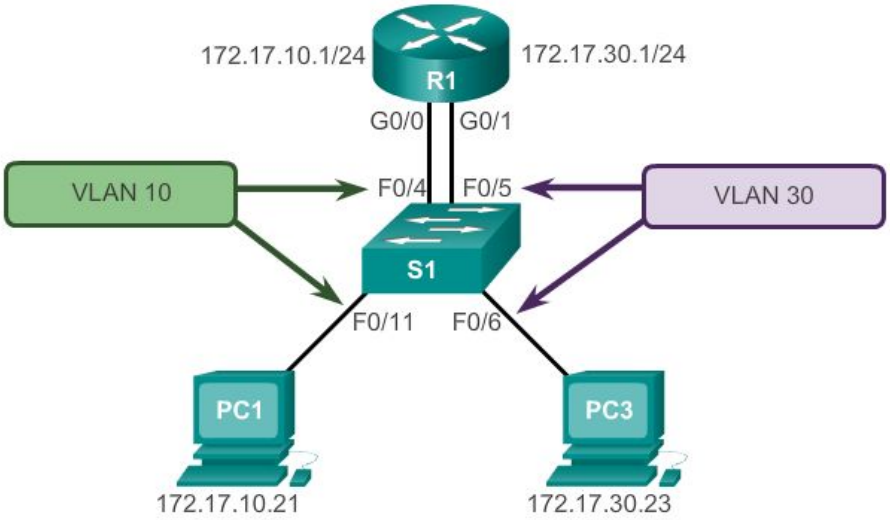
Что такое маршрутизация между VLAN

- Коммутаторы уровня 2 не могут пересылать трафик между VLAN без помощи маршрутизатора.
- Маршрутизация между VLAN — это процесс пересылки сетевого трафика из одной VLAN в другую с помощью маршрутизатора.



Устаревший метод маршрутизации между VLAN

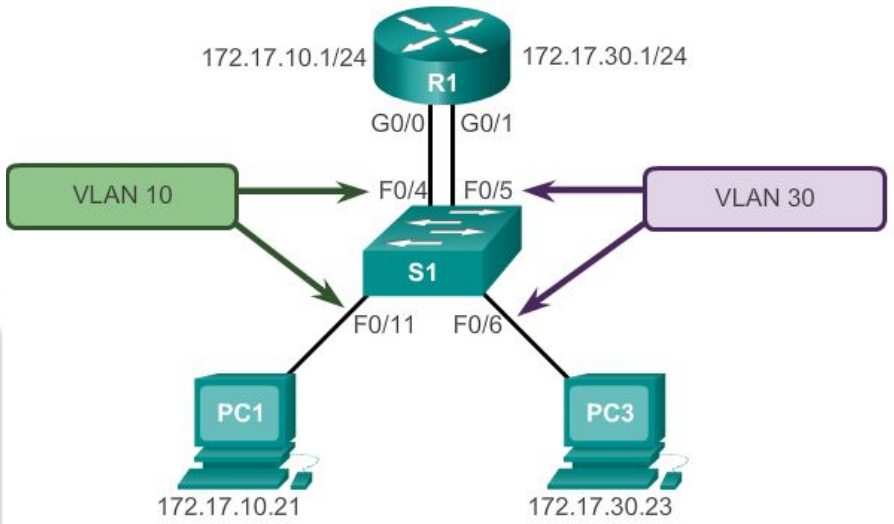
- В прошлом действующие маршрутизаторы использовались для маршрутизации между VLAN.
- Каждая VLAN была подключена к отдельному физическому интерфейсу маршрутизатора.
- Пакеты поступали на маршрутизатор через один интерфейс, маршрутизировались и покидали маршрутизатор через другой интерфейс.
- Поскольку интерфейсы маршрутизатора были подключены к VLAN и имели IP-адреса из общего с соответствующей VLAN адресного пространства, достигалась маршрутизация между VLAN.
- Это простое решение, однако едва ли имеющее возможности масштабирования. Крупные сети с большим количеством VLAN потребовали бы огромного количества интерфейсов маршрутизаторов.



Настройка маршрутизации между VLAN по устаревшему методу

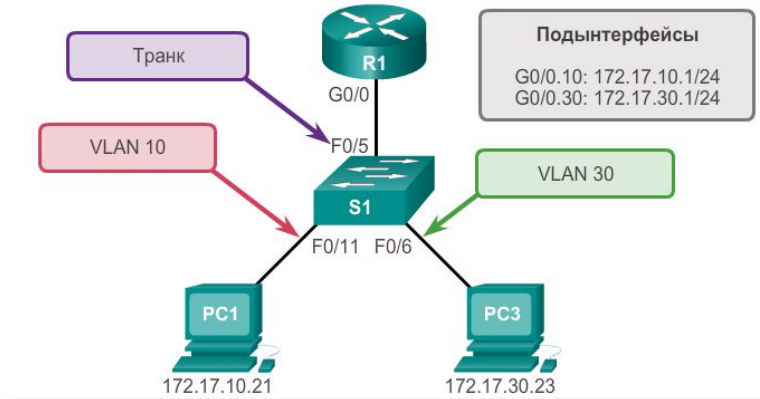
```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/11
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/4
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/6
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/5
S1(config-if)# switchport access vlan 30
S1(config-if)# end
*Mar 20 01:22:56.751: %SYS-5-CONFIG_I: Configured from console by
console
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:12.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 01:42:13.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:54.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/1,
changed state to up
*Mar 20 01:42:55.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)# end
R1# copy running-config startup-config
```



Маршрутизация между VLAN с использованием конфигурации router-on-a-stick «маршрутизатор на палочке» (ROS)

- Один из физических интерфейсов маршрутизатора настраивается в качестве транкового порта 802.1Q. Теперь этот порт может распознавать метки VLAN.
- Затем создаются логические подынтерфейсы. По одному подынтерфейсу для каждой VLAN
- Каждый подынтерфейс настраивается с IP-адресом, полученным от той VLAN, которую он представляет.
- Участники (узлы) VLAN настраиваются для использования адреса подынтерфейса в качестве шлюза по умолчанию.
- Используется только один из физических интерфейсов маршрутизатора.




```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 Interface GigabitEthernet0/0, changed state to up
```

Проверка подынтерфейсов и маршрутизации

```
R1# show vlans
<выходные данные опущены>
Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.10

  Protocols Configured:  Address:     Received:   Transmitted:
          IP             172.17.10.1         11             18
<выходные данные опущены>
Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.30

  Protocols Configured:  Address:     Received:   Transmitted:
          IP             172.17.30.1         11              8
<выходные данные опущены>
```

```
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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP,
       l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

   172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C      172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L      172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C      172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L      172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

- Возможность доступа к устройствам в удалённых VLAN можно проверить с помощью команды **ping**. VLAN отправляет эхо-запрос ICMP на адрес назначения. Когда узел получает эхо-запрос ICMP, он отправляет эхо-ответ ICMP.
- Команда **tracert** — полезный инструмент для подтверждения существования пути между двумя устройствами.

Маршрутизация между VLAN через многоуровневый коммутатор 3 уровня

- Многоуровневые коммутаторы могут выполнять функции коммутаторов уровня 2 и уровня 3. Маршрутизаторы больше не требуются
- Каждая VLAN, настроенная на коммутаторе, представляет собой SVI (виртуальный интерфейс коммутатора).
- SVI выступают как интерфейсы уровня 3.
- Коммутатор понимает протокольные блоки данных на сетевом уровне и, следовательно, может маршрутизировать их между SVI, подобно тому как это делает маршрутизатор.
- При использовании многоуровневого коммутатора трафик маршрутизируется внутри коммутатора.
- Такое решение легко масштабируется.

Протокол DHCP.

Основы маршрутизации и коммутации

Cisco | Networking Academy®
Mind Wide Open™

Введение

Протокол динамической конфигурации узла (DHCP) — это сетевой протокол, обеспечивающий автоматическую IP-адресацию и другую информацию для клиента:

- IP-адрес.
- Маска подсети (IPv4) или длина префикса (IPv6).
- Адрес шлюза по умолчанию.
- Адрес DNS-сервера.

Общие сведения о протоколе DHCPv4

DHCPv4 использует три разных метода присвоения адреса:

Распределение вручную — администратор присваивает устройству-клиенту предварительно выделенный IPv4-адрес, в то время как DHCPv4 только передаёт IPv4-адрес к устройству.

Автоматическое распределение — DHCPv4 автоматически присваивает устройству постоянный ***статический*** IPv4-адрес, выбирая его из пула доступных адресов. Аренда не требуется.

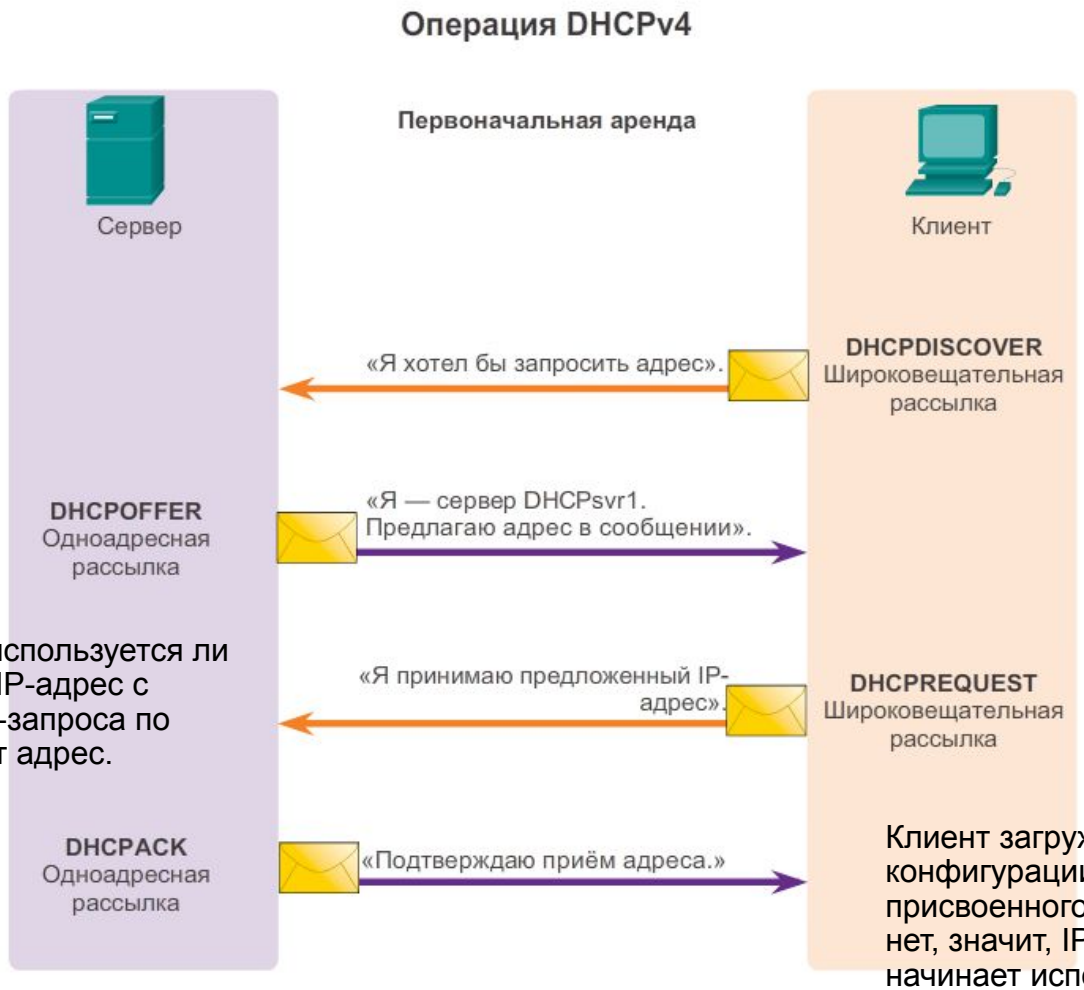
Динамическое распределение — DHCPv4 динамически присваивает или выдаёт в аренду IPv4-адрес из пула адресов на ограниченный период времени по выбору сервера или до тех пор, пока у клиента есть необходимость в адресе. Наиболее распространённый метод.

Общие сведения о протоколе DHCPv4

Резервирование доступных IPv4-адресов для выдачи в аренду клиенту. Создание записи ARP, состоящей из MAC-адреса запрашивающего клиента и выданного клиенту IPv4-адреса. DHCPv4-сервер посылает сообщение привязки DHCPOFFER запрашивающему клиенту.

Сервер проверяет, не используется ли выдаваемый в аренду IP-адрес с помощью отправки эхо-запроса по протоколу ICMP на этот адрес.

После этого сервер создаёт новую запись ARP для клиентской аренды и отвечает сообщением одноадресной рассылки DHCPACK.



Сообщение DHCPDISCOVER широковещательной рассылки со своего MAC-адреса с целью обнаружения доступных DHCPv4-серверов.

Сообщение DHCPREQUEST используется как для первоначальной аренды адреса, так и для её продления. Когда сообщение используется при первоначальной аренде, DHCPREQUEST служит уведомлением о принятии предложения привязки к предложенным сервером параметрам и косвенным отклонением для всех других серверов, которые могли предоставить клиенту предложение привязки.

Клиент загружает информацию о конфигурации и выполняет ARP-проверку присвоенного адреса. Если ARP-ответа нет, значит, IPv4-адрес доступен, и клиент начинает использовать его в качестве собственного.

Принцип работы протокола DHCPv4

Формат сообщений DHCPv4

<table>
<tr><th>8</th><th>16</th><th>24</th><th>32</th></tr>
<tr><td>Код операции (1)
Общий тип сообщения:
1 – сообщение-запрос;
2 — сообщение-ответ.</td><td colspan="2">Тип оборудования (1)
Тип аппаратного оборудования:
1 — Ethernet,
15 — Frame Relay, 20 — последовательный канал и т. д. Эти же коды используются в сообщениях ARP.</td><td>Длина физического адреса (1)</td><td>Переходы (1)
Управление процессом пересылки сообщений. Устанавливается клиентом на 0 перед отправкой сообщения-запроса.</td></tr>
<tr><td colspan="4">Идентификатор транзакции (4) - используется клиентом для согласования запроса с ответами от DHCPv4-серверов.</td></tr>
<tr><td colspan="2">Секунды (2) – количество секунд с момента, когда клиент начал пытаться получить или продлить аренду. Используется DHCPv4-серверами для расстановки приоритетности ответов, в случае нескольких клиентских запросов.</td><td colspan="2">Флаги (2) - применяются клиентом, который не знает своего IPv4-адреса при отправлении запроса. Используется только один из 16 бит. Значение 1 в этом поле сообщает DHCPv4-серверу или агенту-ретранслятору, принимающему запрос, что ответ должен быть послан в форме широковещательной рассылки.</td></tr>
<tr><td colspan="4">IP-адрес клиента (4) – используется клиентом при обновлении адреса по истечении срока аренды для продления аренды. Клиент подставляет собственный IPv4-адрес в это поле только в случае, если у него есть действующий IPv4-адрес, совпадающий с ранее назначенным; в противном случае значение поля устанавливается на 0.</td></tr>
<tr><td colspan="4">Ваш IP-адрес (4) – используется сервером для присвоения нового IPv4-адреса клиенту.</td></tr>
<tr><td colspan="4">IP-адрес сервера (4) – применяется сервером для распознавания адреса сервера, который клиент должен использовать для следующего шага в процессе самонастройки. Этот сервер может являться (или не являться) сервером, посылающим ответ. Сервер, посылающий ответ, всегда включает собственный IPv4-адрес в отдельное поле - опцию Идентификатор сервера DHCPv4.</td></tr>
<tr><td colspan="4">IP-адрес шлюза (4) – Использование адреса шлюза упрощает передачу DHCPv4- запросов и ответов между клиентом и сервером, которые находятся в разных подсетях или сетях.</td></tr>
<tr><td colspan="4">Физический адрес клиента (16)</td></tr>
<tr><td colspan="4">Имя сервера (64) – необязательно для заполнения, используется сервером, отправляющим сообщения DHCPOFFER или DHCPACK. Именем сервера может быть простой текстовый псевдоним или доменное имя DNS-сервера.</td></tr>
<tr><td colspan="4">Имя файла загрузки (128) – используется клиентом для запроса файла загрузки в сообщении DHCPDISCOVER и сервером в сообщении DHCPOFFER для точного задания директории файла загрузки и имени файла.</td></tr>
<tr><td colspan="4">Параметры DHCP (размер не задан) – опции DHCP, а также некоторые параметры, необходимые для основных операций протокола DHCP. Длина этого поля меняется. Поле может использоваться как клиентом, так и сервером.</td></tr>
</table>

Сообщения обнаружения и предложения DHCPv4

Кадр Ethernet	IP	UDP	DHCPDISCOVER
DST MAC: FF:FF:FF:FF:FF:FF SRC MAC: MAC A	IP SRC: 0.0.0.0 IP DST: 255.255.255.255	UDP 67	CIADDR: 0.0.0.0 GIADDR: 0.0.0.0 Маска: 0.0.0.0 CHADDR: MAC A

MAC: адрес управления доступом к среде передачи данных
CIADDR: IP-адрес клиента
GIADDR: IP-адрес шлюза
CHADDR: аппаратный адрес клиента

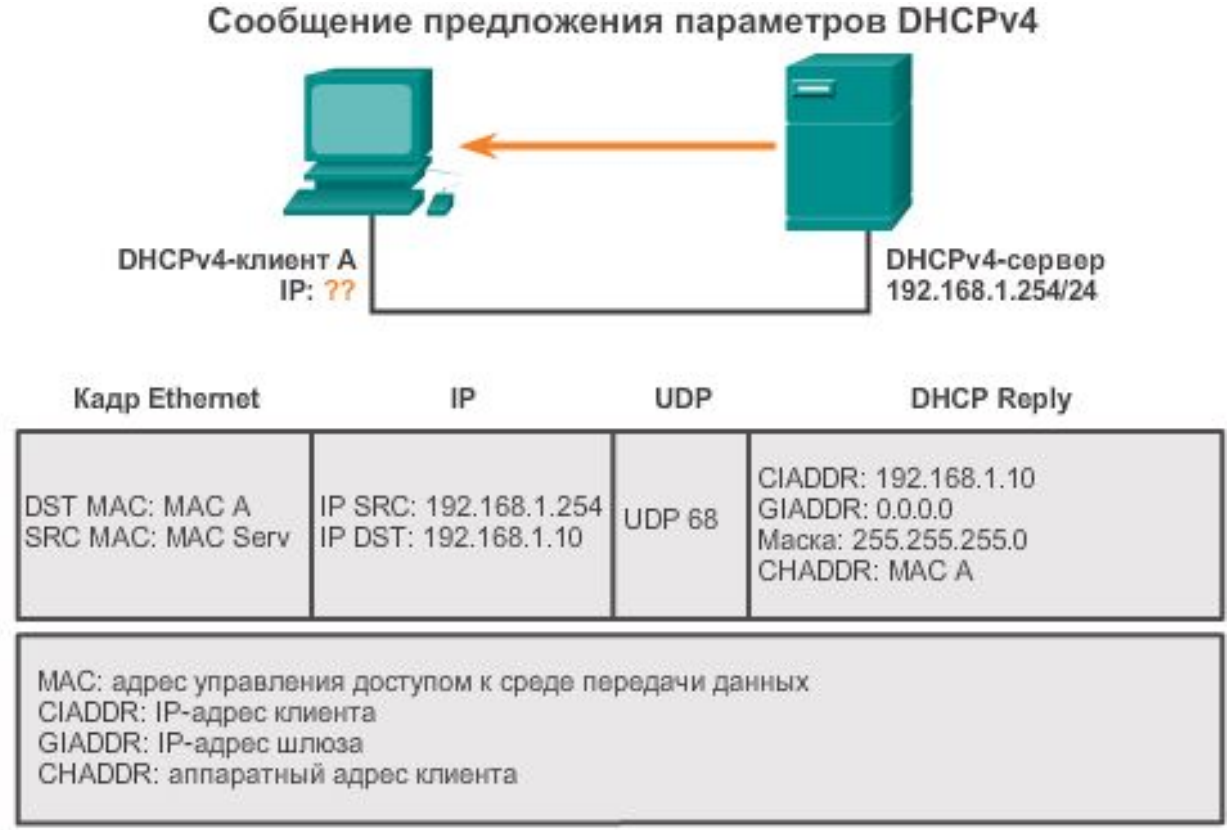
DHCP-клиент посылает направленную широковещательную IP-рассылку с DHCPDISCOVER-пакетом. В этом примере DHCP-сервер находится в том же сегменте и принимает этот запрос. Сервер отмечает, что поле GIADDR пустое, таким образом, клиент находится в том же сегменте. Сервер также отмечает физический адрес клиента в пакете запроса.

Сообщение **DHCPDISCOVER** представляет собой широковещательную рассылку IPv4 (IPv4-адрес назначения 255.255.255.255).

Поскольку у клиента ещё нет настроенного IPv4-адреса, используется IPv4-адрес источника — 0.0.0.0.

IPv4-адрес клиента (CIADDR), адрес основного шлюза (GIADDR) и маска подсети в сообщении DHCPDISCOVER соответствуют используемому адресу 0.0.0.0.

Сообщения обнаружения и предложения DHCPv4



DHCPv4-сервер отвечает на сообщение DHCPDISCOVER сообщением **DHCPOFFER**. Это сообщение содержит предварительные настройки для клиента: IPv4-адрес клиента, предложенный сервером, маску подсети, срок аренды и IPv4-адрес DHCPv4-сервера, от которого исходит предложение.

Сообщение DHCPOFFER может быть также настроено для содержания дополнительных данных, таких как время обновления аренды и адрес DNS-сервера.

Сервер DHCP отвечает на сообщение DHCPDISCOVER, высылая значения IP-адреса (CIADDR) и маски подсети. Используя физический адреса устройства-клиента (CHADDR), сервер создаёт и отправляет кадр запрашивающему клиенту.

Для завершения процесса клиент и сервер отправляют сообщения подтверждения.

Конфигурация сервера DHCPv4. Проверка.

- Маршрутизатор Cisco под управлением ОС Cisco IOS можно настроить в качестве DHCPv4-сервера. Для настройки протокола DHCP:

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

1. Исключите адреса из пула.
2. Задайте имя пула DHCP.
3. Определите диапазон адресов и маску подсети.
4. Назначьте шлюз по умолчанию.
5. Дополнительные элементы, которые можно включить в пул — сервер DNS, имя домена.

- Команды проверки DHCP

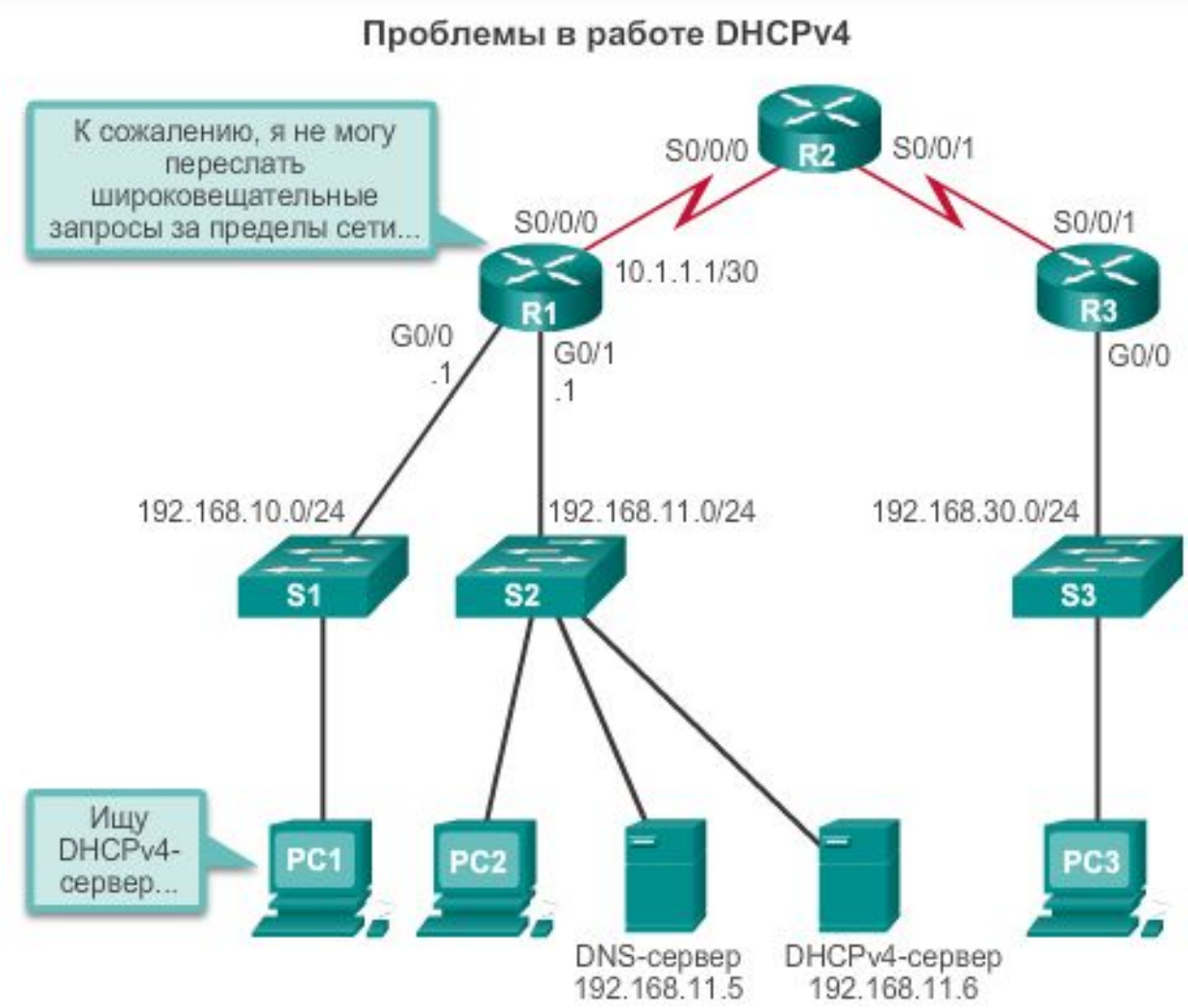
  show running-config | section dhcp

  show ip dhcp binding

  show ip dhcp server statistics

- Для отключения dhcp выполните команду **no service dhcp.**

Ретрансляция DHCPv4



В этом сценарии маршрутизатор R1 не настроен в качестве DHCPv4-сервера и не отправляет сообщения широковещательной рассылки, поскольку DHCPv4-сервер расположен в другой сети, PC1 не может получить IP-адрес через DHCP.

Для этого необходимо R1 сконфигурировать как **агент DHCPv4-ретрансляции** и назначить интерфейсу G0/0 **вспомогательный адрес** DHCPv4-сервера 192.168.11.6.

Ретрансляция DHCPv4

Использование **вспомогательного IP-адреса (ip helper address)** позволяет маршрутизатору пересылать сообщения широковещательной рассылки DHCPv4 на сервер DHCPv4. Выполняет функцию агента-ретранслятора.

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
<Output omitted>
```

Когда маршрутизатор R1 сконфигурирован как агент DHCPv4-ретрансляции, он принимает широковещательные запросы, а затем отправляет эти запросы как одноадресную рассылку на IPv4-адрес 192.168.11.6. Команда **show ip interface** применяется для проверки конфигурации.

Конфигурация маршрутизатора в качестве DHCPv4-клиента


```
SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
SOHO(config-if)#
*Jan 31 17:31:11.507: %DHCP-6-ADDRESS_ASSIGN: Interface
GigabitEthernet0/1 assigned DHCP address 209.165.201.12, mask
255.255.255.224, hostname SOHO
SOHO(config-if)# end
SOHO# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  <Output omitted>
```

В некоторых случаях маршрутизаторы Cisco **в небольших или домашних офисах** (SOHO) и филиалах должны быть настроены **в качестве DHCPv4-клиентов** аналогично настройке клиентских компьютеров. Используемый метод зависит от интернет-провайдера. В простейшей конфигурации для соединения с кабельным или DSL-модемом используется Ethernet-интерфейс. *Для настройки Ethernet-интерфейса в качестве DHCP-клиента* используйте команду режима настройки интерфейса **ip address dhcp**.

Задачи поиска и устранения неполадок

Поиск и устранение неполадок. Задача 1. Разрешение конфликтов IPv4-адресов

У клиента, подключённого к сети, может **истечь срок аренды** IPv4-адреса. Если клиент не возобновит аренду, DHCPv4-сервер может переназначить этот IPv4-адрес другому клиенту. После перезагрузки клиент запросит IPv4-адрес. Если DHCPv4-сервер не даст ответ достаточно быстро, клиент будет использовать IPv4-адрес, использовавшийся в последний раз. Возникает ситуация, когда **два клиента используют один IPv4-адрес**, создавая **конфликт**.

Команда **show ip dhcp conflict** отображает все конфликты адресов, зарегистрированные DHCPv4-сервером. Для обнаружения клиента сервером используется команда **ping**. Для обнаружения конфликта клиент использует протокол разрешения адресов (ARP). **При обнаружении конфликта адрес удаляется из пула и не присваивается до устранения конфликта администратором.**

Выходные данные отображают IP-адреса, конфликтующие с сервером DHCP. В данных указан метод обнаружения (detection method) и время обнаружения (detection time) конфликтующих IP-адресов, предложенных сервером DHCP.

```
R1# show ip dhcp conflict
IP address       Detection Method      Detection time
192.168.10.32    Ping                   Feb 16 2013 12:28 PM
192.168.10.64    Gratuitous ARP         Feb 23 2013 08:12 AM
```

Задачи поиска и устранения неполадок

Поиск и устранение неполадок. Задача 2. Проверка физического соединения

Для начала необходимо применить команду **show interfaces** *interface*, чтобы убедиться, что **интерфейс маршрутизатора**, действующий **в качестве основного шлюза для клиента, функционирует.** Если статус интерфейса отличается от статуса up, трафик (включая запросы DHCP-клиента) не проходит через порт.

Поиск и устранение неполадок. Задача 3. Проверка связности с использованием статического IP-адреса

При проведении работ по поиску и устранению неполадок любой неисправности DHCPv4, **необходимо проверить связность (доступ к сетевым ресурсам) путём настройки статической IPv4-адресации на клиентской рабочей станции.** Если рабочей станции не удаётся получить доступ к сетевым ресурсам, несмотря на наличие статически настроенного IPv4-адреса, DHCPv4 не является источником проблемы. В этом случае необходимо провести проверку сетевого подключения.

Задачи поиска и устранения неполадок

Поиск и устранение неполадок. Задача 4. Проверка настройки порта коммутатора

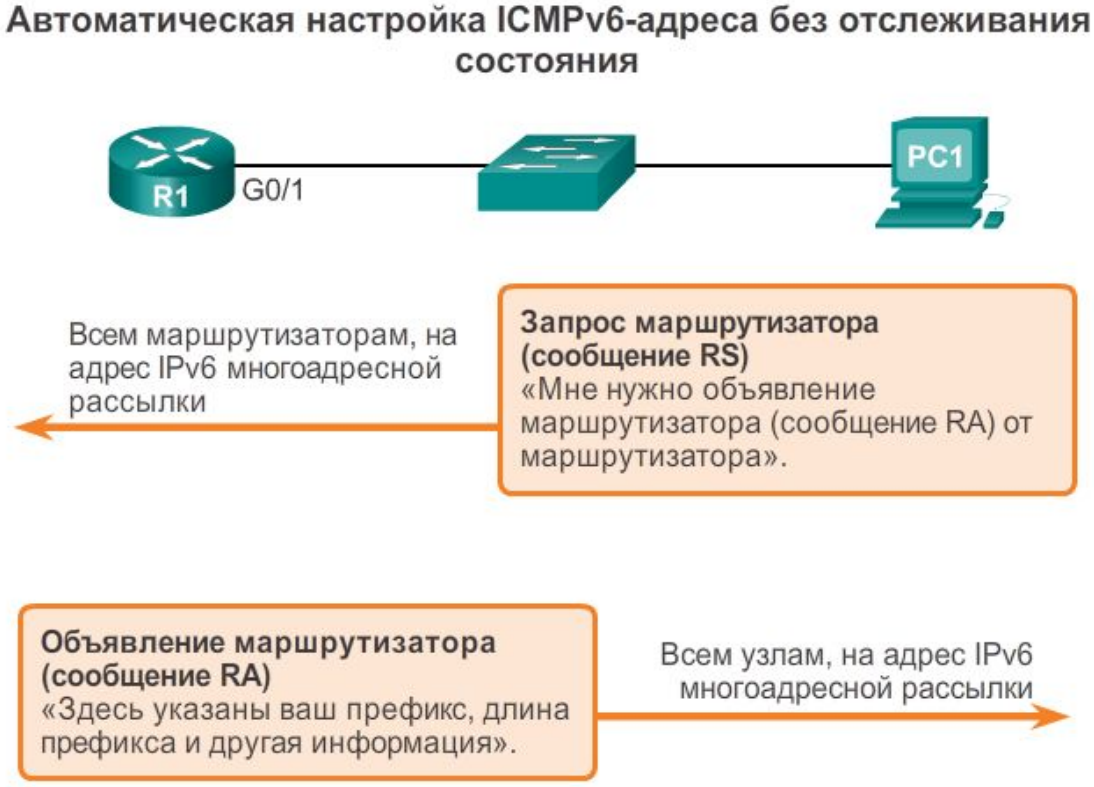
В случае если DHCPv4-клиент не может получить IPv4-адрес от DHCPv4-сервера при загрузке, стоит попробовать получить IPv4-адрес от DHCPv4-сервера, **вручную отправив DHCPv4-запрос с устройства-клиента**.
Примечание. Если между клиентом и DHCPv4-сервером есть **коммутатор**, и клиент не может получить настройки DHCP, причиной могут служить **неполадки в настройке порта коммутатора**. Причиной могут быть проблемы, связанные с созданием транковых и логических каналов, а также с протоколами STP и RSTP. Решением наиболее часто возникающих проблем DHCPv4-клиента при первоначальной установке коммутатора Cisco может стать настройка расширения PortFast и пограничного порта.

Поиск и устранение неполадок. Задача 5. Диагностика работы протокола DHCPv4 в той же подсети или VLAN

Важно различать, **правильно ли функционирует DHCPv4 в качестве DHCPv4-сервера, когда клиент находится в той же подсети или VLAN**. В случае если протокол DHCPv4 работает корректно при условии, что клиент находится в той же подсети или VLAN, **проблема** может заключаться **в агенте DHCP-ретрансляции**. Если неполадки сохраняются даже при проверке работы DHCPv4 в той же подсети или VLAN в качестве DHCPv4-сервера, проблема обычно заключается в DHCPv4-сервере.

Автоматическая настройка адреса без отслеживания состояния (SLAAC) для IPv6

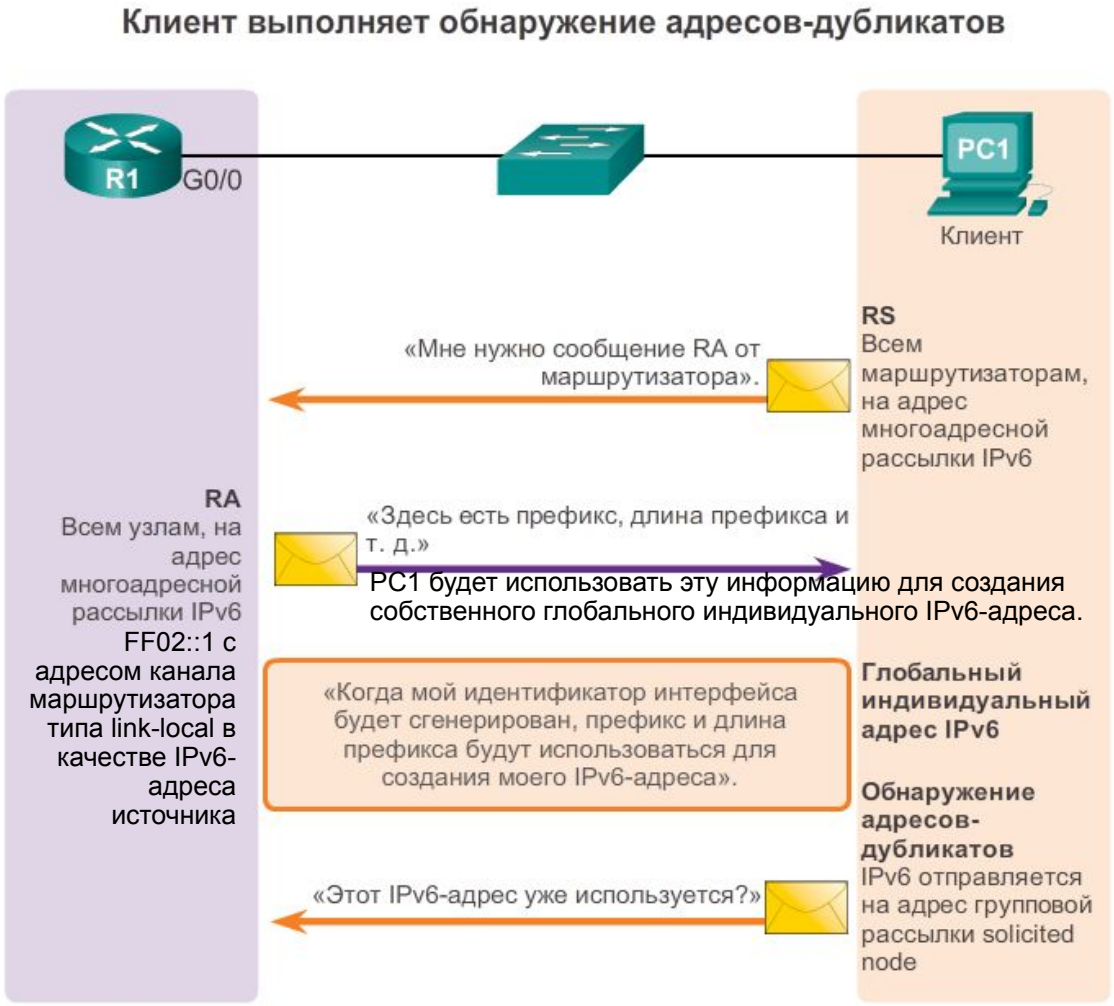
Автоматическая настройка адреса без отслеживания состояния (SLAAC) — это способ получения устройством глобального IPv6-адреса одноадресной рассылки без использования DHCPv6-сервера.



Существует два метода, с помощью которых глобальные индивидуальные IPv6-адреса могут быть присвоены динамически:

- Автоматическая настройка адреса без отслеживания состояния (SLAAC),
- Протокол динамической конфигурации сетевого узла (DHCP) для IPv6 (DHCPv6 с отслеживанием состояния)

Принцип работы SLAAC



PC1 имеет теперь 64-разрядный префикс сети, но требует 64-битный идентификатор интерфейса (IID) для создания глобального индивидуального адреса.

Существует два способа создания для PC1 собственного уникального ID:

EUI-64 — при помощи процесса EUI-64 PC1 создаёт IID, используя свой 48-битный MAC-адрес.

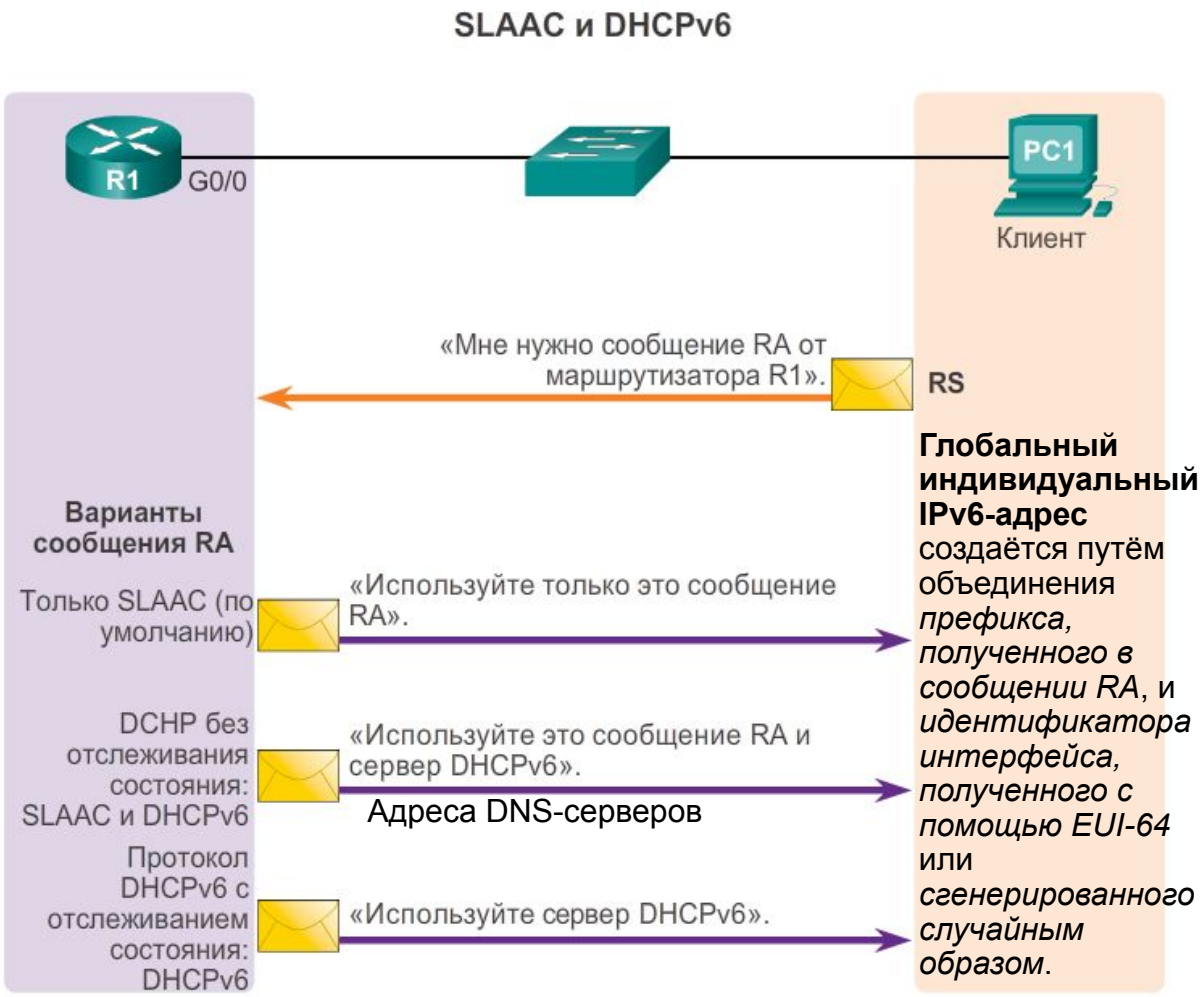
Генерация случайным образом — 64-битный IID может быть случайным числом, сгенерированным операционной системой клиента.

SLAAC и DHCPv6

Настроен ли клиент на автоматическое получение информации об IPv6-адресации с использованием SLAAC, DHCPv6 или сочетанием обоих вариантов, *зависит от настроек, содержащихся в сообщении RA*.

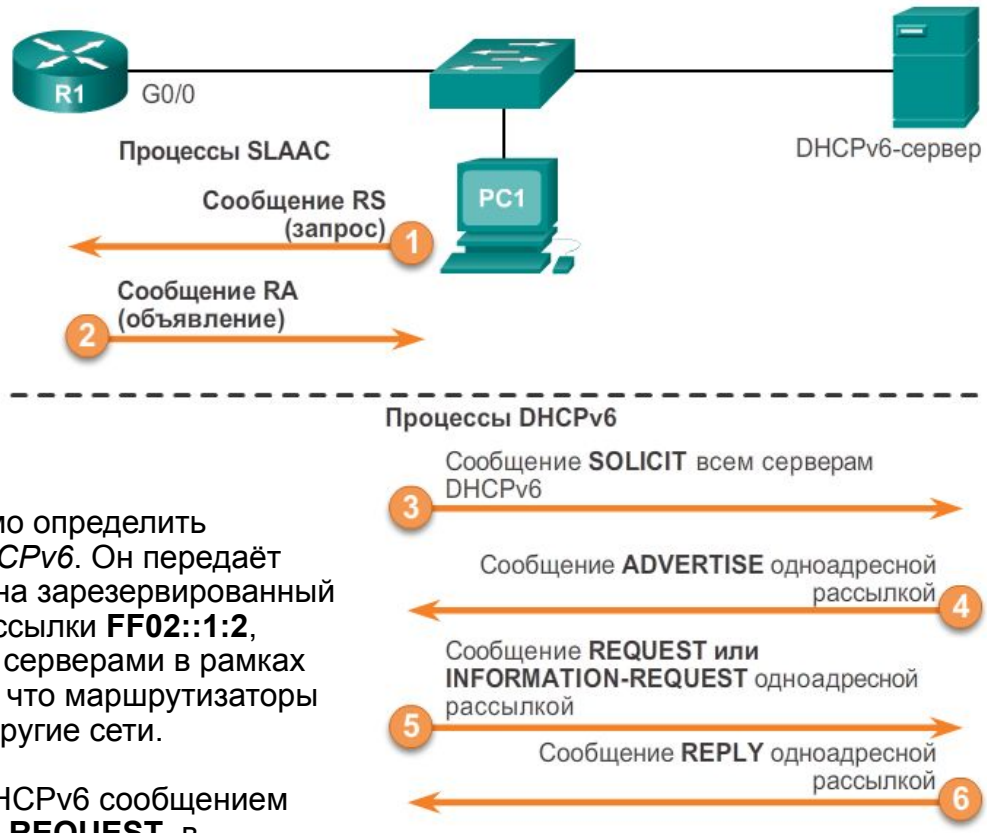
ICMPv6 сообщения RA содержат два флага, обозначающих, какой из вариантов должен быть использован клиентом: *флаг управляемой конфигурации адресов **(M)*** и *флаг другой конфигурации **(O)***. Различные сочетания флагов M и O, сообщения RA выбирают один из трёх вариантов адресации устройства IPv6:

- **M=0, O=0: *SLAAC*** (только объявление маршрутизатора);
- **M=0, O=1: *протокол DHCPv6 без отслеживания состояния*** (объявления маршрутизатора и DHCPv6);
- **M=1: *протокол DHCPv6 с отслеживанием состояния*** (только DHCPv6).



Операции протокола DHCPv6

1-2. Работа DHCPv6 начинается с сообщения **RA**, отправленного от маршрутизатора по протоколу ICMPv6. Сообщение RA может отправляться периодически или в ответ на запрос устройства **RS**. Если вариант работы DHCPv6 указан в сообщении RA, устройство начинает передачу информации по схеме клиент-сервер с использованием DHCPv6.



Сообщения протокола DHCPv6 посылаются через протокол UDP: порт 546 – от сервера к клиенту, порт 547 – от клиента к серверу.

4. Один или несколько серверов DHCPv6 отвечают DHCPv6-сообщением **ADVERTISE**, которое сообщает DHCPv6-клиенту, что *сервер доступен* для предоставления службы DHCPv6.

3. DHCPv6-клиенту необходимо определить *местоположение сервера DHCPv6*. Он передаёт сообщение DHCPv6 **SOLICIT** на зарезервированный IPv6-адрес многоадресной рассылки **FF02::1:2**, используемый всеми DHCPv6 серверами в рамках канала link-local, это означает, что маршрутизаторы не направляют сообщения в другие сети.

6. Сервер отправляет клиенту DHCPv6 сообщение **REPLY**, содержащее запрашиваемую в сообщении REQUEST или INFORMATION-REQUEST информацию.

5. Клиент отвечает серверу DHCPv6 сообщением **REQUEST** или **INFORMATION-REQUEST**, в зависимости от того, является ли DHCPv6-сервер сервером с отслеживанием состояния или без него:

DHCPv6-клиент без отслеживания состояния — клиент отправляет DHCPv6 сообщение **INFORMATION-REQUEST** серверу DHCPv6, запрашивая *только параметры конфигурации*, *например, адрес DNS-сервера*. Клиент создаёт собственный IPv6-адрес при помощи префикса из сообщения RA и самогенерируемого идентификатора интерфейса.
DHCPv6-клиент с отслеживанием состояния — клиент отправляет DHCPv6 сообщение **REQUEST** серверу для получения *IPv6-адреса и всех остальных параметров конфигурации от сервера*.

DHCPv6 без отслеживания состояния

Конфигурация маршрутизатора в качестве DHCPv6-сервера без отслеживания состояния

Настройка DHCPv6-сервера без отслеживания состояния на маршрутизаторе

Шаг 1. Активация маршрутизации IPv6

```
Router(config)# ipv6 unicast-routing
```

необходима для отправки сообщений RA по протоколу ICMPv6

Шаг 2. Настройка DHCPv6-пула

```
Router(config)# ipv6 dhcp pool pool-name
Router(config-dhcpv6)#
```

создаёт пул с именем pool-name и переводит маршрутизатор в режим конфигурации DHCPv6

Шаг 3. Настройка параметров пула

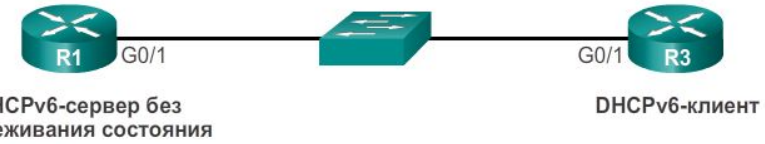
```
Router(config-dhcpv6)# dns-server dns-server-address
Router(config-dhcpv6)# domain-name domain-name
```

С помощью функции SLAAC клиент принимает информацию, необходимую для создания глобального индивидуального IPv6-адреса, информацию о шлюзе по умолчанию. При этом сервер DHCPv6 без отслеживания состояния можно настроить для предоставления информации, которая могла не быть включена в сообщение RA, например, адреса DNS-сервера и доменного имени.

Шаг 4. Настройка DHCPv6-интерфейса

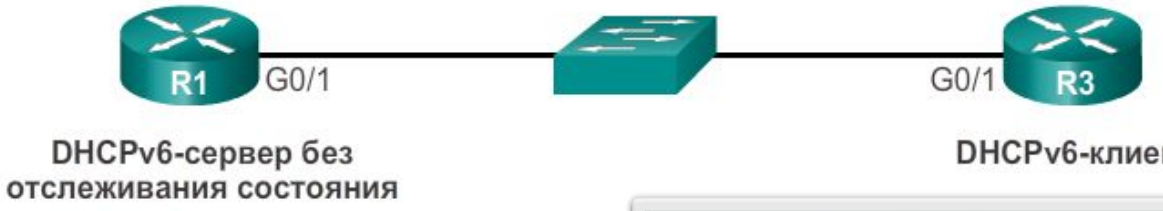
```
Router(config)# interface type number
Router(config-if)# ipv6 dhcp server pool-name
Router(config-if)# ipv6 nd other-config-flag
```

Команда интерфейса **`ipv6 dhcp server`** *`pool-name`* привязывает созданный DHCPv6-пул к интерфейсу. Маршрутизатор отвечает на DHCPv6-запросы на этом интерфейсе информацией, содержащейся в пуле. Значение флага O необходимо изменить с 0 на 1, используя команду интерфейса **ipv6 nd other-config-flag**. Сообщения RA, отправленные на этот интерфейс, указывают, что дополнительная информация доступна на DHCPv6-сервере без отслеживания состояния.



DHCPv6 без отслеживания состояния

Конфигурация маршрутизатора в качестве DHCPv6-клиента без отслеживания состояния




```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address autoconfig
R3(config-if)#
```

- Команда **ipv6 enable** используется ввиду того, что маршрутизатор ещё не имеет глобального индивидуального адреса.
- Команда **ipv6 address autoconfig** включает автоматическую настройку IPv6-адресации с использованием SLAAC.
- Проверка DHCP-клиента без отслеживания состояния с помощью следующих команд:
  - **show IPv6 interface**
  - **debug ipv6 dhcp detail**

Конфигурация маршрутизатора в качестве DHCPv6-сервера с отслеживанием состояния

Настройка DHCPv6-маршрутизатора с отслеживанием состояния

Шаг 1. Активация маршрутизации IPv6

```
Router(config)# ipv6 unicast-routing
```

необходима для отправки сообщений RA по протоколу ICMPv6

Шаг 2. Настройка DHCPv6-пула

```
Router(config)# ipv6 dhcp pool pool-name
Router(config-dhcpv6)#
```

создаёт пул с именем pool-name и переводит маршрутизатор в режим конфигурации DHCPv6

Шаг 3. Настройка параметров пула

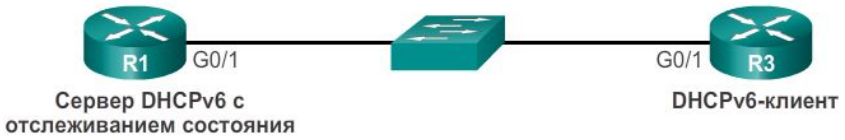
```
Router(config-dhcpv6)# address prefix/length [lifetime
                       {valid-lifetime preferred-lifetime
                       | infinite}]
Router(config-dhcpv6)# dns-server dns-server-address
Router(config-dhcpv6)# domain-name domain-name
```

Команда **address prefix** используется для обозначения адресного пула, из которого сервер будет выделять адреса. Параметр **lifetime** указывает действительное и предпочтительное время аренды в секундах.
Другая информация, предоставленная DHCPv6-сервером с отслеживанием состояния, обычно включает адрес DNS-сервера и доменное имя.

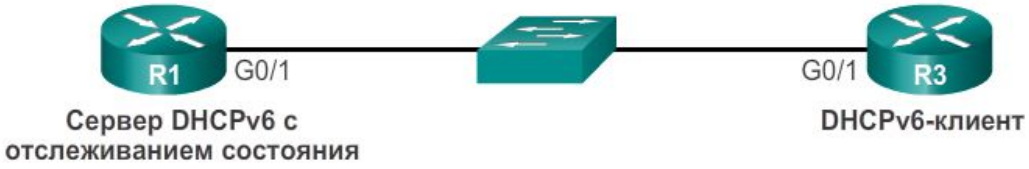
Шаг 4. Настройка DHCPv6-интерфейса

```
Router(config)# interface type number
Router(config-if)# ipv6 dhcp server pool-name
Router(config-if)# ipv6 nd managed-config-flag
```

Команда интерфейса **ipv6 dhcp server** *pool-name* привязывает созданный DHCPv6-пул к интерфейсу. Маршрутизатор отвечает на DHCPv6-запросы на этом интерфейсе информацией, содержащейся в пуле. Значение флага M необходимо изменить с 0 на 1 с помощью команды интерфейса **ipv6 nd managed-config-flag**. Установленное значение говорит устройству не использовать SLAAC, а получить настройки IPv6-адресации и все параметры конфигурации от DHCPv6-сервера с отслеживанием состояния.



Конфигурация маршрутизатора в качестве DHCPv6-клиента с отслеживанием состояния




```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address dhcp
R3(config-if)#
```

Команда **ipv6 enable** позволяет маршрутизатору получить адрес link-local, чтобы отправлять сообщения RS.

Команда режима конфигурации интерфейса **ipv6 address dhcp** разрешает маршрутизатору выполнять функцию DHCPv6-клиента на данном интерфейсе.

Проверка DHCPv6-сервера с отслеживанием состояния при помощи:

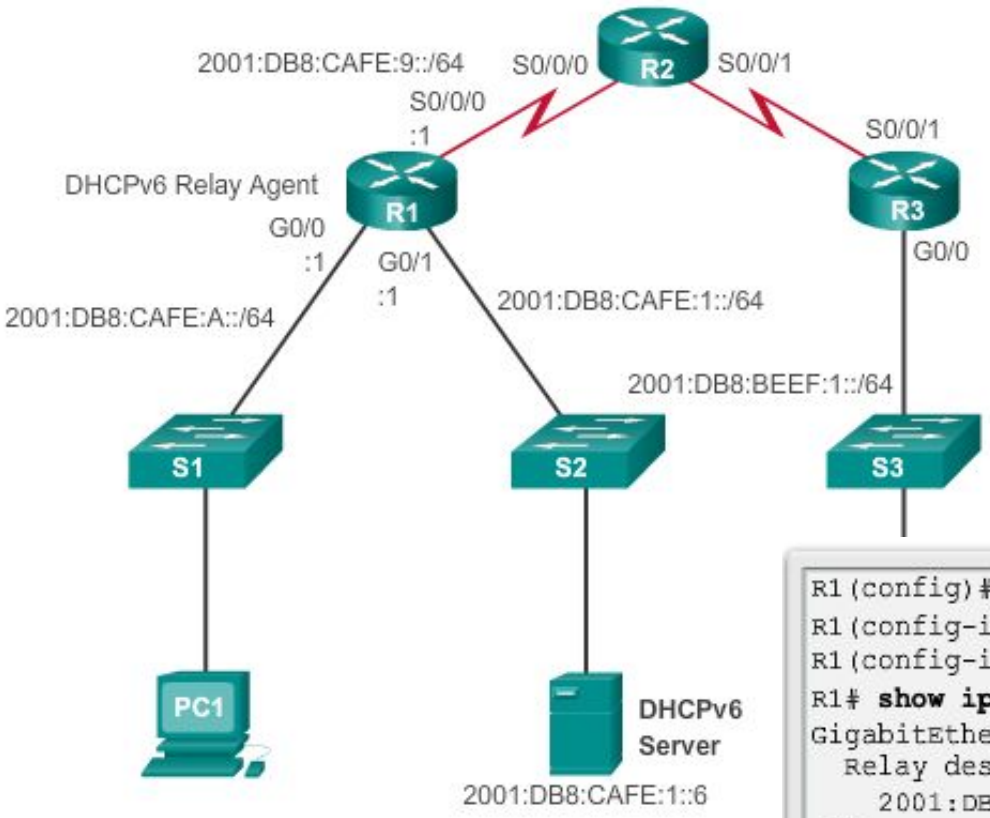
show ipv6 dhcp pool

show ipv6 dhcp binding

Проверка DHCPv6-клиента с отслеживанием состояния при помощи:

show ipv6 interface

Конфигурация маршрутизатора в качестве агента ретрансляции DHCPv6 с отслеживанием состояния



Агент DHCPv6-ретрансляции настроен с помощью команды **ipv6 dhcp relay destination** на интерфейсе, соответствующем DHCPv6-клиенту, с использованием адреса DHCPv6-сервера в качестве адреса назначения.

```
R1(config)# interface g0/0
R1(config-if)# ipv6 dhcp relay destination 2001:db8:cafe:1::6
R1(config-if)# end
R1# show ipv6 dhcp interface g0/0
GigabitEthernet0/0 is in relay mode
  Relay destinations:
    2001:DB8:CAFE:1::6
R1#
```