ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

ИНТЕРНЕТ ВЕЩЕЙ

Сетевые протоколы передачи данных

Классификация беспроводных сетей

NFC
RFID

Bluetooth
ZigBee
Z-Wave
ANT

802.11a/b/g/n/…

Wi-SUN
ZigBee-NAN

4G/5G

	PAN	LAN	MAN	WAN
Стандарты	Bluetooth	IEEE 802.11 a/g/n	802.16 MMDS,LMDS	GPRS,CDMA, 3-5G
Скорость	< 48 Мбит/с	54-300 Мбит/с	40Мбит/с- 1 Гбит/с	10-25 Гбит/с
Диапазон	Короткий	Средний	Длинный	Длинный
Область применения	Точка- Точка	Сеть	Доступ последней мили	Мобильные устройства

Стандарт IEEE 802.11

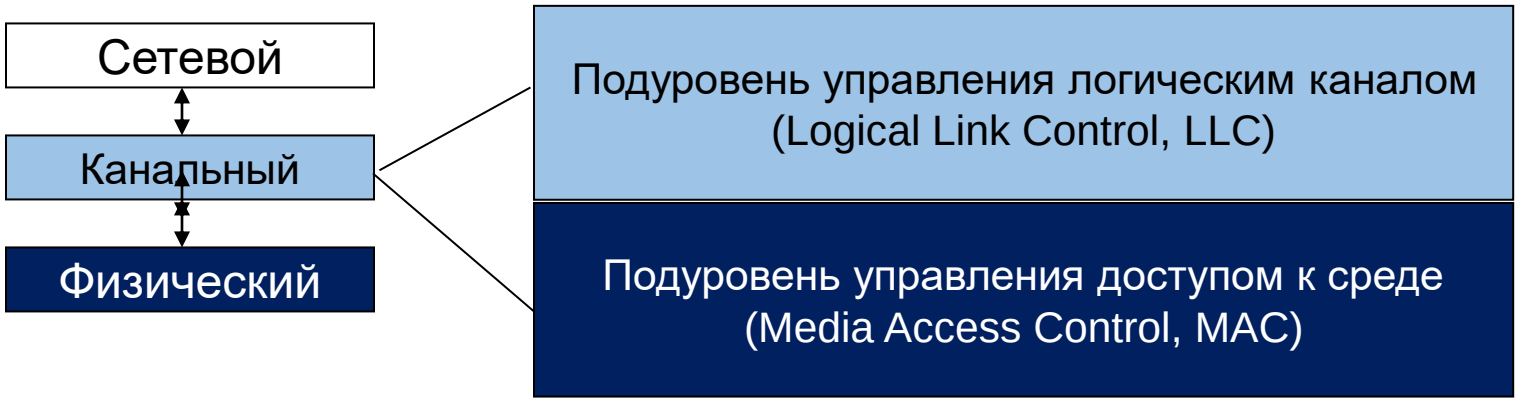
IEEE 802.11 — набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9; 2,4; 3,6; 5 и 60 ГГц.

IEEE определяет четыре основных стандарта WLAN 802.11: 802.11a, 802.11b, 802.11g и 802.11n.

	802.11a	802.11b	802.11g	802.11n
Год принятия	1999	1999	2003	2009
Скорость	54 Мбит/с	11 Мбит/с	54 Мбит/с	До 600 Мбит/с
Полоса частот	5 ГГц	2.4 ГГц	2,4 ГГц	2,4-2,5 или 5 ГГц
Количество каналов	23	3	3	9

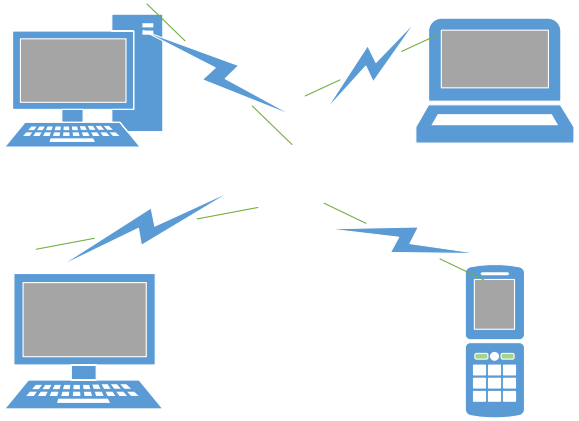
Канальный уровень

- Физический уровень – способ передачи сигналов
- 6 стандартов IEEE серии 802.11 используют электромагнитное излучение:
  - 2,4 ГГц – 802.11b, 802.11g, 802.11n
  - 5 ГГц – 802.11a, 802.11n, 802.11ac
  - не требуют лицензирования
  - наличие помех и коллизий.
- **Уровень MAC** – способ доступа к общей среде выполняет следующие функции: доступ к разделяемой среде; обеспечение перехода станции между базовыми станциями; обеспечение безопасности передачи данных.
- **Уровень LLC** – передача данных



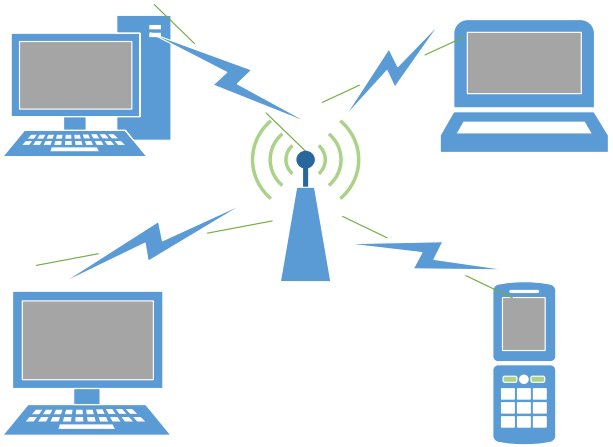
Топология

1. Независимые базовые зоны обслуживания (Сети Ad-hoc)



Проблема: увеличение вероятности коллизий, поскольку в случае одновременной передачи сигналов станциями A и C, эти станции не могут зафиксировать возникновение коллизии.

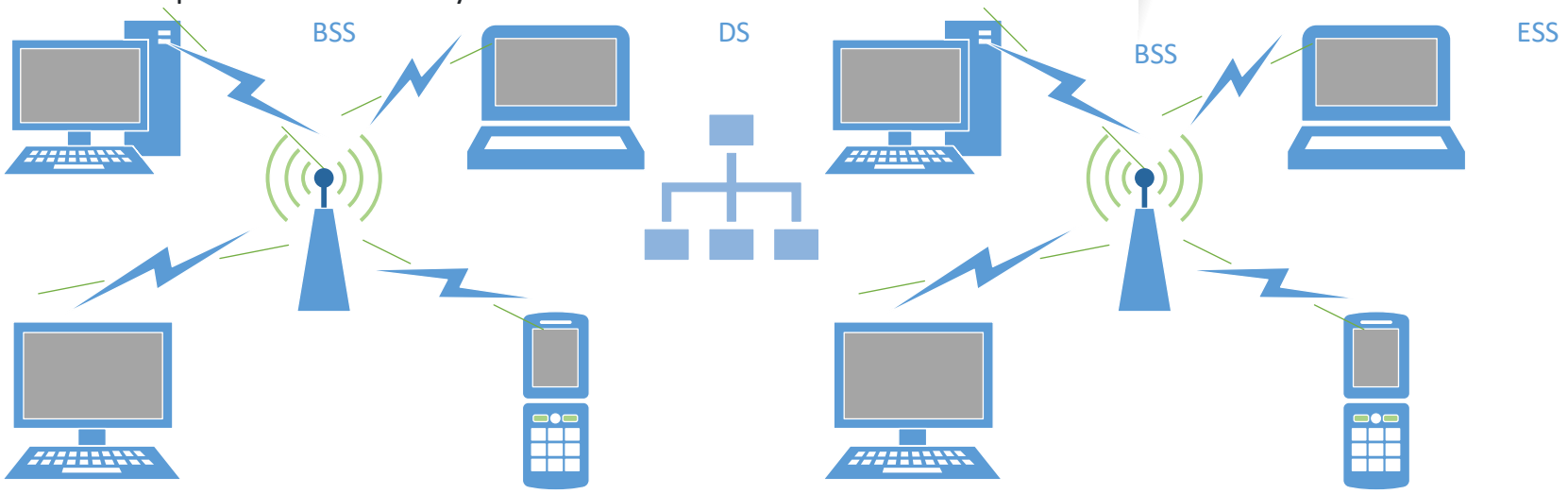
2. Базовый набора служб (Basic Service Set, BSS)



Возможность подключения достаточно большого количества пользователей, более высокая помехоустойчивость . Точка доступа может работать как по прямому назначению, так и в составе проводной сети и служить в качестве моста между проводным и беспроводным сегментами сети.

Топология

3. Расширенные зоны обслуживания

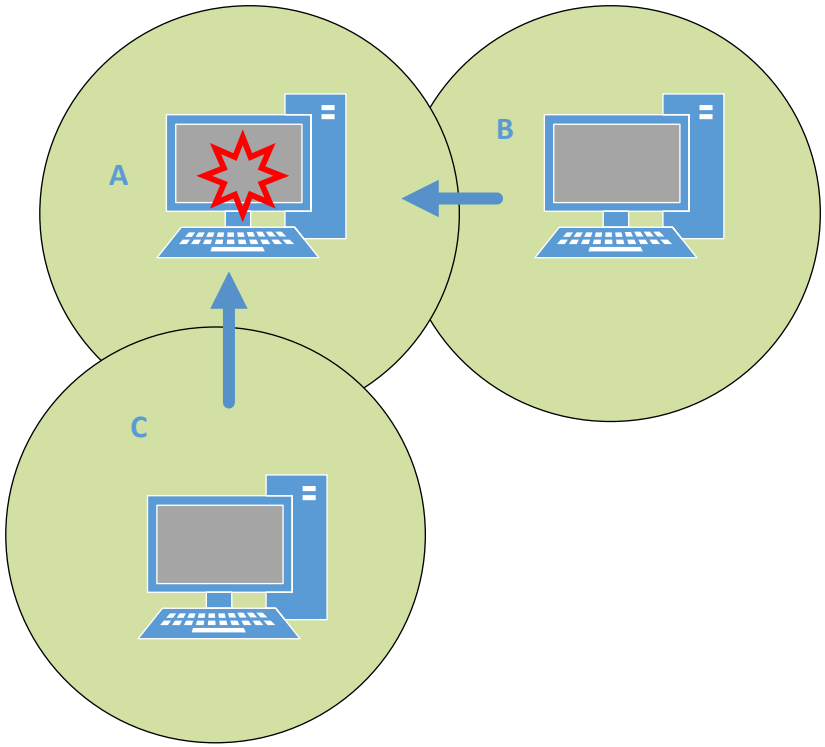


Сеть с базовым набором услуг (Basic Service Set - BSS) – конструктивная единица сети, состоит из нескольких станций, реализующих протокол MAC. Соединяется с распределительной системой (Distribution System - DS) через точку доступа или кабельное соединение.

Сеть с расширенным набором услуг (Extended Service Set - EES) – состоит из нескольких BSS объединенных распределительной системой DSS.

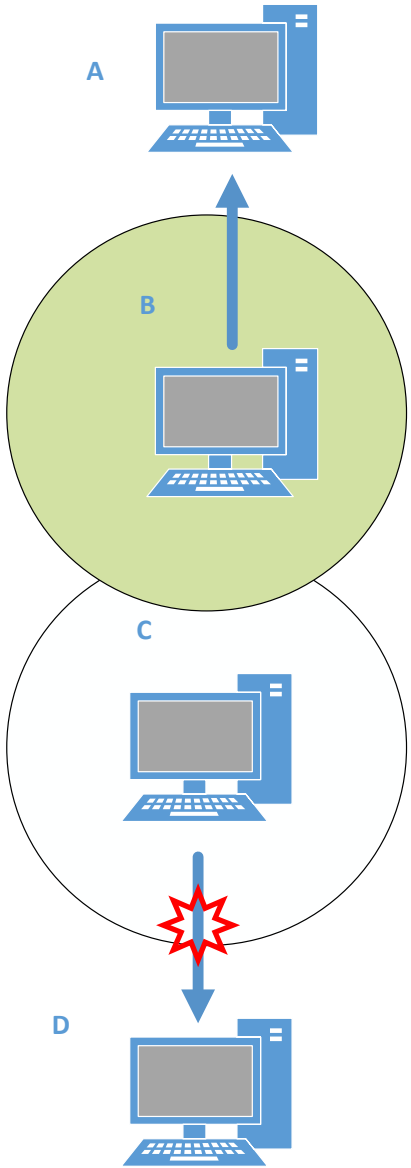
Служба распределенной системы (Distributed System Service - DSS) – служба, обеспечивающая передачу пакетов между станциями, которые не могут взаимодействовать непосредственно. DSS образуется базовыми станциями и распределительной системой DS. DS может быть основана на проводной или беспроводной среде.

Проблемы «засвеченной» станции



1. Хост B планирует осуществить передачу данных A, контроль канала показал, что он свободен.
2. В этот же момент времени хост C тоже решил передать данные хосту A, поскольку зона действия беспроводной среды C свободна.
3. Однако когда эти данные дошли до компьютера A, они столкнулись с теми данными, которые передавал хост B, произошла коллизия и хост A не может принять данные, не от одного хоста.

Проблемы скрытой станции



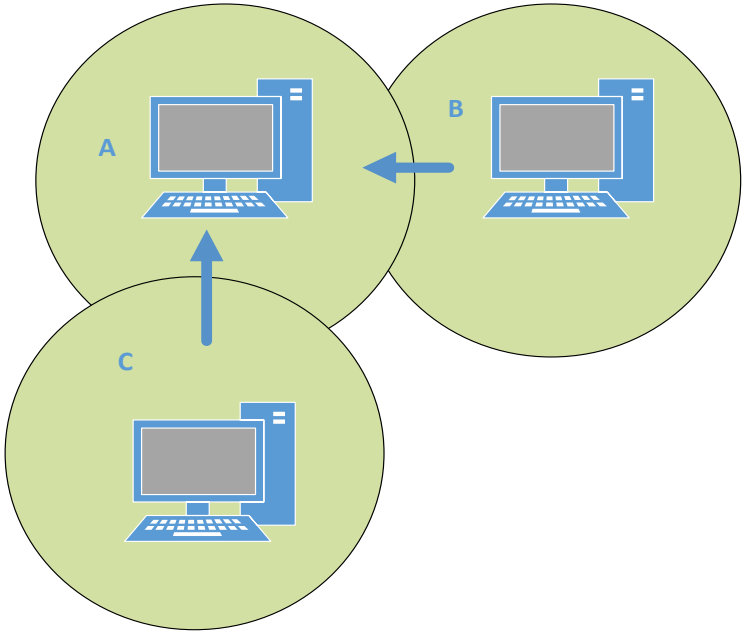
Хост D находится вне зоны действия передатчика хоста B, поэтому хост C может смело передавать данные хосту D, однако сам хост C находится в зоне действия передатчика хоста B, поэтому он считает, что среда занята и ждет когда хост B закончит передачу.

Проблемы передачи в среде Wi-Fi

- Передаваемый сигнал намного мощнее принимаемого
- Проблемы «скрытой» и «засвеченной» станции
- Сигнал о коллизии может не дойти до всех компьютеров
- При отсутствии подтверждения кадр пересылается повторно

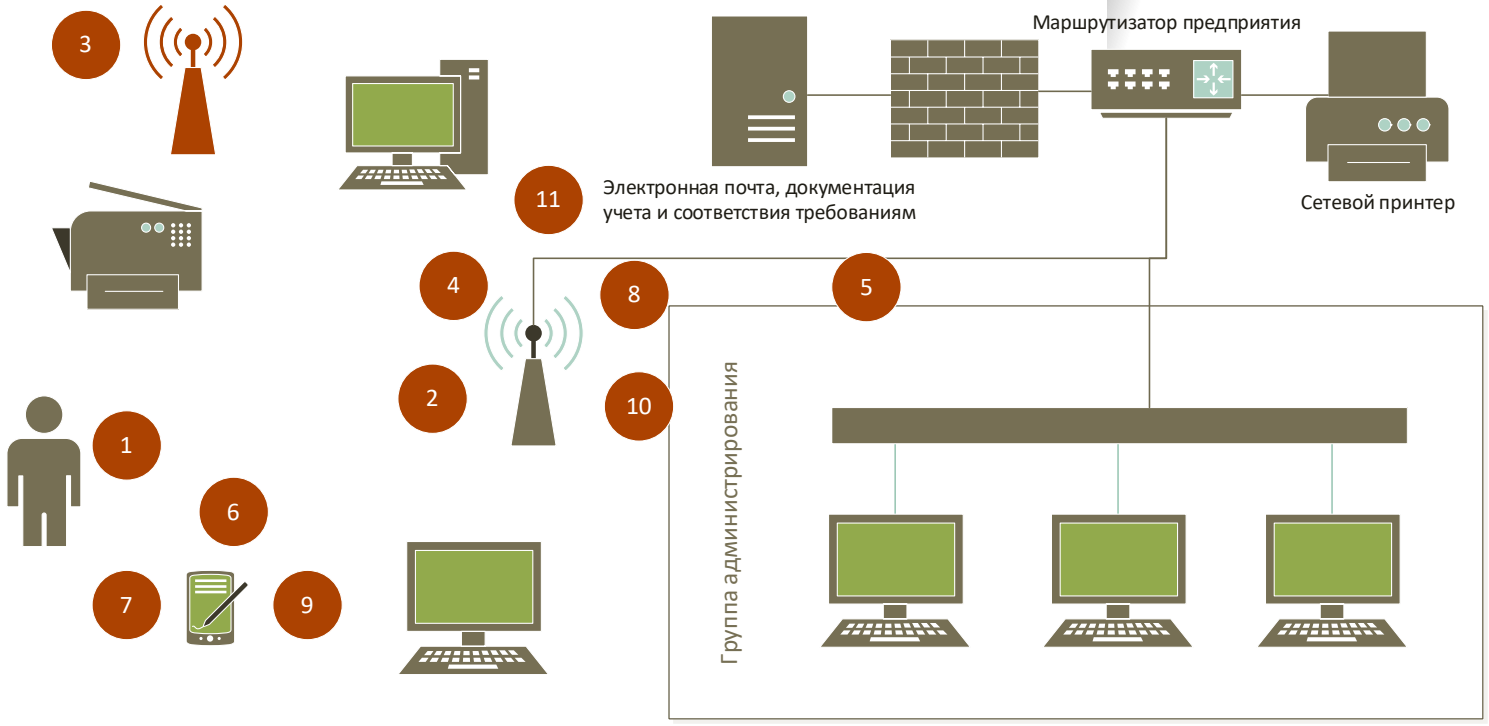
- Коллизия в Wi-Fi обходится очень дорого:
  - Обнаруживается по отсутствию подтверждения
  - Временные затраты: передача кадра, тайм-аут ожидания подтверждения

Решение проблемы скрытой станции



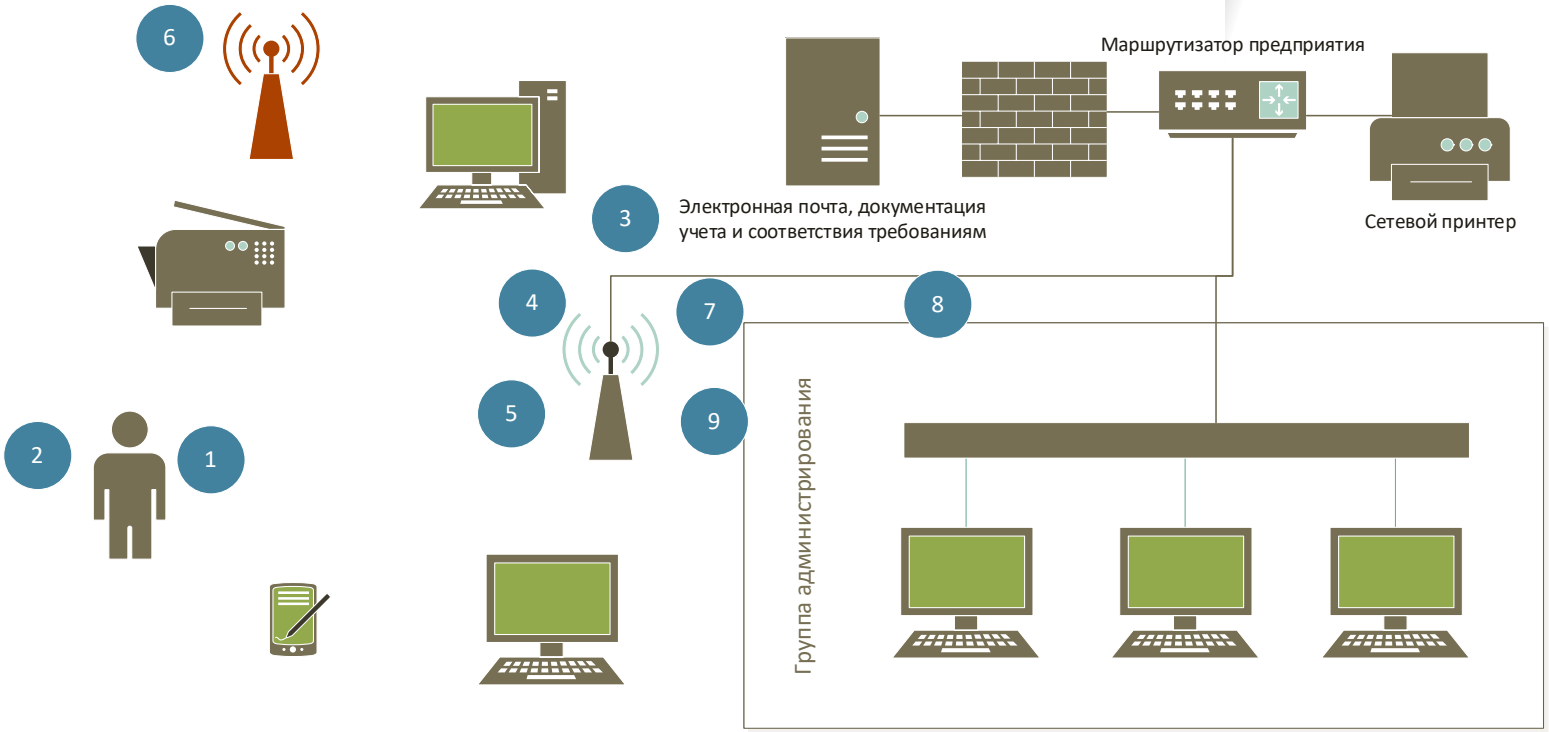
1. *Хост B* инициирует передачу данных с хостом B сообщением RTS и
2. *Хост A в* ответ передает управляющее сообщение CTS и это сообщение получает не только *хост B*, но и *C*, который находятся вне зоны действия передатчика *компьютера B*.
3. *Хост C* понимает, что сейчас *B,* сигнал от которого он не видит, будет передавать данные размером 1500 байт, поэтому он ждет когда передача закончиться.

Вопросы безопасности



1	Несанкционированный доступ	5	Неправильная маршрутизация	9	Незащищенная начальная загрузка
2	Анализ пакетов	6	Перехват IMSI	10	Взлом методов шифрования и ключей
3	Фальшивая точка доступа	7	Отслеживание оборудования пользователя	11	Доступ в нерабочее время
4	Ddos	8	Принудительная передача данных	12	Использование механизма WPS

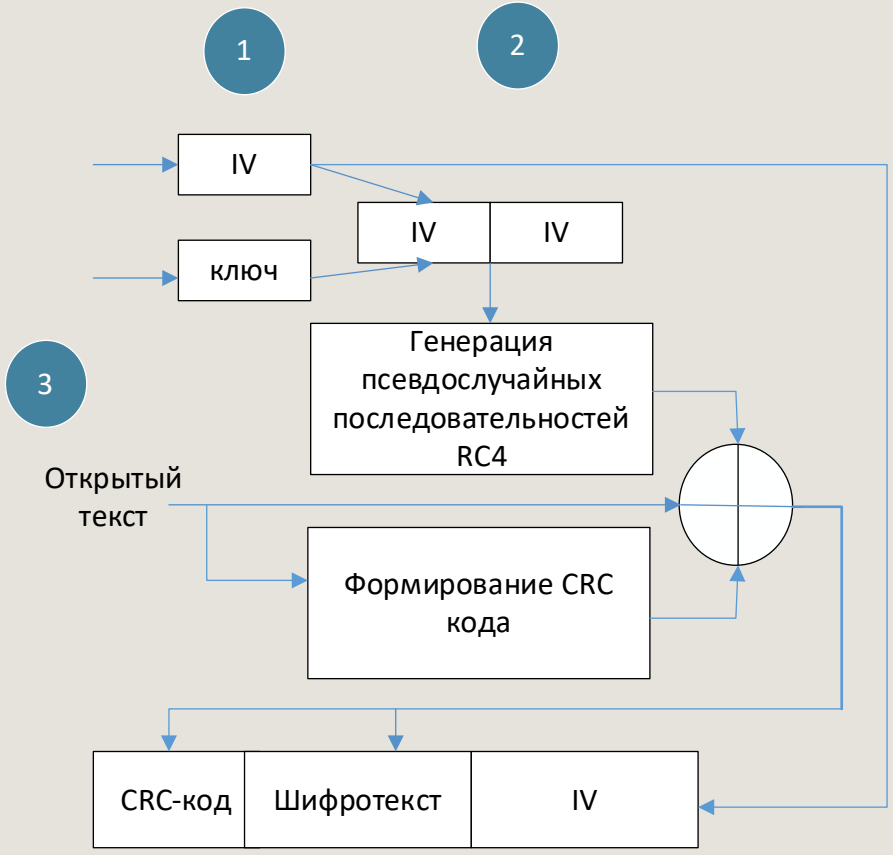
Механизмы обеспечения безопасности



1	Режим изоляции гостевого входа точки доступа	5	Безопасные методы аутнтификации	9	Обновление ПО
2	Запрет на использование гостевого доступа	6	Выявление несанкционированных точек	10	Основные механизмы и средства безопасности беспроводных сетей ориентированы, как правило, на защиту канального уровня. Защита на более высоких уровнях сетевой модели реализуется на базе типичных для проводных сетевых КС механизмах
3	Использование надежных механизмов шифрования	7	Управление доступом		
4	Сегментирование сети	8	Межсетевое экранирование		

WEP

Wired Equivalent Privacy (WEP) — алгоритм для обеспечения безопасности сетей Wi-Fi. Используется для обеспечения конфиденциальности и защиты передаваемых данных авторизированных пользователей беспроводной сети от прослушивания.



1

Каждый участник устанавливает у себя общий секретный ключ (в 802.11 предусмотрено наличие до четырех секретных ключей). Размер секретного ключа может быть установлен равным 40 или 104 битам

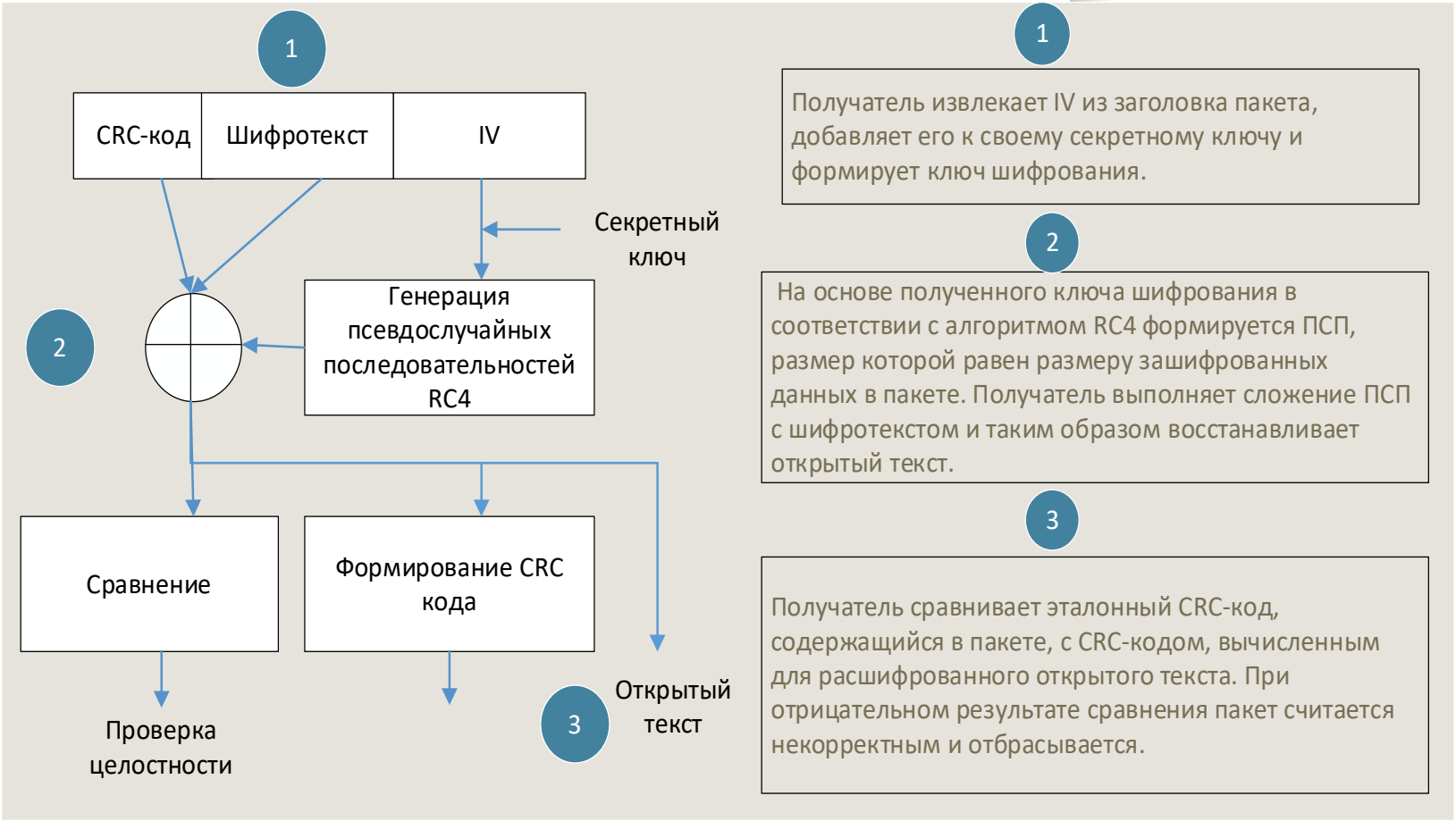
2

Вектор инициализации размером 24 бита, добавляется к секретному ключу со стороны младших байтов и формирует ключ шифрования данного пакета (размером 64 или 128 бит).

3

Использование алгоритма RC4 и полученного ключа шифрования позволяет зашифровать данные с использованием ПСП. Отправитель добавляет IV в соответствующее поле в заголовке пакета и устанавливает битовый флаг, сообщающий об использовании WEP. Пакет отправляется получателю.

WEP

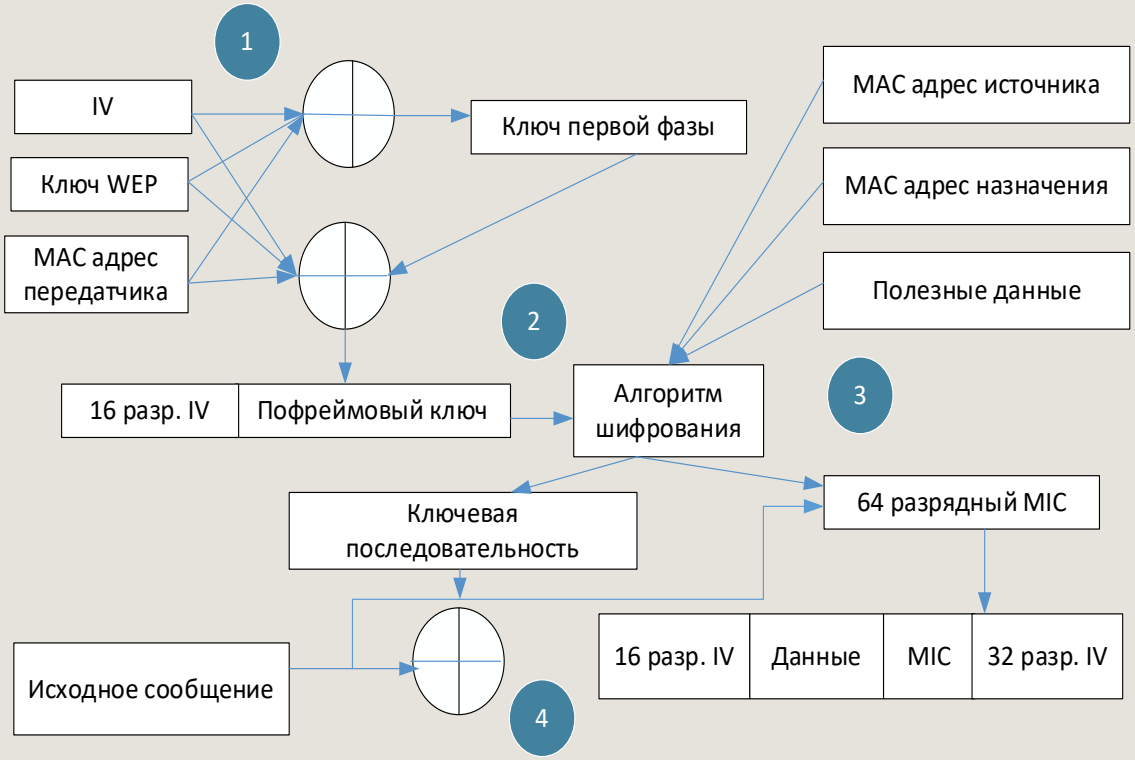


Аутентификация с использованием WEP подвержена атакам человек посередине. Атакующий перехватывает как нешифрованный, так зашифрованный трафик, и формирует ключевую последовательность на основе анализа вектора инициализации

WPA

- WPA (Wi-Fi Protected Access), WPA2 и WPA3 — программы сертификации устройств беспроводной связи, разработанные объединением Wi-Fi Alliance для защиты беспроводной Wi-Fi-сети. Основаны на стандарте IEEE 802.11i-2004.
- Преимущества:
- Обязательная аутентификация с использованием EAP.
- Усовершенствованная схема шифрования RC4
- Система централизованного управления безопасностью, возможность использования в действующих корпоративных политиках безопасности.

WPA



1. Механизм шифрования TKIP осуществляется следующим образом:
2. С помощью алгоритма пофреймового назначения ключей генерируется пофреймовый ключ.
3. Алгоритм MIC генерирует MIC для фрейма в целом.
4. Фрейм фрагментируется в соответствии с установками MAC относительно фрагментации.
5. Фрагменты фрейма шифруются с помощью пофреймового ключа.
6. Осуществляется передача зашифрованных фрагментов.

1

Пофреймовое изменение ключей шифрования. Помимо увеличения 24-разрядный вектор инициализации до 48-разрядного IV, MAC-адрес передатчика и WEP-ключ обрабатываются вместе с помощью двухступенчатой функции перемешивания.

2

Получение пофреймового ключа

3

Использование контроля целостности сообщения (MIC) устраняет проведение атак с использованием поддельных фреймов и манипуляции битами. Для этого MIC формируются уникальный ключ, отличающийся от ключа, используемого для шифрования фреймов данных, перемешивается с назначенным MAC-адресом и исходным MAC-адресом фрейма, а также со всей незашифрованной частью фрейма

Сравнение технологий

Технология	Статический WEP	Динамический WEP	WPA	WPA 2 (Enterprise)	WPA 3
Год принятия	1999	1999	2003	2004	2018
Аутентификация	Общий ключ	EAP	EAP или общий ключ	EAP или общий ключ	Технология SEA
Целостность	32-bit Integrity Check Value (ICV)	32-bit ICV	64-bit Message Integrity Code (MIC)	CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code — CCM) Part of AES	SHA, BIP-GMAC-256
Шифрование	Статический ключ 40 бит	Сессионный ключ	129	CCMP (AES) 40 бит	CCMP (AES) 128 бит, 198 бит

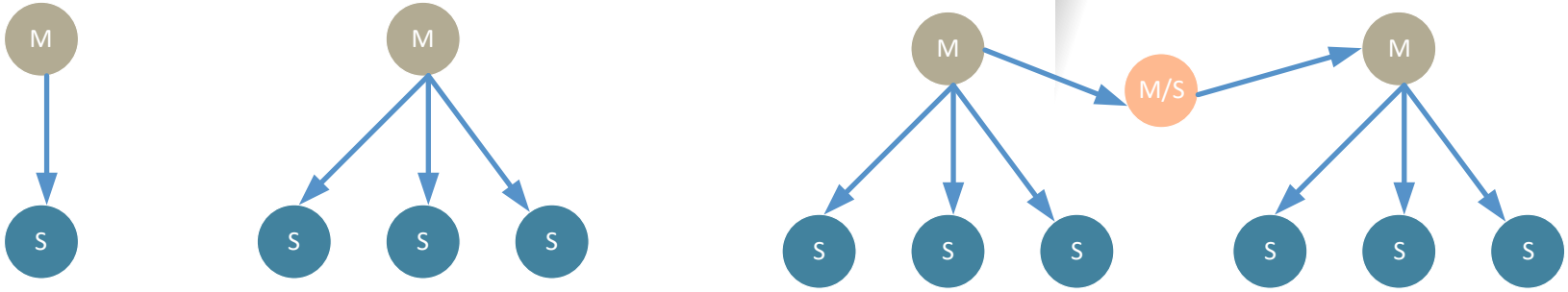
Сравнение технологий

Технология	Статический WEP	Динамический WEP	WPA	WPA 2 (Enterprise)	WPA 3
Распределение ключей	Однократное, вручную	Сегмент Pair-wise Master Key (PMK)	Производное от PMK	Производное от PMK	Производное от PMK
Вектор инициализации	Текст, 24 бита	Текст, 24 бита	Расширенный вектор, 65 бит	48-бит номер пакета (PN)	48-битный вектор инициализации
Алгоритм шифрования	RC4	RC4	RC4	AES	AES
Длина ключа, бит	64/128	64/128	128	до 256	до 256
Требуемая инфраструктура	Нет	RADIUS	RADIUS	RADIUS	RADIUS

Bluetooth

- Bluetooth — производственная спецификация беспроводных персональных сетей WPAN.
- Bluetooth обеспечивает обмен информацией между оконечными пользовательскими устройствами, такими как персональные компьютеры, мобильные телефоны, принтеры, цифровые фотоаппараты, устройства ввода, наушники, гарнитуры на радиочастоте для ближней связи. Протокол Bluetooth относится к физическому уровню модели OSI и в настоящее время определяется спецификацией IEEE 802.15.1.

Топология



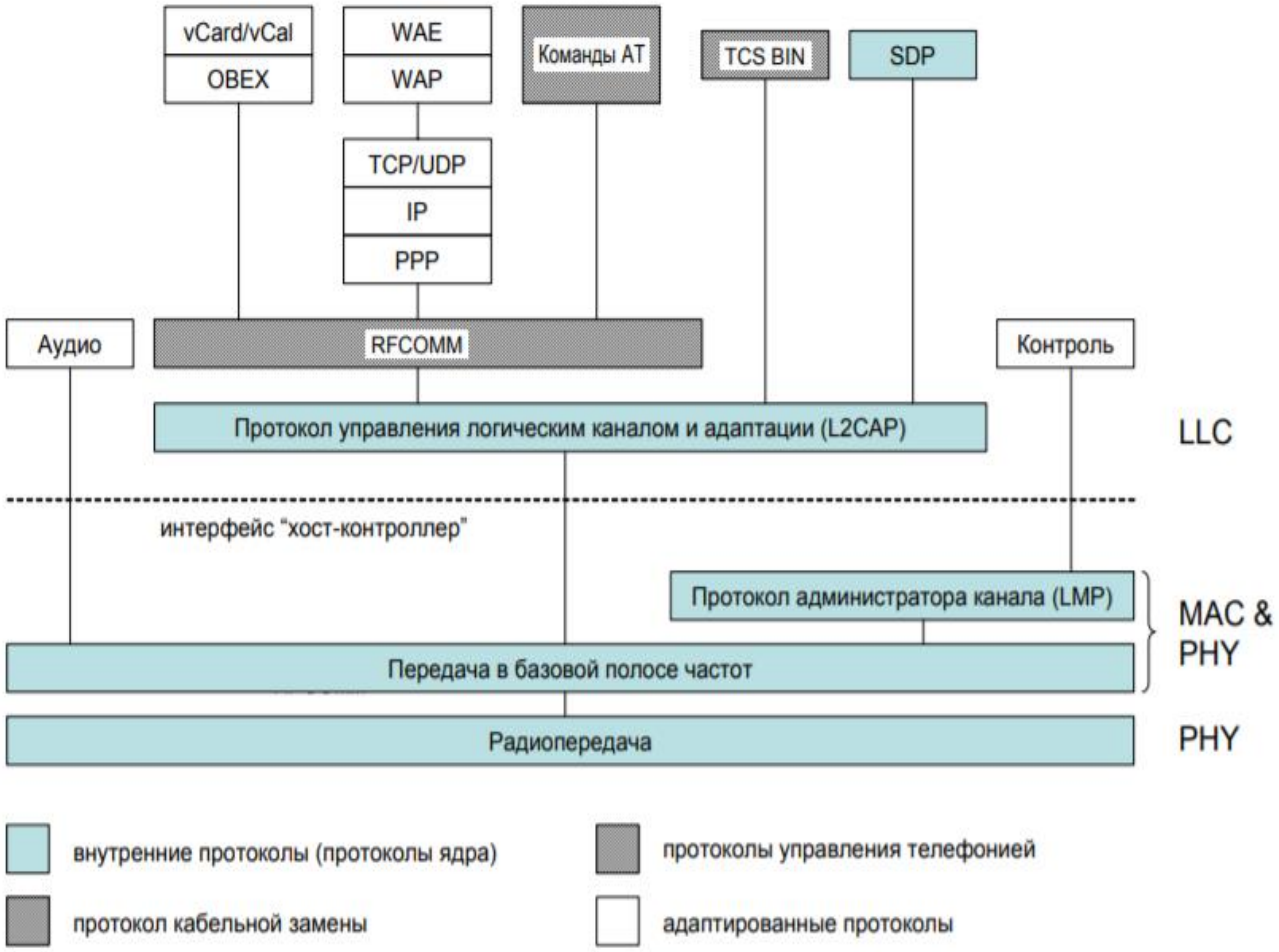
пикосеть типа точка-точка (с одним ведомым устройством)

пикосеть типа звезда (до 7 ведомых устройств)

рассеянная сеть

- **Пикосеть:**
- •в одной пикосети существует только одно ведущее устройство, все остальные – подчинённые;
- •максимальное количество устройств одной пикосети, одновременно участвующих в передаче информации, –не более 8
- •в каждый момент времени обмен данными может идти только между двумя устройствами в одном направлении
- **Рассеянная сеть:**
- •образуется путём перекрытия отдельных пикосетей
- •каждое устройство одной пикосети может входить в другую пикосеть как в качестве подчинённого, так и в качестве ведущего

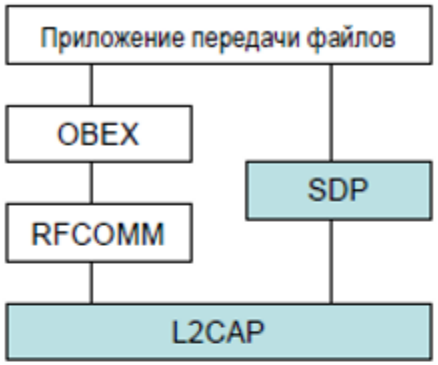
Стек протоколов Bluetooth



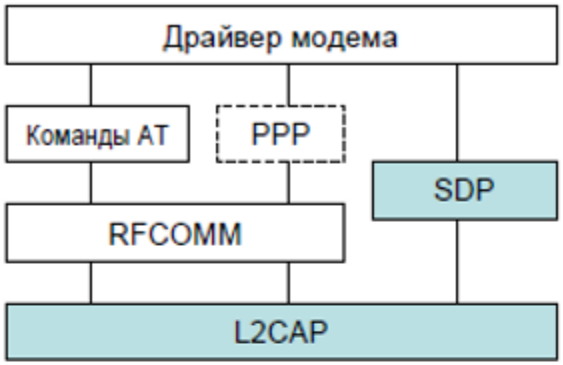
Профили

- Hands-Free Profile (HFP) — используется для соединения беспроводной гарнитуры и телефона, передаёт монозвук в одном канале.
- Human Interface Device Profile (HID) — обеспечивает поддержку устройств с HID (Human Interface Device), таких как мыши, джойстики, клавиатуры и пр. Использует медленный канал, работает на пониженной мощности.

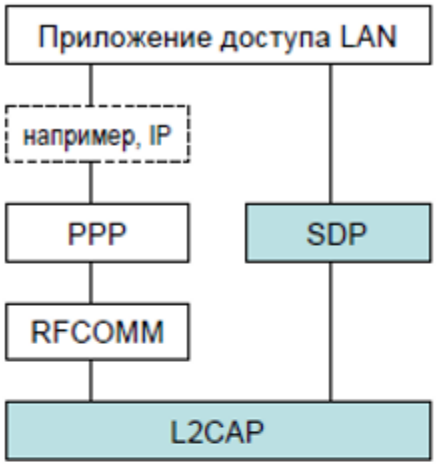
Модели использования



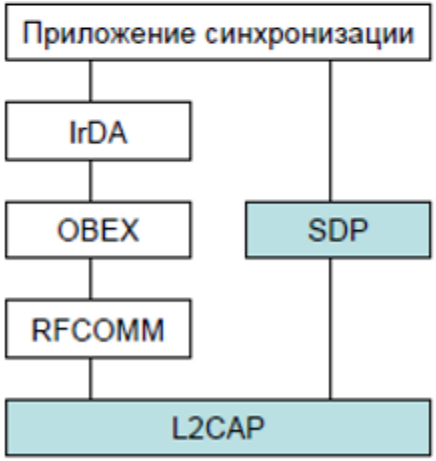
Передача файлов



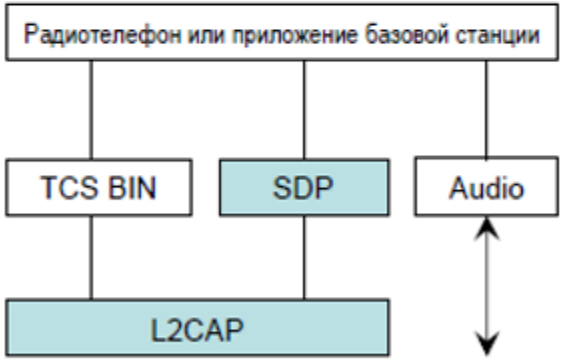
Мост Internet



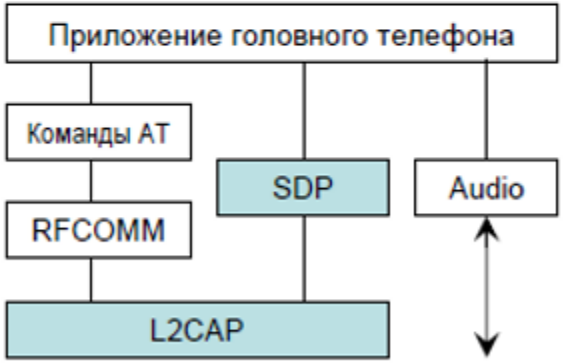
Доступ к локальной сети



Синхронизация

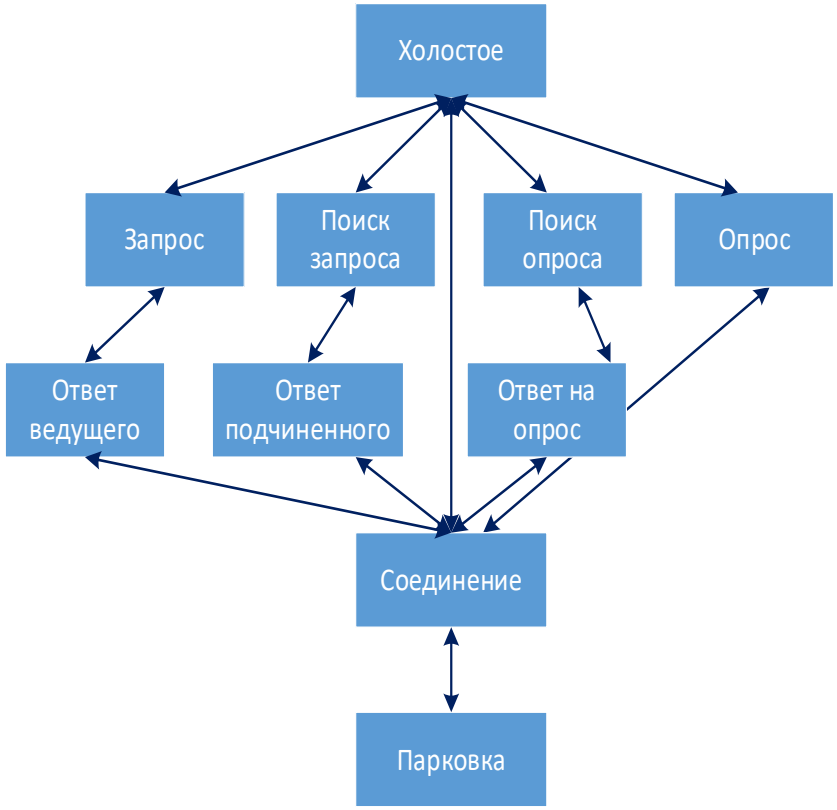


Телефон "три в одном"



Головной телефон

Механизм соединения. Состояния Bluetooth



Основные состояния:

•*холостое состояние* – низкое энергопотребление, работают только часы устройства

•*состояние соединения* – устройство подключено к пикосети

•*состояние парковки* – состояние подчинённого устройства, от которого не требуется участия в работе пикосети, но которое должно оставаться её частью

Промежуточные состояния:

•*опрос* – определение устройством наличия других устройств в пределах его досягаемости

•*поиск опроса* – ожидание устройством опроса

•*ответ на опрос* – устройство, получившее опрос, отвечает на него

•*запрос* – посылается одним устройством другому для установления с ним соединения (запрашивающее устройство становится ведущим, запрашиваемое – подчинённым)

•*поиск запроса* – устройство ожидает запрос

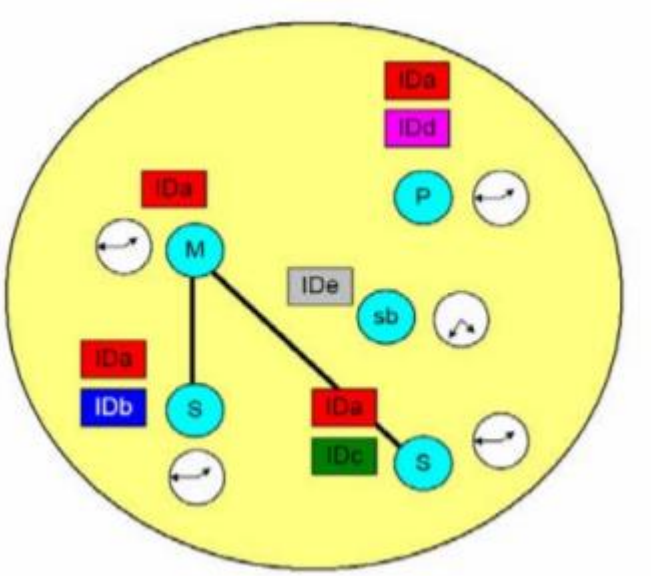
•*ответ подчинённого устройства* – подчинённое устройство отвечает на запрос ведущего

•*ответ ведущего устройства* – ведущее устройство отвечает подчинённому после получения от него ответа на запрос

Механизм соединения [6]

Все подчинённые устройства пикосети имеют:

- одинаковую последовательность перестройки частоты, определяемую адресом IDa ведущего устройства M (FDMA)
- временную синхронизацию с ведущим устройством (TDD, TDMA)
- код доступа к каналу, определяемый адресом ведущего устройства IDa (CDMA)



последовательность перестройки частоты + значение часов ведущего устройства + код доступа к каналу = физический канал пикосети

sb - холостое состояние (standby)

P - парковка

S - подчинённое устройство

Атаки

- *Атака человек по середине*
- Атака BIAS позволяет устанавливать с атакуемым устройством безопасное Bluetooth-соединение в обход механизма аутентификации.
- *Атаки на ключи*
- Компонент CTKD используется для согласования и настройки ключей аутентификации при сопряжении двух устройств с поддержкой Bluetooth. Он работает путем настройки двух разных наборов ключей аутентификации для стандартов Bluetooth Low Energy (BLE) и Basic Rate/Enhanced Data Rate (BR/EDR). Роль CTKD состоит в том, чтобы подготовить ключи и позволить сопряженным устройствам решить, какую версию стандарта Bluetooth они хотят использовать.
- *Атаки на алгоритм шифрования*
- Спецификации BR/EDR (Basic Rate/Enhanced Data Rate) позволяют взломать зашифрованные сообщения по Bluetooth. Для этого злоумышленнику нужно просто зайти в зону покрытия устройств. Уязвимость содержалась в возможности Bluetooth-устройств самостоятельно назначать длину ключа для шифрования информации.

Атаки

- *Атака человек по середине*
- Атака BIAS позволяет устанавливать с атакуемым устройством безопасное Bluetooth-соединение в обход механизма аутентификации.
- *Атаки на ключи*
- Компонент CTKD используется для согласования и настройки ключей аутентификации при сопряжении двух устройств с поддержкой Bluetooth. Он работает путем настройки двух разных наборов ключей аутентификации для стандартов Bluetooth Low Energy (BLE) и Basic Rate/Enhanced Data Rate (BR/EDR). Роль CTKD состоит в том, чтобы подготовить ключи и позволить сопряженным устройствам решить, какую версию стандарта Bluetooth они хотят использовать.
- *Атаки на алгоритм шифрования*
- Спецификации BR/EDR (Basic Rate/Enhanced Data Rate) позволяют взломать зашифрованные сообщения по Bluetooth. Для этого злоумышленнику нужно просто зайти в зону покрытия устройств. Уязвимость содержалась в возможности Bluetooth-устройств самостоятельно назначать длину ключа для шифрования информации.

Обеспечение безопасности [8]

Характеристика	Bluetooth BR/EDR	
	До версии 4.1	Версия 4.1 и новее
Физические радио каналы	79 каналов с шагом в 1 МГц	
Обнаружение / соединение	Опрос (inquiry) / разбиение (paging)	
Конфиденциальность адреса устройства	Отсутствует	
Максимальная скорость данных	1-3 Мбит/с	
Алгоритм сопряжения	До версии 2.1: E21/E22/SAFER+ Версия 2.1-4.0: Elliptic Curve P-192, HMAC-SHA-256	P-256 Elliptic Curve, HMAC-SHA-256
Алгоритм аутентификации устройства	E1/SAFER	HMAC-SHA-256
Алгоритм шифрования	E0/SAFER+	AES-CCM
Стандартный радиус действия	30 метров	
Максимальная выходная мощность	100 мВ (20 дБ)	

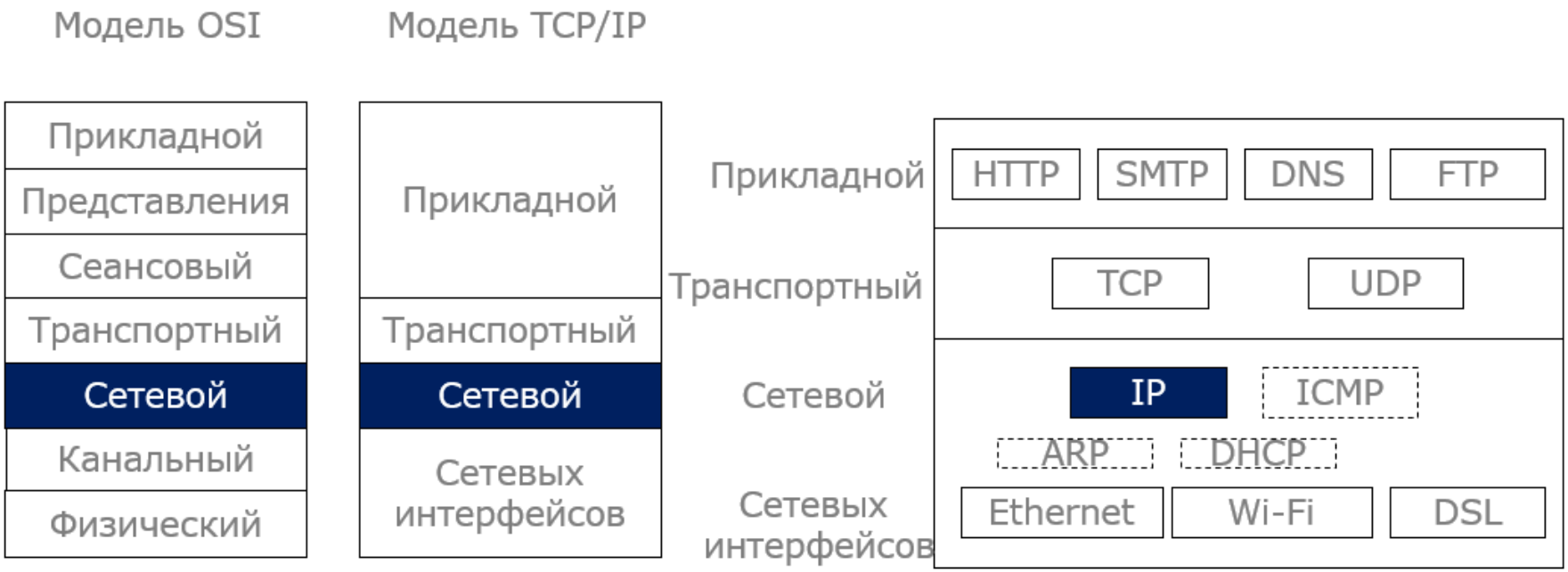
Место в моделях OSI и TCP/IP

Модель OSI была разработана в конце 1970-х годов для поддержания разнообразных методов компьютерных сетей, которые в это время конкурировали за применение в крупных национальных сетевых взаимодействиях во Франции, Великобритании и США. В 1980-х годах она стала рабочим продуктом группы взаимодействия открытых систем Международной организации по стандартизации (ISO).

Модель не смогла дать полное описание сети и не получила поддержку архитекторов на заре Интернета, который впоследствии нашел отражение в менее предписывающем TCP/IP, в основном под руководством Инженерного совета Интернета (IETF).

- Модель OSI, которая была определена в серии стандартов ISO/IEC 7498, состоит из следующих частей:
- ISO/IEC 7498-1 — базовая модель;
- ISO/IEC 7498-2 — архитектура безопасности;
- ISO/IEC 7498-3 — наименования и адресация;
- ISO/IEC 7498-4 — система менеджмента.

Место в моделях OSI и TCP/IP



- Передача данных
  - без гарантии доставки
  - без сохранения порядка следования сообщений
- Протокол IP использует передачу данных без установки соединения

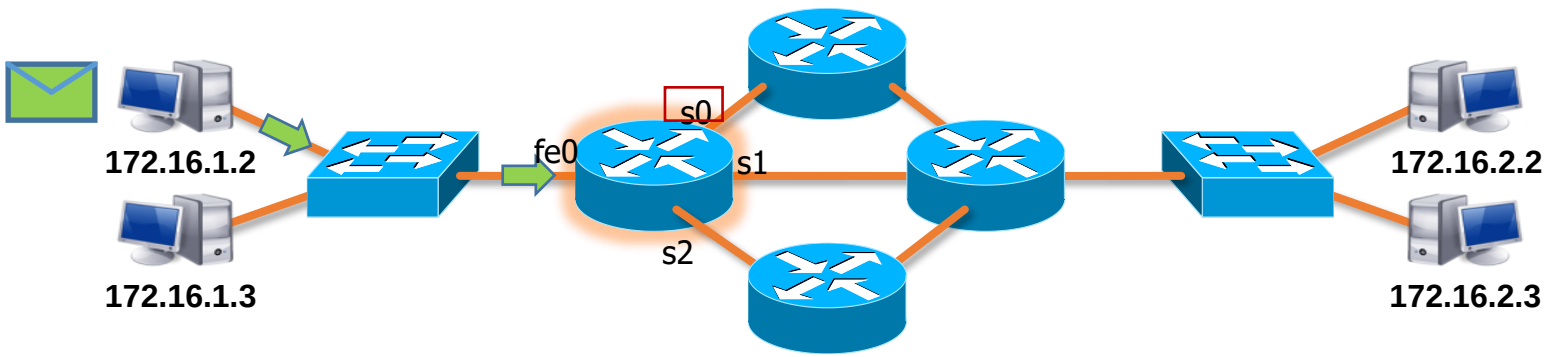
Задачи IP

- Объединение сетей
- Маршрутизация
- Качество обслуживания

Коммутация каналов/пакетов

- Коммутация - экономичное продвижение пакетов на основании локального адреса Обеспечивается продвижение пакета между «соседями»:
  - одной локальной сети (не разделенной маршрутизаторами)
  - по каналу «точка-точка» глобальной сети

1. Таблицы коммутации небольшого размера – учитываются только адреса активно взаимодействующих «соседей»
2. Пакет при продвижении не модифицируется – экономия действий, стоимость скорости



Формат заголовка IP-пакета

4 бита Номер версии	4 бита Длина заголовка	8 бит Тип сервиса	16 бит Общая длина	
16 бит Идентификатор пакета			3 бита Флаги	13 бит Смещение фрагмента
8 бит Время жизни		8 бит Тип протокола	16 бит Контрольная сумма	
32 бита IP-адрес отправителя				
32 бита IP-адрес получателя				
Опции и выравнивание (не обязательно)				

Тип протокола (код протокола, данные которого передаются):

TCP – 6
UDP – 17
ICMP – 1

Заголовок IP-пакета может включать дополнительные поля:

- Записать маршрут
- Маршрут отправителя
  - Жёсткая маршрутизация
  - Свободная маршрутизация
- Временные метки

Общая длина – длина пакета, включая заголовок и данные (измеряется в байтах, максимальное значение – 65535 байт, выбирается с учетом размера кадра канального уровня 1500 байт для Ethernet)

Время жизни (TTL, Time To Live) – максимальное время, в течение которого пакет может перемещаться по сети (введено для предотвращения «бесконечного» продвижения пакетов, секунды, прохождение через маршрутизатор (hop)
Предназначено для реализации функции мультиплексирования/ демультиплексирования

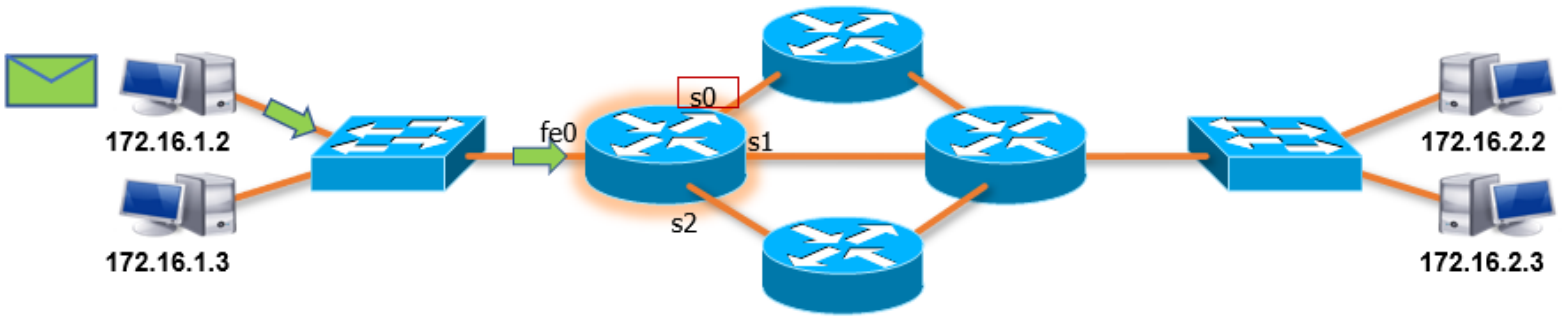
Заполнение:

- Опции могут иметь разный размер
- Длина заголовка IP-пакета должна быть кратна 32 битам
- Для выравнивания до 32 бит поле опций дополняется нулями

Протокол IP. Безопасность

4 бита Номер версии	4 бита Длина заголовка	8 бит Тип сервиса	16 бит Общая длина	
16 бит Идентификатор пакета			3 бита Флаги	13 бит Смещение фрагмента
8 бит Время жизни		8 бит Тип протокола	16 бит Контрольная сумма	
32 бита IP-адрес отправителя				
32 бита IP-адрес получателя				
Опции и выравнивание (не обязательно)				

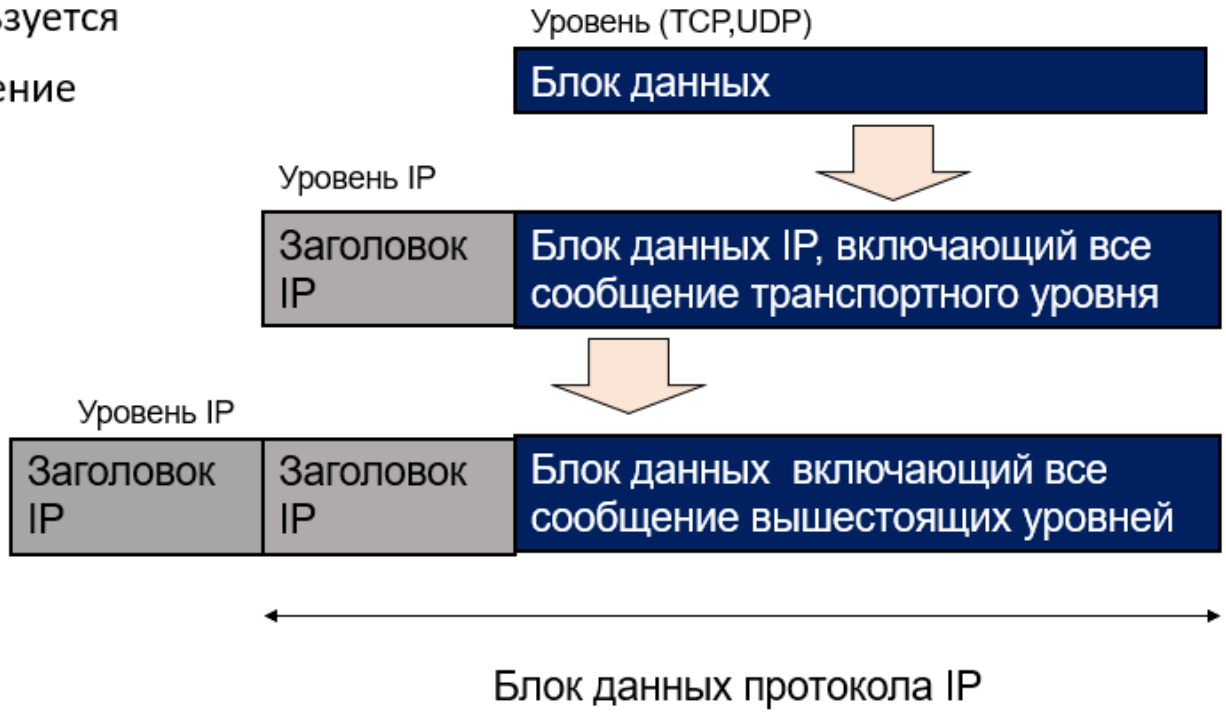
- Идентификатор пакета- неправильное указание идентификатора создает нарушение при сборке пакета
- Флаги- установка флага на запрет фрагментации – нарушения безопасности при передаче между сетями
- Смещение фрагмента- неправильное указание смещения создает нарушение при сборке пакета
- Контрольная сумма- повторная передача и уменьшение пропускной способности сети
- IP адреса- подмена IP адреса



Протокол IP. Туннелирование

Туннелирование используется при необходимости

- Сокрытия в сети IP адресов.
- Данный механизм используется
- В том числе и для построение
- VPN



Инкапсуляция протоколов

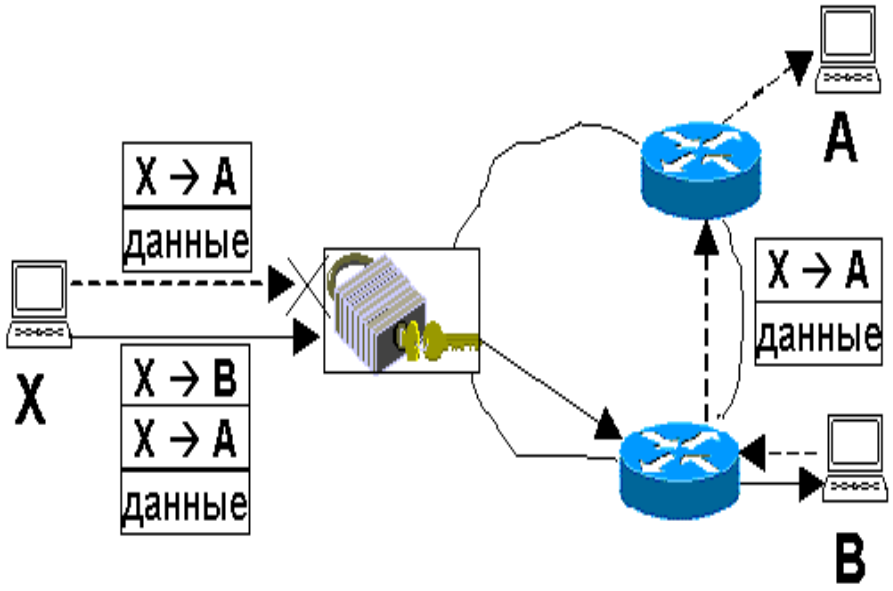
Правила фильтрации запрещают отправку дейтограмм узлу А узлом Х, но разрешают узлу В. Для осуществления атаки злоумышленник:

формирует дейтограмму, заголовок которой заполняет стандартным способом.

Данная дейтограмма инкапсулируется в новую IP-дейтограмму, при этом в поле протокола указывается, инкапсуляция и адрес промежуточного узла В.

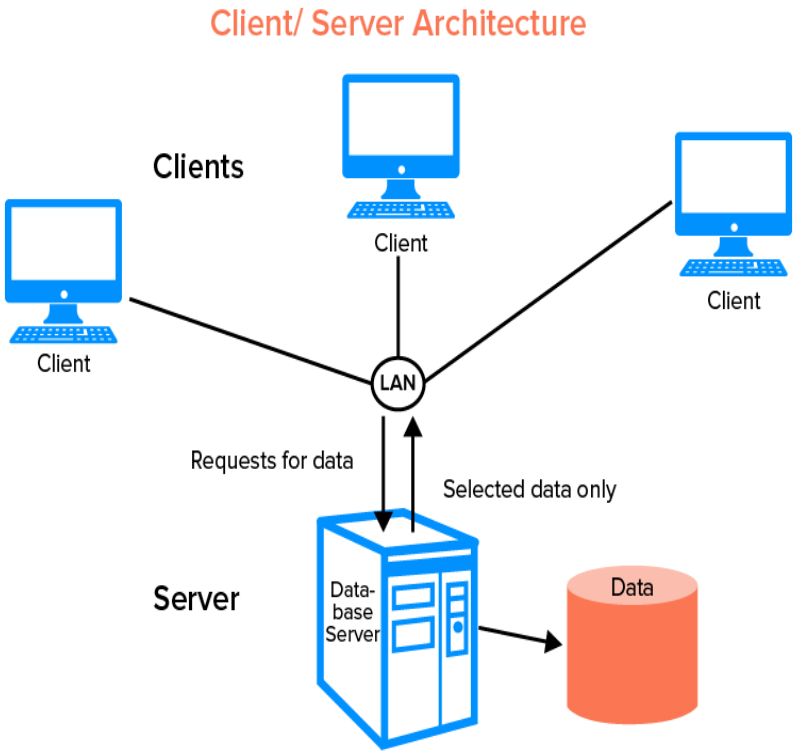
Получив данную дейтограмму узел В анализирует первый заголовок видит, что дейтограмма адресована не узлу А и отправляет ее по назначению, снабдив новым заголовком

В данном случае фильтрующий узел видит, что дейтограмма пришла с разрешенного узла и пропускает ее.

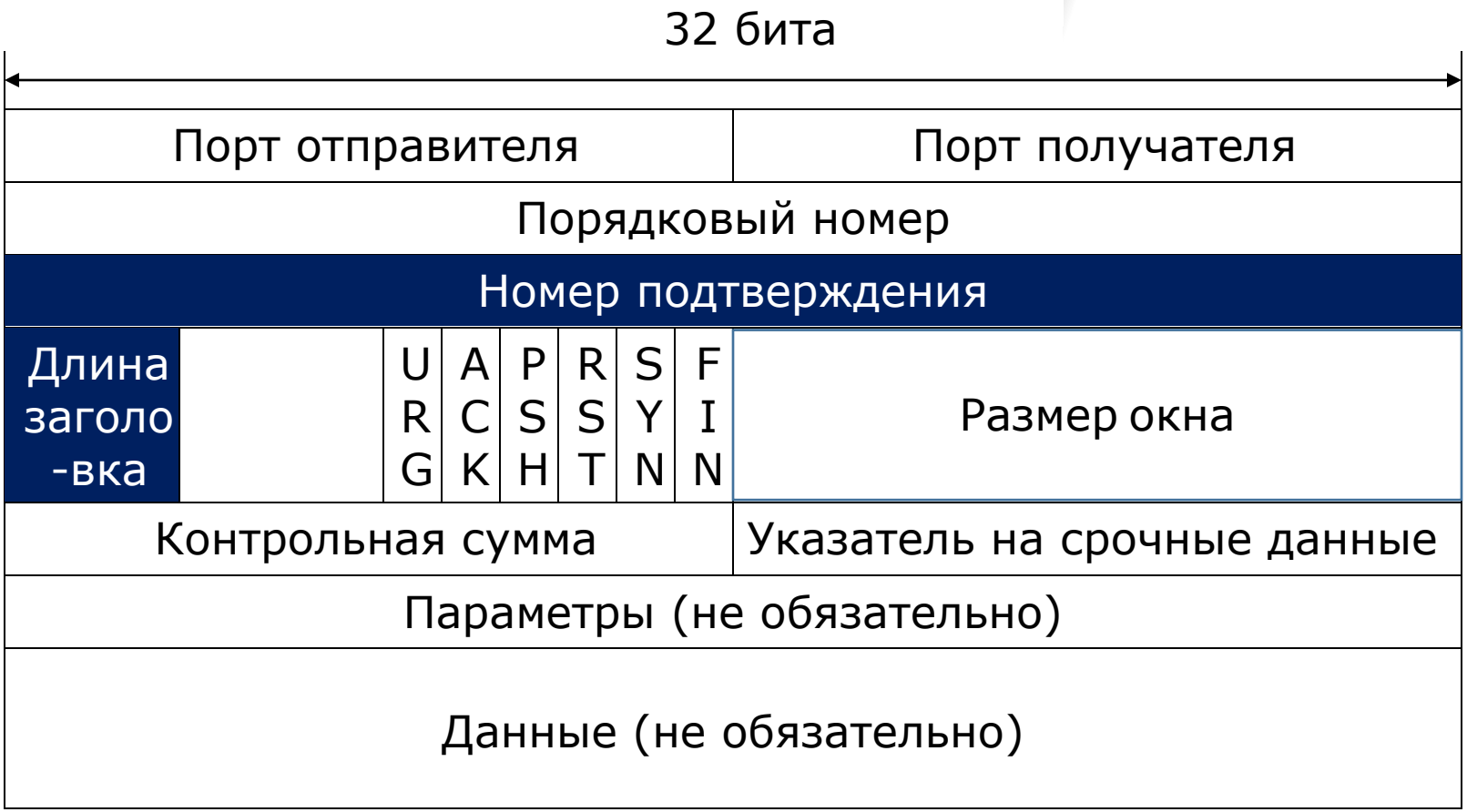


Клиент- серверное соединение

- Передача данных возможна, только если установлено соединение клиент-сервер.
- Сервер – работает (слушает) на известном IP-адресе и пассивно ждет запросов на соединение
- Клиент – активно устанавливает соединение с сервером на заданном IP + порт.
- При получении запроса от клиента создается копия сокета.
- Соединение устанавливается с копией, оригинальный сокет продолжает ждать запросы от других клиентов
- Такой сокет не может принимать и передавать данные.



Безопасность TCP. Заголовок TCP



Гарантия доставки

- Возможные проблемы при доставке:
  - Потеря сегментов
  - Изменение порядка доставки сегментов
  - Повторная доставка сегментов
- Сервис TCP:
  - Гарантия доставки
  - Гарантия сохранения порядка следования сообщений
- Механизмы реализации:
  - Нумерация сообщений
  - Подтверждение получения сообщения
  - Повторная отправка при отсутствии подтверждения

Установка соединения TCP

- Соединение – договоренность между отправителем и получателем о передаче данных
- Соединение задает:
  - Начальные номера для нумерации данных отправителя и получателя
  - Параметры передачи: максимальный размер сегмента и т.п.
  - Объем данных, которые готов принять получатель
- Соединение в TCP дуплексное
  - Данные могут передаваться в обе стороны
  - Подтверждение получения и данные в одном сегменте.

Установка соединения TCP

- TCP использует схему «Трехкратного рукопожатия»
- Флаг SYN – признак установки соединения
  - SYN = 1, ACK = 0 – запрос установки соединения (CONNECTION REQUEST)
  - SYN = 1, ACK = 1 – подтверждение установки соединения (CONNECTION ACCEPT)
  - SYN = 0, ACK = 1 – завершение установки соединения
- ACK – флаг подтверждения
  - Если флаг ACK установлен, значит поле «Номер подтверждения» содержит осмысленные данные

Трехкратное рукопожатие

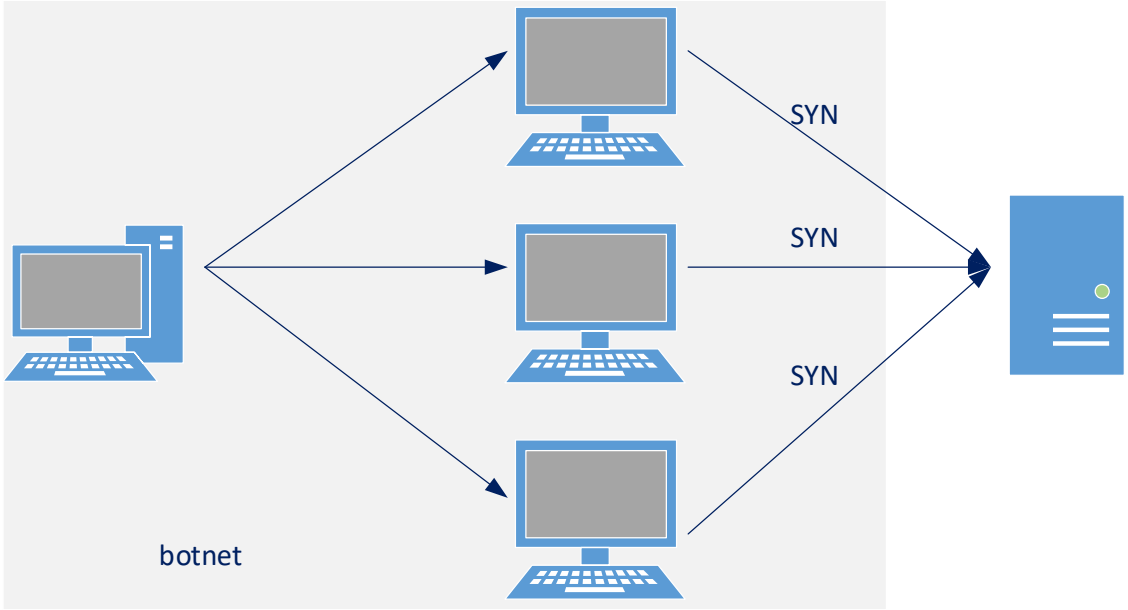
Разрыв соединения TCP

- Соединение в TCP дуплексное
  - Данные могут передаваться в обе стороны
- Схема разрыва соединения
  - Одновременное (обе стороны разорвали соединение)
  - Одностороннее (сторона прекращает передавать данные, но может принимать)
- Флаг FIN – одностороннее закрытие соединение
  - Соединение закрывается, когда обе стороны отправят сегмент с установленным флагом FIN и подтверждение
- Флаг RST – разрыв соединения из-за критической ситуации
  - Одновременный разрыв соединения обеими сторонами

Проблема безопасности TCP

1. Затопление с Ddos
2. Затопление при перегрузке

3. Сканирование с установлением флагаFIN, SYN, RST, PSH,URG



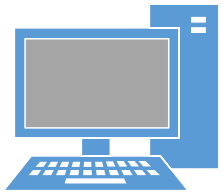
Безопасность TCP. Таймеры TCP

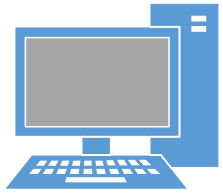
- Таймер повторной передачи:
  - Время ожидания подтверждения получения сегмента.
  - Если подтверждения нет, сегмент отправляется вновь.
- Таймер проверки активности:
  - Используется при длительном простое соединения.
  - Задает время, через которое должна выполниться проверка работоспособности соединения.
- Таймер закрытия соединения:
  - Задает ожидание, равное двойному времени жизни сегмента.
  - За это время все сегменты соединения должны уйти из сети.

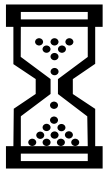
Безопасность TCP. Таймеры TCP

Отправитель

Получатель





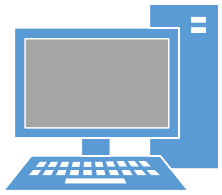


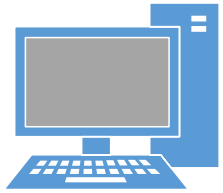
Буфер

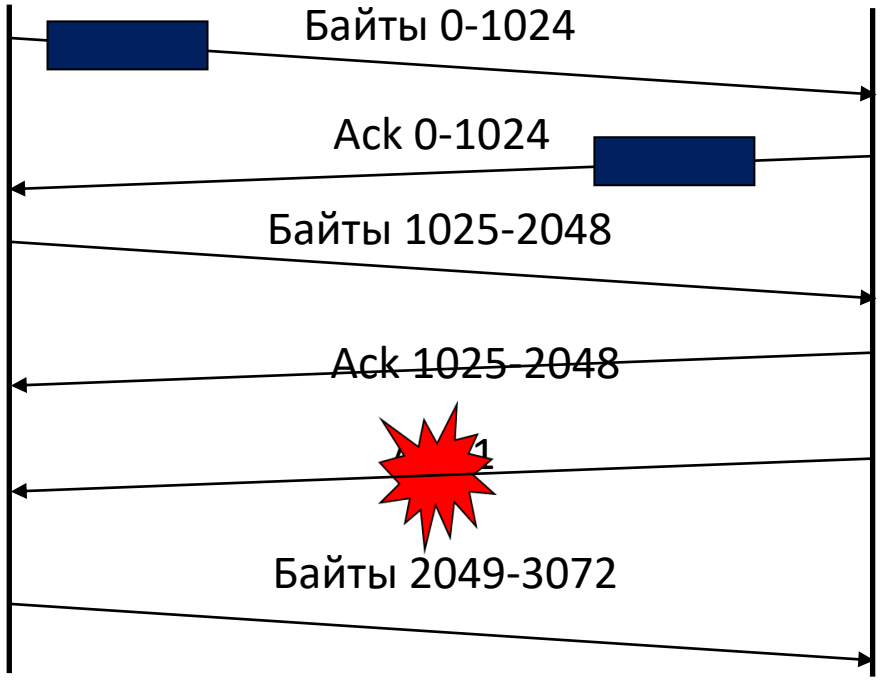
Безопасность TCP. Таймеры TCP

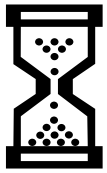
Отправитель

Получатель









Буфер

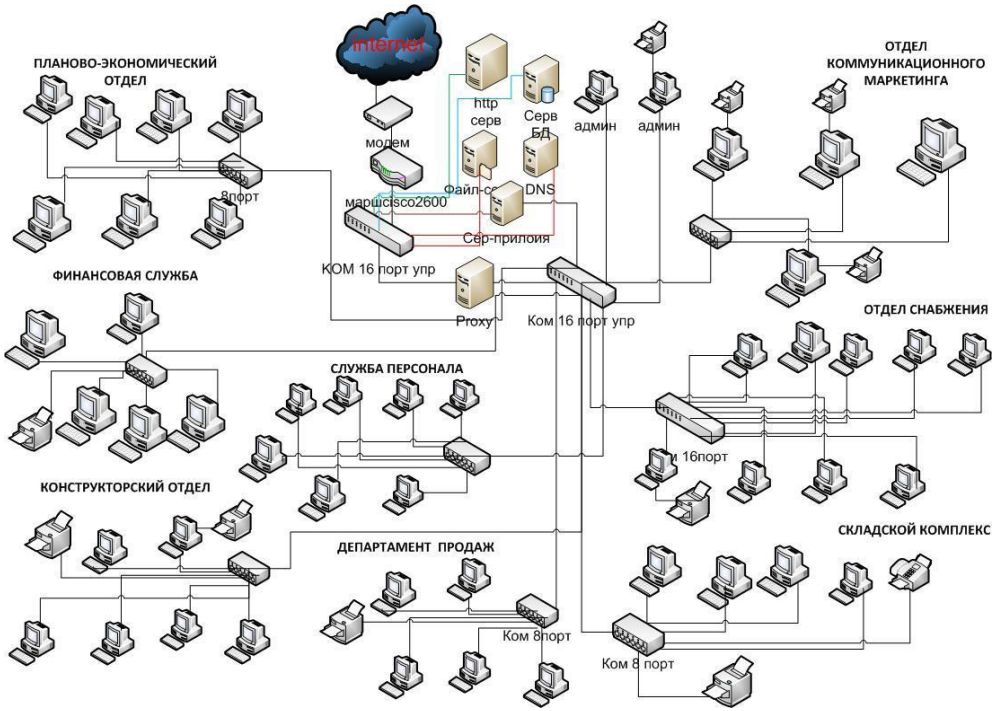
Безопасность TCP. Затопление сети

Сообщение передается не мгновенно:

- Время передачи короткое, но не нулевое

В среде может «находиться» некоторый объем данных:

- Скорость × Задержка
- Небольшой объем для локальных сетей
- Большой объем для широких территориально-протяженных каналов. Ожидание подтверждения приводит к снижению производительности

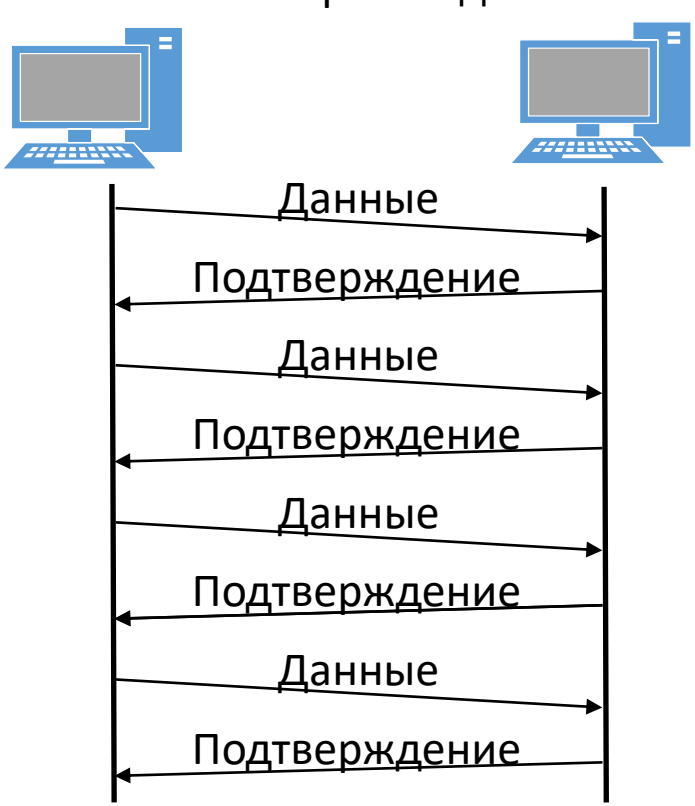


Подтверждение о доставке

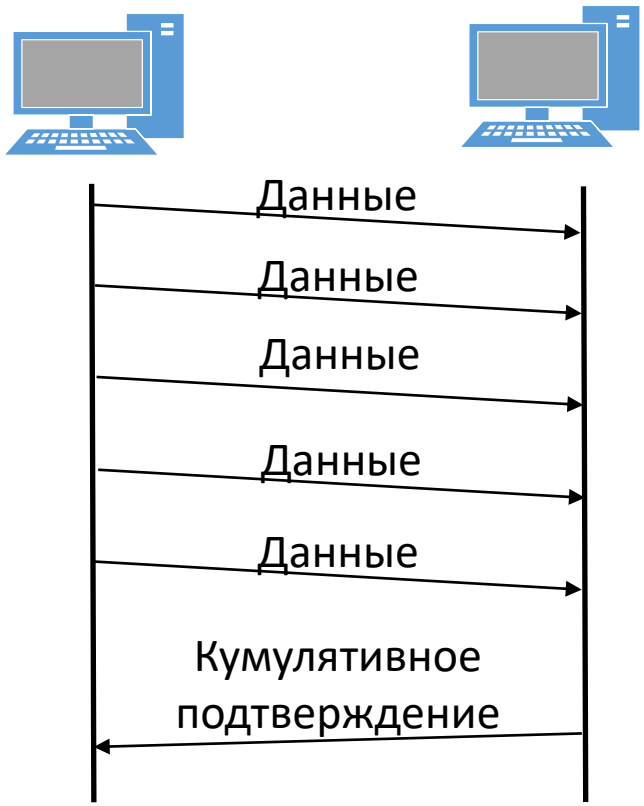
TCP должен обеспечивать

- Гарантированную доставку данных
- Эффективное использование канала связи

- TCP должен хорошо работать как на медленных каналах связи с ошибками, так и на быстрых надежных каналах



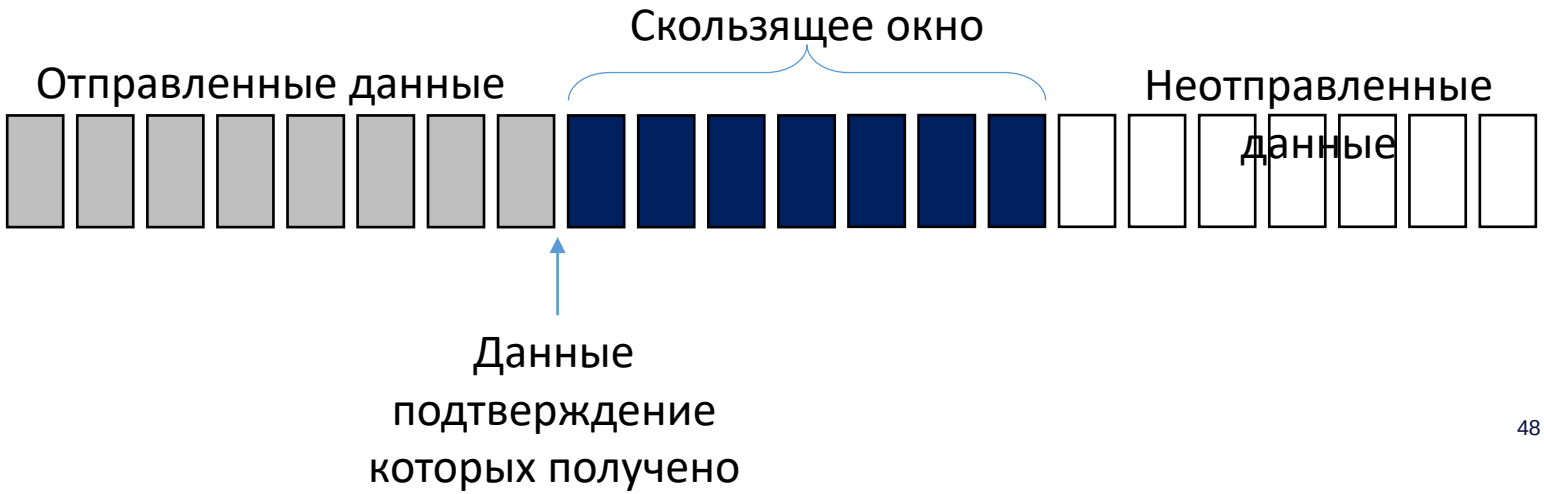
Остановка и ожидание



Скользящее окно

Подтверждение о доставке

- Разные варианты подтверждений:
  - **Остановка и ожидание** – передача данных после получения подтверждения каждого сообщения (Wi-Fi, канальный уровень)
  - **Скользящее окно** – передача заданного количества сообщений без ожидания подтверждения (TCP, транспортный уровень)
- Размер окна – количество байтов данных, которые могут быть переданы без получения подтверждения
- Кумулятивное подтверждение – подтверждение приема указанного байта данных и всех предыдущих



Безопасность скользящего окна

- Атака на размер окна
- Атака на срочность данных

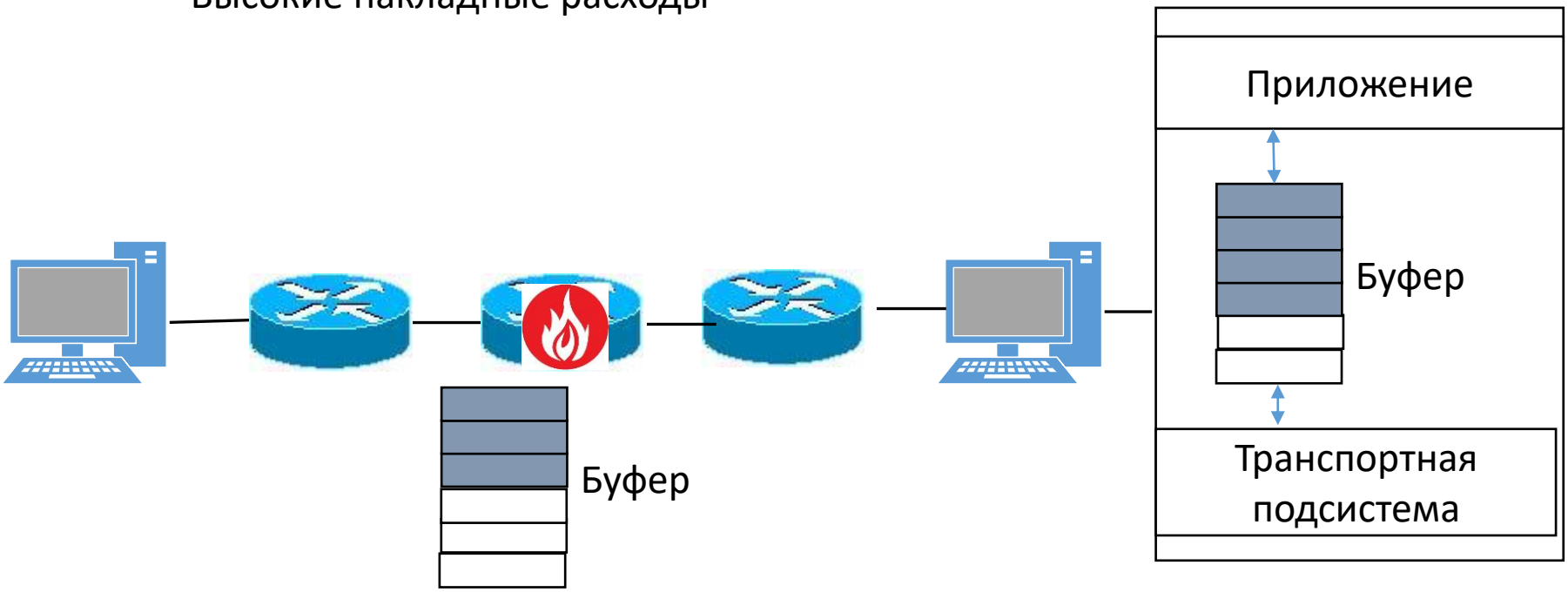
- Приложение может быть готово принять данные, но сеть перегружена
  - Отправляется большая порция данных
  - Многие сегменты будут отброшены сетью

- Перегрузка (congestion) – состояние, при котором в сеть поступает больше пакетов, чем она способна передать

Безопасность скользящего окна

Некоторые приложения читают и пишут данные маленькими порциями

- Эмуляторы терминала telnet или ssh
  - При нажатии каждой клавиши данные передаются на сервер – 1 байт данных
  - Для передачи 1 байта данных требуется передать IP-пакет длиной 41 байт (20 байт заголовок IP, 20 байт заголовок TCP, 1 байт данных)
  - Высокие накладные расходы

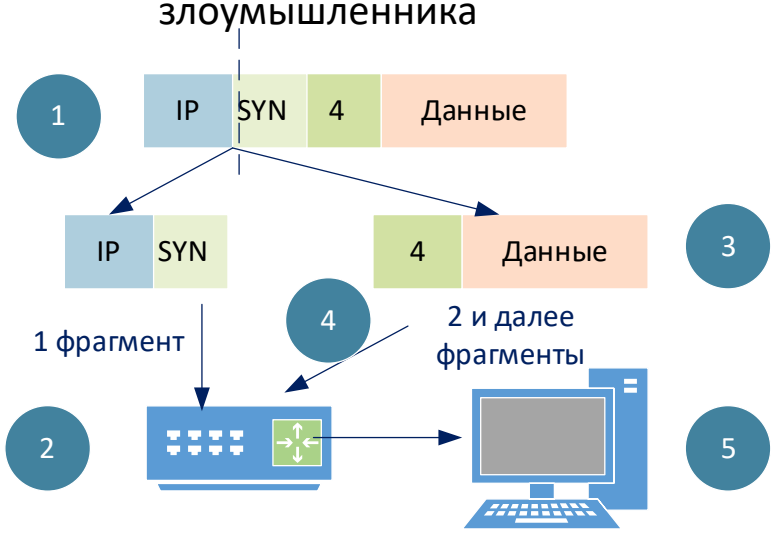


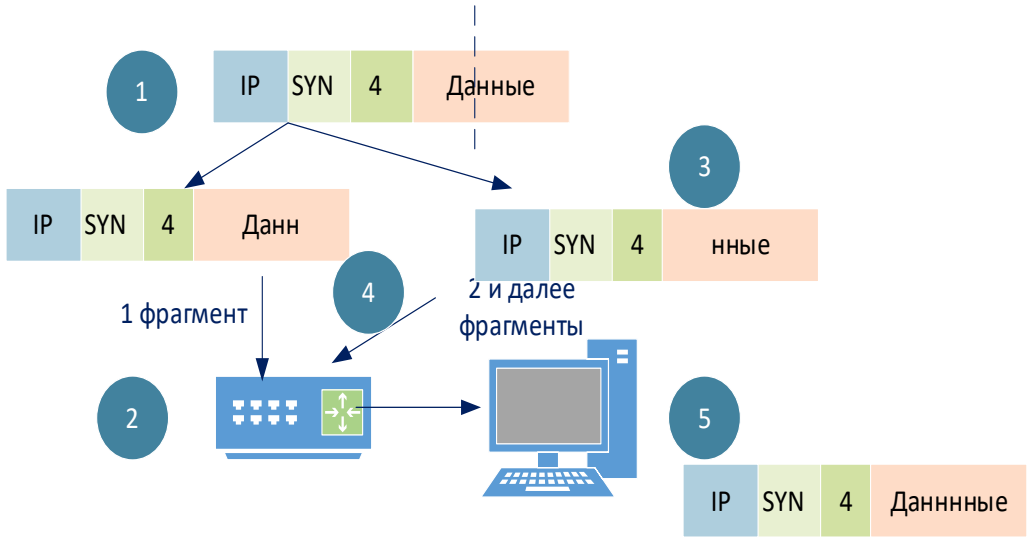
Безопасность скользящего окна

- Учет загрузки сети при формировании размера скользящего окна
  - Традиционный подход – фиксированный размер 8 сегментов TCP
  - Предложенный подход – динамический размер окна в зависимости от нагрузки на сеть
- Окно управления потоком:
  - Задается получателем (поле «Размер окна» в заголовке TCP)
  - Размер определяется возможностями приложения читать данные из буфера
- Окно перегрузки:
  - Задается отправителем
  - Размер определяется загрузкой сети
- Размер скользящего окна определяется меньшим из окон перегрузки или управления потоком
- Балансировка нагрузки
  - Сеть должна быть максимально загружена
  - Все хосты в сети получают примерно одинаковую часть от пропускной способности сети

Атака крошечными и накрадывающимися фрагментами

1. Злоумышленник X формирует датаграмму TCP-сегмента, состоящую из 2 фрагментов: в первом фрагменте датаграммы равной 8 октетам, находятся номера портов отправителя и получателя и поле SYN, однако значения флагов не попадает.
2. Маршрутизатор, используя правила фильтрации проверяет первый фрагмент датаграммы, на наличие флага SYN, так как он отсутствует, то дейтограмма пропускается в сеть.
3. X формирует 2-ой фрагмент дейтограммы, помещая оставшуюся часть заголовка TCP-сегмента, с установленным флагом SYN
4. Так как первый фрагмент дейтограммы проверен, остальные фрагменты маршрутизатором проверяться не будут, и дайтограмма будет пропущена в сеть.
5. Происходит сборка дейтограммы на узле получателе и соединение с компьютером злоумышленника





Архитектура HTTP

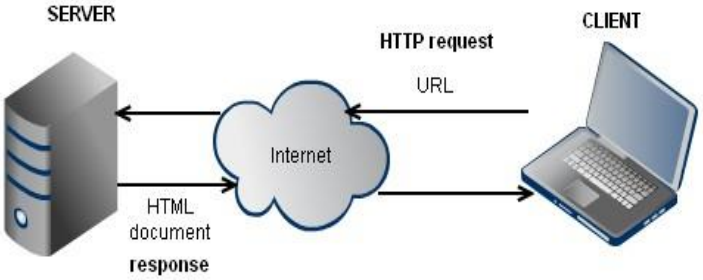
Анализ введенного URL и извлечение имени хоста

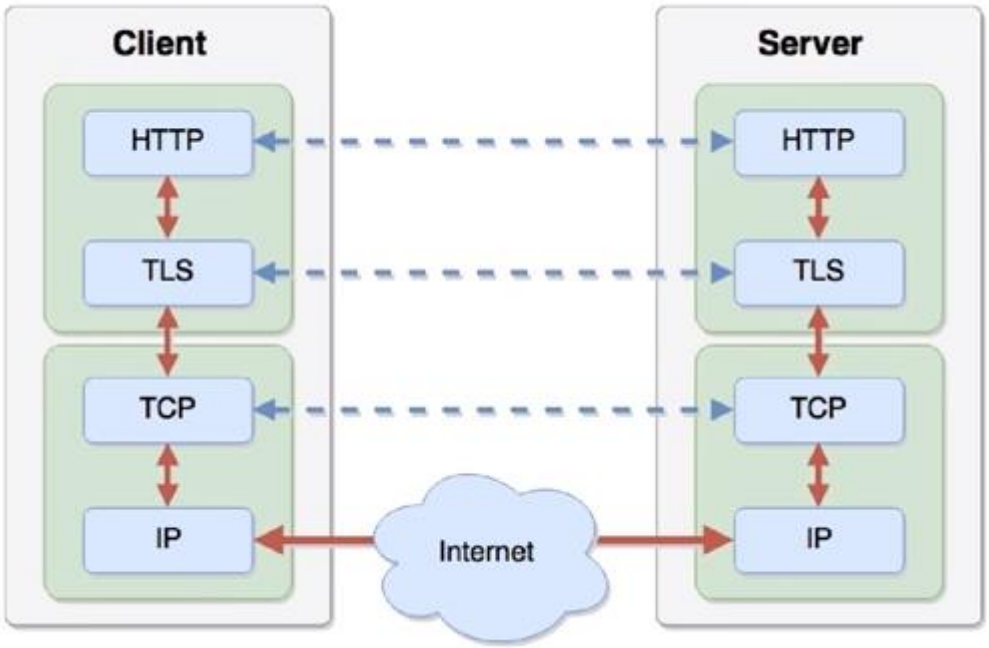
Преобразование системы DNS в доменное имя и адрес web-сервера

Установка TCP –соединение

Опциональная установка TSL соединения

Загрузка связанных ресурсов





Проблемы безопасности

Проблемы безопасности, связанные с использованием HTTP, можно разделить на группы:

- проблемы, связанные с передачей данных;
- уязвимости клиентских приложений;
- уязвимости серверного программного обеспечения:
  - уязвимости серверов (Apache, nginx);
  - уязвимости в серверных сценариях (PHP, ASP).

Проблемы, связанные с передачей данных

Запрос проходит через множество сетей, любая из которых может быть использована для прослушивания или вмешательства в соединение.

- HTTP не использует шифрование, так как:
  - шифрование требует больше вычислительных мощностей;
  - при шифровании передаётся больше данных;
  - шифрованные страницы не кэшируются.

Пример: Когда пользователь просматривает web, злоумышленник может прослушивать незашифрованное Интернет-соединение пользователя, такое как HTTP (наиболее актуально для беспроводных сетей).

Для ослабления таких угроз применяют HTTPS, но наличие хотя бы одного небезопасного запроса сводит эффект к нулю.

Активные адресные атаки

- Активную атаку возможно реализовать с помощью подмены DNS-сервера, либо, в случае беспроводной сети, посредством фальсификации сетевых кадров или путем предоставления вредоносных точек доступа.
- Если пользователь находится позади беспроводного локального маршрутизатора, злоумышленник может попытаться реконфигурировать маршрутизатор, используя пароль по умолчанию и другие уязвимости.

Неадресные угрозы

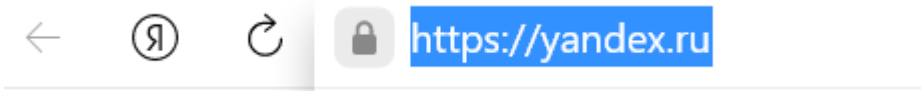
- Фишинг: злоумышленник просит аутентификационные параметры пользователя с помощью сайта, маскирующегося под доверенный ресурс. Атаки фишинга могут быть очень эффективными, так как для пользователей бывает трудно отличить фальшивый сайт от настоящего

Ошибки веб приложений

- Безопасность даже HTTPS-сайта может быть полностью скомпрометирована злоумышленником, использующим простую ошибку, такую как разрешение загрузки каскадного стилевого списка (CSS) или флэш-объекта (SWF), либо используя уязвимости PHP-Include, SQL-injection, Cross-Site Scripting (XSS).

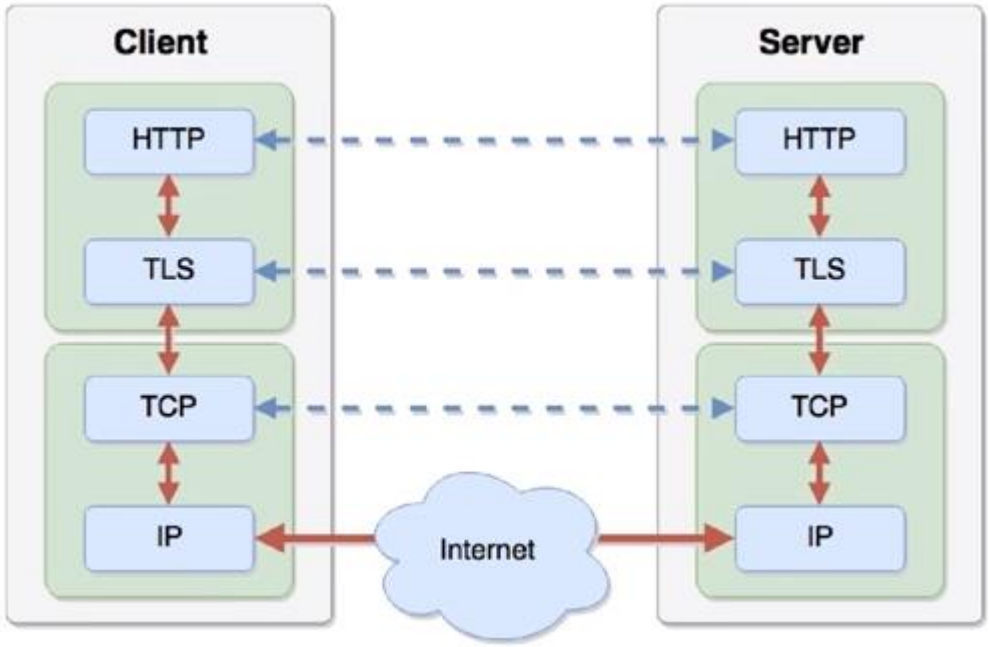
Протокол HTTPS

- HTTPS = HTTP + TLS/SSL
- HTTPS обеспечивает защиту от атак, основанных на прослушивании, при условии, что сертификат сервера проверен и используется шифрование.
- В отличие от HTTP, для HTTPS по умолчанию используется TCP-порт 443.
- Для организации сеанса HTTPS используются серверные сертификаты и, редко, клиентские сертификаты, которые позволяют реализовать взаимную аутентификацию.



Протокол TLS

- TLS (Transport Layer Security) - протокол, наиболее часто применяемый для обеспечения безопасного HTTP соединения.
- В модели протокол TLS размещается между прикладным протоколом и стеком TCP/IP.
- TLS использует:
  - асимметричную криптографию для аутентификации;
  - симметричное шифрование для конфиденциальности;
  - коды аутентичности сообщений (имитовставку) для контроля целостности данных.



Протокол HTTPS

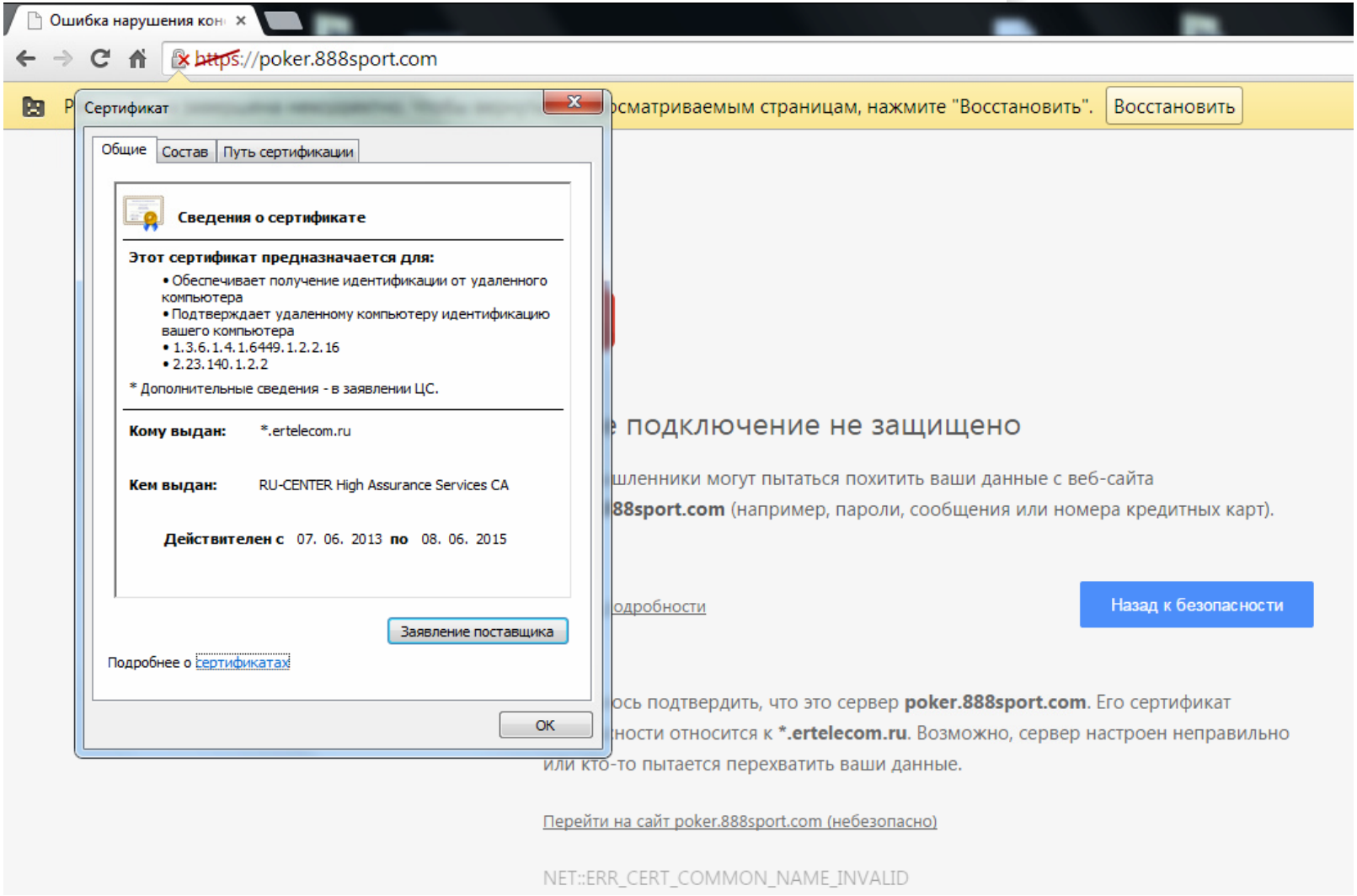
Идентификация сервера

1. После установления соединение, сервер посылает клиенту свой сертификат, чтобы клиент идентифицировал его. Это позволяет предотвратить атаку посредника. В сертификате указывается URI сервера.
2. Если имя сервера не совпадает с указанным в сертификате, то пользовательские программы, например браузеры, сообщают об этом пользователю. В основном, браузеры предоставляют пользователю выбор: продолжить незащищённое соединение или прервать его.

Идентификация клиента

Обычно сервер не располагает информацией о клиенте, достаточной для его идентификации. Однако для обеспечения повышенной защищённости соединения используется так называемая two-way authentication. При этом сервер после подтверждения его сертификата клиентом также запрашивает сертификат. Таким образом, схема подтверждения клиента аналогична идентификации сервера.

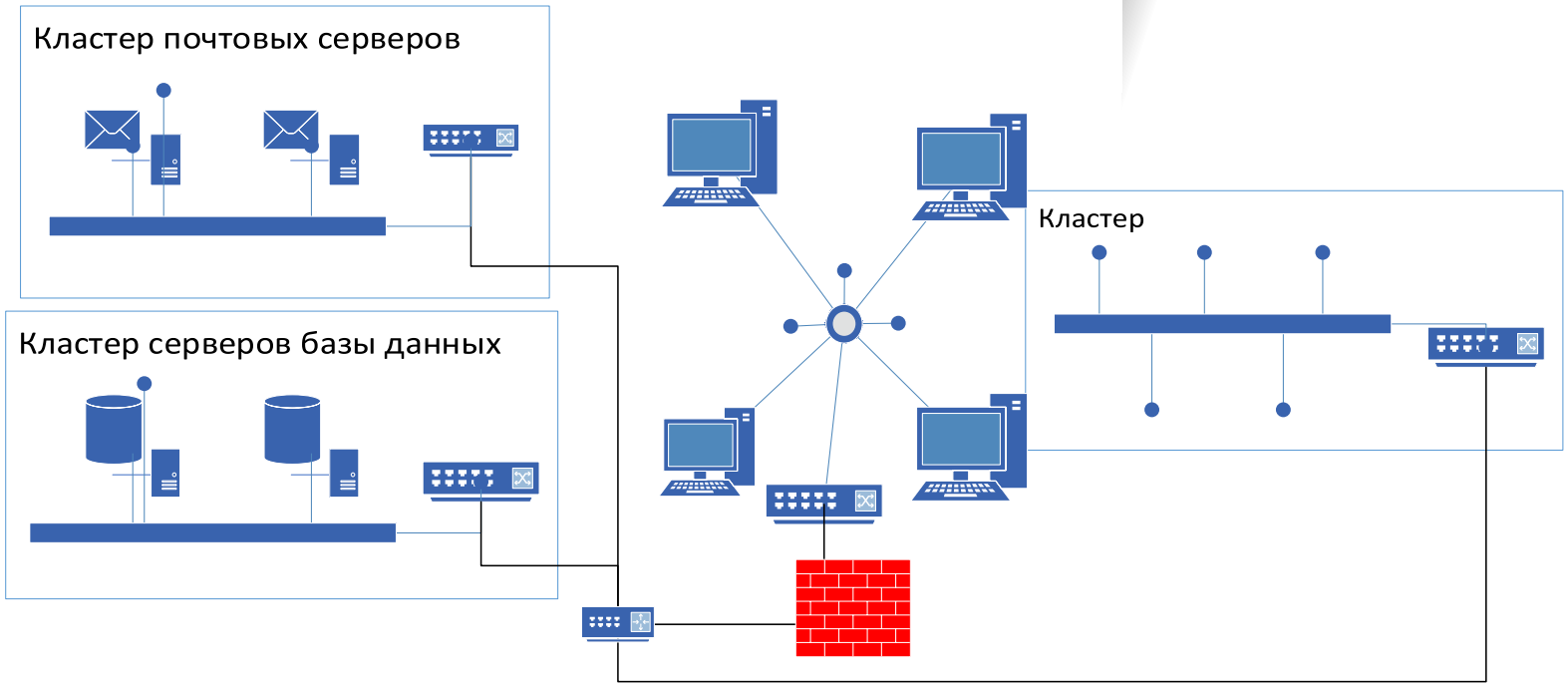
Проблемы HTTPS. Подмена сертификата



Проблемы HTTPS

- Если на компьютере пользователя присутствует троянская программа, имеющая доступ к браузеру, то HTTPS оказывается бесполезным, так как данные могут копироваться вовне до того, как попадут в зашифрованный канал.
- Если атакующая сторона получила соответствующий сеансовый ключ, то она может раскрыть HTTPS-трафик. Секретный серверный ключ или SSL-сертификат для этого не требуются.
- TLS (следовательно, и HTTPS) использует для реализации защищённого канала самые разные наборы криптографических алгоритмов (шифров, подписей, кодов аутентификации, дайджестов и так далее). Если какая-либо часть этого набора выбрана неверно, то соединение будет уязвимым, вне зависимости от того, какие ключи и SSL-сертификаты использовались (пример – уязвимость FREAK).
- Перехват HTTPS-соединения может быть автоматизирован – существуют специальные узлы-прокси, которые выполняют такой перехват на лету, в том числе, генерируя нужные сертификаты

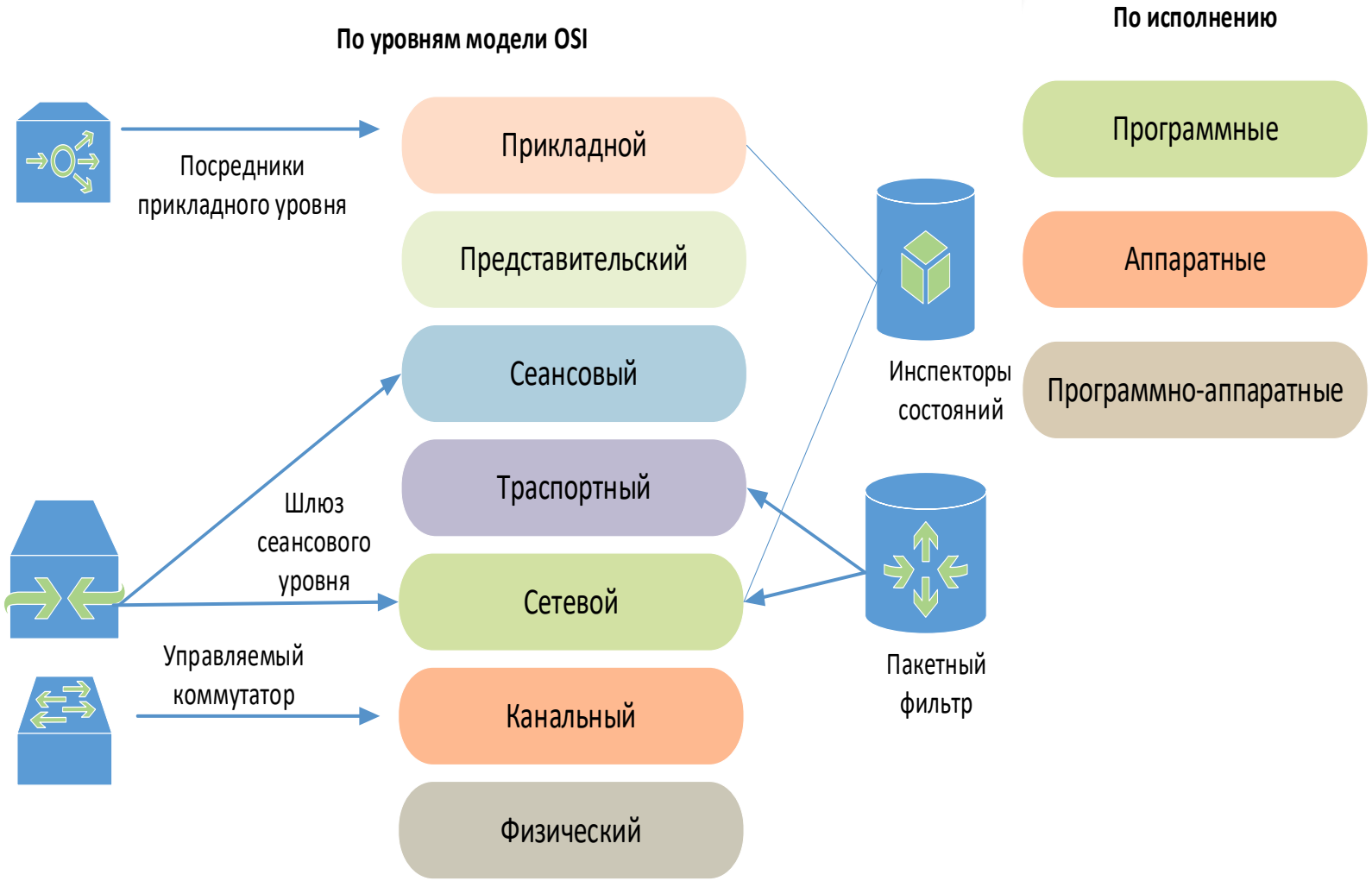
Межсетевые экраны



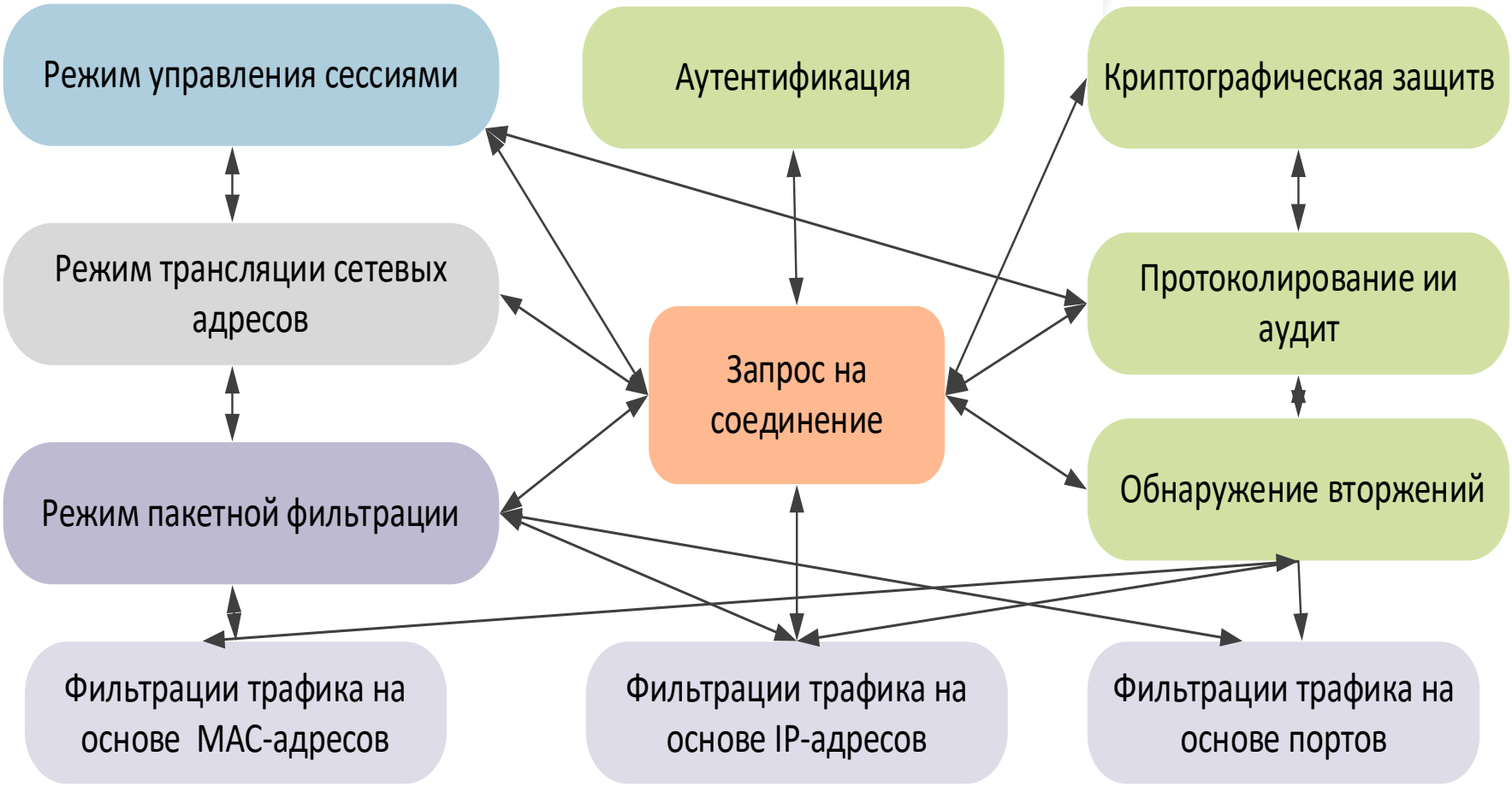
Задачи

1. Защита периметра сети
2. Объединение филиалов организации в виртуальную частную сеть (VPN)
3. Фильтрация трафика
4. Настройка маршрутизации
5. Сегментирование сети
6. Преобразования сетевых адресов
7. Балансировка нагрузки
8. Сбор и мониторинг информации
9. Локальное и удаленное управление

Классификация межсетевых экранов



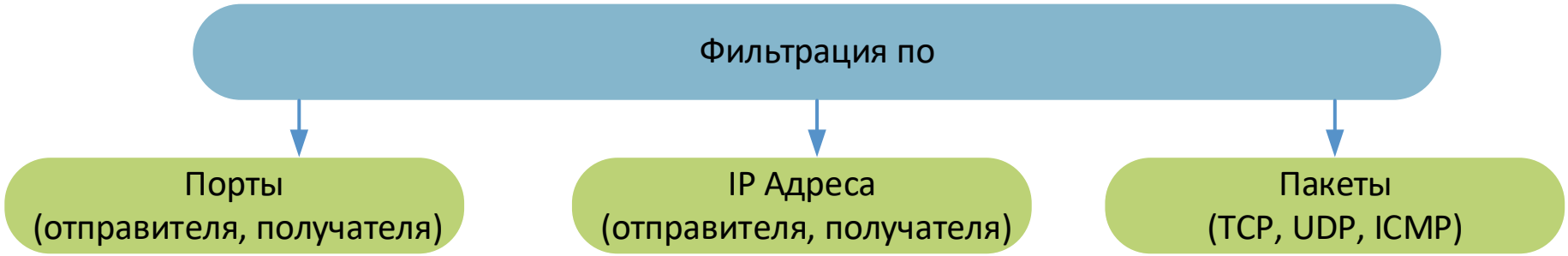
Архитектура межсетевых экранов



Пакетные фильтры (экранирующий маршрутизатор)

Маршрутизатор, обрабатывающий пакеты (сетей TCP/IP и IPX/SPX) на основании информации, содержащейся в заголовках пакетов:

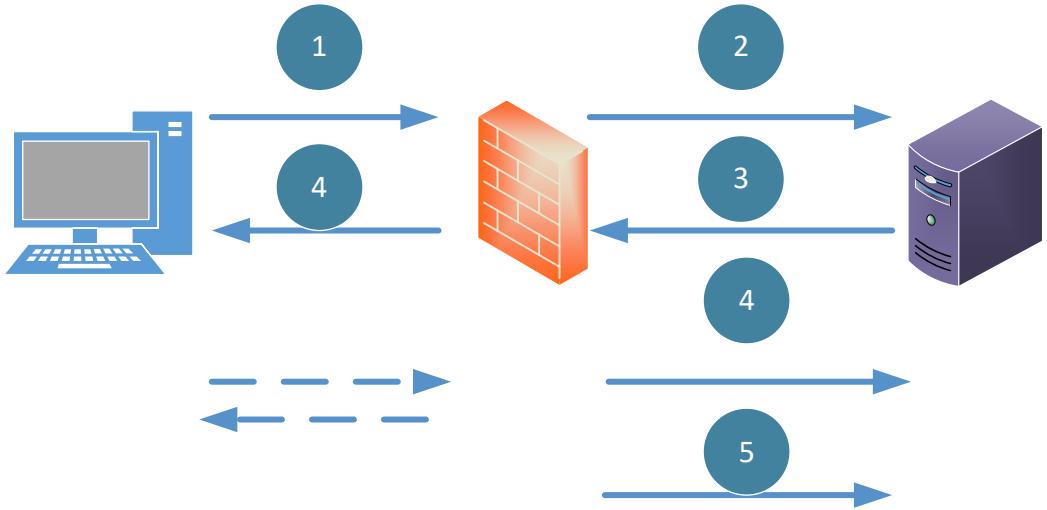
- Используется статическая фильтрация (заданная администратором для каждого уникального типа пакета, требующего обработки).
- для многоканальных соединений требуется учитывать дуплексность соединений.
- Реализованы в в пограничных маршрутизаторах, операционных системах, персональные межсетевые экраны.



Шлюзы сеансового уровня

Пример многоступенчатого порядка установления соединения. Процедура установления соединения состоит из следующих этапов:

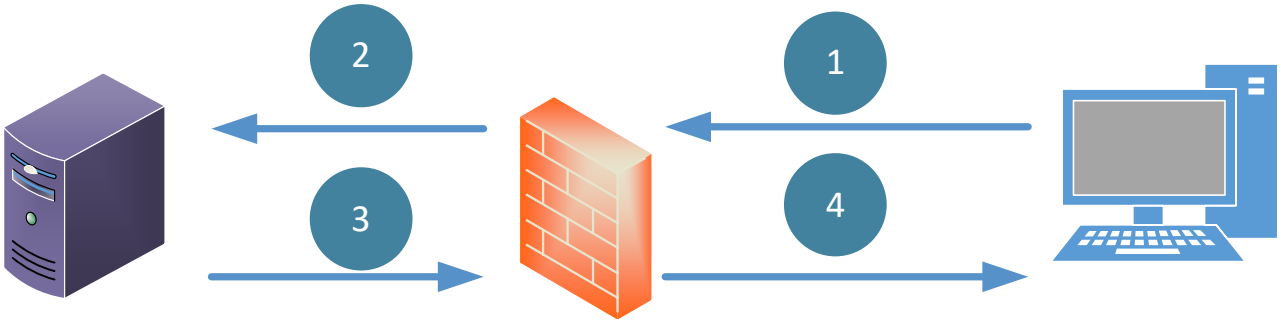
1. МСЭ получает пакет SYN от компьютера A
2. МСЭ передает полученный пакет на сервер B
3. Сервер B передает пакет SYN/ACK на компьютер A, но МСЭ его перехватывает.
4. МСЭ пересылает полученный пакет на компьютер A, кроме того, МСЭ от имени компьютера A посылает пакет ACK на сервер B
5. Если же МСЭ не получит пакета ACK или кончится тайм-аут на установление соединения, то он вышлет в адрес сервера B пакет RST, отменяющий соединение



Шлюзы сеансового уровня

Преобразованием IP-адресов (Network Address Translation, NAT), при которых внутренняя сеть имеет адреса, невидимые в общедоступной сети.

1. При обращении компьютера из внутренней сети наружу шлюз перехватывает этот запрос и заносить его в специальную таблицу.
2. Выступает от имени клиента, используя свой внешний (зарегистрированный) IP-адрес.
3. На полученный ответ шлюз идентифицирует получателя по таблице.
4. Передает ответ получателю.



Внутренний IP	Внутренний порт	Внешний IP	Внешний порт
192.168.1.2	50300	184.86.48.128	49127
192.168.1.3	52001	184.86.48.128	49128
192.168.1.2	49238	184.86.48.128	49129

Шлюзы сеансового уровня

Преимущества:

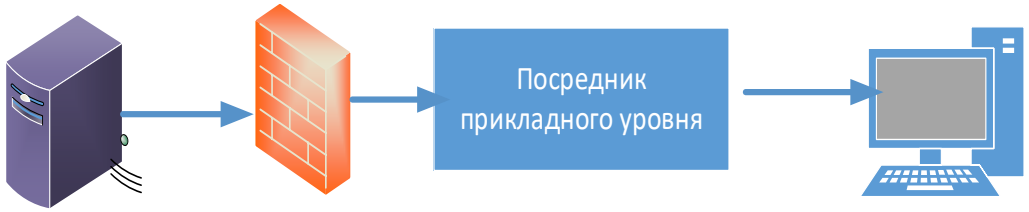
- Позволяет преодолеть нехватку адресов IPv4 и осуществить сокрытие внутренней структуры сети
- Позволяют динамически задавать правила фильтрации трафика

Недостатки:

- Некоторые прикладные протоколы работают неправильно (FTP)
- Нет единого стандарта NAT
- Отсутствует возможность проверки содержания поля данных
- Невозможность регулирования передачи информации на прикладном уровне
- Используют ненадежную систему идентификации и аутентификации, основанную на IP-адресах отправителя/получателя.

Посредники прикладного уровня

Содержат несколько приложений-посредников, каждое из которых обслуживает свой прикладной протокол и позволяют:



Задачи

1. Определение типа сообщения
2. выявление в передаваемых сообщениях несуществующие или нежелательные последовательности команд
3. осуществление проверки аргументов входных данных
4. Аутентификация пользователя
5. Проверка сертификатов
6. Кеширование данных
9. Сбор и мониторинг информации

Посредники прикладного уровня

Преимущества:

- Анализ на прикладном ровне и возможность реализации дополнительных механизмов защиты (например, анализ содержимого).
- Исключение прямого взаимодействия между двумя узлами.
- Высокий уровень защищенности.
- Контроль состояния соединения.

Недостатки:

- большие затраты времени и ресурсов на анализ каждого пакета
- невозможность автоматического подключения поддержки новых сетевых приложений и протоколов, так как для каждого из них необходим свой агент

Инспекторы состояния

Термин «инспектор состояния» был введен компанией Check Point. Инспекторы состояния оперируют на трех уровнях: прикладном, сеансовом и сетевом и позволяют контролировать:

- каждое приложение— на основе разработанных посредников;
- каждую сессию — на основе таблицы состояний;
- каждый передаваемый пакет — на основе таблицы правил.

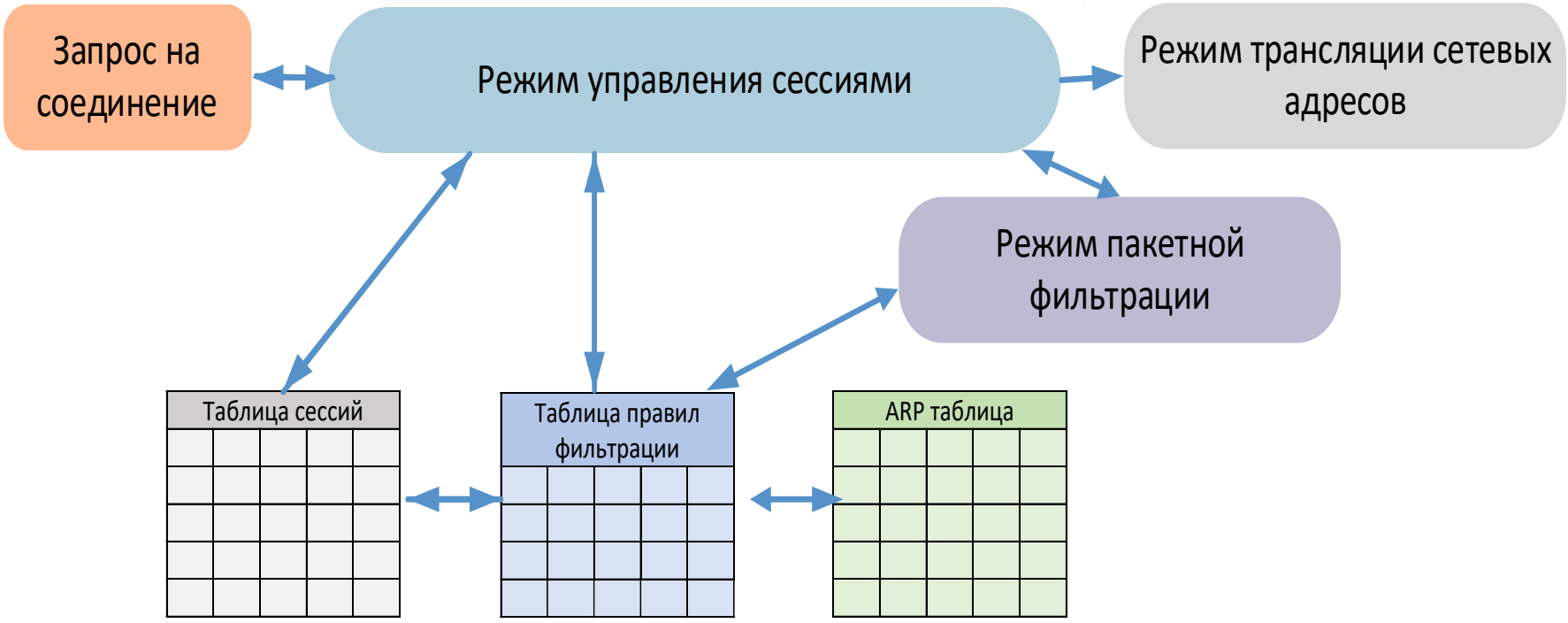
При получении пакета данных содержимое этого пакета сравнивается с некими шаблонами, специфическими для соответствующего протокола прикладного уровня. Осуществляется выполнение следующих действий:

- пропуск пакета;
- удаление пакета и сессии;
- регистрация пакета и сессии.

Дополнительные функции:

- Трансляция сетевых адресов
- Аутентификация пользователей
- Регистрация событий

Инспекторы состояния. Управление сессиями



Инспекторы состояния

Преимущества механизма управления сессиями:

Контроль хода TCP-соединения. Автоматическое открытие клиентских портов, необходимых для текущего соединения.

Контроль данных прикладных протоколов.

Блокировка атак, связанных с некорректной установкой флагов TCP.

Основные параметры сессии, хранящаяся в таблице сессий:

- интерфейсы, MAC-, IP-адреса и порты взаимодействующих сторон
- номера родительской и дочерней сессий
- текущее состояние сессии
- протокол транспортного и прикладного уровней
- информация о контексте прикладного протокола
- номера TCP-последовательностей для последнего принятого пакета
- имя пользователя, которому принадлежит данная сессия
- время начала, время последней активности и значение таймаута неактивности сессии
- количество пакетов и байт, прошедших от клиента к серверу и обратно
- параметры подсчета интенсивности пакетов в сессии
- номер порта трансляции при использовании режима NAT

Инспекторы состояния. Фильтрация прикладных протоколов

Идентификация основных прикладных протоколов независимо от порта сервиса

Протокол HTTP:

фильтрация по адресам WEB-серверов

фильтрация по именам (фрагментам) файлов

фильтрация по методу запроса

Протокол SMTP:

фильтрация по почтовым адресам отправителя и получателя

Протокол FTP:

фильтрация по командам put, get

фильтрация по именам (фрагментам) файлов

фильтрация по имени/паролю пользователя

Сервисы SQL:

фильтрация по SQL-запросам

Инспекторы состояния. Фильтрация прикладных протоколов

Преимущества:

- Прозрачность для конечного пользователя, не требующая дополнительной настройки пли изменения конфигурации клиентского программного обеспечения.
- Высокая скорость обработки информационных потоков.
- Не изменяют IP-адресов проходящих через них пакетов (любой протокол прикладного уровня, использующий IP-адреса, будет корректно работать с этими МЭ без каких-либо изменений или специального программами).

Недостатки:

Допускают прямое соединение между авторизованным клиентом и компьютером внешней сети.

- .

Демилитаризованная зона

Демилитаризованная зона (DMZ - Demilitarized Zone) - сеть, которая добавляется между защищенной сетью и сетью, которая имеет меньший уровень безопасности, для создания дополнительного уровня безопасности.

Архитектура DMZ:

- схема единой защиты локальной сети (Без выделения DMZ).
- схема с одной DMZ (С защищаемой закрытой и не защищаемой открытой подсетями).
- схема с Service-log DMZ (С раздельной защитой закрытой и открытой подсетей для одного МЭ с 3 сетевыми интерфейсами).
- схема с двумя DMZ (С раздельной защитой закрытой и открытой подсетей для двух МЭ с двумя сетевыми интерфейсами).

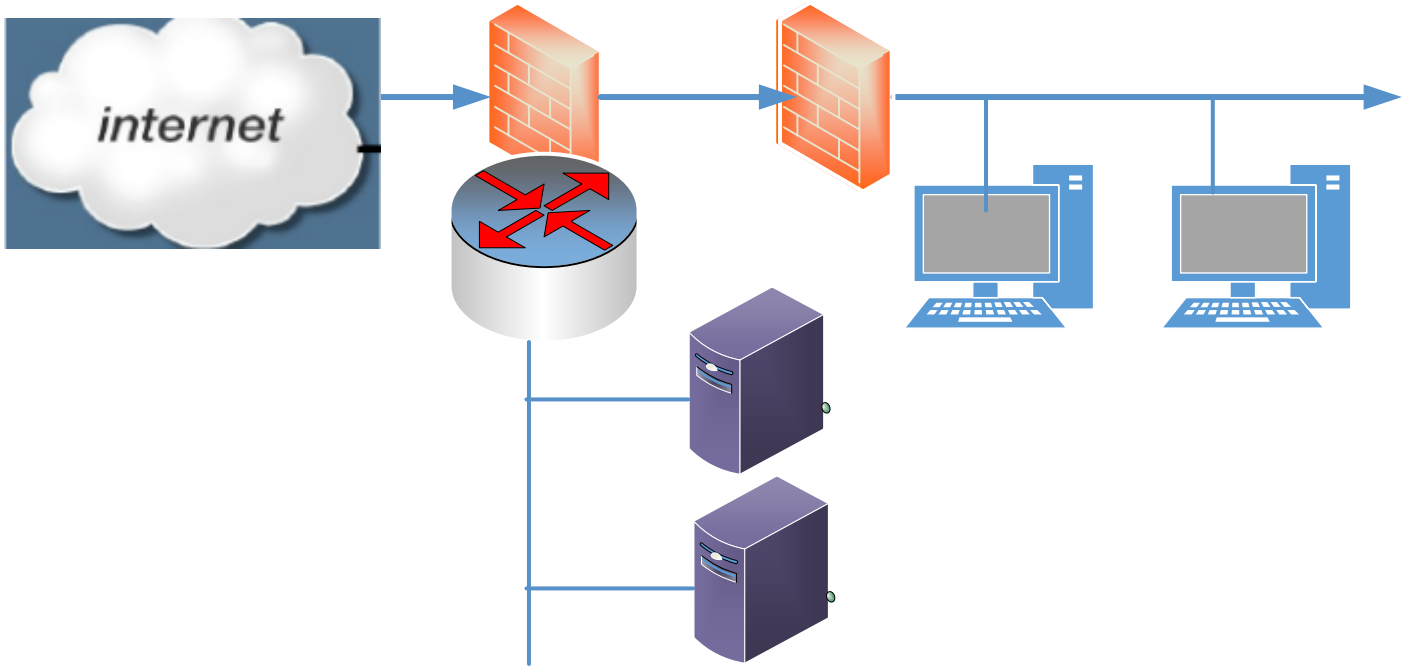
Демилитаризованная зона

Политика:

- Прохождение пакетов от более безопасного интерфейса к менее безопасному разрешено , если не запрещено.
- Прохождение пакетов от менее безопасного интерфейса к более безопасному запрещено, если не разрешено.
- Прохождение пакетов на интерфейсах с одинаковым уровнем безопасности запрещено.
- Размещение межсетевого экрана в том месте, где происходит разветвление маршрута.

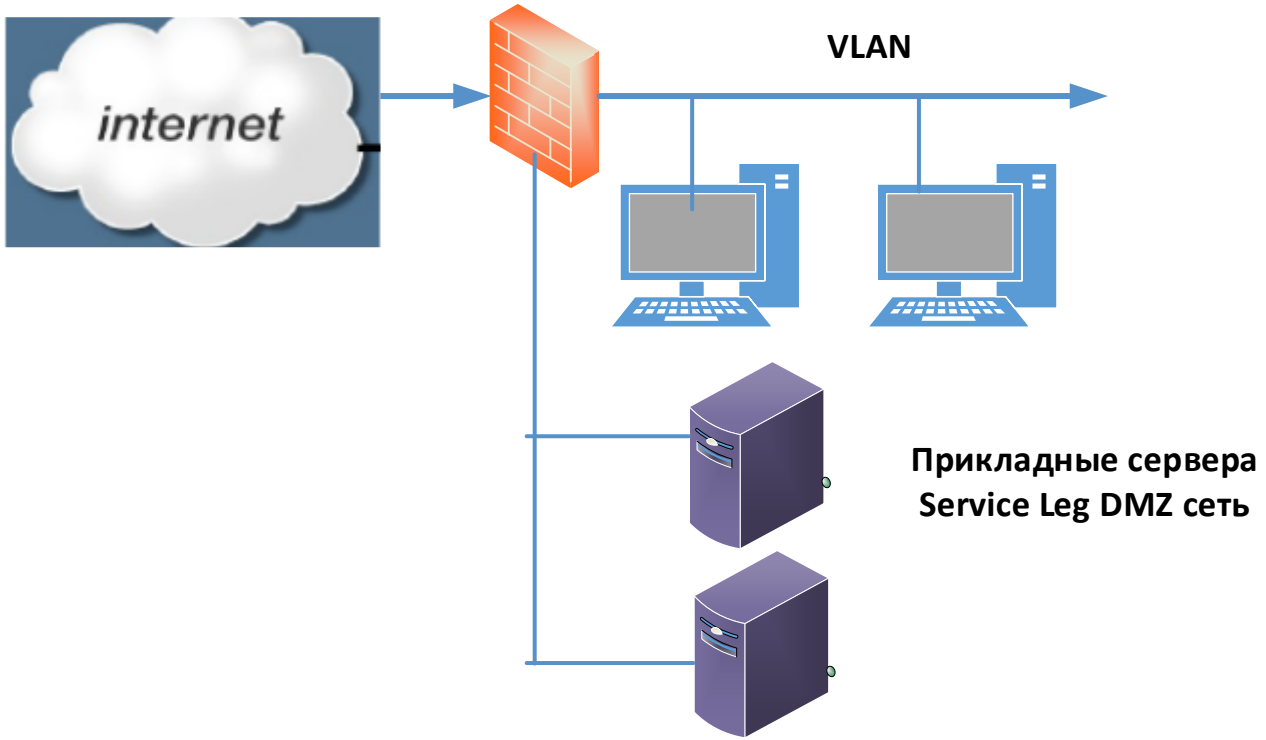
Конфигурация с одной DMZ-сетью

В DMZ располагают публично доступные сервера, такие как веб-сервер или почтовый сервер, которые не должны быть размещены во внутренних защищенных сетях, но к которым необходим доступ либо только извне, либо только изнутри, либо и извне, и изнутри. Причина в том, что никогда нельзя гарантировать, что эти системы и ресурсы не могут быть взломаны. Но взлом этих систем не должен автоматически означать доступ ко всем внутренним системам



Service Leg конфигурация

Сетевые интерфейсы МСЭ соединяются с Интернетом, внутренней сетью, отдельным сетевым интерфейсом формируется DMZ-сеть.



Недостаток: возрастание риска DoS-атаки на межсетевой экран, при интересе со стороны злоумышленника к сервисам, расположенные в DMZ-сети.

Конфигурация с двумя DMZ-сетями

Архитектура:

Пограничный маршрутизатор- осуществляет фильтрацию пакетов и обеспечивает защиту серверов.

Основной межсетевой экран управляет доступом для внутренних серверов, и служит защитой для межсетевых экранов как от внешних, так и от внутренних атак.

Межсетевой экран внутренней DMZ обеспечивает управление доступом и защиту серверов, если внешние сервера атакованы.

Нарушения безопасности

1. Обход МСЭ через модем
2. Обход правил фильтрации персоналом из внутренней сети
3. Использование механизмов туннелирования
4. Атака на МСЭ
5. Подмена IP адреса
6. Перехват, подбор пароля

Литература

1. ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.
2. ГОСТ Р 59162-2020. Национальный стандарт Российской Федерации.
3. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей.
4. Варлатая С. К., Рогова О. С., Юрьев Д. Р. Анализ методов защиты беспроводной сети Wi-Fi от известных способов взлома злоумышленником // Молодой ученый. — 2015. — №1. — С. 36-37.
5. Протоколы беспроводной передачи данных https://intuit.ru/studies/courses/1004/202/lecture/5250?page=3
6. Лекция 1. Обзор архитектуры Bluetooth Версия 2.0 + EDR https://wl.unn.ru/materials/courses/wlnet/Lect/6_Lect_1.pdf
7. Интернет-энциклопедия https://ru.wikipedia.org/wiki/Bluetooth
8. Эксплуатация достоверного Bluetooth-соединения https://www.securitylab.ru/analytics/495788.php
9. Приказ ФСТЭК № 17 от 11 февраля 2013 года
10. Приказ ФСТЭК № 21 от 18 февраля 2013 года
11. Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утверждёнными Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119
12. Приказ ФСТЭК России от 9 февраля 2016 г. №9 Требования к межсетевым экранам
13. Информационное сообщение ФСТЭК «Об утверждении требований к межсетевым экранам» от 28 апреля 2016 г. N 240/24/1986
14. Лапонина О.Р. Л24 Основы сетевой безопасности. Часть 1. Межсетевые экраны: Учебное пособие / О.Р. Лапонина — М.: Национальный Открытый Университет «ИНТУИТ» , 2014. — 378 с., ил., табл.— (Серия «Основы информационных технологий»).