ИРКУТСКИЙ ПОЛИТЕХ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Лекция по дисциплине
«Сети и телекоммуникации»

Соединение «точка-точка» и шифрование трафика

Руководитель лаборатории сетевых технологий
института ИТиАД ИРНИТУ:
Аношко Алексей Федорович
Telegram: @a_anoshko

High-Level Data Link Control (HDLC) - ISO 13239 Publication date : 2002-07

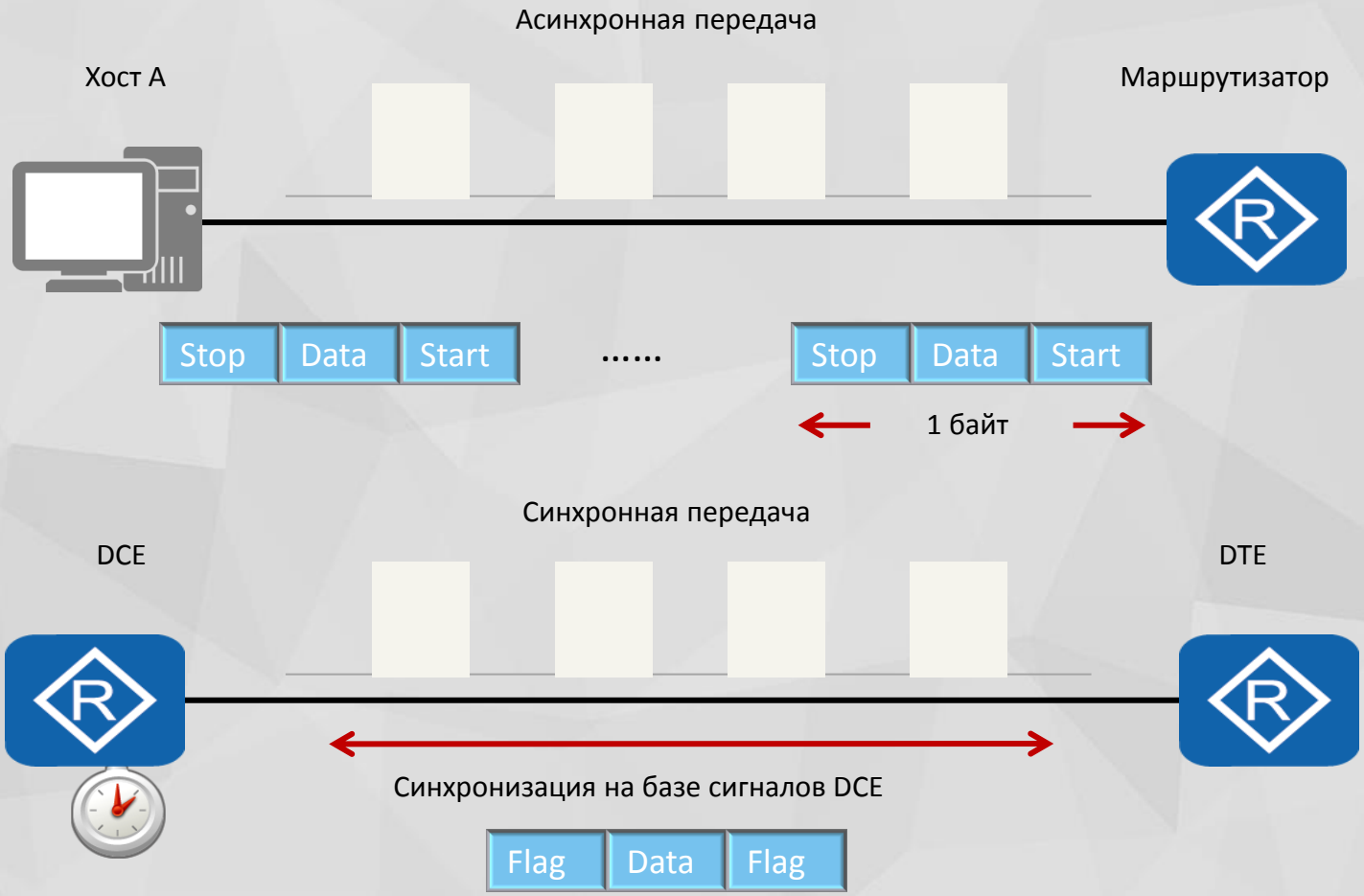
PPP - Point-to-Point Protocol – RFC 1968, June 1996

Основное различие между HDLC и PPP заключается в том, что HDLC - это битно-ориентированный протокол, а PPP - это символьно-ориентированный протокол.

HDLC и PPP являются важнейшими протоколами канального уровня, используемыми в глобальной сети (WAN), где HDLC также может быть реализован с PPP для получения эффективных результатов.

HDLC описывает метод инкапсуляции, применяемый к данным в синхронном последовательном канале передачи данных. С другой стороны, протокол PPP имеет дело с инкапсуляцией данных, транспортируемых в двухточечных каналах, и он может быть синхронным или асинхронным.

Последовательная передача сигнализации



Протокол HDLC

- *Поле адреса - используется для описания терминала.*
- *Поле управления - биты в поле управления предназначены для порядкового номера и подтверждений.*
- *Поле данных - это поле используется для хранения информации.*
- *Поле контрольной суммы -В этом поле биты зарезервированы для выполнения кода с циклическим избыточным кодом.*

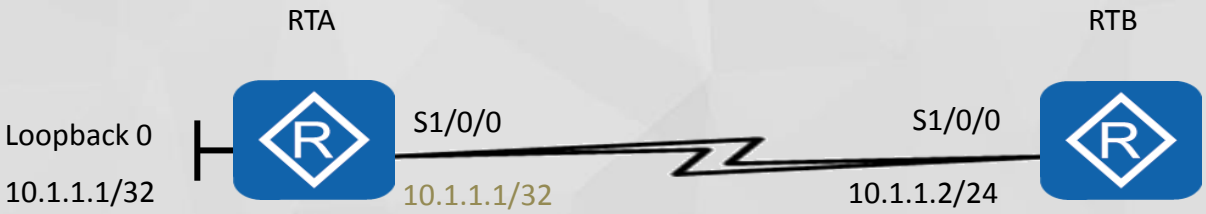
HDLC команды и запросы

- **Формат передачи информации** (I-Frame) - он последовательно транспортирует пронумерованные кадры, которые содержат информационное поле.
- **Контрольный формат** (S-кадр) - контрольные кадры выполняют функции управления, такие как подтверждение, статус передачи информации, опрос и устранение ошибок. Команды и запросы, включенные в это, - ПОЛУЧИТЬ ГОТОВ, ПОЛУЧИТЬ НЕ ГОТОВ, ОТКАЗАТЬ, и так далее.
- **Ненумерованный формат** (U-Frame) - он в основном расширяет функции управления каналом передачи данных. В эту категорию попадают несколько команд и запросов, таких как RESET, TEST, FRAME REJECT, REQUEST DISCONNECT и так далее.

Конфигурирование базовых параметров HDLC


```
[RTA]interface Serial 1/0/0
[RTA-Serial1/0/0]link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y
[RTA-Serial1/0/0]ip address 10.0.1.1 30
```

Назначение адресов ненумерованным интерфейсам в HDLC




```
[RTA]interface Serial 1/0/0
[RTA-Serial1/0/0]link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y
[RTA-Serial1/0/0]ip address unnumbered interface loopBack 0
```

- Для установления соединения по последовательному каналу поддерживается заимствование IP-адресов другого интерфейса.

Протокол PPP

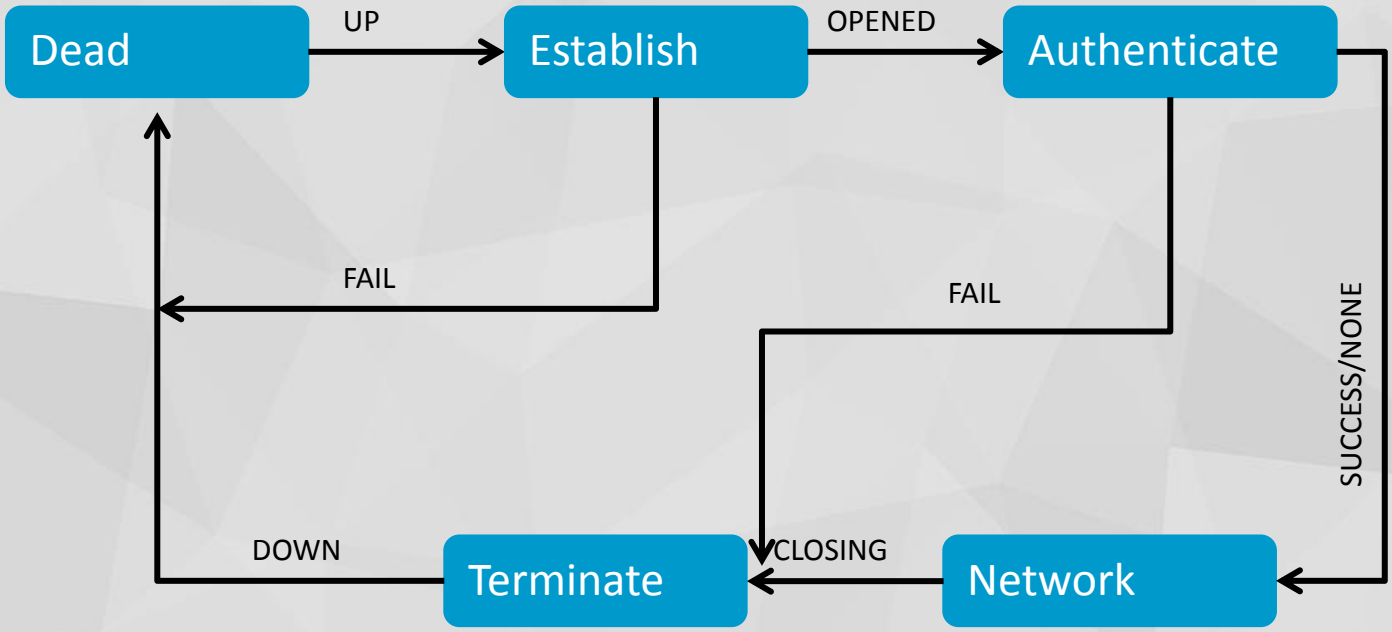
PPP также является протоколом WAN, но в протокол PPP внесены некоторые улучшения после HDLC.

Все ссылки совместно обрабатываются как единая независимая IP-сеть, которая имеет свой собственный формат кадра, метод аппаратной адресации и протокол канала передачи данных

Компоненты PPP

Название	Функция
Метод инкапсуляции PPP	Определение формата, используемого при поддержке инкапсуляции протоколов верхнего уровня, таких как IP, IPX и т.д.
Протокол управления каналом	Определение методов установления, конфигурирования и тестирования каналов передачи данных.
Протокол управления сетью (NCP)	Определение набора протоколов для установления соединения и согласования параметров для различных протоколов сетевого уровня.

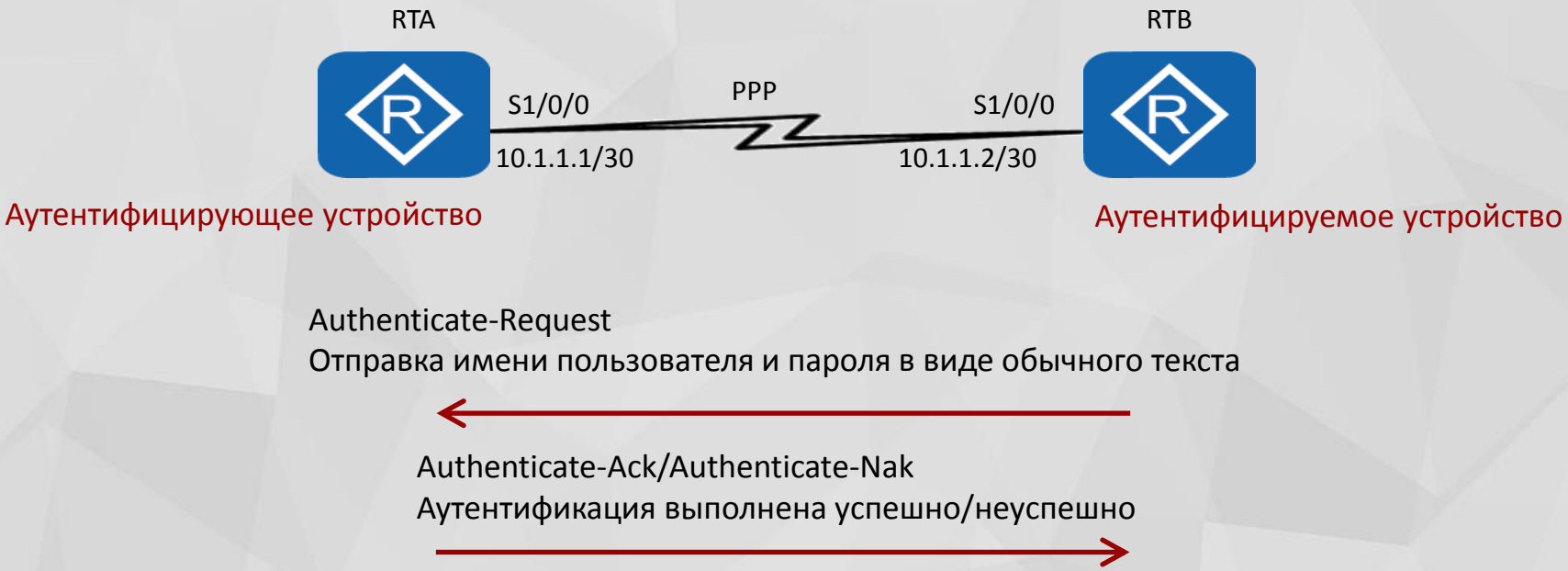
Процесс установления канала PPP



Протокол HDLC

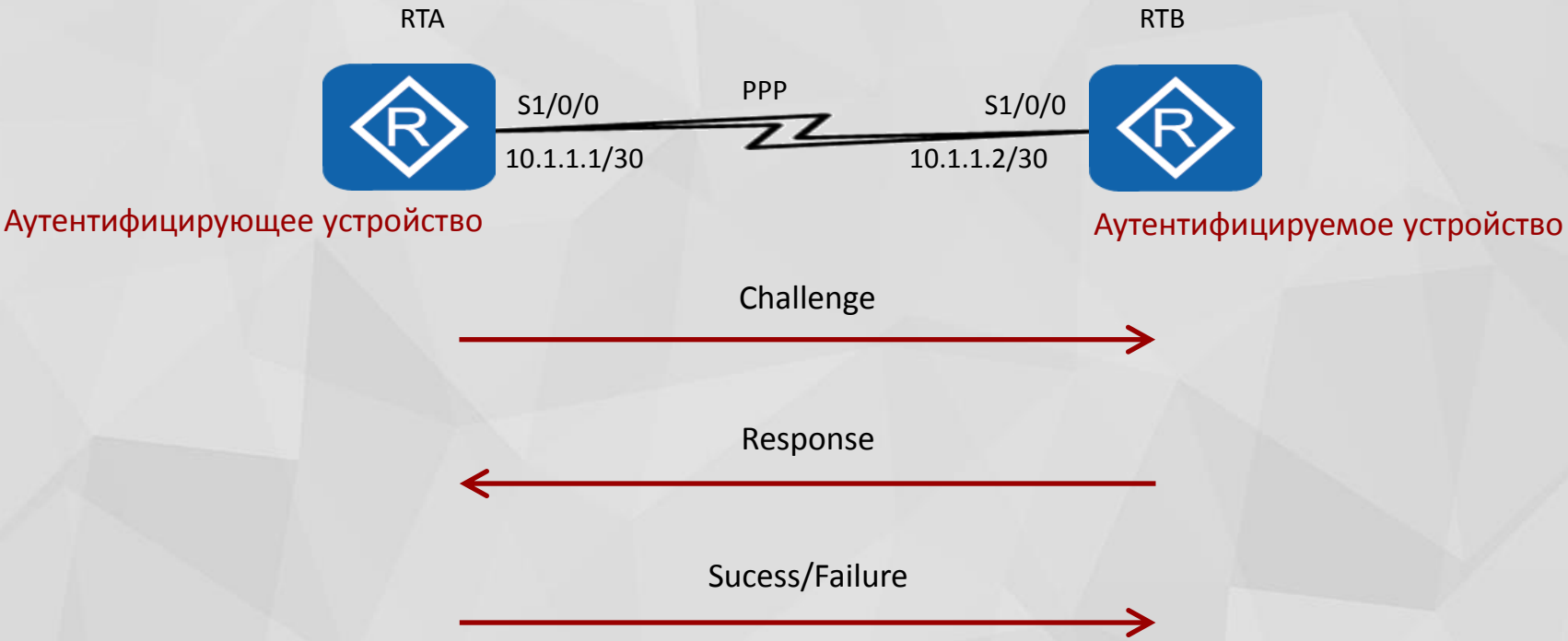
Тип пакета	Функция
Configure-Request	Параметры для установления и конфигурирования канала.
Configure-Ack	Подтверждение, отправляемое после проверки всех параметров Configure-Request.
Configure-Nak	Подтверждение, что все параметры Configure-Request распознаны, но не все значения приемлемы.
Configure-Reject	Отклонение параметров, включенных в Configure-Request от равноправного узла.

Режимы аутентификации PPP – Режим PAP



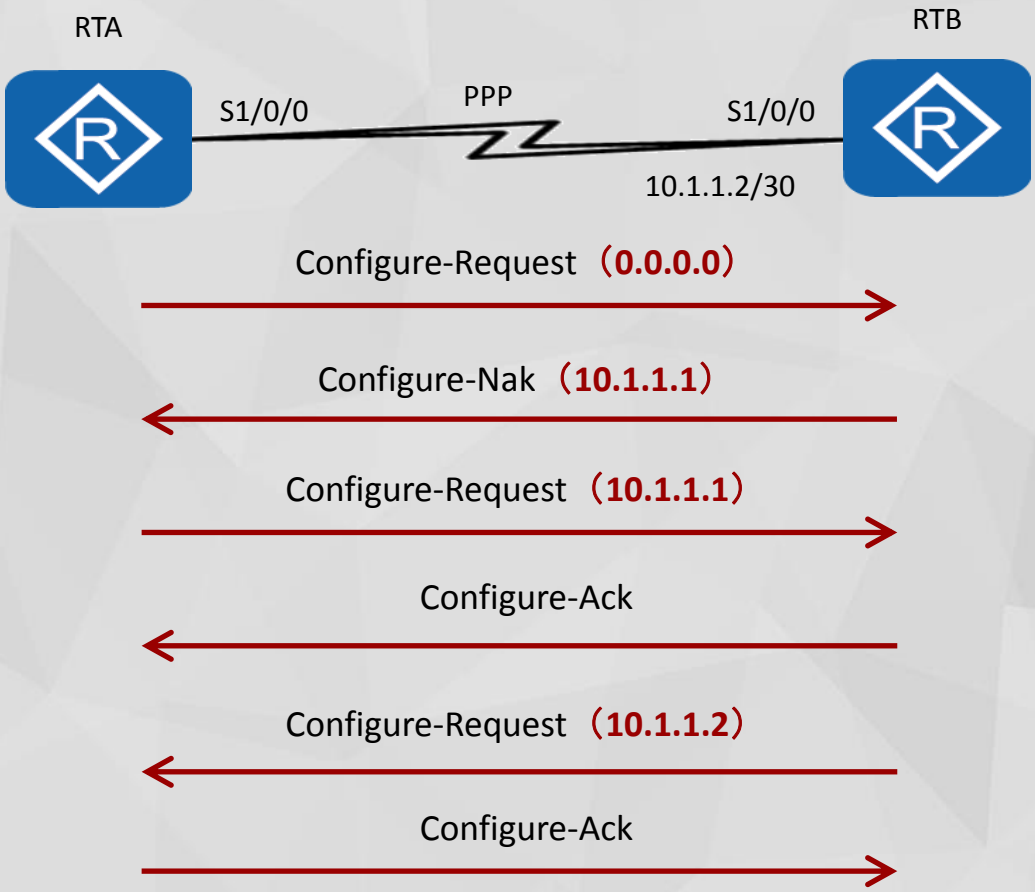
- Протокол аутентификации по паролю (PAP) предусматривает проверку подлинности путем передачи незашифрованного пароля.

Режимы аутентификации PPP – Режим CHAP



Принципиальным отличием CHAP является защита, обеспечиваемая путем предотвращения передачи любого пароля по каналу

Согласование динамических адресов IPCP



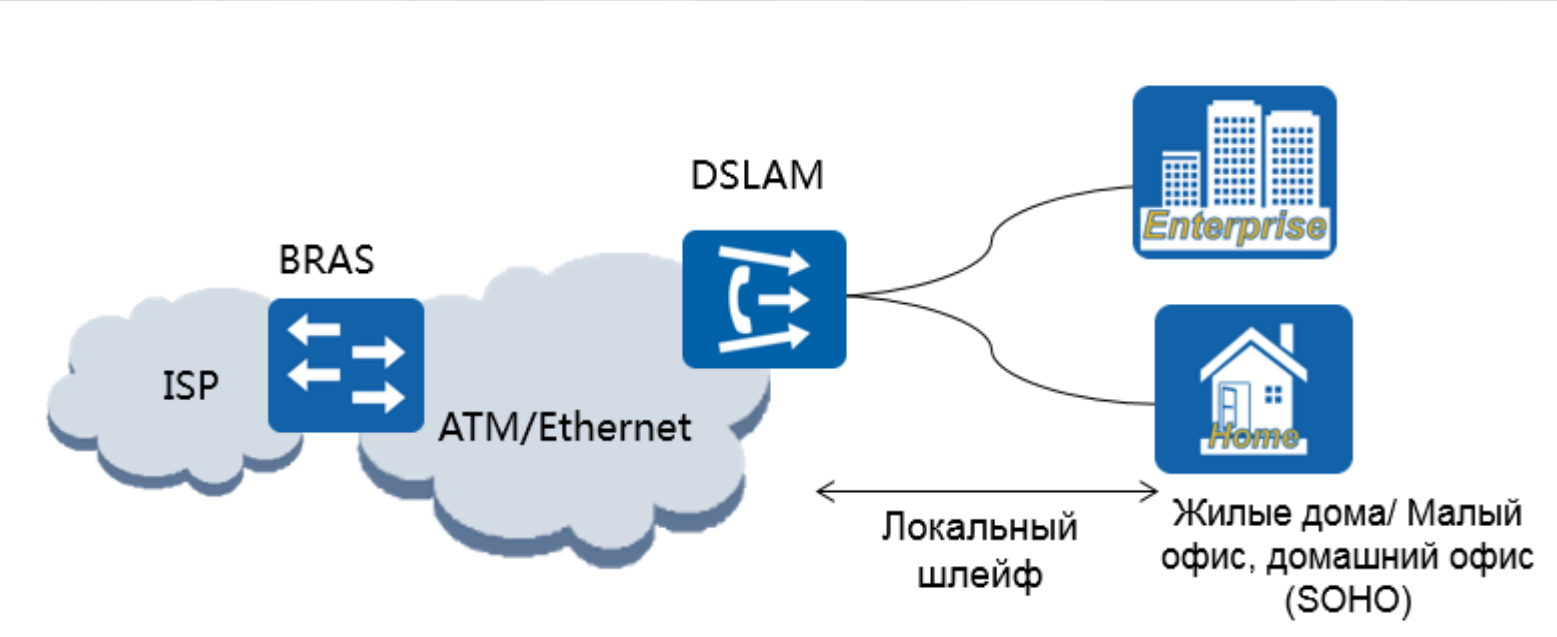
Сравнение HDLC и PPP

Основа для сравнения	HDLC	PPP
Расширяется до	Протокол канального уровня высокого уровня	Двухточечный протокол
Тип протоколов	Бит-ориентированный протокол	Байт-ориентированный протокол
Используется в	Только синхронный носитель	Синхронный, а также асинхронный носитель
Аутентификация	Нет предоставления аутентификации	Обеспечивает аутентификацию
Динамическая адресация	Не предлагает динамическую адресацию.	Динамическая адресация используется.
Реализовано в	Двухточечные и многоточечные конфигурации.	Только двухточечные конфигурации

Принципы работы и конфигурирование PPPoE

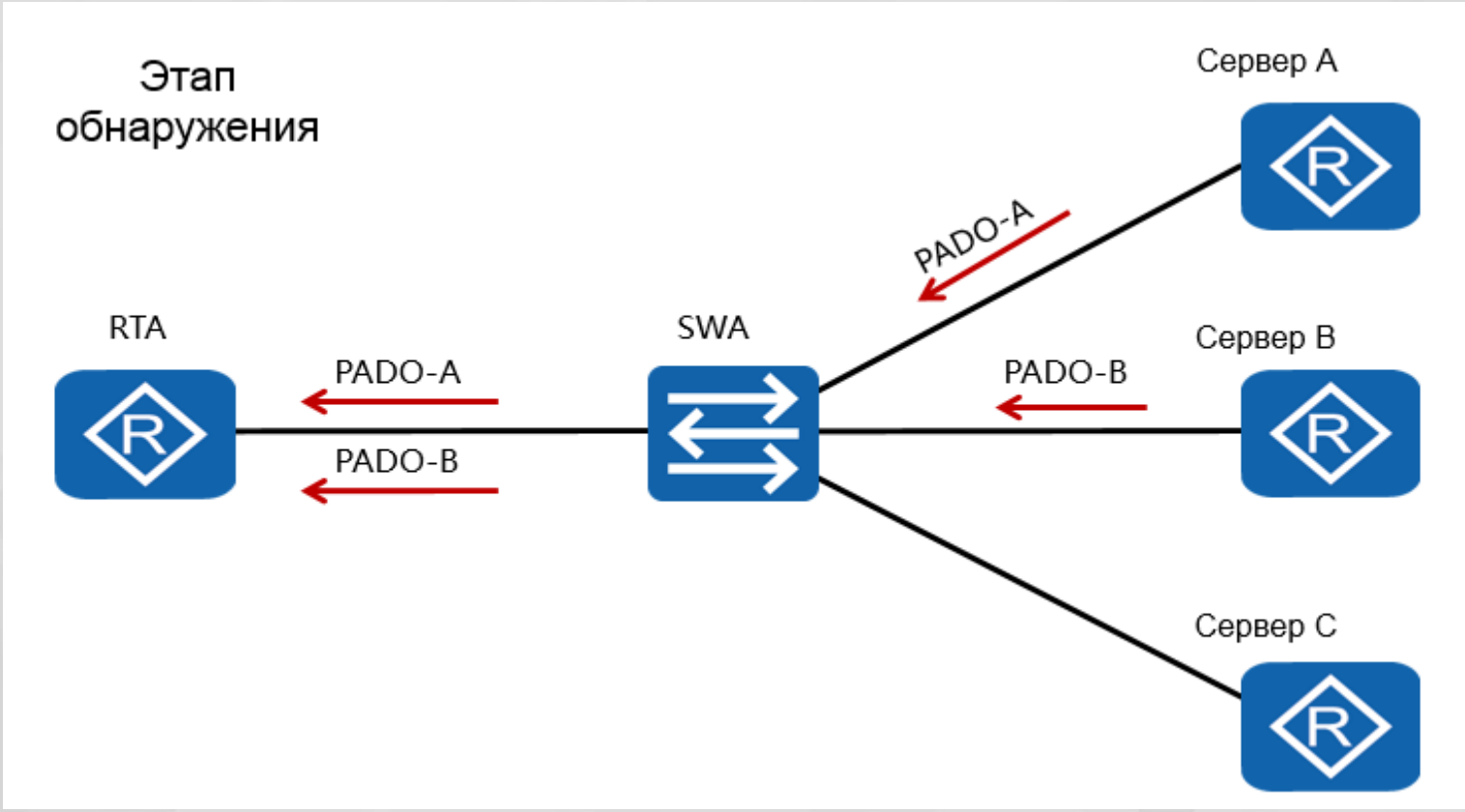
Технология DSL основана на существующей инфраструктуре телефонных линий, которая имеется практически в каждом доме и офисе по всему миру. Появление новых стандартов DSL, обеспечивающих скорость передачи данных до 100 Мбит/с, способствовало тому, что DSL и по сей день широко применяется в качестве WAN в домах и на предприятиях. Изначально развертывание DSL осуществлялось на базе устаревших сетей ATM. Однако с появлением технологии Ethernet многие интернет-провайдеры начали использовать сети Ethernet для развертывания своих сервисов. В данной презентации приводится описание PPPoE (Point-to-point protocol over Ethernet) – протокола передачи кадров PPP через Ethernet, который используется сервисами DSL.

Цифровые абонентские линии



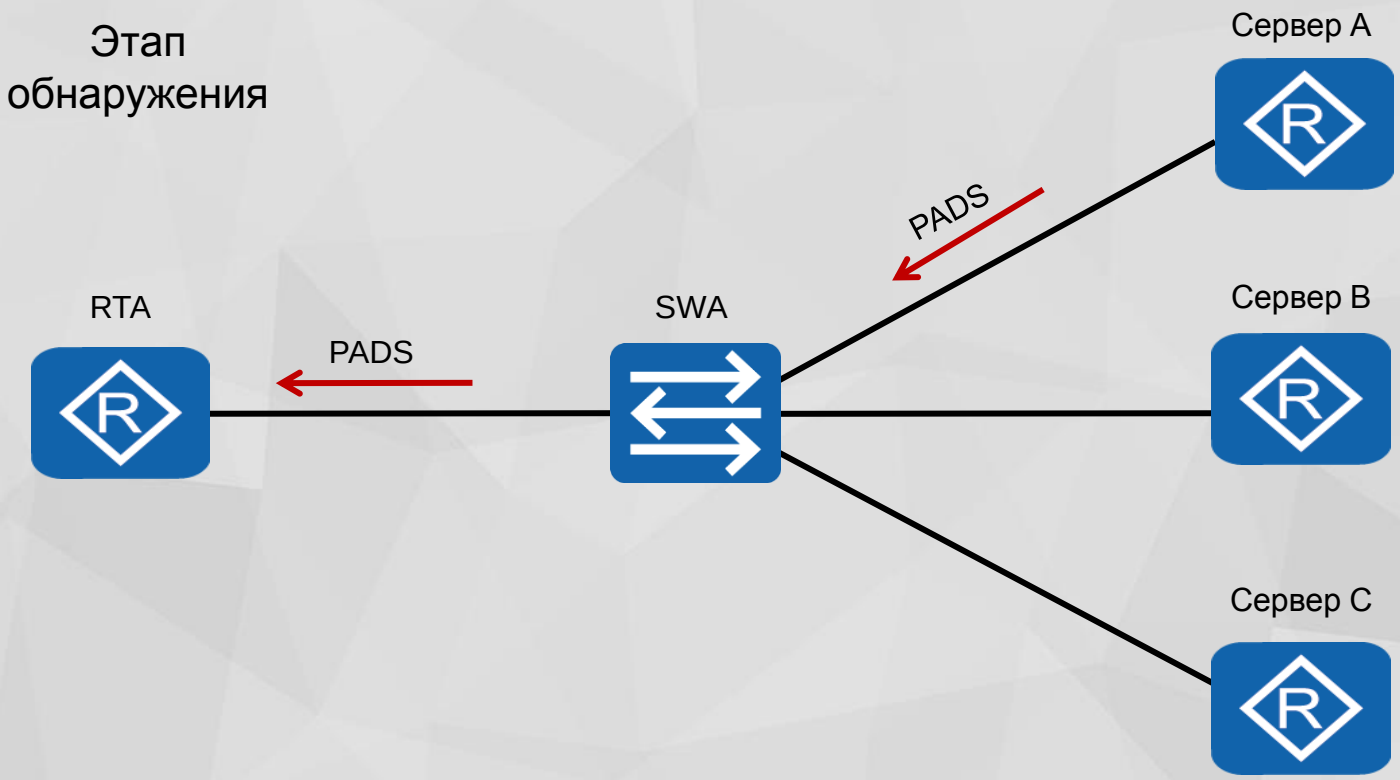
- Широкополосная передача данных приходит на смену коммутируемого доступа.
- Сигналы данных передаются по медным проводам («локальному шлейфу»).

Процесс установления сеанса PPPoE



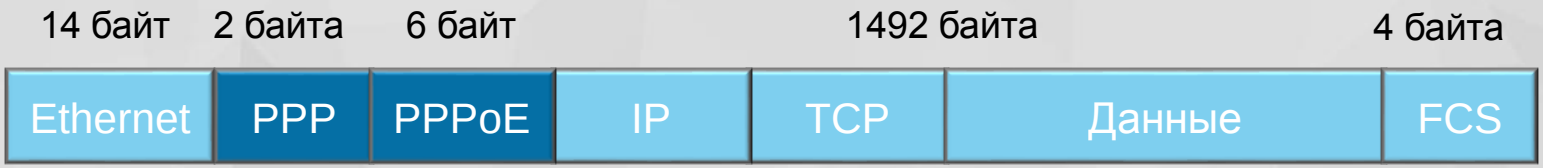
- Все серверы, которые получили пакет PADI и могут предоставить требуемые услуги, отправляют ответный пакет PADO клиенту.

Процесс установления сеанса PPPoE



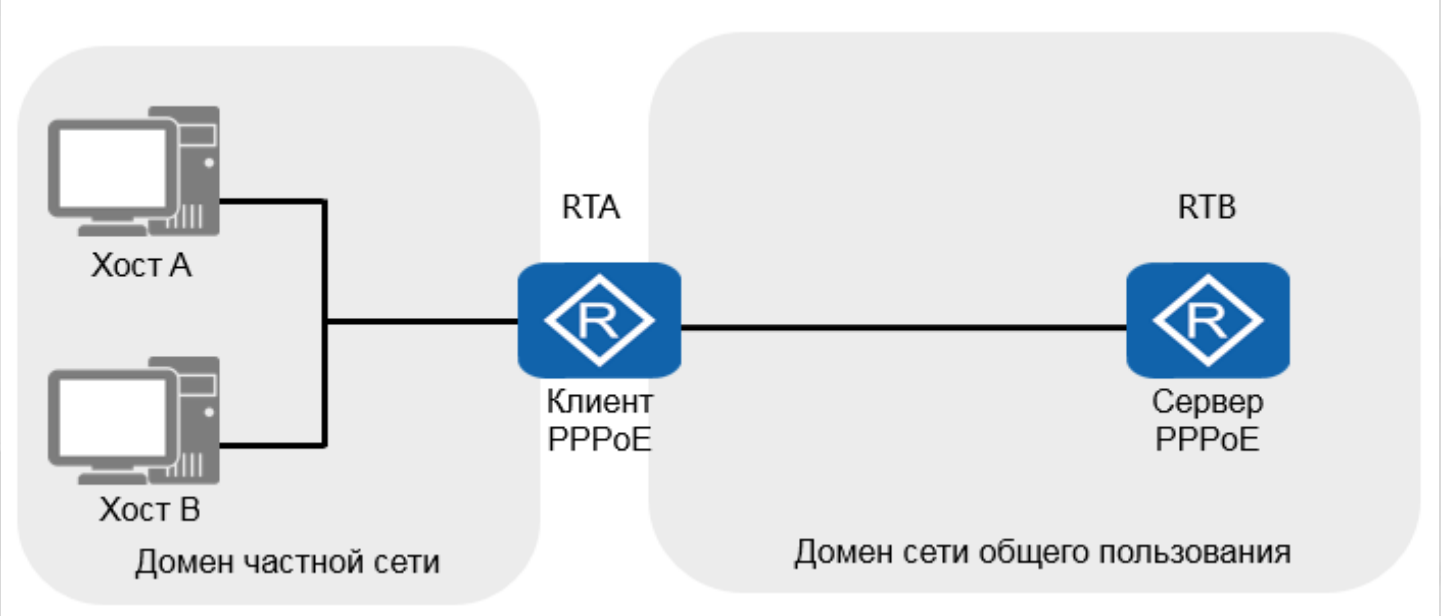
- Выбранный сервер генерирует уникальный идентификатор сеанса PPPoE в процессе подготовки к установлению сеанса PPP.

Согласование размера пакетов



- В кадре передаются дополнительные шесть байтов заголовка PPPoE.
- Для предотвращения потери кадров MTU/MRU должен быть не более 1492 байта.

Применение PPPoE в корпоративных сетях



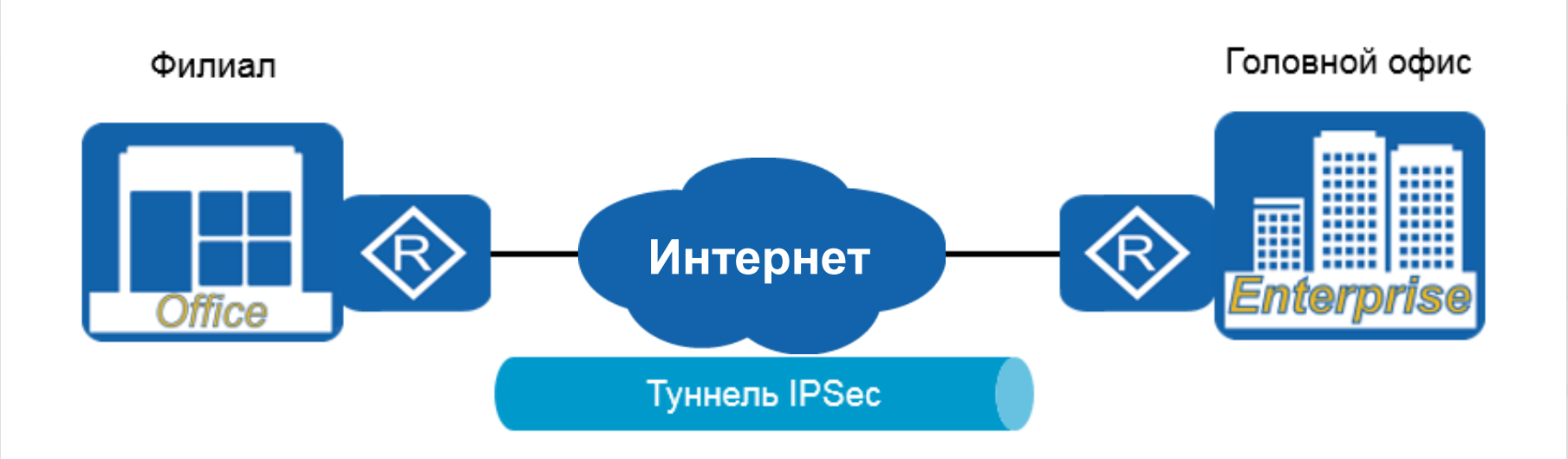
- Хосты с адресами частной сети не могут существовать в домене сети общего пользования.
- Для соединения PPPoE необходимо преобразование адресов.

Защита данных с IPSec VPN

На ранних этапах разработки протокола TCP/IP очень мало внимания уделялось обеспечению безопасности связи между одноранговыми устройствами. Однако по мере развития сетей реализация эффективной защиты передаваемых данных стала актуальной задачей.

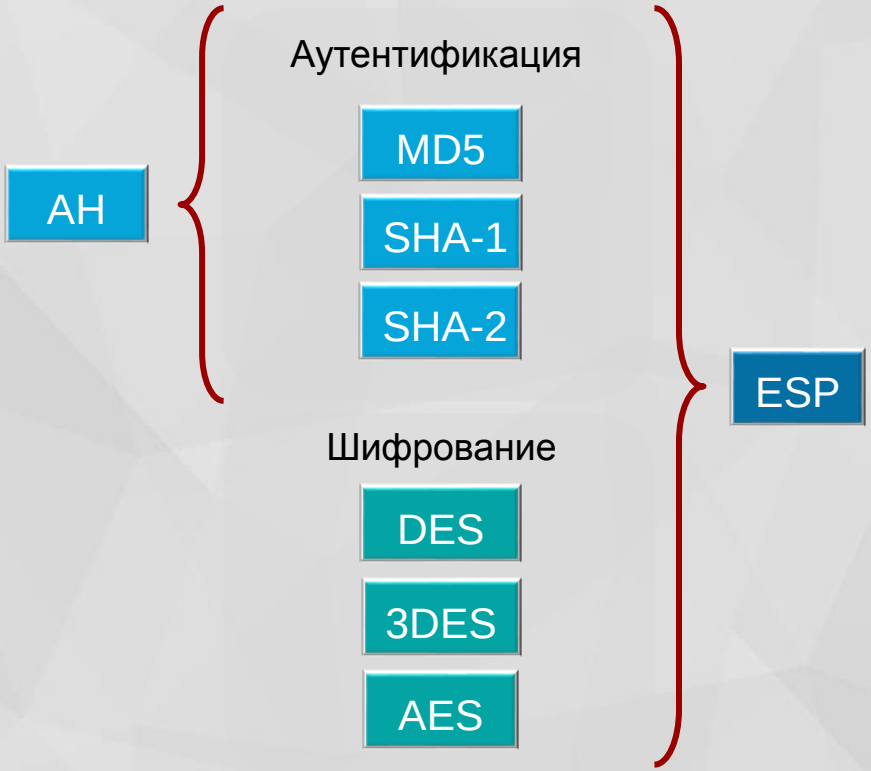
Набор протоколов IPSec предлагает механизм защищенной передачи данных в IP-сетях, обеспечивая конфиденциальность, целостность и достоверность данных, главным образом, благодаря поддержке базовых протоколов. IPSec по-прежнему остается ключевой структурой для защиты данных; компоненты IPSec были интегрированы в стандарты протокола TCP/IP следующего поколения.

Применение IPSec VPN



- Защищает развертывание частной сети связи на базе инфраструктуры сети общего пользования.

Архитектура IPSec VPN



- Конфиденциальность и целостность сервисов поддерживается с помощью протоколов аутентификации и шифрования.

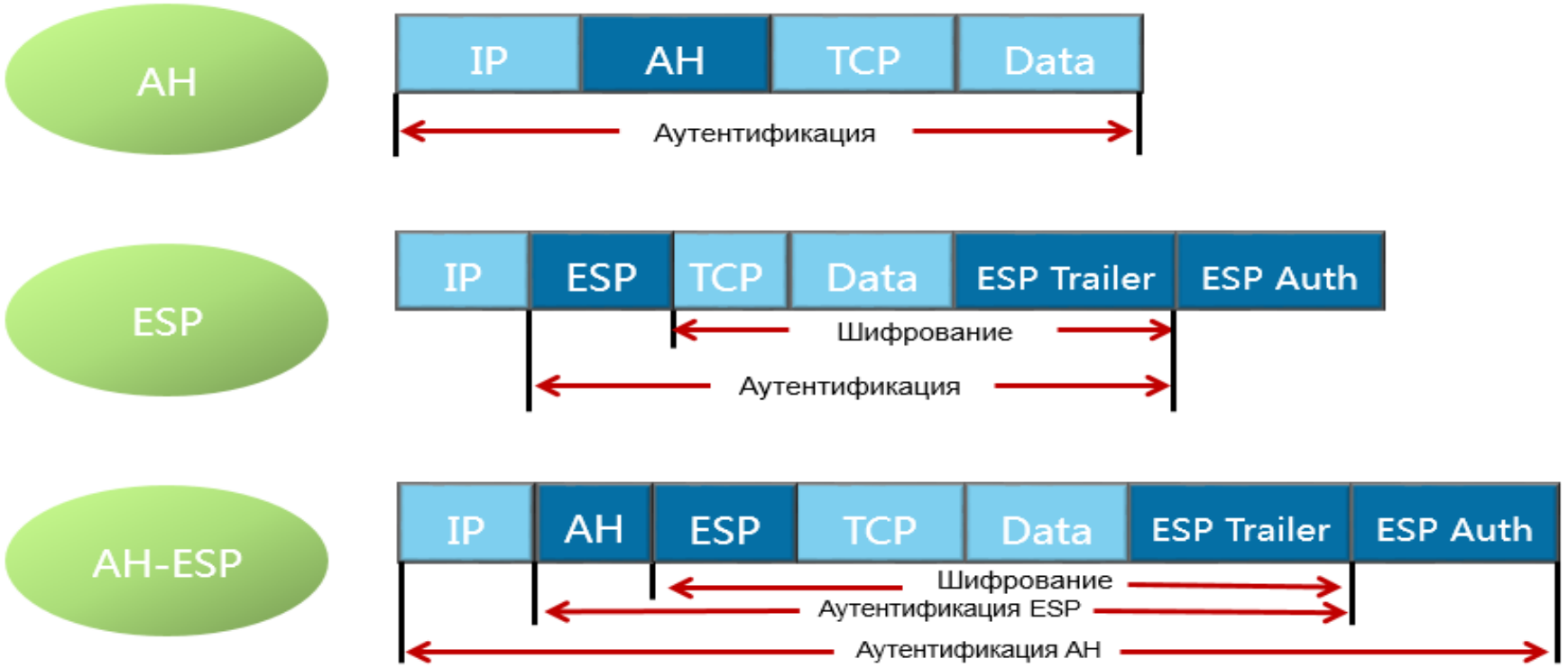
Ассоциация безопасности (Security Association)

Локальный адрес
Удаленный адрес
Входящий SPI
Исходящий SPI
Ключ
Преобразование (предложение)

Локальный адрес
Удаленный адрес
Входящий SPI
Исходящий SPI
Ключ
Преобразование (предложение)

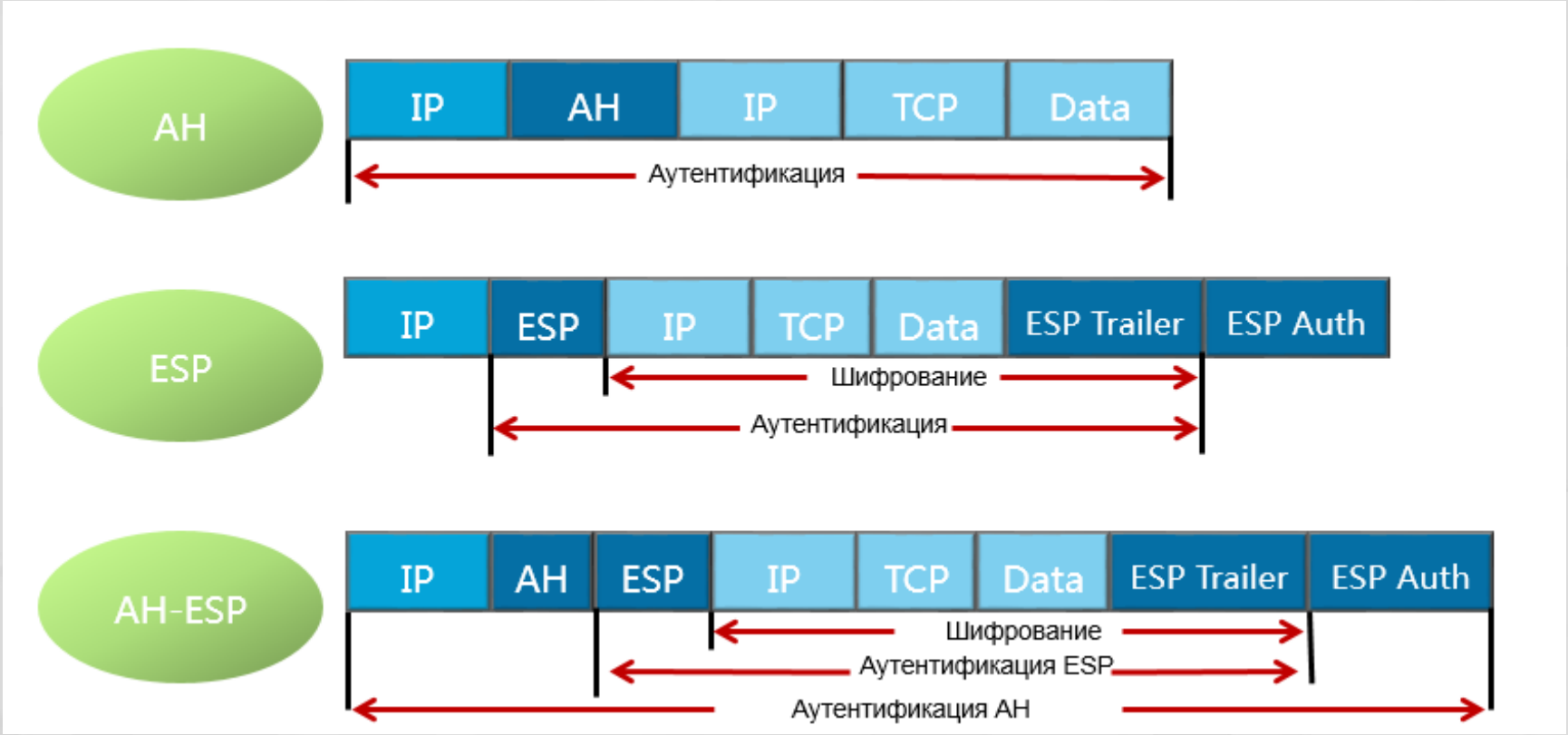
- Определяет параметры для установления соединения.
- Ассоциация безопасности определяет параметры только в одном направлении.

Транспортный режим IPSec



- В ассоциациях безопасности определяются режимы инкапсуляции.
- В транспортном режиме выполняется защита только полезной нагрузки пакета.

Протокол HDLC



- В туннельном режиме происходит инкапсуляция пакетов во второй IP-заголовок.
- Защита распространяется на внутренний IP-заголовок и полезную нагрузку пакета.

Организация IPSec VPN

Универсальная инкапсуляция при маршрутизации

Ограничения IPSec VPN уменьшают возможности передачи маршрутов между разнородными сетями site-to-site и позволяют реализовать только решения для статических маршрутов.

Универсальная инкапсуляция при маршрутизации (Generic Routing Encapsulation; GRE) представляет собой механизм инкапсуляции пакетов одного протокола в пакеты другого протокола. Данный механизм реализуется в качестве основного решения устранения ограничений IPSec VPN, поэтому его знание необходимо для понимания технологии IPSec VPN.

Протокол HDLC

- Поддержка инкапсуляции протоколов поверх других протоколов.
- Возможность маршрутизации между удаленными и разнородными сетями.

Поддержка IPSec VPN для GRE

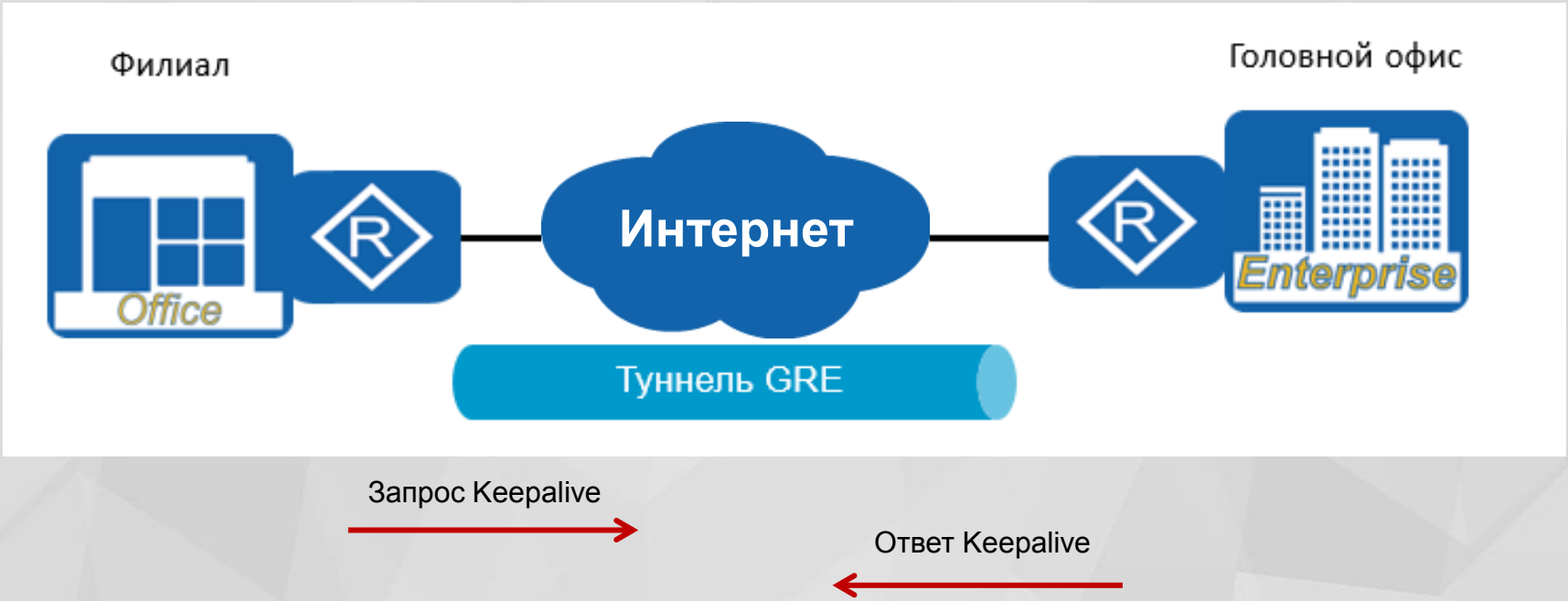
- GRE не включает меры обеспечения конфиденциальности полезной нагрузки.
- Для этой цели можно использовать IPSec.

Аутентификация в GRE с помощью ключа

C	0	K	0	0	Recursion (Рекурсия)	Flags (Флаги)	Version (Версия)	Protocol type (Тип протокола)
Checksum (Контрольная сумма) (опционально)								0
Key (Ключ) (опционально)								

- В поле «Ключ» пакета GRE содержится информация о дополнительном инструменте аутентификации.

GRE Keepalive



- Данные сообщения служат для отслеживания изменений состояния туннеля GRE.
- Отсутствие ответа на Keepalive-запрос приводит к разъединению туннеля GRE.