VPN. Туннели в маршрутизируемых сетях

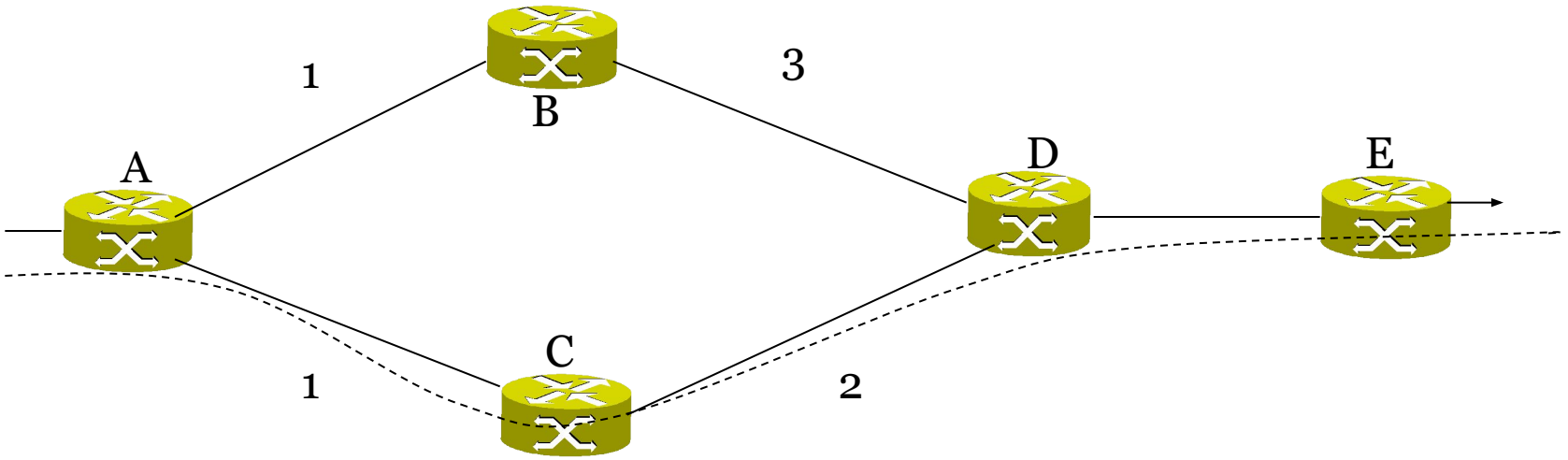
- MPLS+VRF
- L2TP
- PPTP

Цель создания

Недостатки IP-маршрутизации:

- Использование ЦП (в старых моделях)
- Обработка каждого пакета
- отсутствие балансировки нагрузки (кроме специальных настроек OSPF). Т.о. некоторые пути не используются, постоянное переназначение метрик приводит к нестабильности сети, управление трафиком посредством IGP слишком медленное, маршрутизация зависит только от топологии.

Недостатки IP маршрутизации



Пример: Используется путь A-C-D-E, путь A-B-D оказывается не загружен

MPLS

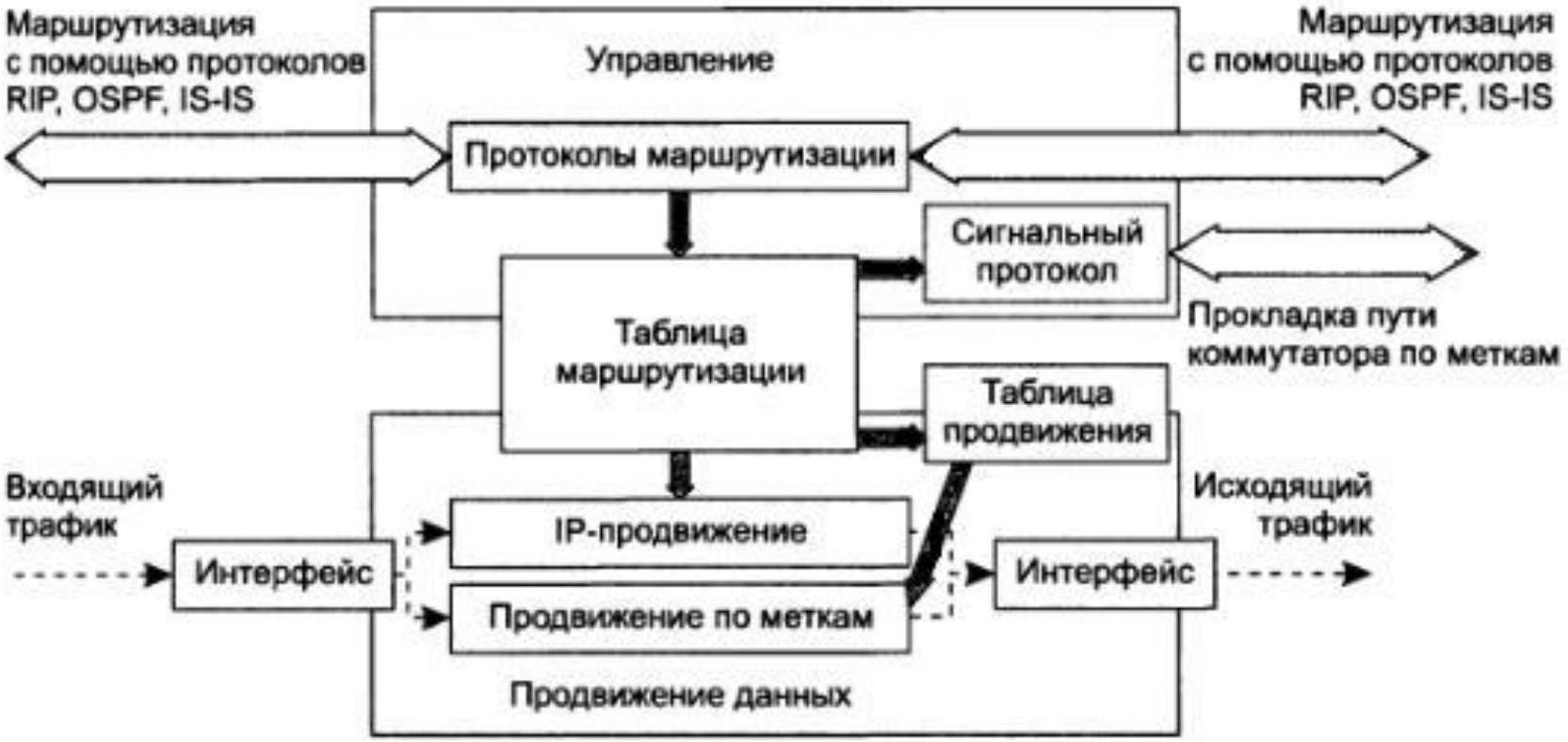
- **Цель:** ускорить процесс маршрутизации IP-пакетов, расширить возможности обработки трафика в зависимости от типа приложения.

- **Идея:** коммутация меток. Каждый пакет снабжается меткой, которая несет в себе информацию о следующем узле сети. Метка добавляется к пакету (т. е. между 2 и 3 уровнем). Т.О. каждый пакет ассоциируется к определенным потоком.

- **Преимущества:** высокая скорость передачи пакетов за счет обработки метки короткого фиксированного размера (20 бит), анализ заголовка IP-пакета только на входе в MPLS-облако, эффективное управление трафиком, поддержка балансировки нагрузки, создание виртуальных каналов.

Как работает IP маршрутизатор

Как работает MPLS коммутатор

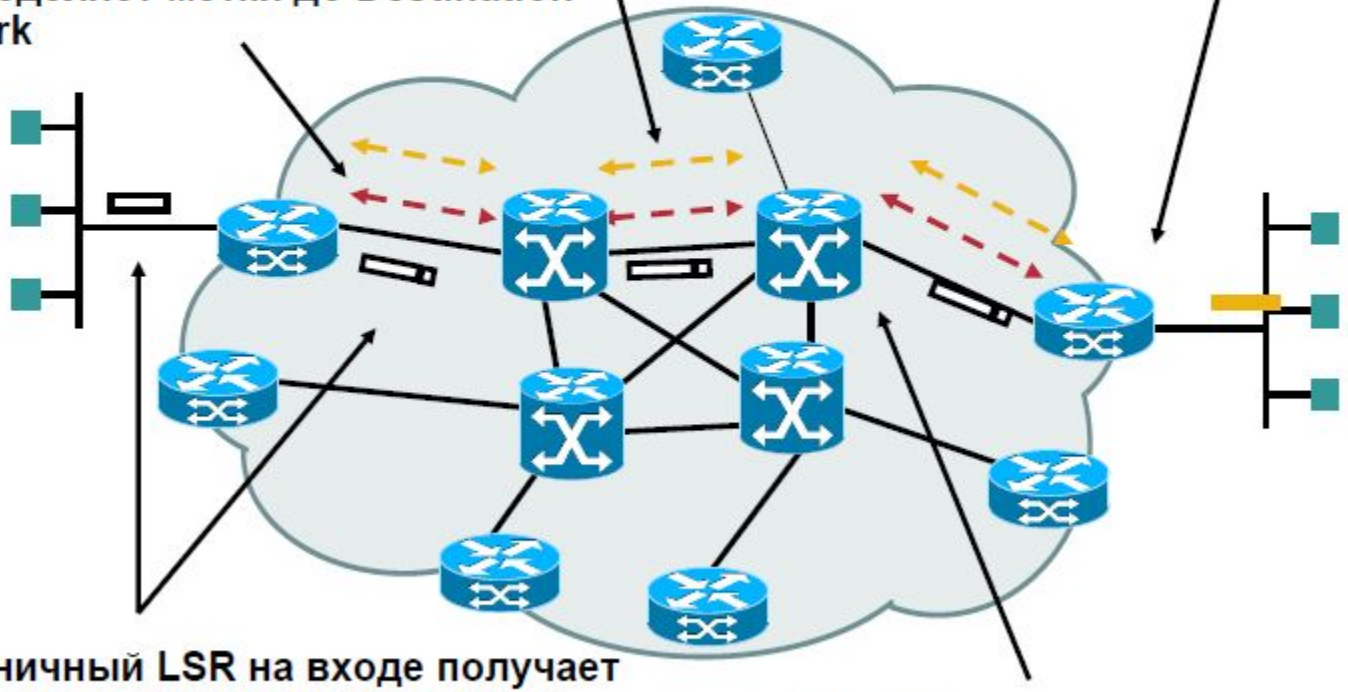


Как работает MPLS

1a. Существующие протоколы маршрутизации (OSPF, IS-IS) устанавливают доступность сети

1b. Label Distribution Protocol (LDP) Распределяет метки до Destination Network

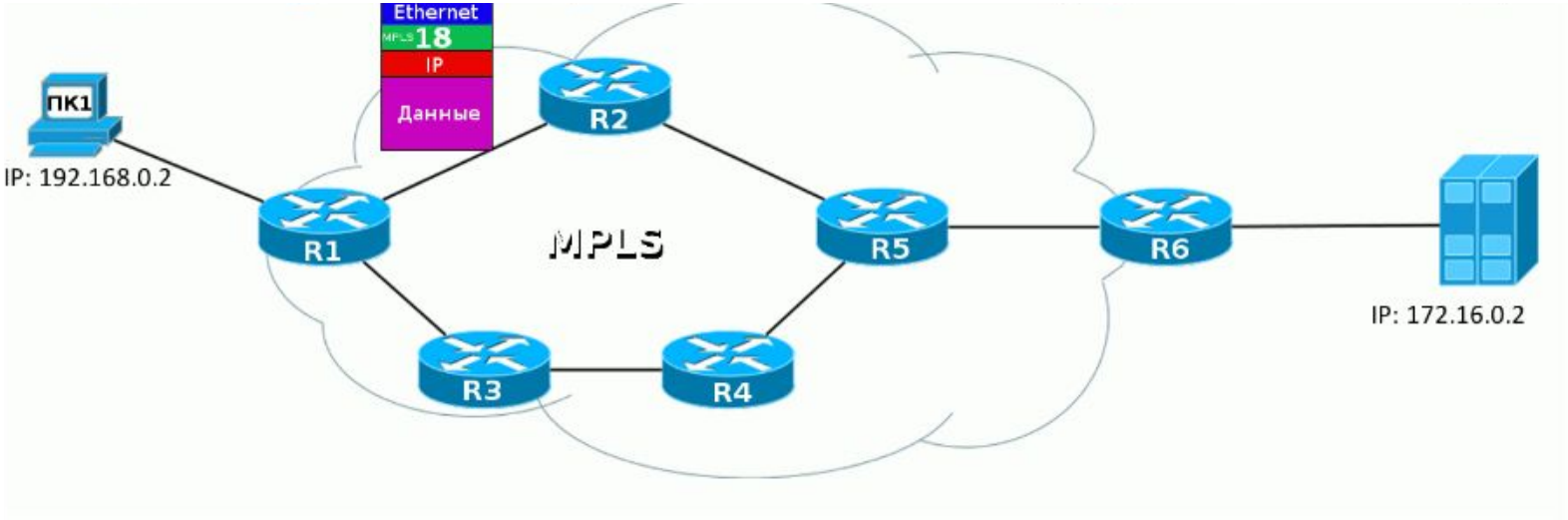
4. Граничный LSR на выходе убирает метку и доставляет пакет



2. Граничный LSR на входе получает пакет, выполняет Layer 3 сервисы, добавляет метку к пакету

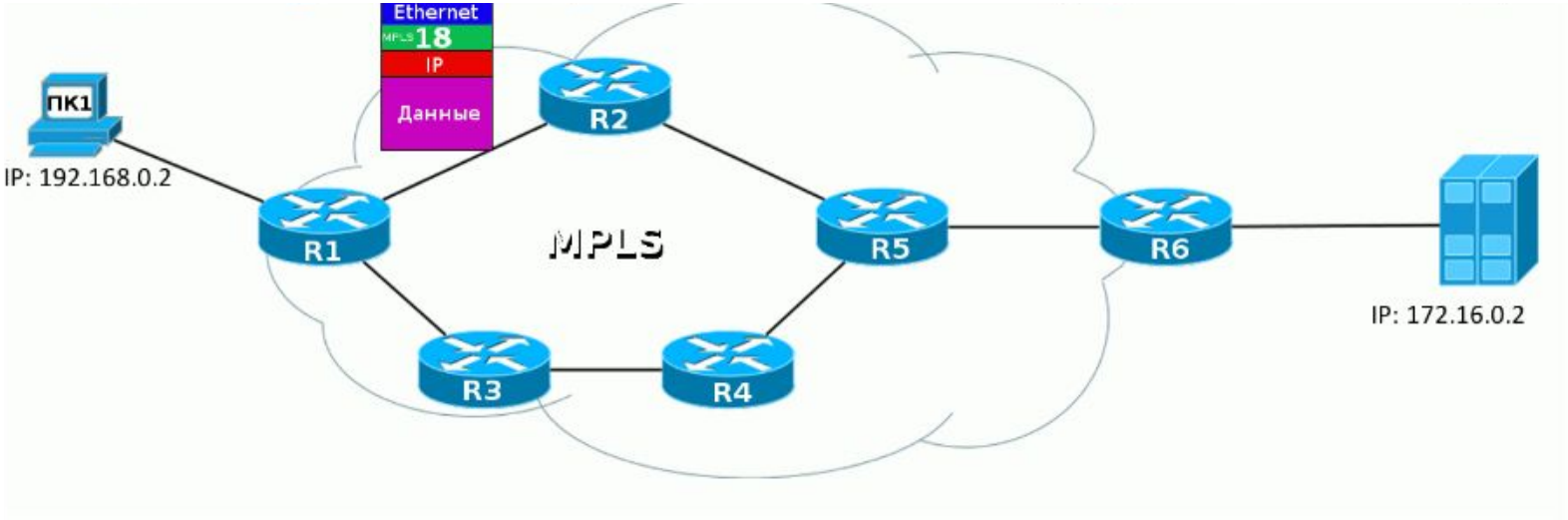
3. LSR коммутируют пакеты на основании меток

Работа MPLS



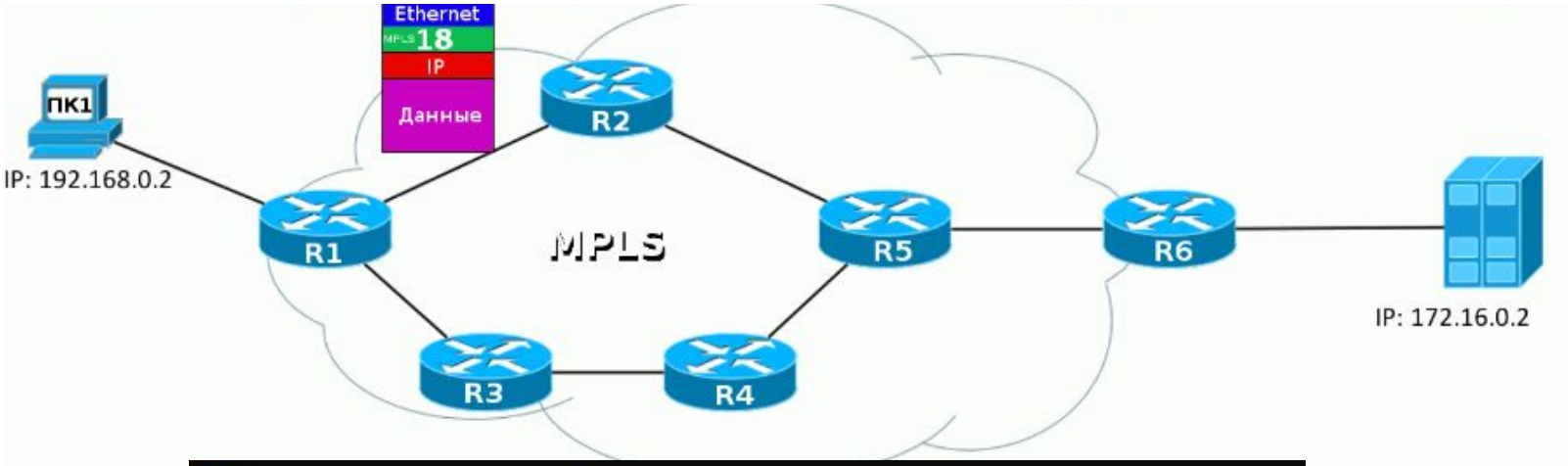

```
R1#sh ip cef detail | begin 172.16.0.0
172.16.0.0/24, version 19, epoch 0, cached adjacency 10.0.12.2
0 packets, 0 bytes
  tag information set
    local tag: 21
    fast tag rewrite with Fa0/0, 10.0.12.2, tags imposed: {18}
  via 10.0.12.2, FastEthernet0/0, 0 dependencies
    next hop 10.0.12.2, FastEthernet0/0
    valid cached adjacency
    tag rewrite with Fa0/0, 10.0.12.2, tags imposed: {18}
```

Работа MPLS




```
R2#sh mpls forwarding-table 172.16.0.0
Local  Outgoing    Prefix           Bytes tag   Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched    interface
18     20          172.16.0.0/24    590         Fa0/0       10.0.25.5
```

Работа MPLS




```
R1#sh mpls forwarding-table 6.6.6.6
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
21     18          6.6.6.6/32       0          Fa0/0       10.0.12.2
```

```
R2#sh mpls forwarding-table 6.6.6.6
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
18     20          6.6.6.6/32       0          Fa0/0       10.0.25.5
```

```
R5#sh mpls forwarding-table 6.6.6.6
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
20     Pop tag     6.6.6.6/32       0          Fa1/0       10.0.56.6
```

```
R6#sh ip interface brief loopback 0
Interface                  IP-Address      OK? Method Status
Loopback0                  6.6.6.6         YES NVRAM  up
```

MPLS терминология

Label — метка — значение от 0 до 1 048 575. На основе неё LSR принимает решение, что с пакетом делать.

Label Stack — стек меток. Каждый пакет может нести одну, две, три, и больше меток
Push Label — операция добавления метки к пакету данных

Swap Label — операция замены метки

Pop Label — операция удаления метки

MPLS терминология

LSR — *Label Switch Router* — это любой маршрутизатор в сети MPLS.
Intermediate LSR — промежуточный маршрутизатор MPLS — он выполняет операцию Swap Label
Ingress LSR — «входной», первый маршрутизатор MPLS — он выполняет операцию Push Label .
Egress LSR — «выходной», последний маршрутизатор MPLS — он выполняет операцию Pop Label ..

MPLS терминология

LER — *Label Edge Router* — это маршрутизатор на границе сети MPLS.
В частности Ingress LSR и Egress LSR являются граничными, а значит они тоже LER.

LSP — *Label Switched Path* — путь переключения меток. Это однонаправленный канал от Ingress LSR до Egress LSR, то есть путь, по которому фактически пройдёт пакет через MPLS-сеть. Иными словами — это последовательность LSR.

MPLS терминология

LIB — *Label Information Base* — таблица меток. Аналог таблицы маршрутизации (RIB) в IP. В ней указано для каждой входной метки, что делать с пакетом — поменять метку или снять её и в какой интерфейс отправить.
LFIB — *Label Forwarding Information Base* — по аналогии с FIB — это база меток, к которой обращается сетевой процессор. При получении нового пакета нет нужды обращаться к CPU и делать lookup в таблицу меток — всё уже под рукой.

Заголовок MPLS

Label — собственно сама метка. Длина — 20 бит.
TC — Traffic Class. Несёт в себе приоритет пакета
S — Bottom of Stack — индикатор дна стека меток длиной в 1 бит.
TTL — Time To Live — полный аналог IP TTL. Даже той же самой длиной обладает — 8 бит. Единственная задача — не допустить бесконечного блуждания пакета по сети в случае петли. При передаче IP-пакета через сеть MPLS значение IP TTL может быть скопировано в MPLS TTL, а потом обратно. Либо отсчёт начнётся опять с 255, а при выходе в чистую сеть IP значение IP TTL будет таким же, как до входа.

Протокол сизнализации

- **Протокол сигнализации необходим для:**
  - уведомлении маршрутизаторов LSR вдоль пути о необходимости настройки меток
  - согласования значения меток – чтобы они относились к одному и тому же пути в разных LSR

Назначение протокола LDP

Протокол LDP предназначен для построения целостных маршрутов коммутации по меткам LSP.

Установка соседских отношений

- Установление соседских отношений между маршрутизаторами осуществляется в две фазы:
- обмен сообщениями Hello;
- установление сессии LDP.

Параметры функционирования LDP

Существует несколько параметров функционирования LDP:

- режим обмена информацией о метках (Label Distribution Mode)
- режим контроля над распространением меток (Label Distribution Control)
- механизм сохранения меток (Label Retention Mode)

Режим обмена информацией о метках

Между соседями возможно использования двух режимов обмена информацией о метках:
Downstream On Demand - с запросом;

- Downstream Unsolicited - без запроса.

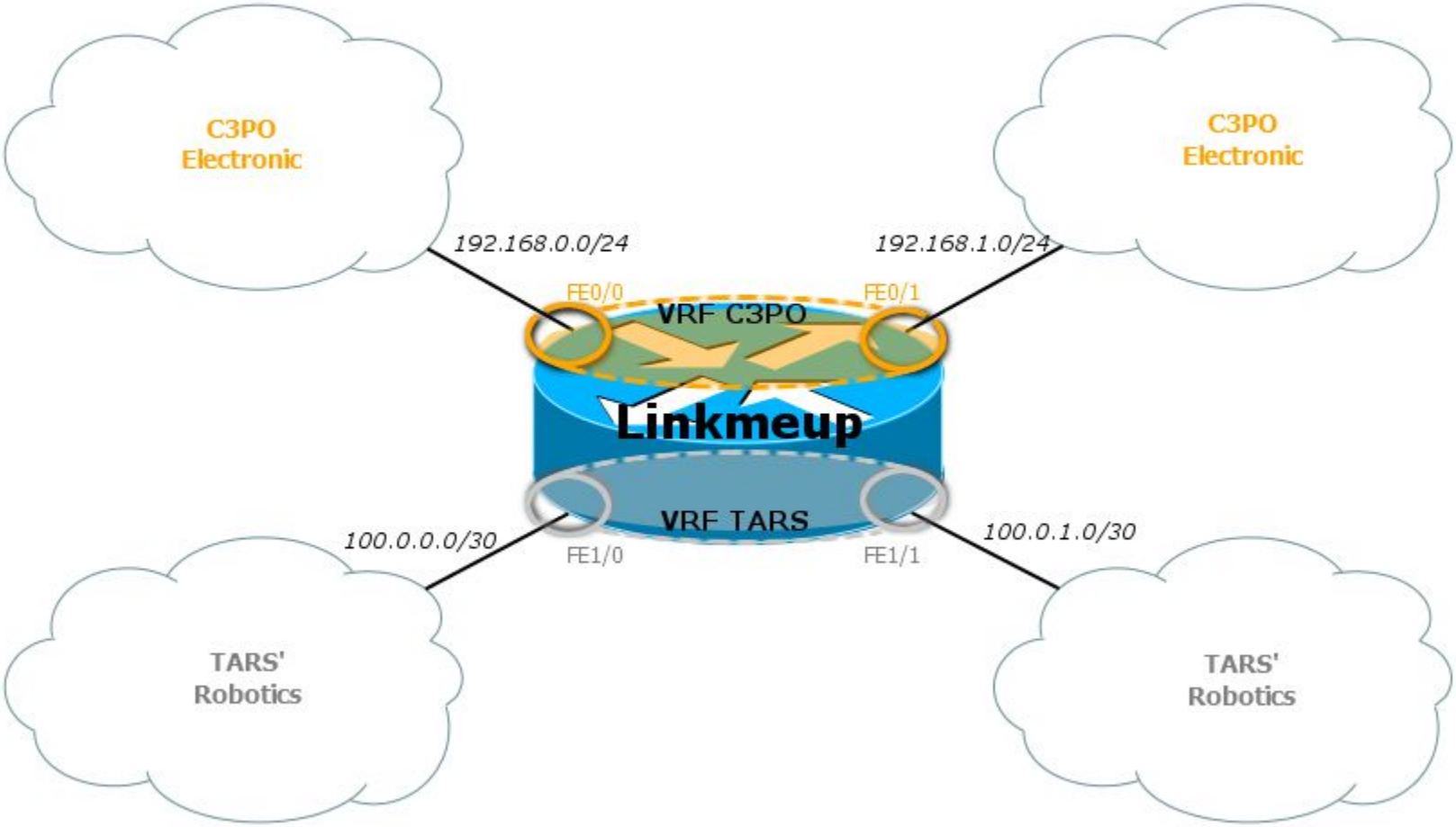
Механизм контроля над распространением меток

- Independent Label Distribution Control - независимый контроль;
- Ordered Label Distribution Control - упорядоченный контроль

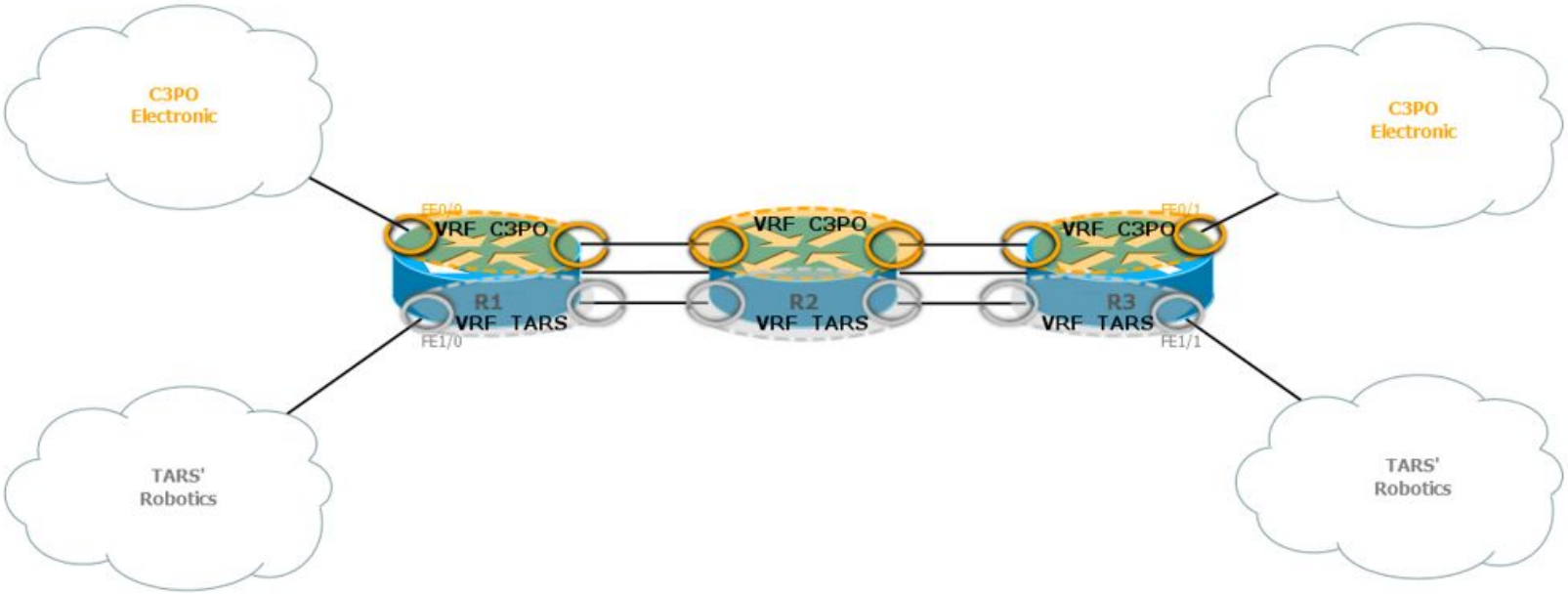
Режим сохранения меток

- Conservative Label Retention Mode (сдержанный режим сохранения меток);
- Liberal Label Retention Mode (свободный режим сохранения меток).

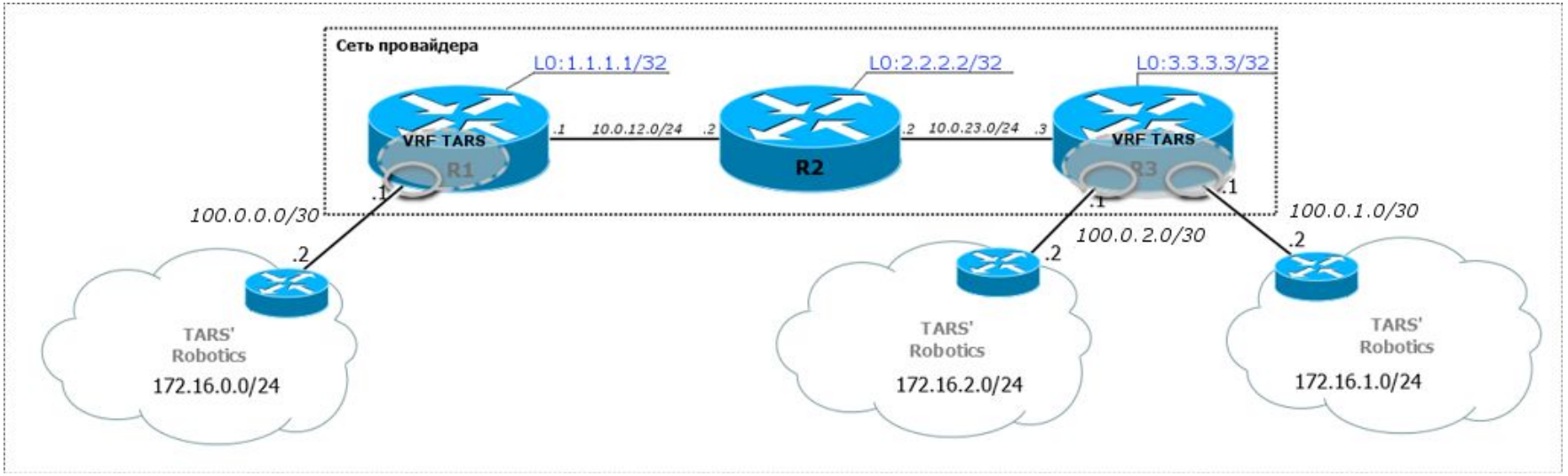
VRF


C3PO
Electronic
C3PO
Electronic
192.168.0.0/24
192.168.1.0/24
FE0/0
FE0/1
VRF C3PO
Linkmeup
VRF TARS
100.0.0.0/30
100.0.1.0/30
FE1/0
FE1/1
TARS'
Robotics
TARS'
Robotics

VRF


C3PO
Electronic
C3PO
Electronic
VRF C3PO
VRF C3PO
VRF C3PO
R1
VRF TARS
R2
VRF TARS
R3
VRF TARS
TARS'
Robotics
TARS'
Robotics

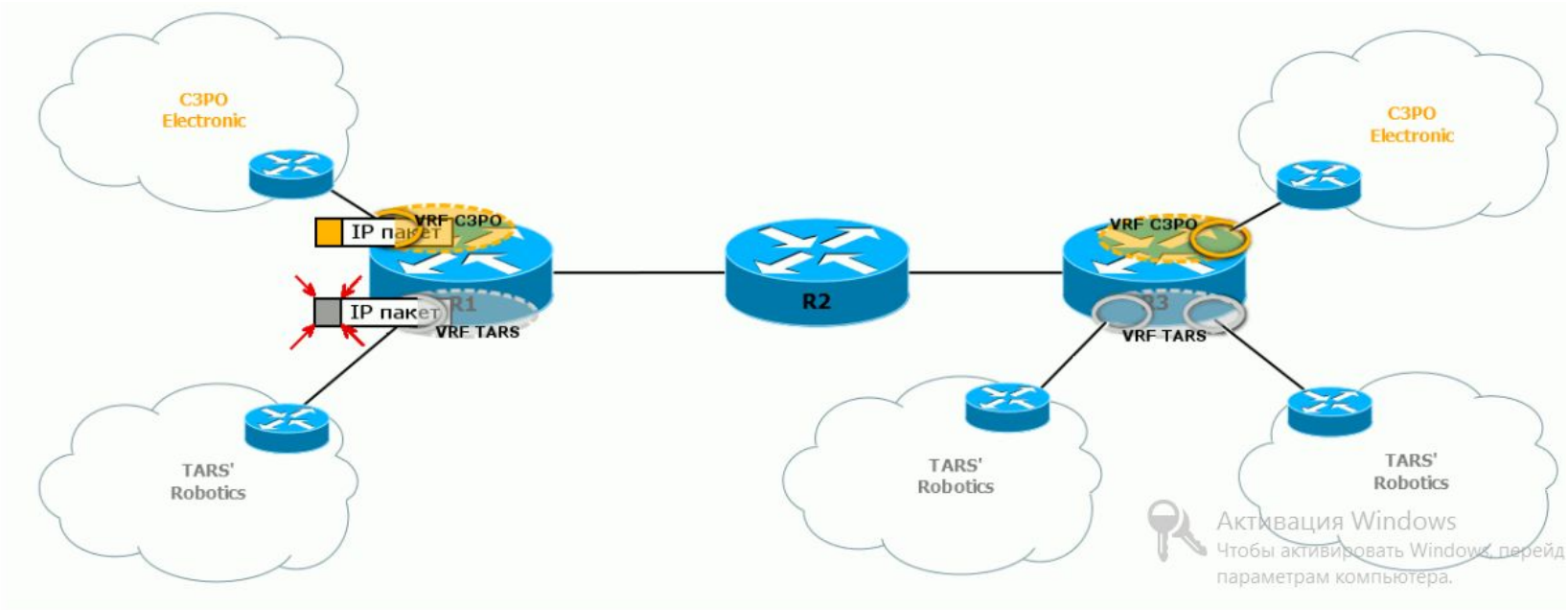
VRF+MPLS


Сеть провайдера
L0:1.1.1.1/32
L0:2.2.2.2/32
L0:3.3.3.3/32
VRF TARS
R1
.1
10.0.12.0/24
.2
R2
.2
10.0.23.0/24
.3
VRF TARS
R3
.1
100.0.0.0/30
.2
.1
100.0.2.0/30
.2
.1
100.0.1.0/30
.2
TARS'
Robotics
172.16.0.0/24
TARS'
Robotics
172.16.2.0/24
TARS'
Robotics
172.16.1.0/24

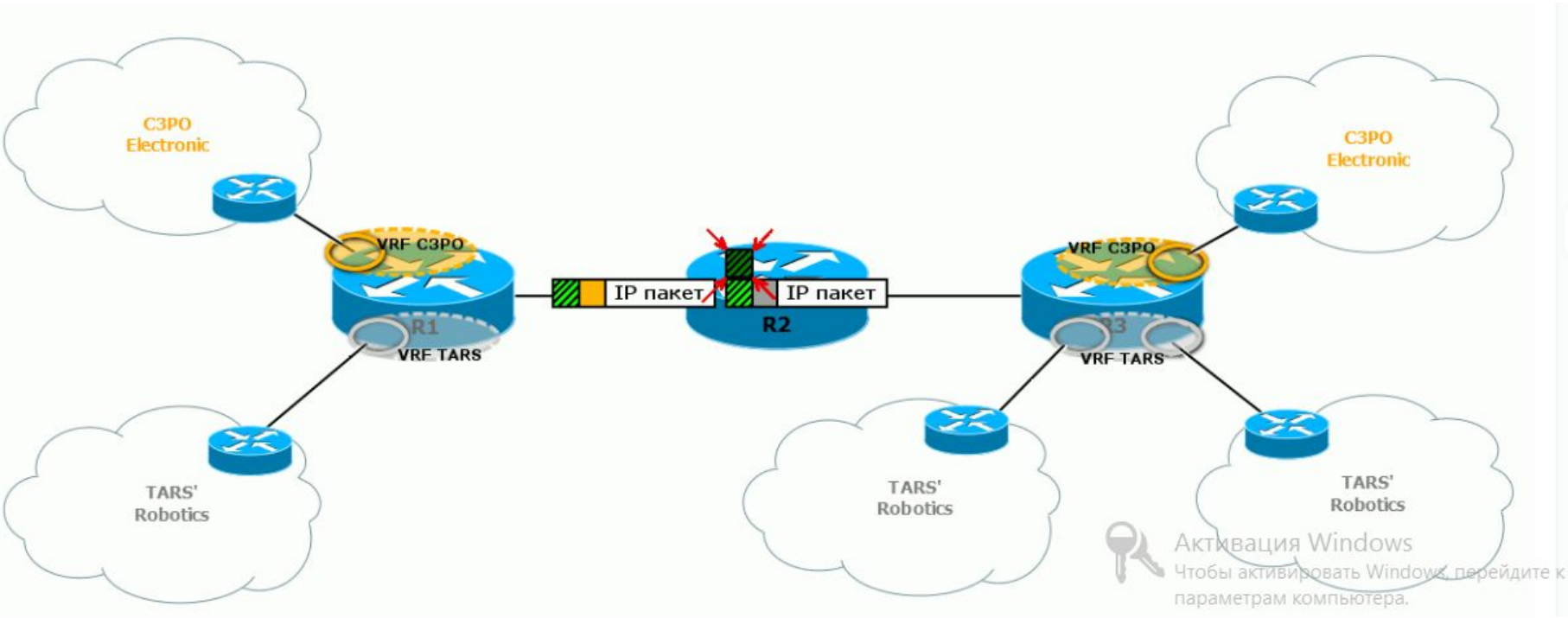
Стек меток


Заголовок L2
Транспортная метка
Сервисная метка
IP
Данные
Заголовок L2
Транспортная метка
Сервисная метка
IP
Данные

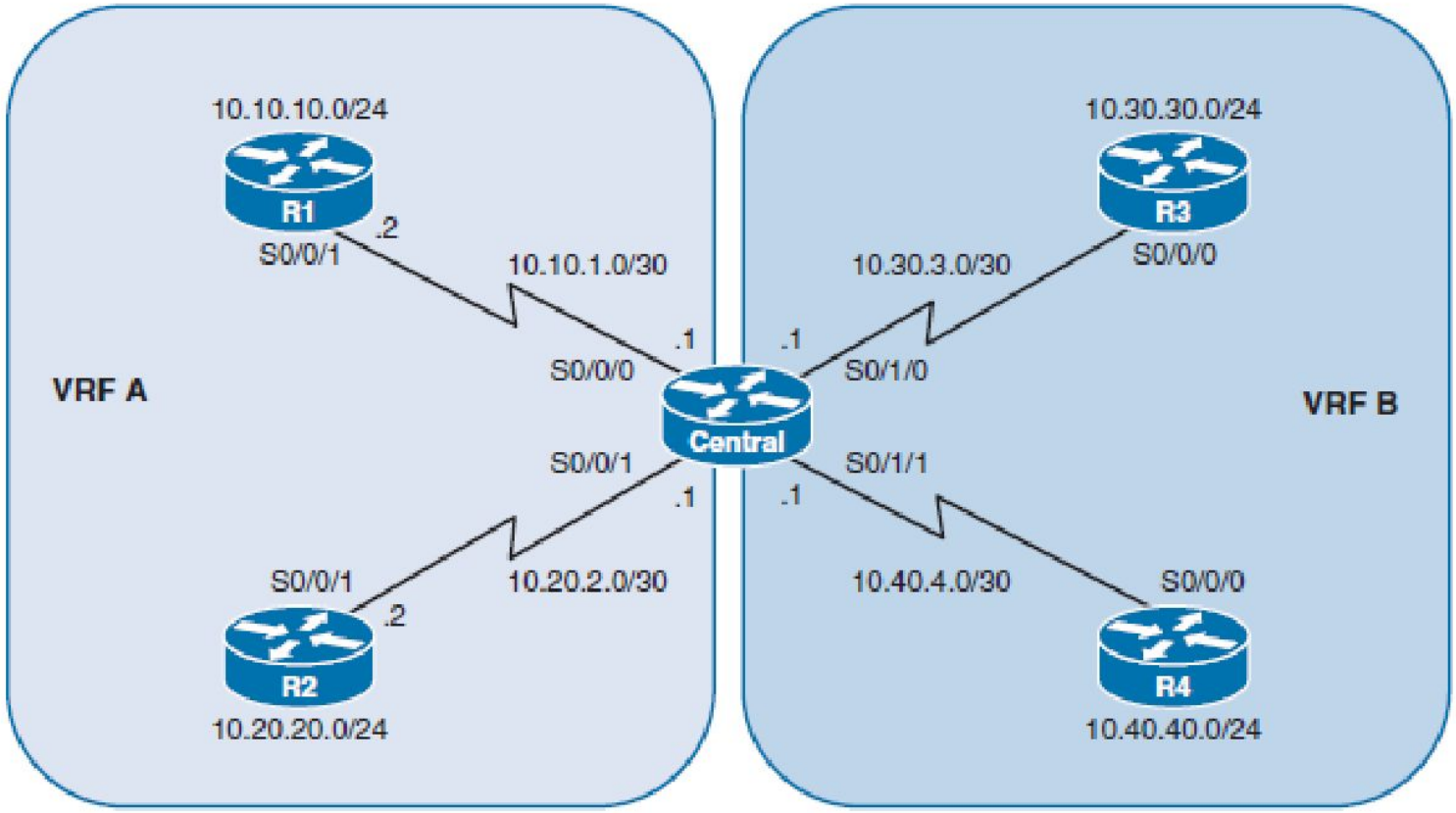
Стек меток


C3PO
Electronic
IP пакет
VRF C3PO
IP пакет
R1
VRF TARS
R2
VRF C3PO
R3
VRF TARS
C3PO
Electronic
TARS'
Robotics
TARS'
Robotics
TARS'
Robotics
Активация Windows
Чтобы активировать Windows, перейд
параметрам компьютера.

VRF+MPLS=VPN



Конфигурация VRF



Конфигурация VRF (1)

```
Central(config)# ip vrf VRF-A
Central(config-vrf)# exit
Central(config)# ip vrf VRF-B
Central(config-vrf)# exit
Central(config)# interface Serial0/0/0
Central(config-if)# ip vrf forwarding VRF-A
Central(config-if)# ip address 10.10.1.1 255.255.255.252
Central(config-if)# clock rate 2000000
Central(config-if)# no shut
Central(config-if)# exit
Central(config)#
Central(config-if)# interface Serial0/0/1
Central(config-if)# ip vrf forwarding VRF-A
Central(config-if)# ip address 10.20.2.1 255.255.255.252
Central(config-if)# no shut
Central(config-if)# exit
```

Конфигурация VRF(2)

```
Central(config-if)# interface Serial0/1/0
Central(config-if)# ip vrf forwarding VRF-B
Central(config-if)# ip address 10.30.3.1 255.255.255.252
Central(config-if)# clock rate 2000000
Central(config-if)# no shut
Central(config-if)# exit
Central(config)#
Central(config-if)# interface Serial0/1/1
Central(config-if)# ip vrf forwarding VRF-B
Central(config-if)# ip address 10.40.4.1 255.255.255.252
Central(config-if)# no shut
Central(config-if)# exit
Central(config)#
```

Проверка таблицы маршрутизации

```
Central# show ip route | begin Gateway
Gateway of last resort is not set

Central#
Central# show ip route vrf VRF-A | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.10.1.0/30 is directly connected, Serial0/0/0
L        10.10.1.1/32 is directly connected, Serial0/0/0
C        10.20.2.0/30 is directly connected, Serial0/0/1
L        10.20.2.1/32 is directly connected, Serial0/0/1
Central#
Central# show ip route vrf VRF-B | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.30.3.0/30 is directly connected, Serial0/1/0
L        10.30.3.1/32 is directly connected, Serial0/1/0
C        10.40.4.0/30 is directly connected, Serial0/1/1
L        10.40.4.1/32 is directly connected, Serial0/1/1
Central#
```

конфигурация EIGRP for VRF-A

```
Central(config)# router eigrp 1
Central(config-router)# address-family ipv4 vrf VRF-A
Central(config-router-af)# network 10.10.1.0 0.0.0.3
Central(config-router-af)# network 10.20.2.0 0.0.0.3
Central(config-router-af)# autonomous-system 1
Central(config-router-af)# no auto-summary
Central(config-router-af)#
*Aug  5 04:45:35.879: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.20.2.2
(Serial0/0/1) is up: new adjacency
*Aug  5 04:45:35.883: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.10.1.2
(Serial0/0/0) is up: new adjacency
Central(config-router-af)# ^Z
Central#
```

Проверка таблицы маршрутизацииVRF-A

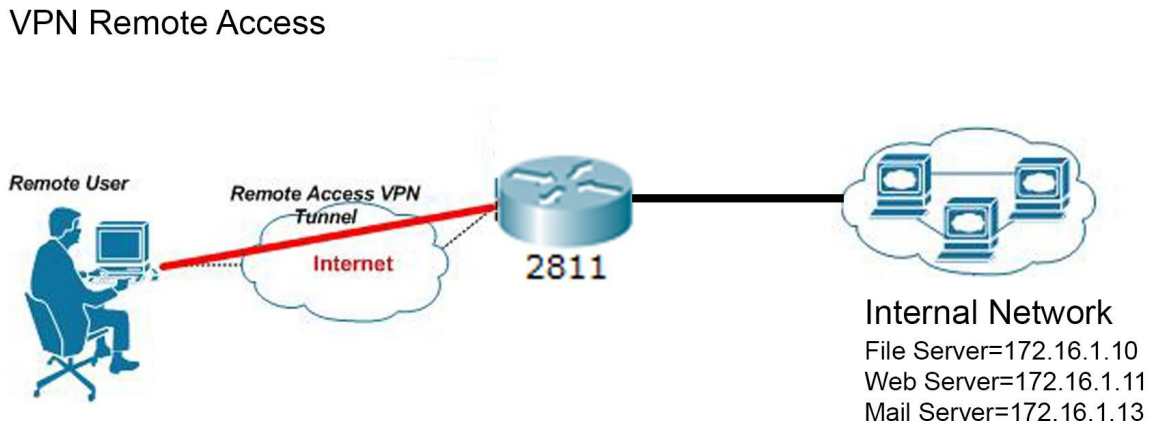
```
Central# show ip route vrf VRF-A | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
C        10.10.1.0/30 is directly connected, Serial0/0/0
L        10.10.1.1/32 is directly connected, Serial0/0/0
D        10.10.10.0/24 [90/2297856] via 10.10.1.2, 00:00:06, Serial0/0/0
C        10.20.2.0/30 is directly connected, Serial0/0/1
L        10.20.2.1/32 is directly connected, Serial0/0/1
D        10.20.20.0/24 [90/2297856] via 10.20.2.2, 00:05:41, Serial0/0/1
Central# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
% No usable Router-ID found
Central#
Central# show ip eigrp vrf VRF-A neighbors
EIGRP-IPv4 Neighbors for AS(1) VRF(VRF-A)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   10.20.2.2               Se0/0/1           13 00:43:42    3   100  0  4
0   10.10.1.2               Se0/0/0           11 00:47:54    1   100  0  5
Central#
```

конфигурация OSPF for VRF-B

```
Central(config)# router ospf 1 vrf VRF-B
Central(config-router)# router-id 5.5.5.5
Central(config-router)# network 10.30.3.0 0.0.0.3 area 0
Central(config-router)# network 10.40.4.0 0.0.0.3 area 0
Central(config-router)#
*Aug  5 04:47:22.327: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/1/0 from
LOADING to FULL, Loading Done
*Aug  5 04:47:22.467: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/1/1 from
LOADING to FULL, Loading Done
Central(config-router)# ^Z
Central#
```

L2pt

Протокол L2TP имитирует соединение типа "точка-точка" путем инкапсуляции дейтаграмм протокола PPP для их транспортировки по маршрутизируемым сетям или по объединенным сетям.
Используется для соединения Site –to-site и Remote Access, bcgjkmpetn IPSec (esp) для шифрования, аутентификация chap

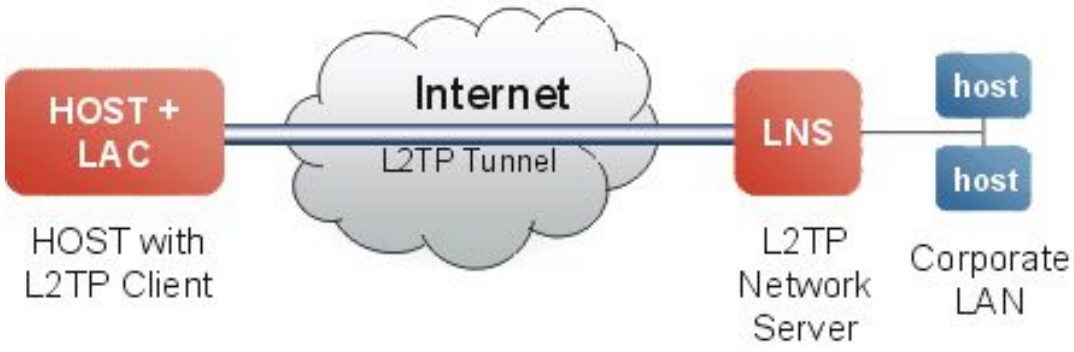


L2pt:инкапсуляция (IP)

Протокол L2TP имитирует соединение типа "точка-точка" путем инкапсуляции дейтаграмм протокола PPP для их транспортировки по маршрутизируемым сетям или по объединенным сетям.
Используется для соединения Site –to-site и Remote Access

protocol:115,
ip 192.168.1.45

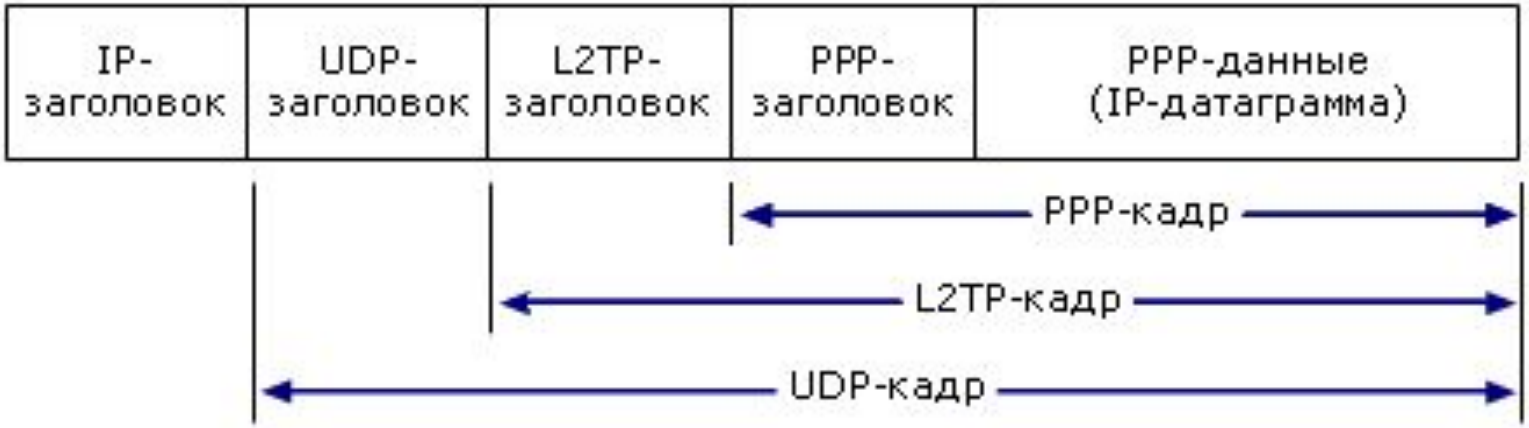
protocol:6
ip 172.16.5.4



ip 172.16.5.0/24

L2pt:инкапсуляция (UDP)

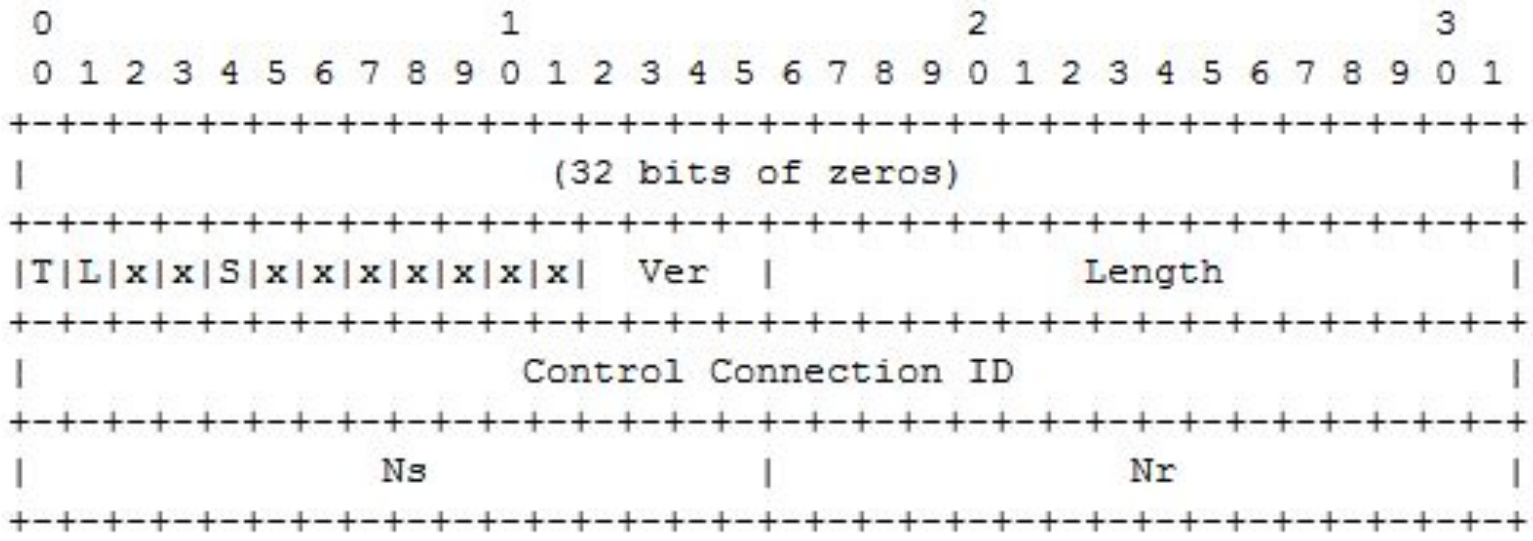
Протокол L2TP имитирует соединение типа "точка-точка" путем инкапсуляции дейтаграмм протокола PPP для их транспортировки по маршрутизируемым сетям или по объединенным сетям.
Используется для соединения Site –to-site и Remote Access



UDP 1701

L2pt:операции канала

Управляющее соединение
Установление сессии
Использование порядковых номеров в канале данных
Механизм keepalive (Hello)
Прерывание сессии



L2pt:конфигурация

Указываем роутеру аутентифицировать pptp клиентов по локальной базе (нужно, если включен aaa new model)
aaa authentication ppp default local
aaa authorization network default local
aaa authorization exec default local

Создаём пользователя (через secret бывают проблемы)
username <user> password <password>

Включаем использование виртуальных частных коммутируемых сетей

vpdn enable

L2pt:конфигурация

```
# Создаем группу
vpdn-group L2TP
   accept-dialin
   protocol l2tp
   virtual-template 10
   no l2tp tunnel authentication

# Настраиваем виртуальный интерфейс
interface Virtual-Template 10
   ip unnumbered FastEthernet0/1 #внутренний
   peer default ip address pool POOL-VPN
   ppp encrypt mppe auto
   ppp authentication pap chap ms-chap ms-chap-v2

# Создаем пул адресов для клиентов
ip local pool POOL-VPN 192.168.10.200 192.168.10.210
```

L2pt:конфигурация

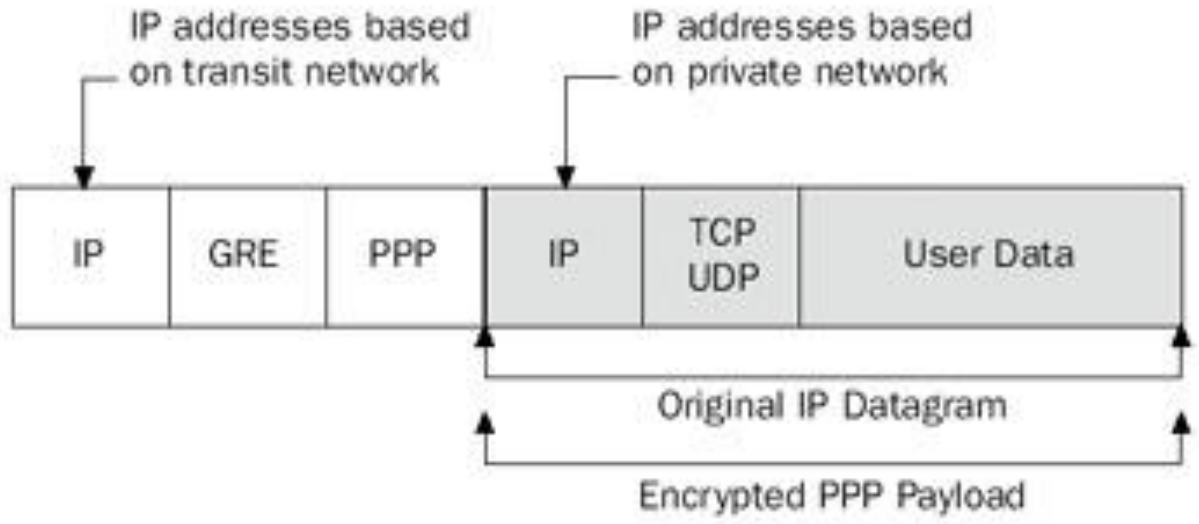
```
# Настраиваем метод авторизации - PreShare-Key
crypto isakmp policy 10
   encr 3des
   authentication pre-share
   group 2
   lifetime 3600
crypto isakmp key cisco address 0.0.0.0 0.0.0.0 no-xauth
crypto isakmp keepalive 3600

# Настраиваем IPSEC
crypto ipsec transform-set L2TP esp-3des esp-sha-hmac
   mode transport

# Создаём CryptoMap
crypto dynamic-map L2TP-map 10
   set nat demux
   set transform-set L2TP
crypto map TEST 10 ipsec-isakmp dynamic L2TP-map
```

L2pt:конфигурация

```
# Применяем CryptoMap на внешнем интрфейсе
interface FastEtherneto/o
   ip address IPвнешний 255.255.255.0
   duplex auto
   speed auto
   crypto map TEST
```

pptp:формат заголовка

PPTP работает, устанавливая обычную PPP сессию с противоположной стороной с помощью протокола Generic Routing Encapsulation.
Второе соединение на TCP-порте 1723 используется для инициации и управления GRE-соединением. PPTP сложно перенаправлять за сетевой экран, так как он требует одновременного установления двух сетевых сессий. PPTP-трафик может быть зашифрован с помощью MPPE.
Для аутентификации клиентов могут использоваться различные механизмы, например — MS-CHAPv2 и EAP-TLS.



Pptp:конфигурация

Указываем роутеру аутентифицировать pptp клиентов по локальной базе (нужно, если включен aaa new model)
aaa authentication ppp default local
aaa authorization network default local
aaa authorization exec default local

Создаём пользователя (через secret бывают проблемы)
username <user> password <password>

Включаем использование виртуальных частных коммутируемых сетей
vpdn enable

pptp:конфигурация

```
vpdn-group 1
   accept-dialin
   protocol pptp
   virtual-template 1

# Настраиваем виртуальный интерфейс
interface Virtual-Template1
   ip unnumbered FastEthernet0/1  (LAN интерфейс)
         # указываем пул из которого клиенту будет выдаваться адрес
   peer default ip address pool VPN
   no keepalive
          # включаем шифрование
   ppp encrypt mppe auto
            # указываем протокол аутентификации
   ppp authentication ms-chap-v2

# Создаем пул адресов для клиентов
ip local pool POOL-VPN 192.168.10.200 192.168.10.210
```