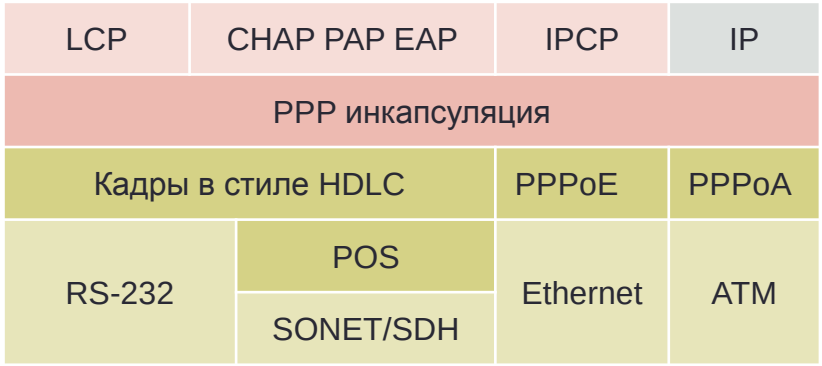
PPP

Point-to-Point Protocol (PPP)

- Двухточечный протокол канального уровня, использующийся для установления прямой связи между двумя сетевыми узлами
- Может обеспечивать
  - Аутентификацию
  - Автоконфигурацию
  - Шифрование передаваемых данных
  - Сжатие
- Используется для работы через различные соединения физического уровня
  - Последовательные порты
  - Телефонные линии, включая сотовые
  - Радиолинии
  - Оптоволоконные линии
- Используются для инкапсуляции при передаче данных через другие протоколы канального уровня
  - Через Ethernet: PPPoE
  - Через ATM: PPPoA

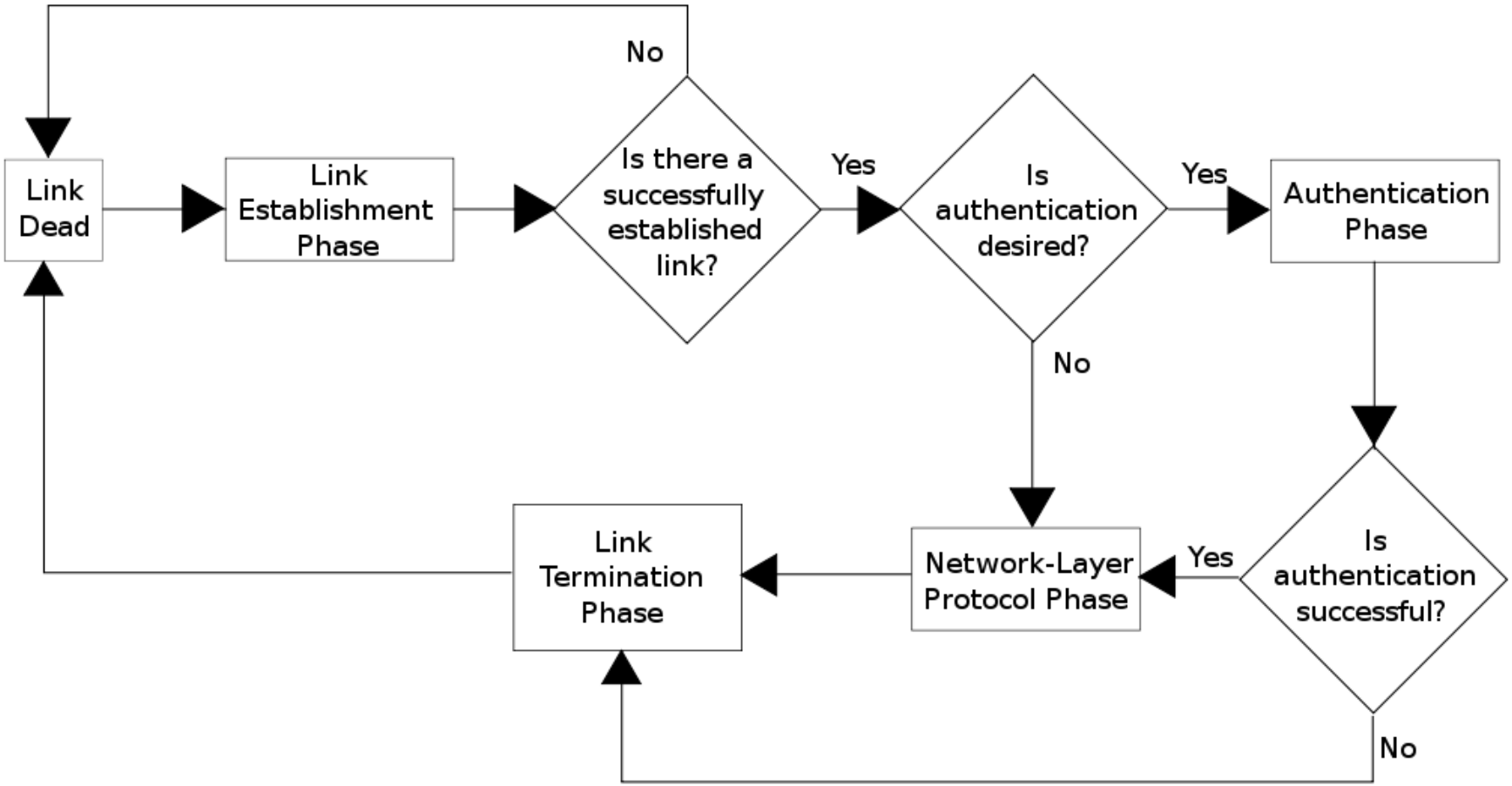
Архитектура протокола PPP (RFC 1661)

- Link Control Protocol (LCP)
  - Отвечает за установку и завершение соединения
  - Позволяет согласовать настройки интерфейсов, использование аутентификации, компрессии и шифрование
- Протоколы аутентификации
  - Password Authentication Protocol (PAP) – RFC 1334 – устарел
  - Challenge-Handshake Authentication Protocol (CHAP) – RFC 1994
  - Extensible Authentication Protocol (EAP) – RFC 2284
- Network Control Protocol (NCP)
  - Используется для согласования опций инкапсулированных поверх PPP протоколов
  - Для IPv4 используется Internet Protocol Control Protocol (IPCP) – RFC 1332
  - Для IPv6 используется IPv6 Control Protocol (IPCP) – RFC 1332



- Инкапсуляция пакетов PPP
  - Через последовательные соединения передаётся в кадрах построенных на подобие кадров HDLC – RFC 1662
  - Point-to-Point Protocol over Ethernet (PPPoE) – RFC 2516
  - Point-to-Point Protocol over ATM (PPPoA) – RFC 2364
- PPP с использованием нескольких линий
  - PPP Multilink Protocol (MLPPP, MP, MPPP, MLP) – RFC 1990

Фазы PPP протокола



PPP через последовательные каналы

	Кадр PPP						
Поле	Flag	Address	Control	Protocol	Information	Padding	FCS
Размер	1	1	1	1 или 2	переменный	переменный	2 или 4

- Flag – 0x07
- Address – 0xFF – все станции
- Control – 0x03 – ненумерованная информация
- FCS – Frame Check Sequence – контрольная сумма CRC32
- Protocol – тип передаваемого протокола
  - от 0x0XXX до 0x3XXX идентифицируют протоколы сетевого уровня. Протоколу IP соответствует флаг 0x0021.
  - от 0x4XXX до 0x7XXX идентифицируют протоколы с низким уровнем трафика.
  - от 0x8XXX до 0xBXXX идентифицируют протокол управления сетью (NCP). Протоколу IPCP соответствует флаг 0x8021.
  - от 0xCXXX до 0xEXXX идентифицируют управляющие протоколы. Протоколу LCP соответствует флаг 0xC021.
- Information – данные передаваемого протокола

Link Control Protocol

- Задачи протокола LCP
  - Идентифицировать устройство и принять или отклонить соединение
  - Определить допустимые размеры кадров
  - Убедиться в отсутствии ошибок в настройке
  - Может завершить связь если требования превосходят возможности
- Передача данных через PPP соединение не может осуществляться до завершения фазы LCP
- Используется три вида LCP пакетов
  - Пакеты конфигурации
  - Пакеты завершения связи
  - Пакеты поддержания соединения
- После завершения LCP может быть согласовано сжатие пакетов с использованием протокола Compression Control Protocol (CCP) – RFC 1962

LCP – пакеты конфигурации

- Configure-Request
  Содержит список опций, предлагаемых к согласованию
- Configure-Ack
  Содержит список подтверждённых опций
- Configure-Nack
  Содержит список распознанных, но отвергнутых опций
- Configure-Reject
  Содержит список нераспознанных опций

- Опции включают
  - Maximum Receive Unit (MRU) – максимальный размер принимаемого кадра
  - Authentication-Protocol – протокол аутентификации
  - Quality-Protocol – протокол мониторинга качества линии
  - Magic-Number – используется для обнаружения петель
  - Protocol-Field-Compression (PFC) – сжатие поля протокол заголовка PPP
  - Address-and-Control-Field-Compression (ACFC) – сжатие полей заголовка PPP

LCP – пакеты завершения соединения

- Terminate-Request

  Передаётся стороной, завершающей соединение до получения подтверждения

- Terminate-Ack

  Подтверждает завершение связи

LCP – пакеты поддержания соединения

- Code-Reject

  Посылается в ответ на LCP пакет неизвестного типа

- Protocol-Reject

  Посылается в ответ на PPP пакет с неизвестным протоколом

- Echo-Request и Echo-Reply

  Используются для тестирования соединения

- Discard-Request

  Предназначен для «прочистки» канала от отправителя. Такие пакеты должны игнорироваться получателем

Challenge-Handshake Authentication Protocol (CHAP)

- Используется для подтверждения личности пользователя в службе аутентификации
- Требует, чтобы пользователь и служба аутентификации знали одинаковую секретную информацию (пароль) в открытом виде
- Секретная информация не пересылается по сети
- Обеспечивает защиту от атаки использующей воспроизведение подслушанной предыдущей сессии
- Существует протокол MS-CHAP, не требующий хранения пароля в открытом виде, однако использованный в нём алгоритм скомпрометирован и может быть дешифрован.

Алгоритм работы CHAP

1. Служба аутентифкации посылает пользователю запрос (Challenge), включающий
   - Последовательный номер попытки аутентификации
   - Случайное число
   - Имя службы
2. Пользователь вычисляет хеш-функцию (контрольную сумму MD5) от информации, включающей полученные идентификатор, случайное число и секрет
3. Пользователь отправляет полученное значение хеш-функции и своё имя в пакете Response
4. Служба аутентификации повторяет вычисление хеш-функции и сверяет значения. В случае совпадения пользователю высылается пакет Success, в случае ошибки – Failure.

- В случае необходимости аутентификации обеих систем использование CHAP согласуется в обе стороны на этапе LCP.

Internet Protocol Control Protocol (IPCP)

- Используется для согласования параметров протокола IP
- Построен на таких же принципах как LCP
- Передача IP пакетов не может осуществляться до завершения процедуры согласования IPCP
- Типы пакетов IPCP:
  - Configure-Request
  - Configure-Ack
  - Configure-Nack
  - Configure-Reject
  - Terminate-Request
  - Terminate-Ack
  - Code-Reject

Опции IPCP

- IP-Address

  Передаёт локальный IP адрес. Значение 0.0.0.0 означает запрос передачи адреса через пакет Config-Nack.
- Mobile-IPv4

  Позволяет перемещать сетевой узел между разными сетями с сохранением сетевого адреса.
- Primary DNS Server Address

  Сообщает локальную настройку DNS сервера. Значение 0.0.0.0 означает запрос адреса DNS сервера в пакете Config-Nack.
- Primary NBNS Server Address

  Сообщает локальную настройку сервера имён NetBIOS. Значение 0.0.0.0 означает запрос адреса NBNS сервера в пакете Config-Nack.
- Secondary DNS Server Address
- Secondary NBNS Server Address
- IP-Compression-Protocol

  Метод сжатия заголовков TCP/IP Ван Якобсона позволяет уменьшить заголовок до 3 байт

Point-to-point protocol over Ethernet (PPPoE) RFC 2516

- Туннелирующий протокол, который позволяет инкапсулировать IP, или другие протоколы, через соединения Ethernet.
- PPPoE устанавливает соединение точка-точка, которое используется для транспортировки пакетов сетевого уровня через сеть Ethernet
- Используется для предоставления доступа к интернет через локальные сети или DSL
- Работа протокола подразумевает две фазы
  - PPPoE Discovery (PPPoED) – фаза поиска
  - PPP session – сессия передачи данных PPP

PPPoE Discovery

1. PPPoE Active Discovery Initiation (PADI)
   - Отправляется клиентом, желающим обнаружить MAC-адрес сервер провайдера / point of presence (POP)
   - Отправляется на широковещательный адрес
   - Может быть получено несколькими POP
2. PPPoE Active Discovery Offer (PADO)
   - Ответ POP отправляемый клиенту в ответ на PADI
   - Содержит имя POP и имя сервиса
   - Клиент может выбрать одно из предложений
3. PPPoE Active Discovery Request (PADR)
   - Посылается клиентом на выбранный POP
4. PPPoE Active Discovery Session-confirmation (PADS)
   - Посылается POP клиенту, подтверждая открытие сессии
5. PPPoE Active Discovery Termination (PADT)
   - Посылается любой из сторон при закрытии сессии

VPN

Виртуальные частные сети

Частные сети

- Главной особенностью частной сети является изолированность
  - Независимый выбор сетевых технологий
  - Независимая система адресации
  - Предсказуемая производительность
  - Максимально возможная безопасность
- Частные сети были популярны, пока общественные сети не получили большого развития.
- Виртуальные частные сети обеспечивают сервисы, приближенные к сервисам частных сетей, на основе сетевой инфраструктуры, разделяемой несколькими потребителями.

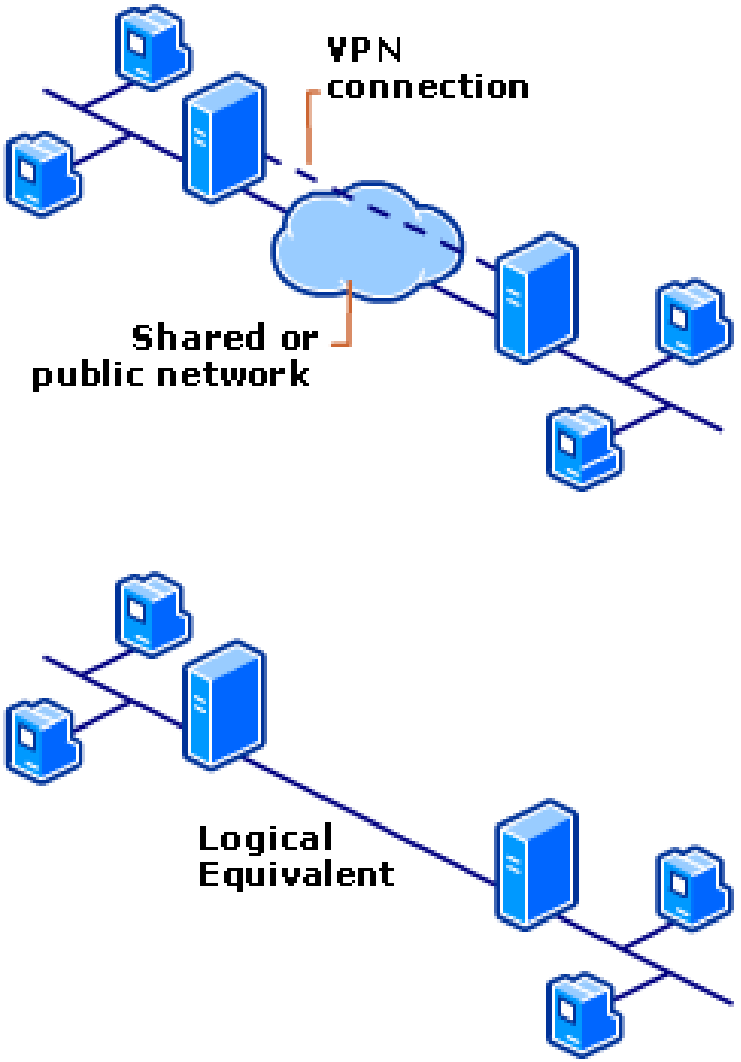
Виртуальные частные сети (VPN)

Виртуальная частная сеть (VPN) – соединение точка-точка через публичную (Internet) или частную сеть.

Для организации VPN используют специальные протоколы, называемые протоколами тунелирования.

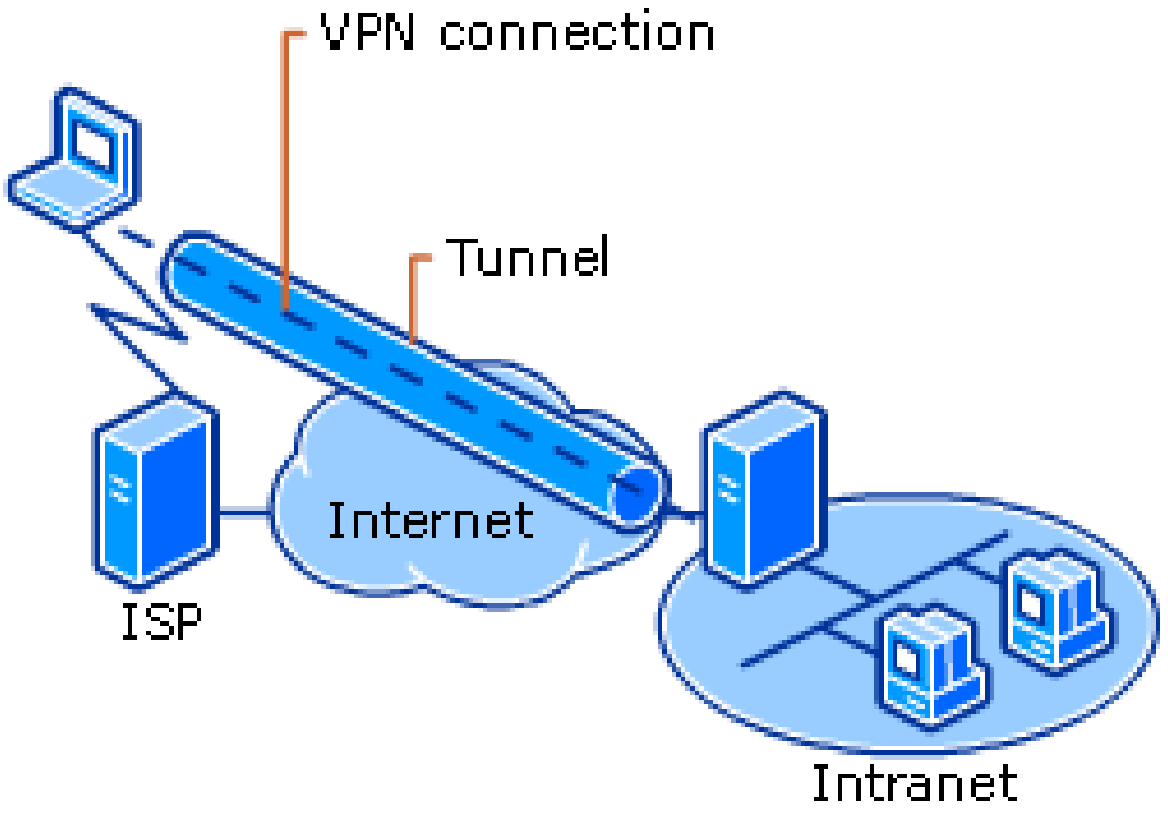
- для передачи данных используются протоколы стека TCP/IP;
- нагрузкой являются IP пакеты частных сетей;
- обеспечиваются:
  - аутентификация;
  - шифрование.

Протоколы туннелирования являются протоколами канального уровня.



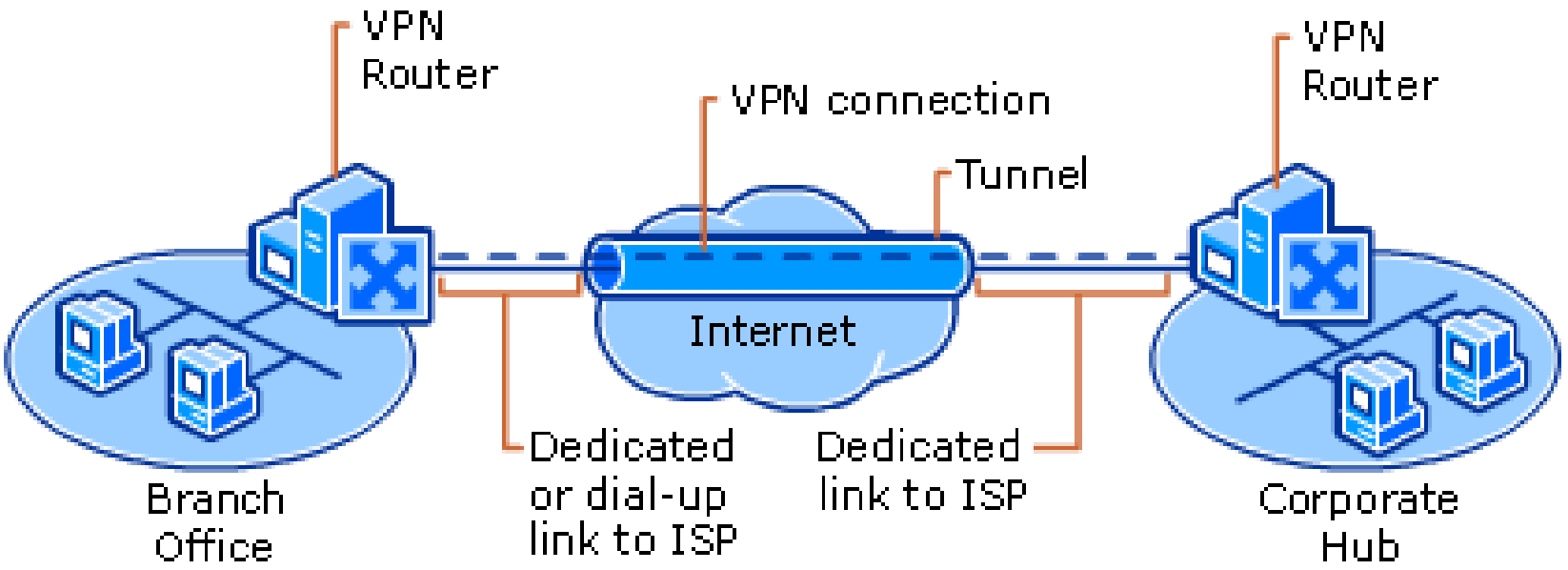
Использование VPN соединений

- Соединение клиента с частной сетью



Использование VPN соединений

- Соединение двух фрагментов частной сети



Протоколы VPN

- Point-to-Point Tunneling Protocol (PPTP)
  - Для управления туннелями используется TCP соединения.
  - Передача туннелированных данных:
    [IP [GRE [PPP [зашифрованный IP виртуальной сети]]]]
  - Для туннелированных данных поддерживаются сжатие и/или шифрование.
  - Для аутентификации используются средства PPP.

- Layer Two Tunneling Protocol (L2TP) – RFC 2661
  - Объединение PPTP и Layer 2 Forwarding (L2F) от Cisco.
  - Использует UDP для управления туннелями и передачи данных.
  - Поддерживается сжатие и шифрование средствами IPSec.
    [IP [IPSec [UDP [L2TP [PPP [IP виртуальной сети]]] IPSec]]

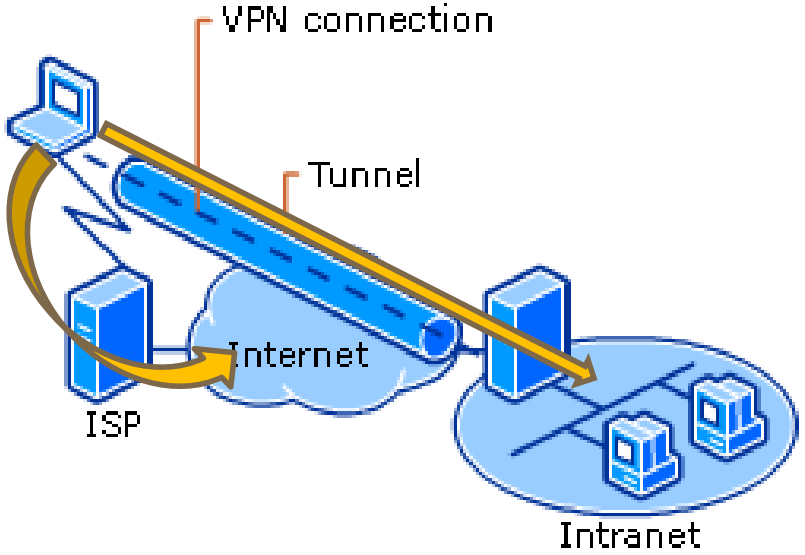
Протоколы VPN

- OpenVPN – протокол VPN с открытой реализацией
  - Для передачи данных может использовать UDP или TCP
    - Если используется TCP необходимо иметь запас по скорости передачи трафика через базовую сеть.
  - Может создавать два вида туннелей:
    - TUN – туннель сетевого уровня (передаёт IP);
    - TAP – туннель канального уровня (передаёт Ethernet).
  - Может работать через прокси-сервера.
  - Может работать из сетей, закрытых NAT/firewall.
  - Для шифрования используется OpenSSL.
  - Для аутентификации могут быть использованы предустановленный ключ, логин/пароль, сертификаты.
  - Может использовать сжатие данных алгоритмом LZO.

VPN и маршрутизация

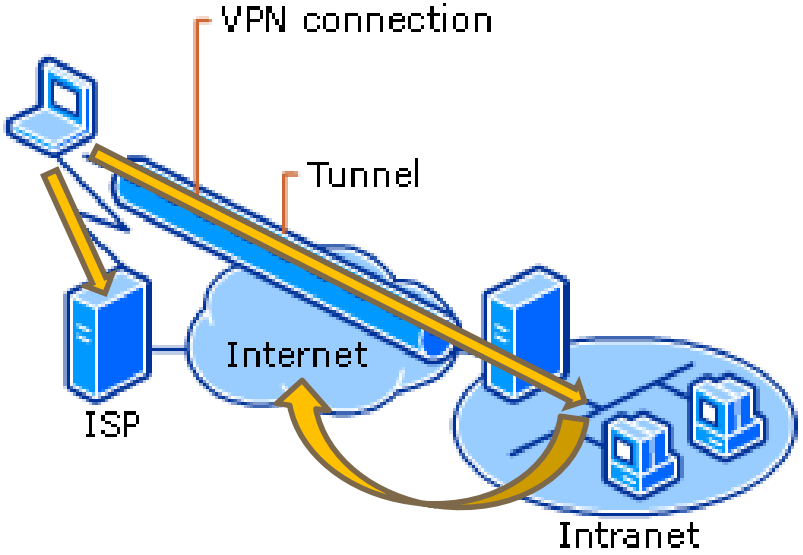
Маршрут по умолчанию – через локальный интерфейс

- Связь «с интернетом» идёт через локального провайдера.
- Если частная сеть имеет сложную структуру, может потребоваться дополнительная настройка маршрутов (split tunneling).



Маршрут по умолчанию – через VPN интерфейс

- Все данные передаются через туннель.
- Напрямую осуществляется связь только с сетью локального провайдера.
- Необходимо иметь роутинг до начала туннеля через провайдера.



Сети VPN на основе разграничения трафика

- Используются технологии виртуальных каналов, обеспечивающая защиту и разграничение трафика клиентов
  - ATM VPN
  - Frame Relay VPN
  - MPLS VPN
- В сетях L2VPN (ATM, FrameRelay, MPLS) при передаче данных используются два уровня стека протоколов, информация третьего уровня не анализируется и не меняется при передаче.
  - Можно передавать любые протоколы третьего уровня.
  - Обеспечивается полная изолированность адресов поставщика и клиентов.
  - Поставщик не может предоставлять услуги, связанные с сервисами IP.
  - Связь между сайтами клиента может быть организована по схеме звезда или полной связанности.
- При использовании MPLS можно строить сети L3VPN
  - Взаимодействие поставщика и клиентов осуществляется на уровне IP
  - Объем работ пропорционален числу клиентов.

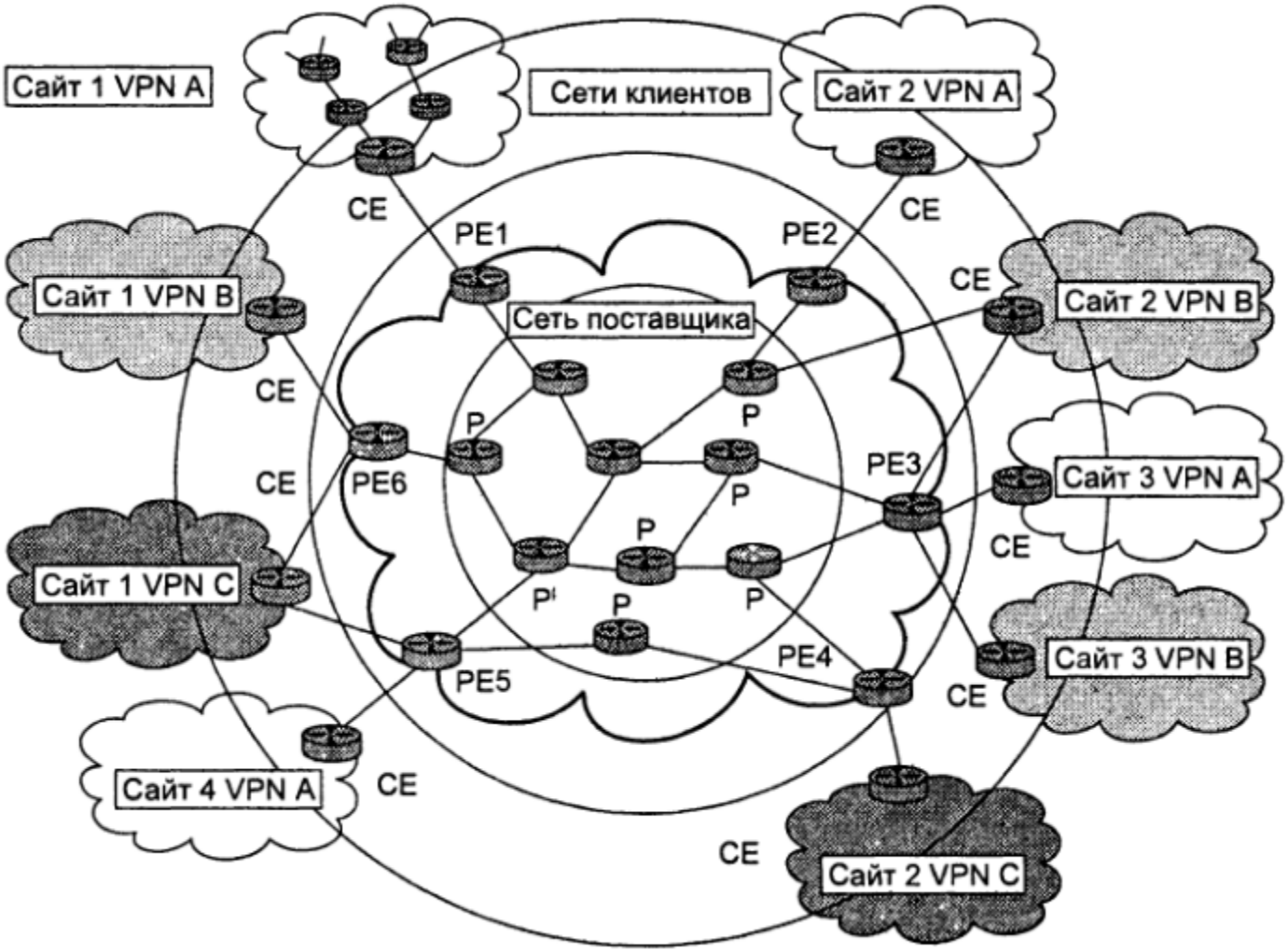
MPLS L3VPN

- Как обеспечить полную связанность IP-сети одновременно с абсолютной изолированностью?
- Связанность IP-сетей обеспечивается за счёт обмена маршрутной информацией.
- Поэтому, поставив заслоны в распространении маршрутной информации, мы можем изолировать сети друг от друга.
- В сетях MPLS L3VPN маршрутные объявления, транслируемые из сети клиента с помощью BGP, передаются только в сеть этого же клиента.
  - Это реализуется с помощью расширения MP-BGP.
- Клиентский трафик передаётся через туннели, создаваемые автоматически.

Компоненты сети MPLS VPN

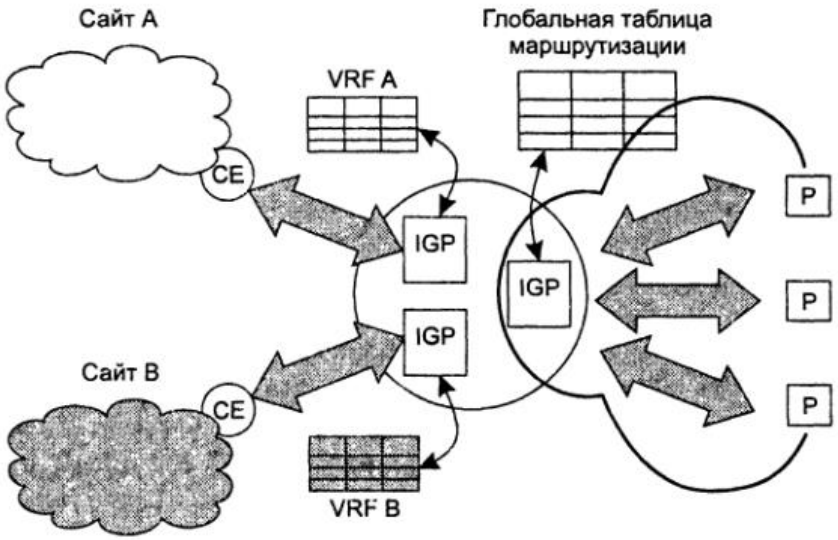
- Коммутация в сети MPLS осуществляется по меткам.
- Устройства, осуществляющие коммутацию, называют LSR
  - Пограничные маршрутизаторы PE (Provider Edge router)
  - Маршрутизаторы магистральной сети P (Provider router)
- Маршрутизатор на стороне клиента называют CE (Customer Edge)
  - CE ничего не знает о VPN
  - Общение CE-PE осуществляется по стандартным протоколам стека TCP/IP
- Главные задачи по поддержанию сети VPN возлагаются на PE
  - Разграничение маршрутов и данных
  - Являются оконечными точками виртуальных каналов, называемых LSP
  - Назначение меток для передачи через сеть MPLS

Компоненты сети MPLS VPN



Разграничение маршрутной информации

- На каждом PE имеются раздельные таблицы маршрутизации:
  - Одна таблица для связи с маршрутизаторами P (глобальная таблица маршрутизации)
  - По одной таблице на каждого клиента. (VPN Routing & Forwarding Instance, VRF)



Обмен маршрутной информацией

- Передача анонсов в сети MPLS осуществляется с помощью протокола MP-BGP (MultiProtocol Extensions for BGP, RFC2858)
- BGP рассчитан на то, что работает в едином адресном пространстве. Чтобы клиенты могли использовать одинаковые адресные пространства, используются адреса VPN-IPv4.
  - К адресам IPv4 добавляется 8-байтное поле Route Distinguisher (RD).
- Маршрутное объявление MP-BGP включает
  - Адрес сети назначения в формате VPN-IPv4
  - Адрес следующего маршрутизатора - адрес интерфейса PE, обращённого во внутреннюю сеть
  - Метка виртуальной частной сети
  - Расширенные атрибуты сообщества
    - Маршрутная цель (Route Target) – набор сайтов, входящих в данную сеть VPN.
- Политика импорта и экспорта маршрутных объявлений на основе Route Target определяет топологию сети клиента внутри сети MPLS.

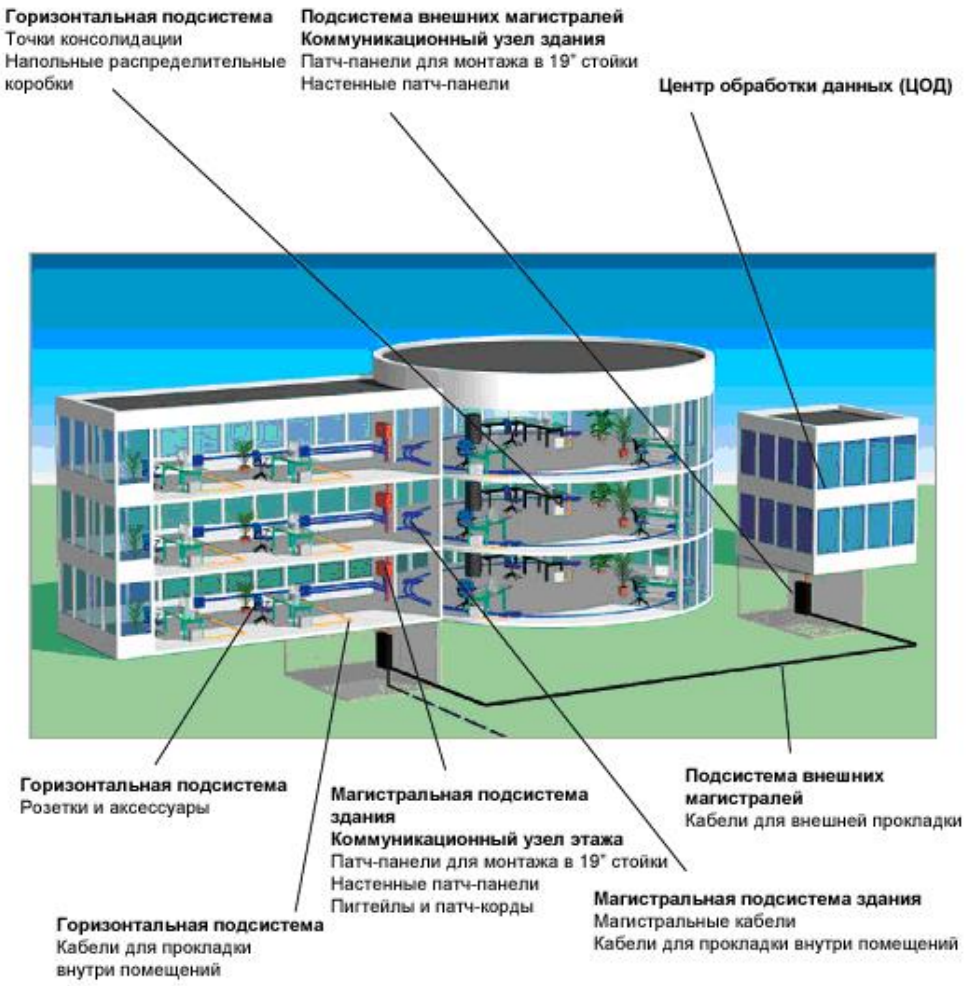
СКС

Структурированные кабельные сети

Структурированные кабельные сети

- СКС - самодостаточная система компьютерных и телефонных коммуникаций, имеющая возможность использования однотипных каналов для передачи сигналов различных систем (включая локальные вычислительные и телефонные сети, системы безопасности, видеонаблюдения).
- Топология СКС – «Иерархическая звезда»
- Коммутация осуществляется вручную коммутационными шнурами и перемычками, что позволяет не ограничивать форматы и способы передачи данных.
- Идея создания СКС предложена AT&T в 1983 г.

Структура СКС



Документация на СКС

- Структурная схема СКС;
- Структурная схема телекоммуникационного заземления;
- схемы кабельных проводок, расположения элементов телекоммуникационной инфраструктуры;
- схемы размещения шкафов и стоек, оборудования распределительных пунктов;
- схемы размещения панелей в телекоммуникационных шкафах / стойках;
- схемы подключений кабелей на панелях / кроссах;
- схемы организации рабочих мест;
- систему администрирования, в том числе, систему маркировки, учетные записи в виде таблицы соединений;
- электрические однолинейные схемы;
- кабельный журнал, таблицы распределения групповых линий по фазам.

Монтаж СКС

- Необходимо обеспечить:
  - Минимальную разбалансировку пар в процессе монтажа разъемов;
  - Допустимые радиусы изгиба кабелей;
  - Отсутствие перетяжки кабельных жгутов;
  - Эквипотенциальность силового и телекоммуникационного заземления;
  - При прокладке кабелей внутри коробов допустимо заполнение не более 50% сечения;
- Заземление
  - Телекоммуникационное заземление должно быть установлено во всех СКС.
- Система электропитания
  - Раздельные силовые розетки для телекоммуникационного оборудования и бытовых приборов;
  - При параллельной прокладке силовых и телекоммуникационных проводов должны быть выдержаны нормы на минимальное расстояние.