Лекция 15. Виртуальные частные сети. Технология MPLS VPN

Дисциплина: Сетевые технологии
Тема лекции: Виртуальные частные сети: технология многопротокольной коммутации с помощью меток (MPLS).

Цель лекции: Изучить принципы организации виртуальных частных сетей на основе технологии MPLS, рассмотреть классификацию MPLS VPN, компоненты сети, механизмы обмена маршрутной информацией и передачи пакетов, а также особенности защиты данных.

План лекции:

1. Понятие виртуальных частных сетей и технология MPLS.
2. Классификация сетей MPLS VPN.
3. Полная связность при абсолютной изолированности.
4. Компоненты сети MPLS VPN.
5. Разграничение маршрутной информации.
6. Использование протокола MP-BGP для связывания сайтов.
7. Независимость адресных пространств.
8. Генерация маршрутных объявлений MP-BGP.
9. Перемещение пакета по сети MPLS VPN.
10. Механизм формирования топологии VPN.
11. Степень защищённости MPLS VPN.

1. Понятие виртуальных частных сетей и технология MPLS

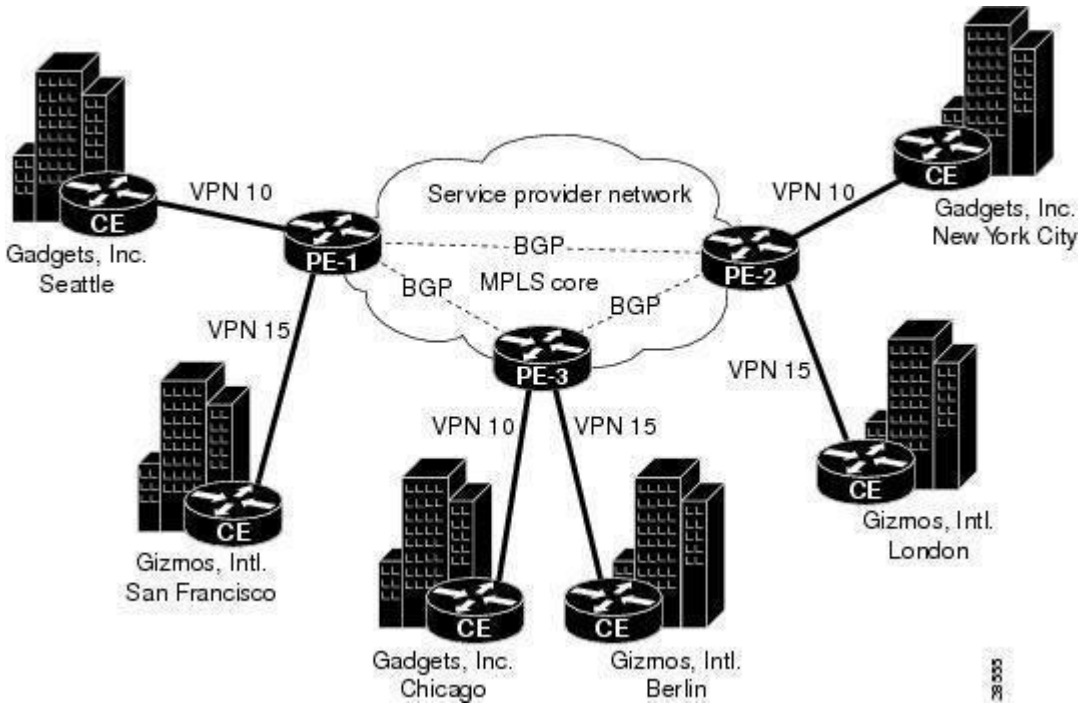
VPN (Virtual Private Network) — это виртуальная частная сеть, которая обеспечивает защищённое или логически изолированное взаимодействие между устройствами и локальными сетями через общую инфраструктуру связи.

VPN позволяет объединить удалённые офисы организации в единую корпоративную сеть. При этом офисы могут находиться в разных городах и странах.

Например, организация имеет три филиала:

- главный офис в Алматы;
- филиал в Астане;
- филиал в Усть-Каменогорске.

Каждый офис имеет собственную локальную сеть. С помощью VPN между ними может быть организован обмен данными через сеть оператора связи.



1.1. Что такое MPLS?

MPLS (Multiprotocol Label Switching) — это технология многопротокольной коммутации с помощью меток.

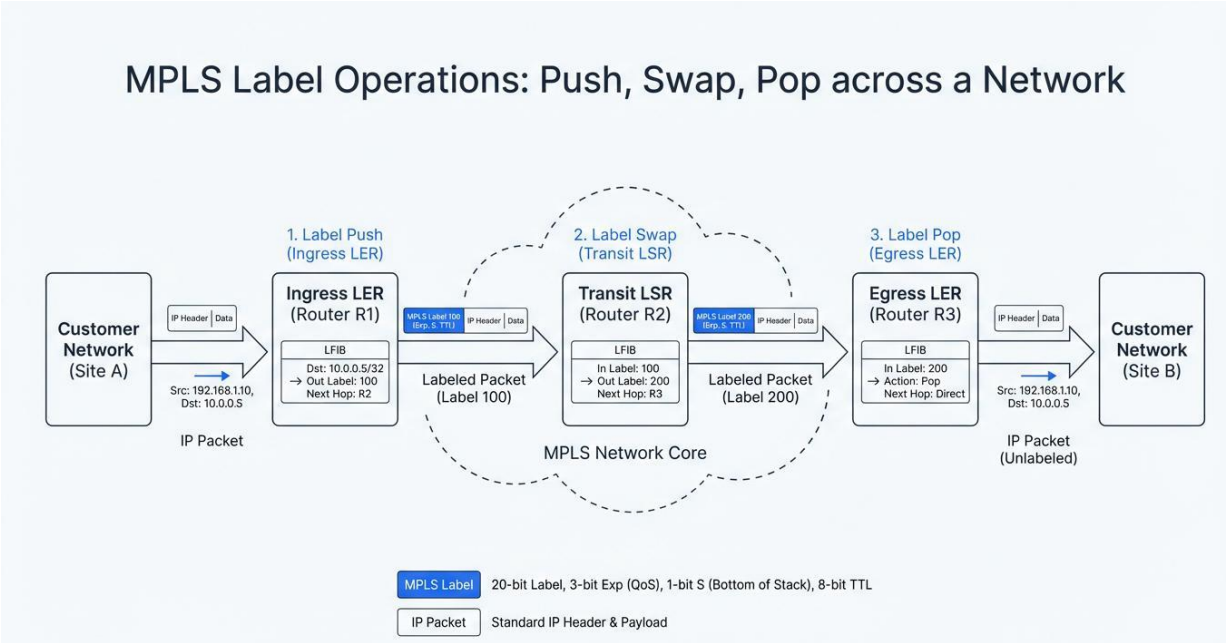
Она применяется в сетях операторов связи для эффективной передачи пакетов между узлами.

В обычной IP-сети маршрутизатор анализирует IP-адрес назначения и на основании таблицы маршрутизации выбирает следующий узел.

В сети MPLS передача данных осуществляется с использованием специальных меток (Labels).

Метка содержит идентификатор, который используется для выбора дальнейшего пути передачи пакета.

Таким образом, MPLS сочетает особенности маршрутизации IP и коммутации на основе меток.



1.2. Основные элементы технологии MPLS

В сети MPLS используются следующие устройства:

1. LER (Label Edge Router)

Пограничный маршрутизатор MPLS-сети. Он принимает пакеты от внешних сетей, добавляет или удаляет метки.

Различают:

- Ingress LER: входной пограничный маршрутизатор;
- Egress LER: выходной пограничный маршрутизатор.

2. LSR (Label Switching Router)

Внутренний маршрутизатор MPLS-сети. Он анализирует метку пакета и заменяет её на другую в соответствии с таблицей коммутации.

3. Label (метка)

Специальное значение, которое используется для определения пути передачи пакета.

1.3. Принцип работы MPLS

Передача данных выполняется в несколько этапов:

1. Пакет поступает на входной маршрутизатор MPLS.
2. Маршрутизатор определяет необходимый путь.
3. К пакету добавляется MPLS-метка.
4. Внутренние маршрутизаторы передают пакет на основании метки.
5. На выходном маршрутизаторе метка удаляется.
6. Пакет передаётся получателю.

Главное отличие MPLS заключается в том, что внутри MPLS-домена решение о передаче пакета принимается на основании метки, а не полного анализа IP-адреса назначения.

2. Классификация сетей MPLS VPN

MPLS VPN применяются для организации взаимодействия между корпоративными сетями через инфраструктуру оператора связи.

Существует несколько основных видов MPLS VPN.

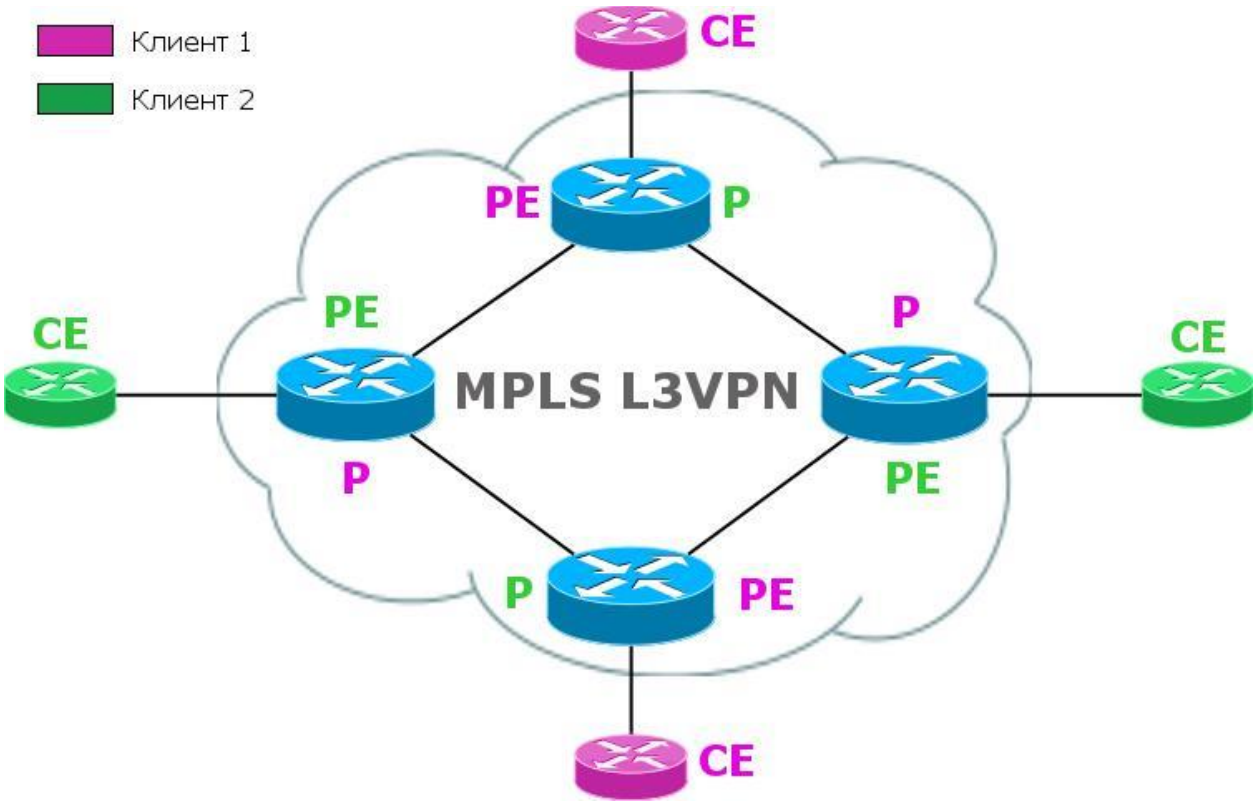
2.1. Layer 3 MPLS VPN (L3VPN)

L3VPN работает на третьем уровне модели OSI, то есть на сетевом уровне.

Оператор связи обеспечивает маршрутизацию между локальными сетями клиентов.

Каждый клиент получает отдельную таблицу маршрутизации на пограничном маршрутизаторе оператора.

Например, две организации могут использовать одну инфраструктуру оператора, но их сетевой трафик будет логически разделён.



Особенности L3VPN:

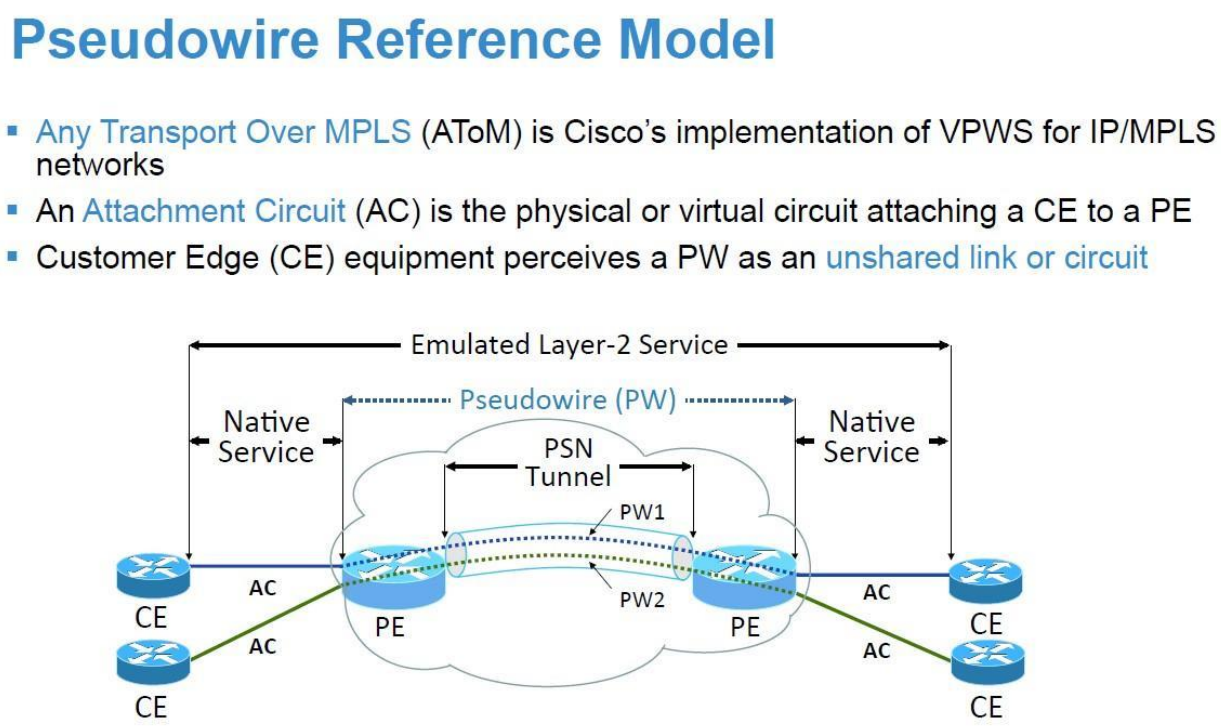
- маршрутизация выполняется оператором связи;
- для каждого клиента создаётся отдельный набор маршрутов;
- поддерживается взаимодействие между удалёнными офисами;
- адресные пространства разных клиентов могут совпадать.

2.2. Layer 2 MPLS VPN (L2VPN)

L2VPN работает на канальном уровне модели OSI.

Оператор связи обеспечивает передачу Ethernet-кадров между удалёнными площадками клиента.

Для клиента соединение может выглядеть как единая локальная сеть, хотя физически офисы находятся на значительном расстоянии.



Основные варианты L2VPN:

- VPWS (Virtual Private Wire Service): организация соединения между двумя точками;
- VPLS (Virtual Private LAN Service): объединение нескольких площадок в общую виртуальную локальную сеть.

2.3. Сравнение L2VPN и L3VPN

Характеристика	L2VPN	L3VPN
Уровень OSI	Канальный	Сетевой
Передаваемые данные	Ethernet-кадры	IP-пакеты
Маршрутизация	Выполняет клиент	Выполняет оператор
Управление IP-адресами	Клиент	Клиент
Основное назначение	Объединение локальных сетей	Связь удалённых IP-сетей

3. Полная связность при абсолютной изолированности

Одной из важных особенностей MPLS VPN является возможность организации полной связности между филиалами при сохранении логической изоляции разных клиентов.

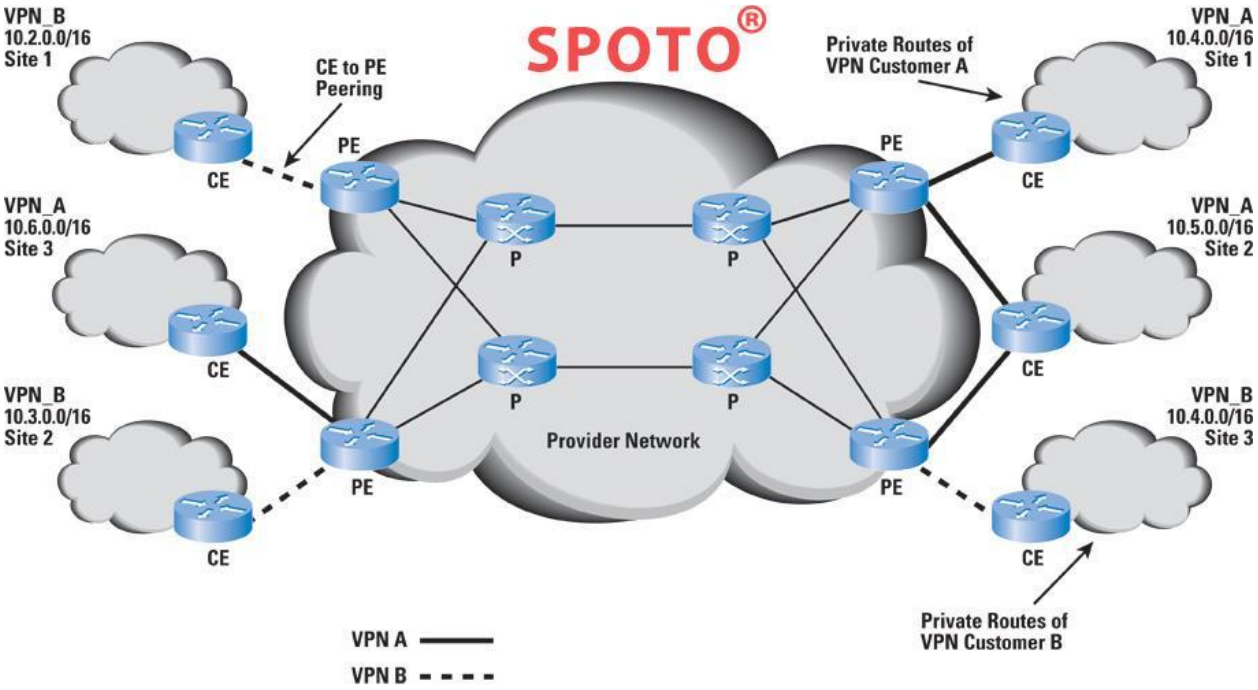
Рассмотрим пример.

Оператор связи обслуживает две организации:

- Компания A имеет три филиала.
- Компания B имеет три филиала.

Все шесть филиалов подключены к одной инфраструктуре MPLS.

При этом филиалы компании A могут обмениваться данными между собой, а филиалы компании B работают независимо.



Что означает полная связность?

Полная связность (Full Mesh) означает, что каждый филиал одной VPN может обмениваться данными с любым другим филиалом той же VPN.

Например:

- филиал A1 взаимодействует с A2;
- филиал A1 взаимодействует с A3;
- филиал A2 взаимодействует с A3.

При этом прямое соединение между каждым филиалом не требуется. Передача осуществляется через инфраструктуру оператора.

Что означает изолированность?

Изолированность означает, что данные одной VPN не должны попадать в другую VPN.

Например:

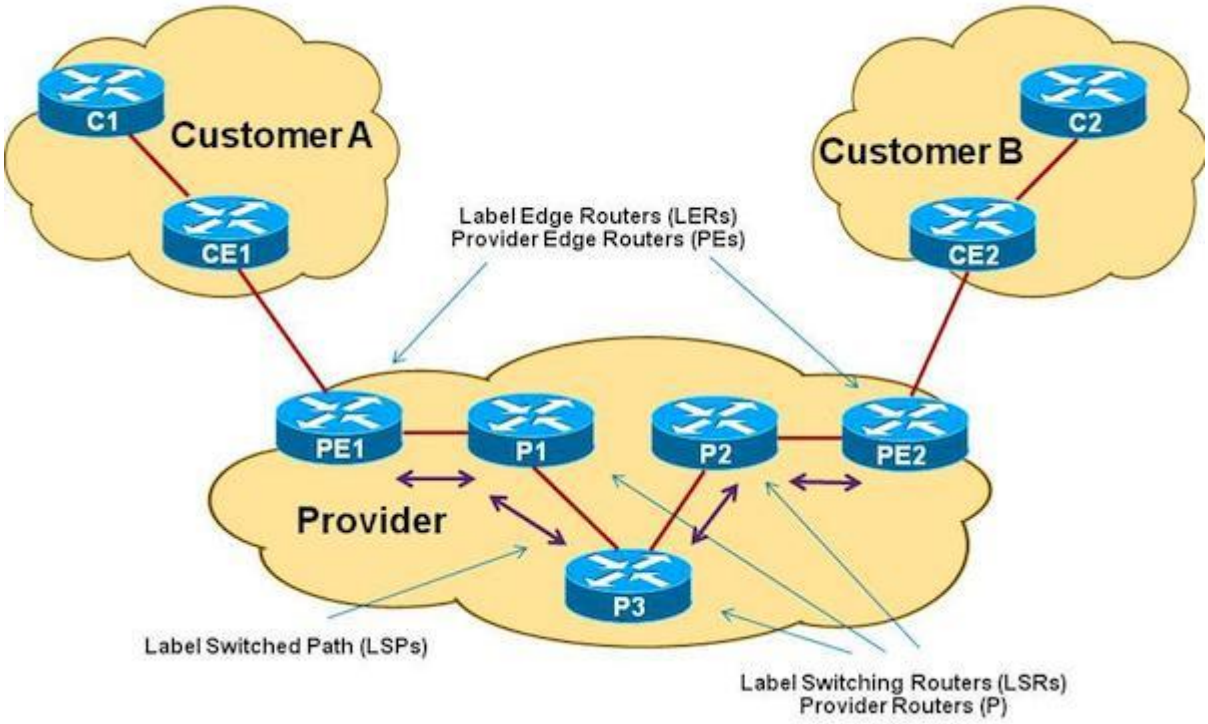
- Компания A не получает маршруты компании B.
- Компания B не получает маршруты компании A.
- Обе компании используют общую физическую инфраструктуру оператора.

Таким образом, одна сеть MPLS может обслуживать большое количество независимых корпоративных VPN.

4. Компоненты сети MPLS VPN

Для организации MPLS VPN используются маршрутизаторы оператора связи и маршрутизаторы клиентов.

В архитектуре MPLS VPN выделяют три основных компонента.



4.1. CE (Customer Edge)

CE — это маршрутизатор или другое сетевое устройство, которое находится на стороне клиента.

Его основные функции:

- подключение локальной сети клиента к сети оператора;
- передача IP-пакетов в сеть оператора;
- получение маршрутов от оператора;
- обмен маршрутной информацией с маршрутизатором PE.

CE не обязан поддерживать технологию MPLS. Обычно он работает с обычными IP-пакетами.

4.2. PE (Provider Edge)

PE — это пограничный маршрутизатор оператора связи.

Он является одним из главных элементов MPLS VPN.

Основные функции PE:

- подключение сетей разных клиентов;
- создание отдельных таблиц маршрутизации VPN;
- получение маршрутов от маршрутизаторов CE;
- передача маршрутов через MP-BGP;
- добавление и удаление MPLS-меток;
- разделение трафика разных клиентов.

На PE создаются специальные виртуальные таблицы маршрутизации, которые называются VRF.

4.3. P (Provider)

P — это внутренний маршрутизатор оператора связи.

Он находится внутри MPLS-сети и не подключается непосредственно к локальным сетям клиентов.

Основные функции:

- передача MPLS-пакетов;
- коммутация меток;
- поддержка путей передачи данных;
- обеспечение связи между пограничными маршрутизаторами PE.

Маршрутизатор P обычно не хранит маршруты отдельных клиентских VPN.

4.4. Сравнение компонентов MPLS VPN

Компонент	Расположение	Основная функция
CE	Сеть клиента	Подключение к оператору
PE	Граница сети оператора	Разделение VPN и маршрутизация клиентов
P	Внутренняя сеть оператора	Передача пакетов по меткам

Таким образом, CE отвечает за подключение клиента, PE за организацию виртуальных сетей, а P за передачу данных внутри сети оператора.

5. Разграничение маршрутной информации

В MPLS VPN необходимо исключить смешивание маршрутной информации разных клиентов.

Для этого применяется механизм VRF (Virtual Routing and Forwarding).

VRF — это технология, которая позволяет создать несколько независимых таблиц маршрутизации на одном физическом маршрутизаторе.

Каждая VRF содержит маршруты определённой VPN.

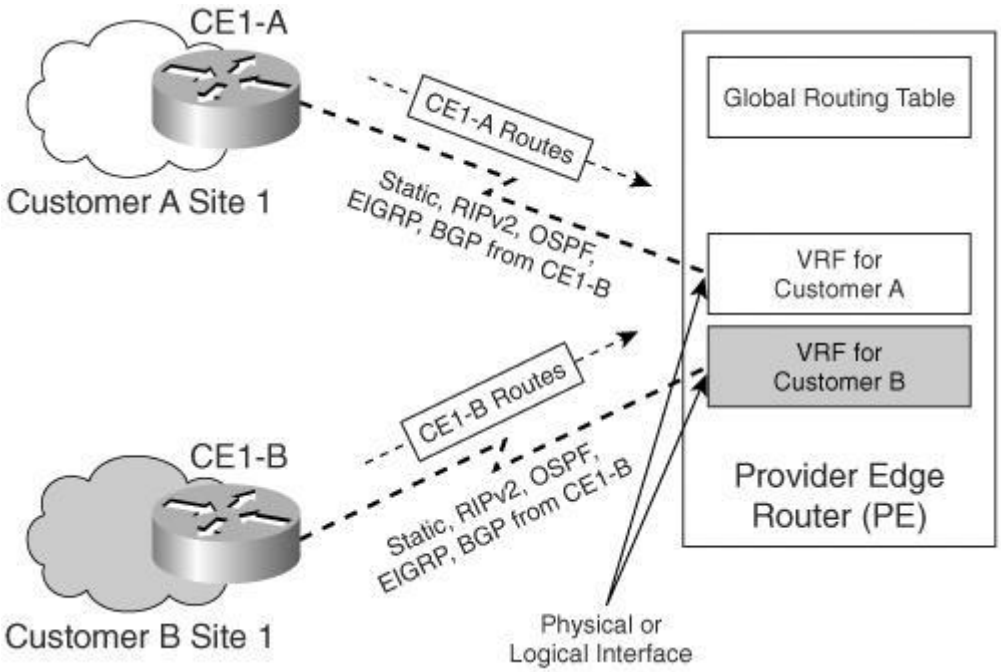
Например, оператор обслуживает две организации.

Параметр	Компания A	Компания B
Название VRF	VRF_A	VRF_B
Локальная сеть	192.168.1.0/24	192.168.1.0/24
Маршрутизатор PE	PE1	PE1
Таблица маршрутизации	Отдельная	Отдельная

Обратите внимание: обе компании используют одинаковую IP-подсеть 192.168.1.0/24.

В обычной общей таблице маршрутизации возник бы конфликт адресов. Но в MPLS VPN каждая сеть находится в своей VRF.

Поэтому одинаковые IP-адреса могут использоваться независимо.



5.1. Route Distinguisher (RD)

Для дополнительного разграничения одинаковых IP-маршрутов используется Route Distinguisher (RD).

RD представляет собой специальное значение, которое добавляется к IPv4-префиксу.

В результате создаётся уникальный VPNv4-маршрут.

Например:

- Компания A: RD 65000:10;
- Компания B: RD 65000:20.

Если обе компании используют сеть 192.168.1.0/24, то получаются разные VPNv4-маршруты:

- 65000:10:192.168.1.0/24;
- 65000:20:192.168.1.0/24.

Таким образом, одинаковые IP-префиксы становятся различимыми внутри MPLS VPN.

5.2. Route Target (RT)

Route Target — это специальный атрибут, который определяет правила импорта и экспорта маршрутов между VRF.

RT используется для определения того, какие маршруты должны быть доступны конкретной VPN.

Различают:

- Export RT: значение, которое присваивается маршрутам при их передаче из VRF в MP-BGP.
- Import RT: значение, по которому VRF принимает маршруты из MP-BGP.

Пример:

Для компании A используется RT 65000:100.

Для компании B используется RT 65000:200.

Если VRF_A импортирует только RT 65000:100, то маршруты компании B не попадут в её таблицу маршрутизации.

5.3. Различие между RD и RT

Характеристика	RD	RT
Полное название	Route Distinguisher	Route Target
Назначение	Различение одинаковых IP-префиксов	Управление импортом и экспортом маршрутов
Основная функция	Обеспечение уникальности VPNv4-маршрута	Определение принадлежности маршрута к VPN
Влияние на связность	Сам по себе не определяет	Определяет

Важно запомнить: RD делает маршрут уникальным, а RT определяет, в какие VPN этот маршрут может быть импортирован.

6. Использование протокола MP-BGP для связывания сайтов

BGP (Border Gateway Protocol) — это протокол динамической маршрутизации, который применяется для обмена маршрутной информацией между автономными системами и сетями.

В MPLS VPN используется его расширение MP-BGP (Multiprotocol BGP).

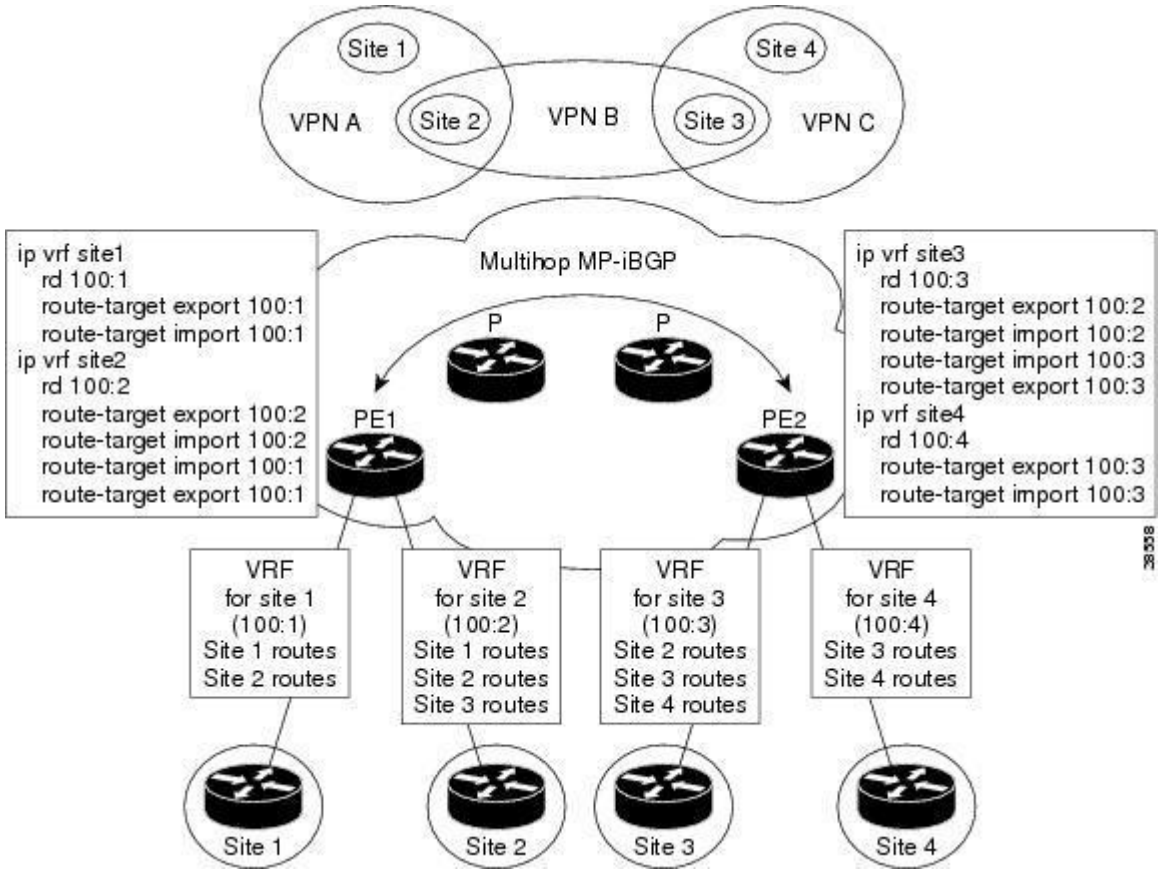
MP-BGP позволяет передавать информацию о маршрутах разных VPN между пограничными маршрутизаторами PE.

Обычный BGP предназначен прежде всего для обмена IPv4-маршрутами. MP-BGP поддерживает дополнительные семейства адресов, в том числе VPNv4.

6.1. Назначение MP-BGP

Основные задачи MP-BGP:

1. Передача маршрутов между маршрутизаторами PE.
2. Обмен информацией о VPNv4-префиксах.
3. Передача атрибутов RD и RT.
4. Связывание удалённых площадок одной VPN.
5. Поддержка нескольких независимых VPN.



6.2. Пример работы MP-BGP

Предположим, что организация имеет два филиала.

- Филиал 1 подключён к маршрутизатору PE1.
- Филиал 2 подключён к маршрутизатору PE2.

Локальная сеть первого филиала: 192.168.10.0/24.

Локальная сеть второго филиала: 192.168.20.0/24.

Маршрутизатор PE1 получает маршрут 192.168.10.0/24 от CE1.

Затем PE1 передаёт этот маршрут через MP-BGP маршрутизатору PE2.

PE2 проверяет атрибуты маршрута и импортирует его в соответствующую VRF.

После этого второй филиал получает возможность передавать данные в первый филиал.

Таким образом, MP-BGP обеспечивает обмен маршрутной информацией между удалёнными площадками одной VPN.

7. Независимость адресных пространств

Одним из преимуществ MPLS VPN является возможность использования одинаковых IP-адресов разными клиентами.

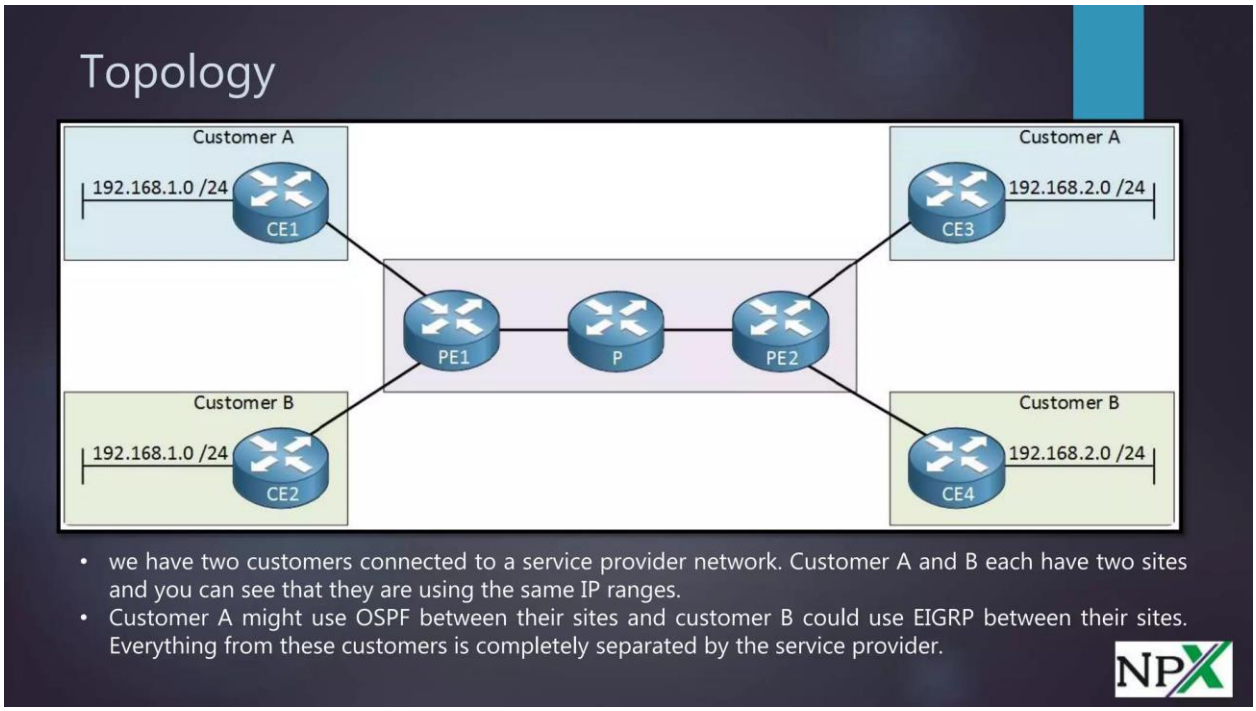
Это свойство называется независимостью адресных пространств.

В обычной IP-сети два устройства в одной таблице маршрутизации не могут без специальных механизмов использовать одинаковые адреса для разных сетей назначения.

В MPLS VPN эта проблема решается с помощью VRF и RD.

7.1. Пример независимых адресных пространств

Предположим, что оператор обслуживает две компании.



Компания A:

- локальная сеть: 192.168.1.0/24;
- шлюз: 192.168.1.1;
- VRF: VRF_A.

Компания B:

- локальная сеть: 192.168.1.0/24;

- шлюз: 192.168.1.1;
- VRF: VRF_B.

Несмотря на совпадение адресов, сети работают независимо.

Причина заключается в том, что маршруты находятся в разных VRF.

7.2. Преимущества независимости адресных пространств

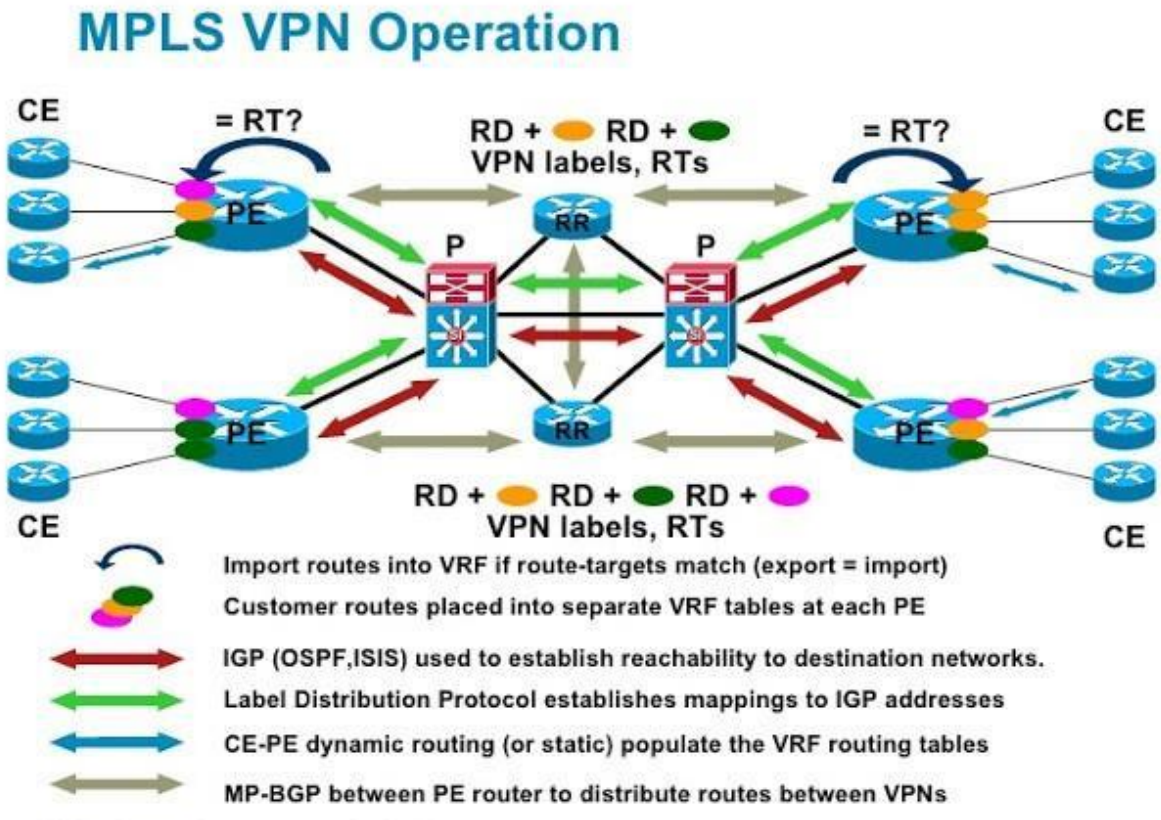
1. Нет необходимости изменять IP-адреса при подключении клиента к оператору.
2. Несколько организаций могут использовать одинаковые адресные диапазоны.
3. Упрощается подключение новых филиалов.
4. Снижается вероятность конфликтов между адресами разных клиентов.
5. Каждая VPN сохраняет собственную структуру адресации.

Следовательно, MPLS VPN позволяет оператору обслуживать большое количество организаций с одинаковыми внутренними IP-адресами.

8. Генерация маршрутных объявлений MP-BGP

Для передачи маршрутов между пограничными маршрутизаторами PE применяется механизм формирования VPNv4-маршрутных объявлений.

Рассмотрим последовательность формирования маршрута.



Этап 1. Получение маршрута от CE

Маршрутизатор CE передаёт информацию о локальной сети на PE.

Например:

192.168.10.0/24.

Этап 2. Помещение маршрута в VRF

Маршрутизатор PE определяет, к какой VPN относится полученный маршрут.

Затем маршрут помещается в соответствующую таблицу VRF.

Этап 3. Добавление RD

К IP-префиксу добавляется Route Distinguisher.

Например:

RD: 65000:10.

IP-префикс: 192.168.10.0/24.

В результате формируется VPNv4-маршрут.

Этап 4. Назначение RT

К маршруту добавляется Route Target.

Например:

RT: 65000:100.

Этот атрибут определяет, какие удалённые VRF могут принять данный маршрут.

Этап 5. Передача через MP-BGP

PE передаёт VPNv4-маршрут другим маршрутизаторам PE через MP-BGP.

Этап 6. Импорт маршрута

Удалённый PE проверяет RT.

Если значение RT соответствует правилам импорта его VRF, маршрут помещается в соответствующую таблицу маршрутизации.

Этап 7. Передача маршрута клиенту

Удалённый PE передаёт маршрут на CE.

В результате удалённый филиал получает информацию о сети первого филиала.

Итог: MP-BGP позволяет автоматически распространять маршруты между удалёнными площадками одной VPN.

9. Перемещение пакета по сети MPLS VPN

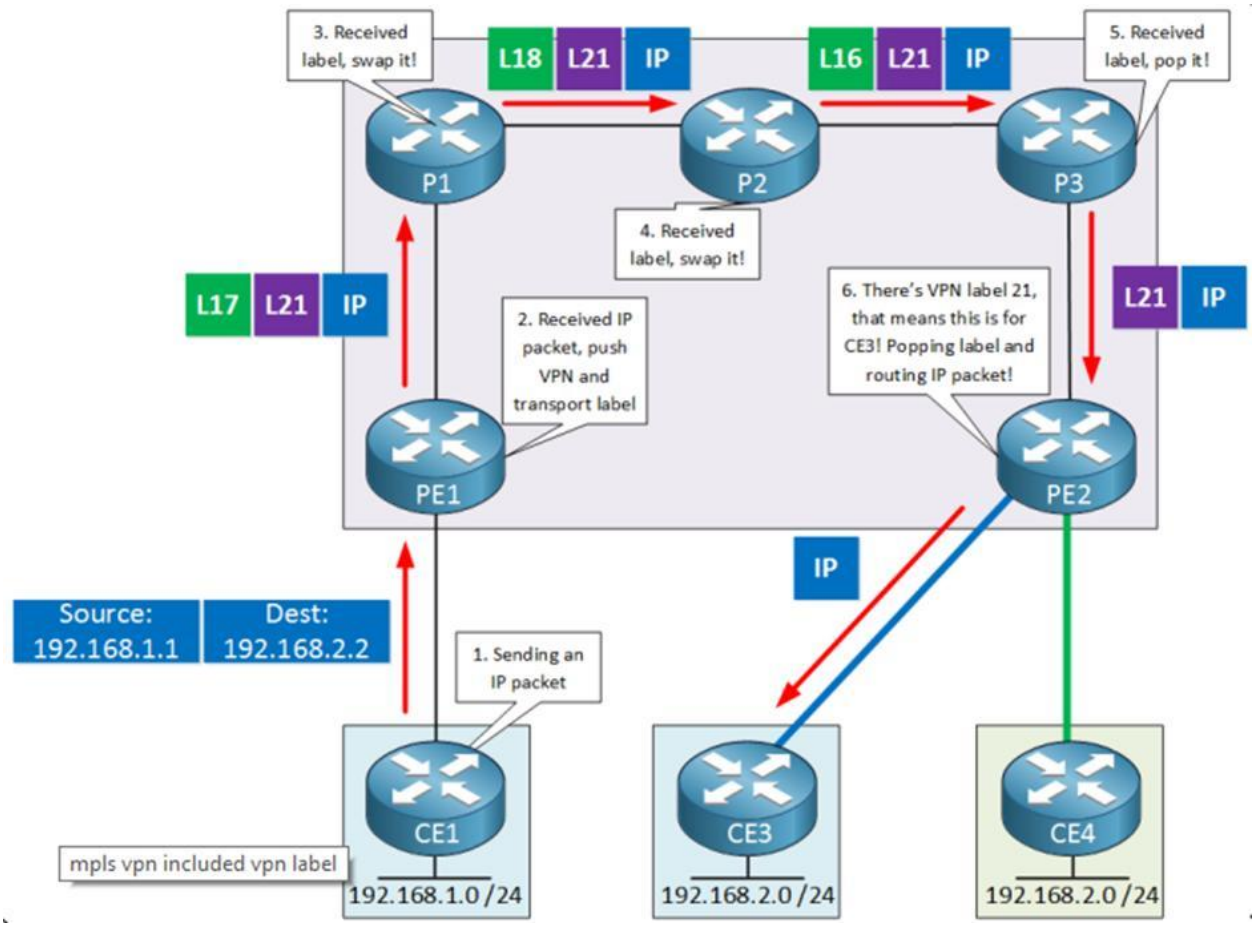
Рассмотрим, как передаётся IP-пакет между двумя филиалами одной организации через MPLS VPN.

Предположим, что имеются две локальные сети:

- Сеть филиала A: 192.168.10.0/24.
- Сеть филиала B: 192.168.20.0/24.

Филиал A подключён к CE1, а филиал B подключён к CE2.

Между ними расположены маршрутизаторы оператора PE1, P и PE2.



9.1. Последовательность передачи пакета

Этап 1. Передача пакета от компьютера.

Компьютер филиала A формирует IP-пакет для компьютера филиала B.

Пакет передаётся на локальный маршрутизатор CE1.

Этап 2. Передача пакета на PE1.

Маршрутизатор CE1 передаёт пакет на пограничный маршрутизатор PE1 оператора.

PE1 определяет, к какой VRF относится данный клиент.

Этап 3. Добавление MPLS-меток.

PE1 добавляет к пакету две метки:

- Внешняя метка (Transport Label) определяет путь до выходного маршрутизатора PE2.
- Внутренняя метка (VPN Label) определяет нужную VPN и соответствующий маршрут на PE2.

Этап 4. Передача через внутренние маршрутизаторы.

Маршрутизатор P получает пакет и анализирует внешнюю метку.

Он заменяет её на другую метку в соответствии с таблицей коммутации MPLS.

При этом внутренняя VPN Label сохраняется.

Этап 5. Приём пакета маршрутизатором PE2.

PE2 получает пакет и обрабатывает оставшуюся VPN-метку.

По этой метке определяется соответствующая VRF.

Этап 6. Передача на CE2.

PE2 удаляет MPLS-метки и передаёт обычный IP-пакет маршрутизатору CE2.

Этап 7. Получение данных.

CE2 передаёт пакет компьютеру назначения в локальной сети филиала B.

9.2. Две метки MPLS

В MPLS VPN часто используются две метки.

Тип метки	Назначение
Transport Label	Передача пакета до нужного PE
VPN Label	Определение VPN и дальнейшей обработки пакета на PE

Важно: внешняя метка отвечает за транспорт внутри сети оператора, а внутренняя метка связана с доставкой данных в нужную клиентскую VPN.

В некоторых конфигурациях внешняя метка может быть удалена до поступления пакета на последний PE. Такой механизм называется PHP (Penultimate Hop Popping).

10. Механизм формирования топологии VPN

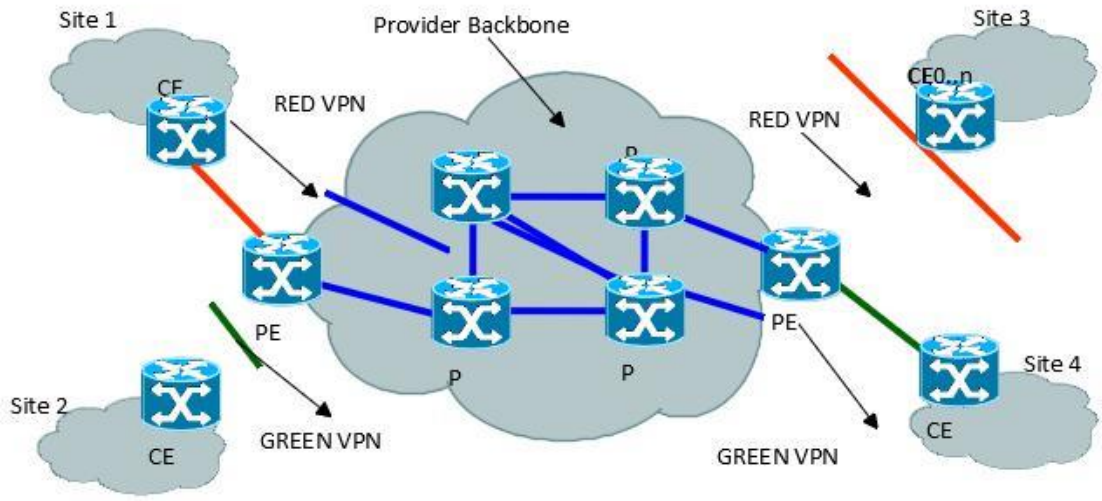
Топология VPN определяет, какие площадки могут обмениваться данными между собой.

В MPLS VPN оператор может создавать различные схемы взаимодействия между филиалами.

10.1. Топология Full Mesh

Full Mesh означает полную связность между всеми площадками одной VPN.

Каждый филиал может обмениваться данными с любым другим филиалом.



Например, организация имеет четыре филиала:

- Алматы;
- Астана;
- Караганда;
- Усть-Каменогорск.

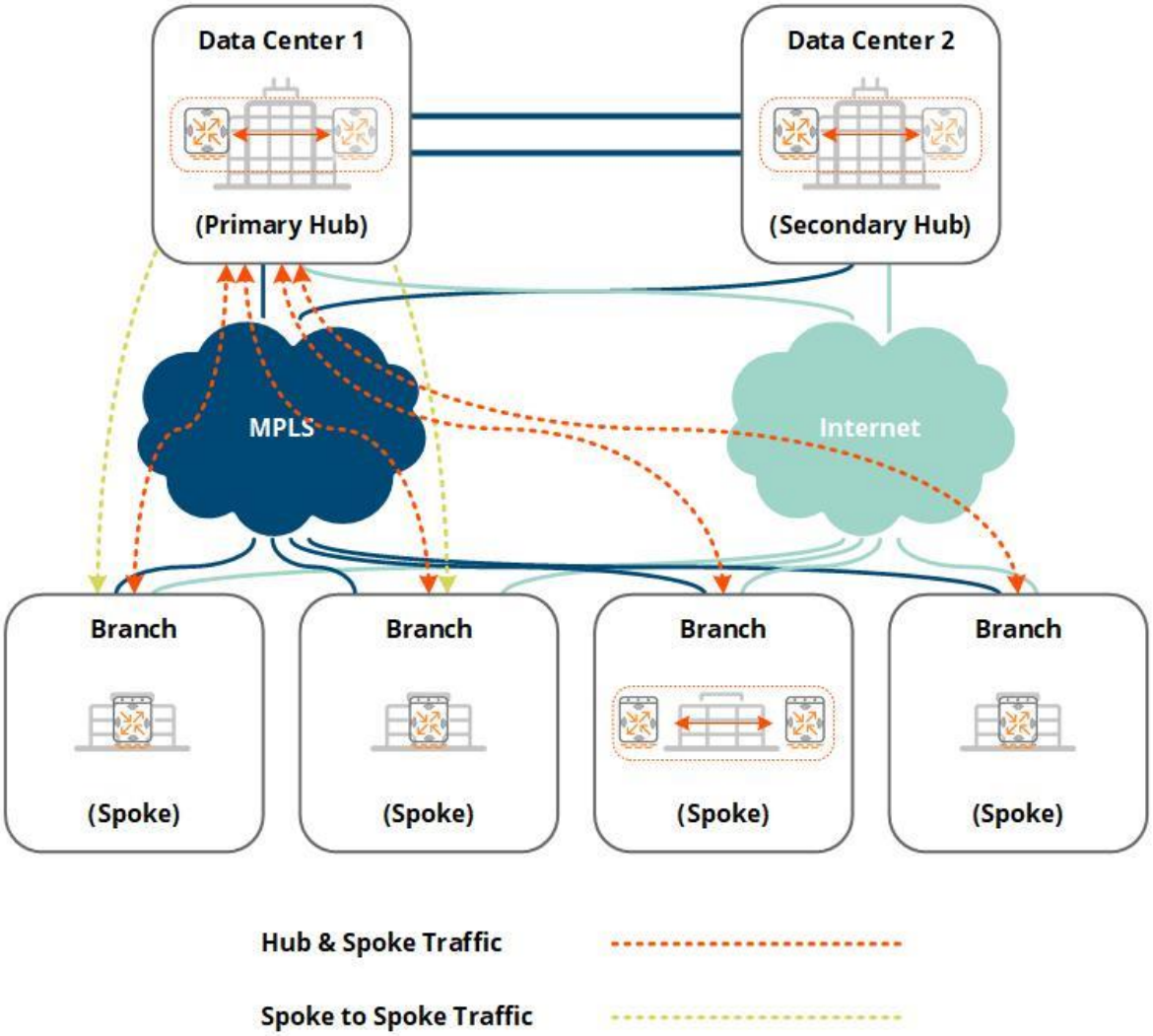
Все четыре филиала могут обмениваться данными между собой.

Преимущества:

- высокая связность;
- прямой логический обмен между любыми площадками;
- отсутствие обязательного центрального узла для передачи данных между филиалами.

10.2. Топология Hub-and-Spoke

Hub-and-Spoke предполагает наличие одного центрального узла (Hub) и нескольких удалённых филиалов (Spoke).



Например:

- центральный офис в Алматы является Hub;
- филиалы в Астане, Караганде и Усть-Каменогорске являются Spoke.

Обмен данными между удалёнными филиалами осуществляется через центральный офис.

Преимущества:

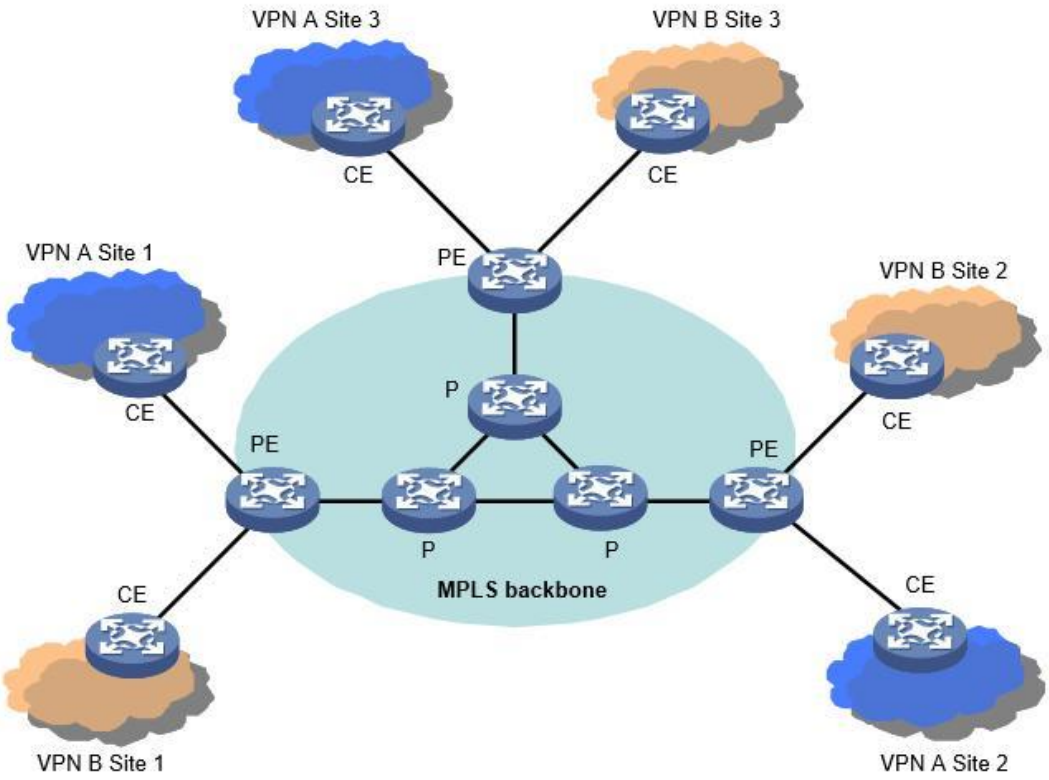
1. Централизованное управление.
2. Упрощение контроля доступа.
3. Возможность размещения общих серверов в центральном офисе.
4. Снижение сложности настройки взаимодействия между филиалами.

Недостаток: центральный узел становится важным элементом сети. При его отказе обмен между филиалами может быть нарушен.

10.3. Частичная связность (Partial Mesh)

Partial Mesh предполагает, что не все филиалы имеют возможность прямого логического взаимодействия друг с другом.

Например, центральный офис связан со всеми филиалами, но удалённые филиалы могут обмениваться данными только через него.



Такая топология позволяет выбрать необходимые связи между подразделениями.

Она подходит для организаций, в которых некоторым филиалам не требуется прямой доступ к ресурсам других филиалов.

10.4. Сравнение топологий VPN

Характеристика	Full Mesh	Hub-and-Spoke	Partial Mesh
Связь между филиалами	Все со всеми	Через центральный узел	Только между выбранными
Управление	Распределённое	Централизованное	Комбинированное
Сложность настройки	Выше	Ниже	Средняя
Основное применение	Крупные корпоративные сети	Организации с главным офисом	Сети с выборочными связями

10.5. Как формируется топология с помощью RT?

В MPLS VPN топология может быть сформирована с помощью правил импорта и экспорта Route Target.

Например, для организации используются следующие значения:

- Центральный офис: RT 65000:100.
- Филиалы: RT 65000:200.

В Hub-and-Spoke центральный офис может принимать маршруты всех филиалов, а филиалы могут принимать маршруты только центрального офиса.

Для этого настраиваются соответствующие правила Import RT и Export RT.

Таким образом, топология VPN определяется не только физическими соединениями, но и правилами распространения маршрутной информации.

11. Степень защищённости MPLS VPN

MPLS VPN обеспечивает логическое разделение трафика разных клиентов внутри инфраструктуры оператора связи.

Однако необходимо понимать, что логическая изоляция не равнозначна криптографическому шифрованию.

11.1. Основные механизмы защиты

1. Разделение таблиц маршрутизации.

Для каждой VPN создаётся отдельная VRF. Это предотвращает смешивание маршрутов разных клиентов.

2. Использование RD и RT.

RD позволяет различать одинаковые IP-префиксы, а RT определяет правила распространения маршрутов между VPN.

3. Изоляция трафика.

MPLS-метки позволяют направлять пакеты в соответствующую VPN.

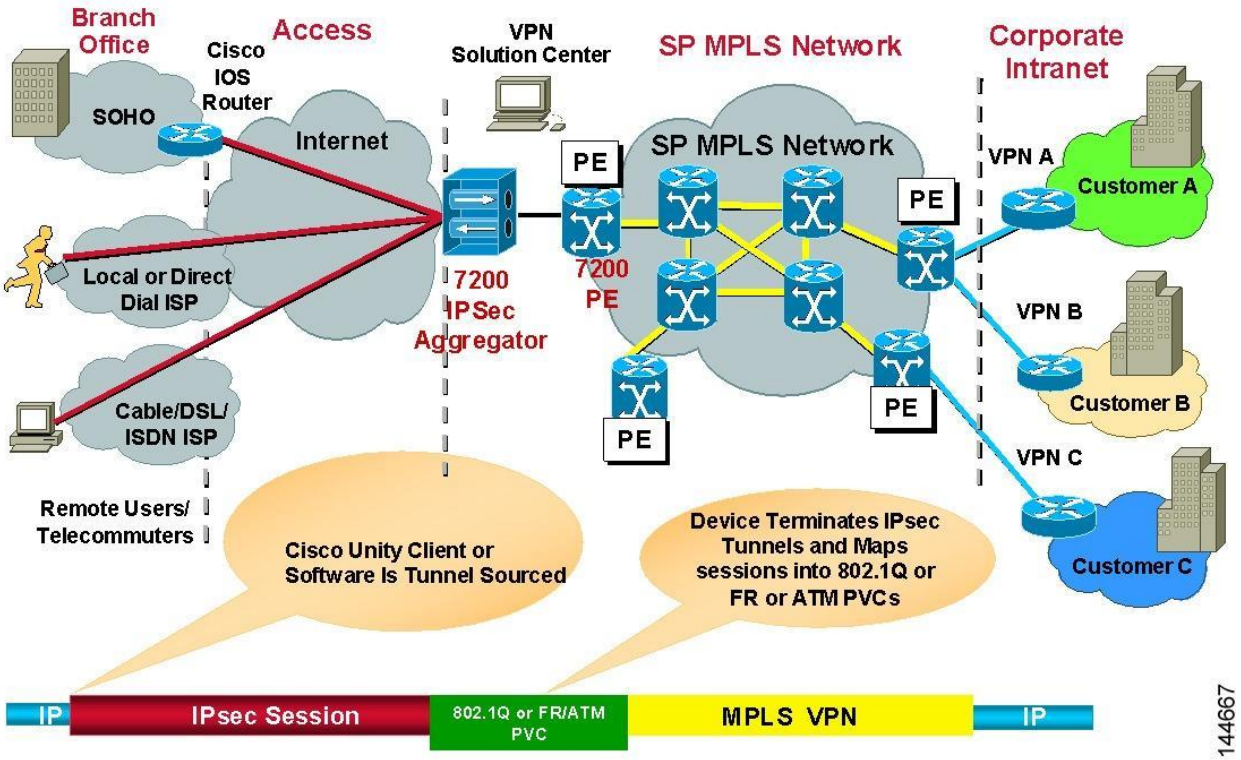
4. Контроль доступа.

Для ограничения доступа применяются ACL, межсетевые экраны и другие средства сетевой безопасности.

5. Шифрование данных.

При необходимости поверх MPLS VPN может использоваться IPsec.

IPsec обеспечивает криптографическую защиту передаваемых данных.



11.2. MPLS VPN и IPsec VPN

Характеристика	MPLS VPN	IPsec VPN
Основной принцип	Логическая изоляция трафика	Криптографическая защита
Работа с метками	Да	Нет
Шифрование	Само по себе не обеспечивает	Обеспечивает
Основное применение	Корпоративные сети оператора	Защищённая передача данных через IP-сети
Зависимость от оператора	Обычно высокая	Может работать через интернет

11.3. Насколько безопасна MPLS VPN?

MPLS VPN обеспечивает разделение клиентского трафика на уровне маршрутизации и передачи пакетов.

Но существуют определённые риски:

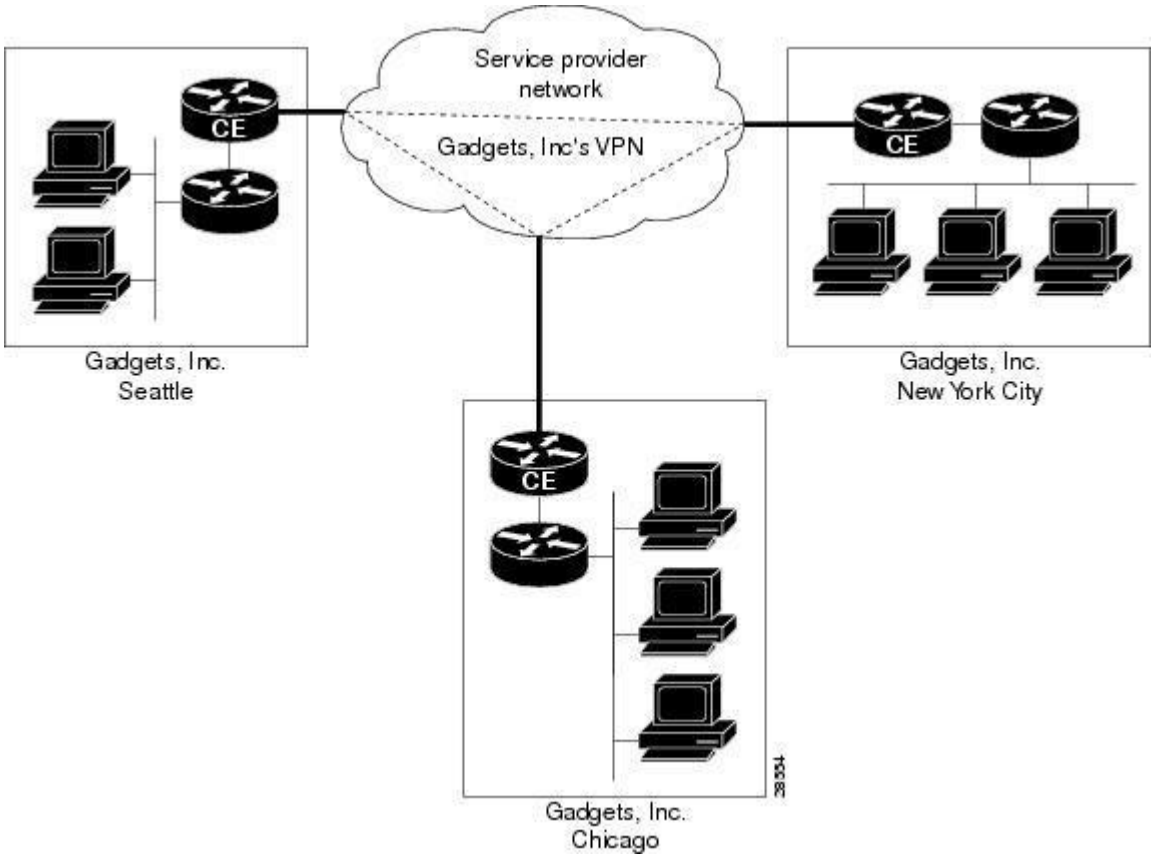
- ошибки в настройках маршрутизаторов;
- неправильное распределение Route Target;
- несанкционированный доступ к оборудованию оператора;
- атаки на сетевую инфраструктуру;
- перехват данных при отсутствии дополнительного шифрования на участках, где оно необходимо.

Поэтому для передачи конфиденциальной информации рекомендуется дополнительное шифрование с помощью IPsec.

Главный вывод: MPLS VPN обеспечивает логическую изоляцию корпоративных сетей, но не гарантирует шифрование данных. Для более высокого уровня защиты MPLS VPN может сочетаться с IPsec.

12. Практический пример организации MPLS VPN

Рассмотрим организацию, которая имеет три филиала в разных городах Казахстана.



Исходные данные:

Филиал	IP-подсеть	Маршрутизатор
Алматы	192.168.10.0/24	CE1
Астана	192.168.20.0/24	CE2
Усть-Каменогорск	192.168.30.0/24	CE3

Все филиалы подключены к сети одного оператора связи.

Необходимо обеспечить:

1. Обмен данными между тремя филиалами.
2. Изоляцию корпоративной сети от других клиентов оператора.
3. Независимость адресных пространств.
4. Автоматическое распространение маршрутов.
5. Возможность централизованного управления сетью.

Решение:

1. На маршрутизаторах PE создаются отдельные VRF.

2. Для маршрутов назначаются RD и RT.
3. Между маршрутизаторами PE настраивается MP-BGP.
4. Между PE и P организуется передача MPLS-пакетов.
5. Маршруты филиалов распространяются через MP-BGP.
6. Для каждого филиала настраивается соответствующая таблица маршрутизации.
7. При необходимости применяется IPsec для шифрования данных.

В результате все три филиала получают возможность обмениваться данными через общую инфраструктуру оператора.

13. Заключение

В ходе лекции мы рассмотрели принципы организации виртуальных частных сетей на основе технологии MPLS.

Мы установили, что MPLS использует специальные метки для передачи пакетов через сеть оператора связи.

Были рассмотрены два основных варианта MPLS VPN: L2VPN и L3VPN.

Мы изучили назначение компонентов CE, PE и P, а также механизм разделения маршрутной информации с помощью VRF.

Особое внимание было уделено протоколу MP-BGP, который обеспечивает обмен маршрутами между удалёнными площадками одной VPN.

Также мы рассмотрели роль RD и RT. RD обеспечивает уникальность VPNv4-маршрутов, а RT определяет правила их распространения между виртуальными сетями.

Были изучены способы организации полной и частичной связности между филиалами.

Таким образом, MPLS VPN позволяет объединять удалённые офисы в единую корпоративную сеть, сохранять логическую изоляцию клиентов и эффективно использовать инфраструктуру оператора связи.

14. Контрольные вопросы

1. Что такое VPN и для чего она используется?
2. Что означает аббревиатура MPLS?
3. В чём заключается принцип коммутации с помощью меток?
4. Какие функции выполняют маршрутизаторы LER и LSR?
5. Чем отличаются L2VPN и L3VPN?
6. Что означает полная связность при логической изолированности?
7. Какие основные компоненты входят в архитектуру MPLS VPN?
8. Для чего используется маршрутизатор CE?
9. Какие функции выполняет маршрутизатор PE?
10. Какую роль выполняет маршрутизатор P?
11. Что такое VRF?
12. Для чего используются RD и RT?
13. Чем отличается RD от RT?
14. Какую функцию выполняет протокол MP-BGP?

15. Как обеспечивается независимость адресных пространств?
16. Как формируются маршрутные объявления MP-BGP?
17. Какие две метки используются при передаче пакетов MPLS VPN?
18. Чем отличаются топологии Full Mesh и Hub-and-Spoke?
19. Как формируется топология VPN с помощью RT?
20. Обеспечивает ли MPLS VPN шифрование передаваемых данных?
21. Для чего применяется IPsec совместно с MPLS VPN?

15. Практические задания для студентов

Задание 1. Анализ архитектуры MPLS VPN

Рассмотрите схему сети, которая состоит из двух офисов и инфраструктуры оператора связи.

Необходимо:

1. Определить устройства CE, PE и P.
2. Объяснить назначение каждого маршрутизатора.
3. Показать направление передачи IP-пакета.
4. Определить место добавления и удаления MPLS-меток.

Задание 2. Анализ независимости адресных пространств

Две организации используют одинаковую IP-подсеть 192.168.1.0/24.

Необходимо:

1. Объяснить, почему возникает конфликт адресов в общей таблице маршрутизации.
2. Объяснить назначение VRF.
3. Привести пример двух разных значений RD.
4. Определить назначение RT.
5. Объяснить, почему данные организаций не смешиваются.

Задание 3. Выбор топологии VPN

Организация имеет пять филиалов и один центральный офис.

Необходимо:

1. Рассмотреть топологию Full Mesh.
2. Рассмотреть топологию Hub-and-Spoke.
3. Рассмотреть топологию Partial Mesh.
4. Сравнить преимущества и недостатки.
5. Выбрать наиболее подходящую топологию и обосновать решение.

Задание 4. Анализ безопасности

Организация передаёт конфиденциальные данные через MPLS VPN.

Необходимо:

1. Объяснить, как обеспечивается логическая изоляция.
2. Определить возможные угрозы.
3. Объяснить различие между MPLS VPN и IPsec VPN.
4. Предложить способ дополнительной защиты информации.

16. Основные термины лекции

Термин	Значение
VPN	Виртуальная частная сеть
MPLS	Многопротокольная коммутация по меткам
L3VPN	VPN на сетевом уровне
L2VPN	VPN на канальном уровне
CE	Маршрутизатор клиента
PE	Пограничный маршрутизатор оператора
P	Внутренний маршрутизатор оператора
VRF	Отдельная таблица маршрутизации
RD	Идентификатор для различения VPN-маршрутов
RT	Атрибут управления распространением маршрутов
MP-BGP	Многопротокольное расширение BGP
Label	Метка MPLS
Full Mesh	Полная связность
Hub-and-Spoke	Централизованная топология
IPsec	Протокол криптографической защиты IP-трафика
QoS	Качество обслуживания сети