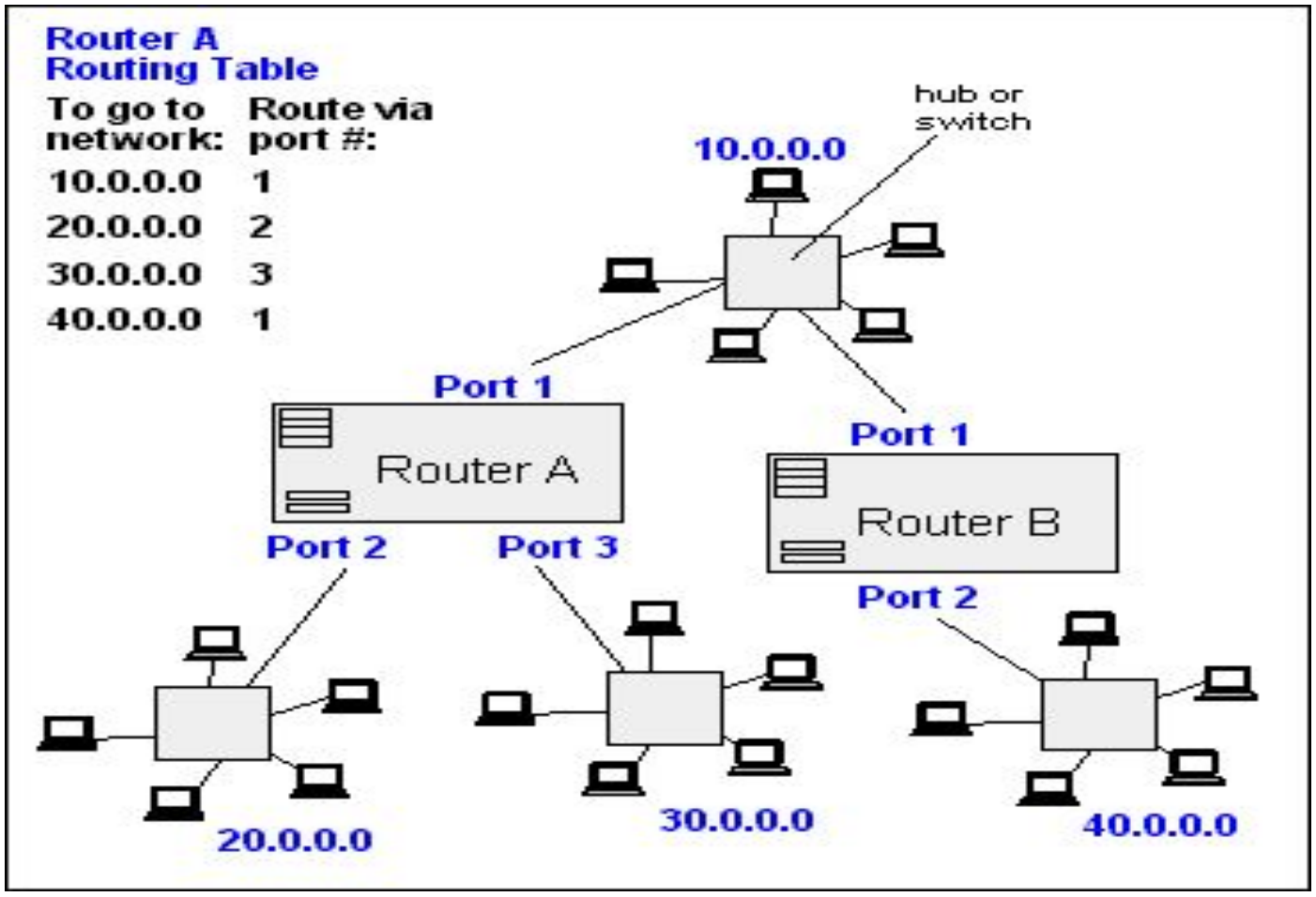
Лекция 9. Безопасность компьютерных сетей

1. Маршрутизация



1. Маска подсети

Маска подсети нужна узлу для определения границ подсети.
Чтобы было возможно определить, кто находится с узлом в одной подсети, а кто — за ее пределами. **Использовать ли шлюз?**

Пусть IP=192.168.11.10
Пример простой и распространенной маски: 255.255.255.0
Записывается так: 192.168.11.10 255.255.255.0

Не может быть маски
120.22.123.12=01111000.00010110.01111011.00001100.

Но может быть маска
255.255.248.0=11111111.11111111.11111000.00000000.

Запись в бесклассовой адресации:

192.168.11.10 255.255.248.0 = 192.168.11.10/21

1. Маска подсети. Пример.

Настройки сетевого адаптера: 192.168.11.10/21:

Определение границы подсети:

11000000.10101000.00001011.00001010
∧ 11111111.11111111.11111000.00000000 (=255.255.255.248)

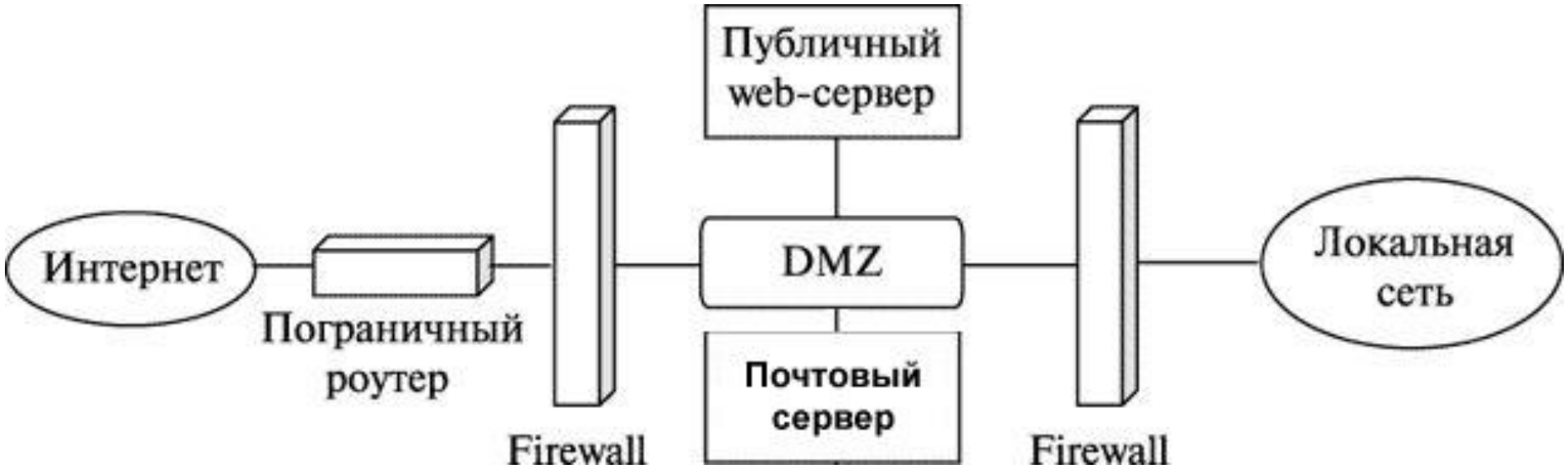
11000000.10101000.00001000.00000000 = 192.168.8.0 - начало

11000000.10101000.00001011.00001010
∨ 00000000.00000000.00000111.11111111 (=¬255.255.255.248)

11000000.10101000.00001111.11111111 = **192.168.15.255** - конец

Границы подсети от 192.168.8.1 до 192.168.15.255.

Типовая сетевая инфраструктура предприятия 1



Типовая сетевая инфраструктура предприятия 2

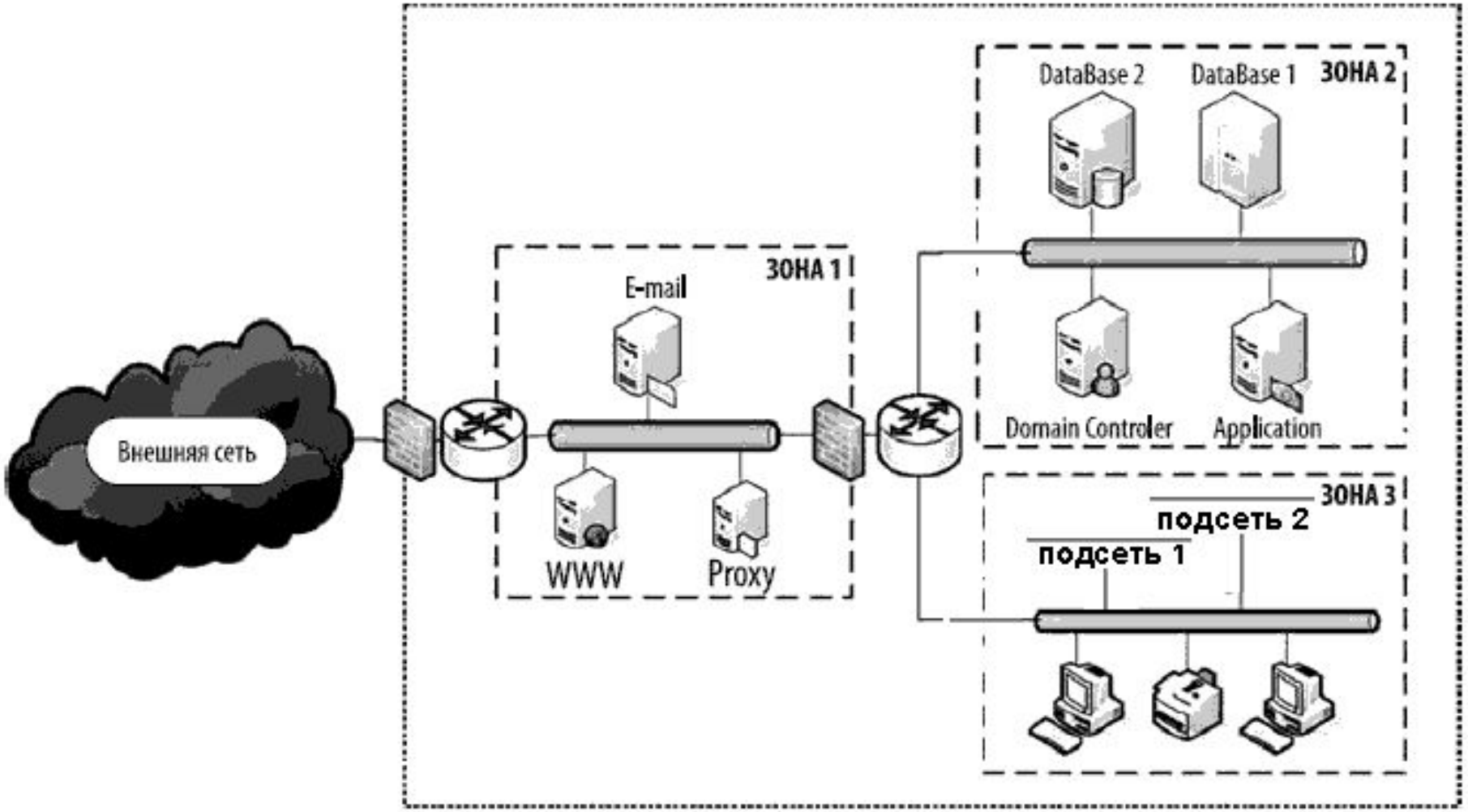
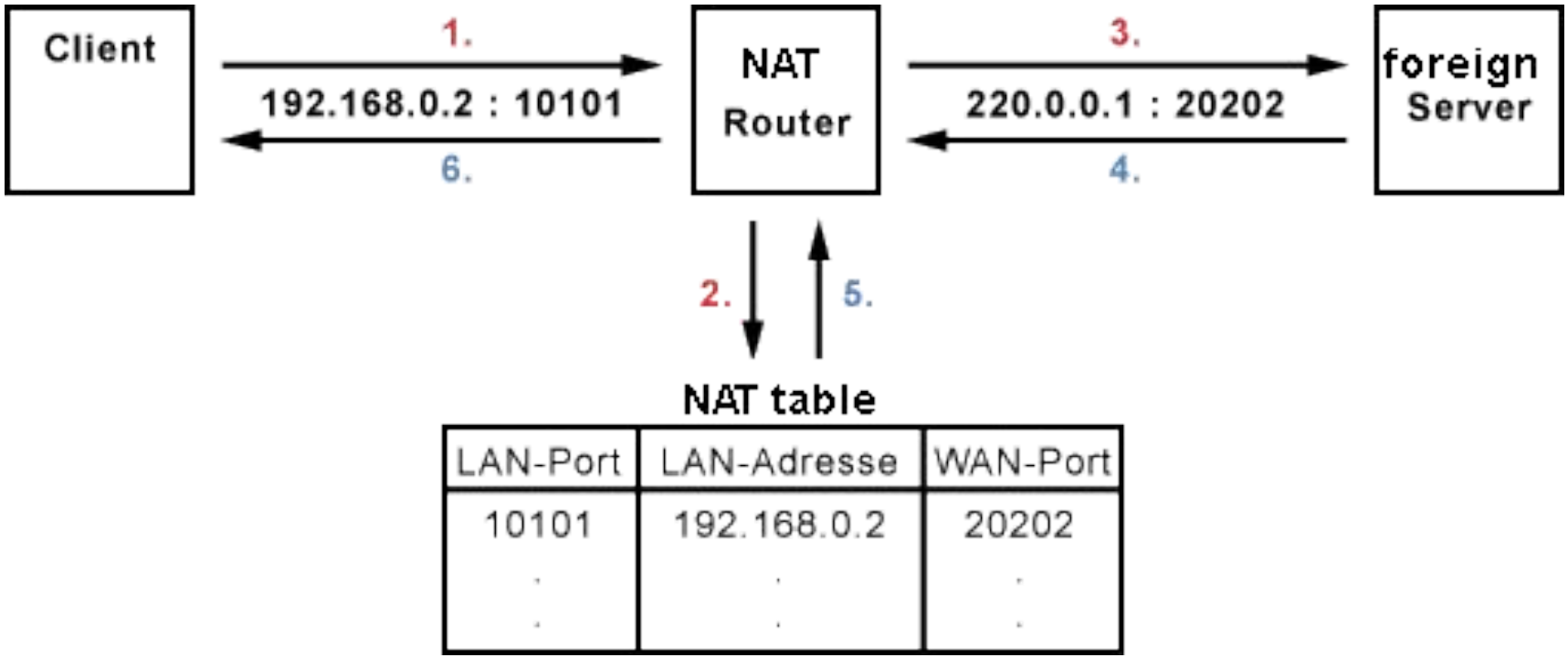


Схема организации сетевой инфраструктуры

2. NAT

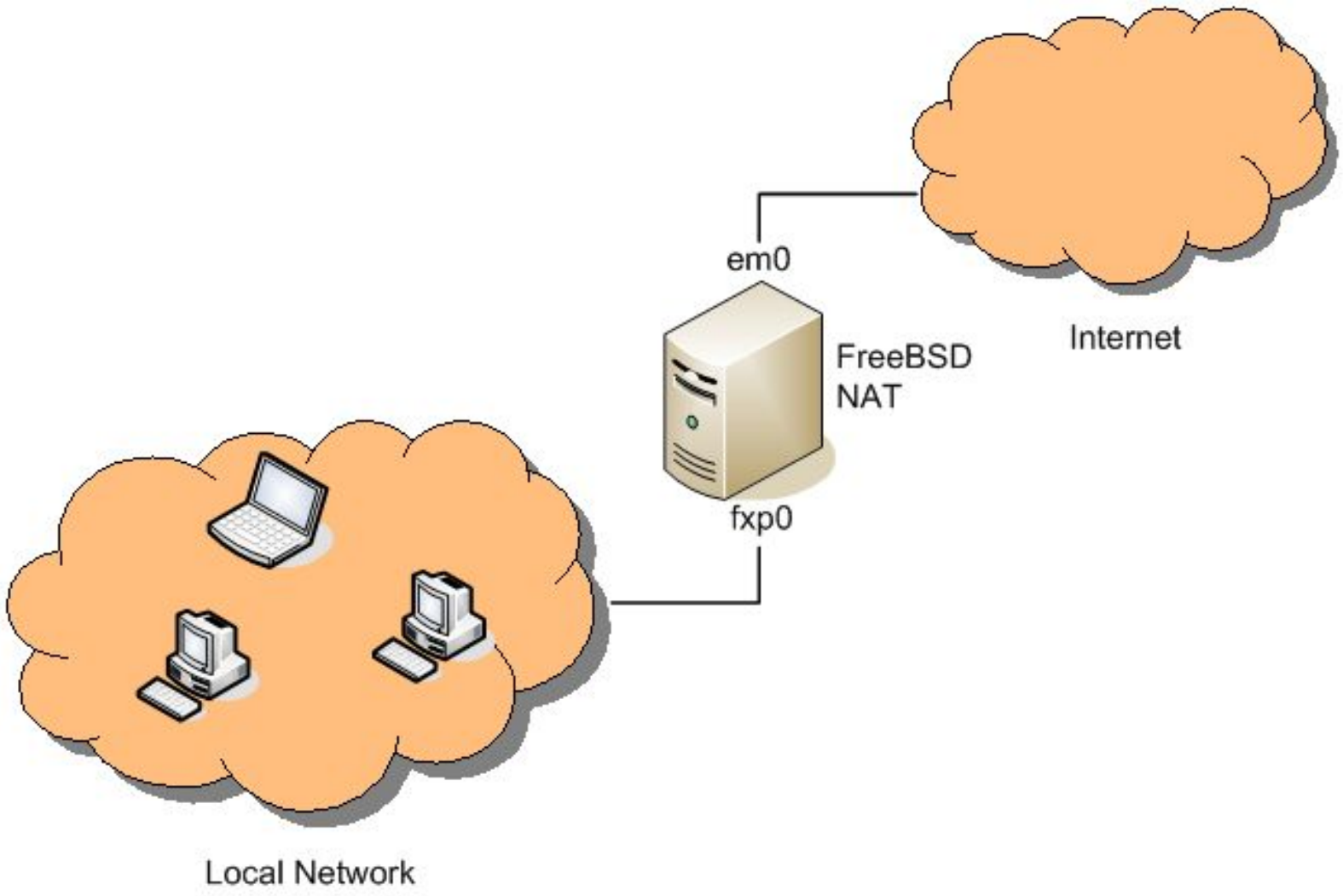

Client
1.
192.168.0.2 : 10101
6.
NAT
Router
3.
220.0.0.1 : 20202
4.
foreign
Server
2.
5.
NAT table
LAN-Port
LAN-Adresse
WAN-Port
10101
192.168.0.2
20202

3. Брандмауэры

Межсетевой экран, сетевой экран, файервол, брандмауэр — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

- Фильтрация
- Пакетная статическая фильтрация , осуществляется путём анализа IP-адреса источника и приёмника, протокола, портов отправителя и получателя
- Контекстная
  - для конкретных пользователей, в зависимости от форматов данных, типов интерфейсов и устройств, сетевых протоколов, направления передачи, дня недели и времени суток и т.д.
- Прикладная используют знания о специфических особенностях приложения для блокировки вредоносных запросов, обеспечивая защиту не на сетевом, а на прикладном уровне

3. Nat+Firewall **IPFW**



3. Nat+Firewall IPFW

nat **1** config log if em0 same_ports deny_in

#разрешаем все по локальной сети

add **100** allow ip from any to any via fxp0

#разрешаем подключение к маршрутизатору с 2-х IP из вне по SSH

add **200** allow tcp from {11.5.5.10 & 11.5.5.15} to me 22 via em0

add **300** allow tcp from me 22 to {11.5.5.10 & 11.5.5.15} via em0

#разрешаем стандартные порты

add 400 allow tcp from any to me 80 in via em0

add 500 allow tcp from any to me 443 in via em0

 # заворачиваем на NAT все что проходит через внешний интерфейс

add **600** nat **1** ip from any to any via em0

 # все что не попадает ни под одно правило запрещаем

add **65534** deny all from any to any

Варианты построения защищенного канала связи

Уровни OSI	Протокол защищенного канала
Прикладной уровень	S/MIME, HTTPS
Уровень представления	SSL, TLS
Сеансовый уровень	
Транспортный уровень	
Сетевой уровень	IPsec (VPN)
Канальный уровень	PPTP
Физический уровень	

Виртуальные частные сети - VPN

VPN – Virtual Private Network – имитируют возможности частной сети в рамках общедоступной, используя существующую инфраструктуру.

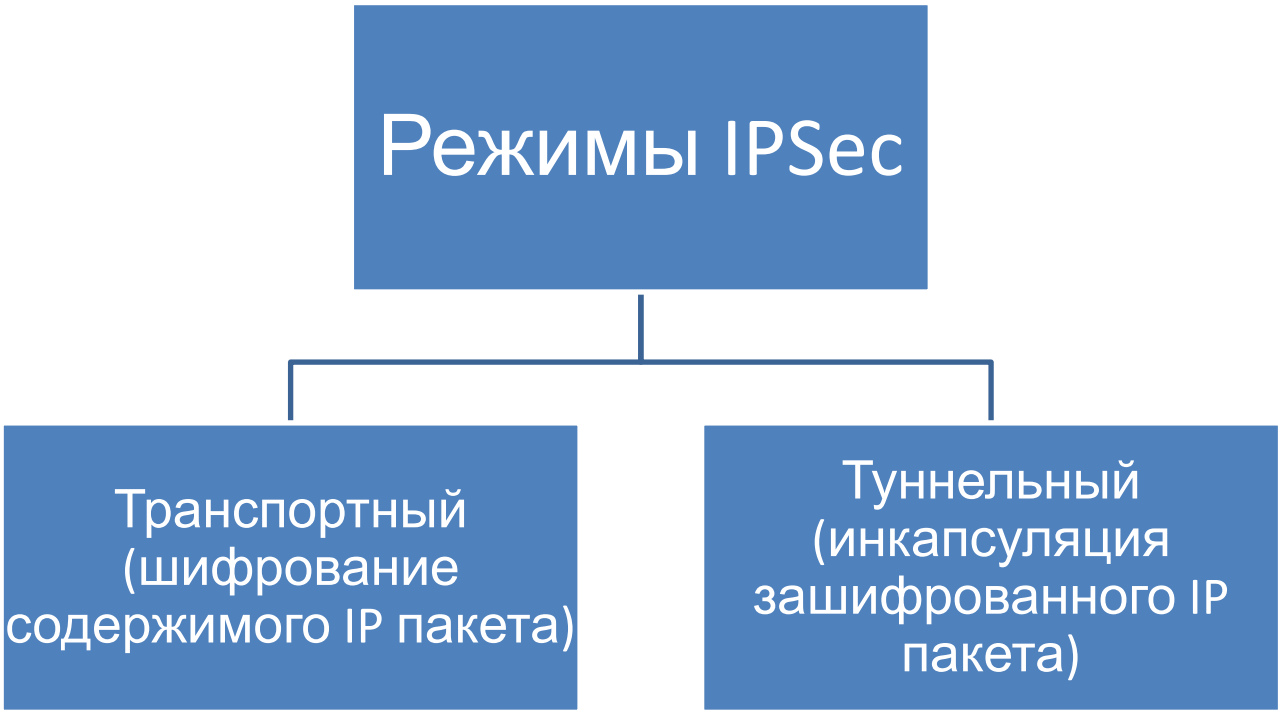
Особенность VPN – формирование логических связей не зависимо от типа физической среды. Позволяют обойтись без использования выделенных каналов.

Задача: обеспечение в общедоступной сети гарантированного качества обслуживания, а также их защита от возможного несанкционированного доступа или повреждения.

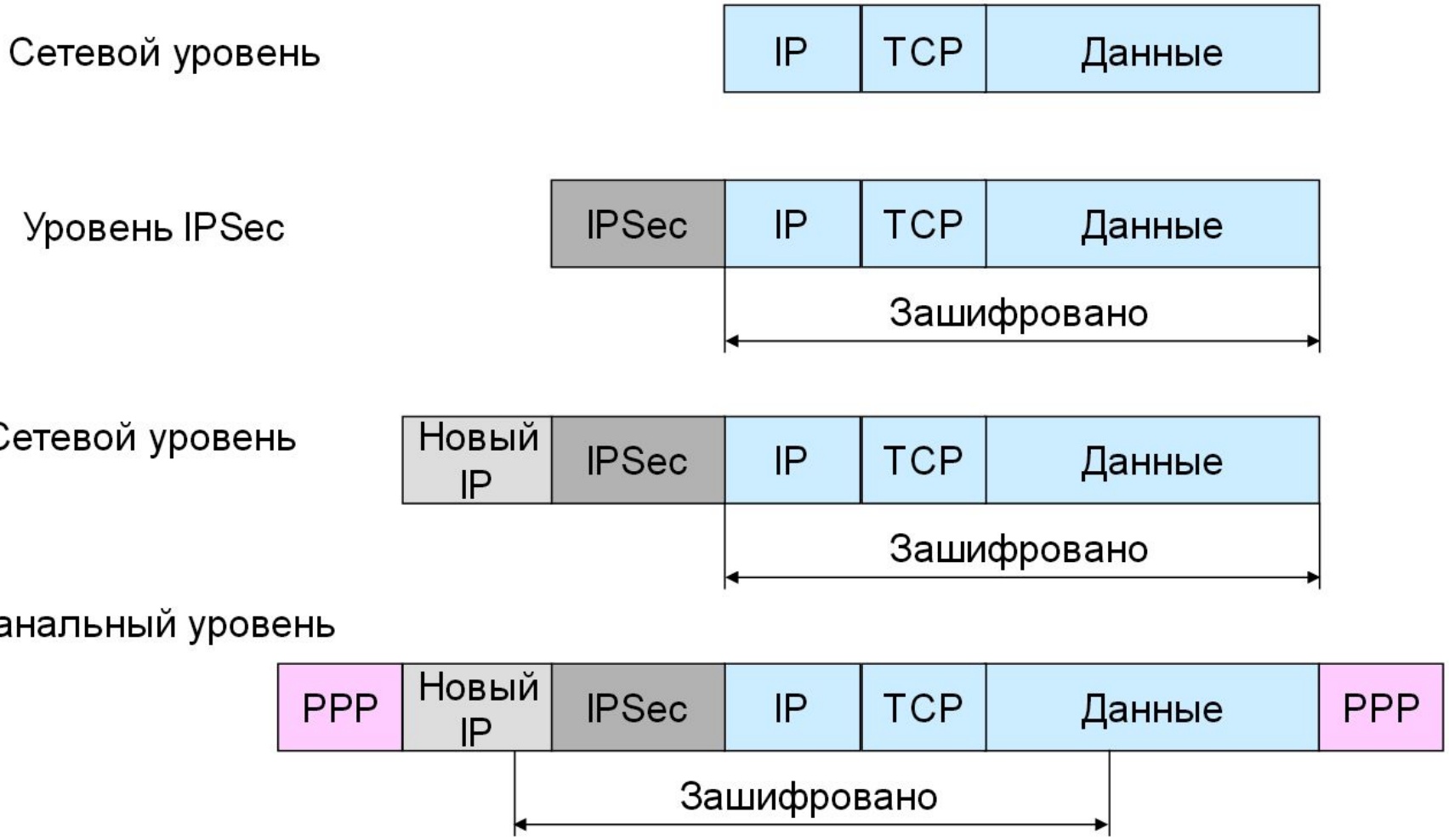
4. IPsecurity

IPsec (сокращение от IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP (надстройка над IP).

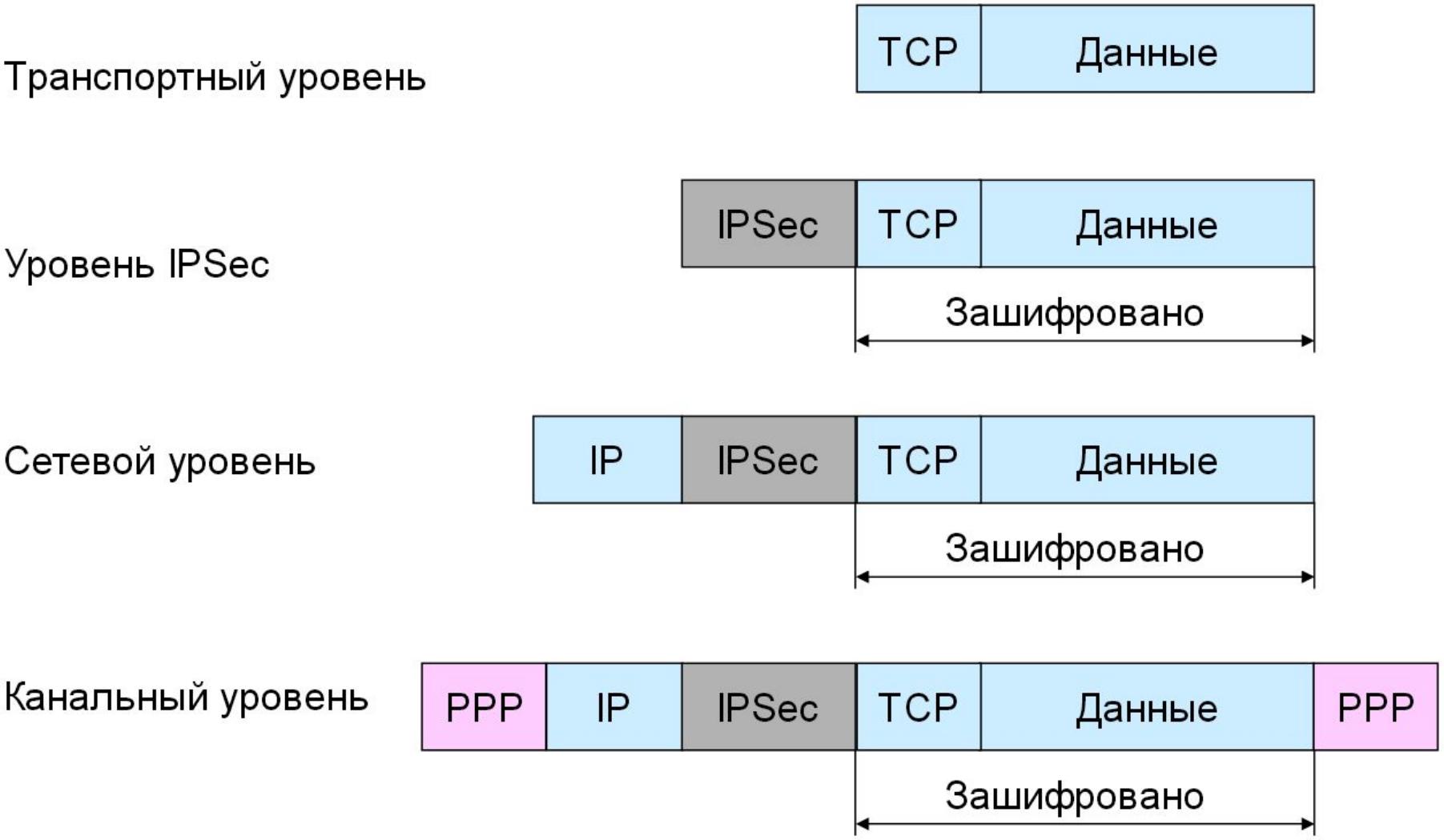
- подтверждение подлинности (аутентификацию),
- проверку целостности
- шифрование IP-пакетов.
- защищённый обмена ключами



Инкапсуляция IPSec для туннельного режима



Инкапсуляция IPSec для транспортного режима



5. VPN на примере PPTP (тунельный уровень)

Принцип инкапсуляции

6. SSL Secure Sockets Layer — уровень защищённых сокетов

- Уровень представления
- Изначально разработан в 1996 году компанией Netscape для HTTPS
- OpenSSL — криптографический пакет с открытым исходным кодом для работы с SSL.

- Применяется для:
  - организации защищенного WEB соединения (HTTPs)
  - используется для обмена мгновенными сообщениями
  - передачи голоса через IP
  - электронная почта,
  - Интернет-факс

8. Безопасность в WiFi сетях

Wi-Fi (Wireless Fidelity) — торговая марка для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

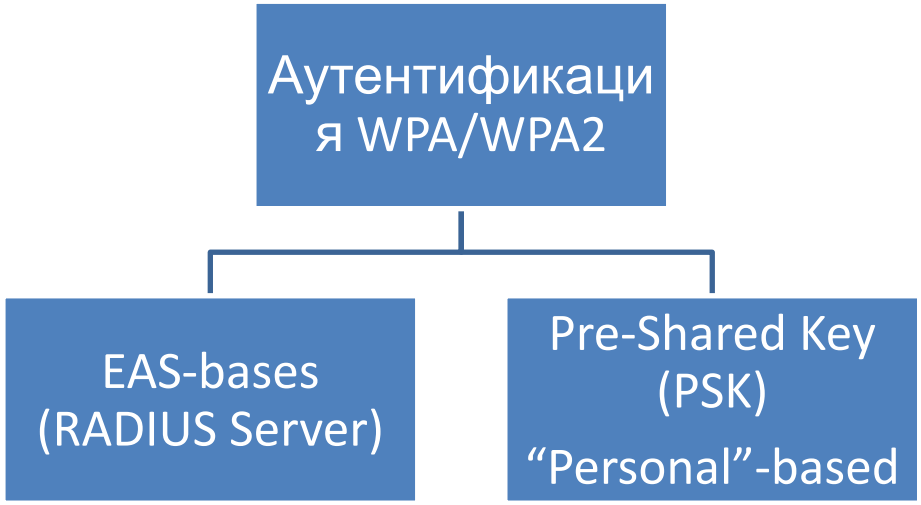
Standard	Speed	Year
802.11n	100 Mbps	2009
802.11g	54 Mbps	2002
802.11a	54 Mbps	1999
802.11b	11 Mbps	1999
802.11	2 Mbps	1997

Mbps (megabits per second).

8. Виды аутентификации в WiFi сетях

- None
- WEP
- WPA-PSK
- WPA2-PSK

WPA=**Wi-Fi Protected Access**



8. 4-шаговый WPA handshake

SSID (Service Set Identifier) – идентификатор беспроводной сети (вводится вручную).

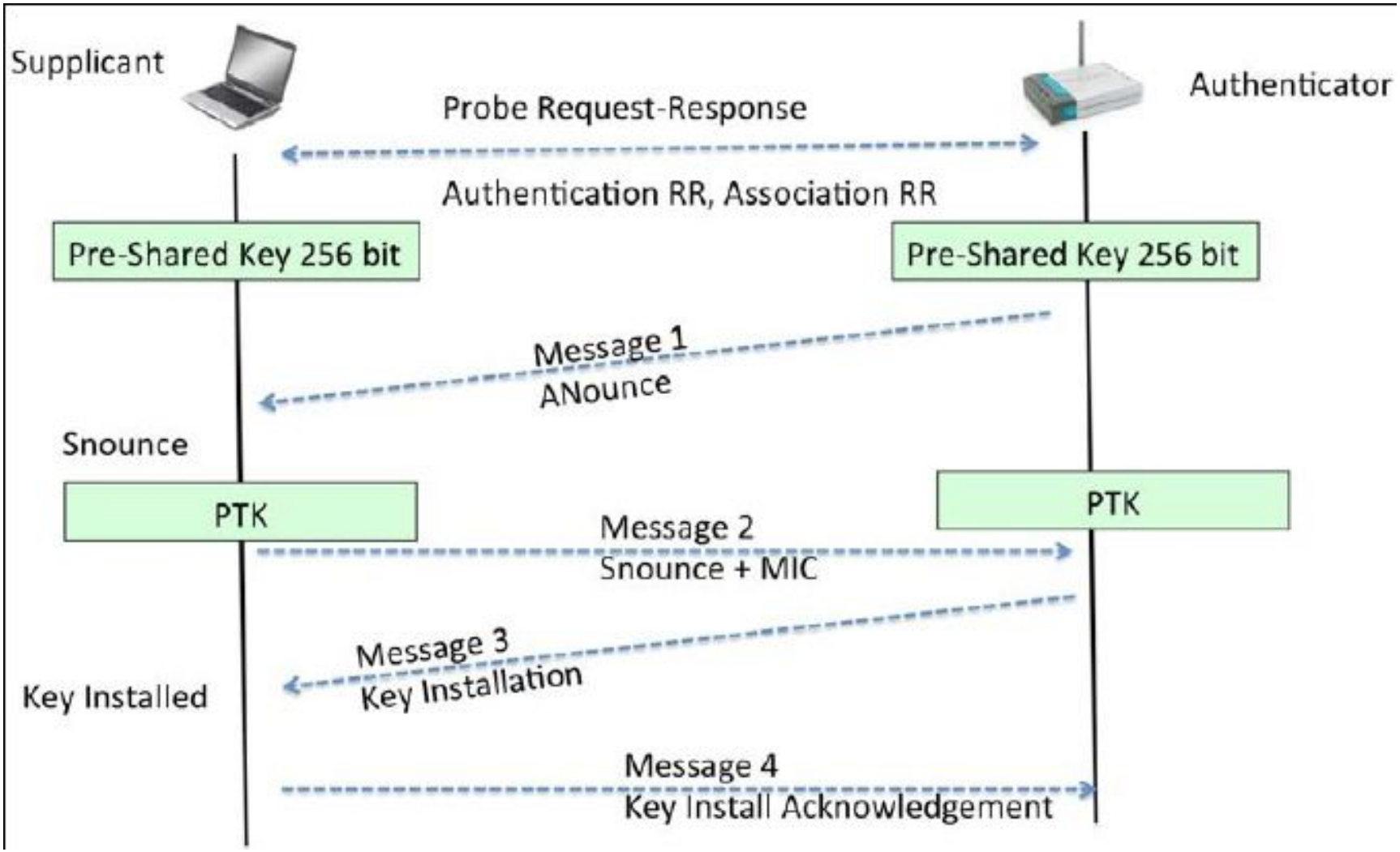
Pre-shared key (PSK) – 256 битный ключ на основе общей парольной фразы и SSID. Получается математическим преобразованием PBKDF2 (Password-Based Key Derivation Function 2.0).

Pairwise Transient Key (PTK) – временный, парный или сеансовый ключ, для взаимодействия беспроводного пользовательского устройства с точкой доступа. Свой для каждого клиентского устройства.

PTK=Мат. преобразование от {PSK, MAC1, MAC2, Anounce, Snounce}

MIC (Message Integrity Check) – код аутентичности сообщения. Гарантирует авторство и целостность передаваемого Snounce и 128 бит PTK.

8. 4-шаговый WPA handshake



8. Криптоанализ wifi с использованием ***aircrack-ng***. Практика.

Пример из статьи: https://forum.antichat.ru/thread309017.html

1. Устанавливаем специальный дистрибутив ***BackTrack Linux или Kali Linux.***
2. Используем WiFi адаптер из списка поддерживаемых.
3. Сканируем доступные сети командой:
   root@bt:~# airodump-ng mon0
4. WEP сети взламываются сразу.
5. Если WEP сетей нет, пробуем атаковать WPA/WPA2:

- получаем фрэймы рукопожатия (команда root@bt:~# besside-ng mon0) в отдельный файл
- пробуем подобрать пароль по словарю используя сохраненные фреймы

Команда root@bt:~# aircrack-ng -e <essid> -b <bssid> -w wordlist.txt testcap.cap