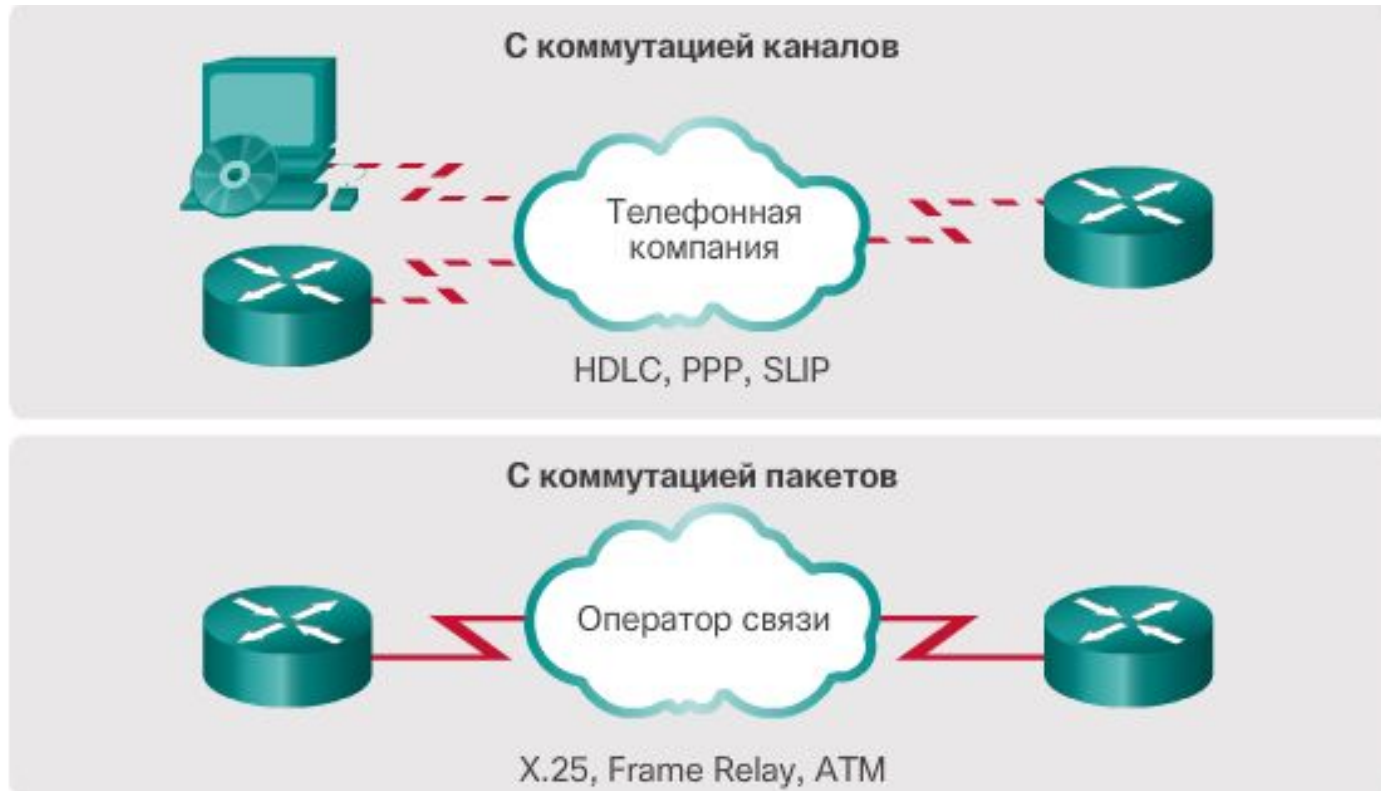


VPN. Туннели L2

- PPPoE
- Q-in-QGRE over



PPP (Point-to-Point Protocol)



PPP (Point-to-Point Protocol)

Метод инкапсуляции
дейтограмм при передаче по
последовательным
коммуникационным каналам.

Протокол LCP для
установления,
конфигурирования и
тестирования
информационных каналов

Набор протоколов NCP для
установки и
конфигурирования различных
протоколов сетевого уровня.



На каналах последовательной связи по умолчанию
используется инкапсуляция HDLC.



Для подключения маршрутизатора Cisco к маршрутизатору
другого изготовителя используйте инкапсуляцию PPP.



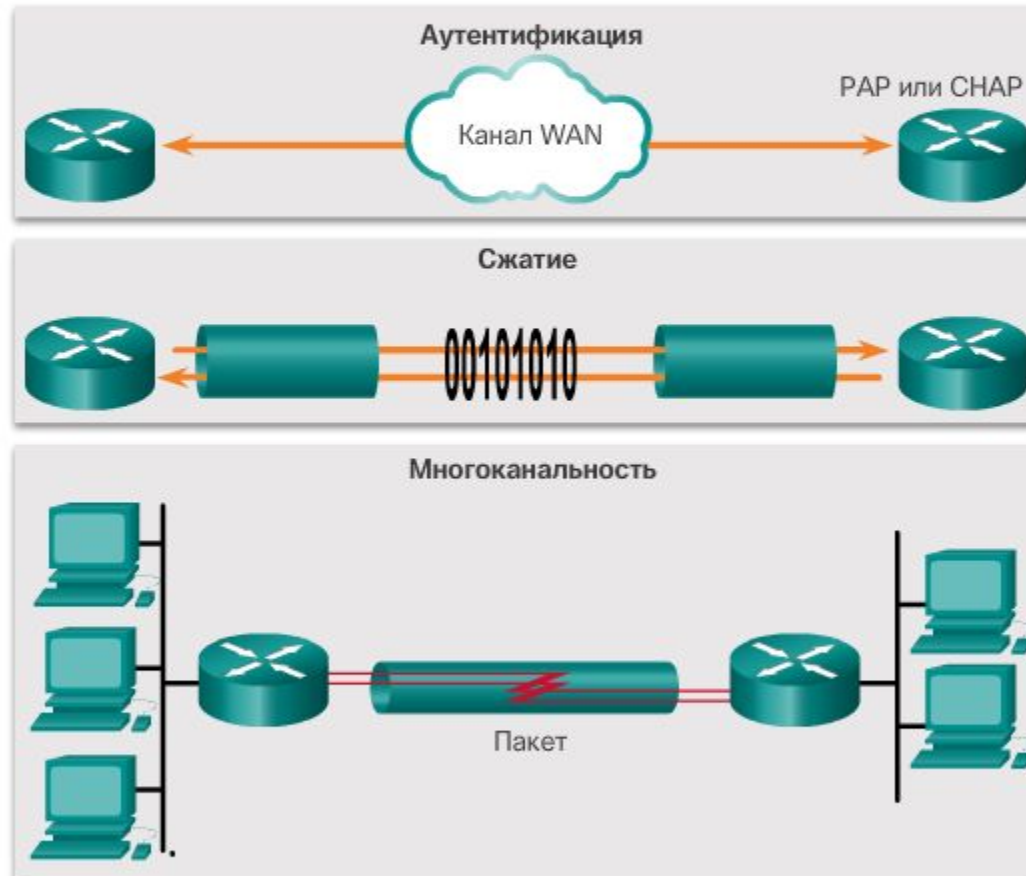
PPP: архитектура



PPP (Point-to-Point Protocol)

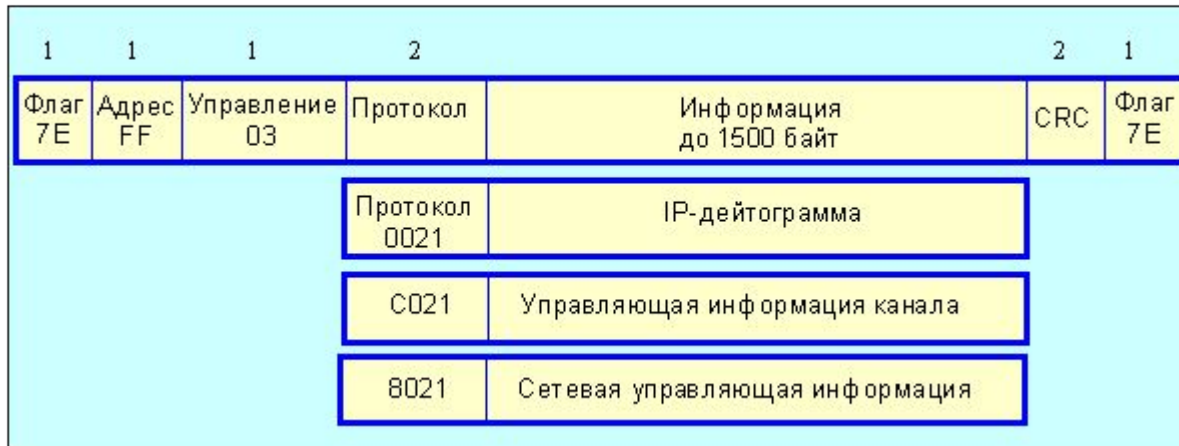
Достоинства протокола:

- Управление каналом (сжатие, аутентификация)
- Работа с несколькими протоколами сетевого уровня

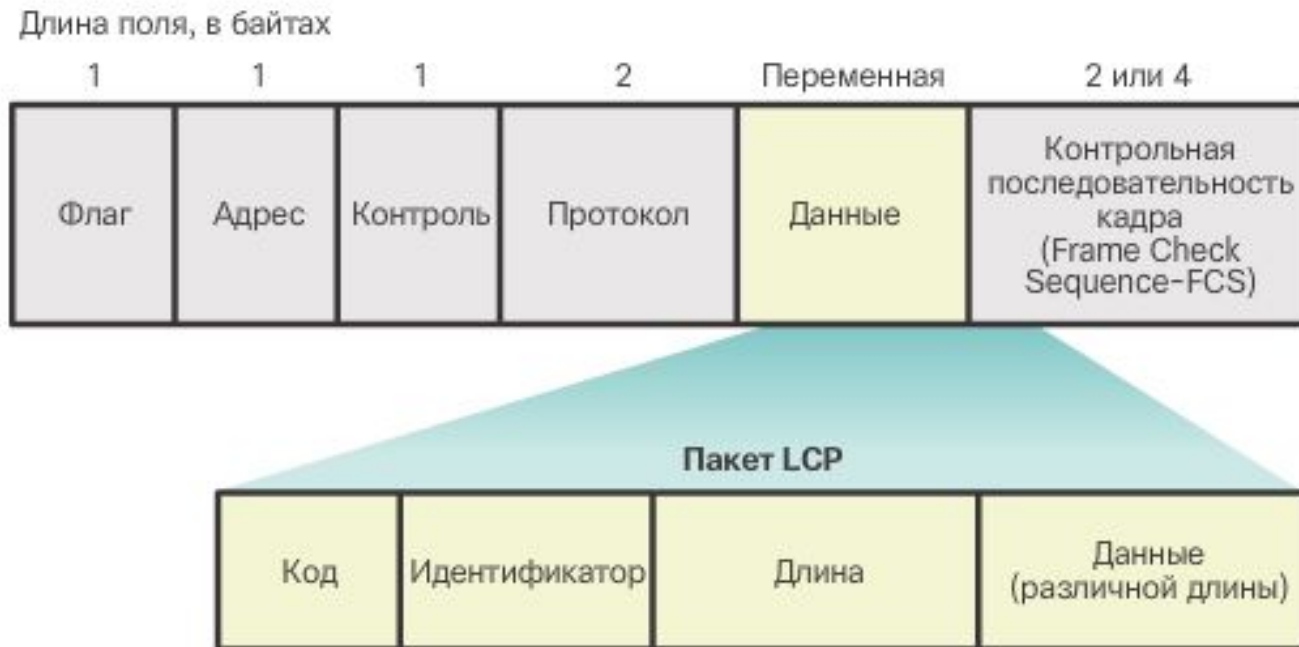


PPP (Point-to-Point Protocol)

Формат пакета



PPP:LCP уровень



Код- Поле длиной 1 байт определяет тип пакета LCP.

Идентификатор- Поле длиной 1 байт используется для сопоставления запросов и ответов пакета.

Длина - Поле длиной 2 байта указывает общую длину (включая все поля) пакета LCP.

Данные- Поле данных имеет длину 0 или больше байтов, согласно значению поля длины. Формат этого поля определяется кодом.

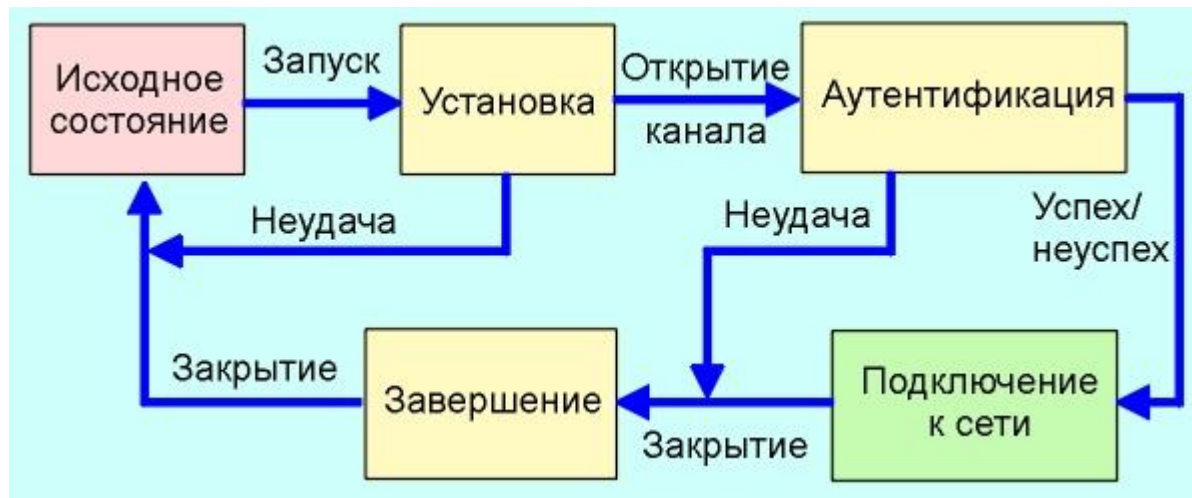
PPP: LCP уровень: опции канала

Тип(8байт)	Длина(8байт)	Значение(перем.)
------------	--------------	------------------

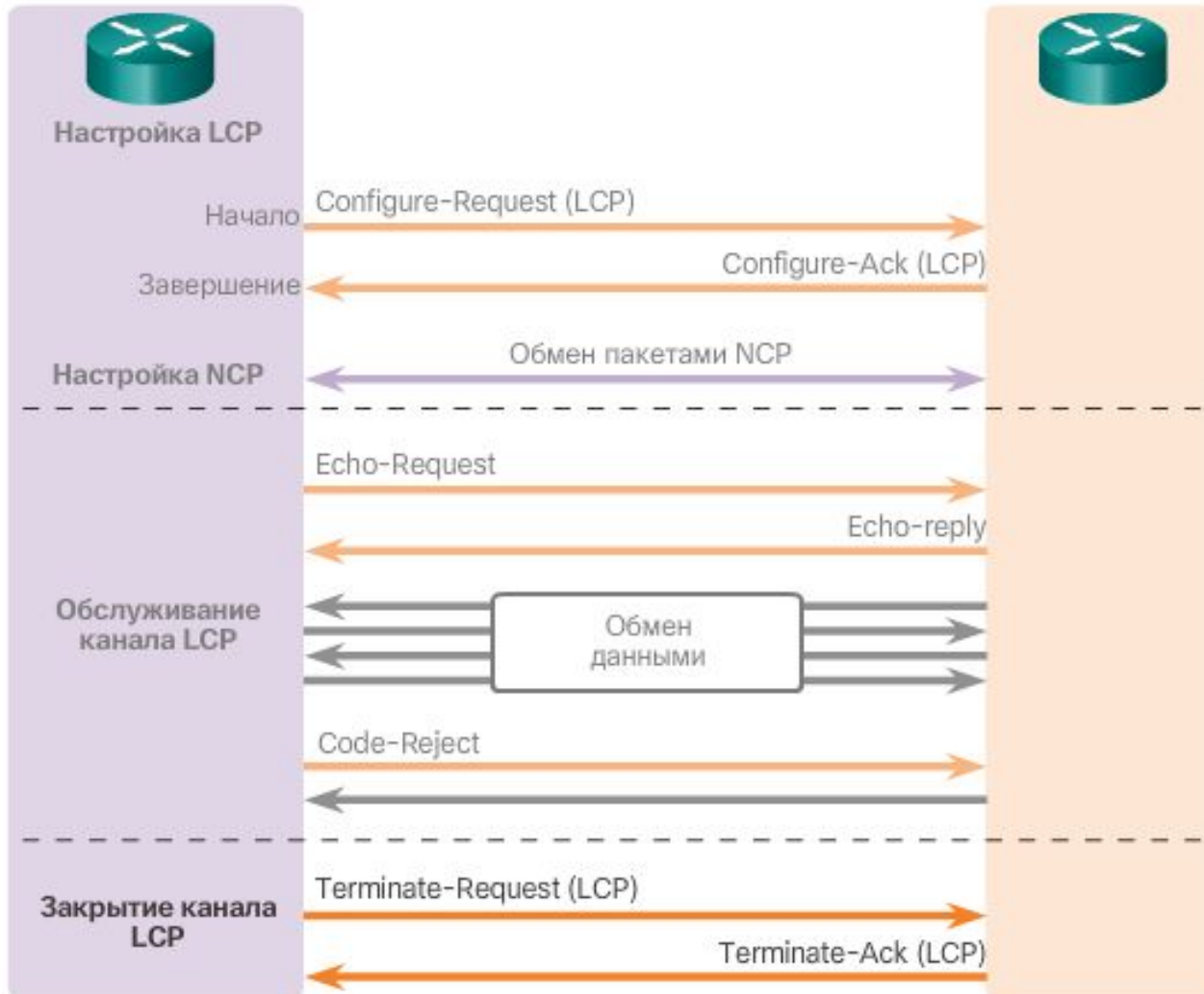
Значение кода поля <i>типа</i>	Назначение опции
0	Зарезервировано
1	Maximum-Receive-Unit (указывает максимальный размер блока данных, который может быть принят)
3	Authentication-Protocol (протокол аутентификации)
4	Quality-Protocol (протокол качества)
5	Magic-Number (магическое число, опция служит для выявления каналов с петлями обратной связи)
6	Protocol-Field-Compression
7	Address-and-Control-Field-Compression

PPP (Point-to-Point Protocol)

При обнаружении несущей или по инициативе клиента система может попытаться установить соединение. В случае успеха система переходит в фазу аутентификации. Если же и фаза аутентификации завершается благополучно, система выполняет подключение к сети (IP, IPX, Appletalk и т.д.), настройка сетевого уровня производится в рамках протокола NCP. Процедура закрытия соединения осуществляется протоколом LCP



PPP (Point-to-Point Protocol)

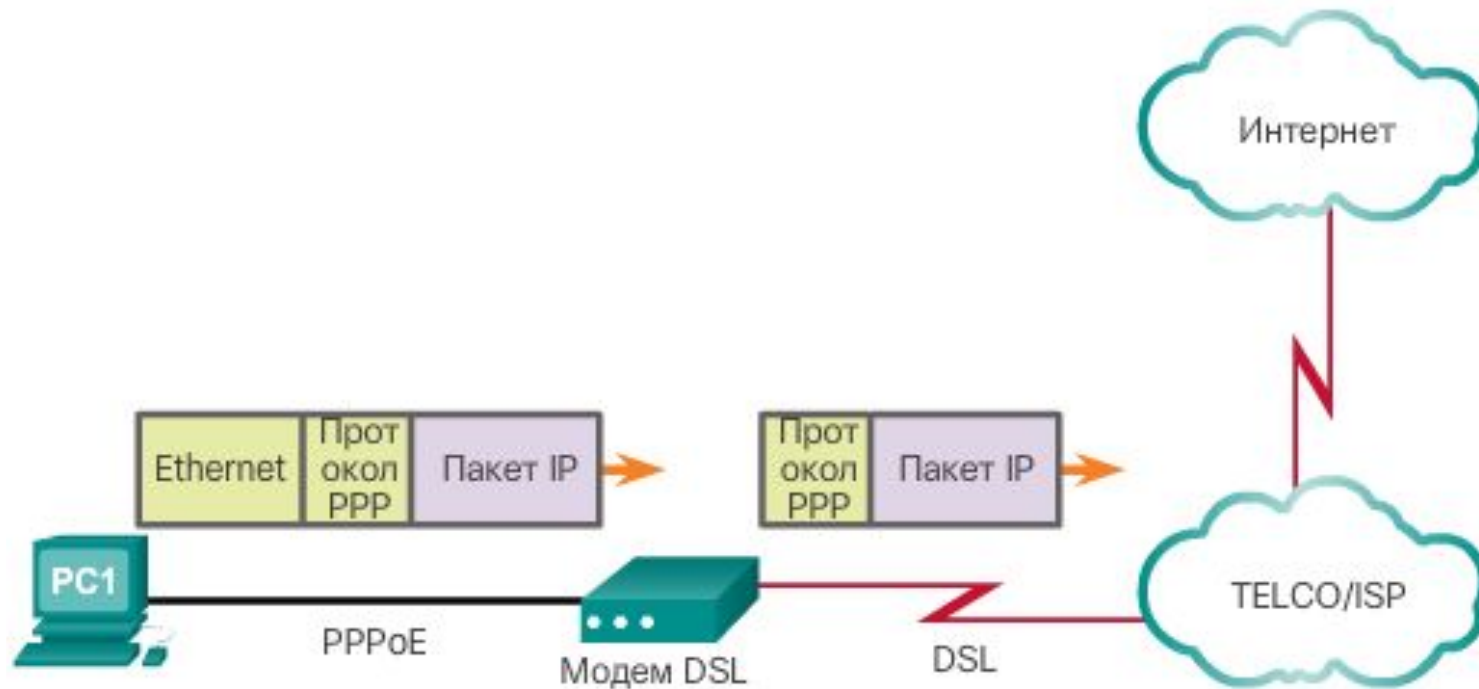


PPPoE



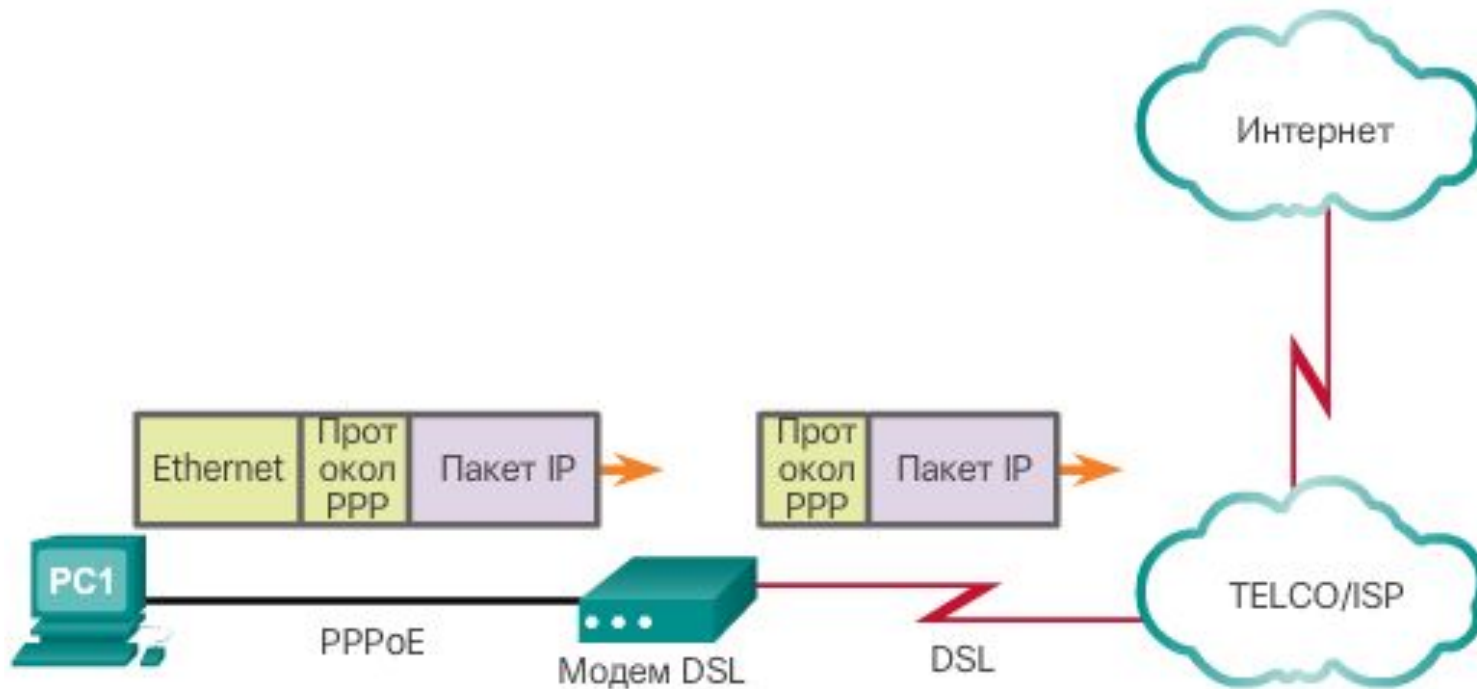
По обычным коммутируемым линиям PC 1 подключается к Интернету через облако TELCO/ISP с помощью устройства FAX/MODEM.

PPPoE



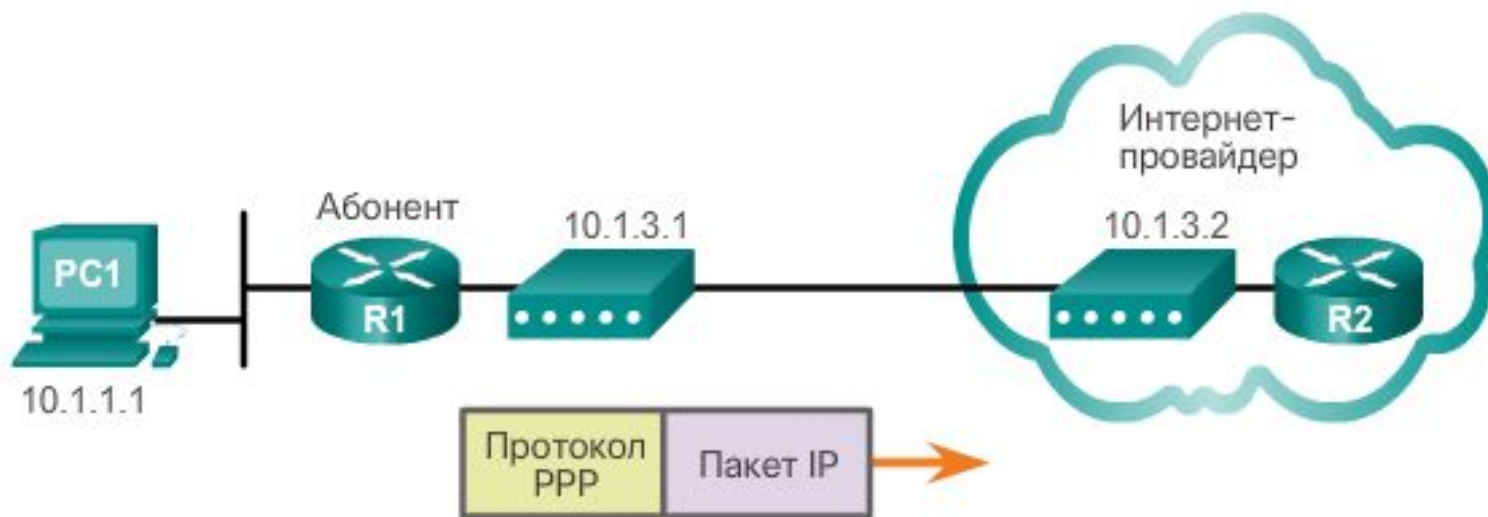
PC1 подключается непосредственно к модему DSL. С помощью соответствующего программного обеспечения (обычно это номеронабиратель DSL или клиент, предоставляемый интернет-провайдером) PC 1 инкапсулирует кадры PPP внутри кадров Ethernet и передаёт их на модем DSL.

PPPoE



PC1 подключается непосредственно к модему DSL. С помощью соответствующего программного обеспечения (обычно это номеронабиратель DSL или клиент, предоставляемый интернет-провайдером) PC 1 инкапсулирует кадры PPP внутри кадров Ethernet и передаёт их на модем DSL.

PPPoE



PPPoE: Конфигурация клиента

1- создать номеронабиратель

```
R1(config)# interface dialer 1
R1(config-if)#mtu 1492
R1(config-if)# ip address negotiated
R1(config-if)# encapsulation ppp
R1(config-if)# dialer pool 1
R1(config-if)# ppp authentication chap callin
R1(config-if)# ppp chap hostname Cust1
R1(config-if)# ppp chap password ciscopppoe
R1(config-if)#exit
```

PPPoE: Конфигурация клиента

2- связать с физическим интерфейсом

```
R1(config)# interface g0/1  
R1(config-if)#pppoe enable  
R1(config-if)#pppoe-client dial-pool-number 1  
R1(config-if)# exit
```

3- создать физический маршрут через номеронабиратель

```
R1(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
```


PPPoE: Конфигурация сервера

1- Создайте в локальной базе учётных записей имя пользователя Cust1 с паролем ciscopppoe.

```
ISP(config)# username Cust1 password ciscopppoe
```

2- Создайте пул адресов, которые будут назначены пользователям.

```
ISP(config)# ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
```

PPPoE: Конфигурация сервера

Создайте виртуальный шаблон Virtual Template и свяжите с ним IP-адрес Go/1. Свяжите виртуальный шаблон с пулом адресов. Настройте CHAP для аутентификации пользователей.

```
ISP(config)# interface virtual-template 1
ISP(config-if)# ip address 10.0.0.254 255.255.255.0
ISP(config-if)# mtu 1492
ISP(config-if)# peer default ip address pool PPPoEPOOL
ISP(config-if)# ppp authentication chap callin
ISP(config-if)# exit
```

PPPoE: Конфигурация сервера

Создайте виртуальный шаблон Virtual Template и свяжите с ним IP-адрес Go/1. Свяжите виртуальный шаблон с пулом адресов. Настройте Назначьте шаблон группе PPPoE.

```
ISP(config)# bba-group pppoe global
```

```
ISP(config-bba-group)# Virtual-template 1
```

```
ISP(config-bba-group)# sessions max limit 1200
```

```
ISP(config-bba-group)# sessions per-mac limit 1 # на всякий случай  
— ограничение в одну сессию с одного mac-адреса.
```

```
ISP(config-bba-group)# sessions auto cleanup
```

```
ISP(config-Bba-group)# exit
```

Связать группу bba-group с физическим интерфейсом Go/1.

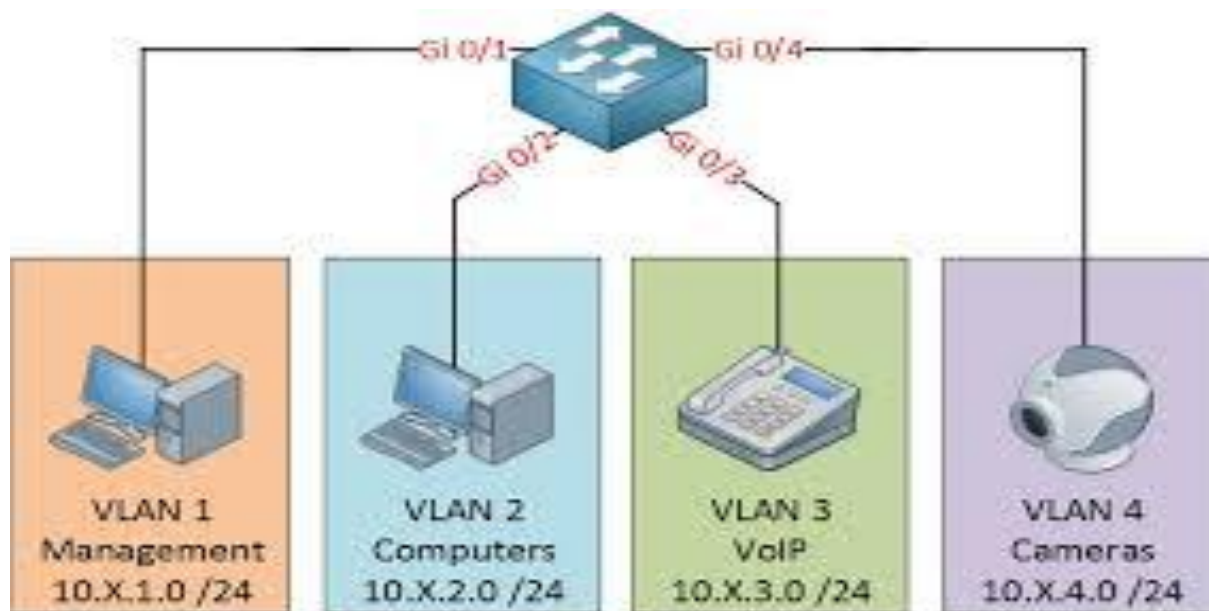
```
ISP(config)# interface go/1
```

```
ISP(config-if# pppoe enable group global
```

```
ISP(config-if)# no shutdown
```

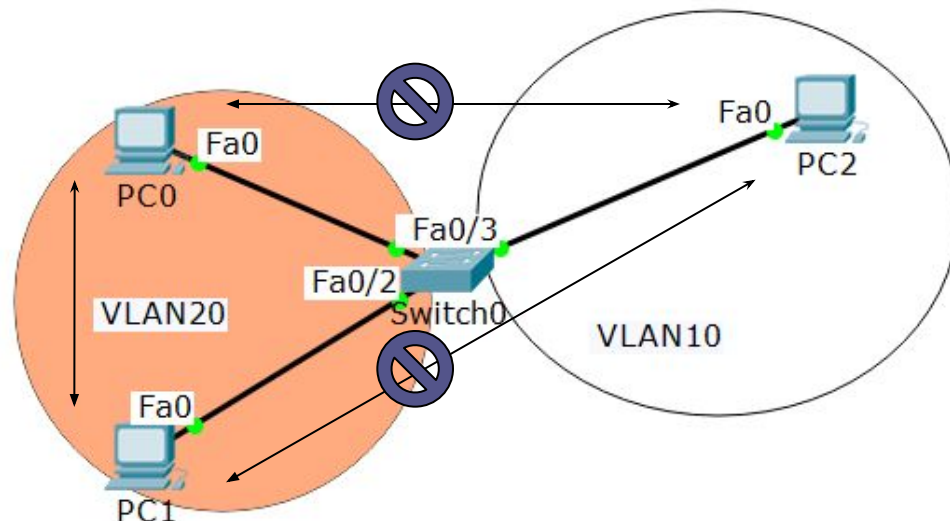
Технология VLAN

- Технология Vlan работает на втором уровне модели OSI
- Позволяет на одном физическом коммутаторе создавать несколько логических изолированных друг от друга коммутаторов, изолируя широковещательный трафик, повышая безопасность работы в сети



Технология VLAN

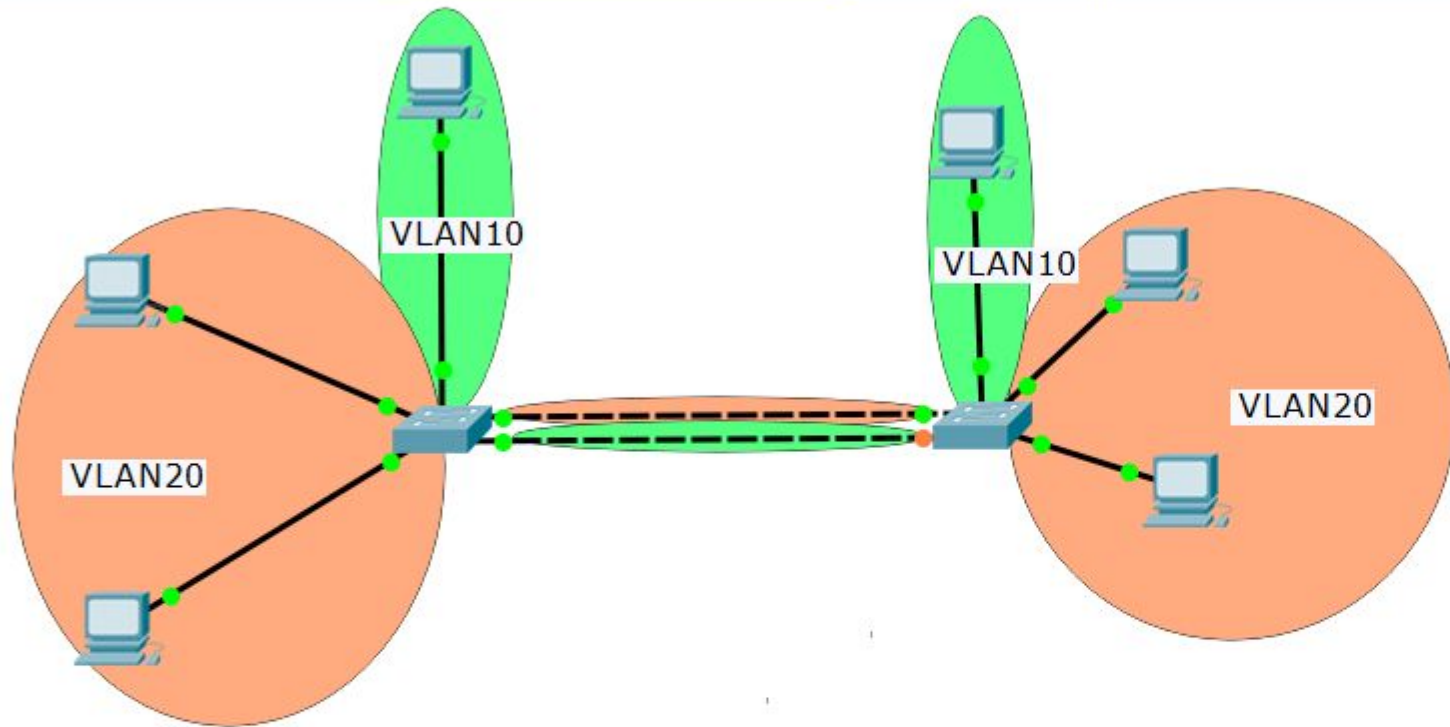
- Общее число VLAN = 2^{12}
- По умолчанию все порты коммутатора принадлежат VLAN1
- Принадлежность порта коммутатора той или иной VLAN конфигурируется на коммутаторе. Оконечные устройства не нуждаются в дополнительных настройках
- Коммутатор передает кадры между портами одной VLAN



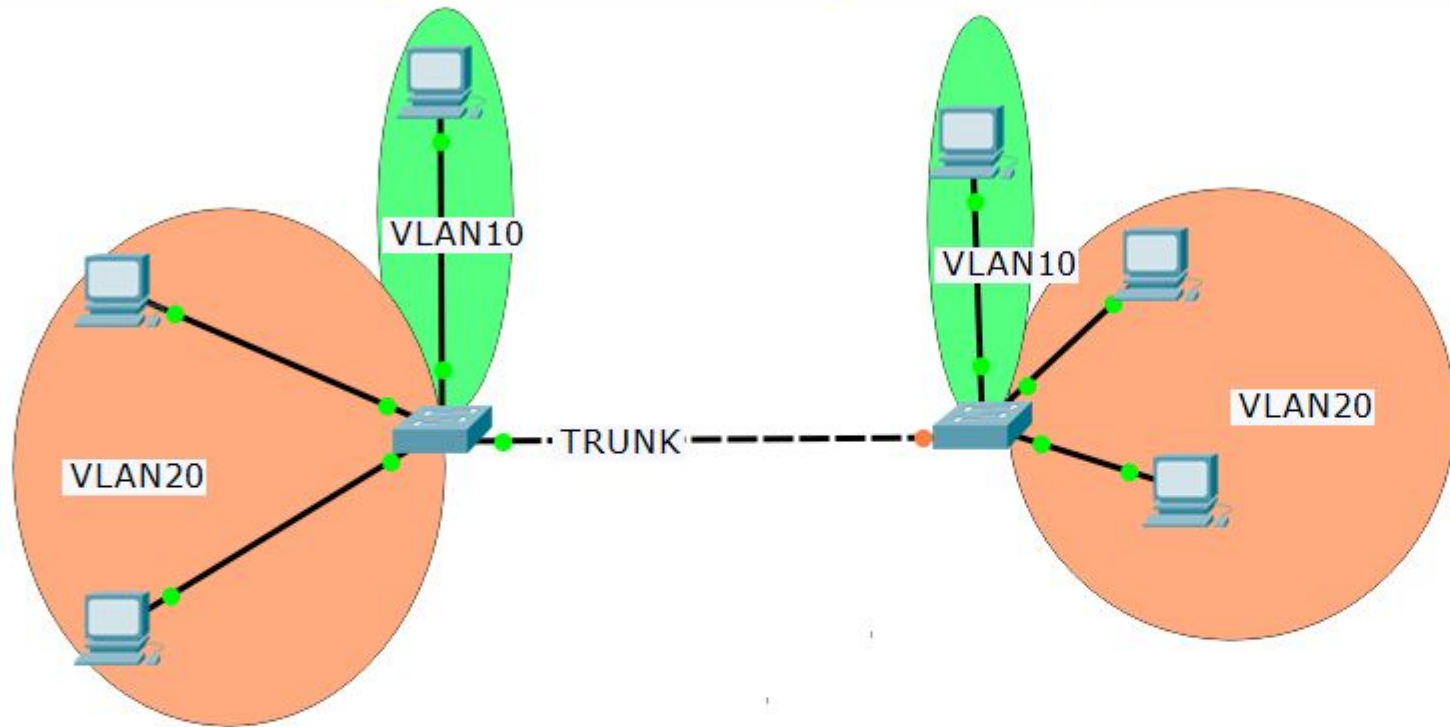
Конфигурация VLAN

```
(config)#vlan 10 // создана VLAN 10
(config-vlan)#name GUEST // задано имя для VLAN 10
(config-vlan)#exit
(config)#vlan 20 // создана VLAN 20
(config-vlan)#name ADMIN // задано имя для VLAN 20
(config-vlan)#exit
(config)#int fo/1
(config-if)#switchport mode access // режим доступа
(config-if)#switchport access vlan 10 // настроен для VLAN 10
(config-if)#int fo/2
(config-if)#switchport mode access // режим доступа
(config-if)#switchport access vlan 20 // настроен для VLAN 20
```

Распределенные VLAN



Распределенные VLAN



Магистральные каналы

- Магистральные каналы используются для возможности передавать трафик нескольких VLAN по одному интерфейсу
- При входе в магистральный канал к каждому кадру добавляется метка VLAN
- При выходе в магистральный канал метка VLAN убирается

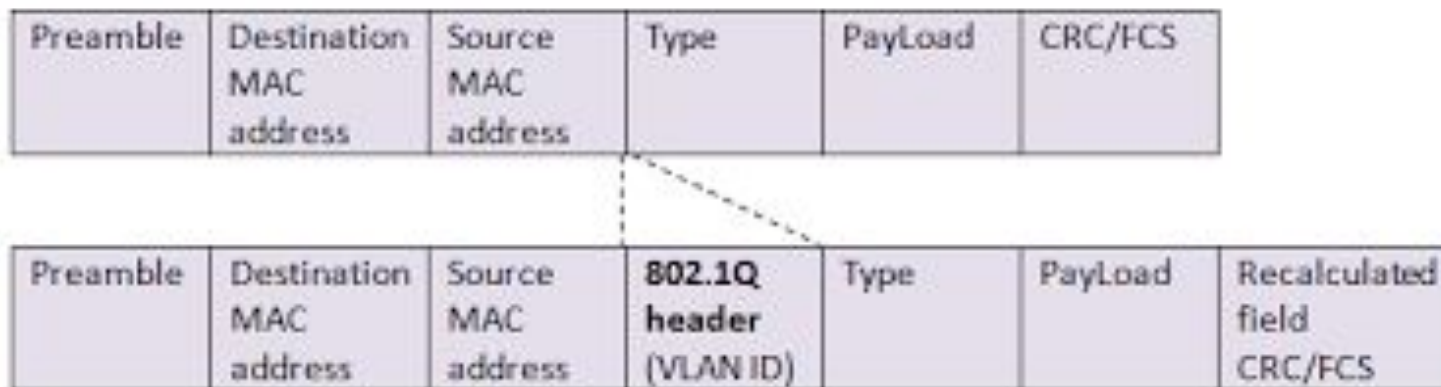
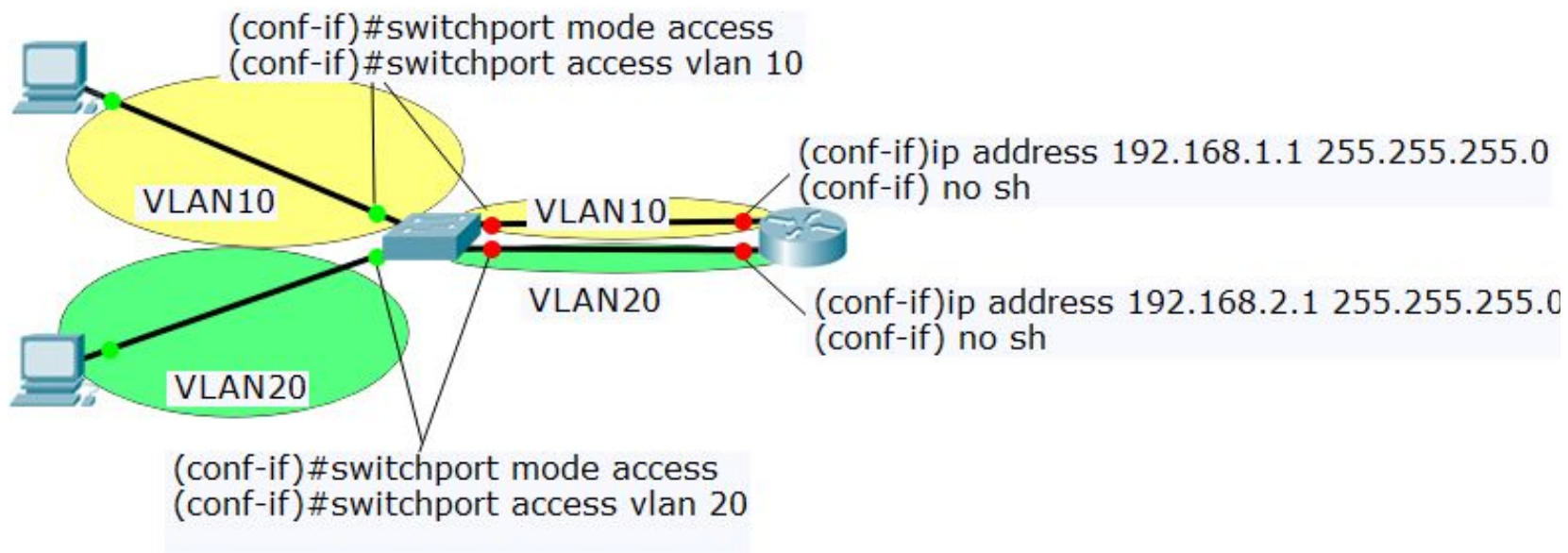


Figure 12.1. Insertion of 802.1Q Tag (VLAN ID) in Ethernet-II frame

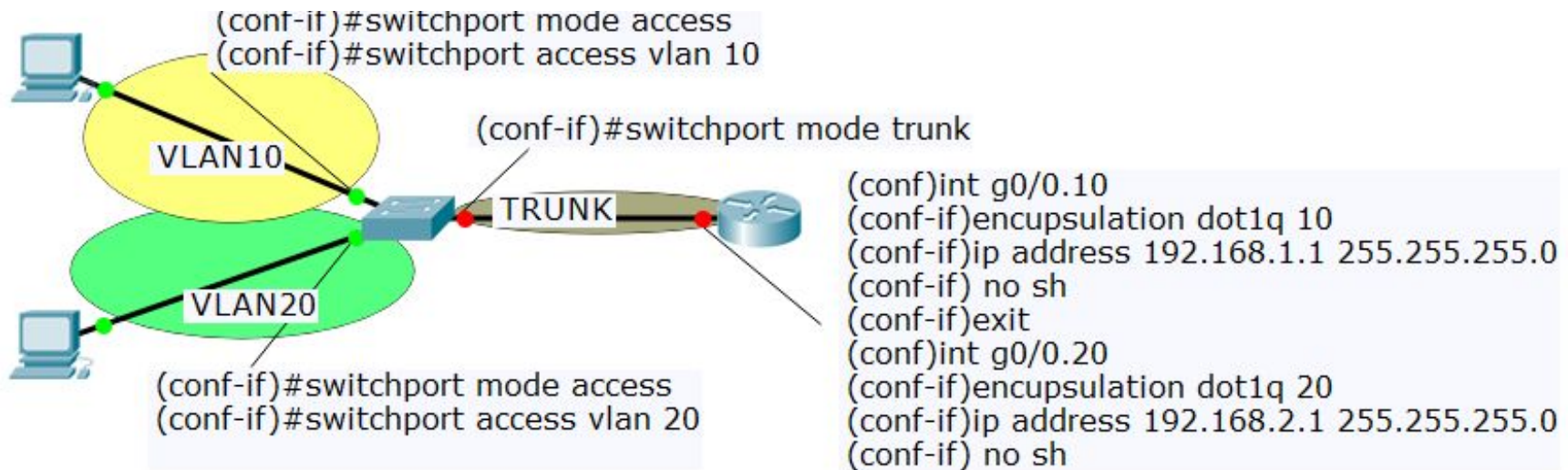
Конфигурация магистрального интерфейса

- (config-if)#int fo/3
- (config-if)#switchport mode trunk //конфигурируем как магистральный
- (config-if)# switchport trunk allowed vlan 10-20,30 //разрешаем VLAN, по умолчанию разрешены все

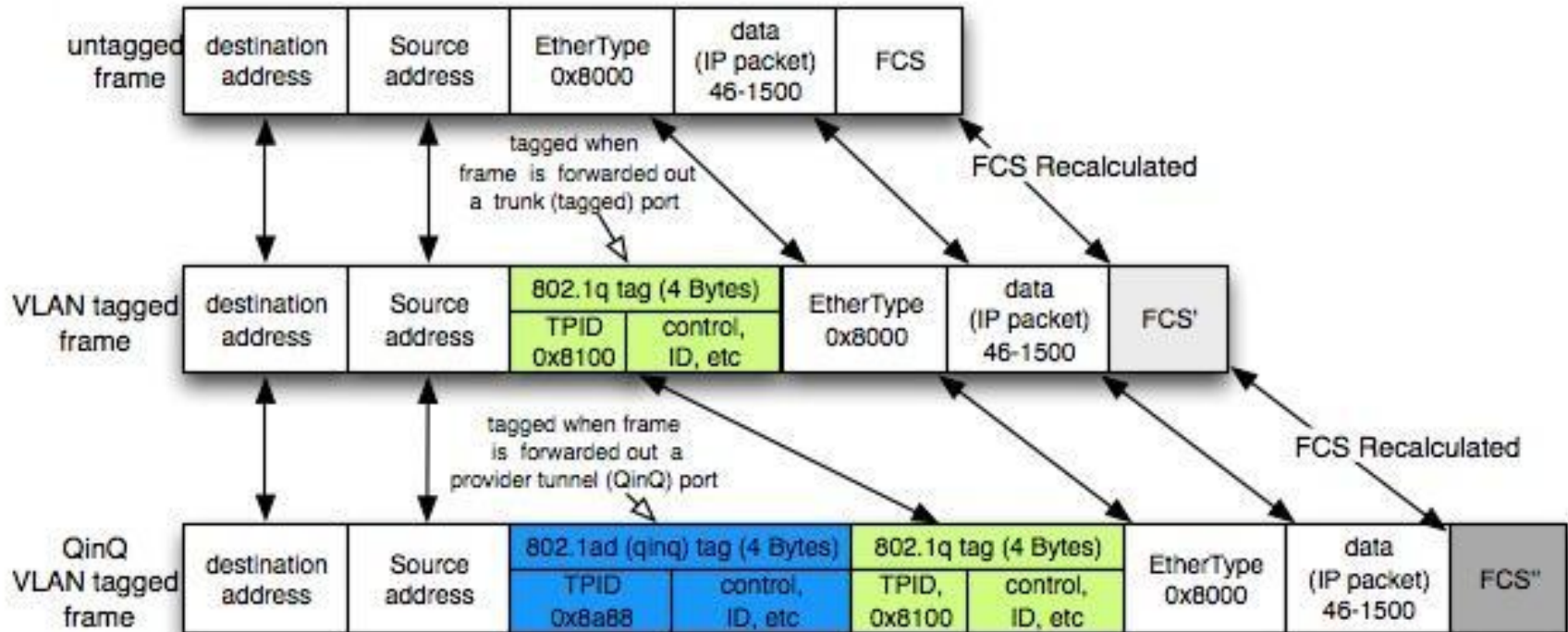
Маршрутизация между VLAN



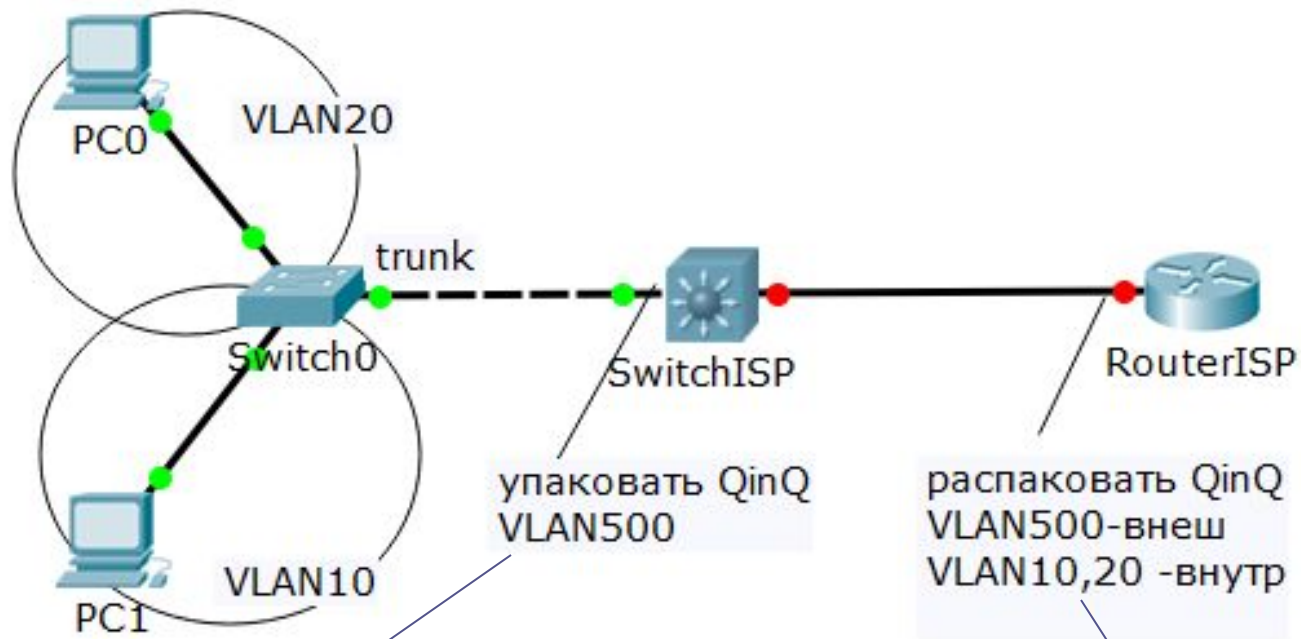
Маршрутизация между VLAN (router-on-the-stick)



Двойное тегирование



Двойное тегирование



```
interface GigabitEthernet0/1  
switchport access vlan 500  
switchport mode dot1q-tunnel
```

```
interface GigabitEthernet0/0.500  
encapsulation dot1Q 500 second-dot1q any
```