ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

конспект к видеокурсу

Курсы-по-ИТ.рф | Автор: Скоромнов Дмитрий Анатольевич
Версия 1.10

Оглавление

Основы 7
Измерения 9
Сетевые обозначения 11
Модель OSI 12
Прикладной уровень 16
Представления уровень 16
Сеансовый уровень 16
Транспортный уровень 17
Сетевой уровень 18
Канальный уровень 18
Физический уровень 19
Суммарная информация по модели OSI 20
Модель TCP/IP 20
Инкапсуляция 21
Витая пара 21
История 22
Виды кабеля, применяемого в сетях 22
Экранирование витой пары 23
Конструкция витопарного кабеля 24
Категории кабеля 25
Схемы обжима 28
Монтаж 29
Оптическое волокно 29
История 29
Материалы 30
Конструкция 30
Классификация 31
Топологии сетей 32
Технологии передачи данных 35
PLC (Power Line Communication) – связь через линии электропередачи (ЛЭП) 35
xDSL 36
PON 37
Ethernet 38

История ... 39
Технология ... 39
Разновидности ... 40
Домен коллизий и широковещательный домен ... 44
Домен коллизий ... 44
Широковещательный домен ... 44
Сравнение домена коллизий и широковещательного домена ... 45
Протокол ARP ... 45
Способы доступа к среде ... 46
TDMA ... 46
CSMA/CD ... 46
CSMA/CA ... 47
Коммутация каналов и коммутация пакетов ... 48
Коммутация ... 49
Петля коммутации и протокол STP ... 49
STP ... 49
Эволюция и расширения ... 52
PoE ... 53
Определение подключения ... 54
Классификация ... 55
Подача полного напряжения ... 56
Отключение ... 56
Passive PoE ... 56
Особенности ... 56
Виды коммутаторов ... 57
Протокол IP ... 57
Введение ... 57
IP-адрес ... 58
TTL ... 58
Фрагментация ... 58
MTU ... 59
QoS ... 62
IP-адресация (введение) ... 62
Перевод из двоичной системы счисления в десятичную ... 64
Перевод из десятичной системы в двоичную ... 64
Классовая и бесклассовая адресации ... 65

Классовая адресация ... 65
Бесклассовая адресация ... 67
Возможные маски ... 67
Расчет IP-адресации в двоичном виде ... 68
Расчет количества подсетей и узлов ... 69
Виды IP-адресов ... 70
IP-адресация (IPv6) ... 70
DNS ... 72
Ключевые характеристики DNS ... 73
Проблемы с безопасностью ... 74
Терминология и принципы работы ... 74
Записи DNS ... 77
Динамический DNS ... 78
Настройки IP-адресации ... 79
Маршрутизация ... 79
Протоколы маршрутизации ... 81
Дистанционно-векторная маршрутизация ... 81
Протоколы состояния каналов связи ... 81
Классификация ... 81
Популярные протоколы ... 82
RIP ... 82
OSPF ... 83
BGP ... 83
Трассировка ... 84
Таблица маршрутизации ... 85
DHCP ... 86
Коммутация-2 ... 89
VLAN ... 89
Протоколы UDP и DCCP ... 91
UDP ... 91
Структура пакета ... 91
Надежность и решения проблемы перегрузок ... 93
DCCP ... 94
Протокол TCP ... 94
Механизм действия протокола ... 95
Заголовок сегмента TCP ... 98

Протокол SCTP ... 98
Безопасное установление соединения ... 99
Поэтапное завершение передачи данных ... 99
Многопоточность ... 100
Безопасность ... 101
Обработка ошибок ... 101
Сравнение возможностей протоколов транспортного уровня ... 102
Сокет ... 102
Порт ... 102
Сокет ... 102
VPN ... 104
AAA ... 104
Классификация VPN ... 105
NAT ... 107
Source NAT ... 108
Destination NAT ... 109
Примеры сложных задач на базе NAT ... 109
Задача № 1 ... 109
Задача № 2 ... 110
Беспроводные сети ... 111
Введение ... 111
Bluetooth ... 111
1G ... 112
2G ... 113
3G ... 113
4G ... 113
5G ... 115
Математика и физика ... 117
Основы Wi-Fi ... 118
История ... 118
Принцип работы ... 119
IEEE 802.11 ... 119
Методы аутентификации ... 123
Методы шифрования ... 124
WPS ... 125
Государственное регулирование в сфере радиочастот в РФ ... 126

Wi-Fi 802.11n и 802.11ac 126
Wi-Fi 802.11n 126
802.11ac 127
Сравнение SISO, MIMO и MU-MIMO 128
Антенны 129
Wi-Fi в жизни 129
Брандмауэр 130
Виды брандмауэров 130
Классификация межсетевых экранов 131
Реализация 133
Ограниченность анализа межсетевого экрана 134
IDS и IPS 134
Пакетные фильтры 135
Гостевая сеть и DMZ 136
Гостевая сеть 136
DMZ 137
Распространенные сетевые атаки 138
Основы сетевой и информационной безопасности 138
Три концепции безопасности 138
Анализ эффективности затрат 139
Классификация активов 139
Протокол Traffic Light 140
Классификация уязвимостей 140
Классификация контрмер 140
Потенциальные атакующие 141
Методы атак 141
Направление атаки 141
Распространенные атаки 141
Классификация атак 141
Краткое описание некоторых сетевых атак 144
Технологии обнаружения атак 146
Социальная инженерия 148
Сетевое оборудование и его выбор 153
Командная строка Windows 154
Диагностика сетевых проблем 154
Идеология работы инженера 154

Основные принципы 155
Что дальше 155

Основы

Типы сетей:

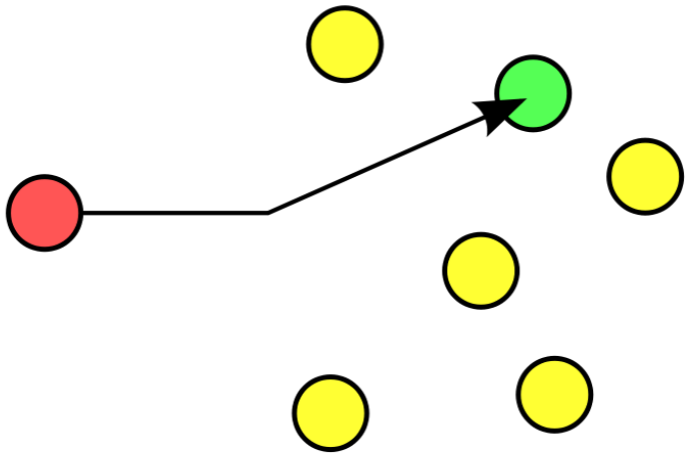
- **PAN** (англ. Personal Area Network) – персональная сеть. Пример: Bluetooth-гарнитура, подключенная к телефону;
- **LAN** (англ. Local Area Network) – локальная вычислительная сеть. Сеть, сосредоточенная на небольшой территории (обычно в радиусе 1–2 км). В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации;
- **CAN** (англ. Campus Area Network) – кампусная сеть. Похожа на LAN, но в больших масштабах. Например, сеть большого университета, у которого много зданий;
- **MAN** (англ. Metropolitan area network) – сеть большого города. Предназначена для обслуживания территории крупного города – мегаполиса;
- **WAN** (англ. Wide Area Network) – глобальная компьютерная сеть. Объединяет территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах.

Компоненты LAN:

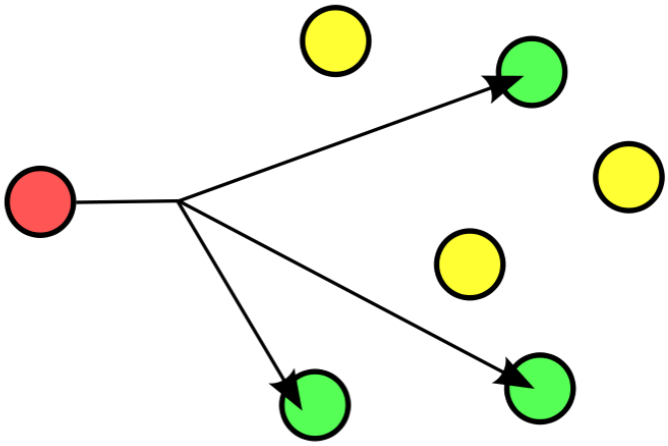
- **хосты** – компьютеры, серверы, принтеры. Хост – это любое устройство, которому может быть назначен IP-адрес;
- **устройства соединения** – сетевые карты;
- **сетевые устройства** – коммутаторы, маршрутизаторы;
- **протоколы** – ARP, DNS, Ethernet, IP.

Схемы передачи данных:

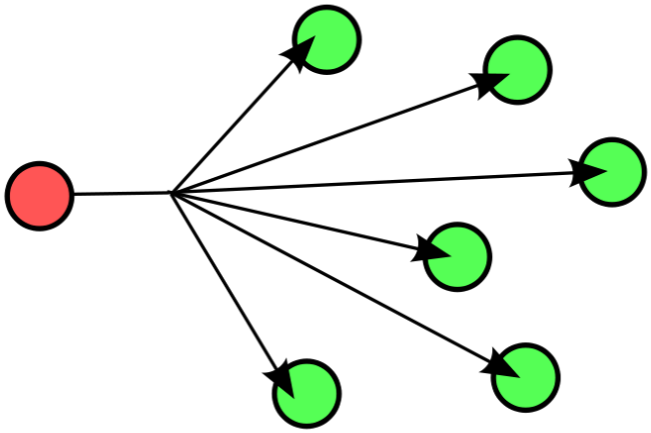
- **однонаправленное вещание** (англ. unicast) – один одному:



- **многоадресное вещание** (англ. multicast) – один многим:



- **широковещание** (англ. broadcasting) – один всем:



Режимы связи:

- **симплекс** – информация всегда передается только в одном направлении. Такая связь используется в радио-, теле- и спутниковом вещании, поскольку нет необходимости передавать какие-либо данные обратно на радиопередающую станцию;
- **полудуплекс** – информация в один момент времени может либо передаваться, либо приниматься. Пример полудуплексной связи – разговор по рации: каждый из корреспондентов в один момент времени либо говорит, либо слушает. Для обозначения конца передачи и перехода в режим приема корреспондент произносит слово «прием» (англ. over);
- **дуплекс** – информация может одновременно и передаваться, и получаться. Пример дуплексной связи – разговор двух людей (корреспондентов) по городскому телефону: каждый из говорящих в один момент времени может и говорить, и слушать своего корреспондента. Дуплексный способ связи иногда называют полнодуплексным (от англ. full-duplex); это синонимы.

Виды оборудования:

- **Активное оборудование** – это оборудование, содержащее электронные схемы, получающее питание от электрической сети или других источников и выполняющее функции усиления, преобразования сигналов и иные (ГОСТ Р 51513-99). Примеры: сетевая карта, коммутатор, маршрутизатор, точка доступа Wi-Fi и др.
- **Пассивное сетевое оборудование** – это оборудование, не получающее питание от электрической сети или других источников и выполняющее функции распределения или снижения уровня сигналов (ГОСТ Р 51513-99). Примеры: кабель, вилка, розетка, патч-панель и др.

Регулирующие организации:

- Международная организация по стандартизации (International Organization for Standardization, ISO);
- Институт инженеров электротехники и электроники (Institute of Electrical and Electronics Engineers, IEEE);
- Рабочее предложение (Request for Comments, RFC) – документы, содержащие технические спецификации и стандарты, широко применяемые во Всемирной сети.

Измерения

Международная система единиц (СИ)

Система единиц физических величин, современный вариант метрической системы. СИ является наиболее широко используемой системой единиц в мире, как в повседневной жизни, так и в науке и технике. В настоящее время СИ принята в качестве основной системы единиц большинством стран мира и почти всегда используется в области техники, даже в тех странах, в которых в повседневной жизни используются традиционные единицы. В этих немногих странах (например, в США) определения традиционных единиц были изменены таким образом, чтобы связать их фиксированными коэффициентами с соответствующими единицами СИ.

Полное официальное описание СИ вместе с ее толкованием содержится в действующей редакции Брошюры СИ (фр. Brochure SI, англ. The SI Brochure) и Дополнении к ней, опубликованных Международным бюро мер и весов (МБМВ) и представленных на сайте МБМВ. Брошюра СИ издается с 1970 года, с 1985 года выходит на французском и английском языках, переведена также на ряд других языков, однако официальным считается текст только на французском языке.

Строгое определение СИ формулируется таким образом: «Международная система единиц (СИ) – система единиц, основанная на Международной системе величин, вместе с наименованиями и обозначениями, а также набором приставок, их наименованиями и обозначениями вместе с правилами их применения, принятая Генеральной конференцией по мерам и весам (CGPM)».

Десятичный множитель	Приставка		Обозначение		Пример
	русская	международная	русское	международное	
10^1	дека	deca	да	da	дал – декалитр
10^2	гекто	hecto	г	h	гПа – гектопаскаль
10^3	кило	kilo	к	k	кН – килоньютон
10^6	мега	mega	М	M	Мпа – мегапаскаль
10^9	гига	giga	Г	G	ГГц – гигагерц
10^{12}	тера	tera	Т	T	ТВ – теравольт
10^{15}	пета	peta	П	P	Пфлопс – петафлопс
10^{18}	экса	exa	Э	E	Эм – эксаметр
10^{21}	зетта	zetta	З	Z	ЗВ – зеттавольт
10^{24}	иотта	yotta	И	Y	Иг – иоттаграмм

Желательно знать наизусть:

- кило = 10^3 = 1000;
- мега = 10^6 = 1 000 000;
- гига = 10^9 = 1 000 000 000;
- тера = 10^{12} = 1 000 000 000 000.

Скорости передачи данных:

- килобиты в секунду – Кбит/с (kbps, kbit/s или kb/s);
- мегабиты в секунду – Мбит/с (Mbps, Mbit/s или Mb/s);
- гигабиты в секунду – Гбит/с (Gbps, Gbit/s или Gb/s).

Биты и байты:

- 1 байт = 8 бит
- 100 Мбит/с (мегабит в секунду) = 12,5 МБайт/с (мегабайт в секунду)
- 1 Гбит/с (гигабит в секунду) = 125 МБайт/с (мегабайт в секунду)

- 1 килобайт = $1024^1 = 2^{10}$ = 1024 байта
- 1 мегабайт = $1024^2 = 2^{20}$ = 1 048 576 байт
- 1 гигабайт = $1024^3 = 2^{30}$ = 1 073 741 824 байта
- 1 терабайт = $1024^4 = 2^{40}$ = 1 099 511 627 776 байт

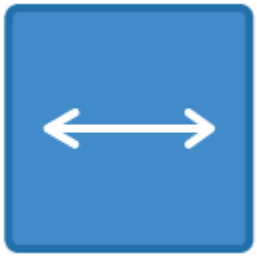
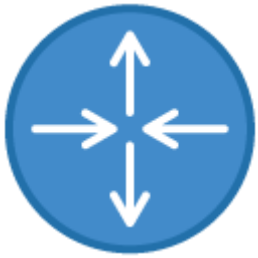
С обозначениями может возникнуть путаница:

- часто путают MB/s и Mb/s (1 MB/s = 8 Mb/s), поэтому рекомендуется использовать сокращение Mbit/s;
- ГОСТ 8.417-2002 предусматривает обозначение битов без сокращения;
- используем: ГБ/с (гигабайт в секунду) и Гбит/с (гигабит в секунду);
- имеем в виду, что «б» может использоваться как «бит»: Гб/с (гигабит в секунду);
- в англоязычной терминологии допускается использование «b» как «bit»: Mbps, Mb/s и др.

Онлайн-конвертер битов в байты: http://курсы-по-ит.рф/tools/bit-to-byte-converter.

Сетевые обозначения

В этом разделе приведены сетевые обозначения. Обозначения не закреплены каким-то стандартом, но являются общепринятыми.

Интернет, сеть	Концентратор 	Модем
Коммутатор L2	Коммутатор L3	Маршрутизатор 
Файрвол	Точка доступа Wi-Fi однодиапазонная	Точка доступа Wi-Fi двухдиапазонная
Общее обозначение	Компьютер	Компьютер

Модель OSI

Изначально оборудование и протоколы разных вендоров не могли работать друг с другом из-за несовместимости. Для устранения этой проблемы было решено ввести общие стандарты. Одним из таких нововведений стали эталонные модели, которые должны были описывать, что должно быть в сети, и состоять из нескольких уровней, и в них должно было быть описание, что именно работает на каждом уровне.

Наибольшее распространение получили открытые системы, т.к. они состояли из общедоступных спецификаций. Использование именно открытых систем позволило всем производителям привести свое оборудование к общему стандарту. Также появилась возможность объединения разных сетей и возможность замены отдельных элементов сети на другие элементы другого производителя.

Большое распространение получила сетевая модель OSI. Сетевая модель OSI (англ. open systems interconnection basic reference model «базовая эталонная модель взаимодействия открытых систем» (ЭМВОС)) – сетевая модель стека сетевых протоколов OSI/ISO (ГОСТ Р ИСО/МЭК 7498-1-99). Посредством данной модели различные сетевые устройства могут взаимодействовать друг с другом. Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определенные функции при таком взаимодействии.

Наиболее часто принято начинать описание уровней модели OSI с 7-го уровня, называемого прикладным, на котором пользовательские приложения обращаются к сети. Модель OSI заканчивается 1-м уровнем – физическим.

Любой протокол модели OSI должен взаимодействовать либо с протоколами своего уровня, либо с протоколами на единицу выше и/или ниже своего уровня. Взаимодействия с протоколами своего уровня называются горизонтальными, а с уровнями на единицу выше или ниже – вертикальными. Любой протокол модели OSI может выполнять только функции своего уровня и не может выполнять функций другого уровня, что не выполняется в протоколах альтернативных моделей.

- 7 – прикладной (Application)
- 6 – представления (Presentation)
- 5 – сеансовый (Session)
- 4 – транспортный (Transport)
- 3 – сетевой (Network)
- 2 – канальный (Data Link)
- 1 – физический (Physical)

Каждому уровню с некоторой долей условности соответствует свой операнд – логически неделимый элемент данных, которым на отдельном уровне можно оперировать в рамках модели и используемых протоколов: на физическом уровне мельчайшая единица – бит, на канальном уровне информация объединена в кадры, на сетевом – в пакеты, на транспортном – в сегменты или дейтаграммы. Любой фрагмент данных, логически объединенных для передачи, – кадр, пакет, дейтаграмма – считается сообщением. Именно сообщения в общем виде являются операндами сеансового, представительского и прикладного уровней.

Уровень	**Тип данных**	**Назначение**
7. Прикладной	Сообщение (данные)	Доступ к сетевым службам
6. Представления	Сообщение (данные)	Представление и шифрование данных
5. Сеансовый	Сообщение (данные)	Управление сеансом связи
4. Транспортный	Сегмент/дейтаграмма	Прямая связь между конечными пунктами и надежность
3. Сетевой	Пакет	Определение маршрута и логическая адресация
2. Канальный	Кадр (фрейм)	Физическая адресация
1. Физический	Бит	Работа со средой передачи, сигналами и двоичными данными

Прикладной уровень

Прикладной уровень (уровень приложений; англ. application layer) – верхний уровень модели, обеспечивающий взаимодействие пользовательских приложений с сетью:

- позволяет приложениям использовать сетевые службы:
    - удаленный доступ к файлам и базам данных,
    - пересылку электронной почты;
- отвечает за передачу служебной информации;
- предоставляет приложениям информацию об ошибках;
- формирует запросы к уровню представления.

Протоколы прикладного уровня: RDP, HTTP, SMTP, SNMP, POP3, FTP, XMPP, OSCAR, SIP, TELNET и другие.

Уровень представления

Уровень представления (англ. presentation layer) обеспечивает преобразование протоколов и кодирование/декодирование данных. Запросы приложений, полученные с прикладного уровня, на уровне представления преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат приложений. На этом уровне может осуществляться сжатие/распаковка или шифрование/дешифрование, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально.

Сеансовый уровень

Сеансовый уровень (англ. session layer) модели обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений.

Протоколы сеансового уровня: ADSP (AppleTalk Data Stream Protocol), ASP (AppleTalk Session Protocol), H.245 (Call Control Protocol for Multimedia Communication), ISO-SP (OSI Session Layer Protocol (X.225, ISO 8327)), iSNS (Internet Storage Name Service), NetBIOS (Network Basic Input Output System), PAP (Password Authentication Protocol), PPTP (Point-to-Point Tunneling Protocol), RPC (Remote Procedure Call Protocol), RTCP (Real-time Transport Control Protocol), SMPP (Short Message Peer-to-Peer), SCP (Session Control Protocol), ZIP (Zone Information Protocol), SDP (Sockets Direct Protocol) и др.

Транспортный уровень

Транспортный уровень (англ. transport layer) модели предназначен для обеспечения надежной передачи данных от отправителя к получателю. При этом уровень надежности может варьироваться в широких пределах.

Протоколы транспортного уровня: ATP (AppleTalk Transaction Protocol), CUDP (Cyclic UDP), DCCP (Datagram Congestion Control Protocol), FCP (Fiber Channel Protocol), IL (IL Protocol), NBF (NetBIOS Frames protocol), NCP (NetWare Core Protocol), SCTP (Stream Control Transmission Protocol), SPX (Sequenced Packet Exchange), SST (Structured Stream Transport), TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

Сетевой уровень

Сетевой уровень (англ. network layer) модели предназначен для определения пути передачи данных и отвечает за определение кратчайших маршрутов.

Протоколы сетевого уровня маршрутизируют данные от источника к получателю. Работающие на этом уровне устройства (маршрутизаторы) условно называют устройствами третьего уровня (по номеру уровня в модели OSI).

Пример оборудования: маршрутизатор.

Протоколы сетевого уровня: IP/IPv4/IPv6 (Internet Protocol), IPX (Internetwork Packet Exchange, протокол межсетевого обмена), X.25 (частично этот протокол реализован на уровне 2), CLNP (сетевой протокол без организации соединений), IPsec (Internet Protocol Security). Протоколы маршрутизации – RIP (Routing Information Protocol), OSPF (Open Shortest Path First).

Канальный уровень

Канальный уровень (англ. data link layer) предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля за ошибками, которые могут возникнуть. Полученные с физического уровня данные, представленные в битах, он упаковывает в кадры, проверяет их на целостность и, если нужно, исправляет ошибки (формирует повторный запрос поврежденного кадра) и отправляет на сетевой уровень. Процедура исправления ошибок часто не используется многими средами передачи данных с высокой степенью надежности доставки (Ethernet, оптическое волокно и т.д.). Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

Пример оборудования: коммутатор.

Протоколы канального уровня: ARCnet, ATM, Controller Area Network (CAN), Econet, IEEE 802.3 (Ethernet), Ethernet Automatic Protection Switching (EAPS), Fiber Distributed Data Interface (FDDI), Frame Relay, High-Level Data Link Control (HDLC), IEEE 802.2 (предоставляет функции LLC для подуровня IEEE 802 MAC), Link Access Procedures, D channel (LAPD), IEEE 802.11 wireless LAN, LocalTalk, Multiprotocol Label Switching (MPLS), Point-to-Point Protocol (PPP), Point-to-Point Protocol over Ethernet (PPPoE), Serial Line Internet Protocol (SLIP, устарел), StarLan, Token ring, Unidirectional Link Detection (UDLD), x.25, ARP.

Физический уровень

Физический уровень (англ. physical layer) – нижний уровень модели, который определяет метод передачи данных, представленных в двоичном виде, от одного устройства (компьютера) к другому. На физическом уровне осуществляется передача электрических или оптических сигналов в кабель или в радиоэфир и, соответственно, их прием и преобразование в биты данных. Составлением таких методов занимаются разные организации, в том числе: Институт инженеров по электротехнике и электронике, Альянс электронной промышленности, Европейский институт телекоммуникационных стандартов и другие.

Пример оборудования: концентратор.

Протоколы физического уровня: IEEE 802.15 (Bluetooth), IRDA, EIA RS-232, EIA-422, EIA-423, RS-449, RS-485, DSL, ISDN, SONET/SDH, 802.11 Wi-Fi, Etherloop, GSM Um radio interface, ITU и ITU-T, TransferJet, ARINC 818, G.hn/G.9960.

Прикладной уровень

Прикладной уровень (англ. Application layer) – протокол верхнего (7-го) уровня сетевой модели OSI, обеспечивает взаимодействие сети и пользователя. Уровень разрешает приложениям пользователя иметь доступ к сетевым службам, таким как обработчик запросов к базам данных, доступ к файлам, пересылке электронной почты. Также отвечает за передачу служебной информации, предоставляет приложениям информацию об ошибках и формирует запросы к уровню представления. Пример: HTTP, POP3, SMTP. Также может называться уровнем приложений.

Обеспечивает взаимодействие пользовательских приложений с сетью:

- позволяет приложениям использовать сетевые службы:
    - удаленный доступ к файлам и базам данных,
    - пересылку электронной почты;
- отвечает за передачу служебной информации;
- предоставляет приложениям информацию об ошибках;
- формирует запросы к уровню представления.

Протоколы прикладного уровня: RDP, HTTP, SMTP, SNMP, POP3, FTP, XMPP, OSCAR, Modbus, SIP, TELNET и другие.

Представления уровень

Уровень представления (англ. Presentation layer) – 6-й уровень сетевой модели OSI. Отвечает за преобразование протоколов и кодирование/декодирование данных. Запросы приложений, полученные с прикладного уровня (уровня приложений), он преобразует в формат для передачи по сети, а полученные из сети данные преобразует в формат, понятный приложениям. На этом важном уровне может осуществляться сжатие/распаковка или кодирование/декодирование данных, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально.

На представительском уровне передаваемая по сети информация не меняет содержания. С помощью средств, реализованных на данном уровне, протоколы прикладных программ преодолевают синтаксические различия в представляемых данных или же различия в кодах символов, например, согласовывая представления данных расширенного двоичного кода обмена информацией EBCDIC, используемого мейнфреймом компании IBM, с одной стороны и американского стандартного кода обмена информацией ASCII с другой.

На уровне представления реализованы следующие функции:

- преобразование данных;
- преобразование между различными наборами символов;
- сжатие данных для увеличения пропускной способности канала;
- шифрование и дешифровка.

Сеансовый уровень

Сеансовый уровень (англ. Session layer) – 5-й уровень сетевой модели OSI. Отвечает за поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений. Синхронизация передачи

обеспечивается помещением в поток данных контрольных точек, начиная с которых, возобновляется процесс при нарушении взаимодействия.

Транспортный уровень

Транспортный уровень (англ. Transport layer) – 4-й уровень сетевой модели OSI, предназначен для доставки данных. При этом не важно, какие данные передаются, откуда и куда, то есть он предоставляет сам механизм передачи. Протоколы этого уровня предназначены для взаимодействия типа «точка-точка». Пример: TCP, UDP, DCCP, SCTP.

Существует множество различных протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции, например функции передачи данных без подтверждения приема, и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности.

Некоторые протоколы транспортного уровня, называемые протоколами без установки соединения, не гарантируют, что данные доставляются по назначению в том порядке, в котором они были посланы устройством-источником. Некоторые протоколы транспортного уровня справляются с этим, собирая данные в нужной последовательности до передачи их на сеансовый уровень. Мультиплексирование (multiplexing) данных означает, что транспортный уровень способен одновременно обрабатывать несколько потоков данных (потоки могут поступать и от различных приложений) между двумя системами. Механизм управления потоком данных – это механизм, позволяющий регулировать количество данных, передаваемых от одной системы к другой. Протоколы транспортного уровня часто имеют функцию контроля доставки данных, заставляя принимающую данные систему отправлять подтверждения передающей стороне о приеме данных.

Протоколы транспортного уровня:

- **TCP** (англ. Transmission Control Protocol «протокол управления передачей»);
- **UDP** (англ. User Datagram Protocol «протокол пользовательских датаграмм»);
- **SCTP** (англ. Stream Control Transmission Protocol «протокол передачи с управлением потоком»);
- **DCCP** (англ. Datagram Congestion Control Protocol «управляющий протокол с контролем плотности датаграмм»).

Порт (англ. port) – число, записываемое в заголовках протоколов транспортного уровня модели OSI (UDP, TCP, DCCP, SCTP). Количество портов 65 536 (это 2^{16}, начало – «0»). Порты разделены на три диапазона:

- общеизвестные (системные): 0–1023;
- зарегистрированные (пользовательские): 1024–49151;
- динамические (частные): 49152–65535.

Порты разных протоколов не пересекаются.

Сетевой уровень

Сетевой уровень (англ. Network layer) – 3-й уровень сетевой модели OSI, предназначается для определения пути передачи данных. Отвечает за определение кратчайших маршрутов (маршрутизацию), отслеживание неполадок и заторов в сети. На этом уровне работает такое сетевое устройство, как маршрутизатор. Маршрутизатор работает с IP-адресами.

Канальный уровень

Канальный уровень (англ. data link layer) – второй уровень сетевой модели OSI. Уровень предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля за ошибками, которые могут возникнуть. Полученные с физического уровня данные, представленные в битах, он упаковывает в кадры, проверяет их на целостность и, если нужно, исправляет ошибки (формирует повторный запрос поврежденного кадра) и отправляет на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

Заголовок кадра содержит аппаратные адреса отправителя и получателя, что позволяет определить, какое устройство отправило кадр и какое устройство должно получить и обработать его. В отличие от иерархических и маршрутизируемых адресов, аппаратные адреса одноуровневые. Это означает, что никакая часть адреса не может указывать на принадлежность к какой-либо логической или физической группе.

Многие протоколы канального уровня не имеют подтверждения о приеме кадра, некоторые протоколы даже не имеют контрольной суммы для проверки целостности кадра. В таких случаях протоколы более высокого уровня должны обеспечивать управление потоком данных, контроль ошибок, подтверждение доставки и ретрансляции утерянных данных.

На этом уровне работают коммутаторы, мосты.

Канальный уровень состоит из двух подуровней:

1. Подуровень управления логическим каналом (LLC – Logical Link Control). В задачи LLC входит: проверка и передача данных (создание кадров, обработка ошибок), согласование скоростей. Подуровень общий для разных технологий.
2. Подуровень управления доступом к среде (MAC – Media Access Control). В задачи MAC входит совместное использование разделяемой среды, адресация. Подуровень не является обязательным и может иметь специфику для разных технологий.

MAC-адрес

MAC-адрес (от англ. Media Access Control «управление доступом к среде», также Hardware Address «аппаратный адрес») – уникальный идентификатор, присваиваемый сетевому интерфейсу в сетях Ethernet. Длина – 48 бит. Записывается в виде 12-значного шестнадцатеричного числа. Могут быть использованы значения: 0–9 и A–F. Может записываться с большой и маленькой букв, через дефис или двоеточие и без них.

Примеры записи:

- 38-63-BB-CC-FA-55;
- 38:63:BB:CC:FA:55;
- 3863BBCCFA55;
- 38-63-bb-cc-fa-55.

Первые 6 знаков – идентификатор производителя, следующие 6 знаков – идентификатор устройства.

Зарезервированный MAC-адрес: FF:FF:FF:FF:FF:FF – широковещательный адрес.

При проектировании стандарта Ethernet было предусмотрено, что каждая сетевая карта (равно как и встроенный сетевой интерфейс) должна иметь уникальный шестибайтный номер (MAC-адрес), прошитый в ней при изготовлении. Этот номер используется для идентификации отправителя и получателя кадра, и предполагается, что при появлении в сети нового компьютера (или другого устройства, способного работать в сети) сетевому администратору не придется настраивать MAC-адрес.

Уникальность MAC-адресов достигается тем, что каждый производитель получает в координирующем комитете IEEE Registration Authority диапазон из шестнадцати миллионов (2^{24}) адресов и по мере исчерпания выделенных адресов может запросить новый диапазон. Поэтому по трем старшим байтам MAC-адреса можно определить производителя. Существуют таблицы, позволяющие определить производителя по MAC-адресу (в частности, они включены в программы типа arpalert).

MAC-адрес считывается один раз из ПЗУ при инициализации сетевой карты, в дальнейшем все кадры генерируются операционной системой. Все современные операционные системы позволяют поменять его. Для Windows, начиная как минимум с Windows 98, он менялся в реестре. Некоторые драйверы сетевых карт давали возможность изменить его в настройках, но смена работает для абсолютно любых карт.

Некоторое время назад, когда драйверы сетевых карт не давали возможности изменить свой MAC-адрес, а альтернативные возможности не были слишком известны, некоторые провайдеры Internet использовали его для идентификации машины в сети при учете трафика. Программы из Microsoft Office, начиная с версии Office 97, записывали MAC-адрес сетевой платы в редактируемый документ в качестве составляющей уникального GUID-идентификатора.

Физический уровень

Физический уровень (англ. physical layer) – первый уровень сетевой модели OSI. Уровень работает с физической и электрической средами передачи данных. Физический уровень описывает способы передачи битов (а не пакетов данных) через физические среды линий связи, соединяющие сетевые устройства. На этом уровне описываются параметры сигналов, такие как амплитуда, частота, фаза, используемая модуляция, манипуляция. Решаются вопросы, связанные с синхронизацией, избавлением от помех, скоростью передачи данных.

Если посмотреть с той точки зрения, что сеть включает в себя оборудование и программы, контролирующие оборудование, то здесь физический слой будет относиться именно к первой части определения.

Примеры оборудования, работающего на физическом уровне: концентратор, медная витая пара, оптический кабель.

Суммарная информация по модели OSI

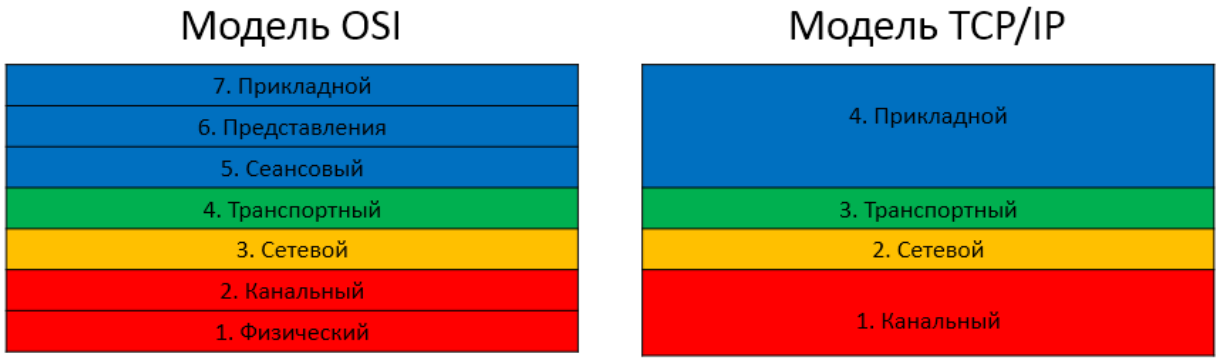
Уровень	Тип данных	Назначение
7. Прикладной	Сообщение (данные)	Доступ к сетевым службам
6. Представления	Сообщение (данные)	Представление и шифрование данных
5. Сеансовый	Сообщение (данные)	Управление сеансом связи
4. Транспортный	Сегмент/дейтаграмма	Прямая связь между конечными пунктами и надежность
3. Сетевой	Пакет	Определение маршрута и логическая адресация
2. Канальный	Кадр (фрейм)	Физическая адресация
1. Физический	Бит	Работа со средой передачи, сигналами и двоичными данными

Модель TCP/IP

TCP/IP – сетевая модель передачи данных, представленных в цифровом виде. Модель описывает способ передачи данных от источника информации к получателю. В модели предполагается прохождение информации через четыре уровня, каждый из которых описывается правилом (протоколом передачи). Наборы правил, решающих задачу по передаче данных, составляют стек протоколов передачи данных, на которых базируется Интернет. Название «TCP/IP» происходит от двух важнейших протоколов семейства – Transmission Control Protocol (TCP) и Internet Protocol (IP), которые первыми были разработаны и описаны в данном стандарте. Также изредка упоминается как модель DOD в связи с историческим происхождением от сети ARPANET из 1970-х годов (под управлением DARPA, Министерства обороны США).

Модель TCP/IP ≠ стек протоколов TCP/IP.

Сравнение модели TCP/IP с моделью OSI:

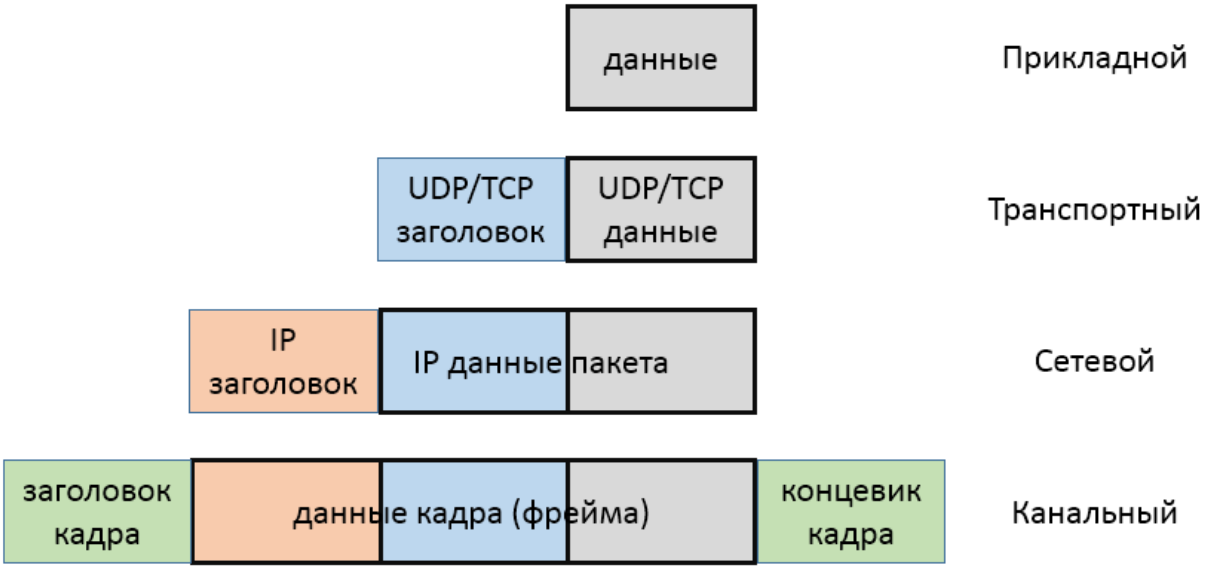


Модель для практического применения сетевыми администраторами:

Инкапсуляция

Инкапсуляция – это метод построения модульных сетевых протоколов, при котором логически независимые функции сети абстрагируются от нижележащих механизмов путем включения этих механизмов в более высокоуровневые объекты.

Инкапсуляция в TCP/IP:



Витая пара

Витая пара (англ. twisted pair) – вид кабеля связи. Представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой.

Свивание проводников производится с целью повышения степени связи между собой проводников одной пары (электромагнитные помехи одинаково влияют на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а также взаимных наводок при передаче дифференциальных сигналов. Для снижения связи отдельных пар кабеля (периодического сближения проводников различных пар) в кабелях UTP категории 5 и выше провода пары свиваются с различным шагом. Витая пара – один из компонентов

современных структурированных кабельных систем. Используется в телекоммуникациях и в компьютерных сетях в качестве физической среды передачи сигнала во многих технологиях, таких как Ethernet, Arcnet, Token Ring, USB. В настоящее время, благодаря своей дешевизне и легкости монтажа, является самым распространенным решением для построения проводных (кабельных) локальных сетей.

Кабель подключается к сетевым устройствам при помощи разъема 8P8C (который ошибочно называют RJ45).

История

Первые телефоны использовали телеграфные линии или однопроводные линии с цепью заземления, проложенные открытым способом. В 1880 году во многих городах были пущены электрические трамваи, которые наводили много шумов на эти линии. Судиться было бесполезно, и телефонные компании переделали свои линии в сбалансированную схему, имевшую дополнительную выгоду, заключавшуюся в снижении затухания сигнала.

Когда линии электропередачи стали более распространенным явлением, этой меры оказалось недостаточно. Телеграфные провода шли параллельно с линиями электропередачи, и в течение нескольких лет растущее использование электроэнергии снова принесло увеличение помех, поэтому инженеры разработали метод транспозиции проводов, чтобы свести на нет помехи.

В транспозиции проводов их положение менялось через определенное количество опор. Таким образом, два провода сбалансированной пары получали аналогичные помехи от линий электропередачи. Это представляло собой раннюю реализацию скручивания с шагом транспозиции проводов около четырех перекрестий на километр, или шесть на милю. Такие открытые симметричные линии с периодическими транспозициями дожили до наших дней в некоторых сельских районах.

Витая пара была изобретена Александром Грейамом Беллом в 1881 году. К 1900 году вся американская сеть телефонных линий была или на витой паре, или на открытых проводах с транспозицией для защиты от помех.

Виды кабеля, применяемого в сетях

В защите нуждаются как сигналы, передаваемые по кабелю, так и элементы конструкции кабеля. Защитные элементы разделяют в зависимости от назначения:

- химическая защита – защита кабеля от внешних воздействий (почвы, воды, газов, солнечного света);
- механическая защита – защита кабеля от механических повреждений;
- экранирование – защита сигнала от помех (от внешних и внутренних электромагнитных наводок).

Защитные элементы продлевают срок службы кабеля.

Для механической защиты провода используют особо прочные оболочки и оплетку из медной проволоки. Оболочка из черного полиэтилена защищает кабель от солнечного света (специальная защита, применяемая для кабелей, предназначенных для прокладки на открытом воздухе). Кабели, имеющие дополнительные слои защиты, называют термином «double jacket».

Для химической защиты кабеля используют фольгу и полиэтилен. Кабели, защищенные фольгой, обозначают термином «foiled» – «фольгированные».

Алюминиевая фольга и медная оплетка также используются для экранирования кабеля и отдельных пар для дополнительной защиты от электромагнитных помех.

По числу проволок (числу жил) провода разделяют на:

- одножильные, однопроволочные – провода, состоящие из одной медной проволоки (одной жилы);
- многожильные, многопроволочные – провода, состоящие из нескольких жил.

Однопроволочный кабель не предполагает прямых контактов с подключаемой периферией. То есть, как правило, его применяют для прокладки в коробах, стенах и т.д. с последующим терминированием розетками. Связано это с тем, что медные жилы довольно толсты и при частых изгибах быстро ломаются. Однако для «врезания» в разъемы панелей розеток такие жилы подходят как нельзя лучше.

Многопроволочный кабель плохо переносит «врезание» в разъемы панелей розеток (тонкие жилы разрезаются), но замечательно ведет себя при изгибаниях и скручивании. Кроме того, многопроволочный провод обладает бóльшим затуханием сигнала. Поэтому многопроволочный кабель используют в основном для изготовления патч-кордов (англ. patchcord), соединяющих периферию с розетками.

Экранирование витой пары

Общая классификация:

- UTP (англ. Unshielded Twisted Pair) – неэкранированная витая пара;
- STP (англ. Shielded Twisted Pair) – экранированная витая пара.

Для защиты от электрических помех при использовании высокочастотных сигналов в кабелях категорий 6a–8 используется экранирование. Экранирование применяется как к отдельным витым парам, которые оборачиваются в алюминиевую фольгу (металлизированную алюминием полиэтиленовую ленту), так и к кабелю в целом в виде общего экрана из фольги и/или оплетки из медной проволоки. Экран также может быть соединен с неизолированным дренажным проводом, который служит для заземления и механически поддерживает экран в случае разделения на секции при излишнем изгибании или растяжении кабеля.

Согласно международному стандарту ISO/IEC 11801 (приложение E), для обозначения конструкции экранированного кабеля используется комбинация из трех букв. Вариант букв:

- U – unshielded, без экрана;
- F – foil, фольга;
- S – braided screening, оплетка из проволоки (только внешний экран);
- TP – twisted pair, витая пара;
- TQ – индивидуальный экран для двух витых пар (на 4 провода).

Из этих букв формируется аббревиатура вида xx/xTP, обозначающая тип общего экрана и тип экрана для отдельных пар.

- Неэкранированный кабель (U/UTP) – экранирование отсутствует. Категория 6 и ниже.
- Индивидуальный экран (U/FTP) – экранирование фольгой каждой отдельной пары. Защищает от внешних помех и от перекрестных помех между витыми парами.
- Общий экран (F/UTP, S/UTP, SF/UTP) – общий экран из фольги, оплетки или фольги с оплеткой. Защищает от внешних электромагнитных помех.

- Индивидуальный и общий экран (F/FTP, S/FTP, SF/FTP) – индивидуальные экраны из фольги для каждой витой пары плюс общий экран из фольги, оплетки или фольги с оплеткой. Защищает от внешних помех и от перекрестных помех между витыми парами.

Экранированные кабели категорий 5e, 6/6A и 8/8.1 чаще всего используют конструкцию F/UTP (общий экран из фольги), тогда как экранированные кабели категорий 7/7A и 8.2 используют конструкцию S/FTP (с общей металлической оплеткой и фольгой для каждой пары).

Обозначения для распространенных типов кабелей из витых пар

Общепринятое название	Обозначение по ISO/IEC 11801	Общий экран	Экран для пар
UTP	U/UTP	Нет	Нет
STP, ScTP, PiMF	U/FTP	Нет	Фольга
FTP, STP, ScTP	F/UTP	Фольга	Нет
STP, ScTP	S/UTP	Оплетка	Нет
SFTP, S-FTP, STP	SF/UTP	Оплетка, фольга	Нет
FFTP	F/FTP	Фольга	Фольга
SSTP, SFTP, STP PiMF	S/FTP	Оплетка	Фольга
SSTP, SFTP	SF/FTP	Оплетка, фольга	Фольга

Конструкция витопарного кабеля

Витопарный кабель состоит из нескольких витых пар. Проводники в парах изготовлены из монолитной медной проволоки толщиной 0,4–0,6 мм либо из множества более тонких проводников (кабель получается более гибкий и обычно используется в патч-кордах). Кроме метрической, применяется американская система AWG, в которой эти величины составляют 26–22 AWG. В стандартных 4‑парных кабелях в основном используются проводники диаметром 0,51 мм (24 AWG). Толщина изоляции проводника – около 0,2 мм. Материал изоляции – обычно поливинилхлорид (ПВХ, англ. PVC), для более качественных образцов 5 категории – полипропилен (ПП, англ. PP), полиэтилен (ПЭ, англ. PE). Особенно высококачественные кабели имеют изоляцию из вспененного (ячеистого) полиэтилена, который обеспечивает низкие диэлектрические потери, или тефлона, обеспечивающего широкий рабочий диапазон температур.

Также внутри кабеля иногда встречается так называемая разрывная нить (обычно капрон), которая используется для облегчения разделки внешней оболочки – при вытягивании она делает на оболочке продольный разрез, который открывает доступ к кабельному сердечнику, гарантированно не повреждая изоляцию проводников. Также разрывная нить, ввиду своей высокой прочности на разрыв, выполняет защитную функцию.

Внешняя оболочка 4‑парных кабелей имеет толщину 0,5–0,9 мм в зависимости от категории кабеля и обычно изготавливается из поливинилхлорида с добавлением мела, который повышает хрупкость. Это необходимо для точного облома по месту надреза лезвием отрезного инструмента. Для изготовления оболочки могут использоваться полимеры, которые не распространяют горения при групповой прокладке и не выделяют при нагреве галогены (такие кабели маркируются аббревиатурой LSZH (англ. low smoke zero halogen «малой дымности, не выделяющий галогенов»); российская маркировка: нг(A)-HF, нг(B)-HF, нг(C)-HF, нг(D)-HF). Кабели, не поддерживающие горение и не выделяющие дым, по европейским стандартам разрешается прокладывать и использовать в закрытых областях, где могут проходить воздушные потоки системы кондиционирования и вентиляции (так называемых пленум-областях). Кабели для внешней прокладки поверх поливинилхлоридной оболочки имеют оболочку из полиэтилена для защиты от солнечного излучения. Эти кабели распространяют горение даже при одиночной прокладке. Открытая прокладка таких кабелей в зданиях и сооружениях запрещена.

В общем случае цвета не обозначают особых свойств, но их применение позволяет легко отличать коммуникации с разным функциональным назначением, как при монтаже, так и в обслуживании. Самый распространенный цвет оболочки кабелей – серый. У внешних кабелей внешняя оболочка черного цвета. Оранжевая окраска, как правило, указывает на негорючий материал оболочки.

Отдельно нужно отметить маркировку. Маркировка на кабеле в бухтах, кроме данных о производителе и типе кабеля, обязательно включает в себя метровые или футовые метки. Эти метки позволяют узнать длину уже проложенного закрытым способом кабеля. Маркировка патч-кордов не включает в себя метки о длине.

Форма внешней оболочки кабеля «витая пара» может быть различной. Чаще других применяется круглая форма. Для прокладки под ковровым покрытием может использоваться плоский кабель. В плоском кабеле провода также скручены в пары, однако пары не скручены вокруг общей оси. В результате плоский кабель более подвержен влиянию помех.

Кабели для наружной прокладки обязательно имеют влагостойкую оболочку из полиэтилена, которая наносится (как правило) вторым слоем поверх обычной, поливинилхлоридной. Кроме этого, возможно заполнение пустот в кабеле водоотталкивающим гелем и бронирование с помощью гофрированной ленты или стальной проволоки.

Категории кабеля

Существует несколько категорий кабеля «витая пара», которые нумеруются от 1 до 7 и определяют эффективный пропускаемый частотный диапазон. Кабель более высокой категории обычно содержит больше пар проводов, и каждая пара имеет больше витков на единицу длины. Категории неэкранированной витой пары описываются в стандарте EIA/TIA 568 (Американском стандарте проводки в коммерческих зданиях) и в международном стандарте ISO 11801, а также в ГОСТ Р 53246-2008 и ГОСТ Р 53245-2008.

Категория	Полоса частот, МГц	Применение	Примечания
1	0,1	Телефонные и старые модемные линии	1 пара, не описан в рекомендациях EIA/TIA для передачи данных (в России применяется кабель и вообще без скруток – *лапша*, у него характеристики не хуже, но больше влияние помех). В США использовался ранее, только в скрученном виде. Используется только для передачи голоса или данных при помощи модема (не подходит для современных систем)
2	1	Старые терминалы (такие как IBM 3270)	2 пары проводников, старый тип кабеля, не описан в рекомендациях EIA/TIA для передачи данных, поддерживал передачу данных на скоростях до 4 Мбит/с, использовался в сетях Token ring и Arcnet (не подходит для современных систем). Сейчас иногда встречается в телефонных сетях
3	16	10BASE-T, 100BASE-T4 Ethernet	4-парный кабель, используется при построении телефонных и локальных сетей 10BASE-T и token ring, поддерживает скорость передачи данных до 10 Мбит/с или 100 Мбит/с по технологии 100BASE-T4 на расстояние не дальше 100 метров. В отличие от предыдущих двух, отвечает требованиям стандарта IEEE 802.3. Сейчас используется в основном для телефонных линий
4	20	Token Ring	Кабель состоит из 4 скрученных пар, использовался в сетях token ring, 10BASE-T, 100BASE-T4, скорость передачи данных не превышает 16 Мбит/с по одной паре
5	100	Fast Ethernet (100BASE-TX), Gigabit Ethernet (1000BASE-T)	4-парный кабель, используется при построении локальных сетей 10BASE-T, 100BASE-TX и 1000BASE-T и для прокладки телефонных линий, поддерживает скорость передачи данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар

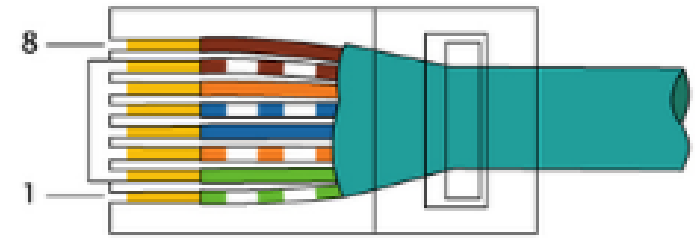
5e	100	Fast Ethernet (100BASE-TX), Gigabit Ethernet (1000BASE-T)	4-парный кабель, усовершенствованная категория 5 (уточненные/улучшенные спецификации). Скорость передачи данных: до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар. Кабель категории 5e является самым распространенным и используется для построения компьютерных сетей. Иногда встречается двухпарный кабель категории 5e. Преимущества данного кабеля в более низкой себестоимости и меньшей толщине
6	250	10 Gigabit Ethernet (10GBASE-T)	Неэкранированный кабель (UTP) состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с на расстояние до 55 м. Добавлен в стандарт в июне 2002 года
6A	500	10 Gigabit Ethernet (10GBASE-T)	Состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с на расстояние до 100 метров. Добавлен в стандарт в феврале 2008 года, ISO/IEC 11801:2002, поправка 2. Кабель этой категории имеет либо общий экран (F/UTP), либо экраны вокруг каждой пары (U/FTP)
7	600	10 Gigabit Ethernet (10GBASE-T)	Спецификация на данный тип кабеля утверждена только международным стандартом ISO 11801, но не ANSI/TIA-568-C. Скорость передачи данных – до 10 Гбит/с. Кабель этой категории имеет общий экран и экраны вокруг каждой пары (F/FTP или S/FTP)
7A	1000	10 Gigabit Ethernet (10GBASE-T)	Международный стандарт ISO 11801, скорость передачи данных – до 10 Гбит/с. Общий экран и экраны вокруг каждой пары (F/FTP или S/FTP)
8/8.1	1600–2000	100 Gigabit Ethernet (40GBASE-T)	В разработке, техническая рекомендация ISO/IEC TR 11801-99-1 и международный стандарт ISO 11801, редакция 3 (для Cat. 8.1), американский стандарт ANSI/TIA-568-C.2-1 (для Cat. 8). Полностью совместим с

			кабелем категории 6A. Скорость передачи данных – до 40 Гбит/с при использовании стандартных коннекторов 8P8C. Кабель этой категории имеет либо общий экран, либо экраны вокруг каждой пары (F/UTP или U/FTP)
8.2	1600–2000	100 Gigabit Ethernet (40GBASE-T)	В разработке, международный стандарт ISO 11801, редакция 3. Полностью совместим с кабелем категории 7A. Скорость передачи данных – до 40 Гбит/с при использовании стандартных коннекторов 8P8C либо GG45/ARJ45 и TERA. Кабель этой категории имеет общий экран и экраны вокруг каждой пары (F/FTP или S/FTP)

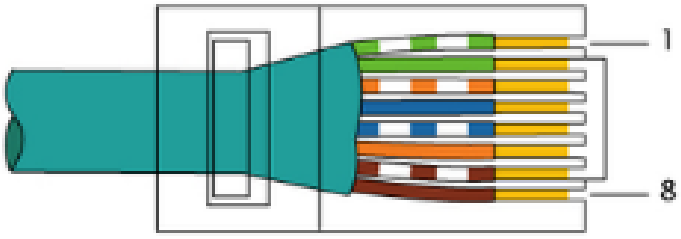
Каждая отдельно взятая витая пара, входящая в состав кабеля, предназначенного для передачи данных, должна иметь волновое сопротивление 100±15 Ом, в противном случае форма электрического сигнала будет искажена и передача данных станет невозможной. Причиной проблем с передачей данных может быть не только некачественный кабель, но также наличие «скруток» в кабеле и использование розеток более низкой категории, чем кабель.

Схемы обжима

Вариант по стандарту TIA/EIA-568A

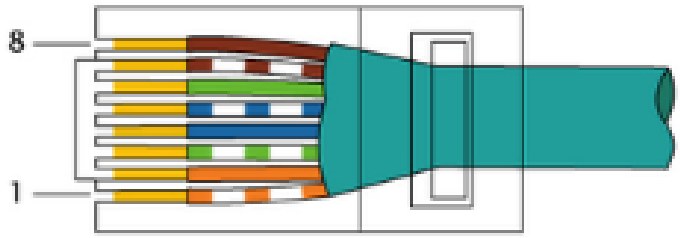


EIA/TIA-568A

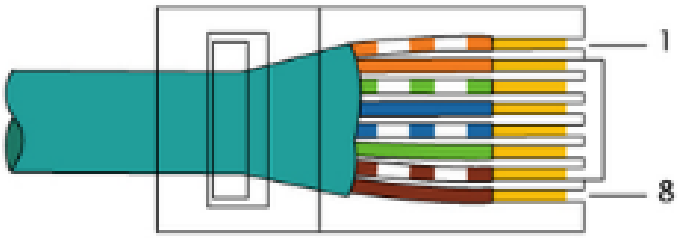


EIA/TIA-568A

Вариант по стандарту TIA/EIA-568B (используется чаще)



EIA/TIA-568B



EIA/TIA-568B

Монтаж

При резких изгибах витой пары нарушается однородность симметричной среды передачи, иногда необратимо. Регламентированный минимальный радиус изгиба неэкранированного кабеля при монтаже – 8 внешних диаметров кабеля, экранированного – 10.

При монтаже экранированной витой пары необходимо следить за целостностью экрана по всей длине кабеля. Растяжение или изгиб кабеля приводит к разрушению экрана, что ведет к снижению устойчивости к электромагнитным помехам. Дренажный провод должен быть соединен с экраном разъема.

Оптическое волокно

Оптическое волокно – нить из оптически прозрачного материала (стекла, пластика), используемая для переноса света внутри себя посредством полного внутреннего отражения.

Волоконная оптика – раздел прикладной науки и машиностроения, описывающий такие волокна. Кабели на базе оптических волокон используются в волоконно-оптической связи, позволяющей передавать информацию на бóльшие расстояния с более высокой скоростью передачи данных, чем в электронных средствах связи. В ряде случаев они также используются при создании датчиков.

История

Принцип передачи света, используемый в волоконной оптике, был впервые продемонстрирован в XIX веке, но повсеместное применение было затруднено отсутствием соответствующих технологий.

В 1934 году американец Норман Р. Френч получил патент на оптическую телефонную систему, речевые сигналы в которой передавались при помощи света по стержням чистого стекла. В

1962 году были созданы полупроводниковый лазер и фотодиод, используемые как источник и приемник оптического сигнала.

Повсеместному переходу на технологии ВОЛС мешали высокие затухания в оптическом волокне, поэтому конкуренция с медными линиями была невозможна. Только к 1970 году компании Corning (Англия) удалось наладить коммерческое производство волокна с низким затуханием – до 17 дБ/км, через пару лет – до 4 дБ/км. Волокно являлось многомодовым, и по нему передавалось несколько мод света. К 1983 году был освоен выпуск одномодовых волокон, по которым передавалась одна мода.

В России первые волоконно-оптические линии появились в Москве. Первой подводной ВОЛС стала магистраль Санкт-Петербург – Аберслунд (Дания), проложенная АО «Совтелеком» (ныне ПАО «Ростелеком»).

Материалы

Стеклянные оптические волокна делаются из кварцевого стекла, но для дальнего инфракрасного диапазона могут использоваться другие материалы, такие как фторцирконат, фторалюминат и халькогенидные стекла. Как и другие стекла, эти имеют показатель преломления около 1,5.

В настоящее время развивается применение пластиковых оптических волокон. Сердечник в таком волокне изготовляют из полиметилметакрилата (PMMA), а оболочку – из фторированных PMMA (фторполимеров).

Конструкция

Оптическое волокно, как правило, имеет круглое сечение и состоит из двух частей – сердцевины и оболочки. Для обеспечения полного внутреннего отражения абсолютный показатель преломления сердцевины несколько выше показателя преломления оболочки. Сердцевина изготавливается из чистого материала (стекла или пластика) и имеет диаметр 9 мкм (для одномодового волокна), 50 или 62,5 мкм (для многомодового волокна). Оболочка имеет диаметр 125 мкм и состоит из материала с легирующими добавками, изменяющими показатель преломления. Например, если показатель преломления оболочки равен 1,474, то показатель преломления сердцевины – 1,479. Луч света, направленный в сердцевину, будет распространяться по ней, многократно отражаясь от оболочки.

Возможны и более сложные конструкции: в качестве сердцевины и оболочки могут применяться двумерные фотонные кристаллы, вместо ступенчатого изменения показателя преломления часто используются волокна с градиентным профилем показателя преломления, форма сердцевины может отличаться от цилиндрической. Такие конструкции обеспечивают волокнам специальные свойства: удержание поляризации распространяющегося света, снижение потерь, изменение дисперсии волокна и др.

Оптические волокна, используемые в телекоммуникациях, как правило, имеют диаметр 125±1 микрон. Диаметр сердцевины может отличаться в зависимости от типа волокна и национальных стандартов.

Классификация

Оптические волокна могут быть одномодовыми и многомодовыми.

Одномодовое	**Многомодовое**
Передача одного светового сигнала	Передача более чем одного светового сигнала
Меньший диаметр сердечника	Больший диаметр сердечника
Меньше рассеивание (дисперсия)	Больше рассеивание (дисперсия)
Большее расстояние передачи (десятки км)	Меньшее расстояние передачи (до 1000 м)
Более критичен к качеству сварки	Менее критичен к качеству сварки
Дороже	Дешевле

Топологии сетей

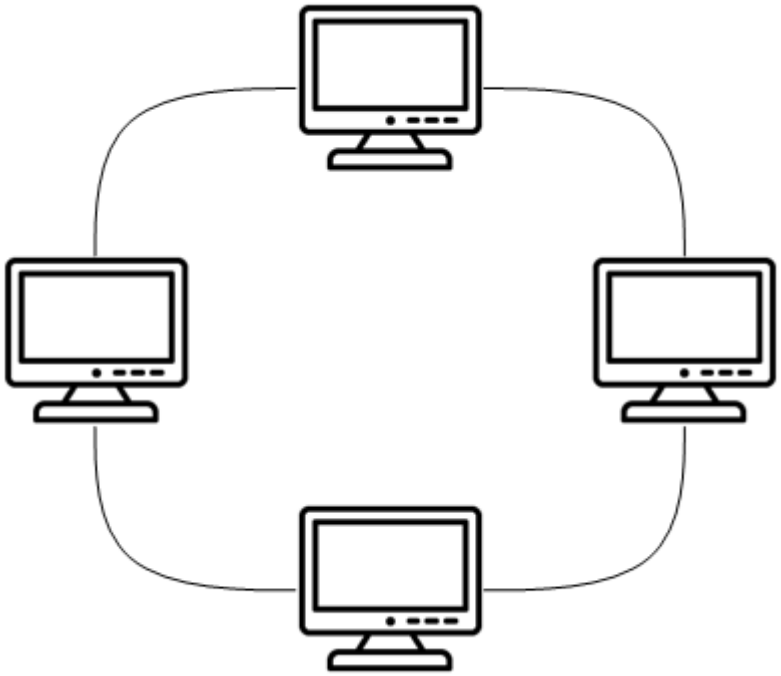
Топологии сетей могут быть двух видов:

- **физическая топология** описывает реальное расположение и связи между узлами сети;
- **логическая топология** описывает хождение сигнала в рамках физической топологии.

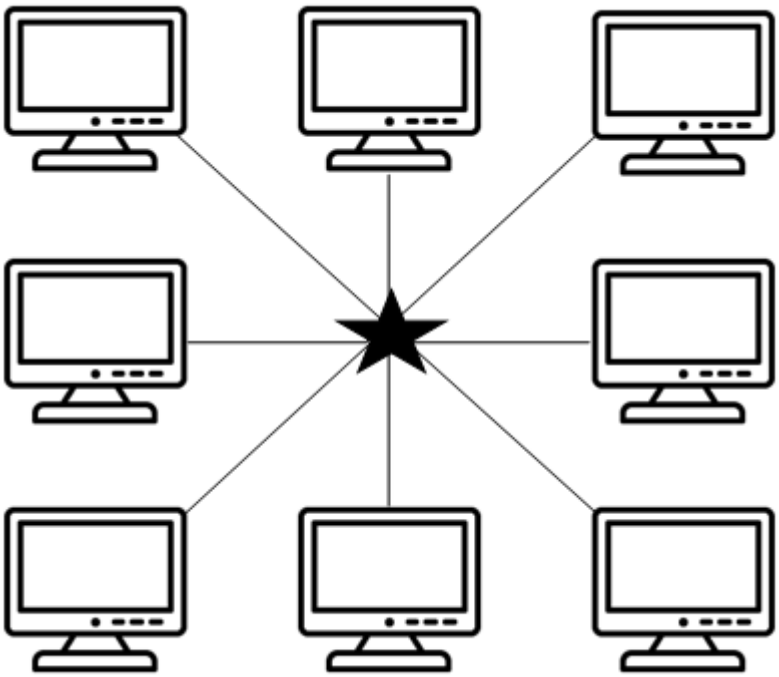
Физическая и логическая топологии могут как совпадать, так и не совпадать.

Шина

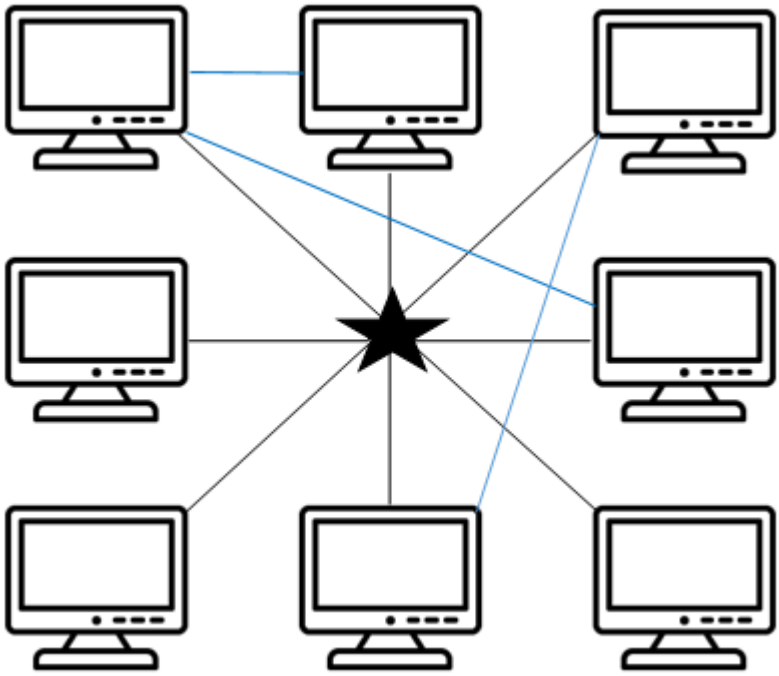
Кольцо



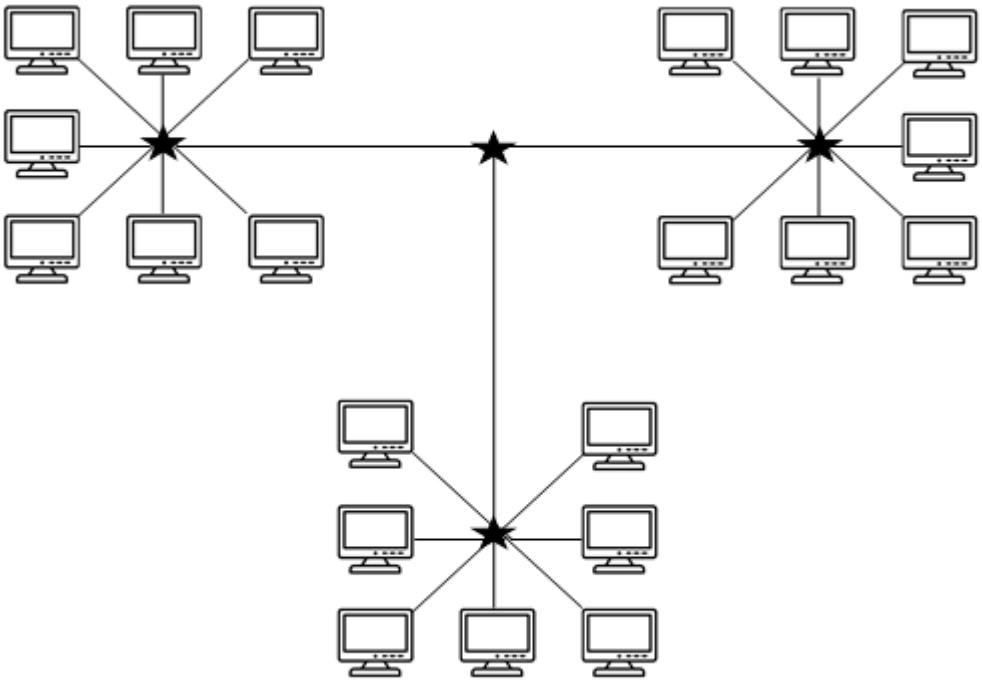
Звезда



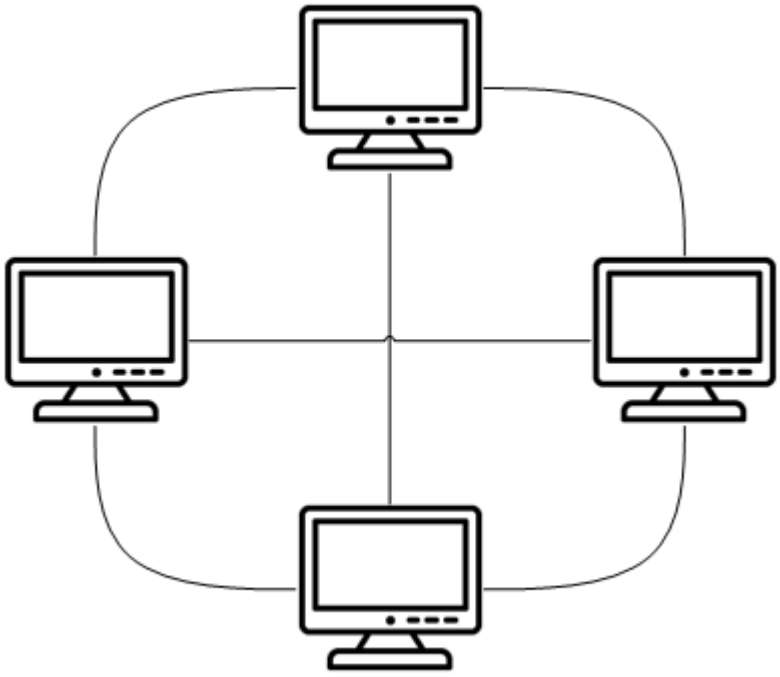
Смешанная звезда



Расширенная звезда



Полносвязанная топология



Технологии передачи данных

Существуют различные технологии передачи данных. В этой теме будет рассмотрена только часть из них.

PLC (Power Line Communication) – связь через линии электропередачи (ЛЭП)

Связь через ЛЭП, PLC (англ. Power line communication) – термин, описывающий несколько разных систем для использования линий электропередачи (ЛЭП) для передачи голосовой информации или данных. Сеть может передавать голос и данные, накладывая аналоговый сигнал поверх стандартного переменного тока частотой 50 Гц или 60 Гц. PLC включает BPL (англ. Broadband over Power Lines «широкополосная передача через линии электропередачи»), обеспечивающий передачу данных со скоростью до 500 Мбит/с, и NPL (англ. Narrowband over Power Lines «узкополосная передача через линии электропередачи») со значительно меньшими скоростями передачи данных – до 1 Мбит/с.

В 2000 году несколько крупных лидеров на рынке телекоммуникаций объединились в HomePlug Powerline Alliance с целью совместного проведения научных исследований и практических испытаний, а также принятия единого стандарта на передачу данных по системам электропитания. Прототипом Powerline является технология PowerPacket фирмы Intellon, положенная в основу при создании единого стандарта HomePlug1.0 (принят альянсом HomePlug 26 июня 2001 года), в котором определена скорость передачи данных до 14 Мб/сек.

Однако на данный момент стандарт HomePlug AV поднял скорость передачи данных до 500 Мбит/с.

Подключение к Интернету

В настоящее время подавляющее большинство конечных подключений осуществляется посредством прокладки кабеля от высокоскоростной линии до квартиры или офиса пользователя. Это наиболее дешевое и надежное решение, но если прокладка кабеля невозможна, то можно воспользоваться имеющейся в каждом здании системой силовых электрических коммуникаций. При этом любая электрическая розетка в здании может стать точкой выхода в Интернет. От пользователя требуется только наличие Powerline-модема для связи с аналогичным устройством, установленным, как правило, в электрощитовой здания и подключенным к высокоскоростному каналу. PLC может быть хорошим решением «последней мили» в коттеджных поселках и в малоэтажной застройке в связи с тем, что традиционные провода стоят в несколько раз дороже PLC.

Преимущества

- Простота использования – не требуется прокладка отдельного кабеля.
- Можно использовать любые другие провода, в том числе и контактные сети электротранспорта и метро.
- Оперативность при развертывании сети передачи данных – электрические провода есть почти везде.
- Не требуется регистрация оборудования как радиочастотного, несмотря на то что мощность передатчика составляет 75 мВт, а это создает уровень помех, превышающий допустимые ГОСТом нормы по ЭМС.
- В случае, если каким-то образом есть влияние на какие-то частоты, в PLC-оборудовании предусмотрен механизм подавления сигнала в заданном диапазоне.

Недостатки

- Пропускная способность сети по электропроводке делится между всеми ее участниками (используется топология сети «общая шина»).
- Иногда требуются специальные совместимые сетевые фильтры и ИБП. Сигнал может существенно ослабляться, проходя через многие сетевые разветвители-фильтры.
- На качество, скорость и надежность связи оказывают отрицательное влияние электробытовые приборы (энергосберегающие лампы, импульсные блоки питания, зарядные устройства, выключатели освещения и т.д., и т.п.). В результате наблюдается снижение скорости от 5 до 50 %.
- На качество, скорость и надежность связи оказывает отрицательное влияние исполнение/топология/качество электропроводки, тип/режим/мощность бытовых электроприборов и устройств, наличие скруток. В результате наблюдается снижение скорости передачи данных до полного пропадания сигнала.
- Уязвима для сигналов от радиопередающих устройств коротковолнового (КВ) диапазона, в том числе и устройств службы любительской радиосвязи.
- Не может серьезно рассматриваться как надежная технология передачи данных ввиду уязвимости к помехам из общих электросетей и несоответствия нормам по электромагнитной совместимости как по приему (уязвимость к помехам из электросети, сигналам КВ-передатчиков), так и по передаче сигналов (создание помех в электросети и КВ-приемникам).
- Создает помехи в коротковолновом диапазоне, что особенно чувствительно для службы любительской радиосвязи (ЛСР). Учитывая, что ЛСР использует КВ-частоты исключительно на официальной и разрешительной основе в государственных органах, ЛСР имеет безусловный приоритет перед PLC.

xDSL

xDSL (англ. digital subscriber line «цифровая абонентская линия») – семейство технологий, позволяющих значительно повысить пропускную способность абонентской линии телефонной сети общего пользования путем использования эффективных линейных кодов и адаптивных методов коррекции искажений линии на основе современных достижений микроэлектроники и методов цифровой обработки сигнала.

Технологии xDSL появились в середине 1990-х годов как альтернатива цифровому абонентскому окончанию ISDN.

В аббревиатуре xDSL символ «x» используется для обозначения первого символа в названии конкретной технологии, а «DSL» обозначает цифровую абонентскую линию DSL (англ. Digital Subscriber Line «цифровая абонентская линия»; также есть другой вариант названия – Digital Subscriber Loop «цифровой абонентский шлейф»). Технологии xDSL позволяют передавать данные со скоростями, значительно превышающими те скорости, которые доступны даже лучшим аналоговым и цифровым модемам. Эти технологии поддерживают передачу голоса, высокоскоростную передачу данных и видеосигналов, создавая при этом значительные преимущества как для абонентов, так и для провайдеров. Многие технологии xDSL позволяют совмещать высокоскоростную передачу данных и передачу голоса по одной и той же медной паре. Существующие типы технологий xDSL различаются в основном по используемой форме модуляции и скорости передачи данных.

Службы xDSL разрабатывались для достижения определенных целей: они должны работать на существующих телефонных линиях, они не должны мешать работе различной аппаратуры

абонента, такой как телефонный аппарат, факс и т.д., скорость работы должна быть выше теоретического предела в 56 Кбит/сек., и наконец, они должны обеспечивать постоянное подключение. Широкое распространение технологий xDSL должно сопровождаться некоторой перестройкой работы поставщиков услуг Интернета и поставщиков услуг телефонных сетей, так как их оборудование теперь должно работать совместно. Возможен также вариант, когда альтернативный оператор связи берет оптом в аренду большое количество абонентских окончаний у традиционного местного оператора или же арендует некоторое количество модемов в DSLAM.

К основным типам xDSL относятся ADSL, HDSL, IDSL, MSDSL, PDSL, RADSL, SDSL, SHDSL, UADSL, VDSL. Все эти технологии обеспечивают высокоскоростной цифровой доступ по абонентской телефонной линии. Некоторые технологии xDSL являются оригинальными разработками, другие представляют собой просто теоретические модели, в то время как третьи уже стали широко используемыми стандартами. Основным различием данных технологий являются методы модуляции, используемые для кодирования данных.

Технология DSL	**Максимальная скорость (прием/передача)**	**Максимальное расстояние**	**Количество телефонных пар**	**Основное применение**
ADSL	24 Мбит/с / 1,4 Мбит/с	5,5 км	1	Доступ в Интернет, голос, видео
IDSL	144 Кбит/с	5,5 км	1	Передача данных
HDSL	2 Мбит/с	4,5 км	1,2	Объединение сетей, услуги E1
SDSL	2 Мбит/с	3 км	1	Объединение сетей, услуги E1
VDSL	62 Мбит/с / 26 Мбит/с	1,3 км на макс. скорости	1	Объединение сетей
SHDSL	2,32 Мбит/с	7,5 км	1	Объединение сетей
UADSL	1,5 Мбит/с / 384 Кбит/с	3,5 км на max. скорости	1	Доступ в Интернет, голос, видео

PON

PON (аббр. от англ. Passive optical network «пассивная оптическая сеть») – технология пассивных оптических сетей.

Распределительная сеть доступа PON основана на древовидной волоконно-кабельной архитектуре с пассивными оптическими разветвителями на узлах, представляет собой экономичный способ обеспечить широкополосную передачу информации. При этом архитектура PON обладает необходимой эффективностью наращивания узлов сети и пропускной способности в зависимости от настоящих и будущих потребностей абонентов.

Первые шаги в технологии PON были предприняты в 1995 году, когда группа из 7 компаний (British Telecom, France Telecom, Deutsche Telecom, NTT, KPN, Telefonica и Telecom Italia) создала консорциум для реализации идеи множественного доступа по одному волокну. Эта организация, поддерживаемая ITU-T, получила название «FSAN» (англ. full service access network). Много новых членов, как операторов, так и производителей оборудования, вошло в нее в конце 1990-х годов. Целью FSAN была разработка общих рекомендаций и требований к

оборудованию PON для того, чтобы производители оборудования и операторы могли сосуществовать вместе на конкурентном рынке систем доступа PON. На ноябрь 2011 года во FSAN состояло 26 операторов и 50 производителей. FSAN работает в тесном сотрудничестве с такими организациями по стандартизации, как ITU-T, ETSI и ATM Forum.

Стандарты:

- ITU-T G.983:
  - APON (ATM Passive Optical Network),
  - BPON (Broadband PON);
- ITU-T G.984:
  - GPON (Gigabit PON);
- IEEE 802.3ah:
  - EPON или GEPON (Ethernet PON);
- IEEE 802.3av:
  - 10GEPON (10 Gigabit Ethernet PON).

Существуют четыре основные топологии построения оптических сетей доступа:

- «кольцо»;
- «точка-точка»;
- «дерево с активными узлами»;
- «дерево с пассивными узлами».

Преимущества технологии PON:

- отсутствие промежуточных активных узлов;
- экономия оптических приемопередатчиков в центральном узле;
- экономия волокон;
- древовидная топология P2MP позволяет оптимизировать размещение оптических разветвителей, исходя из реального расположения абонентов, затрат на прокладку ОК и эксплуатацию кабельной сети.

Недостатки сетевой технологии PON:

- возросшая сложность технологии PON;
- отсутствие резервирования в простейшей топологии дерева.

Ethernet

Локальная сеть (англ. Ethernet [ˈiːθəˌnɛt] от англ. ether [ˈiːθə] «эфир» и англ. network «сеть, цепь») – семейство технологий пакетной передачи данных между устройствами для компьютерных и промышленных сетей.

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде – на канальном уровне модели OSI. Ethernet в основном описывается стандартами IEEE группы 802.3. Ethernet стал самой распространенной технологией ЛВС в середине 1990-х годов, вытеснив такие устаревшие технологии, как Token Ring, FDDI и ARCNET.

Название «Ethernet» (буквально «эфирная сеть» или «среда сети») отражает первоначальный принцип работы этой технологии: всё, передаваемое одним узлом, одновременно принимается всеми остальными (то есть имеется некое сходство с радиовещанием). В настоящее время практически всегда подключение происходит через коммутаторы (switch), так что кадры, отправляемые одним узлом, доходят лишь до адресата (исключение составляют передачи на широковещательный адрес) – это повышает скорость работы и безопасность сети.

История

Технология Ethernet была разработана вместе со многими первыми проектами корпорации Xerox PARC. Общепринято считать, что Ethernet был изобретен 22 мая 1973 года, когда Роберт Меткалф (Robert Metcalfe) составил докладную записку для главы PARC о потенциале технологии Ethernet. Но законное право на технологию Меткалф получил через несколько лет. В 1976 году он и его ассистент Дэвид Боггс (David Boggs) издали брошюру под названием «Ethernet: Distributed Packet-Switching For Local Computer Networks».

Меткалф ушел из Xerox в 1979 году и основал компанию 3Com для продвижения компьютеров и локальных вычислительных сетей (ЛВС). Ему удалось убедить DEC, Intel и Xerox работать совместно и разработать стандарт Ethernet (DIX). Впервые этот стандарт был опубликован 30 сентября 1980 года. Он начал соперничество с двумя крупными запатентованными технологиями: token ring и ARCNET, – которые вскоре были раздавлены под накатывающимися волнами продукции Ethernet. В процессе борьбы 3Com стала основной компанией в этой отрасли.

Технология

В стандарте первых версий (Ethernet v1.0 и Ethernet v2.0) указано, что в качестве передающей среды используется коаксиальный кабель, в дальнейшем появилась возможность использовать витую пару и оптический кабель.

Преимущества использования витой пары по сравнению с коаксиальным кабелем:

- возможность работы в дуплексном режиме;
- низкая стоимость кабеля витой пары;
- более высокая надежность сетей: при использовании витой пары сеть строится по топологии «звезда», поэтому обрыв кабеля приводит лишь к нарушению связи между двумя объектами сети, соединенными этим кабелем (при использовании коаксиального кабеля сеть строится по топологии «общая шина», для которой требуется наличие терминальных резисторов на концах кабеля, поэтому обрыв кабеля приводит к неисправности сегмента сети);
- уменьшен минимально допустимый радиус изгиба кабеля;
- большая помехоустойчивость из-за использования дифференциального сигнала;
- возможность питания по кабелю маломощных узлов, например IP-телефонов (стандарт Power over Ethernet, PoE);
- гальваническая развязка трансформаторного типа. В условиях СНГ, где, как правило, отсутствует заземление компьютеров, применение коаксиального кабеля часто приводило к выходу из строя сетевых карт в результате электрического пробоя.

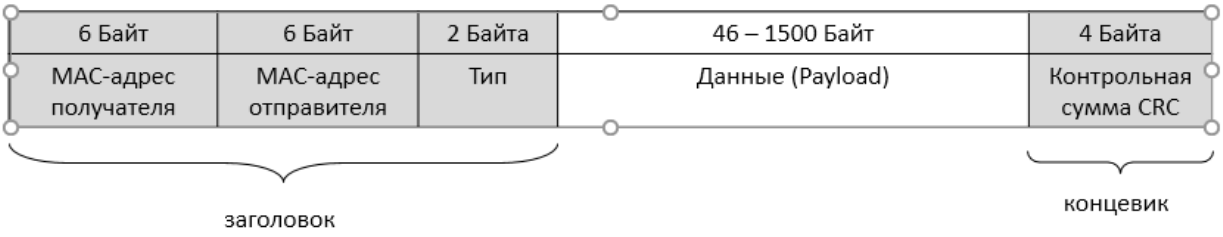
Причиной перехода на оптический кабель была необходимость увеличить длину сегмента без повторителей.

В полудуплексном режиме узел не может одновременно передавать и принимать информацию. Количество узлов в одном разделяемом сегменте сети ограничено предельным значением в 1024 рабочие станции (спецификации физического уровня могут устанавливать более жесткие ограничения; например, к сегменту тонкого коаксиала может подключаться не более 30 рабочих станций, а к сегменту толстого коаксиала – не более 100). Однако сеть, построенная на одном разделяемом сегменте, становится неэффективной задолго до достижения предельного значения количества узлов, в основном по причине полудуплексного режима работы.

В 1995 году принят стандарт IEEE 802.3u Fast Ethernet со скоростью 100 Мбит/с, и появилась возможность работы в режиме «полный дуплекс». В 1997 году был принят стандарт IEEE 802.3z Gigabit Ethernet со скоростью 1000 Мбит/с для передачи по оптическому волокну и еще через два года – для передачи по витой паре.

Существует несколько форматов Ethernet-кадра:

- первоначальный Version I (больше не применяется);
- Ethernet Version 2, или Ethernet-кадр II, еще называемый DIX (аббревиатура первых букв фирм-разработчиков DEC, Intel, Xerox), – наиболее распространен и используется по сей день. Часто используется непосредственно протоколом Интернет.



Разновидности

В зависимости от скорости передачи данных и передающей среды существует несколько вариантов технологии. Независимо от способа передачи, стек сетевого протокола и программы работают одинаково практически во всех нижеперечисленных вариантах.

В этом разделе дано краткое описание всех официально существующих разновидностей. По некоторым причинам в дополнение к основному стандарту многие производители рекомендуют пользоваться другими запатентованными носителями – например, для увеличения расстояния между точками сети используется волоконно-оптический кабель.

Большинство Ethernet-карт и других устройств имеет поддержку нескольких скоростей передачи данных, используя автоопределение (autonegotiation) скорости и дуплексности для достижения наилучшего соединения между двумя устройствами. Если автоопределение не срабатывает, скорость подстраивается под партнера, и включается режим полудуплексной передачи. Например, наличие в устройстве порта Ethernet 10/100 говорит о том, что через него можно работать по технологиям 10BASE-T и 100BASE-TX, а порт Ethernet 10/100/1000 поддерживает стандарты 10BASE-T, 100BASE-TX и 1000BASE-T.

Ранние модификации Ethernet

- **Xerox Ethernet** – оригинальная технология, скорость 3 Мбит/с, существовала в двух вариантах: Version 1 и Version 2; формат кадра последней версии до сих пор имеет широкое применение.
- **1BROAD36** – широкого распространения не получил. Один из первых стандартов, позволяющих работать на больших расстояниях. Использовал технологию широкополосной модуляции, похожей на ту, что применяется в кабельных модемах. В качестве среды передачи данных использовался коаксиальный кабель.
- **1BASE5** – также известный как StarLAN, стал первой модификацией Ethernet-технологии, использующей витую пару. Работал на скорости 1 Мбит/с, но не нашел коммерческого применения.

10 Мбит/с Ethernet

- **10BASE5**, **IEEE 802.3** (называемый также «толстый Ethernet») – первоначальная разработка технологии со скоростью передачи данных 10 Мбит/с. Следуя раннему стандарту, IEEE использует коаксиальный кабель с волновым сопротивлением 50 Ом (RG-8), с максимальной длиной сегмента 500 метров.
- **10BASE2**, **IEEE 802.3a** (называемый «тонкий Ethernet») – используется кабель RG-58 с максимальной длиной сегмента 185 метров, компьютеры присоединяются один к другому, для подключения кабеля к сетевой карте нужен Т-коннектор, а на кабеле должен быть BNC-коннектор. Требуется наличие терминаторов на каждом конце. Многие годы этот стандарт был основным для технологии Ethernet.
- **StarLAN 10** – первая разработка, использующая витую пару для передачи данных на скорости 10 Мбит/с. В дальнейшем эволюционировал в стандарт 10BASE-T.
- **10BASE-T, IEEE 802.3i** – для передачи данных используется 4 провода кабеля витой пары (две скрученные пары) категории 3 или категории 5. Максимальная длина сегмента – 100 метров.
- **FOIRL** (акроним от англ. Fiber-optic inter-repeater link). Базовый стандарт для технологии Ethernet, использующий для передачи данных оптический кабель. Максимальное расстояние передачи данных без повторителя – 1 км.
- **10BASE-F**, **IEEE 802.3j** – основной термин для обозначения семейства 10 Мбит/с ethernet-стандартов, использующих оптический кабель на расстоянии до 2 километров: 10BASE-FL, **10BASE-FB** и **10BASE-FP**. Из перечисленных только 10BASE-FL получил широкое распространение.
- **10BASE-FL** (Fiber Link) – улучшенная версия стандарта FOIRL. Улучшение коснулось увеличения длины сегмента до 2 км.
- **10BASE-FB** (Fiber Backbone) – сейчас неиспользуемый стандарт, предназначался для объединения повторителей в магистраль.
- **10BASE-FP** (Fiber Passive) – топология «пассивная звезда», в которой не нужны повторители. Никогда не применялся.

Быстрый Ethernet (Fast Ethernet, 100 Мбит/с)

- **100BASE-T** – общий термин для обозначения стандартов, использующих в качестве среды передачи данных витую пару. Длина сегмента – до 100 метров. Включает в себя стандарты 100BASE-TX, 100BASE-T4 и 100BASE-T2.
- **100BASE-TX**, **IEEE 802.3u** – развитие стандарта 10BASE-T для использования в сетях топологии «звезда». Задействована витая пара категории 5, фактически используются только две неэкранированные пары проводников, поддерживается дуплексная передача данных, расстояние – до 100 м.
- **100BASE-T4** – стандарт, использующий витую пару категории 3. Задействованы все четыре пары проводников, передача данных идет в полудуплексе. Практически не используется.
- **100BASE-T2** – стандарт, использующий витую пару категории 3. Задействованы только две пары проводников. Поддерживается полный дуплекс, когда сигналы распространяются в противоположных направлениях по каждой паре. Скорость передачи в одном направлении – 50 Мбит/с. Практически не используется.
- **100BASE-FX** – стандарт, использующий многомодовое волокно. Максимальная длина сегмента – 400 метров в полудуплексе (для гарантированного обнаружения коллизий) или 2 километра в полном дуплексе.

- **100BASE-SX** – стандарт, использующий многомодовое волокно. Максимальная длина сегмента 2–10 км. Максимальная длина ограничена величиной затухания в оптическом кабеле и мощностью передатчиков.
- **100BASE-FX WDM** – стандарт, использующий одномодовое волокно. Максимальная длина ограничена только величиной затухания в волоконно-оптическом кабеле и мощностью передатчиков. Интерфейсы бывают двух видов, отличаются длиной волны передатчика и маркируются либо цифрами (длина волны), либо одной латинской буквой A (1310) или B (1550). В паре могут работать только парные интерфейсы: с одной стороны передатчик на 1310 нм, а с другой – на 1550 нм.

Гигабитный Ethernet (Gigabit Ethernet, 1 Гбит/с)

- **1000BASE-T**, **IEEE 802.3ab** – основной гигабитный стандарт, опубликованный в 1999 году, использует витую пару категории 5e. В передаче данных участвуют 4 пары, каждая пара используется одновременно для передачи по обоим направлениям со скоростью 250 Мбит/с. Используется метод кодирования PAM5 (5-level Phase Amplitude Modulation, пятиуровневая фазоамплитудная модуляция) с 4 линиями (4D-PAM5) и 4-мерной треллис-модуляцией (TCM), частота основной гармоники – 62,5 МГц. Расстояние – до 100 метров.
- **1000BASE-TX** был создан Ассоциацией телекоммуникационной промышленности (англ. Telecommunications Industry Association, TIA) и опубликован в марте 2001 года как «Спецификация физического уровня дуплексного Ethernet 1000 Мб/с (1000BASE-TX) симметричных кабельных систем категории 6 (ANSI/TIA/EIA-854-2001)». Распространения не получил из-за высокой стоимости кабелей, фактически устарел. Стандарт разделяет принимаемые и посылаемые сигналы по парам (две пары передают данные, каждая на 500 Мбит/с, и две пары принимают). Это упрощает конструкцию приемо-передающих устройств. Еще одним существенным отличием 1000BASE-TX является отсутствие схемы цифровой компенсации наводок и возвратных помех, в результате чего сложность, уровень энергопотребления и цена реализаций должны становиться ниже, чем у стандарта 1000BASE-T. Для работы технологии требуется кабельная система 6-й категории. На основе данного стандарта создано большое количество продуктов для промышленных сетей.
- **1000BASE-X** – общий термин для обозначения стандартов со сменными приемопередатчиками в форм-факторах GBIC или SFP.
- **1000BASE-SX**, **IEEE 802.3z** – стандарт, использующий многомодовое волокно в первом окне прозрачности с длиной волны, равной 850 нм. Дальность прохождения сигнала составляет до 550 метров.
- **1000BASE-LX**, **IEEE 802.3z** – стандарт, использующий одномодовое или многомодовое оптическое волокно во втором окне прозрачности с длиной волны, равной 1310 нм. Дальность прохождения сигнала зависит только от типа используемых приемопередатчиков и, как правило, составляет для одномодового оптического волокна до 5 км и для многомодового оптического волокна до 550 метров.
- **1000BASE-CX** – стандарт для коротких расстояний (до 25 метров), использующий 2-парный экранированный кабель (150 Ом, STP IBM Type I или лучше). Применяется кодирование 8B/10B, сигнал передается по одной паре, принимается по другой паре проводов; разъемы – 9-контактный D, HSSDC. Заменен стандартом 1000BASE-T и сейчас не используется.
- **1000BASE-LH** (Long Haul) – стандарт, использующий одномодовое волокно. Дальность прохождения сигнала без повторителя – до 100 километров.

2,5- и 5-гигабитные варианты (NBASE-T, MGBASE-T)

В 2014 году появились частные инициативы NBASE-T (Cisco) и MGBASE-T (Broadcom) по созданию стандартов Ethernet со скоростью, промежуточной между 1 и 10 Гбит/с. Новый стандарт должен использовать существующую кабельную инфраструктуру категории 5e на расстоянии до 100 метров, предоставляя скорости в 2,5 или, что менее вероятно, 5 Гбит/с. Среди причин появления инициатив – распространение Wi-Fi-маршрутизаторов, поддерживающих скорости более 1 гигабита (802.11ac Wave 2, 802.11ad, 802.11ax, LiFi), и невозможность использования 10 Гбит/с стандартов Ethernet по длинным кабелям категорий 5e и 6. Ранее группа IEEE 802 отмечала, что гипотетический стандарт 2500BASE-T мог бы быть близок по стоимости к 1000BASE-T-решениям. Стандарт на 2,5 и 5 Гбит/с Ethernet по кабелям Cat 5e и Cat 6 был принят осенью 2016 года как IEEE 802.3bz.

10-гигабитный Ethernet (10G Ethernet, 10 Гбит/с)

Стандарт 10-гигабитного Ethernet включает в себя семь стандартов физической среды для LAN, MAN и WAN. В настоящее время он описывается поправкой IEEE 802.3ae и должен войти в следующую ревизию стандарта IEEE 802.3.

- **10GBASE-CX4** – технология 10-гигабитного Ethernet для коротких расстояний (до 15 метров), используется медный кабель CX4 и коннекторы InfiniBand.
- **10GBASE-SR** – технология 10-гигабитного Ethernet для коротких расстояний (до 26 или 82 метров, в зависимости от типа кабеля), используется многомодовое волокно. Она также поддерживает расстояния до 300 метров с использованием нового многомодового волокна (2000 МГц/км).
- **10GBASE-LX4** – использует уплотнение по длине волны для поддержки расстояний от 240 до 300 метров по многомодовому волокну. Также поддерживает расстояния до 10 километров при использовании одномодового волокна.
- **10GBASE-LR** и **10GBASE-ER** – эти стандарты поддерживают расстояния до 10 и 40 километров соответственно.
- **10GBASE-SW**, **10GBASE-LW** и **10GBASE-EW** – эти стандарты используют физический интерфейс, совместимый по скорости и формату данных с интерфейсом OC-192 / STM-64 SONET/SDH. Они подобны стандартам 10GBASE-SR, 10GBASE-LR и 10GBASE-ER соответственно, так как используют те же самые типы кабелей и расстояния передачи.
- **10GBASE-T**, **IEEE 802.3an-2006** – принят в июне 2006 года после 4 лет разработки. Использует витую пару категории 6 (максимальное расстояние 55 метров) и 6a (максимальное расстояние 100 метров).
- **10GBASE-KR** – технология 10-гигабитного Ethernet для кросс-плат (backplane/midplane) модульных коммутаторов/маршрутизаторов и серверов (Modular/Blade).

40-гигабитный и 100-гигабитный Ethernet

Согласно наблюдениям Группы 802.3ba, требования к полосе пропускания для вычислительных задач и приложений ядра сети растут с разными скоростями, что определяет необходимость двух соответствующих стандартов для следующих поколений Ethernet – 40 Gigabit Ethernet (или 40GbE) и 100 Gigabit Ethernet (или 100GbE). В настоящее время серверы, высокопроизводительные вычислительные кластеры, блейд-системы, SAN и NAS используют технологии 1GbE и 10GbE, при этом в 2007 и 2008 годах был отмечен значительный рост последней.

Домен коллизий и широковещательный домен

В сетевых технологиях коллизия кадров – это наложение двух и более кадров (пакетов) от станций, пытающихся передать кадр в один и тот же момент времени из-за наличия задержки распространения сигнала по сети или наличия неисправной сетевой платы.

Домен коллизий

Домен коллизий – это часть сети Ethernet, все узлы которой конкурируют за общую разделяемую среду передачи и, следовательно, каждый узел которой может создать коллизию с любым другим узлом этой части сети.

Другими словами, это сегмент сети, имеющий общий канальный уровень (Data Link layer) модели OSI, в котором передать фрейм может только один абонент одновременно. Задержка распространения фреймов между станциями либо одновременное начало передачи вызывают возникновение коллизий, которые требуют специальной обработки и снижают производительность сети.

Чем больше узлов в таком сегменте, тем выше вероятность коллизий. Для разделения домена коллизий применяются коммутаторы.

Сетевые устройства, работающие на канальном уровне модели OSI, могут продлевать либо ограничивать домен коллизий.

Возможны следующие варианты:

1. Устройства первого уровня OSI (концентраторы, повторители) только ретранслируют любой сигнал, поступающий из среды передачи, и продлевают домен коллизий.
2. Устройства второго уровня OSI (мосты, коммутаторы) разделяют домен коллизий.
3. Домен коллизий отдельный при подключении к порту коммутатора в полудуплексном режиме либо при соединении типа «точка-точка» двух сетевых адаптеров; в полнодуплексном режиме коллизии отсутствуют.

Термины:

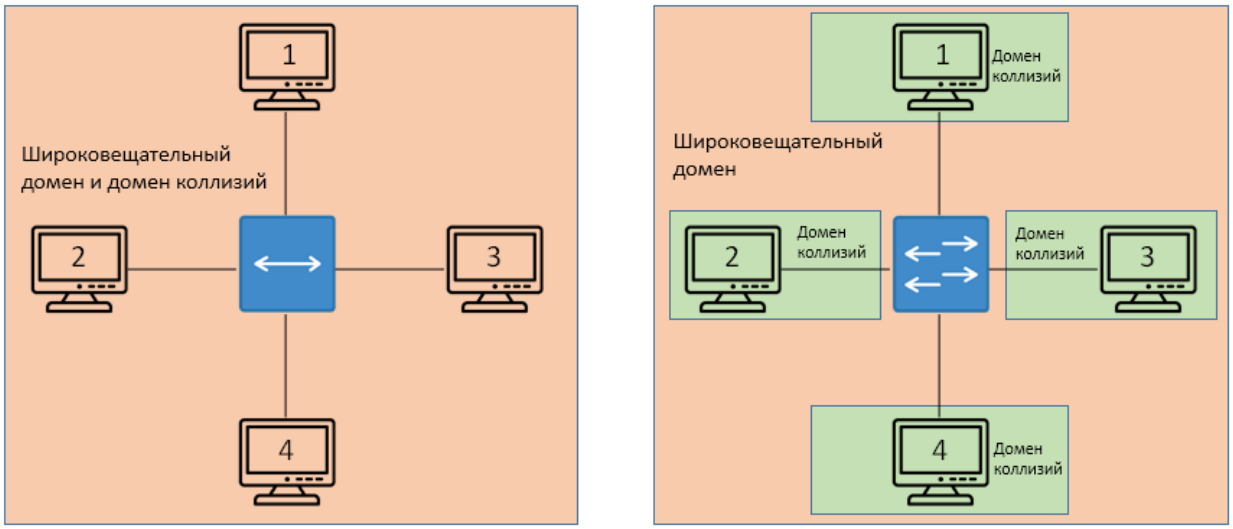
- Задержка распространения – время передачи временного сегмента, так называемого slotTime, равного 512 битам для скоростей до 100 Мбит/с и 4096 битам для скорости 1 Гбит/с, в течение которого может произойти коллизия. Определяется скоростью прохождения сигнала по проводу и скоростью передачи. Для Ethernet 10 Мбит/с задержка распространения составляет 51,2 мкс, для 100 Мбит/с – 5,12 мкс. Большая часть сетевого оборудования контролирует возникновение коллизий при передаче только в течение задержки распространения.
- Запоздалая коллизия – коллизия, произошедшая после задержки распространения. Такие коллизии не обнаруживаются большинством сетевого оборудования и приводят к потерям фреймов.
- Диаметр коллизионного домена – максимальная задержка распространения сигнала между двумя любыми станциями. Обычно определяется в единицах времени и соответствует удвоенному времени передачи кадра минимальной длины для данного типа Ethernet: D = 2 × <минимальная длина кадра> × 0,1 мкс.

Широковещательный домен

Широковещательный домен (сегмент) (англ. broadcast domain) – группа доменов коллизий, соединенных с помощью устройств второго уровня. Иными словами, логический участок компьютерной сети, в котором все узлы могут передавать данные друг другу с помощью широковещания на канальном уровне сетевой модели OSI.

Устройства, управляющие широковещательным доменом, – маршрутизаторы, работающие на третьем, сетевом уровне модели OSI, и коммутаторы на втором уровне модели OSI, поддерживающие функции виртуальных сетей. Устройства первого уровня – концентраторы (устарели) и повторители, а также коммутаторы без поддержки виртуальных сетей или изоляции портов не ограничивают широковещательный домен, т.е. узлы, подключенные к портам этих устройств, находятся в одном широковещательном домене.

Сравнение домена коллизий и широковещательного домена



Протокол ARP

ARP (англ. Address Resolution Protocol «протокол определения адреса») – протокол в компьютерных сетях, предназначенный для определения MAC-адреса, имея IP-адрес другого компьютера.

Наибольшее распространение ARP получил благодаря повсеместности сетей IP, построенных поверх Ethernet, поскольку практически в 100 % случаев при таком сочетании используется ARP. В семействе протоколов IPv6 ARP не существует, его функции возложены на ICMPv6.

Описание протокола было опубликовано в ноябре 1982 года в RFC 826. ARP был спроектирован для случая передачи IP-пакетов через кадры Ethernet. При этом общий принцип, предложенный для ARP, возможно, был использован и для сетей других типов.

Существуют следующие типы сообщений ARP: запрос ARP (ARP request) и ответ ARP (ARP reply). Система-отправитель при помощи запроса ARP запрашивает физический адрес системы-получателя. Ответ (физический адрес узла-получателя) приходит в виде ответа ARP.

Перед тем как передать пакет сетевого уровня через сегмент Ethernet, сетевой стек проверяет кеш ARP, чтобы выяснить, не зарегистрирована ли в нем уже нужная информация об узле-получателе. Если такой записи в кеше ARP нет, то выполняется широковещательный запрос ARP. Этот запрос для устройств в сети имеет следующий смысл: «Кто-нибудь знает физический адрес устройства, обладающего следующим IP-адресом?» Когда получатель с этим IP-адресом примет этот пакет, то должен будет ответить: «Да, это мой IP-адрес. Мой физический адрес следующий: …» После этого отправитель обновит свой кеш ARP и будет способен передать информацию получателю.

Записи в кеше ARP могут быть статическими и динамическими. Пример, данный выше, описывает динамическую запись кеша.

Принцип работы:

1. Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно.
2. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным.
3. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP-запросе отправитель указывает свой локальный адрес.

Преобразование адресов выполняется путем поиска в таблице. Эта таблица, называемая ARP-таблицей, хранится в памяти и содержит строки для каждого узла сети. В двух столбцах содержатся IP- и Ethernet-адреса. Если требуется преобразовать IP-адрес в Ethernet-адрес, то ищется запись с соответствующим IP-адресом.

Способы доступа к среде

Способы доступа к каналу или методы множественного доступа позволяют хостам подключаться к одной среде с множеством подключенных узлов с целью передачи информации через нее. Основные виды: FDMA, TDMA, CDMA/SSMA, SDMA, PDMA.

TDMA

TDMA (англ. Time Division Multiple Access «множественный доступ с разделением по времени») – способ использования радиочастот, при котором в одном частотном интервале находятся несколько абонентов, разные абоненты используют разные временные слоты (интервалы) для передачи. Является приложением мультиплексирования канала с разделением по времени (TDM – Time Division Multiplexing) к радиосвязи.

Таким образом, TDMA предоставляет каждому пользователю полный доступ к интервалу частоты в течение короткого периода времени (в GSM один частотный интервал делится на 8 временных слотов). TDMA в настоящее время является доминирующей технологией для мобильных сотовых сетей и используется в стандартах GSM, TDMA (ANSI-136), PDC. Также применяется в системах спутниковой связи и в кабельных сетях.

Разновидности TDMA:

- CSMA/CD (англ. Carrier Sense Multiple Access with Collision Detection «множественный доступ с контролем несущей и обнаружением коллизий») – используется в Ethernet;
- CSMA/CA (англ. Carrier Sense Multiple Access With Collision Avoidance «множественный доступ с контролем несущей и предотвращением коллизий») – используется в Wi-Fi;
- другие.

CSMA/CD

CSMA/CD (англ. Carrier Sense Multiple Access with Collision Detection «множественный доступ с контролем несущей и обнаружением коллизий») – технология (IEEE 802.3) множественного доступа к общей передающей среде в локальной компьютерной сети с контролем коллизий. CSMA/CD относится к децентрализованным случайным (точнее, квазислучайным) методам. Он используется как в обычных сетях типа Ethernet, так и в высокоскоростных сетях (Fast Ethernet, Gigabit Ethernet).

Так же называют сетевой протокол, в котором используется схема CSMA/CD. Протокол CSMA/CD работает на канальном уровне в модели OSI.

Характеристики и области применения этих популярных на практике сетей связаны именно с особенностями используемого метода доступа. CSMA/CD является модификацией «чистого» Carrier Sense Multiple Access (CSMA).

Сигнал преднамеренной помехи (англ. jam signal) в телекоммуникациях – сигнал с битовым шаблоном, отправленным станцией, чтобы информировать остальные станции о том, что они не должны осуществлять передачу.

Если во время передачи кадра рабочая станция обнаруживает другой сигнал, занимающий передающую среду, она останавливает передачу, посылает сигнал преднамеренной помехи (jam signal) и ждет в течение случайного промежутка времени (известного как «backoff delay» и находимого с помощью экспоненциального двоичного алгоритма выдержки), перед тем как снова отправить кадр.

Обнаружение коллизий используется для улучшения производительности CSMA с помощью прерывания передачи сразу после обнаружения коллизии и снижения вероятности второй коллизии во время повторной передачи.

Методы обнаружения коллизий зависят от используемого оборудования, но на электрических шинах, таких как Ethernet, коллизии могут быть обнаружены сравнением передаваемой и получаемой информации. Если она различается, то другая передача накладывается на текущую (возникла коллизия), и передача прерывается немедленно. Посылается сигнал преднамеренной помехи, что вызывает задержку передачи всех передатчиков на произвольный интервал времени, снижая вероятность коллизии во время повторной попытки.

Ethernet является классическим примером протокола CSMA/CD.

CSMA/CA

Carrier Sense Multiple Access With Collision Avoidance или Carrier sensing multiple access with collision avoidance (если как в тексте рекомендации ITU-R M.1450) (CSMA/CA, «множественный доступ с контролем несущей и избеганием коллизий» или «многостанционный доступ с контролем несущей и предотвращением конфликтов» (перевод в русском тексте рекомендации ITU-R M.1450)).

CSMA/CA отличается от CSMA/CD тем, что коллизиям подвержены не пакеты данных, а только jam-сигналы. Отсюда и название «Collision Avoidance» – «предотвращение коллизий» (именно пакетов данных).

Избегание коллизий используется для того, чтобы улучшить производительность CSMA, отдав сеть единственному передающему устройству. Эта функция возлагается на jamming signal в CSMA/CA. Улучшение производительности достигается за счет снижения вероятности коллизий и повторных попыток передачи. Но ожидание jam signal создает дополнительные задержки, поэтому другие методики позволяют достичь лучших результатов. Избегание коллизий полезно на практике в тех ситуациях, когда своевременное обнаружение коллизии невозможно – например, при использовании радиопередатчиков.

Принцип действия:

1. Хост, который собирается начать передачу, посылает сигнал преднамеренной помехи.
2. После продолжительного ожидания всех хостов, которые могут послать jam signal, станция начинает передачу фрейма.
3. Если во время передачи хост обнаруживает jam signal от другого хоста, то он останавливает передачу на отрезок времени случайной длины.

4. Повторяет попытку.

Wi-Fi является классическим примером протокола CSMA/CA.

Коммутация каналов и коммутация пакетов

Соединение с коммутацией каналов – вид телекоммуникационной сети, в которой между двумя узлами сети должно быть установлено соединение (канал), прежде чем они начнут обмен информацией. Это соединение на протяжении всего сеанса обмена информацией может использоваться только указанными двумя узлами. После завершения обмена соединение должно быть соответствующим образом разорвано.

Типичным примером являются ранние телефонные сети. Абонент должен попросить оператора соединить его с другим абонентом, подключенным к тому же коммутатору или иному коммутатору через линию связи. В любом случае конечным результатом было физическое электрическое соединение между телефонными аппаратами абонентов в течение всего разговора. Проводник, задействованный для подключения, не мог быть использован для передачи других разговоров в это время, даже если абоненты на самом деле не разговаривали и на линии была тишина.

Соединение с коммутацией пакетов – способ доступа нескольких абонентов к общей сети, при котором информация разделяется на части небольшого размера (так называемые пакеты), которые передаются в сети независимо друг от друга. Узел-приемник собирает сообщение из пакетов. В таких сетях по одной физической линии связи может обмениваться данными много узлов.

Мультиплексирование – уплотнение канала, т.е. передача нескольких потоков (каналов) данных с меньшей скоростью (пропускной способностью) по одному каналу.

Сравнение коммутации каналов и коммутации пакетов

Коммутация каналов	Коммутация пакетов
Высокая стабильность параметров канала во времени	При перегрузе сети никого не «выбрасывает» с сообщением «сеть занята», сеть просто снижает всем абонентам скорость передачи
Отсутствие необходимости в передаче служебной информации после установления соединения	Необходимость в передаче служебной информации после установления соединения
Может использоваться как в аналоговых, так и в цифровых сетях связи	Может использоваться только в цифровых сетях связи
Недостаточно эффективный метод, потому что канальная емкость частично расходуется на поддержание соединений, которые установлены, но (в настоящее время) не используются	Эффективный метод использования пропускной способности. Абонент, использующий свой канал не полностью, фактически отдает пропускную способность сети остальным
Простое устройство	Сложное устройство; без микропроцессорной техники пакетную сеть наладить практически невозможно

Коммутация

Коммутация – процесс соединения абонентов коммуникационной сети через транзитные узлы.

Для коммутации служат коммутаторы. У каждого коммутатора есть CAM-таблица. CAM-таблица (Content Addressable Memory) – это таблица сопоставления MAC-адресов и портов коммутатора. Таблица очищается с определенной периодичностью и содержит информацию о всех MAC-адресах, доступных через конкретный порт.

Петля коммутации и протокол STP

Широковещательный шторм (англ. Broadcast storm) – всплеск широковещательных пакетов, который парализует работу сети. Широковещательные пакеты должны составлять не более 10 % от общего числа пакетов в сети.

Петля коммутации (Bridging loop, Switching loop) – состояние в сети, при котором происходит бесконечная пересылка фреймов между коммутаторами, подключенными в один и тот же сегмент сети.

Единственной возможностью прекратить циркулирование фрейма между сегментами сети является выключение одного из каналов связи между ними. Данную функцию реализует протокол STP, который оставляет только один возможный канал связи между сегментами сети.

STP

Spanning Tree Protocol (STP, протокол остовного дерева) – канальный протокол. Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.

Необходимость устранения топологических петель в сети Ethernet следует из того, что их наличие в реальной сети Ethernet с коммутатором с высокой вероятностью приводит к бесконечным повторам передачи одних и тех же кадров Ethernet одним и более коммутатором, отчего пропускная способность сети оказывается почти полностью занятой этими бесполезными повторами; в этих условиях, хотя формально сеть может продолжать работать, на практике ее производительность становится настолько низкой, что может выглядеть как полный отказ сети.

STP относится ко второму уровню модели OSI. Протокол описан в стандарте IEEE 802.1d. Алгоритм, заложенный в основу STP, был разработан в 1985 году Радией Перлман (Radia Perlman). Ей дали 1 неделю на разработку алгоритма. Она сделала это за 1 день, а в оставшееся время описала алгоритм в виде стихотворения.

Если в сети с мостовыми подключениями (в сегменте сети из коммутаторов) имеется несколько путей, могут образоваться циклические маршруты, и следование простым правилам пересылки данных через мост (коммутатор) приведет к тому, что один и тот же пакет будет бесконечно передаваться с одного моста на другой (передаваться по кольцу из коммутаторов).

Алгоритм остовного дерева позволяет по мере необходимости автоматически отключать передачу через мост в отдельных портах (блокировать порты коммутатора), чтобы предотвратить зацикливание в топологии маршрутов пересылки пакетов. Для использования алгоритма остовного дерева в сетевом мосте никакой дополнительной настройки не требуется.

Алгоритм остовного дерева является основой протокола STP (Spanning Tree Protocol), динамически отключающего избыточные связи в сети стандарта Ethernet (для образования древовидной топологии). STP стандартизован IEEE и поддерживается многими моделями управляемых коммутаторов, в частности включен по умолчанию на всех коммутаторах Cisco.

Суть работы протокола заключается в том, что поддерживающие его коммутаторы сети Ethernet обмениваются друг с другом информацией «о себе». На основании определенных условий (обычно в соответствии с настройками) один из коммутаторов выбирается корневым (или «root»), после чего все остальные коммутаторы по алгоритму остовного дерева выбирают для работы порты, «ближайшие» к корневому коммутатору (учитывается количество посредников и скорость линий). Все прочие сетевые порты, ведущие к корневому коммутатору, блокируются. Таким образом образуется несвязное дерево с корнем в выбранном коммутаторе.

В коммутаторах Cisco с поддержкой VLAN протокол STP по умолчанию выполняется независимо для каждой виртуальной сети.

Кроме STP, в коммутаторах могут применяться другие методики обнаружения и устранения петель – например, сравнением таблиц коммутации (списков MAC-адресов) разных портов или сравнением контрольных сумм проходящих пакетов (совпадение указывает на одинаковые пакеты, которые появляются из-за петель). По сравнению с описанными методами, случайным образом (или основываясь на каких-то догадках) блокирующими «дублирующие» порты, протокол STP обеспечивает древовидную структуру всего сегмента при любом количестве резервных линий между произвольными коммутаторами, поддерживающими STP.

Принцип действия:

1. Выбирается один корневой коммутатор.
2. Далее каждый коммутатор просчитывает кратчайший путь к корневому коммутатору. Соответствующий порт называется корневым портом (англ. Root Port). У любого некорневого коммутатора может быть только один корневой порт.
3. После этого для каждого сегмента сети, к которому присоединен более чем один мост (или несколько портов одного моста), просчитывается кратчайший путь к корневому мосту (порту). Мост, через который проходит этот путь, становится назначенным для этой сети (англ. Designated Bridge), а соответствующий порт – назначенным портом (англ. Designated port).
4. Далее во всех сегментах, с которыми соединено более одного порта моста, все мосты блокируют все порты, не являющиеся корневыми и назначенными. В итоге получается древовидная структура (математический граф) с вершиной в виде корневого коммутатора.

Основные понятия:

- Bridge ID = Bridge priority + MAC;
- Bridge priority = vlan xxx + 4096 × N, N-множитель, который назначается администратором сети (4096 × 8 = 32768 default cost);
- Cost – стоимость портов;
- Pathcost – стоимость линка в STP;
- Hello BPDU = root ID + bridge ID + cost;
- Root port (корневой порт) – это порт, который имеет минимальную стоимость до любого порта корневого коммутатора;

- Designated port (назначенный порт) – это порт, который имеет кратчайшее расстояние от назначенного коммутатора до корневого коммутатора.

Скорость передачи и стоимость пути:

Скорость передачи	**Стоимость (802.1D-1998)**	**Стоимость (802.1W-2001)**
4 Мбит/с	250	5 000 000
10 Мбит/с	100	2 000 000
16 Мбит/с	62	1 250 000
100 Мбит/с	19	200 000
1 Гбит/с	4	20 000
2 Гбит/с	3	10 000
10 Гбит/с	2	2000

Важные правила:

- Корневым (root) портом назначается порт с самой низкой стоимостью пути (path cost).
- Возможны случаи, когда стоимость пути по двум и более портам коммутатора будет одинакова, тогда выбор корневого (root) порта будет происходить на основании полученных от соседей приоритета и порядкового номера порта (Lowest Sender Port ID), например fa0/1, fa0/2, fa0/3, и корневым (root) станет порт с наименьшим номером.
- Коммутаторы по умолчанию не измеряют состояние загрузки сети в реальном времени и работают в соответствии со стоимостью (cost) интерфейсов в момент построения дерева STP.
- Каждый порт имеет свою стоимость (cost), обратно пропорциональную пропускной способности (bandwidth) порта и которую можно настраивать вручную.

Алгоритм действия:

1. После включения коммутаторов в сеть по умолчанию каждый коммутатор считает себя корневым (root).
2. Каждый коммутатор начинает посылать по всем портам конфигурационные Hello BPDU-пакеты раз в 2 секунды.
3. Если мост получает BPDU с идентификатором моста (Bridge ID) меньшим, чем свой собственный, он прекращает генерировать свои BPDU и начинает ретранслировать BPDU с этим идентификатором. Таким образом, в конце концов в этой сети Ethernet остается только один мост, который продолжает генерировать и передавать собственные BPDU. Он и становится корневым мостом (root bridge).

4. Остальные мосты ретранслируют BPDU корневого моста, добавляя в них собственный идентификатор и увеличивая счетчик стоимости пути (path cost).
5. Для каждого сегмента сети, к которому присоединено два и более портов мостов, происходит определение designated port – порта, через который BPDU, приходящие от корневого моста, попадают в этот сегмент.
6. После этого все порты в сегментах, к которым присоединено 2 и более портов моста, блокируются, за исключением root port и designated port.
7. Корневой мост продолжает посылать свои Hello BPDU раз в 2 секунды.

Каждый порт, задействованный в STP, может работать в одном из следующих режимов (ролей):

- Root Port (корневой) – порт для передачи трафика корневому коммутатору. Каждый некорневой коммутатор имеет только один корневой порт, выбранный из соображений минимальной стоимости пути.
- Designated Port (назначенный) – некорневой порт моста между сегментами сети, принимающий трафик из соответствующего сегмента. Сам мост также называется назначенным. В каждом сегменте сети может быть только один назначенный порт. У корневого коммутатора все порты – назначенные.
- Non-designated Port (неназначенный) – порт, не являющийся корневым или назначенным. Передача фреймов данных через такой порт запрещена.
- Disabled Port (отключенный) – порт, не участвующий в STP либо выключенный административно (командой shutdown).

Эволюция и расширения

Rapid Spanning Tree Protocol (RSTP)

Rapid STP (RSTP) является значительным усовершенствованием STP. В первую очередь необходимо отметить уменьшение времени сходимости и более высокую устойчивость. В немалой степени это достигнуто за счет идей, использованных Cisco Systems в качестве проприетарных расширений STP. RSTP описан в стандарте IEEE 802.1w (впоследствии включен в 802.1D-2004).

Rapid STP совместим с STP – если некое устройство использует STP, то RSTP тоже будет использовать STP с этим устройством, но в этом режиме может оказаться, что наличие RSTP на остальных устройствах не дает преимуществ по сравнению с STP.

Per-VLAN Spanning Tree Protocol (PVSTP)

Per-VLAN STP (PVSTP) в соответствии с названием расширяет функциональность STP для использования VLAN. В рамках данного протокола в каждой VLAN работает отдельный экземпляр STP. Является проприетарным расширением Cisco. Изначально протокол PVST работал только через ISL-транки, потом было разработано расширение PVST+, которое позволяло работать через гораздо более распространенные 802.1Q-транки. Существуют реализации, объединяющие свойства PVST+ и RSTP, поскольку эти расширения затрагивают независимые части протокола, в результате получается (в терминологии Cisco) Rapid PVST+. PVST+ совместим с STP и даже коммуницирует «через» коммутаторы, не поддерживающие ни PVST+, ни Rapid PVST+, за счет использования мультикастовых фреймов. Но Cisco Systems рекомендует не смешивать в одной сети коммутаторы различных производителей, чтобы избежать проблем совместимости разных реализаций и вариаций STP.

Multiple Spanning Tree Protocol (MSTP)

Вышеописанные вариации протоколов STP можно классифицировать по количеству экземпляров STP в случае, когда число VLAN более единицы. Имеются вариации протоколов, у которых на все VLAN приходится единственный экземпляр STP (собственно STP, RSTP), и вариации, у которых каждой VLAN соответствует свой экземпляр STP (PVST, PVST+, Rapid PVST+).

Некоторая избыточность вариаций с отдельным экземпляром STP для каждой VLAN состоит в том, что если топология нескольких VLAN совпадает, то соответствующие им экземпляры STP полностью повторяют работу друг друга. В таком случае в принципе ненужная работа по сути дублирующих друг друга экземпляров STP оборачивается ненужной дополнительной нагрузкой на процессор коммутатора и в конечном счете может вынудить конструкторов оборудования для обеспечения его устойчивой работы выбирать более мощный процессор с большим энергопотреблением, что может повлечь за собой дополнительные затраты на электропитание и охлаждение как при изготовлении оборудования, так и при эксплуатации.

В этом отношении особняком стоит Multiple STP (MSTP). В один экземпляр MST могут входить несколько виртуальных сетей, при условии что их топология одинакова (в смысле входящих во VLAN коммутаторов и соединений между ними). Минимальное количество экземпляров MSTP соответствует количеству уникальных топологически групп VLAN в домене второго уровня (опять же на уровне коммутаторов и соединений между ними). MSTP налагает важное ограничение: все коммутаторы, участвующие в MSTP, должны иметь одинаково сконфигурированные группы VLAN (MST instances), что ограничивает гибкость при изменении конфигурации сети.

MSTP описан в стандарте IEEE 802.1s (впоследствии включен в 802.1Q-2003).

Shortest Path Bridging (SPB)

Shortest Path Bridging (SPB) IEEE 802.1aq преодолевает ограничения блокировки.

PoE

Power over Ethernet (PoE) – технология, позволяющая передавать удаленному устройству электрическую энергию вместе с данными через стандартную витую пару в сети Ethernet. Данная технология предназначается для IP-телефонии, точек доступа беспроводных сетей, IP-камер, сетевых концентраторов и других устройств, к которым нежелательно или невозможно проводить отдельный электрический кабель.

Технология PoE описана стандартами IEEE 802.3af-2003 и IEEE 802.3at-2009. Существует несколько вариантов этой технологии, предшествующих первому стандарту, но они мало распространены.

Согласно стандарту IEEE 802.3af, обеспечивается постоянный ток до 400 мА с номинальным напряжением 48 В (от 36 до 57 В) через две пары проводников в четырехпарном кабеле для обеспечения максимальной мощности 15,4 Вт. Стандарт определяет 5 классов устройств, питаемых по технологии PoE, от нулевого до четвертого. Каждому классу соответствуют свои параметры мощности и тока. Наиболее распространен первый класс. Для него выходной ток равен 120 мА, а мощность может варьироваться от 0,44 до 3,84 Вт. Четвертый класс не используется и зарезервирован на будущее.

Стандарт IEEE 802.3at-2009, известный также как PoE+ или PoE plus, предусматривает подачу мощности до 25,5 Вт. Этот стандарт запрещает устройству-потребителю получать питание по

всем четырем парам Ethernet-кабеля одновременно. Однако некоторые производители заявили о выпуске устройств, потребляющих питание по всем парам и таким образом получающих мощность до 60 Вт.

Помимо использования двух свободных пар в сети 10/100Base-T, стандарт предусматривает использование фантомного питания для передачи электроэнергии. Подача питающего напряжения осуществляется как разность потенциалов между парами проводников (например, по методу B между парами 4–5 и 7–8). Более современные устройства поддерживают передачу электричества по сигнальным проводам, а именно – по 1, 2, 3, 6. Этот вариант существенно снижает затраты на кабель и монтажные работы. Такая технология PoE часто встречается в сфере IP-видеонаблюдения и точках доступа. Стандарт определяет пары проводников для подачи питания и их полярность электропитания. Эта технология работает с существующей кабельной системой, включая кабели категории 5, без необходимости внесения каких-либо модификаций в существующую СКС.

Технология PoE не оказывает влияния на качество передачи данных. Для ее реализации используются свойства физического уровня Ethernet:

- *с использованием высокочастотных трансформаторов на обоих концах линии с центральным отводом от обмоток.* Постоянное напряжение питания подается на центральные отводы вторичных обмоток этих трансформаторов и так же с центральных отводов снимается на приемной стороне. Использование центральных отводов сигнальных трансформаторов позволяет без взаимного влияния передавать питание по сигнальным парам, то есть передавать по одним и тем же проводникам и высокочастотные данные, и постоянное напряжение питания;
- *использование свободных пар для подачи питания.* Современные кабельные сети Ethernet, соответствующие стандарту 100BASE-TX, состоят из четырех пар, две из которых не задействованы.

Питающие устройства (инжекторы; англ. power sourcing equipment, сокр. PSE) отличаются по способу подключения питания, при этом питаемые устройства (сплиттеры; англ. powered device, сокр. PD) являются универсальными. Питаемые устройства должны проектироваться с возможностью приема питания в любом варианте, в том числе и при изменении полярности (например, когда используется перекрестный кабель).

Питающее устройство подает питание в кабель только в том случае, если подключаемое устройство является устройством питаемого типа. Таким образом, оборудование, не поддерживающее технологию PoE и случайно подключенное к питающему устройству, не будет выведено из строя. Процедура подачи и отключения питания на кабель состоит из нескольких этапов.

Определение подключения

Этап определения подключения служит для определения, является ли подключенное на противоположном конце кабеля устройство питаемым (PD). На этом этапе питающее устройство (PSE) подает на кабель напряжение от 2,8 до 10 В и определяет параметры входного сопротивления подключаемого устройства. Для питаемого устройства это сопротивление составляет от 19 до 26,5 кОм с параллельно подключенным конденсатором емкостью от 0 до 150 нФ. Только после проверки соответствия параметров входного сопротивления для питаемого устройства питающее устройство переходит к следующему этапу, в противном случае питающее устройство повторно, через промежуток времени не менее 2 мс, пытается определить подключение.

Классификация

После этапа определения подключения питающее устройство может дополнительно выполнять этап классификации, определяя диапазон мощностей, потребляемых питаемым устройством, чтобы затем управлять этой мощностью. Каждому питаемому устройству, в зависимости от заявленной потребляемой мощности, будет присвоен класс от 0 до 4. Минимальный диапазон мощностей имеет класс 0. Класс 4 зарезервирован стандартом для дальнейшего развития. Питающее устройство может снять напряжение с кабеля, если питаемое устройство стало потреблять мощность больше объявленной во время классификации. Классификация выполняется путем введения в кабель питающим устройством напряжения от 14,5 до 20,5 В и измерения тока в линии.

Токи классификации:

Класс	**Максимальная мощность, потребляемая запитываемым устройством (PD), Вт**	**Токи классификации по стандартам IEEE 802.3af/at, измеряемые источником питания (PSE), мА**
0	0,44–12,95	0–5
1	0,44–3,94	8–13
2	3,84–6,49	16–21
3	6,49–12,95	25–31
4	12,95–25,5	35–45
5	> 25,5	

Классы потребления мощности питаемых устройств:

Класс	**Вт на порт PoE**	**Вт на устройство**
0	15,4	От 0,44 до 12,95
1	4,5	От 0,44 до 3,84
2	7	От 3,84 до 6,49
3	15,4	От 6,49 до 12,95
4	30	От 12,95 до 25,5

Подача полного напряжения

После прохождения этапов определения и классификации питающее устройство подает в кабель напряжение 48 В с фронтом нарастания не быстрее 400 мс. После подачи полного напряжения на питаемое устройство питающее устройство осуществляет контроль его работы двумя способами:

- если питаемое устройство в течение 400 мс будет потреблять ток меньше 5 мА, то питающее устройство снимает питание с кабеля;
- питающее устройство подает в кабель напряжение 1,9–5,0 В с частотой 500 Гц и вычисляет входное сопротивление; если это сопротивление будет больше 1980 кОм в течение 400 мс, питающее устройство снимает питание с кабеля.

Кроме того, питающее устройство непрерывно следит за током перегрузки. Если питаемое устройство будет потреблять ток более 400 мА в течение 75 мс, питающее устройство снимет питание с кабеля.

Отключение

Когда питающее устройство определяет, что питаемое устройство отключено от кабеля или произошло превышение потребляемого тока питаемым устройством, происходит снятие напряжения с кабеля за время не менее 500 мс.

Passive PoE

Альтернативное решение, называемое Passive PoE, в виде промежуточного комплекта адаптеров (инжектор и сплиттер) может поддерживать только электрические характеристики соответствия стандарту 802.3af, но не протокольные. Passive PoE несовместим со стандартом IEEE 802.3af, тем не менее его используют многие компании, и об этом необходимо помнить при подключении устройства посредством PoE, так как маркировка такого оборудования также содержит указание на совместимость с PoE (например, Planet POE-100, D-Link DWL-P200).

Особенности

Реализация схемотехники потребителя предусматривает два возможных варианта:

- с гальванической развязкой (импульсный трансформатор);
- с непосредственной связью (понижающий конвертер).

Использование второго типа допускается только в случае, если потребитель не имеет гальванически связанных интерфейсных разъемов, таких как антенный соединитель, и не имеет гальванической связи с корпусом или внешними металлическими частями устройства (или используется непроводящий корпус).

При использовании молниезащиты в системах с PoE следует учитывать совместимость защитных устройств с той или иной реализацией стандарта питания по Ethernet (в частности, дополнительная гальваническая развязка в грозозащитном устройстве естественным образом приводит к неработоспособности PoE, как и слишком низковольтные нелинейные элементы защиты).

Виды коммутаторов

При выборе коммутаторов надо учитывать следующие параметры:

- скорость;
- количество портов;
- управляемые и неуправляемые;
- L2 и L3;
- наличие аплинков (uplink);
- пассивное или активное охлаждение;
- настольное или стоечное исполнение;
- наличие PoE (Power over Ethernet);
- суммарная мощность PoE;
- производительность;
- поддержка STP;
- поддержка VLAN.

Протокол IP

Введение

Internet Protocol (IP, досл. «межсетевой протокол») – маршрутизируемый протокол сетевого уровня стека TCP/IP. Именно IP стал тем протоколом, который объединил отдельные компьютерные сети во всемирную сеть Интернет. Неотъемлемой частью протокола является адресация сети.

IP объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами сети через произвольное число промежуточных узлов (маршрутизаторов). Он классифицируется как протокол сетевого уровня по сетевой модели OSI. IP не гарантирует надежной доставки пакета до адресата – в частности, пакеты могут прийти не в том порядке, в котором были отправлены, продублироваться (приходят две копии одного пакета), оказаться поврежденными (обычно поврежденные пакеты уничтожаются) или не прийти вовсе. Гарантию безошибочной доставки пакетов дают некоторые протоколы более высокого уровня – транспортного уровня сетевой модели OSI – например, TCP, которые используют IP в качестве транспорта.

Существует две версии протокола: IPv4 и IPv6:

Характеристика	**IPv4**	**IPv6**
Год	1981	1996
Спецификация	RFC 791	RFC 2460
Длина адреса	32 бита	128 бит
Количество адресов	4 294 967 296 (2^{32})	79 228 162 514 264 337 593 543 950 336 (2^{128})
Формат записи	nnn.nnn.nnn.nnn	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
Применение	Используется	Вводится в эксплуатацию

IP-адрес

Уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP. IP-адрес может быть назначен статически или динамически.

TTL

Time to live (TTL) в вычислительной технике и компьютерных сетях – предельный период времени или повторенийв течение которых набор данных (пакет) может существовать до своего исчезновения.

В IPv4 TTL представляет собой восьмиразрядное поле IP-заголовка.

Определяет максимальное количество хопов (hop, то есть прыжок, участок между маршрутизаторами), которые пакет может пройти. Наличие этого параметра не позволяет пакету бесконечно ходить по сети. Каждый маршрутизатор при маршрутизации должен уменьшать значение TTL на единицу, но некоторые шлюзы можно настроить, чтобы игнорировать это. Пакеты, не достигшие адресата, но время жизни которых стало равно нулю, уничтожаются, а отправителю посылается сообщение ICMP Time Exceeded. Если требуется, чтобы пакет не был маршрутизирован (то есть был принят только в своем сегменте), то выставляется TTL=1. На отправке пакетов с разным временем жизни основана трассировка их пути прохождения (traceroute). Максимальное значение TTL=255. Обычное начальное значение TTL=64 (Linux, Mac, Android, iOS), TTL=128 (Windows).

Изначально, по стандарту RFC 791, время жизни (TTL) в протоколе IPv4 должно было измеряться в секундах (отсюда и название). Каждая секунда ожидания в очереди узла (например, маршрутизатора), а также каждый переход на новый узел, через который проходит датаграмма, должен был уменьшить значение TTL на одну единицу. На практике это не прижилось, и поле TTL просто уменьшается на единицу на каждом транзитном узле (хопе), через который проходит датаграмма. Для того чтобы отразить это, в протоколе IPv6 поле TTL переименовано в «хоп лимит» (Hop Limit).

Коммутаторы традиционно работают на канальном уровне и не уменьшают TTL.

Контроль TTL часто используется провайдерами для обнаружения трафика несанкционированного подключенного устройства. К примеру, если на смартфоне включить режим «Мобильная точка доступа» (тетеринг), TTL от подключенных устройств будет на 1 меньше ожидаемого. Тем самым блокируется доступ для этих устройств.

Фрагментация

При доставке IP-пакета он проходит через разные каналы доставки. Возможно возникновение ситуации, когда размер пакета превысит возможности узла системы связи. В этом случае протокол предусматривает возможность дробления пакета на уровне IP в процессе доставки. Соответственно, к конечному получателю пакет придет в виде нескольких пакетов, которые необходимо собрать в один перед дальнейшим анализом. Возможность дробления пакета с последующей сборкой называется IP-фрагментацией.

В протоколе предусмотрена возможность запрещения фрагментации конкретного пакета. Если такой пакет нельзя передать через сегмент связи целиком, то он уничтожается, а отправителю направляется ICMP-сообщение о проблеме.

MTU

В компьютерных сетях термин «maximum transmission unit» (MTU) означает максимальный размер полезного блока данных одного пакета (англ. payload), который может быть передан протоколом без фрагментации. Обычно заголовки протокола не входят в MTU, но в некоторых протоколах заголовки могут учитываться. Когда говорят об MTU, обычно имеют в виду протокол канального уровня сетевой модели OSI. Однако этот термин может применяться и для других уровней:

- L1 – media mtu (полный L2-кадр);
- L2 – hw mtu, system mtu;
- L3 – ip mtu (ip-заголовок учитывается), mtu;
- L4 – tcp mss.

Внесистемные: tunnel mtu, vlan mtu, mpls mtu.

Ограничение на максимальный размер кадра накладывается по нескольким причинам:

- Для уменьшения времени на повторную передачу в случае потери или неисправимого искажения пакета. Вероятность потерь растет с увеличением длины пакета.
- Чтобы при полудуплексном режиме работы хост не занимал долгое время канал (также для этой цели используется межкадровый интервал (англ. Interframe gap)).
- Чем больше отправляемый пакет, тем дольше ждут отправления другие пакеты, особенно в последовательных интерфейсах. Поэтому маленький MTU был актуален во времена медленных коммутируемых соединений.
- Малый размер и быстродействие сетевых буферов входящих и исходящих пакетов. Однако слишком большие буферы тоже ухудшают производительность.

Значение MTU определяется стандартом соответствующего протокола, но может быть задано автоматически для нужного потока (протоколом PMTUD) или вручную для нужного интерфейса. На некоторых интерфейсах MTU по умолчанию может быть установлено ниже максимально возможного. Значение MTU ограничено снизу, как правило, минимально допустимой длиной кадра.

Для высокопроизводительной сети причины, вызвавшие начальные ограничения MTU, устарели. В связи с этим для Ethernet был разработан стандарт Jumbo-кадров с увеличенным MTU.

Некоторые протоколы, например из группы протоколов ATM, оперируют ячейками фиксированной длины. Для них нет возможности изменить MTU. В некоторых случаях этот подход приводит к лучшему управлению сетевыми потоками.

Номинальная скорость – битовая скорость передачи данных, поддерживаемая на интервале передачи одного пакета без различия служебных и пользовательских заголовков. Очевидно, что чем меньше пакет, тем быстрее он передастся.

Эффективная скорость – это средняя скорость передачи пользовательских данных (нагрузки) в потоке. Этот параметр зависит от соотношения длин служебных заголовков к нагрузке. Во многих случаях некоторый объем информации эффективнее передавать большими пакетами из-за меньших накладных расходов. Корректно сравнивать скорости потоков можно только для одного и того же объема данных, которые требуется передать единовременно.

Чем больше полезная нагрузка пакета по отношению к его заголовкам, тем выше скорость передачи полезной информации и процент использования канала (channel utilization).

Поскольку MTU – это верхняя граница длины полезной нагрузки, то максимальная скорость достигается, когда нагрузки всех пакетов в потоке имеют длину, равную MTU.

Существует несколько способов увеличения пропускной способности в контексте длин пакетов:

1. Уменьшение межкадрового интервала. Для Fast Ethernet он по умолчанию равен 0,96 мкс, т.е. времени, за которое могло бы быть передано 12 байт. Некоторые сетевые адаптеры в полнодуплексном режиме могут передавать и получать кадры с уменьшенным межкадровым интервалом.
2. Сжатие заголовков. Пример реализации – метод сжатия заголовков TCP/IP Якобсона.
3. Сжатие нагрузки низкого уровня. Пример реализации – IP Payload Compression Protocol.
4. Решение проблемы передачи небольших данных (tinygram problem) за счет придерживания в буфере малых данных, чтобы отправить один большой пакет. Пример реализации – алгоритм Нейгла. Частный случай этой проблемы – «болтливые» протоколы, посылающие множество запросов там, где можно обойтись одним. Существуют программные и аппаратные решения, осуществляющие оптимизацию таких соединений, – например, у компании Riverbed Technology.

Известные проблемы

Хост знает значение MTU для собственного (возможно, и своих соседей) интерфейса, но минимальное значение MTU для всех узлов сети обычно неизвестно. Другая потенциальная проблема заключается в том, что протоколы более высокого уровня могут создавать пакеты большего размера, не поддерживаемые другими узлами сети.

Прохождение больших пакетов по сети с фрагментацией

Для устранения этих проблем IP поддерживает фрагментацию, что позволяет разбивать дейтаграмму на меньшие кусочки, каждый из которых будет достаточно мал, чтобы беспрепятственно пройти через узел, из-за которого происходит фрагментация. Фрагменты пакетов маркируются таким образом, чтобы IP целевого хоста мог произвести сборку фрагментов в оригинальную дейтаграмму. Фрагментация пакетов имеет свои недостатки:

- целевой хост должен получить все фрагменты для того, чтобы собрать пакет. Если хотя бы один фрагмент утерян – весь пакет должен быть отправлен заново;
- как правило, фрагментацию выполняют более медленные процессоры, нежели те, что обрабатывают транзитный трафик. В некоторых случаях задержки, которые вызовет фрагментация всех пакетов, могут быть сочтены неприемлемыми;
- увеличивается нагрузка на процессоры промежуточных маршрутизаторов и машины адресата;
- увеличиваются требования к памяти маршрутизатора, т.к. необходимо хранить в буфере все фрагменты IP-пакета;
- некоторые межсетевые экраны могут блокировать фрагменты;
- из-за копии IP-заголовка для каждого фрагмента неэффективно используется полоса пропускания;
- протоколам маршрутизации, например OSPF, требуется согласованный MTU для корректной работы.

Для обозначения кадров, которые имеют ненормативный размер, в сетях Ethernet применяются следующие термины:

- RUNT (коротышка) – кадр, размер которого менее 64 байт (512 бит);
- LONG (длинный) – кадр, размер которого лежит в пределах от 1518 до 6000 байт;
- GIANT (гигант) – кадр, размер которого превышает 6000 байт.

Path MTU discovery

Термин Path MTU означает наименьший MTU на пути следования пакета в сети.

Хотя фрагментация решает проблему несоответствия размеров пакетов и значения MTU, она ощутимо снижает производительность сетевых устройств. В связи с этим в 1988 году была предложена альтернативная технология, названная Path MTU discovery (RFC 1191). Суть технологии заключается в том, что при соединении двух хостов устанавливается параметр DF (англ. don't fragment «не фрагментировать»), который запрещает фрагментацию пакетов. Это приводит к тому, что узел, значение MTU которого меньше размера пакета, отклоняет передачу пакета и отправляет сообщение ICMP: «Необходима фрагментация, но установлен флаг ее запрета (DF)». Хост-отправитель уменьшает размер пакета и отсылает его заново. Такая операция происходит до тех пор, пока пакет не будет достаточно мал, чтобы дойти до хоста-получателя без фрагментации.

Однако и у этой технологии существуют потенциальные проблемы. Некоторые маршрутизаторы настраиваются администраторами на полное блокирование ICMP-пакетов (это не очень грамотно, но может быть самым простым решением нескольких проблем безопасности). В результате, если размер пакета не соответствует значению MTU на определенном участке, пакет отбрасывается, а хост-отправитель не может получить информацию о значении MTU и не отправляет пакет заново. Поэтому соединение между хостами не устанавливается. Проблема получила название «MTU Discovery Black Hole» (RFC 2923), и протокол был модифицирован для детектирования таких маршрутизаторов. Одной из распространенных проблем при работе в сети, блокирующей ICMP-пакеты, является работа в IRC, когда пользователь успешно проходит авторизацию, но не может получить так называемое MOTD (message of the day), в результате чего использование сети не представляется возможным.

Проблема представляет потенциальную опасность для любого PPPoE-соединения, использующего MTU меньше типового (1500 байт).

Существует несколько вариантов решения этой проблемы. Самым простым, безусловно, является отмена фильтрации пакетов ICMP. Однако зачастую подобная операция находится вне компетенции пользователя. Поэтому проблему решают путем ручной настройки размера передаваемого пакета на шлюзе пользователя. Для этого меняют значение MSS (максимальный размер сегмента, то есть величина у которой MTU меньше на 40 байт в случае протокола IPv4). При установке соединения хосты обмениваются информацией о максимальном размере сегмента, который каждый из них сможет принять. Поэтому, меняя значение MSS, заставляют оба хоста обмениваться пакетами, которые шлюз пользователя сможет заведомо принять без фрагментации.

Кроме того, существуют методы отмены бита DF с целью разрешения фрагментации. Однако метод корректировки MSS является предпочтительным.

В маршрутизаторах Cisco реализация PMTUD для туннеля поддерживает только TCP-пакеты.

QoS

QoS (англ. quality of service «качество обслуживания») – этим термином в области компьютерных сетей называют вероятность того, что сеть связи соответствует заданному соглашению о трафике. В узком техническом значении этот термин означает набор методов для управления ресурсами пакетных сетей.

Для большинства случаев качество связи определяется четырьмя параметрами:

1. Скорость передачи информации (Bitrate). Описывает номинальную пропускную способность среды передачи информации. Зависит от ширины полосы пропускания канала связи (Гц) и отношения сигнал/шум. Измеряется в bit/s (bps), kbit/s (Kbps), Mbit/s (Mbps), Gbit/s (Gbps).
2. Задержка при передаче пакета (Delay). Измеряется в миллисекундах.
3. Колебания (дрожание) задержки при передаче пакетов – джиттер.
4. Потеря пакетов (Packet loss). Определяет количество пакетов, потерянных в сети во время передачи.

Для простоты понимания канал связи можно представить в виде условной трубы, а пропускную способность описать как функцию двух параметров: диаметра трубы и ее длины.

Когда передача данных сталкивается с проблемой «бутылочного горлышка» для приема и отправки пакетов на маршрутизаторах, то обычно используется метод FIFO: первый пришел – первый ушел (First In – First Out). При интенсивном трафике это создает заторы. Ситуация решается крайне простым образом: все пакеты, не вошедшие в буфер очереди FIFO (на вход или на выход), игнорируются маршрутизатором и, соответственно, теряются безвозвратно. Более разумный метод – использовать «умную» очередь, в которой приоритет у пакетов зависит от типа сервиса, – ToS. Необходимое условие: пакеты должны уже нести метку типа сервиса для создания «умной» очереди. Обычные пользователи чаще всего сталкиваются с термином «QoS» в домашних маршрутизаторах с поддержкой QoS. Например, весьма логично дать высокий приоритет пакетам VoIP и низкий – пакетам FTP, SMTP и клиентам файлообменной сети.

Определенное качество обслуживания может потребоваться для ряда сетевых приложений, в частности:

- потоковые мультимедиаприложения требуют гарантированную пропускную способность канала;
- VoIP и видеоконференция требуют небольших значений джиттера и задержки;
- ряд приложений, например удаленная хирургия, требуют гарантированного уровня надежности.

IP-адресация (введение)

IP-адрес (ˌaɪ ˈpiː-адрес; является словообразовательной полукалькой английского IP address, буквенной аббревиатурой от англ. Internet Protocol Address «адрес интернет-протокола») – уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP. IP-адрес может быть назначен статически или динамически.

- Статический IP-адрес – это адрес, назначенный хосту администратором сети вручную.
- Динамический IP-адрес – это адрес, назначенный хосту с помощью DHCP-сервера.
- Постоянный IP-адрес – это адрес, который назначен хосту на постоянной основе. Он может быть назначен статически или динамически.

Изначальная система счисления двоичная. Для удобства используется перевод в десятичную.

В сети Интернет требуется глобальная уникальность адреса; в случае работы в локальной сети требуется уникальность адреса в пределах сети. В версии протокола IPv4 IP-адрес имеет длину 4 байта, а в версии протокола IPv6 IP-адрес имеет длину 16 байт.

IPv4 использует 32-битные (4-байтные) адреса, ограничивающие адресное пространство 4 294 967 296 (232) возможными уникальными адресами. Традиционной формой записи IPv4-адреса является запись в виде четырех десятичных чисел (от 0 до 255), разделенных точками. Через дробь указывается длина маски подсети. Например, 192.168.35.16/24. Одно такое число называется октет.

Существуют служебные IP-адреса, которые не могут быть назначены хосту:

- адрес сети – адрес логической группы IP-адресов;
- широковещательный адрес – адрес для отправки сообщений всем устройствам в сети.

Один и тот же адрес может быть адресом узла, адресом сети или широковещательным адресом в зависимости от маски сети.

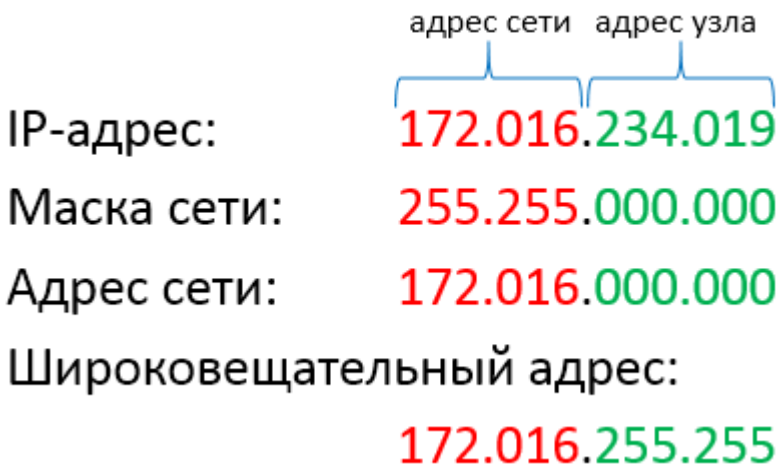
Маска сети

Маска сети разделяет IP-адрес на две части: адрес сети и адрес узла. Формат записи:

- полный десятичный вид (пример: 255.255.255.0);
- через дробь (пример: 192.168.10.15/24).

Все нули в двоичном виде в адресе узла – это адрес сети. Все единицы в двоичном виде в адресе узла – это широковещательный адрес.

При наложении маски сети на IP-адрес можно выяснить, какая часть IP-адреса относится к идентификатору сети, а какая к идентификатору узла.



Такой способ подходит только для масок со значениями 255 и 0!

Для объединения разных сетей нужен маршрутизатор. Если к коммутатору подключены хосты с разными сетями, то они не смогут взаимодействовать.

Перевод из двоичной системы счисления в десятичную

Система счисления (англ. numeral system или system of numeration) – символический метод записи чисел, представление чисел с помощью письменных знаков. Существуют: двоичная, десятичная, шестнадцатеричная и др. системы счисления.

Степени двойки:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Пример расчета: 00100110 = 0 + 0 + 2^5 + 0 + 0 + 2^2 + 2^1 + 0 = 32 + 4 + 2 = 38

Перевод из десятичной системы в двоичную

Делимое : делитель = частное (15 : 3 = 5)

Алгоритм:

1. Делим число на два.
2. Если делится без остатка, то записываем 0, если делится с остатком, то записываем 1.
3. Частное заново делим на два.
4. Если делится без остатка, то записываем 0, если делится с остатком, то записываем 1.
5. И т.д., пока не дойдем до 1 : 2 = 0 с остатком – значит, записываем 1.
6. Результат записываем справа налево. То есть последняя (нижняя) цифра (1) будет самой левой.
7. Если число знаков меньше 8, то слева дописываем недостающее до 8 количество нулей. Например, если результат: 11010, то записываем: 00011010.

Пример № 1. Число 137

137:2 = 68 с остатком 1

68:2 = 34 без остатка 0

34:2 = 17 без остатка 0

17:2 = 8 с остатком 1

8:2 = 4 без остатка 0

4:2 = 2 без остатка 0

2:2 = 1 без остатка 0

1:2 = 0 с остатком 1

- Результат записываем справа налево. То есть нижняя цифра (1) будет самой левой и т.д. : 10001001
- Т. к. число знаков равно 8-ми, то слева дописывать нули не надо

137 = 10001001

Пример № 2. Число 56

56:2 = 28 без остатка 0

28:2 = 14 без остатка 0

14:2 = 7 без остатка 0

7:2 = 3 с остатком 1

3:2 = 1 с остатком 1

1:2 = 0 с остатком 1

- Результат записываем справа налево. То есть нижняя цифра (1) будет самой левой и т.д. : 111000
- Т. к. число знаков меньше 8-ми, то слева дописываем недостающее до 8-ми количество нулей: 00111000

56 = 00111000

Классовая и бесклассовая адресации

Классовая адресация

Классовая адресация IP-сетей – архитектура сетевой адресации, которая использовалась в Интернете в период с 1981 по 1993 год, до введения бесклассовой междоменной маршрутизации (CIDR, англ. Classless Inter-Domain Routing).

Этот метод адресации делит адресное пространство протокола Интернета версии 4 (IPv4) на пять классов адресов: A, B, C, D и E. Принадлежность адреса к конкретному классу задается первыми битами адреса. Каждый класс определяет либо соответствующий размер сети, то есть количество возможных адресов хостов внутри данной сети (классы A, B, C), либо сеть многоадресной передачи (класс D). Диапазон адресов пятого класса (E) был зарезервирован для будущих или экспериментальных целей.

Использование адресации на базе классов адресов в IP-сетях в основном прекращено: остатки классовых сетевых концепций на практике остаются лишь в ограниченном объеме в параметрах конфигурации по умолчанию некоторых сетевых программных и аппаратных компонентов (например, маски подсети по умолчанию). Применение этого метода адресации не позволяет экономно использовать ограниченный ресурс адресов IPv4, поскольку невозможно применение произвольных масок подсетей к различным подсетям.

Изначально адресация в сетях IP осуществлялась на основе классов: первые биты определяли класс сети, а по классу сети можно было сказать, сколько битов было отведено под номер сети и номер узла. Всего существовало 5 классов:

Одним из подходов был классовый метод адресации.

Класс	Первые биты	Распределение байтов (C – сеть, X – хост)	Число возможных адресов сетей	Число возможных адресов хостов	Маска подсети	Начальный адрес	Конечный адрес
A	0	C.X.X.X	128	16 777 214	255.0.0.0	0.0.0.0	127.255.255.255
B	10	C.C.X.X	16 384	65 534	255.255.0.0	128.0.0.0	191.255.255.255
C	110	C.C.C.X	2 097 152	254	255.255.255.0	192.0.0.0	223.255.255.255
D	1110	Групповой адрес				224.0.0.0	239.255.255.255
E	1111	Зарезервировано				240.0.0.0	255.255.255.255

Другая версия таблицы:

Класс	Маска	Начальный адрес	Конечный адрес	Число сетей	Число адресов
A	255.0.0.0	0.0.0.0	127.255.255.255	128	16 777 216
B	255.255.0.0	128.0.0.0	191.255.255.255	16 384	65 536
C	255.255.255.0	192.0.0.0	223.255.255.255	2 097 152	256
D	Групповой адрес	224.0.0.0	239.255.255.255	-	-
E	Зарезервировано	240.0.0.0	255.255.255.255	-	-

Бесклассовая адресация

Бесклассовая адресация (англ. Classless Inter-Domain Routing, CIDR) – метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жесткие рамки классовой адресации. Использование этого метода позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку возможно применение различных масок подсетей к различным подсетям.

IP-адрес является массивом битов. Принцип IP-адресации – выделение множества (диапазона, блока, подсети) IP-адресов, в котором некоторые битовые разряды имеют фиксированные значения, а остальные разряды пробегают все возможные значения. Блок адресов задается указанием начального адреса и маски подсети. Бесклассовая адресация основывается на переменной длине маски подсети (англ. variable length subnet mask, VLSM), в то время как в классовой (традиционной) адресации длина маски строго фиксирована 0, 1, 2 или 3 установленными октетами.

Множество всех адресов соответствует нулевой маске подсети и обозначается /0, а конкретный адрес IPv4 – маске подсети с длиной префикса в 32 бита, обозначаемой /32.

Возможные маски

Р/маска	**До последнего IP в подсети**	**Маска**	**Всего адресов**	**Хостовых адресов**	**Класс**
a.b.c.d**/32**	+0.0.0.0	255.255.255.255	1	(нет)	1/256 C
a.b.c.d**/31**	+0.0.0.1	255.255.255.254	2	2	1/128 C
a.b.c.d**/30**	+0.0.0.3	255.255.255.252	4	2	1/64 C
a.b.c.d**/29**	+0.0.0.7	255.255.255.248	8	6	1/32 C
a.b.c.d**/28**	+0.0.0.15	255.255.255.240	16	14	1/16 C
a.b.c.d**/27**	+0.0.0.31	255.255.255.224	32	30	1/8 C
a.b.c.d**/26**	+0.0.0.63	255.255.255.192	64	62	1/4 C
a.b.c.d**/25**	+0.0.0.127	255.255.255.128	128	126	1/2 C
a.b.c.0**/24**	+0.0.0.255	255.255.255.000	256	254	1 C
a.b.c.0**/23**	+0.0.1.255	255.255.254.000	512	510	2 C
a.b.c.0**/22**	+0.0.3.255	255.255.252.000	1024	1022	4 C
a.b.c.0**/21**	+0.0.7.255	255.255.248.000	2048	2046	8 C
a.b.c.0**/20**	+0.0.15.255	255.255.240.000	4096	4094	16 C
a.b.c.0**/19**	+0.0.31.255	255.255.224.000	8192	8190	32 C
a.b.c.0**/18**	+0.0.63.255	255.255.192.000	16 384	16 382	64 C
a.b.c.0**/17**	+0.0.127.255	255.255.128.000	32 768	32 766	128 C
a.b.0.0**/16**	+0.0.255.255	255.255.000.000	65 536	65 534	256 C = 1 B
a.b.0.0**/15**	+0.1.255.255	255.254.000.000	131 072	131 070	2 B
a.b.0.0**/14**	+0.3.255.255	255.252.000.000	262 144	262 142	4 B
a.b.0.0**/13**	+0.7.255.255	255.248.000.000	524 288	524 286	8 B
a.b.0.0**/12**	+0.15.255.255	255.240.000.000	1 048 576	1 048 574	16 B
a.b.0.0**/11**	+0.31.255.255	255.224.000.000	2 097 152	2 097 150	32 B
a.b.0.0**/10**	+0.63.255.255	255.192.000.000	4 194 304	4 194 302	64 B
a.b.0.0**/9**	+0.127.255.255	255.128.000.000	8 388 608	8 388 606	128 B
a.0.0.0**/8**	+0.255.255.255	255.000.000.000	16 777 216	16 777 214	256 B = 1 A
a.0.0.0**/7**	+1.255.255.255	254.000.000.000	33 554 432	33 554 430	2 A
a.0.0.0**/6**	+3.255.255.255	252.000.000.000	67 108 864	67 108 862	4 A

a.0.0.0/**5**	+7.255.255.255	248.000.000.000	134 217 728	134 217 726	8 A
a.0.0.0/**4**	+15.255.255.255	240.000.000.000	268 435 456	268 435 454	16 A
a.0.0.0/**3**	+31.255.255.255	224.000.000.000	536 870 912	536 870 910	32 A
a.0.0.0/**2**	+63.255.255.255	192.000.000.000	1 073 741 824	1 073 741 822	64 A
a.0.0.0/**1**	+127.255.255.255	128.000.000.000	2 147 483 648	2 147 483 646	128 A
0.0.0.0/**0**	+255.255.255.255	000.000.000.000	4 294 967 296	4 294 967 294	256 A

Расчет IP-адресации в двоичном виде

Конъюнкция (от лат. conjunctio «союз, связь») – логическая операция, по смыслу максимально приближенная к союзу «и». Синонимы: логическое «И», логическое умножение, иногда просто «И». В булевой алгебре конъюнкция – это функция двух, трех или более переменных (они же – операнды операции, они же – аргументы функции). Переменные могут принимать значения из множества {0,1}. Результат также принадлежит множеству {0,1}. Правило: результат равен 1, если все операнды равны 1; во всех остальных случаях результат равен 0. Пример из жизни: машина поедет, если в ней есть бензин «И» ее завести.

Алгоритм расчета IP-адресации в двоичном виде:

1. IP-адрес и маску сети представить в двоичном виде.
2. Наложить маску сети на IP-адрес.
3. Произвести операцию логического «И».
4. Адрес сети – это все нули в адресе хоста.
5. Широковещательный адрес – это все единицы в адресе хоста.
6. Первый IP-адрес – в адресе хоста все знаки «0», кроме последнего, который «1».
7. Последний IP-адрес – в адресе хоста все знаки «1», кроме последнего, который «0».

Пример № 1

IP-адрес	192.168.035.046/24	11000000.10101000.00100011.00101110
Маска	255.255.255.000	11111111.11111111.11111111.00000000
Адрес сети	192.168.035.000/24	11000000.10101000.00100011.00000000
Широковещательный адрес	192.168.035.255	11000000.10101000.00100011.11111111
Первый IP-адрес	192.168.035.001	11000000.10101000.00100011.00000001
Последний IP-адрес	192.168.035.254	11000000.10101000.00100011.11111110

Пример № 2

IP-адрес	010.010.146.014/18	00001010.00001010.10010010.00001110
Маска	255.255.192.000	11111111.11111111.11000000.00000000
Адрес сети	010.010.128.000/18	00001010.00001010.10000000.00000000
Широковещательный адрес	010.010.191.255	00001010.00001010.10111111.11111111
Первый IP-адрес	010.010.128.001	00001010.00001010.10000000.00000001
Последний IP-адрес	010.010.191.254	00001010.00001010.10111111.11111110

Онлайн-IP-калькулятор: http://Курсы-по-ИТ.рф/tools/ip-calculator.

Расчет количества подсетей и узлов

Шлюз – устройство для связи с хостами в других сетях. Чаще всего это либо первый, либо последний адрес, который может быть назначен хосту.

Расчет количества подсетей и узлов:

- Количество подсетей = $2^{(\text{количество битов в маске, которые отведены для подсети})}$
- Количество устройств = $2^{(\text{количество битов в адресе устройства})} - 2$
    - - 2 потому, что один адрес для адреса сети и один широковещательный
- Количество компьютеров = $2^{(\text{количество битов в адресе устройства})} - 3$
    - - 3 потому, что один адрес для адреса сети, один широковещательный и один адрес для шлюза

Пример

Для адреса 192.168.015.189/29 нужно определить максимально возможное количество подсетей и компьютеров.

192.168.015.189/29 = 11000000.10101000.00001111.10111101

Количество подсетей = $2^5 = 32$

Количество компьютеров = $2^3 - 3 = 8 - 3 = 5$

Пример задачи

Условие

Сеть хоста 192.168.0.15/24 надо разбить на 28 подсетей с максимально возможным количеством устройств в каждой подсети.

Задача

Необходимо определить маску сети, максимально возможное количество подсетей и максимальное количество узлов в каждой подсети с учетом приведенного условия.

Решение

1. **Количество битов, необходимое для создания заданного количества подсетей**. Определить ближайшее к заданному количеству подсетей число – степень двойки. В нашем случае это 32. 32 – это 2^5. Ответ – 5.
2. **Количество подсетей при заданной маске.** Возвести 2 в степень, равную количеству битов, отведенных под адрес подсети. В нашем случае это $2^5 = 32$. Ответ – 32.
3. **Количество битов, отведенное под адрес узла.** От 32 отнять количество битов в исходной маске и количество битов, необходимое для создания заданного количества подсетей. В нашем случае это 32 - 24 - 5 = 3. Ответ – 3.
4. **Количество узлов в каждой подсети.** Возвести 2 в степень, равную количеству битов, отведенных под адрес узла, и отнять 2. В нашем случае это $2^3 - 2 = 8 - 2 = 6$. Ответ – 6.

Итог

Для того чтобы для сети 192.168.0.15/24 получить 28 подсетей с максимальным количеством узлов в каждой подсети, надо разбить ее на 32 подсети. Для этого надо добавить к основной маске 5 бит. Итоговая маска будет /29 или 255.255.255.248. В каждой подсети можно разместить 6 устройств.

Виды IP-адресов

Публичный IP-адрес (белый, маршрутизируемый, глобальный) – это IP-адрес, который может использоваться для выхода в Интернет без подмены на другой IP-адрес. Если какой-либо сервис должен быть доступен из Интернета, то он должен иметь публичный IP-адрес либо иметь проброс портов от другого устройства с публичным IP-адресом.

Частный IP-адрес (внутренний, серый, приватный) – IP-адрес, принадлежащий к специальному диапазону, не используемому в сети Интернет. Такие адреса предназначены для применения в локальных сетях. Распределение таких адресов никем не контролируется.

Класс сети	Диапазон приватных адресов	Маска
A	10.0.0.0–10.255.255.255	255.0.0.0
B	172.16.0.0–172.31.255.255	255.240.0.0
C	192.168.0.0–192.168.255.255	255.255.0.0

Способы назначения:

- статический IP-адрес – это адрес, назначенный хосту администратором сети вручную;
- динамический IP-адрес – это адрес, назначенный хосту с помощью DHCP-сервера;
- постоянный IP-адрес – это адрес, который назначен хосту на постоянной основе. Он может быть назначен статически или динамически.

Зарезервированные IP-адреса:

- 169.254.0.0/16 – подсеть используется для автоматического назначения IP-адреса операционной системой самой себе, если настроено получение адреса по DHCP, но ни один сервер не отвечает;
- 127.0.0.1 – localhost («я сам»).

IP-адресация (IPv6)

IPv6 (англ. Internet Protocol version 6) – новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при ее использовании в Интернете, за счет использования длины адреса 128 бит вместо 32. Протокол был разработан IETF.

В настоящее время протокол IPv6 уже используется в нескольких тысячах сетей по всему миру (более 14 000 сетей на осень 2013 года), но пока еще не получил столь широкого распространения в Интернете, как IPv4. На конец 2012 года доля IPv6 в сетевом трафике составляла около 1 %. В России коммерческое использование операторами связи невелико (не более 1 % трафика). DNS-серверы многих российских регистраторов доменов и провайдеров хостинга используют IPv6.

После того как адресное пространство в IPv4 закончится, два стека протоколов – IPv6 и IPv4 – будут использоваться параллельно (англ. dual stack), с постепенным увеличением доли трафика IPv6 по сравнению с IPv4. Такая ситуация станет возможной из-за наличия огромного количества устройств, в том числе устаревших, не поддерживающих IPv6 и требующих специального преобразования для работы с устройствами, использующими только IPv6.

В конце 1980-х стала очевидна необходимость разработки способов сохранения адресного пространства Интернета. В начале 1990-х, несмотря на внедрение бесклассовой адресации, стало ясно, что этого недостаточно для предотвращения исчерпания адресов и необходимы дальнейшие изменения инфраструктуры Интернета. К началу 1992 года появилось несколько предложений, и к концу 1992 года IETF объявила конкурс для рабочих групп на создание интернет-протокола следующего поколения (англ. IP Next Generation, IPng). 25 июля 1994 года IETF утвердила модель IPng с образованием нескольких рабочих групп IPng. К 1996 году была выпущена серия спецификаций RFC, определяющих интернет-протокол версии 6, начиная с RFC 1883.

IETF назначила новому протоколу версию 6, так как версия 5 была ранее назначена экспериментальному протоколу, предназначенному для передачи видео и аудио.

8 июня 2011 года состоялся Международный день IPv6 – мероприятие по тестированию готовности мирового интернет-сообщества к переходу с IPv4 на IPv6, в рамках которого участвующие в акции компании добавили к своим сайтам IPv6-записи на один день.

Перевод на IPv6 начал осуществляться внутри Google с 2008 года. Тестирование IPv6 признано успешным. 6 июня 2012 года состоялся Всемирный запуск IPv6. Интернет-провайдеры включат IPv6 как минимум для 1 % своих пользователей (уже подписались AT&T, Comcast, Free Telecom, Internode, KDDI, Time Warner Cable, XS4ALL). Производители сетевого оборудования активируют IPv6 в качестве настроек по умолчанию в маршрутизаторах (Cisco, D-Link).

Увеличенное пространство адресов сделает NAT необязательным. Классическое применение IPv6 (по сети /64 на абонента; используется только unicast-адресация) обеспечит возможность использования более 300 млн IP-адресов на каждого жителя Земли.

Из IPv6 убраны функции, усложняющие работу маршрутизаторов:

- маршрутизаторы больше не должны фрагментировать пакет, вместо этого пакет отбрасывается с ICMP-уведомлением о превышении MTU. Передающая сторона в IPv6, таким образом, обречена на использование технологии Path MTU discovery. Для лучшей работы протоколов, требовательных к потерям, минимальный MTU поднят до 1280 байт. Фрагментация поддерживается как опция (информация о фрагментации пакетов вынесена из основного заголовка в расширенные) и возможна только по инициативе передающей стороны;
- из IP-заголовка исключена контрольная сумма. С учетом того, что канальные (Ethernet) и транспортные (TCP и UDP) протоколы имеют свои контрольные суммы, еще одна контрольная сумма на уровне IP воспринимается как излишняя. Кроме того, модификация поля hop limit (или TTL в IPv4) на каждом маршрутизаторе в IPv4 приводила к необходимости ее постоянного перерасчета.

Несмотря на больший по сравнению с предыдущей версией протокола размер адреса IPv6 (16 байт вместо 4), заголовок пакета удлинился всего лишь вдвое: с 20 до 40 байт.

Улучшения IPv6 по сравнению с IPv4:

- в сверхскоростных сетях возможна поддержка огромных пакетов (джамбограмм) – до 4 гигабайт;
- Time to Live переименовано в Hop Limit;
- появились метки потоков и классы трафика;
- появилось многоадресное вещание.

Формат записи

Восемь четырехзначных шестнадцатеричных чисел, разделенных двоеточием. Пример: 2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d. Если две и более группы подряд равны 0000, то они могут быть опущены и заменены на двойное двоеточие (::). Пример: 2001:0db8:0000:0000:0000:0000:ae21:ad12 может быть сокращен до 2001:db8::ae21:ad12. При использовании IPv6-адреса в URL необходимо заключать адрес в квадратные скобки. Пример: http://[2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d]:8080/.

DNS

DNS (англ. Domain Name System «система доменных имен») – компьютерная распределенная система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись). Порт/ID: 53/TCP, 53/UDP, спецификация: RFC 1034, RFC 1035 / STD 13.

Распределенная база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определенному протоколу.

Основой DNS является представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения – другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Начиная с 2010 года в систему DNS внедряются средства проверки целостности передаваемых данных, называемые DNS Security Extensions (DNSSEC). Передаваемые данные не шифруются, но их достоверность проверяется криптографическими способами. Внедряемый стандарт DANE обеспечивает передачу средствами DNS достоверной криптографической информации (сертификатов), используемой для установления безопасных и защищенных соединений транспортного и прикладного уровней.

Использование более простого и запоминающегося имени вместо числового адреса хоста относится к эпохе ARPANET. Стэнфордский исследовательский институт (теперь SRI International) поддерживал текстовый файл HOSTS.TXT, который сопоставлял имена узлов с числовыми адресами компьютеров в ARPANET.

Адреса назначались вручную. Чтобы запросить имя хоста и адрес и добавить компьютер в главный файл, пользователи связывались с сетевым информационным центром (NIC) SRI, руководимым Элизабет Фейнлер, по телефону в рабочее время.

К началу 1980-х годов поддержание единой централизованной таблицы хостов стало медленным и громоздким, а развивающейся сети требовалась автоматическая система именования для решения технических и кадровых вопросов. Постел поставил перед собой

задачу выработать компромисс между пятью конкурирующими предложениями для решения задачи, сформулированной Полом Мокапетрисом. Мокапетрис вместо этого создал концепцию иерархической системы доменных имен.

Рабочая группа IETF опубликовала оригинальные спецификации в RFC 882 и RFC 883 в ноябре 1983 года.

В 1984 году четыре ученика UC Berkeley, Дуглас Терри, Марк Пейнтер, Дэвид Риггл и Сонгниан Чжоу, написали первую версию сервера имен Unix для домена имени Интернета в Беркли, обычно называемого BIND. В 1985 году Кевин Данлэп из DEC существенно пересмотрел реализацию DNS. Майк Карел, Фил Альмквист и Пол Викси поддерживали BIND с тех пор. В начале 1990-х годов BIND был перенесен на платформу Windows NT. Он широко распространен, особенно в Unix-системах, и по-прежнему является наиболее широко используемым программным обеспечением DNS в Интернете.

Доменное имя может состоять только из ограниченного набора ASCII-символов, позволяя набрать адрес домена независимо от языка пользователя. ICANN утвердила основанную на Punycode систему IDNA, преобразующую любую строку в кодировке Unicode в допустимый DNS набор символов.

Документ RFC 2606 (Reserved Top Level DNS Names «Зарезервированные имена доменов верхнего уровня») определяет названия доменов, которые следует использовать в качестве примеров (например, в документации), а также для тестирования. Кроме example.com, example.org и example.net, в эту группу также входят test, invalid и др.

Ключевые характеристики DNS

- Распределенность администрирования. Ответственность за разные части иерархической структуры несут разные люди или организации.
- Распределенность хранения информации. Каждый узел сети в обязательном порядке должен хранить только те данные, которые входят в его зону ответственности, и (возможно) адреса корневых DNS-серверов.
- Кеширование информации. Узел может хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.
- Иерархическая структура, в которой все узлы объединены в дерево и каждый узел может или самостоятельно определять работу нижестоящих узлов, или делегировать (передавать) их другим узлам.
- Резервирование. За хранение и обслуживание своих узлов (зон) отвечают (обычно) несколько серверов, разделенных как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

DNS важна для работы Интернета, так как для соединения с узлом необходима информация о его IP-адресе, а для людей проще запоминать буквенные (обычно осмысленные) адреса, чем последовательность цифр IP-адреса. В некоторых случаях это позволяет использовать виртуальные серверы, например HTTP-серверы, различая их по имени запроса. Первоначально преобразование между доменными и IP-адресами производилось с использованием специального текстового файла hosts, который составлялся централизованно и автоматически рассылался на каждую из машин в своей локальной сети. С ростом Сети возникла необходимость в эффективном, автоматизированном механизме, которым и стала DNS.

DNS была разработана Полом Мокапетрисом в 1983 году; оригинальное описание механизмов работы содержится в RFC 882 и RFC 883. В 1987 году публикация RFC 1034 и RFC 1035 изменила спецификацию DNS и отменила RFC 882, RFC 883 и RFC 973 как устаревшие.

Проблемы с безопасностью

Первоначально проблемы безопасности не учитывались при разработке программного обеспечения DNS или любого программного обеспечения для развертывания в раннем Интернете, поскольку Сеть не была открыта для широкой общественности. Однако рост Интернета в коммерческом секторе в 1990-х годах изменил требования к мерам безопасности для защиты целостности данных и аутентификации пользователей.

Несколько уязвимостей были обнаружены и использованы злоумышленниками. Одной из таких проблем является отравление кеша DNS, в котором данные распространяются на кеширующие преобразователи под предлогом того, что они являются авторитетным сервером происхождения, тем самым загрязняя хранилище данных потенциально ложной информацией и длительными сроками действия (время жизни). Впоследствии запросы легитимных приложений могут быть перенаправлены на сетевые хосты, контролируемые злоумышленником.

DNS-ответы ранее не имели криптографической подписи, что давало возможность для множества вариантов атаки. Современные расширения системы безопасности доменных имен (DNSSEC) изменяют DNS, чтобы добавить поддержку криптографически подписанных ответов. Другие расширения, такие как TSIG, добавляют поддержку криптографической аутентификации между доверенными одноранговыми узлами и обычно используются для авторизации передачи зоны или операций динамического обновления.

Некоторые доменные имена могут использоваться для достижения эффектов спуфинга. Например, paypal.com и paypa1.com – это разные имена, но пользователи могут не различать их в графическом пользовательском интерфейсе в зависимости от выбранного шрифта пользователя. Во многих шрифтах буква l и цифра 1 выглядят очень похоже или даже идентично. Эта проблема остро стоит в системах, которые поддерживают интернационализированные доменные имена, поскольку многие коды символов в ISO 10646 могут отображаться на типичных экранах компьютеров. Эта уязвимость иногда используется в фишинге.

Для подтверждения результатов DNS также могут использоваться такие методы, как обратный DNS с подтверждением прямых записей, но криптографически достоверными они не являются; при этом не учитывается вариант подмены маршрутной информации (en:BGP-hijacking).

Терминология и принципы работы

Ключевыми понятия DNS:

- Доме́н (англ. domain «область») – узел в дереве имен вместе со всеми подчиненными ему узлами (если таковые имеются), то есть именованная ветвь или поддерево в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается слева направо, от младших доменов к доменам высшего уровня (в порядке повышения значимости): вверху находится корневой домен (не имеющий идентификатора), ниже идут домены первого уровня (доменные зоны), затем – домены второго уровня, третьего и т.д. (например, для адреса ru.wikipedia.org. домен первого уровня – org, второго – wikipedia, третьего – ru). На практике точку перед корневым доменом часто опускают («ru.wikipedia.org» вместо «ru.wikipedia.org.»), но

она бывает важна в случаях разделения между относительными доменами и FQDN (англ. Fully Qualifed Domain Name «полностью определенное имя домена»).

- Поддомен (англ. subdomain) – подчиненный домен (например, wikipedia.org – поддомен домена org, а ru.wikipedia.org – домена wikipedia.org). Теоретически такое деление может достигать глубины 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов. Но на практике регистраторы доменных имен используют более строгие ограничения. Например, если у вас есть домен вида mydomain.ru, вы можете создать для него различные поддомены вида mysite1.mydomain.ru, mysite2.mydomain.ru и т.д.
- Ресурсная запись – единица хранения и передачи информации в DNS. Каждая ресурсная запись имеет имя (то есть привязана к определенному доменному имени, узлу в дереве имен), тип и поле данных, формат и содержание которого зависят от типа.
- Зона – часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имен (DNS-сервере, см. ниже), а чаще – одновременно на нескольких серверах (см. ниже). Целью выделения части дерева в отдельную зону является передача ответственности (см. ниже) за соответствующий домен другому лицу или организации. Это называется делегированием (см. ниже). Как связная часть дерева, зона внутри тоже представляет собой дерево. Если рассматривать пространство имен DNS как структуру из зон, а не отдельных узлов/имен, тоже получается дерево; оправданно говорить о родительских и дочерних зонах, о старших и подчиненных. На практике большинство зон 0-го и 1-го уровня ('.', ru, com, …) состоят из единственного узла, которому непосредственно подчиняются дочерние зоны. В больших корпоративных доменах (2-го и следующих уровней) иногда встречается образование дополнительных подчиненных уровней без выделения их в дочерние зоны.
- Делегирование – операция передачи ответственности за часть дерева доменных имен другому лицу или организации. За счет делегирования в DNS обеспечивается распределенность администрирования и хранения. Технически делегирование выражается в выделении этой части дерева в отдельную зону и размещении этой зоны на DNS-сервере (см. ниже), управляемом этим лицом или организацией. При этом в родительскую зону включаются «склеивающие» ресурсные записи (NS и A), содержащие указатели на DNS-серверы дочерней зоны, а вся остальная информация, относящаяся к дочерней зоне, хранится уже на DNS-серверах дочерней зоны.
- DNS-сервер – специализированное ПО для обслуживания DNS, а также компьютер, на котором это ПО выполняется. DNS-сервер может быть ответственным за некоторые зоны и/или может перенаправлять запросы вышестоящим серверам.
- DNS-клиент – специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.
- Авторитетность (англ. authoritative) – признак размещения зоны на DNS-сервере. Ответы DNS-сервера могут быть двух типов: авторитетные (когда сервер заявляет, что сам отвечает за зону) и неавторитетные (англ. Non-authoritative), когда сервер обрабатывает запрос и возвращает ответ других серверов. В некоторых случаях вместо передачи запроса дальше DNS-сервер может вернуть уже известное ему (по запросам ранее) значение (режим кеширования).
- DNS-запрос (англ. DNS query) – запрос от клиента (или сервера) серверу. Запрос может быть рекурсивным или нерекурсивным

Система DNS содержит иерархию DNS-серверов, соответствующую иерархии зон. Каждая зона поддерживается как минимум одним авторитетным сервером DNS (от англ. authoritative «авторитетный»), на котором расположена информация о домене.

Имя и IP-адрес не тождественны – один IP-адрес может иметь множество имен, что позволяет поддерживать на одном компьютере множество веб-сайтов (это называется виртуальный хостинг). Обратное тоже справедливо – одному имени может быть сопоставлено множество IP-адресов: это позволяет создавать балансировку нагрузки.

Для повышения устойчивости системы используется множество серверов, содержащих идентичную информацию, а в протоколе есть средства, позволяющие поддерживать синхронность информации, расположенной на разных серверах. Существует 13 корневых серверов, их адреса практически не изменяются.

Протокол DNS использует для работы TCP- или UDP-порт 53 для ответов на запросы. Традиционно запросы и ответы отправляются в виде одной UDP-датаграммы. TCP используется, когда размер данных ответа превышает 512 байт, и для AXFR-запросов.

Рекурсия

Термином «рекурсия» в DNS обозначают алгоритм поведения DNS-сервера, при котором сервер выполняет от имени клиента полный поиск нужной информации во всей системе DNS, при необходимости обращаясь к другим DNS-серверам.

DNS-запрос может быть рекурсивным – требующим полного поиска – и нерекурсивным (или итеративным) – не требующим полного поиска.

Аналогично: DNS-сервер может быть рекурсивным (умеющим выполнять полный поиск) и нерекурсивным (не умеющим выполнять полный поиск). Некоторые программы DNS-серверов, например BIND, можно сконфигурировать так, чтобы запросы одних клиентов выполнялись рекурсивно, а запросы других – нерекурсивно.

При ответе на нерекурсивный запрос, а также при неумении или запрете выполнять рекурсивные запросы DNS-сервер либо возвращает данные о зоне, за которую он ответственен, либо возвращает ошибку. Настройки нерекурсивного сервера, когда при ответе выдаются адреса серверов, которые обладают большим объемом информации о запрошенной зоне, чем отвечающий сервер (чаще всего – адреса корневых серверов), являются некорректными, и такой сервер может быть использован для организации DoS-атак.

В случае рекурсивного запроса DNS-сервер опрашивает серверы (в порядке убывания уровня зон в имени), пока не найдет ответ или не обнаружит, что домен не существует (на практике поиск начинается с наиболее близких к искомому DNS-серверов, если информация о них есть в кеше и не устарела, сервер может не запрашивать другие DNS-серверы).

Рассмотрим на примере работу всей системы.

Предположим, мы набрали в браузере адрес ru.wikipedia.org. Браузер спрашивает у сервера DNS: «Какой IP-адрес у ru.wikipedia.org?» Однако сервер DNS может ничего не знать не только о запрошенном имени, но и даже обо всем домене wikipedia.org. В этом случае сервер обращается к корневому серверу – например, 198.41.0.4. Этот сервер сообщает: «У меня нет информации о данном адресе, но я знаю, что 204.74.112.1 является ответственным за зону org.». Тогда сервер DNS направляет свой запрос к 204.74.112.1, но тот отвечает: «У меня нет информации о данном сервере, но я знаю, что 207.142.131.234 является ответственным за зону

wikipedia.org.». Наконец, тот же запрос отправляется к третьему DNS-серверу и получает ответ – IP-адрес, который и передается клиенту – браузеру.

В данном случае при разрешении имени, то есть в процессе поиска IP по имени:

1) браузер отправил известному ему DNS-серверу рекурсивный запрос – в ответ на такой тип запроса сервер обязан вернуть «готовый результат», то есть IP-адрес либо пустой ответ и код ошибки NXDOMAIN;
2) DNS-сервер, получивший запрос от браузера, последовательно отправлял нерекурсивные запросы, на которые получал от других DNS-серверов ответы, пока не получил ответ от сервера, ответственного за запрошенную зону;
3) остальные упоминавшиеся DNS-серверы обрабатывали запросы нерекурсивно (и, скорее всего, не стали бы обрабатывать запросы рекурсивно, даже если бы такое требование стояло в запросе).

Иногда допускается, чтобы запрошенный сервер передавал рекурсивный запрос «вышестоящему» DNS-серверу и дожидался готового ответа.

При рекурсивной обработке запросов все ответы проходят через DNS-сервер, и он получает возможность кешировать их. Повторный запрос на те же имена обычно не идет дальше кеша сервера, обращения к другим серверам не происходит вообще. Информация о допустимом времени хранения ответов в кеше приходит вместе с ответами (поле TTL ресурсной записи).

Рекурсивные запросы требуют больше ресурсов от сервера (и создают больше трафика), так что обычно принимаются от «известных» владельцу сервера узлов (например, провайдер предоставляет возможность делать рекурсивные запросы только своим клиентам, в корпоративной сети рекурсивные запросы принимаются только из локального сегмента). Нерекурсивные запросы обычно принимаются от всех узлов сети (и содержательный ответ дается только на запросы о зоне, которая размещена на узле, на DNS-запрос о других зонах обычно возвращаются адреса других серверов).

Обратный DNS-запрос

DNS используется в первую очередь для преобразования символьных имен в IP-адреса, но он также может выполнять обратный процесс. Для этого используются уже имеющиеся средства DNS. Дело в том, что с записью DNS могут быть сопоставлены различные данные, в том числе и какое-либо символьное имя. Существует специальный домен in-addr.arpa, записи в котором используются для преобразования IP-адресов в символьные имена. Например, для получения DNS-имени для адреса 11.22.33.44 можно запросить у DNS-сервера запись 44.33.22.11.in-addr.arpa, и тот вернет соответствующее символьное имя. Обратный порядок записи частей IP-адреса объясняется тем, что в IP-адресах старшие биты расположены в начале, а в символьных DNS-именах старшие (находящиеся ближе к корню) части расположены в конце.

Записи DNS

Записи DNS, или ресурсные записи (англ. Resource Records, RR), – единицы хранения и передачи информации в DNS. Каждая ресурсная запись состоит из следующих полей:

- имя (NAME) – доменное имя, к которому привязана или которому «принадлежит» данная ресурсная запись;
- тип (TYPE) ресурсной записи – определяет формат и назначение данной ресурсной записи;

- класс (CLASS) ресурсной записи; теоретически считается, что DNS может использоваться не только с TCP/IP, но и с другими типами сетей, код в поле «Класс» определяет тип сети;
- TTL (Time To Live) – допустимое время хранения данной ресурсной записи в кеше неответственного DNS-сервера;
- длина поля данных (RDLEN);
- поле данных (RDATA), формат и содержание которого зависят от типа записи.

Наиболее важные типы DNS-записей:

1. Запись A (address record), или запись адреса, связывает имя хоста с адресом протокола IPv4. Например, запрос A-записи на имя referrals.icann.org вернет его IPv4-адрес – 192.0.34.164.
2. Запись AAAA (IPv6 address record) связывает имя хоста с адресом протокола IPv6. Например, запрос AAAA-записи на имя K.ROOT-SERVERS.NET вернет его IPv6-адрес – 2001:7fd::1.
3. Запись CNAME (canonical name record), или каноническая запись имени (псевдоним), используется для перенаправления на другое имя.
4. Запись MX (mail exchange), или почтовый обменник, указывает сервер(ы) обмена почтой для данного домена.
5. Запись NS (name server) указывает на DNS-сервер для данного домена.
6. Запись PTR (pointer), обратная DNS-запись или запись указателя, связывает IP-адрес хоста с его каноническим именем. Запрос в домене in-addr.arpa на IP-адрес хоста в reverse-форме вернет имя (FQDN) данного хоста. Например (на момент написания), для IP-адреса 192.0.34.164 запрос записи PTR 164.34.0.192.in-addr.arpa вернет его каноническое имя referrals.icann.org. В целях уменьшения объема нежелательной корреспонденции (спама) многие серверы-получатели электронной почты могут проверять наличие PTR-записи для хоста, с которого происходит отправка. В этом случае PTR-запись для IP-адреса должна соответствовать имени отправляющего почтового сервера, которым он представляется в процессе SMTP-сессии.
7. Запись SOA (Start of Authority), или начальная запись зоны, указывает, на каком сервере хранится эталонная информация о данном домене, содержит контактную информацию лица, ответственного за данную зону, тайминги (параметры времени) кеширования зонной информации и взаимодействия DNS-серверов.
8. SRV-запись (server selection) указывает на серверы для сервисов, используется, в частности, для Jabber и Active Directory.

Динамический DNS

Динамический DNS – технология, позволяющая информации на DNS-сервере обновляться в реальном времени и, по желанию, в автоматическом режиме. Она применяется для назначения постоянного доменного имени устройству (компьютеру, сетевому накопителю) с динамическим IP-адресом. Это может быть IP-адрес, полученный по DHCP или по IPCP в PPP-соединениях – например, при удаленном доступе через модем. Другие машины в Интернете могут устанавливать соединение с этой машиной по доменному имени и даже не знать, что IP-адрес изменился.

Время жизни (TTL) (см. RFC 1034) для динамической записи делается очень маленьким (не более двух-трех минут), иначе другие DNS-серверы поместят ее в свой кеш, а когда она изменится, их клиенты долго будут получать устаревшую информацию.

Динамическая DNS также часто применяется в локальных сетях, где клиенты получают IP-адрес по DHCP, а потом регистрируют свои имена в локальном DNS-сервере.

Протокол для обновления DNS описан в RFC 2136 и реализован, например, утилитой nsupdate. Для безопасной аутентификации клиента можно использовать технологию TSIG (RFC 2845), в которой используется заранее известный ключ. Минус этой технологии в том, что ключ должен быть установлен на каждом клиенте и на сервере.

Для обновления обычно используются специальные программы-клиенты, которые для обновления данных могут использовать и запросы HTTP GET.

Microsoft для своего Active Directory (которому динамическая DNS необходима, так как контроллеры домена регистрируют в DNS свои SRV-записи, чтобы другие машины могли их найти) использует другой способ, основанный на Kerberos-аутентификации и не требующий ручного распространения ключей. Это называется GSS-TSIG, но является лишь предложением стандарта и поддерживается только в ОС Windows NT версий от 5.0.

BIND (очень популярный DNS-сервер для UNIX-подобных ОС, таких как GNU/Linux, FreeBSD) поддерживает TSIG (RFC 2845), а по GSS-TSIG работать не может, однако версии от 8.2.2 поддерживают SRV-запись, что обеспечивает совместимость с Windows NT.

Хостинговые и прочие компании, хранящие у себя DNS-информацию клиентов и позволяющие клиентам эту информацию изменять, по сути тоже предоставляют динамическую DNS. Чаще всего клиент может изменить информацию, зайдя через веб-интерфейс.

«Динамический DNS» И DynDNS – это не одно и то же. DynDNS – это сервис динамического DNS американской компании Dyn.

Настройки IP-адресации

К минимальным настройкам IP-адресации относятся:

- IP-адрес хоста,
- маска сети,
- IP-адрес шлюза,
- адреса DNS-сервера(ов).

Шлюз нужен для того, чтобы хост знал, куда направлять пакеты, которые предназначены для других сетей.

Маршрутизация

Маршрутизация (англ. Routing) – процесс определения маршрута следования данных в сетях связи.

Маршруты могут задаваться административно (статические маршруты) либо вычисляться с помощью алгоритмов маршрутизации, базируясь на информации о топологии и состоянии сети, полученной с помощью протоколов маршрутизации (динамические маршруты).

Статическими маршрутами могут быть:

- маршруты, не изменяющиеся во времени;
- маршруты, изменяющиеся по расписанию.

Маршрутизация в компьютерных сетях выполняется специальными программно-аппаратными средствами – маршрутизаторами; в простых конфигурациях может выполняться и компьютерами общего назначения, соответственно настроенными.

Протокол маршрутизации – сетевой протокол, используемый маршрутизаторами для определения возможных маршрутов следования данных в составной компьютерной сети.

Маршрутизируемый протокол – это любой сетевой протокол, адрес сетевого уровня которого предоставляет достаточно информации для доставки пакета от одного сетевого узла другому.

Протокол маршрутизации ≠ маршрутизируемый протокол.

Протокол маршрутизации может работать только с пакетами, принадлежащими к одному из маршрутизируемых протоколов, – например, IP, IPX или Xerox Network System, AppleTalk. Маршрутизируемые протоколы определяют формат пакетов (заголовков), важнейшей информацией из которых для маршрутизации является адрес назначения. Протоколы, не поддерживающие маршрутизацию, могут передаваться между сетями с помощью туннелей. Подобные возможности обычно предоставляют программные маршрутизаторы и некоторые модели аппаратных маршрутизаторов.

Первые маршрутизаторы представляли собой специализированное ПО, обрабатывающее приходящие IP-пакеты специфичным образом. Это ПО работало на компьютерах, у которых было несколько сетевых интерфейсов, входящих в состав различных сетей (между которыми осуществляется маршрутизация). В дальнейшем появились маршрутизаторы в форме специализированных устройств. Компьютеры с маршрутизирующим ПО называют программными маршрутизаторами, оборудование – аппаратными маршрутизаторами.

В современных аппаратных маршрутизаторах для построения таблиц маршрутизации используется специализированное ПО («прошивка»), для обработки же IP-пакетов используется коммутационная матрица (или другая технология аппаратной коммутации), расширенная фильтрами адресов в заголовке IP-пакета.

Маршрутизация в сети Интернет основана на протоколах TCP/IP.

Передача информации осуществляется с помощью IP-пакетов, заголовок каждого IP-пакета содержит IP-адреса получателя и отправителя пакета. Каждый пакет обрабатывается маршрутизатором в соответствии с его таблицей маршрутизации. Таблица, в свою очередь, содержит информацию, компьютеру с каким адресом направлять пакеты с тем или иным диапазоном адресов. Например, все пакеты определенного диапазона могут направляться другому маршрутизатору, который «отвечает» за этот сегмент.

В ряде случаев маршрутизатор может преобразовывать заголовок пакета, заменяя адреса отправителя и/или получателя пакета. В частности, это происходит при взаимодействии локальной сети (имеющей свои адреса) с глобальной сетью Интернет. В этом случае локальная сеть может быть видна извне по одному глобальному IP-адресу. Для того чтобы маршрутизатор мог направлять пакеты с одним глобальным адресом тем или иным получателям в локальной сети, используется таблица NAT, где помимо IP-адресов указываются порты, идентифицирующие приложения, устанавливающие соединение. При этом номера портов указаны не в заголовке IP-пакета, а в заголовке сегмента TCP либо UDP (сегменты инкапсулируются в поле данных IP-пакетов). Это позволяет осуществлять взаимно-однозначную идентификацию получателя и отправителя в тех случаях, когда за одним глобальным адресом находится множество компьютеров локальных сетей.

Протоколы маршрутизации

Протокол маршрутизации – сетевой протокол, используемый маршрутизаторами для определения возможных маршрутов следования данных в составной компьютерной сети. Применение протокола маршрутизации позволяет избежать ручного ввода всех допустимых маршрутов, что, в свою очередь, снижает количество ошибок, обеспечивает согласованность действий всех маршрутизаторов в сети и облегчает труд администраторов.

Дистанционно-векторная маршрутизация

В дистанционно-векторных алгоритмах (DVA) каждый маршрутизатор периодически и широковещательно рассылает по сети вектор, компонентами которого являются расстояния (измеренные в той или иной метрике) от данного маршрутизатора до всех известных ему сетей. Пакеты протоколов маршрутизации обычно называют объявлениями о расстояниях, так как с их помощью маршрутизатор объявляет остальным маршрутизаторам известные ему сведения о конфигурации сети.

Получив от некоторого соседа вектор расстояний (дистанций) до известных тому сетей, маршрутизатор наращивает компоненты вектора на величину расстояния от себя до данного соседа. Кроме того, он дополняет вектор информацией об известных ему самому других сетях, о которых он узнал непосредственно (если они подключены к его портам) или из аналогичных объявлений других маршрутизаторов. Обновленное значение вектора маршрутизатор рассылает своим соседям. В конце концов каждый маршрутизатор узнает через соседние маршрутизаторы информацию обо всех имеющихся в составной сети сетях и о расстояниях до них.

Затем он выбирает из нескольких альтернативных маршрутов к каждой сети тот маршрут, который обладает наименьшим значением метрики. Маршрутизатор, передавший информацию о данном маршруте, отмечается в таблице маршрутизации как следующий (next hop).

Дистанционно-векторные алгоритмы хорошо работают только в небольших сетях. В больших сетях они периодически засоряют линии связи интенсивным трафиком, к тому же изменения конфигурации не всегда корректно могут отрабатываться алгоритмом этого типа, так как маршрутизаторы не имеют точного представления о топологии связей в сети, а располагают только косвенной информацией – вектором расстояний.

Наиболее распространенным протоколом, основанным на дистанционно-векторном алгоритме, является протокол RIP.

Протоколы состояния каналов связи

Протоколы состояния каналов связи разработаны для преодоления ограничений, связанных с использованием дистанционно-векторных протоколов. Имеют возможность быстро реагировать на изменения сети. Рассылают обновления только в случае появления изменений и периодические обновления через большие промежутки времени.

Классификация

В зависимости от алгоритма маршрутизации протоколы делятся на два вида:

- дистанционно-векторные протоколы (основаны на алгоритме DVA – англ. distance vector algorithm);
- протоколы состояния каналов связи (основаны на алгоритме LSA – англ. link state algorithm).

По области применения выделяют протоколы:

- для междоменной маршрутизации;
- для внутридоменной маршрутизации.

Дистанционно-векторные протоколы:

- RIP – англ. routing information protocol;
- IGRP – англ. interior gateway routing protocol (лицензированный протокол фирмы Cisco Systems);
- BGP – англ. border gateway protocol;
- EIGRP – англ. enhanced interior gateway routing protocol (на самом деле этот протокол гибридный – объединяет свойства дистанционно-векторных протоколов и протоколов по состоянию канала); лицензированный протокол фирмы Cisco Systems;
- AODV – англ. ad hoc on-demand distance vector.

Протоколы состояния каналов связи:

- IS-IS – англ. intermediate system to intermediate system (стек OSI);
- OSPF – англ. open shortest path first;
- NLSP – англ. NetWare link-services protocol (стек Novell);
- HSRP – англ. hot standby router/redundancy protocol (протокол резервирования шлюза в сетях Ethernet);
- CARP – англ. common address redundancy protocol (протокол резервирования шлюза в сетях Ethernet);
- OLSR – англ. optimized link-state routing;
- TBRPF – англ. topology dissemination based on reverse-path forwarding.

Протоколы междоменной маршрутизации:

- EGP – англ. exterior gateway protocol;
- BGP – англ. border gateway protocol;
- IDRP – англ. inter-domain routing protocol;
- IS-IS level 3 – англ. intermediate system to intermediate system level 3.

Протоколы внутридоменной маршрутизации:

- RIP – англ. routing information protocol;
- IS-IS level 1–2 – англ. intermediate system to intermediate system level 1–2;
- OSPF – англ. open shortest path first;
- IGRP – англ. interior gateway routing protocol;
- EIGRP – англ. enhanced interior gateway routing protocol.

Популярные протоколы

RIP

Протокол маршрутной информации (англ. Routing Information Protocol) – один из самых простых протоколов маршрутизации. Применяется в небольших компьютерных сетях, позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопах), получая ее от соседних маршрутизаторов.

Алгоритм маршрутизации RIP (алгоритм Беллмана – Форда) был впервые разработан в 1969 году как основной для сети ARPANET.

Прототип протокола RIP – Gateway Information Protocol, часть пакета PARC Universal Packet. Протокол был унифицирован в документе RFC 1058.

В 1994 году был разработан протокол RIP-2 (RFC 2453), который является расширением протокола RIP, обеспечивающим передачу дополнительной маршрутной информации в сообщениях RIP и повышающим уровень безопасности.

Для работы в среде IPv6 была разработана версия RIPng.

RIP – так называемый протокол дистанционно-векторной маршрутизации, который оперирует транзитными участками в качестве метрики маршрутизации. Максимальное количество хопов, разрешенное в RIP, – 15 (метрика 16 означает «бесконечно большую метрику»). Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд, довольно сильно нагружая низкоскоростные линии связи. RIP работает на 3 (сетевом) уровне стека TCP/IP, используя UDP-порт 520.

В современных сетевых средах RIP – не самое лучшее решение для выбора в качестве протокола маршрутизации, так как его возможности уступают более современным протоколам, таким как EIGRP, OSPF. Ограничение на 15 хопов не дает применять его в больших сетях. Преимущество этого протокола – простота конфигурирования.

OSPF

OSPF (англ. Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Протокол OSPF был разработан IETF в 1988 году. Последняя версия протокола представлена в RFC 2328 (1998 год). Протокол OSPF представляет собой протокол внутреннего шлюза (Interior Gateway Protocol, IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

OSPF имеет следующие преимущества:

- высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации;
- поддержка сетевых масок переменной длины (VLSM);
- оптимальное использование пропускной способности с построением дерева кратчайших путей.

OSPF делит сеть на зоны. Маршрутизаторы, принадлежащие одной зоне, не знают информацию о детальной топологии других зон. Каждой зоне присваивается идентификатор зоны (area ID).

Распределение в OSPF на зоны помогает:

- снизить нагрузку на ЦП маршрутизаторов за счет уменьшения количества перерасчетов по алгоритму OSPF;
- уменьшить размер таблиц маршрутизации;
- уменьшить количество пакетов обновлений состояния канала.

BGP

BGP (англ. Border Gateway Protocol «протокол граничного шлюза») – динамический протокол маршрутизации.

Относится к классу протоколов маршрутизации внешнего шлюза (англ. EGP – External Gateway Protocol).

На текущий момент является основным протоколом динамической маршрутизации в сети Интернет.

Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (АС, англ. AS – autonomous system), то есть группами маршрутизаторов под единым техническим и административным управлением, использующими протокол внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация включает в себя список АС, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляется исходя из правил, принятых в сети.

BGP поддерживает бесклассовую адресацию и использует суммирование маршрутов для уменьшения таблиц маршрутизации. С 1994 года действует четвертая версия протокола, все предыдущие версии являются устаревшими.

BGP, наряду с DNS, является одним из главных механизмов, обеспечивающих функционирование Интернета.

BGP является протоколом прикладного уровня и функционирует поверх протокола транспортного уровня TCP (порт 179). После установки соединения передается информация обо всех маршрутах, предназначенных для экспорта. В дальнейшем передается только информация об изменениях в таблицах маршрутизации. При закрытии соединения удаляются все маршруты, информация о которых передана противоположной стороной.

Трассировка

Traceroute – это служебная компьютерная программа, предназначенная для определения маршрутов следования данных в сетях TCP/IP. Traceroute может использовать разные протоколы передачи данных в зависимости от операционной системы устройства. Такими протоколами могут быть UDP, TCP, ICMP или GRE. Компьютеры с установленной операционной системой Windows используют ICMP-протокол, при этом операционные системы Linux и маршрутизаторы Cisco – протокол UDP.

Traceroute входит в поставку большинства современных сетевых операционных систем. В системах Microsoft Windows эта программа носит название «tracert», а в системах GNU/Linux, Cisco IOS и Mac OS – traceroute.

Рассмотрим пример работы программы в операционной системе Windows. Программа tracert выполняет отправку данных указанному узлу сети, при этом отображая сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к целевому узлу. В случае проблем при доставке данных до какого-либо узла программа позволяет определить, на каком именно участке сети возникли неполадки. Необходимо отметить, что программа работает только в направлении от источника пакетов и является весьма грубым инструментом для выявления неполадок в сети. В силу особенностей работы протоколов маршрутизации в сети Интернет, обратные маршруты часто не совпадают с прямыми, причем это справедливо для всех промежуточных узлов в трейсе. Поэтому ICMP-ответ от каждого промежуточного узла может идти своим собственным маршрутом, затеряться или прийти с большой задержкой, хотя в реальности с пакетами, которые адресованы конечному узлу, этого не происходит. Кроме

того, на промежуточных маршрутизаторах часто стоит ограничение числа ответов ICMP в единицу времени, что приводит к появлению ложных потерь.

Для определения промежуточных маршрутизаторов traceroute отправляет целевому узлу серию ICMP-пакетов (по умолчанию 3 пакета), с каждым шагом увеличивая значение поля TTL («Время жизни») на 1. Это поле обычно указывает максимальное количество маршрутизаторов, которое может быть пройдено пакетом. Первая серия пакетов отправляется с TTL, равным 1, и поэтому первый же маршрутизатор возвращает обратно ICMP-сообщение «time exceeded in transit», указывающее на невозможность доставки данных. Traceroute фиксирует адрес маршрутизатора, а также время между отправкой пакета и получением ответа (эти сведения выводятся на монитор компьютера). Затем traceroute повторяет отправку серии пакетов, но уже с TTL, равным 2, что заставляет первый маршрутизатор уменьшить TTL пакетов на единицу и направить их ко второму маршрутизатору. Второй маршрутизатор, получив пакеты с TTL=1, также возвращает «time exceeded in transit».

Процесс повторяется до тех пор, пока пакет не достигнет целевого узла. При получении ответа от этого узла процесс трассировки считается завершенным.

На оконечном хосте IP-дейтаграмма с TTL=1 не отбрасывается и не вызывает ICMP-сообщения типа «Срок истек», а должна быть отдана приложению. Достижение пункта назначения определяется следующим образом: отсылаемые traceroute дейтаграммы содержат UDP-пакет с заведомо неиспользуемым номером порта на адресуемом хосте. Номер порта будет равен 33 434 + (максимальное количество транзитных участков до узла) - 1. В пункте назначения UDP-модуль, получая подобные дейтаграммы, возвращает ICMP-сообщения об ошибке «Порт недоступен». Таким образом, чтобы узнать о завершении работы, программе traceroute достаточно обнаружить, что поступило ICMP-сообщение об ошибке этого типа.

Таблица маршрутизации

Таблица маршрутизации – база данных, хранящаяся на маршрутизаторе или сетевом компьютере, которая описывает соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора. Является простейшей формой правил маршрутизации.

Таблица маршрутизации обычно содержит:

- **адрес** сети или узла назначения либо указание, что маршрут является маршрутом по умолчанию;
- **маску сети назначения** (для IPv4-сетей маска /32 (255.255.255.255) позволяет указать единичный узел сети);
- **шлюз**, обозначающий адрес маршрутизатора в сети, на который необходимо отправить пакет, следующий до указанного адреса назначения;
- **интерфейс**, через который доступен шлюз (в зависимости от системы, это может быть порядковый номер, GUID или символьное имя устройства; интерфейс может быть отличен от шлюза, если шлюз доступен через дополнительное сетевое устройство, например сетевую карту);
- **метрику** – числовой показатель, задающий предпочтительность маршрута. Чем меньше число, тем более предпочтителен маршрут (интуитивно представляется как расстояние).

В таблице может быть один, а в некоторых операционных системах и несколько шлюзов по умолчанию. Такой шлюз используется в сетях, для которых нет более конкретных маршрутов в таблице маршрутизации.

Маршрут по умолчанию и шлюз по умолчанию

Маршрут по умолчанию (англ. Default Route) указывает, куда направлять пакет, если к сети нет явно прописанного маршрута. Обозначение: «сеть 0.0.0.0 с маской сети 0.0.0.0». Доступен через шлюз по умолчанию (англ. Default Gateway).

Шлюз по умолчанию (англ. Default gateway), шлюз последней надежды (англ. Last hope gateway) – в маршрутизируемых протоколах сетевой шлюз, на который пакет отправляется в том случае, если маршрут к сети назначения пакета неизвестен (не задан явным образом в таблице маршрутизации хоста). Применяется в сетях с хорошо выраженными центральными маршрутизаторами, в малых сетях, в клиентских сегментах сетей. Шлюз по умолчанию задается записью в таблице маршрутизации вида «сеть 0.0.0.0 с маской сети 0.0.0.0».

Пример таблицы маршрутизации Windows

```
IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0      172.18.0.1     172.18.0.110     20
          0.0.0.0          0.0.0.0      172.18.0.1     172.18.0.117    281
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
       172.18.0.0      255.255.0.0         On-link      172.18.0.110    276
       172.18.0.0      255.255.0.0         On-link      172.18.0.117    281
     172.18.0.110  255.255.255.255         On-link      172.18.0.110    276
     172.18.0.117  255.255.255.255         On-link      172.18.0.117    281
   172.18.255.255  255.255.255.255         On-link      172.18.0.110    276
   172.18.255.255  255.255.255.255         On-link      172.18.0.117    281
     192.168.42.0    255.255.255.0         On-link      192.168.42.1    276
     192.168.42.1  255.255.255.255         On-link      192.168.42.1    276
   192.168.42.255  255.255.255.255         On-link      192.168.42.1    276
    192.168.109.0    255.255.255.0         On-link     192.168.109.1    276
    192.168.109.1  255.255.255.255         On-link     192.168.109.1    276
  192.168.109.255  255.255.255.255         On-link     192.168.109.1    276
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link      172.18.0.110    276
        224.0.0.0        240.0.0.0         On-link      192.168.42.1    276
        224.0.0.0        240.0.0.0         On-link     192.168.109.1    276
        224.0.0.0        240.0.0.0         On-link      172.18.0.117    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link      172.18.0.110    276
  255.255.255.255  255.255.255.255         On-link      192.168.42.1    276
  255.255.255.255  255.255.255.255         On-link     192.168.109.1    276
  255.255.255.255  255.255.255.255         On-link      172.18.0.117    281
===========================================================================
Постоянные маршруты:
  Отсутствует
```

DHCP

DHCP (англ. Dynamic Host Configuration Protocol «протокол динамической настройки хоста») – сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP-адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP.

Стандарт протокола DHCP был принят в октябре 1993 года. Действующая версия протокола (март 1997 года) описана в RFC 2131. Новая версия DHCP, предназначенная для использования в среде IPv6, носит название «DHCPv6» и определена в RFC 3315 (июль 2003 года).

Протокол DHCP предоставляет три способа распределения IP-адресов:

1. Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet-сетей это MAC-адрес) каждого клиентского компьютера определенный IP-адрес. Фактически данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.
2. Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определенного администратором диапазона.
3. Динамическое распределение. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдается компьютеру не в постоянное пользование, а на определенный срок. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса.

Некоторые реализации службы DHCP способны автоматически обновлять записи DNS, соответствующие клиентским компьютерам, при выделении им новых адресов. Это осуществляется при помощи протокола обновления DNS, описанного в RFC 2136.

Протокол DHCP является клиент-серверным, то есть в его работе участвуют клиент DHCP и сервер DHCP. Передача данных производится при помощи протокола UDP. По умолчанию запросы от клиента делаются на 67 порт к серверу, сервер в свою очередь отвечает на порт 68 к клиенту, выдавая адрес IP и другую необходимую информацию, такую как сетевая маска, шлюз по умолчанию и серверы DNS.

Опции DHCP

Помимо IP-адреса, DHCP также может сообщать клиенту дополнительные параметры, необходимые для нормальной работы в сети. Эти параметры называются опциями DHCP. Список стандартных опций можно найти в RFC 2132.

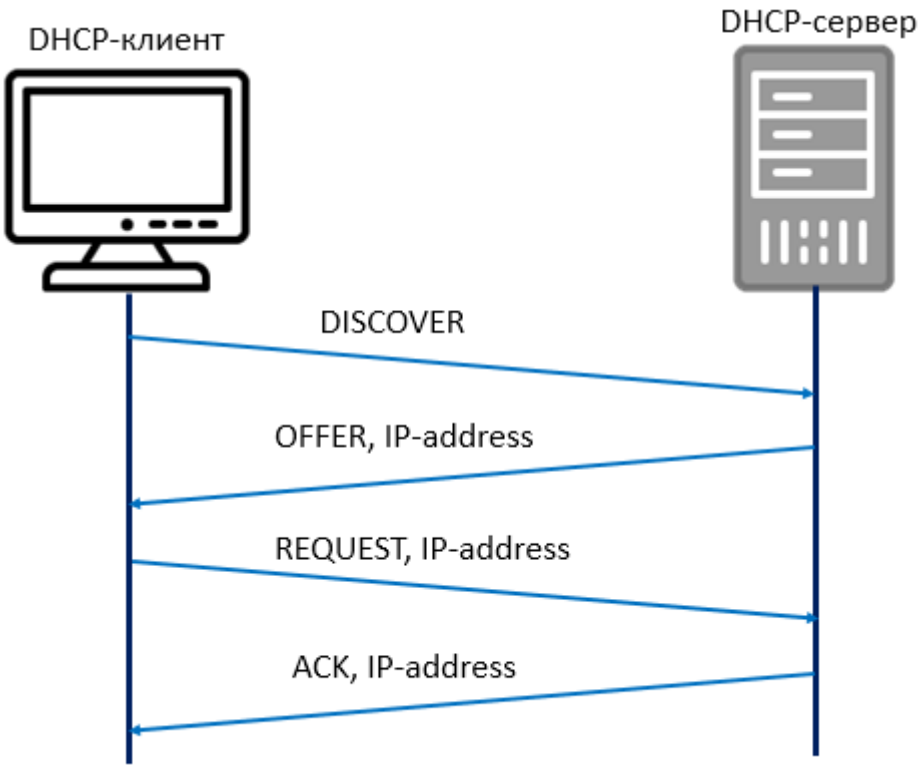
Опции – строки переменной длины, состоящие из октетов. Первый октет – код опции, второй октет – количество следующих октетов, остальные октеты зависят от кода опции.

Некоторыми из наиболее часто используемых опций являются:

- IP-адрес маршрутизатора по умолчанию;
- маска подсети;
- адреса серверов DNS;
- имя домена DNS.

Некоторые поставщики программного обеспечения могут определять собственные дополнительные опции DHCP (RFC 2132).

Процесс получения IP-адреса



Этапы:

- DISCOVER – поиск DHCP-сервера;
- OFFER – предложение DHCP-сервера;
- REQUEST – выбор DHCP-сервера;
- ACK – подтверждение выбора DHCP-сервера;
- NACK – отказ в подтверждении выбора DHCP-сервера.

Окончание аренды

Окончание аренды возможно по времени или через сообщение «RELEASE». После окончания аренды IP-адрес освобождается и может быть назначен другому хосту.

DHCP relay

Функция DHCP Relay Option 82 (стандарт RFC 3046) применяется для предоставления DHCP-серверу данных о полученном запросе. В частности, к этим данным можно отнести:

- адрес DHCP-ретранслятора, с которого шел запрос;
- номер порта ретранслятора, через который поступил запрос.

При настройке, например, коммутатора в режиме DHCP Relay можно значительно повысить эффективность сети за счет сокращения количества DHCP-серверов, которые при другой схеме понадобились бы для каждой подсети. В данном случае коммутатор сам переадресует DHCP-запрос от клиента к удаленному DHCP-серверу и добавит указанные выше данные.

В общем случае назначение опции DHCP Relay Option 82 – это привязка IP-адреса, выдаваемого DHCP-сервером, к порту коммутатора, к которому подключен клиент, либо к ретранслятору, с которого поступил запрос, что может помочь с систематизацией IP-адресов в локальной сети при использовании DHCP-сервера.

APIPA

APIPA (англ. Automatic Private IP Addressing) – автоматическая приватная IP-адресация. Если хост не может получить IP-адрес от DHCP-сервера, то он производит автоматическую самонастройку с адресом из сети 169.254.0.0/16.

Коммутация-2

Компьютеры смогут общаться, только если они находятся в одной IP-сети.

VLAN

VLAN (аббр. от англ. Virtual Local Area Network) – логическая (виртуальная) локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

Мультиплексирование – уплотнение канала, т.е. передача нескольких потоков (каналов) данных с меньшей скоростью (пропускной способностью) по одному каналу.

Транк (англ. Trunk) – линия связи «точка-точка», по которой осуществляется отправка и получение трафика между коммутаторами или коммутаторами и маршрутизаторами. По каналам типа «транк» передается трафик из нескольких VLAN.

Преимуществом транков является экономия портов коммутатора, а недостатком – то, что транк становится узким местом. Для устранения этой проблемы рекомендуется использовать uplink. Uplink – это более производительный интерфейс, чем остальные. Также термин «uplink» применяется к интерфейсу, через который подключается интернет-провайдер.

Предоставляемые возможности:

1. Логическое деление коммутатора на несколько не сообщающихся между собой сетей.
2. Устройство такового деления на сети с 2 или более коммутаторами без требования проведения дополнительных кабелей. Кабель, по которому передается трафик нескольких VLAN, называется trunk, а порты коммутаторов, к которым он подключен, – trunk port. Для идентификации кадров, относящихся к разным VLAN, используется стандарт 802.1Q (дополнительный тег в Ethernet-кадре). Зачастую понятие «802.1Q» используется как синоним понятия «VLAN». IEEE 802.1Q – открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN. 802.1Q не изменяет заголовки кадра. Сетевые устройства без поддержки 802.1Q могут передавать трафик без учета его принадлежности к VLAN.
3. Асимметричные VLAN. В этом случае порт (не trunk, по кабелю движутся кадры без тега 802.1Q) подключен к одной внутренней VLAN коммутатора по входящим кадрам (она называется PVID) и к более чем одной внутренней VLAN коммутатора по исходящим

кадрам. При этом может отсутствовать подключение по исходящим кадрам к PVID VLAN.

4. Через предыдущий пункт реализуется и более высокоуровневая абстракция – Promiscous/Community/Isolated-порты. В этом случае используется логическое вложение нескольких вторичных VLAN в одну первичную.
5. Promiscous-порт (порт на первичной VLAN) может общаться с любым Promiscous/Community/Isolated-портом как на первичной, так и на любой вложенной в нее вторичной VLAN.
6. Community-порт (порт на вторичной VLAN) может общаться с любым Promiscous-портом, а также с любым Community-портом в пределах своей вторичной VLAN.
7. Isolated-порт (тоже порт на вторичной VLAN, но это специальная isolated VLAN, которая может быть только одна в данной первичной VLAN) может общаться только с Promiscous-портами и не может общаться даже с другими Isolated-портами (принцип «все клиенты видят сервер и не видят друг друга», часто используется в гостевых Wi-Fi-сетях).
8. Двухуровневое вложение VLAN-меток в кадр, а также трансляция значений меток «на лету». Данная технология называется QinQ и поддерживается не во всех устройствах с поддержкой VLAN.

Обозначение членства во VLAN:

1. По порту (англ. port-based, 802.1Q): порту коммутатора вручную назначается одна VLAN. В случае если одному порту должны соответствовать несколько VLAN (например, если соединение VLAN проходит через несколько сетевых коммутаторов), то этот порт должен быть членом транка. Только одна VLAN может получать все кадры, не отнесенные ни к одной VLAN (в терминологии 3Com, Planet, D-Link, Zyxel, HP – untagged, в терминологии Cisco, Juniper – native VLAN). Сетевой коммутатор будет добавлять метки данной VLAN ко всем принятым кадрам, не имеющим никаких меток. VLAN, построенные на базе портов, имеют некоторые ограничения.
2. По MAC-адресу (MAC-based): членство во VLAN`е основывается на MAC-адресе рабочей станции. В таком случае сетевой коммутатор имеет таблицу MAC-адресов всех устройств вместе с VLAN`ами, к которым они принадлежат.
3. По протоколу (Protocol-based): данные 3–4 уровня в заголовке инкапсулированного в кадр пакета используются, чтобы определить членство во VLAN`е. Например, IP-машины могут быть переведены в первую VLAN, а AppleTalk-машины во вторую. Основной недостаток этого метода в том, что он нарушает независимость уровней, поэтому, например, переход с IPv4 на IPv6 приведет к нарушению работоспособности сети.
4. Методом аутентификации (англ. authentication based): устройства могут быть автоматически перемещены во VLAN, основываясь на данных аутентификации пользователя или устройства при использовании протокола 802.1x.

   Преимущества:
   1. Облегчается перемещение, добавление устройств и изменение их соединений друг с другом.
   2. Достигается большая степень административного контроля вследствие наличия устройства, осуществляющего между сетями VLAN маршрутизацию на 3-м уровне.

3. Уменьшается потребление полосы пропускания по сравнению с ситуацией одного широковещательного домена.
4. Сокращается непроизводственное использование CPU за счет сокращения пересылки широковещательных сообщений.
5. Предотвращение широковещательных штормов и предотвращение потерь.

Маршрутизация между VLAN

Так как сети в разных VLAN, как правило, находятся в разных логических подсетях, то для их объединения требуется маршрутизация. Возможные варианты:

- с помощью маршрутизатора:
  - 1 VLAN подключается к 1 порту маршрутизатора,
  - Router on the Stick – подключение с помощью trunk-порта;
- использование L3-коммутатора.

Протоколы UDP и DCCP

UDP и DCCP относятся к протоколам с негарантированной доставкой. Это значит, что:

- возможна недоставка сообщения,
- возможна доставка в другом порядке,
- возможно дублирование сообщений.

Протоколы с негарантированной доставкой применяются для трафика, чувствительного ко времени, и для трафика, где от большого числа клиентов идут небольшие запросы. Примеры: DNS и потоковые мультимедийные приложения вроде IPTV, Voice over IP, протоколы туннелирования IP и многие онлайн-игры.

Чувствительные ко времени приложения часто используют протоколы с негарантированной доставкой, так как предпочтительнее сбросить пакеты, чем ждать задержавшиеся пакеты, что может оказаться невозможным в системах реального времени. Использование этих протоколов подразумевает, что проверка ошибок и исправление либо не нужны, либо должны исполняться в приложении. При необходимости исправления ошибок на сетевом уровне интерфейса приложение может задействовать TCP или SCTP, разработанные для этой цели.

UDP

UDP (англ. User Datagram Protocol «протокол пользовательских датаграмм») – один из ключевых элементов стека протоколов TCP/IP. С UDP компьютерные приложения могут посылать сообщения (в данном случае называемые дейатаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных. Протокол был разработан Дэвидом П. Ридом в 1980 году и официально определен в RFC 768.

Структура пакета

UDP – минимальный ориентированный на обработку сообщений протокол транспортного уровня, задокументированный в RFC 768.

UDP не предоставляет никаких гарантий доставки сообщения для вышестоящего протокола и не сохраняет состояния отправленных сообщений. По этой причине UDP иногда называют Unreliable Datagram Protocol («ненадежный протокол датаграмм»).

UDP обеспечивает многоканальную передачу (с помощью номеров портов) и проверку целостности (с помощью контрольных сумм) заголовка и существенных данных. Надежная передача в случае необходимости должна реализовываться пользовательским приложением.

Порт отправителя

В этом поле указывается номер порта отправителя. Предполагается, что это значение задает порт, на который при необходимости будет посылаться ответ. В противном же случае значение должно быть равным 0. Если хостом-источником является клиент, то номер порта будет, скорее всего, динамическим. Если источником является сервер, то его порт будет одним из «хорошо известных».

Порт получателя

Это поле обязательно и содержит порт получателя. Аналогично порту отправителя: если хостом-получателем является клиент, то номер порта динамический, если получатель – сервер, то это будет «хорошо известный» порт.

Длина дейтаграммы

Поле, задающее длину всей дейтаграммы (заголовка и данных) в байтах. Минимальная длина равна длине заголовка – 8 байт. Теоретически максимальный размер поля – 65 535 байт для UDP-дейтаграммы (8 байт на заголовок и 65 527 на данные). Фактический предел для длины данных при использовании IPv4 – 65 507 (помимо 8 байт на UDP-заголовок требуется еще 20 на IP-заголовок).

На практике также следует учитывать, что если длина IPv4-пакета с UDP будет превышать MTU (для Ethernet по умолчанию 1500 байт), то отправка такого пакета может вызвать его фрагментацию, что может привести к тому, что он вообще не сможет быть доставлен, если промежуточные маршрутизаторы или конечный хост не будут поддерживать фрагментированные IP-пакеты. Также в RFC 791 указывается минимальная длина IP-пакета 576 байт, которую должны поддерживать все участники, и рекомендуется отправлять IP-пакеты большего размера только в том случае, если вы уверены, что принимающая сторона может принять пакеты такого размера. Следовательно, чтобы избежать фрагментации UDP-пакетов (и возможной их потери), размер данных в UDP не должен превышать: MTU - (Max IP Header Size) - (UDP Header Size) = 1500 - 60 - 8 = 1432 байта. Для того чтобы быть уверенным, что пакет будет принят любым хостом, размер данных в UDP не должен превышать: (минимальная длина IP-пакета) - (Max IP Header Size) - (UDP Header Size) = 576 - 60 - 8 = 508 байт.

В Jumbogram’max IPv6-пакеты UDP могут иметь больший размер. Максимальное значение составляет 4 294 967 295 байт (232 - 1), из которых 8 байт соответствуют заголовку, а остальные 4 294 967 287 байт – данным.

Следует заметить, что большинство современных сетевых устройств отправляют и принимают пакеты IPv4 длиной до 10 000 байт без их разделения на отдельные пакеты. Неофициально такие пакеты называют Jumbo-пакетами, хотя понятие «Jumbo» официально относится к IPv6. Тем не менее Jumbo-пакеты поддерживают не все устройства, и перед организацией связи с помощью UDP/IP IPv4-сообщений с длиной, превышающей 1500 байт, нужно проверять возможность такой связи опытным путем на конкретном оборудовании.

Контрольная сумма

Поле контрольной суммы используется для проверки заголовка и данных на ошибки. Если сумма не сгенерирована передатчиком, то поле заполняется нулями. Поле не является обязательным для IPv4.

Метод для вычисления контрольной суммы определен в RFC 1071.

Перед расчетом контрольной суммы, если длина UDP-сообщения в байтах нечетна, то UDP-сообщение дополняется в конце нулевым байтом (псевдозаголовок и добавочный нулевой байт не отправляются вместе с сообщением, они используются только при расчете контрольной суммы). Поле контрольной суммы в UDP-заголовке во время расчета контрольной суммы принимается нулевым.

Для расчета контрольной суммы псевдозаголовок и UDP-сообщение разбиваются на двухбайтные слова. Затем рассчитывается сумма всех слов в арифметике обратного кода (то есть кода, в котором отрицательное число получается из положительной инверсии всех разрядов числа и существует два нуля: 0x0000 (обозначается +0) и 0xffff (обозначается -0)). Результат записывается в соответствующее поле в UDP-заголовке.

Значение контрольной суммы, равное 0x0000 (+0 в обратном коде), зарезервировано и означает, что для посылки контрольная сумма не вычислялась. В случае если контрольная сумма вычислялась и получилась равной 0x0000, в поле контрольной суммы заносят значение 0xffff (-0 в обратном коде).

При получении сообщения получатель считает контрольную сумму заново (уже учитывая поле контрольной суммы), и если в результате получится -0 (то есть 0xffff), то контрольная сумма считается сошедшейся. Если сумма не сходится (данные были повреждены при передаче, либо контрольная сумма неверно посчитана на передающей стороне), то решение о дальнейших действиях принимает принимающая сторона. Как правило, в большинстве современных устройств, работающих с UDP/IP-пакетами, имеются настройки, позволяющие либо игнорировать такие пакеты, либо пропускать их на дальнейшую обработку, невзирая на неправильность контрольной суммы.

Надежность и решения проблемы перегрузок

Из-за недостатка надежности приложения UDP должны быть готовы к некоторым потерям, ошибкам и дублированиям. Некоторые из них (например, TFTP) могут при необходимости добавить элементарные механизмы обеспечения надежности на прикладном уровне.

Но чаще такие механизмы не используются UDP-приложениями и даже мешают им. Потоковые медиа, многопользовательские игры в реальном времени и VoIP – примеры приложений, часто использующих протокол UDP. В этих конкретных приложениях потеря пакетов обычно не является большой проблемой. Если приложению необходим высокий уровень надежности, то можно использовать другой протокол (TCP) или воспользоваться методами помехоустойчивого кодирования (Erasure coderuen).

Более серьезной потенциальной проблемой является то, что, в отличие от TCP, основанные на UDP приложения не обязательно имеют хорошие механизмы контроля и избегания перегрузок. Чувствительные к перегрузкам UDP-приложения, которые потребляют значительную часть доступной пропускной способности, могут поставить под угрозу стабильность в Интернете.

Сетевые механизмы были предназначены для того, чтобы свести к минимуму возможные эффекты от перегрузок при неконтролируемых высокоскоростных нагрузках. Такие сетевые

элементы, как маршрутизаторы, использующие пакетные очереди и техники сброса, часто являются единственным доступным инструментом для замедления избыточного UDP-трафика. DCCP (англ. Datagram Congestion Control Protocol «протокол контроля за перегрузками датаграмм») разработан как частичное решение этой потенциальной проблемы с помощью добавления к конечному хосту механизмов для отслеживания перегрузок для высокоскоростных UDP-потоков вроде потоковых медиа.

DCCP

DCCP (англ. Datagram Congestion Control Protocol) – протокол транспортного уровня модели OSI, разрабатываемый IETF. Он предоставляет механизмы для отслеживания перегрузок в сети, избегая необходимости создавать их на прикладном уровне. Этот протокол не гарантирует доставку информации в нужном порядке. Основным отличием от UDP является наличие механизма контроля перегрузок.

Протокол создан в 2002 году, принят в качестве стандарта в марте 2006 года, номер протокола: 33/IP, и он описан в спецификации RFC 4340. Протокол DCCP доступен в ядре Linux с версии 2.6.14 и улучшается с каждым выпуском. Для туннелирования пакетов DCCP через NAT разработан специальный протокол DCCP-UDP.

Протокол TCP

Transmission Control Protocol (TCP, протокол управления передачей) – один из основных протоколов передачи данных Интернета, предназначенный для управления передачей данных. Сети и подсети, в которых совместно используются протоколы TCP и IP, называются сетями TCP/IP.

Протокол принят в качестве стандарта в сентябре 1981 года, номер протокола: 6/IP и он описан в спецификации RFC 793.

В стеке протоколов IP TCP выполняет функции протокола транспортного уровня модели OSI.

Механизм TCP предоставляет поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета, гарантируя тем самым, в отличие от UDP, целостность передаваемых данных и уведомление отправителя о результатах передачи.

Реализации TCP обычно встроены в ядра ОС. Существуют реализации TCP, работающие в пространстве пользователя.

Когда осуществляется передача от компьютера к компьютеру через Интернет, TCP работает на верхнем уровне между двумя конечными системами, например браузером и веб-сервером. TCP осуществляет надежную передачу потока байтов от одной программы на некотором компьютере к другой программе на другом компьютере (например, программы для электронной почты, для обмена файлами). TCP контролирует длину сообщения, скорость обмена сообщениями, сетевой трафик.

Механизм действия протокола

В отличие от традиционной альтернативы – UDP, который может сразу же начать передачу пакетов, TCP устанавливает соединения, которые должны быть созданы перед передачей данных. TCP-соединение можно разделить на 3 стадии:

- установка соединения,
- передача данных,
- завершение соединения.

Возможные состояния сеанса TCP

- CLOSED – начальное состояние узла. Фактически фиктивное.
- LISTEN – сервер ожидает запросов установления соединения от клиента.
- SYN-SENT – клиент отправил запрос серверу на установление соединения и ожидает ответа.
- SYN-RECEIVED – сервер получил запрос на соединение, отправил ответный запрос и ожидает подтверждения.
- ESTABLISHED – соединение установлено, идет передача данных.
- FIN-WAIT-1 – одна из сторон (назовем ее узел-1) завершает соединение, отправив сегмент с флагом FIN.
- CLOSE-WAIT – другая сторона (узел-2) переходит в это состояние, отправив, в свою очередь, сегмент ACK, и продолжает одностороннюю передачу.
- FIN-WAIT-2 – узел-1 получает ACK, продолжает чтение и ждет получения сегмента с флагом FIN.
- LAST-ACK – узел-2 заканчивает передачу и отправляет сегмент с флагом FIN.
- TIME-WAIT – узел-1 получил сегмент с флагом FIN, отправил сегмент с флагом ACK и ждет 2 × MSL секунд, перед окончательным закрытием соединения.
- CLOSING – обе стороны инициировали закрытие соединения одновременно: после отправки сегмента с флагом FIN узел-1 также получает сегмент FIN, отправляет ACK и находится в ожидании сегмента ACK (подтверждения на свой запрос о разъединении).

Установка соединения

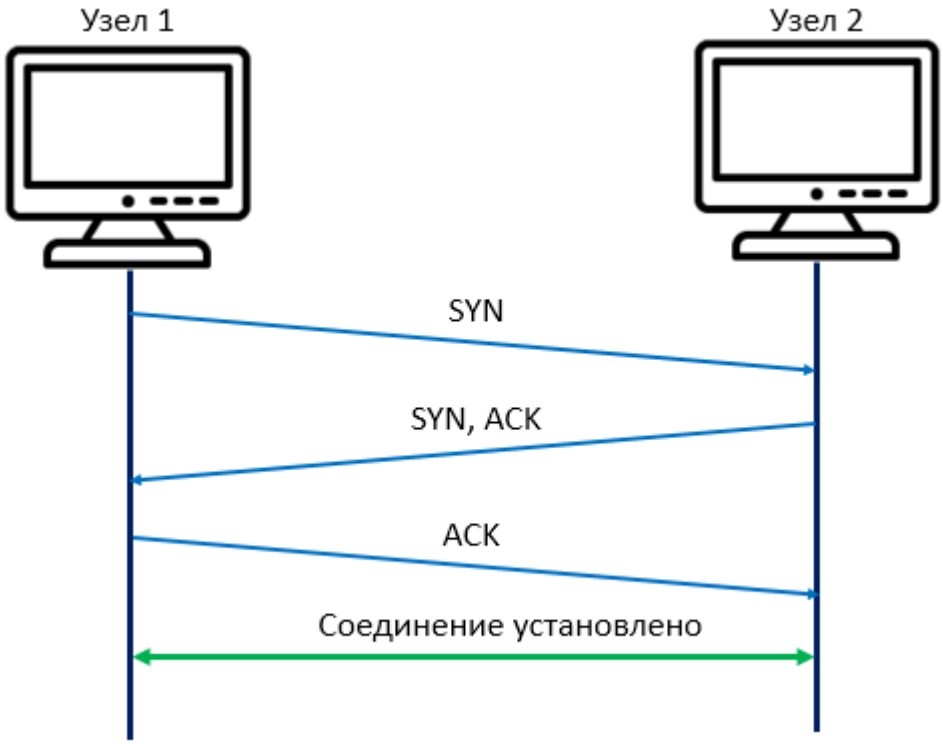
Процесс начала сеанса TCP (также называемый «рукопожатие» (англ. handshake)) состоит из трех шагов:

1. Клиент, который намеревается установить соединение, посылает серверу сегмент с номером последовательности и флагом SYN.Сервер получает сегмент, запоминает номер последовательности и пытается создать сокет (буферы и управляющие структуры памяти) для обслуживания нового клиента:
    - в случае успеха сервер посылает клиенту сегмент с номером последовательности и флагами SYN и ACK и переходит в состояние SYN-RECEIVED;
    - в случае неудачи сервер посылает клиенту сегмент с флагом RST.
2. Если клиент получает сегмент с флагом SYN, то он запоминает номер последовательности и посылает сегмент с флагом ACK.
    - Если клиент одновременно получает и флаг ACK (что обычно и происходит), то он переходит в состояние ESTABLISHED.
    - Если клиент получает сегмент с флагом RST, то он прекращает попытки соединиться.

- Если клиент не получает ответа в течение 10 секунд, то он повторяет процесс соединения заново.

3. Если сервер в состоянии SYN-RECEIVED получает сегмент с флагом ACK, то он переходит в состояние ESTABLISHED. В противном случае после тайм-аута он закрывает сокет и переходит в состояние CLOSED.

Процесс называется «трехэтапным согласованием» (англ. three way handshake), так как, несмотря на то что возможен процесс установления соединения с использованием четырех сегментов (SYN в сторону сервера, ACK в сторону клиента, SYN в сторону клиента, ACK в сторону сервера), на практике для экономии времени используется три сегмента.



Передача данных

При обмене данными приемник использует номер последовательности, содержащийся в получаемых сегментах, для восстановления их исходного порядка. Приемник уведомляет передающую сторону о номере последовательности, до которой он успешно получил данные, включая его в поле «Номер подтверждения». Все получаемые данные, относящиеся к промежутку подтвержденных последовательностей, игнорируются. Если полученный сегмент содержит номер последовательности больший, чем ожидаемый, то данные из сегмента буферизируются, но номер подтвержденной последовательности не изменяется. Если впоследствии будет принят сегмент, относящийся к ожидаемому номеру последовательности, то порядок данных будет автоматически восстановлен исходя из номеров последовательностей в сегментах.

Для того чтобы передающая сторона не отправляла данные интенсивнее, чем их может обработать приемник, TCP содержит средства управления потоком. Для этого используется поле «Окно». В сегментах, направляемых от приемника передающей стороне, в поле «Окно» указывается текущий размер приемного буфера. Передающая сторона сохраняет размер окна

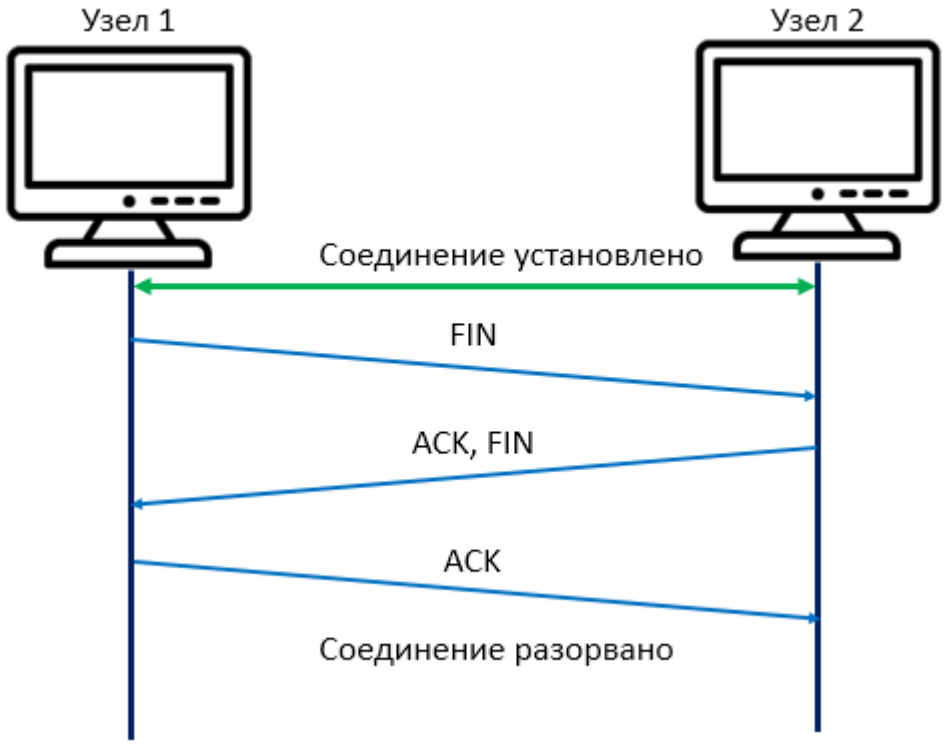
и отправляет данных не более, чем указал приемник. Если приемник указал нулевой размер окна, то передача данных в направлении этого узла не происходит, пока приемник не сообщит о большем размере окна.

В некоторых случаях передающее приложение может явно затребовать протолкнуть данные до некоторой последовательности принимающему приложению, не буферизируя их. Для этого используется флаг PSH. Если в полученном сегменте обнаруживается флаг PSH, то реализация TCP отдает все буферизированные на текущий момент данные принимающему приложению. «Проталкивание» используется, например, в интерактивных приложениях. В сетевых терминалах нет смысла ожидать ввода пользователя после того, как он закончил набирать команду. Поэтому последний сегмент, содержащий команду, обязан содержать флаг PSH, чтобы приложение на принимающей стороне смогло начать ее выполнение.

Завершение соединения

Завершение соединения можно рассмотреть в три этапа:

1. Клиент отправляет серверу флаг FIN на завершение соединения.
2. Сервер посылает клиенту флаги ответа ACK, FIN, что соединение закрыто.
3. После получения этих флагов клиент закрывает соединение и в подтверждение отправляет серверу ACK, что соединение закрыто.



Заголовок сегмента TCP

Одним из полей, которые указываются в заголовке сегмента TCP, является «Флаг». Это поле содержит 6 битовых флагов:

- URG – поле «Указатель важности» задействовано (англ. Urgent pointer field is significant);
- ACK – поле «Номер подтверждения» задействовано (англ. Acknowledgement field is significant);
- PSH (англ. Push function) – инструктирует получателя протолкнуть данные, накопившиеся в приемном буфере, в приложение пользователя;
- RST – оборвать соединения, сбросить буфер (очистка буфера) (англ. Reset the connection);
- SYN – синхронизация номеров последовательности (англ. Synchronize sequence numbers);
- FIN (англ. final «бит») – флаг, будучи установленным, указывает на завершение соединения (англ. FIN bit used for connection termination).

Протокол SCTP

SCTP (англ. Stream Control Transmission Protocol «протокол передачи с управлением потоком») – протокол транспортного уровня в компьютерных сетях, появившийся в 2000 году в IETF. RFC 4960 описывает этот протокол, а RFC 3286 содержит техническое вступление к нему.

Как и любой другой протокол передачи данных транспортного уровня, SCTP работает аналогично TCP или UDP. Будучи более новым протоколом, SCTP имеет несколько нововведений, таких как многопоточность, защита от DDoS-атак, синхронное соединение между двумя хостами по двум и более независимым физическим каналам (multi-homing).

Преимущества:

1. Использование множественных интерфейсов (англ Multihoming). Допустим, у нас есть два хоста. И хотя бы один из них имеет несколько сетевых интерфейсов и, соответственно, несколько IP-адресов. В TCP понятие «соединение» означает обмен данными между двумя точками, в то время как в SCTP имеет место концепция ассоциации (англ. association), обозначающая все происходящее между двумя хостами.
2. Многопоточность. Данные приходят в точку по независимым потокам. Это позволяет устранить феномен en:Head-of-line blocking, которым так страдает TCP.
3. Поиск пути с мониторингом. Протоколом выбирается первичный маршрут передачи данных, а также производится проверка и мониторинг связности пути.
4. Механизмы валидации и проверки подлинности.
5. Защита адресата от flood-атак (технология 4-way handshake) и уведомление о потерянных пакетах и нарушенных цепочках.
6. Улучшенная система контроля ошибок, подходящая для jumbo-пакетов в Ethernet.

Часть достоинств вытекает из того факта, что изначально разработчики SCTP проектировали протокол под нужды передачи телефонии (SS7) по протоколу IP.

Недостаток:

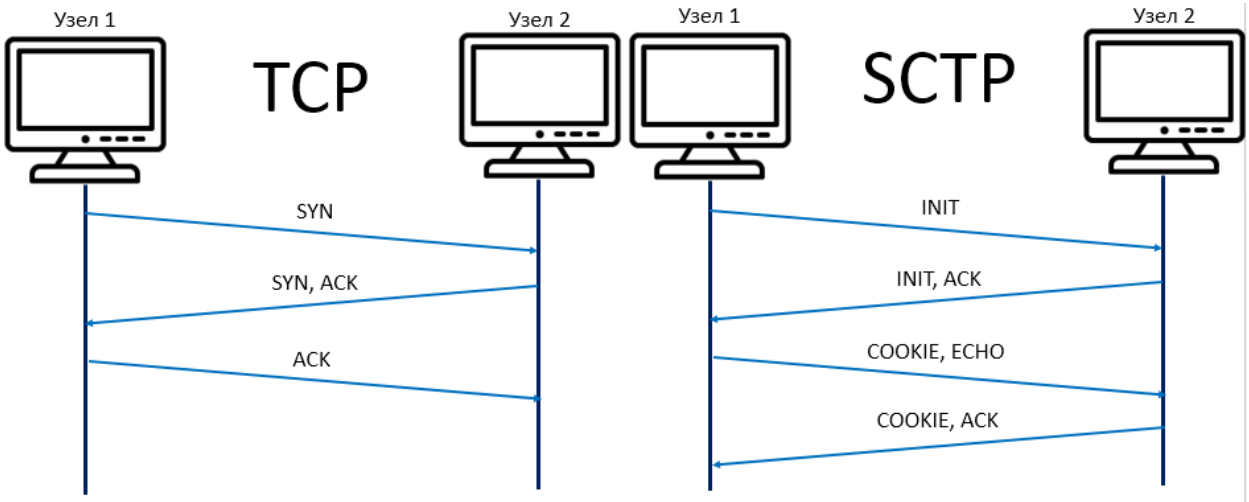
1. Бóльшая занимаемая полоса, то есть относительный объем служебного трафика больше, чем при использовании TCP/UDP.

Безопасное установление соединения

Создание нового подключения в протоколах TCP и SCTP происходит при помощи механизма подтверждения (квитирования) пакетов. В протоколе TCP данная процедура получила название «трехэтапное квитирование» (three-way handshake). Клиент посылает пакет SYN (сокр. Synchronize). Сервер отвечает пакетом SYN-ACK (Synchronize-Acknowledge). Клиент подтверждает прием пакета SYN-ACK пакетом ACK. На этом процедура установления соединения завершается.

Протокол TCP имеет потенциальную уязвимость, обусловленную тем, что нарушитель, установив фальшивый IP-адрес отправителя, может послать серверу множество пакетов SYN. При получении пакета SYN сервер выделяет часть своих ресурсов для установления нового соединения. Обработка множества пакетов SYN рано или поздно затребует все ресурсы сервера и сделает невозможной обработку новых запросов. Такой вид атак называется «отказ в обслуживании» (Denial of Service, DoS).

Протокол SCTP защищен от подобных атак с помощью механизма четырехэтапного квитирования (four-way handshake) и вводом маркера (cookie). По протоколу SCTP клиент начинает процедуру установления соединения, посылая пакет INIT. В ответ сервер посылает пакет INIT-ACK, который содержит маркер (уникальный ключ, идентифицирующий новое соединение). Затем клиент отвечает посылкой пакета COOKIE-ECHO, в котором содержится маркер, полученный от сервера. Только после этого сервер выделяет свои ресурсы новому подключению и подтверждает это отправкой клиенту пакета COOKIE-ACK.

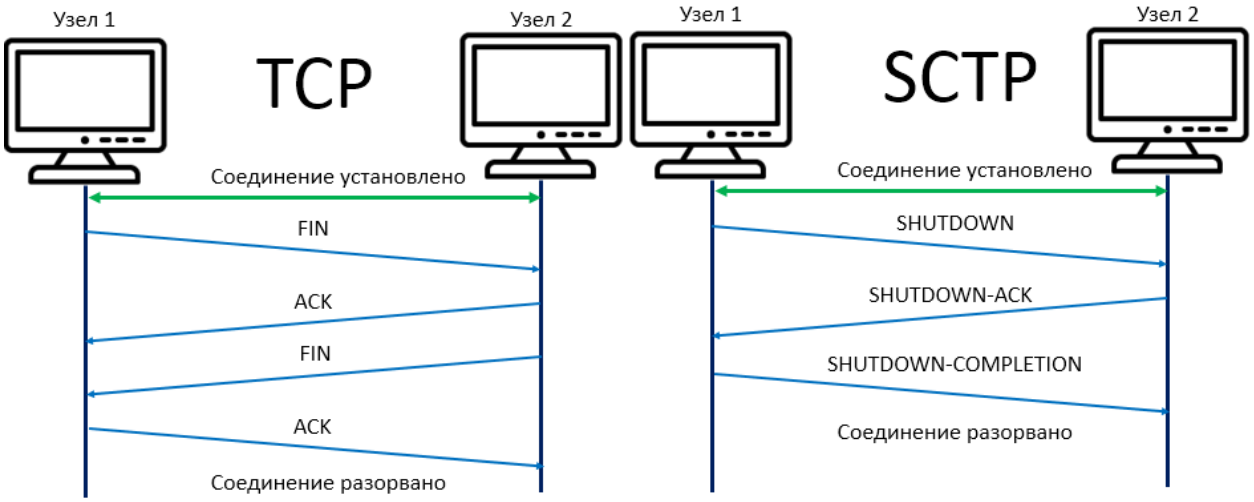


Поэтапное завершение передачи данных

Рассмотрим отличия между процедурой закрытия сокетов протокола SCTP и процедурой частичного закрытия (half-close) протокола TCP.

В протоколе TCP возможна ситуация частичного закрытия соединения, когда один узел закончил передачу данных (выполнив посылку пакета FIN), но продолжает принимать данные по этому соединению. Другой узел может продолжать передавать данные до тех пор, пока сам не проведет закрытие соединения на своей стороне. Состояние частичного закрытия используется приложениями крайне редко, поэтому разработчики протокола SCTP посчитали нужным заменить его последовательностью сообщений для разрыва существующей ассоциации. Когда узел закрывает свой сокет (посылает сообщение SHUTDOWN), оба

корреспондента должны прекратить передачу данных, при этом разрешается лишь обмен пакетами, подтверждающими прием ранее отправленных данных.



Многопоточность

TCP управляет последовательностью байтов: данные, посланные приложением-отправителем, должны поступать приложению-получателю строго в том же порядке (в то время как протокол IP способен поменять последовательность пакетов; кроме того, пропавшие пакеты посылаются повторно и обычно прибывают к получателю с нарушением последовательности; для борьбы с этими явлениями данные накапливаются в буфере). SCTP может транспортировать данные между двумя точками (узлами) одновременно по нескольким потокам сообщений. В противоположность TCP, SCTP обрабатывает целые сообщения, а не обычные байты информации. Это означает, что если отправитель отсылает серверу сообщение, состоящее из 100 байт за первый шаг, а за ним еще 50 байт, то получатель за первый шаг получит именно первые 100 байт в первом сообщении, а только затем 50 байт на второй операции чтения из сокета.

Термин «многопоточность» (англ. multi-streaming) обозначает способность SCTP параллельно передавать один сеанс связи по нескольким независимым потокам сообщений. Например, мы передаем несколько фотографий через HTTP-приложение (например, браузер). Можно использовать для этого связку из нескольких TCP-соединений, однако также допустима SCTP-ассоциация (англ. SCTP-association), управляющая несколькими потоками сообщений для этой цели.

TCP достигает правильного порядка байтов в потоке, абстрактно назначая порядковый номер каждой отосланной единице, а упорядочивая принятые байты, используя назначенные

порядковые номера, по мере их прибывания. С другой стороны, SCTP присваивает различные порядковые номера сообщениям, посылаемым в конкретном потоке. Это разрешает независимое упорядочивание сообщений по разным потокам. Так или иначе, многопоточность является опцией в SCTP. В зависимости от желаний пользовательского приложения, сообщения могут быть обработаны не в порядке их отправления, а в порядке их поступления.

Безопасность

SCTP был разработан с некоторыми функциями, позволяющими повысить безопасность, такими как «4-кратное рукопожатие» (по сравнению с «трехкратным рукопожатием» в TCP), чтобы предотвратить SYN-flood-атаки, и использования больших Cookie для проверки подлинности ассоциации.

Надежность была одним из ключевых аспектов разработки безопасности протокола SCTP. Multi-homing позволяет ассоциации оставаться открытой, даже если некоторые используемые маршруты и интерфейсы стали недоступны.

Шифрование не является частью оригинального дизайна SCTP.

В некоторых случаях SCTP является хорошим кандидатом для проверки на прочность стека TCP/IP (англ.). Причиной для этого является тот факт, что некоторые операционные системы распространяются с поддержкой протокола SCTP, но ввиду его слабой известности (по сравнению с TCP или UDP) администраторы иногда забывают настроить в брандмауэре обнаружение вторжений, что дает возможность для сканирования трафика.

Обработка ошибок

Повтор передачи

Повторная передача блоков DATA может быть обусловлена: а) тайм-аутом, определяемым таймером повтора (retransmission timer), или б) получением SACK, показывающим, что блок DATA не был получен адресатом. Для снижения вероятности насыщения повтор передачи блоков DATA ограничивается. Значение тайм-аута для повтора (RTO) устанавливается на основе оценки времени кругового обхода и уменьшается экспоненциально с ростом частоты потери сообщений. Для активных ассоциаций с почти постоянным уровнем трафика DATA причиной повтора, скорее всего, будут сообщения SACK, а не тайм-аут. Для снижения вероятности ненужных повторов используется правило 4 SACK, в соответствии с которым повтор передачи происходит только по четвертому SACK, указывающему на пропуск блока данных. Это позволяет предотвратить повторы передачи, вызванные нарушением порядка доставки.

Сбой в пути

Поддерживается счетчик для числа повторов передачи по конкретному адресу получателя без подтверждения успешной доставки. Когда значение этого счетчика достигает заданного порога (конфигурационный параметр), адрес объявляется неактивным и протокол SCTP начинает использовать другой адрес для передачи блоков DATA. Кроме того, по всем неиспользуемым (дополнительным) адресам периодически передаются специальные блоки Heartbeat и поддерживается счетчик числа блоков Heartbeat, переданных без возврата, соответствующего Heartbeat Ack. Когда значение счетчика достигает заданного порога (параметр конфигурации), соответствующий адрес объявляется неактивным. Блоки Heartbeat передаются по неактивным адресам до тех пор, пока не будет получено сообщение Ack, говорящее о восстановлении активности адреса. Частота передачи блоков Heartbeat определяется значением RTO и дополнительной задержкой, которая позволяет передавать блоки Heartbeat без помех для пользовательского трафика.

Отказ в конечной точке

Для всех адресов получателя поддерживается общий счетчик числа повторов или блоков Heartbeat, передачи данных удаленной точке без получения от нее соответствующего подтверждения (Ack). Когда значение счетчика достигает заданного порога (параметр конфигурации), конечная точка декларируется как недостижимая, и ассоциация SCTP закрывается.

Сравнение возможностей протоколов транспортного уровня

Параметр	UDP	TCP	SCTP
Установка соединения	Нет	Да	Да
Надёжная передача	Нет	Да	Да
Сохранение границ сообщения	Да	Нет	Да
Упорядоченная доставка	Нет	Да	Да
Неупорядоченная доставка	Да	Нет	Да
Контрольные суммы данных	Да	Да	Да
Управление накоплением	Нет	Да	Да
Многопоточность	Нет	Нет	Да
Поддержка множественных интерфейсов	Нет	Нет	Да

Сокет

Порт

Порт (англ. port) – это число, записываемое в заголовках протоколов транспортного уровня модели OSI (UDP, TCP, DCCP, SCTP). Количество портов 65 536 (это 2^{16}, начало – 0). Порты разделены на три диапазона:

2. общеизвестные (системные): 0–1023;
3. зарегистрированные (пользовательские): 1024–49 151;
4. динамические (частные): 49 152–65 535.

Порты разных протоколов не пересекаются.

Сокет

Сокет (англ. socket «разъем») – название программного интерфейса для обеспечения обмена данными между процессами. Процессы при таком обмене могут исполняться как на одной ЭВМ, так и на различных ЭВМ, связанных между собой сетью. Сокет – абстрактный объект, представляющий конечную точку соединения.

Следует различать клиентские и серверные сокеты. Клиентские сокеты грубо можно сравнить с конечными аппаратами телефонной сети, а серверные – с коммутаторами. Клиентское приложение (например, браузер) использует только клиентские сокеты, а серверное (например, веб-сервер, которому браузер посылает запросы) – как клиентские, так и серверные сокеты.

Интерфейс сокетов впервые появился в BSD Unix. Программный интерфейс сокетов описан в стандарте POSIX.1 и в той или иной мере поддерживается всеми современными операционными системами.

Для взаимодействия между машинами с помощью стека протоколов TCP/IP используются адреса и порты. IP-адрес на текущий момент представляет собой 32-битный адрес (для протокола IPv4, 128-битный для IPv6), наиболее часто его представляют в символьной форме mmm.nnn.ppp.qqq (адрес, разбитый на четыре поля, разделенных точками, по одному байту в поле). Порт – это номер порта в диапазоне от 0 до 65 535 (для протоколов TCP или UDP).

Эта пара и есть сокет («гнездо», соответствующее адресу и порту).

В процессе обмена, как правило, используется два сокета – сокет отправителя и сокет получателя. Например, при обращении к серверу на HTTP-порт сокет будет выглядеть так: 194.106.118.30:80, а ответ будет поступать на mmm.nnn.ppp.qqq: xxxxx.

В упрощенном виде для установления соединения необходимы:

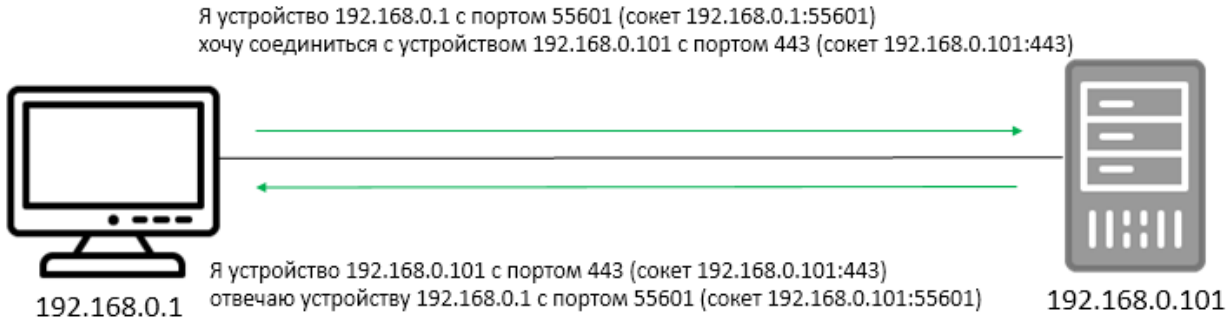
1. протокол;
2. два IP-адреса:
    - адрес отправителя,
    - адрес получателя;
3. два номера порта (для UDP, TCP, DCCP, SCTP):
    - порт отправителя,
    - порт получателя.

Каждый процесс может создать «слушающий» сокет (серверный сокет) и привязать его к какому-нибудь порту операционной системы (в UNIX непривилегированные процессы не могут использовать порты меньше 1024).

Слушающий процесс обычно находится в цикле ожидания, то есть просыпается при появлении нового соединения. При этом сохраняется возможность проверить наличие соединений на данный момент, установить тайм-аут для операции и т.д.

Каждый сокет имеет свой адрес. ОС семейства UNIX могут поддерживать много типов адресов, но обязательными являются INET-адрес и UNIX-адрес. Если привязать сокет к UNIX-адресу, то будет создан специальный файл (файл сокета) по заданному пути, через который смогут сообщаться любые локальные процессы путем чтения/записи из него. Сокеты типа INET доступны из сети и требуют выделения номера порта.

Обычно клиент явно «подсоединяется» к слушателю, после чего любое чтение или запись через его файловый дескриптор будет передавать данные между ним и сервером.



VPN

VPN (англ. Virtual Private Network «виртуальная частная сеть») – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрование, аутентификация, инфраструктура открытых ключей, средства для защиты от повторов и изменений передаваемых по логической сети сообщений).

Обычно VPN развертывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP, UDP).

Пользователи Microsoft Windows обозначают термином «VPN» одну из реализаций виртуальной сети – PPTP, причем используемую зачастую не для создания частных сетей.

Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP в какой-нибудь другой протокол – IP (такой способ использует реализация PPTP – Point-to-Point Tunneling Protocol) или Ethernet (PPPoE) (хотя и они имеют различия). Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» на постсоветском пространстве для предоставления выхода в Интернет.

При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации. При правильной настройке всех компонентов технология VPN обеспечивает анонимность в сети.

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть (таких сетей может быть несколько) и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет). Возможно также подключение к виртуальной сети отдельного компьютера. Подключение удаленного пользователя к VPN производится посредством сервера доступа, который подключен как к внутренней, так и к внешней (общедоступной) сети. При подключении удаленного пользователя (либо при установке соединения с другой защищенной сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов удаленный пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации.

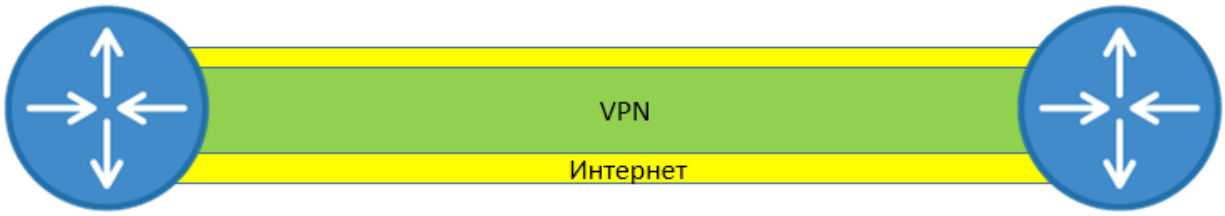
AAA

Для обеспечения безопасности сети необходимо обеспечить контроль за доступом к различным элементам сети со стороны пользователей. Такими элементами могут быть сетевые устройства, серверы, компьютеры, приложения или даже сегменты самой сети. Сценарии разные, а принцип один – аутентификация, авторизация и учет (AAA – Authentication, Authorization, Accounting).

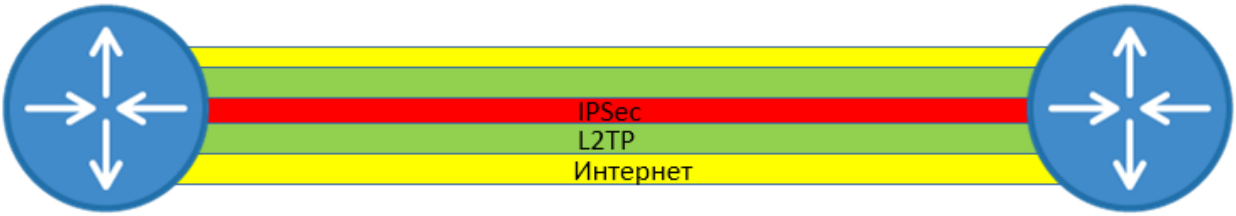
Аутентификация (authentication) – заключается в том, что первая сторона предоставляет второй стороне весомые доказательства того, что она говорит правду (логин и пароль, сертификат и др.), а вторая сторона оценивает эти доказательства и на основе совокупности представленных доказательств принимает решение, верить или не верить первой стороне.

Авторизация (authorization) – процесс, происходящий всегда после успешной аутентификации первой стороны, в котором вторая сторона, уже зная, кто перед ней стоит, смотрит в своих записях данные о том, что разрешено делать второй стороне.

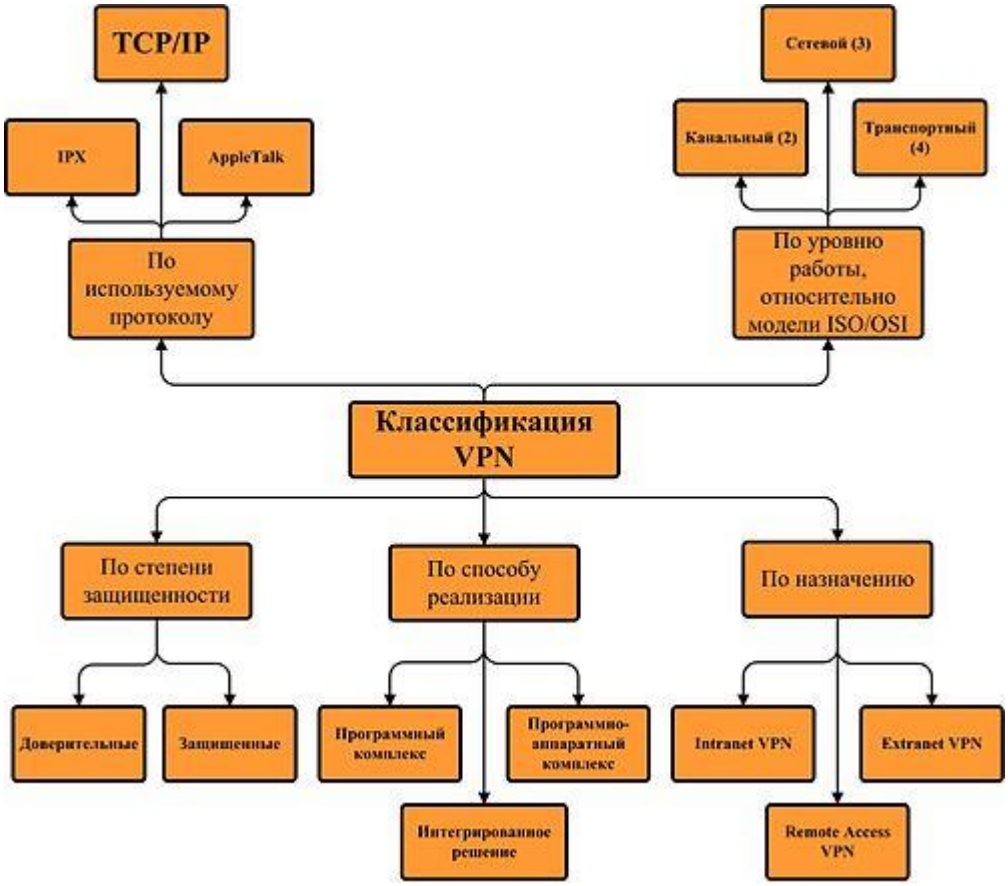
Учет (accounting) – параллельный с аутентификацией и авторизацией этап во время которого в журнал записывается сообщение об успешной или безуспешной попытке выполнения какого-либо действия.



Возможно использование связки из двух VPN. В таком случае объединяются преимущества каждой из VPN. Например, GRE/IPSec, L2TP/IPSec и др.



Классификация VPN



1. По степени защищенности используемой среды:

- *защищенные.* Наиболее распространенный вариант виртуальных частных сетей. С его помощью возможно создать надежную и защищенную сеть на основе ненадежной сети, как правило Интернета. Примером защищенных VPN являются: IPSec, OpenVPN и PPTP;
- *доверительные.* Используются в случаях, когда передающую среду можно считать надежной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Проблемы безопасности становятся неактуальными. Примерами подобных решений VPN являются: Multi-protocol label switching (MPLS) и L2TP (Layer 2 Tunnelling Protocol) (точнее будет сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие – например, L2TP, как правило, используется в паре с IPSec).

2. По способу реализации:
   - *в виде специального программно-аппаратного обеспечения.* Реализация сети VPN осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищенности;
   - *в виде программного решения.* Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN;
   - *интегрированное решение.* Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.
3. По назначению:
   - *Intranet VPN.* Используют для объединения в единую защищенную сеть нескольких распределенных филиалов одной организации, обменивающихся данными по открытым каналам связи;
   - *Remote Access VPN.* Используют для создания защищенного канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона или интернет-киоска;
   - *Extranet VPN.* Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ злоумышленников к особо ценной, конфиденциальной информации;
   - *Internet VPN.* Используется для предоставления доступа к Интернету провайдерами, обычно если по одному физическому каналу подключаются несколько пользователей. Протокол PPPoE стал стандартом в ADSL-подключениях. L2TP был широко распространен в середине 2000-х годов в домовых сетях: в те времена внутрисетевой трафик не оплачивался, а внешний стоил дорого. Это давало возможность контролировать расходы: когда VPN-соединение выключено, пользователь ничего не платит. В настоящее время проводной Интернет дешевый или безлимитный, а на стороне пользователя зачастую есть маршрутизатор, на котором включать-выключать Интернет не так удобно, как на компьютере. Поэтому L2TP-доступ отходит в прошлое;
   - *Client/Server VPN.* Он обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том,

что VPN строится между узлами, находящимися, как правило, в одном сегменте сети – например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающимися к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, но вместо разделения трафика используется его шифрование.

4. По типу протокола. Существуют реализации виртуальных частных сетей под TCP/IP, IPX и AppleTalk. Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол TCP/IP, и абсолютное большинство решений VPN поддерживает именно его. Адресация в нем чаще всего выбирается в соответствии со стандартом RFC5735 из диапазона приватных сетей TCP/IP.
5. По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI.

NAT

NAT (от англ. Network Address Translation «преобразование сетевых адресов») – это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Также имеет названия: IP Masquerading, Network Masquerading и Native Address Translation.

Преобразование адреса методом NAT может производиться почти любым маршрутизирующим устройством – маршрутизатором, сервером доступа, межсетевым экраном.

Существует два вида NAT:

- Source NAT (SNAT, SRC-NAT) – изменение IP-адреса и/или порта источника и выполнение обратной функции для ответа;
- Destination NAT (DNAT, DST-NAT) – изменение IP-адреса и/или порта назначения и выполнение обратной функции для ответа.

Преимущества:

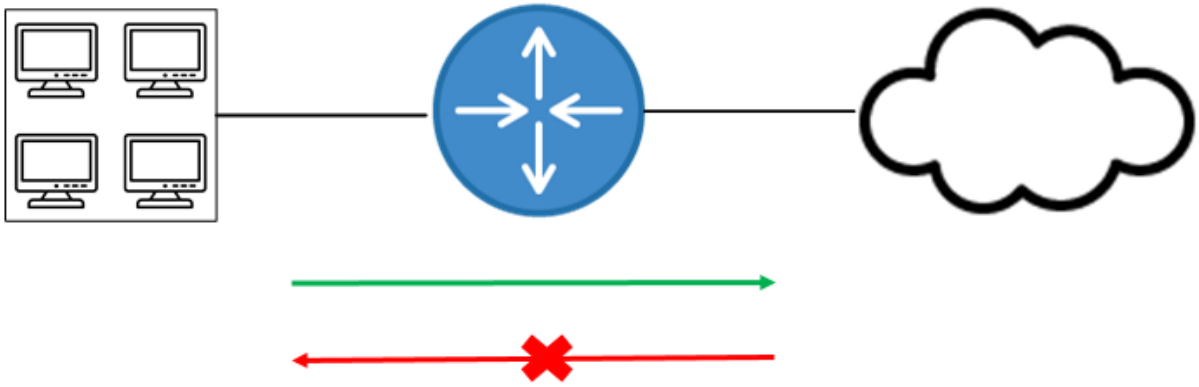
1. Позволяет сэкономить IP-адреса (только в случае использования NAT в режиме PAT), транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 публичный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с приватными (внутренними) IP-адресами.
2. Позволяет предотвратить или ограничить обращение снаружи к внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создается трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или с помощью статической записи), они не пропускаются.
3. Позволяет скрыть определенные внутренние сервисы внутренних хостов/серверов. По сути, выполняется та же указанная выше трансляция на определенный порт, но возможно подменить внутренний порт официально зарегистрированной службы (например, 80-й порт TCP (HTTP-сервер) на внешний 54055-й). Тем самым снаружи, на внешнем IP-адресе после трансляции адресов на сайт (или форум) для осведомленных

посетителей можно будет попасть по адресу http://example.org:54055, но на внутреннем сервере, находящемся за NAT, он будет работать на обычном 80-м порте. Повышение безопасности и скрытие «непубличных» ресурсов.

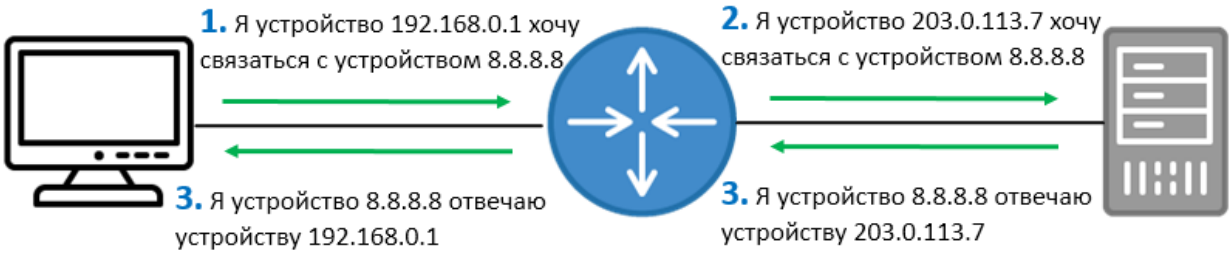
Source NAT

Задача Source NAT (SNAT, SRC-NAT) – изменение IP-адреса и/или порта источника и выполнение обратной функции для ответа.

99 % случаев использования Source NAT – это выход множества ПК из LAN в Интернет. LAN-сеть, находящаяся за NAT = использующая NAT (NAT'ed). Связь доступна из NAT'ed-сети вовне. Наоборот – нет.



Принцип действия Source NAT:



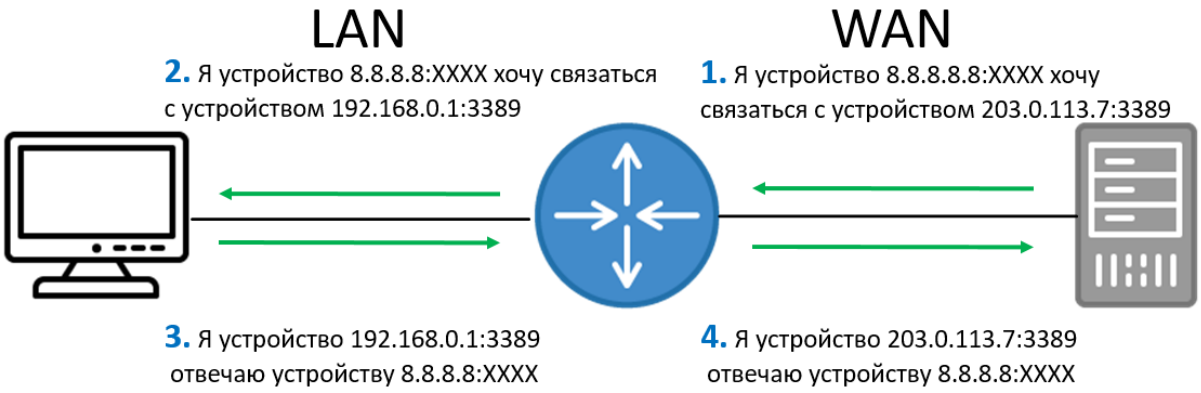
Базовые концепции:

1. «Базовый» NAT («один к одному», one-to-one). Количество одновременных выходов в Интернет из NAT'ed-сети равно количеству белых IP-адресов.
    - Статический – отображение незарегистрированного IP-адреса на зарегистрированный IP-адрес на основании «один к одному».
    - Динамический – отображает незарегистрированный IP-адрес на зарегистрированный адрес из группы зарегистрированных IP-адресов.
2. «Классический» NAT («многие к одному», many-to-one). Количество одновременных выходов в Интернет из NAT'ed-сети ограничено количеством свободных портов TCP/UDP. Самая распространенная версия NAT.

Destination NAT

Задача Destination NAT (DNAT, DST-NAT) – изменение IP-адреса и/или порта назначения и выполнение обратной функции для ответа. 99 % использования – проброс портов.

Проброс портов позволяет обращаться из Интернета к хосту в LAN за маршрутизатором, использующим NAT.



Примеры сложных задач на базе NAT

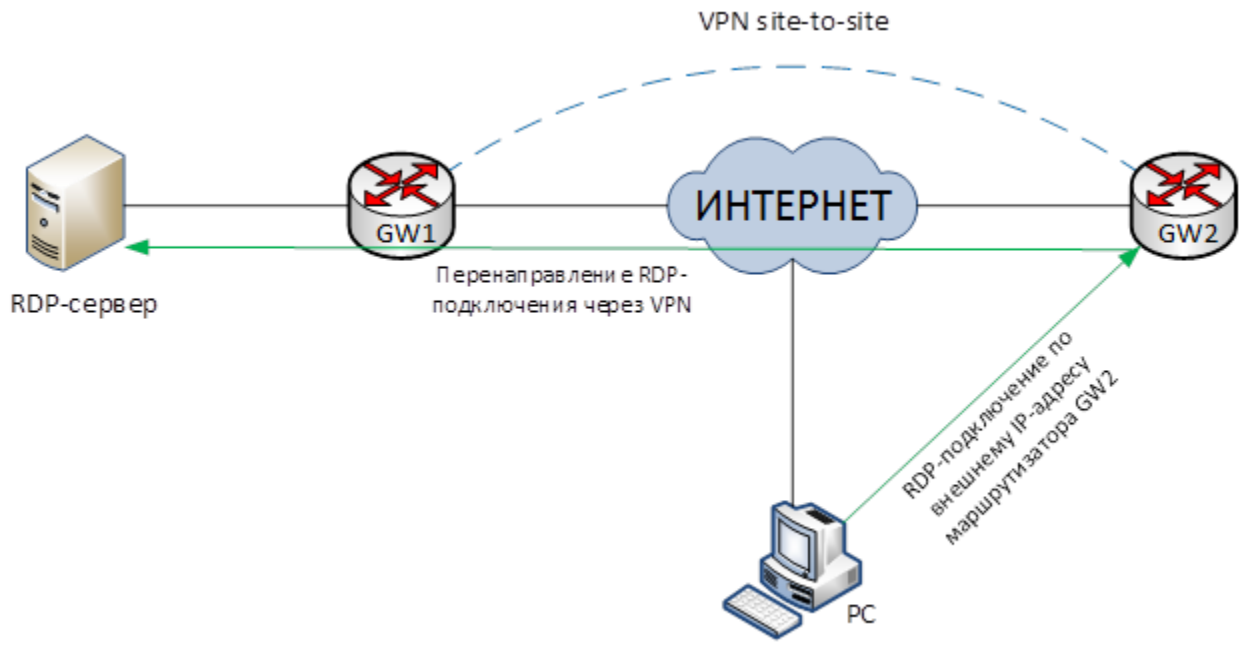
Самые частые примеры использования NAT – это:

1. обеспечение выхода в Интернет множества ПК при наличии одного белого IP-адреса;
2. проброс портов.

Но на этом задачи, которые можно решить с помощью NAT, не заканчиваются. Ниже приведены примеры задач, которые могут быть решены с помощью NAT. Такие задачи решаются в одном из курсов по настройке сетевого оборудования MikroTik от проекта «Курсы-по-ИТ.рф».

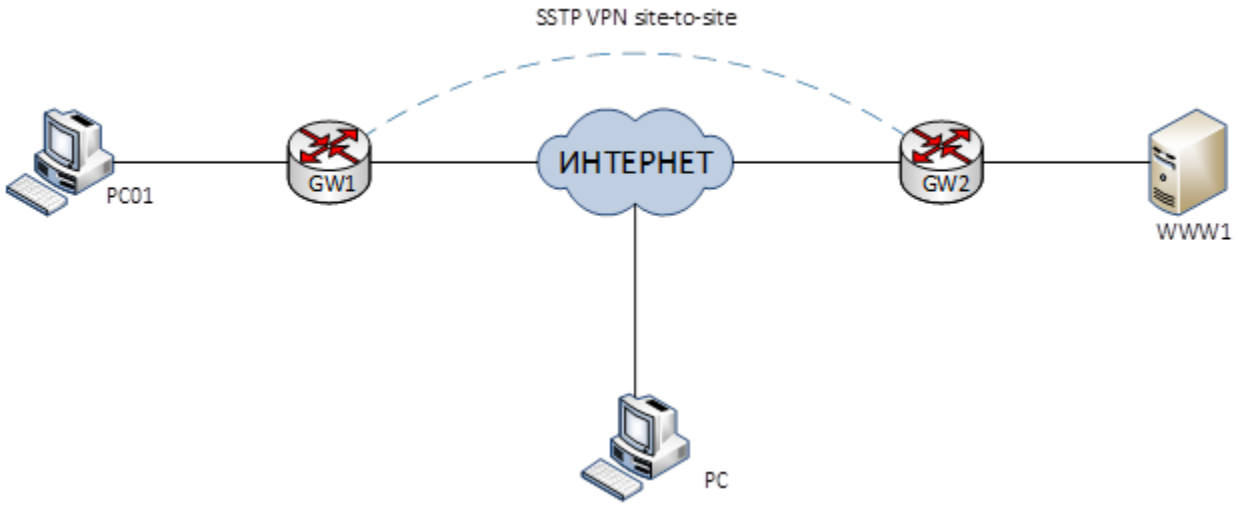
Задача № 1

Необходимо сделать так, чтобы при подключении с любого ПК в Интернет на белый IP-адрес маршрутизатора GW2 на самом деле происходило подключение на RDP-сервер, который находится во внутренней сети маршрутизатора GW1. Обмен информацией между двумя маршрутизаторами должен проходить через VPN.



Задача № 2

Необходимо сделать так, чтобы было подключение SSTP VPN, когда будет происходить подключение от маршрутизатора GW1 до GW2. Во всех остальных случаях должно срабатывать правило проброса порта. Т.е., если к GW2 обратится PC01 или PC02, должен сработать проброс портов. Номер порта, по которому работает SSTP-сервер или подключается SSTP-клиент, изменять нельзя. Т.е. запрос в обоих случаях должен прийти на 443-й порт.



Беспроводные сети

Введение

Беспроводная вычислительная сеть – вычислительная сеть, основанная на беспроводном (без использования кабельной проводки) принципе, полностью соответствующая стандартам для обычных проводных сетей (например, Ethernet). В качестве носителя информации в таких сетях могут выступать радиоволны СВЧ-диапазона.

Существует два основных направления применения беспроводных компьютерных сетей:

- работа в замкнутом объеме (офис, выставочный зал и т.п.);
- соединение удаленных локальных сетей (или удаленных сегментов локальной сети).

Виды:

- Bluetooth,
- 1G/2G/3G/4G/5G,
- Wi-Fi,
- прочее.

Bluetooth

Bluetooth (от англ. blue «синий» и tooth «зуб»; произносится /bluːtuːθ/) – производственная спецификация беспроводных персональных сетей (Wireless personal area network, WPAN). Bluetooth обеспечивает обмен информацией между такими устройствами, как персональные компьютеры (настольные, карманные, ноутбуки), мобильные телефоны, принтеры, цифровые фотоаппараты, мышки, клавиатуры, джойстики, наушники, гарнитуры на надежной, бесплатной, повсеместно доступной радиочастоте для ближней связи. Bluetooth позволяет этим устройствам сообщаться, когда они находятся в радиусе до 10 м друг от друга (дальность сильно зависит от преград и помех), даже в разных помещениях.

Логотип Bluetooth является сочетанием двух нордических («скандинавских») рун: «хагалаз» младшего футарка (ᚼ) и «беркана» (ᛒ), звуковые значения которых соответствуют инициалам Харальда I Синезубого – h и b (дат. Harald Blåtand, норв. Harald Blåtann). Логотип похож на более старый логотип для Beauknit Textiles, подразделения корпорации Beauknit. В нем используется слияние отраженной K и B для «Beauknit», он шире и имеет скругленные углы, но в общем он такой же.

Работы по созданию Bluetooth как беспроводной альтернативы кабелям RS-232 в 1994 году начал производитель телекоммуникационного оборудования Ericsson. Первоначально эта технология была приспособлена под потребности системы FLYWAY в функциональном интерфейсе между путешественниками и системой.

Спецификация Bluetooth была разработана группой Bluetooth Special Interest Group (Bluetooth SIG), которая была основана в 1998 году. В нее вошли компании Ericsson, IBM, Intel, Toshiba и Nokia. Впоследствии Bluetooth SIG и IEEE достигли соглашения, на основе которого спецификация Bluetooth стала частью стандарта IEEE 802.15.1 (дата опубликования – 14 июня 2002 года).

Безопасность

В июне 2006 года Авишай Вул и Янив Шакед опубликовали статью, содержащую подробное описание атаки на устройства Bluetooth. Материал содержал описание как активной, так и пассивной атаки, позволяющей заполучить PIN-код устройства и в дальнейшем осуществить соединение с данным устройством. Пассивная атака позволяет соответствующе экипированному злоумышленнику «подслушать» (sniffing) процесс инициализации соединения и в дальнейшем использовать полученные в результате «прослушки» и анализа данные для установления соединения (spoofing). Естественно, для проведения данной атаки злоумышленнику нужно находиться в непосредственной близости и непосредственно в момент установления связи. Это не всегда возможно. Поэтому родилась идея активной атаки. Была обнаружена возможность отправки в определенный момент особого сообщения, позволяющего начать процесс инициализации с устройством злоумышленника. Обе процедуры взлома достаточно сложны и включают несколько этапов, основной из которых – сбор пакетов данных и их анализ. Сами атаки основаны на уязвимостях в механизме аутентификации и создания ключа-шифра между двумя устройствами.

Принцип действия Bluetooth

Принцип действия основан на использовании радиоволн. Радиосвязь Bluetooth осуществляется в ISM-диапазоне (англ. Industry, Science and Medicine), который используется в различных бытовых приборах и беспроводных сетях (свободный от лицензирования диапазон 2,4–2,4835 ГГц). В Bluetooth применяется метод расширения спектра со скачкообразной перестройкой частоты (англ. Frequency Hopping Spread Spectrum, FHSS). Метод FHSS прост в реализации, обеспечивает устойчивость к широкополосным помехам, а оборудование недорогое.

Согласно алгоритму FHSS, в Bluetooth несущая частота сигнала скачкообразно меняется 1600 раз в секунду (всего выделяется 79 рабочих частот шириной в 1 МГц, а в Японии, Франции и Испании полоса у́же – 23 частотных канала). Последовательность переключения между частотами для каждого соединения является псевдослучайной и известна только передатчику и приемнику, которые каждые 625 мкс (один временной слот) синхронно перестраиваются с одной несущей частоты на другую. Таким образом, если рядом работают несколько пар «приемник-передатчик», то они не мешают друг другу. Этот алгоритм является также составной частью системы защиты конфиденциальности передаваемой информации: переход происходит по псевдослучайному алгоритму и определяется отдельно для каждого соединения. При передаче цифровых данных и аудиосигнала (64 Кбит/с в обоих направлениях) используются различные схемы кодирования: аудиосигнал не повторяется (как правило), а цифровые данные в случае утери пакета информации будут переданы повторно.

Протокол Bluetooth поддерживает не только соединение point-to-point, но и соединение point-to-multipoint.

1G

1G (или 1-G) – первое поколение беспроводных телефонных технологий и мобильных телекоммуникаций. Это аналоговые телекоммуникационные стандарты, которые были введены в 1980-х и в начале 1990-х были вытеснены более совершенной цифровой технологией 2G. Основным различием между системами 1G и 2G является то, что сети 1G используют аналоговую модуляцию радиосигналов, в то время как сети 2G являются цифровыми, что позволяет, среди прочего, шифровать разговоры и посылать СМС.

2G

2G (2-G) – аббревиатура для обозначения второго поколения беспроводной телефонной технологии.

Второе поколение сотовой связи 2G было запущено в коммерческую эксплуатацию по стандарту GSM в Финляндии компанией Radiolinja (сейчас является частью Elisa Oyj) в 1991 году. Основными преимуществами сетей 2G было то, что телефонные разговоры были зашифрованы с помощью цифрового шифрования; система 2G была значительно более эффективной; предоставила услуги передачи данных, начиная с текстовых сообщений СМС. Технология 2G позволила различным мобильным сетям предоставлять услуги, такие как текстовые сообщения, сообщения с изображениями и ММС (мультимедийные сообщения). Технология 2G достаточно безопасна как для отправителя, так и для получателя. Все текстовые сообщения зашифрованы в цифровой вид. Это цифровое шифрование передает данные таким образом, что только тот приемник, которому они предназначены, может получить их и прочитать.

После того как технология 2G была запущена, предыдущая технология была названа 1G. В то время как радиосигналы сети 1G являются аналоговыми, радиосигналы в сетях 2G являются цифровыми. Позднее 2G была заменена на новые технологии, такие как 2.50G, 2.750G, 3,6G и 4,20G, однако сеть 2G до сих пор используется во многих частях мира.

3G

3G (от англ. third generation «третье поколение»), технологии мобильной связи 3 поколения – набор услуг, который объединяет как высокоскоростной мобильный доступ с услугами сети Интернет, так и технологию радиосвязи, которая создает канал передачи данных. В настоящее время из-за массовых рекламных акций под этим термином чаще всего подразумевается технология UMTS с надстройкой HSPA.

В сетях 3G обеспечивается предоставление двух базовых услуг: передача данных и передача голоса. Согласно регламентам ITU (англ. International Telecommunications Union «Международный союз электросвязи») сети 3G должны поддерживать следующие скорости передачи данных:

- для абонентов с высокой мобильностью (до 120 км/ч) – не более 144 Кбит/с;
- для абонентов с низкой мобильностью (до 3 км/ч) – 384 Кбит/с;
- для неподвижных объектов – 2048 Кбит/с.

4G

4G (от англ. fourth generation «четвертое поколение») – поколение мобильной связи с повышенными требованиями. К четвертому поколению принято относить перспективные технологии, позволяющие осуществлять передачу данных со скоростью, превышающей 100 Мбит/с, – подвижным (с высокой мобильностью) и 1 Гбит/с – стационарным абонентам (с низкой мобильностью).

Технологии LTE Advanced (LTE-A) и WiMAX 2 (WMAN-Advanced, IEEE 802.16m) (сим-карта не требуется) были официально признаны беспроводными стандартами связи четвертого поколения 4G (IMT-Advanced) Международным союзом электросвязи на конференции в Женеве в 2012 году.

Спецификации любого поколения связи, как правило, содержат изменения фундаментального характера.

Новые поколения мобильной связи начинали разрабатываться практически через каждые десять лет с момента перехода от разработок первого поколения аналоговых сотовых сетей в 1970-х годах (1G) к сетям с цифровой передачей (2G) в 1980-х годах. От начала разработок до реального внедрения проходило достаточное количество времени (например, сети 1G были внедрены в 1984 году, сети 2G – в 1991 году). В 1990-х годах начал разрабатываться стандарт 3G, основанный на методе множественного доступа с кодовым разделением каналов (CDMA); он был внедрен только в 2000-х годах (в России – в 2002 году). Сети поколения 4G, основанные на IP-протоколе, стали разрабатываться в 2000 году и начали внедряться во многих странах с 2010 года.

В 2000 году, когда только шло освоение технологии связи третьего поколения 3G, один из ведущих производителей персональных компьютеров Hewlett-Packard и японский гигант сотовой связи NTT DoCoMo объявили о начале совместных исследований по разработке технологий передачи мультимедиаданных в беспроводных сетях четвертого поколения. Помимо них, разработки вели Ericsson и AT&T совместно с Nortel Networks. Впоследствии появилось два действительно пригодных к реализации стандарта: LTE и WiMAX, которые, по мнению IMT-Advanced, и стали новой эрой в развитии сетей

LTE

Стандарт LTE разрабатывался в рамках 3GPP (The 3rd Generation Partnership Project) как продолжение CDMA и UMTS и первоначально не относился к четвертому поколению мобильной связи. Международным союзом электросвязи как стандарт связи, отвечающий всем требованиям беспроводной связи четвертого поколения, был избран десятый релиз LTE – LTE Advanced, который впервые был представлен японской компанией NTT DoCoMo. Так как данный стандарт можно реализовать на существующих сотовых сетях, то он стал более популярен у операторов сотовой связи. В апреле 2008 года компания Nokia заручилась поддержкой ряда компаний (Sony Ericsson, NEC) для развития стандарта LTE и придания этому стандарту конкурентоспособности против WiMAX. В том же году аналитическая компания Analysys Mason спрогнозировала увеличение роста потребности сотовых технологий, таких как LTE.

Первая коммерческая сеть LTE была запущена 14 декабря 2009 года шведской телекоммуникационной компанией TeliaSonera совместно с Ericsson в Стокгольме и Осло.

WiMAX

Стандарт WiMAX (или IEEE 802.16) разрабатывается созданной в июне 2001 года организацией WiMAX Forum и является продолжением беспроводного стандарта Wi-Fi, альтернативой выделенным линиям связи и DSL. У стандарта WiMAX много версий, но преимущественно они подразделяются на фиксированный WiMAX (спецификация IEEE 802.16d, также известная как IEEE 802.16-2004, которая была утверждена в 2004 году) и мобильный WiMAX (спецификация IEEE 802.16e, более известная как IEEE 802.16-2005, которая была утверждена в 2005 году). По названиям стандартов ясно, что фиксированный WiMAX предоставляет услуги только «статичным» абонентам после установления и закрепления соответствующего оборудования, а мобильный WiMAX предоставляет возможность подключения пользователям, передвигающимся в зоне покрытия со скоростью до 115 км/час. Преимуществом стандарта WiMAX было то, что он гораздо раньше стандарта LTE стал пригоден к коммерческой эксплуатации. В настоящее время компаниями, составляющими WiMAX Forum, являются такие известные производители, как Intel Corporation, Samsung, Huawei Technologies, Hitachi и многие другие.

Первую сеть, основанную на технологии WiMAX, построила в Канаде компания Nortel 7 декабря 2005 года. Через два дня услуги беспроводного широкополосного доступа в сеть Интернет стала предоставлять украинская компания «Украинские новейшие технологии» (тем самым став первой в странах СНГ) на основе микросхем Intel® PRO/Wireless 5116.

Технология

В марте 2008 года сектор радиосвязи Международного союза электросвязи (ITU-R) определил ряд требований для стандарта международной подвижной беспроводной широкополосной связи 4G, получившего название спецификаций International Mobile Telecommunications Advanced (IMT-Advanced), в частности установив требования к скорости передачи данных для обслуживания абонентов: скорость 100 Мбит/с должна предоставляться высокоподвижным абонентам (например, поездам и автомобилям), а абонентам с небольшой подвижностью (например, пешеходам и фиксированным абонентам) должна предоставляться скорость 1 Гбит/с.

Так как первые версии мобильного WiMAX и LTE поддерживают скорости значительно меньше 1 Гбит/с, их нельзя назвать технологиями, соответствующими IMT-Advanced, хотя они часто упоминаются поставщиками услуг как технологии 4G. В свою очередь, после запуска мобильными операторами сетей LTE-Advanced в маркетинговых целях их стали называть 4G+. 6 декабря 2010 года МСЭ-Р признал, что наиболее продвинутые технологии рассматривают как «4G», хотя этот термин не определен.

Системы связи 4G основаны на пакетных протоколах передачи данных. Для пересылки данных используется протокол IPv4; в будущем планируется поддержка IPv6.

С технической точки зрения основное отличие сетей четвертого поколения от третьего заключается в том, что технология 4G полностью основана на протоколах пакетной передачи данных, в то время как 3G соединяет в себе как пакетную коммутацию, так и коммутацию каналов. Для передачи голоса в 4G предусмотрены технологии VoLTE (англ. Voice over LTE).

Основные исследования при создании систем связи четвертого поколения ведутся в направлении использования технологии ортогонального частотного уплотнения OFDM. Кроме того, для максимальной скорости передачи используется технология передачи данных с помощью N-антенн и их приема M-антеннами – MIMO. При данной технологии передающие и приемные антенны разнесены так, чтобы достичь слабой корреляции между соседними антеннами.

5G

5G (от англ. fifth generation «пятое поколение») – разрабатываемое пятое поколение мобильной связи, действующее на основе стандартов телекоммуникаций, следующих за существующими стандартами 4G/IMT-Advanced. В настоящее время стандартов для развертывания 5G-сетей не существует.

Предполагается, что технологии 5G будут обеспечивать более высокую пропускную способность по сравнению с технологиями 4G, что позволит обеспечить большую доступность широкополосной мобильной связи, а также использование режимов device-to-device (букв. «устройство с устройством»), сверхнадежные масштабные системы коммуникации между устройствами, а также более короткое время задержки, меньший расход энергии батареек, чем у 4G-оборудования, что благоприятно скажется на развитии интернета вещей.

Альянс мобильных сетей следующего поколения (NGMN) определяет следующие требования, которым должны соответствовать стандарты 5G:

- скорость передачи данных – десятки Мбит/с для десятков тысяч пользователей одновременно;
- скорость передачи данных 100 Мбит/с в условиях мегаполисов;
- скорость передачи данных 1 Гбит/с одновременно для многих пользователей на одном этаже;
- одновременное подключение нескольких сот тысяч беспроводных датчиков;
- более высокая спектральная эффективность по сравнению с 4G;
- улучшение охвата;
- повышение эффективности передачи сигнала;
- значительное снижение задержки по сравнению с LTE.

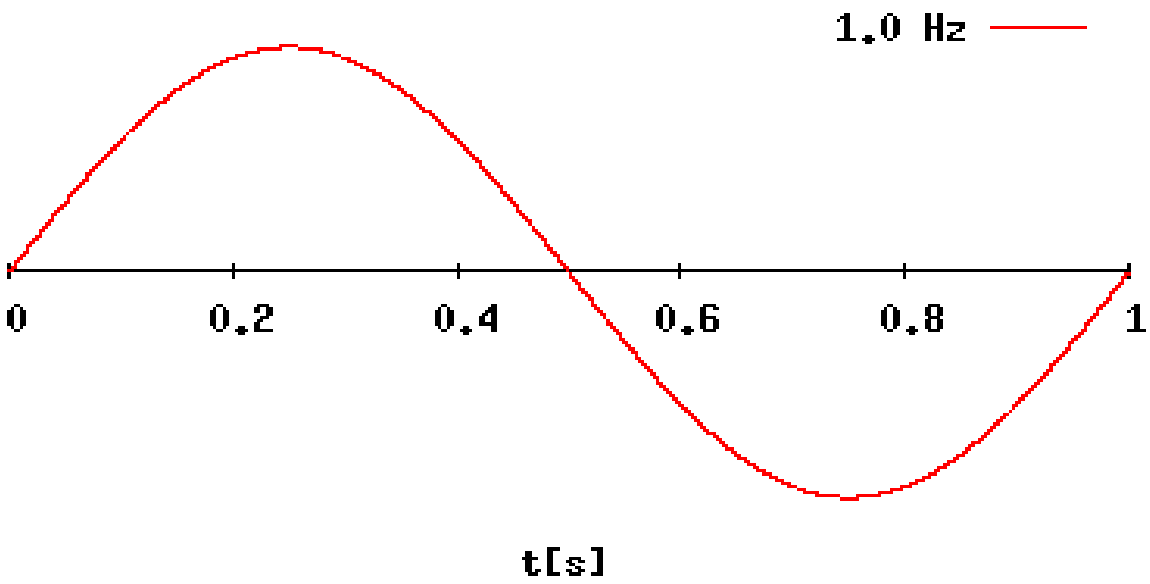
Предполагается, что наряду с перечисленными качественными характеристиками, 5G-сети создадут новые возможности для пользователей, такие как интернет вещей, а также широкополосные медиасервисы и связь в реальном времени в районах природных катастроф. Поскольку базовые станции и мобильные устройства потребуют для 5G-стандартов новых и более быстрых процессоров и программных приложений, ведущие производители носителей информации, чипмейкеры, такие как Advanced Semiconductor Engineering (ASE) и Amkor Technology, Inc., готовят производство соответствующей продукции.

Федеральная комиссия по связи США (FCC) в преддверии выхода на рынок 5G-технологий начала пересмотр действующих 4G-стандартов, утвержденных ITU-T. Так, своим решением 14 июля 2016 года FCC одобрила спектр частот для 5G, включающий частоты 28, 37 и 39 ГГц.

В опытных сетях скорость передачи данных доходит до 25 Гбит/с (4G), рекордная скорость передачи данных, которая составила 35 Гбит/с, была достигнута в России во время тестирования технологии 5G.

Математика и физика

Герц (русское обозначение: Гц, международное обозначение: Hz) – единица частоты периодических процессов (например, колебаний) в Международной системе единиц (СИ).



Децибел – это логарифмическая единица уровней, затуханий и усилений. Величина, выраженная в децибелах, численно равна десятичному логарифму безразмерного отношения физической величины к одноименной физической величине, принимаемой за исходную, умноженному на десятых

Формула: dB = 10 × log10 (P2/P1)

Изменение мощности	Значение в dB
/1000	-30 dB
/100	-20 dB
/10	-10 dB
/2	-3 dB
=	0 dB
x2	+3 dB
x10	+10 dB
x100	+20 dB
x1000	+30 dB

Основы Wi-Fi

Wi-Fi – торговая марка Wi-Fi Alliance для беспроводных компьютерных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «беспроводное качество» или «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

Любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

История

Wi-Fi был создан в 1998 году в лаборатории радиоастрономии CSIRO (Commonwealth Scientific and Industrial Research Organisation) в Канберре (Австралия). Создателем беспроводного протокола обмена данными является инженер Джон О'Салливан (John O'Sullivan).

Стандарт IEEE 802.11n был утвержден 11 сентября 2009 года. Его применение позволяет повысить скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с) при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с. С 2011 по 2013 год разрабатывался стандарт IEEE 802.11ac, стандарт был принят в январе 2014 года. Скорость передачи данных при использовании 802.11ac может достигать нескольких Гбит/с. Большинство ведущих производителей оборудования уже анонсировали устройства, поддерживающие данный стандарт.

27 июля 2011 года Институт инженеров электротехники и электроники (IEEE) выпустил официальную версию стандарта IEEE 802.22. Системы и устройства, поддерживающие этот

стандарт, позволяют принимать данные на скорости до 22 Мбит/с в радиусе 100 км от ближайшего передатчика.

Происхождение названия

Термин «Wi-Fi» изначально был придуман как игра слов для привлечения внимания потребителя с намеком на Hi-Fi (англ. High Fidelity «высокая точность»). Несмотря на то что поначалу в некоторых пресс-релизах WECA фигурировало словосочетание «Wireless Fidelity» («беспроводная точность»), на данный момент от такой формулировки отказались, и термин «Wi-Fi» никак не расшифровывается.

Принцип работы

Обычно схема Wi-Fi-сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме «точка-точка» (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров напрямую. Точка доступа передает свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с – наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приемник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi дает клиенту полную свободу при выборе критериев для соединения. Более подробно принцип работы описан в официальном тексте стандарта.

Однако стандарт не описывает всех аспектов построения беспроводных локальных сетей Wi-Fi. Поэтому каждый производитель оборудования решает эту задачу по-своему, применяя те подходы, которые он считает наилучшими с той или иной точки зрения. Поэтому возникает необходимость классификации способов построения беспроводных локальных сетей.

По способу объединения точек доступа в единую систему можно выделить:

- автономные точки доступа (называются также самостоятельными, децентрализованными, умными);
- точки доступа, работающие под управлением контроллера (называются также «легковесными», централизованными);
- бесконтроллерные, но не автономные (управляемые без контроллера).

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

- со статическими настройками радиоканалов;
- с динамическими (адаптивными) настройками радиоканалов;
- со «слоистой» или многослойной структурой радиоканалов.

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.

Пользователям более известен по названию «Wi-Fi», фактически являющемуся брендом, предложенным и продвигаемым организацией Wi-Fi Alliance. Получил широкое распространение благодаря развитию мобильных электронно-вычислительных устройств: КПК и ноутбуков.

История

Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости не более 1 Мбит/с и опционально на скорости 2 Мбит/с. Один из первых высокоскоростных стандартов беспроводных сетей – IEEE 802.11a – определяет скорость передачи уже до 54 Мбит/с брутто. Рабочий диапазон стандарта – 5 ГГц.

Вопреки своему названию, принятый в 1999 году стандарт IEEE 802.11b не является продолжением стандарта 802.11a, поскольку в них используются различные технологии: DSSS (точнее, его улучшенная версия HR-DSSS) в 802.11b против OFDM в 802.11a. Стандарт предусматривает использование нелицензируемого диапазона частот 2,4 ГГц. Скорость передачи – до 11 Мбит/с.

Продукты стандарта IEEE 802.11b, поставляемые разными изготовителями, тестируются на совместимость и сертифицируются организацией Wireless Ethernet Compatibility Alliance (WECA), которая в настоящее время больше известна под названием «Wi-Fi Alliance». Совместимые беспроводные продукты, прошедшие испытания по программе «Альянса Wi-Fi», могут быть маркированы знаком Wi-Fi.

Долгое время IEEE 802.11b был распространенным стандартом, на базе которого было построено большинство беспроводных локальных сетей. Сейчас его место занял стандарт IEEE 802.11g, постепенно вытесняемый высокоскоростным IEEE 802.11n.

Проект стандарта IEEE 802.11g был утвержден в октябре 2002 года. Этот стандарт предусматривает использование диапазона частот 2,4 ГГц, обеспечивая скорость соединения до 54 Мбит/с брутто и превосходя, таким образом, стандарт IEEE 802.11b, который обеспечивает скорость соединения до 11 Мбит/с. Кроме того, он гарантирует обратную совместимость со стандартом 802.11b. Обратная совместимость стандарта IEEE 802.11g может быть реализована в режиме модуляции DSSS, и тогда скорость соединения будет ограничена одиннадцатью мегабитами в секунду, либо в режиме модуляции OFDM, при котором скорость может достигать 54 Мбит/с. Таким образом, данный стандарт является наиболее приемлемым при построении беспроводных сетей.

Список стандартов

При описании стандарта в скобках указан год его принятия.

- 802.11 – изначальный 1 Мбит/с и 2 Мбит/с, 2,4 ГГц и ИК-стандарт (1997).
- 802.11a – 54 Мбит/с, 5 ГГц стандарт (1999, выход продуктов – в 2001 году).
- 802.11b – улучшения к 802.11 для поддержки 5,5 и 11 Мбит/с (1999).
- 802.11c – процедуры операций с мостами; включен в стандарт IEEE 802.1D (2001).
- 802.11d – интернациональные роуминговые расширения (2001).
- 802.11e – улучшения: QoS, пакетный режим (packet bursting) (2005).
- 802.11F – Inter-Access Point Protocol (2003). Рекомендация, а не стандарт, поэтому используется заглавная буква.
- 802.11g – 54 Мбит/с, 2,4 ГГц стандарт (обратная совместимость с b) (2003).
- 802.11h – распределенный по спектру 802.11a (5 GHz) для совместимости в Европе (2004).
- 802.11i – улучшенная безопасность (2004).
- 802.11j – расширения для Японии (2004).
- 802.11k – улучшение измерения радиоресурсов.
- 802.11l – зарезервирован.

- 802.11m – поправки и исправления для всей группы стандартов 802.11.
- 802.11n – увеличение скорости передачи данных (600 Мбит/с). 2,4–2,5 или 5 ГГц. Обратная совместимость с 802.11a/b/g (сентябрь 2009 года).
- 802.11o – зарезервирован.
- 802.11p – WAVE – Wireless Access for the Vehicular Environment (беспроводной доступ для среды транспортного средства).
- 802.11q – зарезервирован, иногда его путают с 802.1Q.
- 802.11r – быстрый роуминг.
- 802.11s – ESS Wireless mesh network (Extended Service Set – расширенный набор служб; Mesh Network – многосвязная сеть).
- 802.11T – Wireless Performance Prediction (WPP, предсказание производительности беспроводного оборудования) – методы тестов и измерений. Рекомендация, а не стандарт, поэтому используется заглавная буква.
- 802.11u – взаимодействие с не-802-сетями (например, сотовыми).
- 802.11v – управление беспроводными сетями.
- 802.11w – Protected Management Frames (защищенные управляющие фреймы).
- 802.11x – зарезервирован и не будет использоваться. Не нужно путать со стандартом контроля доступа IEEE 802.1X.
- 802.11y – дополнительный стандарт связи, работающий на частотах 3,65–3,70 ГГц. Обеспечивает скорость до 54 Мбит/с на расстоянии до 5000 м на открытом пространстве.
- 802.11ac – новый стандарт IEEE. Скорость передачи данных – до 6,77 Гбит/с для устройств, имеющих 8 антенн. Утвержден в январе 2014 года.
- 802.11ad – новый стандарт с дополнительным диапазоном 60 ГГц (частота не требует лицензирования). Скорость передачи данных – до 7 Гбит/с.

Актуальные стандарты

Наиболее актуальными в наше время являются стандарты 802.11n и 802.11ac.

802.11b/g/n			
Канал	**Центральная частота[1], ГГц**	**Канал**	**Центральная частота[1], ГГц**
1	2,412	8	2,447
2	2,417	9	2,452
3	2,422	10	2,457
4	2,427	11	2,462
5	2,432	12	2,467
6	2,437	13	2,47
7	2,442	14	2,484

802.11a/n/ac					
Канал	**Частота, ГГц**	**Канал**	**Частота, ГГц**	**Канал**	**Частота, ГГц**
34	5,170	104	5,520	153	5,765
36	5,180	108	5,540	155	5,775
38	5,190	112	5,560	157	5,785
40	5,200	116	5,580	159	5,795
42	5,210	120	5,600	161	5,805
44	5,220	124	5,620	163	5,815
46	5,230	128	5,640	165	5,825
48	5,240	132	5,660	167	5,835
52	5,260	136	5,680	171	5,855
56	5,280	140	5,700	173	5,865
60	5,300	147	5,735	177	5,885
64	5,320	149	5,745	180	5,905
100	5,500	151	5,755		

Сравнение 2,4 и 5 ГГц

2,4 ГГц	**5 ГГц**
Более распространено	Больше каналов
Сигнал распространяется на большие дистанции	Менее загружено
Частоты не требуют разрешения или регистрации	Некоторые частоты требуют либо регистрации, либо разрешения

SSID и BSSID

SSID (Service Set Identifier) – имя сети.

BSSID (Basic Service Set Identifier) – MAC-адрес точки доступа.

Методы аутентификации

Открытая аутентификация (англ. Open Authentication)

Рабочая станция делает запрос аутентификации, в котором присутствует только MAC-адрес клиента. Точка доступа отвечает либо отказом, либо подтверждением аутентификации. Решение принимается на основе MAC-фильтрации, то есть по сути это защита беспроводной Wi-Fi-сети на основе ограничения доступа, что небезопасно.

Используемые шифры: без шифрования, статический WEP, CKIP.

Аутентификация с общим ключом (англ. Shared Key Authentication)

Необходимо настроить статический ключ шифрования алгоритма WEP (англ. Wired Equivalent Privacy). Клиент делает запрос у точки доступа на аутентификацию, на что получает подтверждение, которое содержит 128 байт случайной информации. Станция шифрует полученные данные алгоритмом WEP (проводится побитовое сложение по модулю 2 данных сообщения с последовательностью ключа) и отправляет зашифрованный текст вместе с запросом на ассоциацию. Точка доступа расшифровывает текст и сравнивает с исходными данными. В случае совпадения отсылается подтверждение ассоциации, и клиент считается подключенным к сети.

Схема аутентификации с общим ключом уязвима к атакам Man in the middle. Алгоритм шифрования WEP – это простой XOR ключевой последовательности с полезной информацией, следовательно, прослушав трафик между станцией и точкой доступа, можно восстановить часть ключа.

Используемые шифры: без шифрования, динамический WEP, CKIP.

Аутентификация по MAC-адресу

Данный метод не предусмотрен в IEEE 802.11, но поддерживается большинством производителей оборудования, например D-Link и Cisco. Происходит сравнение MAC-адреса клиента с таблицей разрешенных MAC-адресов, хранящейся на точке доступа, либо используется внешний сервер аутентификации. Используется как дополнительная мера защиты.

IEEE начал разработку нового стандарта IEEE 802.11i, но из-за трудностей утверждения организация WECA (англ. Wi-Fi Alliance) совместно с IEEE анонсировала стандарт WPA (Wi-Fi Protected Access). В WPA используется TKIP (англ. Temporal Key Integrity Protocol «протокол проверки целостности ключа»), который использует усовершенствованный способ управления ключами и покадровое изменение ключа.

Wi-Fi Protected Access (WPA)

После первых успешных атак на WEP было принято решение разработать новый стандарт 801.11i. Но до него был выпущен «промежуточный» стандарт WPA, который включал в себя новую систему аутентификации на базе 801.1x и новый метод шифрования TKIP. Существуют два варианта аутентификации: с помощью RADIUS-сервера (WPA-Enterprise) и с помощью предустановленного ключа (WPA-PSK).

Используемые шифры: TKIP (стандарт), AES-CCMP (расширение), WEP (в качестве обратной совместимости).

WI-FI Protected Access2 (WPA2, 801.11I)

WPA2, или стандарт 801.11i, – это финальный вариант стандарта безопасности беспроводных сетей. В качестве основного шифра был выбран стойкий блочный шифр AES. Система аутентификации по сравнению с WPA претерпела минимальные изменения. Так же, как и в WPA, в WPA2 есть два варианта аутентификации: WPA2-Enterprise с аутентификацией на RADIUS-сервере и WPA2-PSK с предустановленным ключом.

Используемые шифры: AES-CCMP (стандарт), TKIP (в качестве обратной совместимости).

Методы шифрования

WEP-шифрование (Wired Equivalent Privacy)

Аналог шифрования трафика в проводных сетях. Используется симметричный потоковый шифр RC4 (англ. Rivest Cipher 4), который достаточно быстро функционирует. На сегодняшний день WEP и RC4 не считаются криптостойкими. Есть два основных протокола WEP:

- 40-битный WEP (длина ключа 64 бита, 24 из которых – это вектор инициализации, который передается открытым текстом);
- 104-битный WEP (длина ключа 128 бит, 24 из которых – это тоже вектор инициализации); вектор инициализации используется алгоритмом RC4. Увеличение длины ключа не приводит к увеличению надежности алгоритма.

Основные недостатки:

- использование для шифрования непосредственно пароля, введенного пользователем;
- недостаточная длина ключа шифрования;
- использование функции CRC32 для контроля целостности пакетов;
- повторное использование векторов инициализации и др.

TKIP-шифрование (англ. Temporal Key Integrity Protocol)

Используется тот же симметричный потоковый шифр RC4, но само TKIP-шифрование является более криптостойким. Вектор инициализации составляет 48 бит. Учтены основные атаки на WEP. Используется протокол Message Integrity Check для проверки целостности сообщений, который блокирует станцию на 60 секунд, если в течение 60 секунд были посланы два сообщения, не прошедшие проверку целостности. С учетом всех доработок и усовершенствований TKIP все равно не считается криптостойким.

CKIP-шифрование (англ. Cisco Key Integrity Protocol)

Имеет сходство с протоколом TKIP. CKIP создан компанией Cisco. Используется протокол CMIC (англ. Cisco Message Integrity Check) для проверки целостности сообщений.

WPA

Стандарт WPA вместо уязвимого RC4 используется криптостойкий алгоритм шифрования AES (англ. Advanced Encryption Standard). Возможно использование EAP (англ. Extensible Authentication Protocol «расширяемый протокол аутентификации»). Есть два режима:

- Pre-Shared Key (WPA-PSK) – каждый узел вводит пароль для доступа к сети;
- Enterprise – проверка осуществляется серверами RADIUS.

WPA2 (IEEE 802.11i)

Стандарт принят в 2004 году, с 2006 года WPA2 должно поддерживать все выпускаемое Wi-Fi-оборудование. В данном стандарте применяется RSN (англ. Robust Security Network «сеть с повышенной безопасностью»). Изначально в WPA2 используется протокол CCMP (англ. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol «протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счетчика»). Основой является алгоритм AES. Для совместимости со старым оборудованием имеется поддержка TKIP и EAP (англ. Extensible Authentication Protocol) с некоторыми его дополнениями. Как и в WPA, есть два режима работы: Pre-Shared Key и Enterprise.

WPA и WPA2 имеют следующие преимущества:

- ключи шифрования генерируются во время соединения, а не распределяются статически;
- для контроля целостности передаваемых сообщений используется алгоритм Michael;
- используется вектор инициализации существенно большей длины.

WPS

Wi-Fi Protected Setup (защищенная установка), WPS – стандарт (и одноименный протокол) полуавтоматического создания беспроводной сети Wi-Fi, созданный Wi-Fi Alliance. Официально запущен 8 января 2007 года.

Целью протокола WPS является упрощение процесса настройки беспроводной сети, поэтому изначально он назывался Wi-Fi Simple Config. Протокол призван оказать помощь пользователям, которые не обладают широкими знаниями о безопасности в беспроводных сетях и, как следствие, имеют сложности при осуществлении настроек. WPS автоматически обозначает имя сети и задает шифрование для защиты беспроводной Wi-Fi-сети от несанкционированного доступа, при этом нет необходимости вручную задавать все параметры.

Есть два типа WPS: WPS с пин-кодом из 8 цифр (на клиенте нужно ввести тот же код, что и на точке доступа) и кнопка WPS (нужно нажать кнопку на точке доступа и на клиенте с интервалом меньше двух минут, тогда они соединятся друг с другом).

В декабре 2011 года Стефан Фибек (англ. Stefan Viehböck) и Крейг Хеффнер (англ. Craig Heffner) рассказали о серьезных прорехах в протоколе WPS. Оказалось, что если в точке доступа активирован WPS с PIN (который по умолчанию включен в большинстве роутеров), то подобрать PIN-код для подключения можно за считаные часы.

PIN-код состоит из восьми цифр – следовательно, существует 10^8 (100 000 000) вариантов PIN-кода для подбора. Однако количество вариантов можно существенно сократить. Дело в том, что последняя цифра PIN-кода представляет собой контрольную сумму, которую можно вычислить на основании первых семи цифр. Таким образом, количество вариантов уже сокращается до 10^7 (10 000 000).

Авторизация по WPS предполагает отправку клиентом последовательности цифр PIN-кода и пакетов M4 или M6 и ответы на них от базовой станции. Если первые 4 цифры PIN-кода некорректны, то, получив их, точка доступа отправит EAP-NACK сразу после получения M4, а если была ошибка в последних трех цифрах правой части (8-е число не считаем, так как оно легко генерируется атакующим по формуле) – то после получения M6. Таким образом, недостаток протокола позволяет разделить PIN-код на две части, четыре начальные цифры и

три последующие, и проверять каждую часть на корректность отдельно, используя базовую станцию как оракула, который подсказывает, правильная ли последовательность цифр была отправлена.

Если PIN-код разбить на две части, то получается 10^4 (10 000) вариантов для первой половины и 10^3 (1000) для второй. В итоге это составляет всего лишь 11 000 вариантов для полного перебора, что в более чем 9000 раз меньше исходного числа вариантов (10^8).

Таким образом, вместо одного большого пространства значений 10^7 мы получаем два – по 10^4 и 10^3, – и понятно, что $10^7 < > 10^4 + 10^3$. В итоге достаточно протестировать 11 000 комбинаций (больше четырех цифр на тысячу) вместо 10 000 000.

Также были обнаружены уязвимости в ГСЧ маршрутизаторов некоторых производителей. Уязвимость получила название «pixie dust». Для уязвимых роутеров можно получить pin после первой попытки и офлайн-брутфорса. Защититься от атаки можно пока одним способом – отключить WPS с пином в настройках роутера. Правда, сделать это возможно далеко не всегда, иногда WPS отключается только полностью. Самое большее, что могут сделать производители, – выпустить прошивку, позволяющую вводить тайм-аут на блокировку функции, например, после 5 неудачных попыток ввода PIN-кода, что усложнит брутфорс и увеличит время подбора идентификатора злоумышленником.

Государственное регулирование в сфере радиочастот в РФ

Постановление Правительства РФ от 12.10.2004 № 539 (ред. от 14.12.2017) «О порядке регистрации радиоэлектронных средств и высокочастотных устройств» (с изм. и доп., вступ. в силу с 01.09.2018): http://www.consultant.ru/document/cons_doc_LAW_49884/.

Wi-Fi 802.11n и 802.11ac

Стандарты Wi-Fi 802.11n и 802.11ac являются наиболее распространенными в наше время.

Wi-Fi 802.11n

Стандарт был утвержден 11 сентября 2009 года. Стандарт 802.11n повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с) при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с брутто, применяя передачу данных сразу по четырем антеннам. По одной антенне – до 150 Мбит/с.

Устройства 802.11n работают в диапазонах 2,4 или 5,0 ГГц.

Кроме того, устройства 802.11n могут работать в трех режимах:

- наследуемом (Legacy), в котором обеспечивается поддержка устройств 802.11b/g и 802.11a;
- смешанном (Mixed), в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n;
- «чистом» режиме – 802.11n (именно в этом режиме и можно воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n).

Черновую версию стандарта 802.11n (DRAFT 2.0) поддерживают многие современные сетевые устройства. Итоговая версия стандарта (DRAFT 11.0), которая была принята 11 сентября

2009 года, обеспечивает скорость до 300 Мбит/с, многоканальный вход/выход, известный как MIMO, и большее покрытие.

Нововведения в 802.11n:

- увеличение ширины канала до 40 МГц вместо 20 МГц. В диапазоне 2,4 ГГц можно разместить только два непересекающихся широкополосных канала;
- поддержка MIMO (Multiple-Input Multiple-Output – много входов, много выходов). Обозначения MIMO 4×4, 3×3, 2×2 или 1×1 (SISO – Single-Input Single-Output – один вход, один выход).

MIMO (англ. Multiple Input Multiple Output) – метод пространственного кодирования сигнала, позволяющий увеличить полосу пропускания канала, в котором передача данных и прием данных осуществляются системами из нескольких антенн. Передающие и приемные антенны разносят так, чтобы корреляция между соседними антеннами была слабой.

Стандарт сетевого питания IEEE 802.3af-2003 (PoE) не обеспечивает мощности, необходимой для электроснабжения точек доступа с антенными конфигурациями 3×3 и выше. Ему на смену пришел стандарт IEEE 802.3at-2009, предусматривающий увеличение максимальной мощности в два раза, что достаточно для питания устройств с конфигурацией антенн 4×4.

С учетом того, что у точек доступа, поддерживающих данный стандарт, пропускная способность может превысить 100 Мбит/с, каналы Fast Ethernet вполне могут стать узким местом на пути сетевого трафика. Поэтому при разворачивании беспроводной сети желательно использовать коммутаторы Gigabit Ethernet.

802.11ac

IEEE 802.11ac – стандарт беспроводных локальных сетей, работающий в диапазоне частот 5 ГГц. Обратно совместим с IEEE 802.11n.

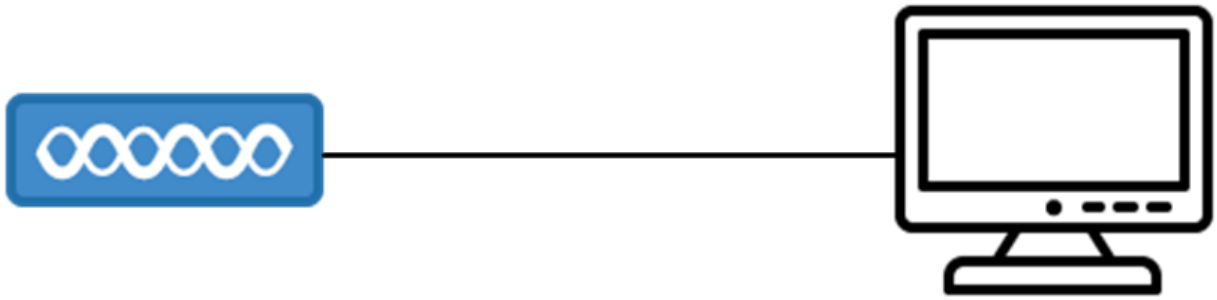
Стандарт позволяет существенно расширить пропускную способность сети, начиная от 433 Мбит/с (устройства с 433 Мбит/с на канал уже были доступны летом 2014 года) и заканчивая 6,77 Гбит/с при 8x MU-MIMO-антеннах. Это наиболее существенное нововведение относительно IEEE 802.11n. Кроме того, ожидается снижение энергопотребления (Дж/бит), что, в свою очередь, продлит время автономной работы мобильных устройств.

Нововведения по сравнению с 802.11n:

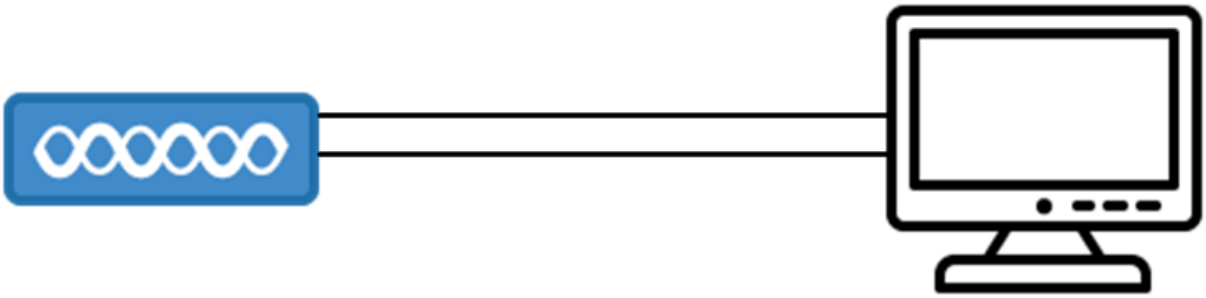
- увеличение ширины канала до 80 МГц вместо 40 МГц (опционально возможно увеличение ширины канала до 160 МГц);
- увеличение числа пространственных потоков до 8 вместо 4;
- использование новой и более эффективной модуляции сигнала 256-QAM;
- использование MU-MIMO (Multi-User MIMO – многопользовательская MIMO);
- поддержка технологии формирования направленного сигнала Beamforming.

Сравнение SISO, MIMO и MU-MIMO

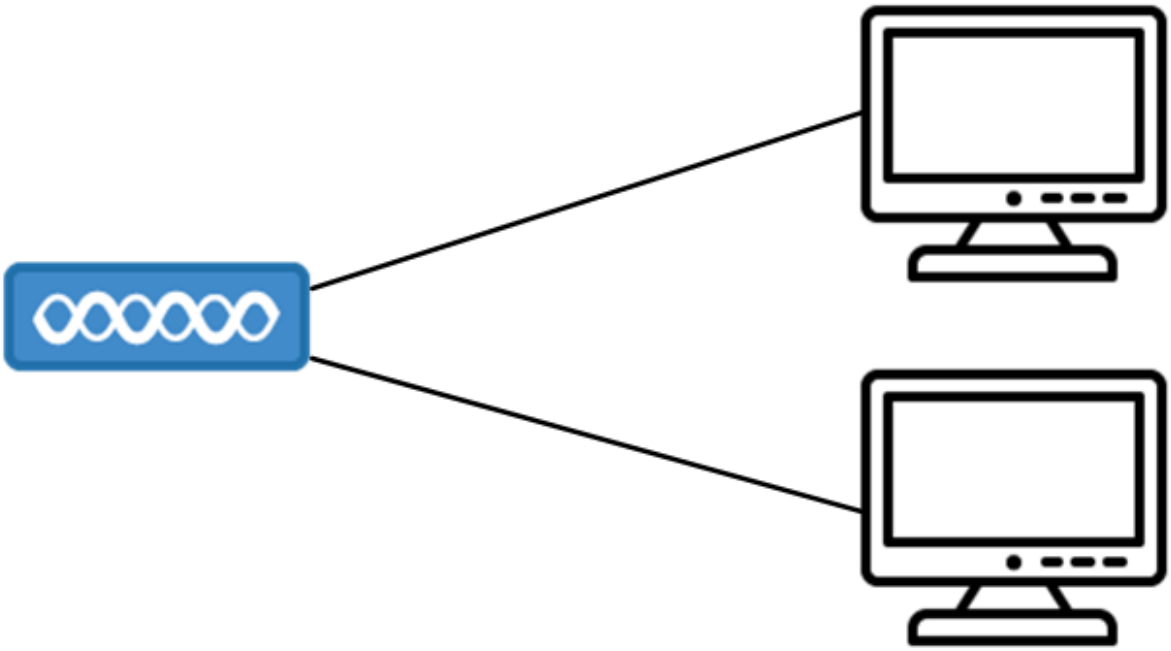
SISO



MIMO



MU-MIMO



Антенны

Антенна – устройство, предназначенное для излучения или приема радиоволн.

Антенны в зависимости от назначения подразделяются на приемные, передающие и приемо-передающие. Антенна в режиме передачи преобразует энергию поступающего от радиопередатчика электромагнитного колебания в распространяющуюся в пространстве электромагнитную волну. Антенна в режиме приема преобразует энергию падающей на антенну электромагнитной волны в электромагнитное колебание, поступающее в радиоприемник. Таким образом, антенна является преобразователем подводимого к ней по фидеру электромагнитного колебания (переменного электрического тока, канализированной в волноводе электромагнитной волны) в электромагнитное излучение и наоборот.

Первые антенны были созданы в 1888 году Генрихом Герцем в ходе его экспериментов по доказательству существования электромагнитной волны (вибратор Герца). Форма, размеры и конструкция созданных впоследствии антенн чрезвычайно разнообразны и зависят от рабочей длины волны и назначения антенны. Нашли широкое применение антенны, выполненные в виде отрезка провода, системы проводников, металлического рупора, металлических и диэлектрических волноводов, волноводов с металлическими стенками с системой прорезанных щелей, а также многие другие типы. Для улучшения направленных свойств первичный излучатель может снабжаться рефлекторами – отражающими элементами различной конфигурации или их системами, а также линзами.

Единица измерения коэффициента усиления антенны – изотропный децибел (дБи, dBi).

Виды антенн

- Изотропная антенна – воображаемая (идеальная) антенна, излучающая по всем направлениям электромагнитную энергию одинаковой интенсивности. Диаграмма направленности изотропного излучателя – круговая во всех сечениях, в частности по векторам E и H. Изотропный излучатель излучает без потерь, то есть его КПД равен 100 %.
- Всенаправленная (Omni) антенна покрывает территорию во всем радиусе действия. Обычно это штырь, который стоит вертикально и распространяет сигнал в плоскости, которая перпендикулярна своей оси.
- Направленная (Directional) антенна предназначена для связи «точка-точка» или «точка-многоточка». Направленные антенны принято делить на секторные, антенны типа «волновой канал», параболические и сегментно-параболические антенны, панельные антенны и прочие.

Wi-Fi в жизни

В реальной жизни для стабильной работы беспроводной сети необходимо учитывать множество факторов, среди которых:

- возможные помехи от соседей;
- наложение разных сигналов;
- отражение сигналов;
- помехи на пути;
- переключение при переходе от точки к точке;
- количество одновременно подключенных устройств;

Также очень полезно понимать, что означают следующие величины: мощность передатчика, коэффициент усиления антенны, затухание сигнала и др.

Брандмауэр

Виды брандмауэров

Термины «файрвол», «брандмауэр» и «межсетевой экран» обозначают одно и то же.

Файрвол – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Брандмауэр (нем. Brandmauer от Brand «пожар» и Mauer «стена») – глухая противопожарная стена здания, выполняемая из несгораемых материалов и предназначенная для воспрепятствования распространению огня на здания или соседние части здания.

Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.

Наиболее распространенное место для установки межсетевых экранов – граница периметра локальной сети для защиты внутренних хостов от атак извне. Однако атаки могут начинаться и с внутренних узлов – в этом случае, если атакуемый хост расположен в той же сети, трафик не пересечет границу сетевого периметра, и межсетевой экран не будет задействован. Поэтому в настоящее время межсетевые экраны размещают не только на границе, но и между различными сегментами сети, что обеспечивает дополнительный уровень безопасности

Первые устройства, выполняющие функцию фильтрации сетевого трафика, появились в конце 1980-х, когда Интернет был новшеством и не использовался в глобальных масштабах. Этими устройствами были маршрутизаторы, инспектирующие трафик на основании данных, содержащихся в заголовках протоколов сетевого уровня. Впоследствии, с развитием сетевых технологий, данные устройства получили возможность выполнять фильтрацию трафика, используя данные протоколов более высокого, транспортного уровня. Маршрутизаторы можно считать первой программно-аппаратной реализацией межсетевого экрана.

Программные межсетевые экраны появились существенно позже и были гораздо моложе, чем антивирусные программы. Например, проект Netfilter/iptables (один из первых программных межсетевых экранов, встраиваемых в ядро Linux с версии 2.4) был основан в 1998 году. Такое позднее появление вполне объяснимо, так как долгое время антивирус решал проблему защиты персональных компьютеров от вредоносных программ. Однако в конце 1990-х вирусы стали активно использовать отсутствие межсетевых экранов на компьютерах, что привело к повышению интереса пользователей к данному классу устройств.

Фильтрация трафика осуществляется на основе набора предварительно сконфигурированных правил. Удобно представлять межсетевой экран как последовательность фильтров, обрабатывающих информационный поток. Каждый из фильтров предназначен для интерпретации отдельного правила. Последовательность правил в наборе существенно влияет на производительность межсетевого экрана. Например, многие межсетевые экраны последовательно сравнивают трафик с правилами до тех пор, пока не будет найдено соответствие. Для таких межсетевых экранов правила, которые соответствуют наибольшему

количеству трафика, следует располагать как можно выше в списке, увеличивая тем самым производительность.

Классификация межсетевых экранов

До сих пор не существует единой и общепризнанной классификации межсетевых экранов. Однако в большинстве случаев поддерживаемый уровень сетевой модели OSI является основной характеристикой при их классификации. Учитывая данную модель, различают следующие типы межсетевых экранов:

- управляемые коммутаторы;
- пакетные фильтры;
- шлюзы сеансового уровня;
- посредники прикладного уровня;
- инспекторы состояния.

Управляемые коммутаторы

Управляемые коммутаторы иногда причисляют к классу межсетевых экранов, так как они осуществляют фильтрацию трафика между сетями или узлами сети. Однако они работают на канальном уровне и разделяют трафик в рамках локальной сети, а значит, не могут быть использованы для обработки трафика из внешних сетей (например, из Интернета).

Многие производители сетевого оборудования, такие как Cisco, Nortel, ZyXEL, предоставляют в своих коммутаторах возможность фильтрации трафика на основе MAC-адресов, содержащихся в заголовках фреймов. Например, в коммутаторах семейства Cisco Catalyst эта возможность реализована при помощи механизма Port Security. Однако данный метод фильтрации не является эффективным, так как аппаратно установленный в сетевой карте MAC-адрес легко меняется программным путем, поскольку значение, указанное через драйвер, имеет более высокий приоритет, чем зашитое в плату. Поэтому многие современные коммутаторы позволяют использовать другие параметры в качестве признака фильтрации – например, VLAN ID. Технология виртуальных локальных сетей (англ. Virtual Local Area Network) позволяет создавать группы хостов, трафик которых полностью изолирован от других узлов сети.

При реализации политики безопасности в рамках корпоративной сети, основу которой составляют управляемые коммутаторы, они могут быть мощным и достаточно дешевым решением. Взаимодействуя только с протоколами канального уровня, такие межсетевые экраны фильтруют трафик с очень высокой скоростью. Основным недостатком такого решения является невозможность анализа протоколов более высоких уровней.

Пакетные фильтры

Пакетные фильтры функционируют на сетевом уровне и контролируют прохождение трафика на основе информации.

Шлюзы сеансового уровня

Межсетевой экран сеансового уровня исключает прямое взаимодействие внешних хостов с узлом, расположенным в локальной сети, выступая в качестве посредника (англ. proxy), который реагирует на все входящие пакеты и проверяет их допустимость на основании текущей фазы соединения. Шлюз сеансового уровня гарантирует, что ни один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению. Как только приходит запрос на установление соединения, в специальную таблицу помещается соответствующая информация (адреса отправителя и получателя, используемые протоколы сетевого и транспортного уровня, состояние соединения и т.д.). В случае если соединение установлено, пакеты, передаваемые в рамках данной сессии, будут просто копироваться в локальную сеть без дополнительной фильтрации. Когда сеанс связи завершается, сведения о нем удаляются из данной таблицы. Поэтому все последующие пакеты, «притворяющиеся» пакетами уже завершенного соединения, отбрасываются.

Так как межсетевой экран данного типа исключает прямое взаимодействие между двумя узлами, шлюз сеансового уровня является единственным связующим элементом между внешней сетью и внутренними ресурсами. Это создает видимость того, что на все запросы из внешней сети отвечает шлюз, и делает практически невозможным определение топологии защищаемой сети. Кроме того, так как контакт между узлами устанавливается только при условии его допустимости, шлюз сеансового уровня предотвращает возможность реализации DoS-атаки, присущей пакетным фильтрам.

Несмотря на эффективность этой технологии, она обладает серьезным недостатком: как и у всех вышеперечисленных классов межсетевых экранов, у шлюзов сеансового уровня отсутствует возможность проверки содержания поля данных, что позволяет злоумышленнику передавать «троянских коней» в защищаемую сеть.

Посредники прикладного уровня

Межсетевые экраны прикладного уровня, так же как и шлюзы сеансового уровня, исключают прямое взаимодействие двух узлов. Однако, функционируя на прикладном уровне, они способны «понимать» контекст передаваемого трафика. Межсетевые экраны, реализующие эту технологию, содержат несколько приложений-посредников (англ. application proxy), каждое из которых обслуживает свой прикладной протокол. Такой межсетевой экран способен выявлять в передаваемых сообщениях и блокировать несуществующие или нежелательные последовательности команд, которые зачастую означают DoS-атаку, либо запрещать использование некоторых команд (например, FTP PUT, которая дает возможность пользователю записывать информацию на FTP-сервер).

Посредник прикладного уровня может определять тип передаваемой информации. Например, это позволяет заблокировать почтовое сообщение, содержащее исполняемый файл. Другой возможностью межсетевого экрана данного типа является проверка аргументов входных данных. Например, аргумент имени пользователя длиной в 100 символов либо содержащий бинарные данные является по крайней мере подозрительным.

Посредники прикладного уровня способны выполнять аутентификацию пользователя, а также проверять, что SSL-сертификаты подписаны конкретным центром. Межсетевые экраны прикладного уровня доступны для многих протоколов, включая HTTP, FTP, почтовые (SMTP, POP, IMAP), Telnet и другие.

Недостатком данного типа межсетевых экранов являются большие затраты времени и ресурсов на анализ каждого пакета. По этой причине они обычно не подходят для приложений реального времени. Другим недостатком является невозможность автоматического подключения поддержки новых сетевых приложений и протоколов, так как для каждого из них необходим свой агент.

Инспекторы состояния

Каждый из вышеперечисленных типов межсетевых экранов используется для защиты корпоративных сетей и обладает рядом преимуществ. Однако куда эффективней было бы собрать все эти преимущества в одном устройстве и получить межсетевой экран, осуществляющий фильтрацию трафика с сетевого по прикладной уровень. Данная идея была реализована в инспекторах состояний, совмещающих в себе высокую производительность и защищенность. Данный класс межсетевых экранов позволяет контролировать:

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

Осуществляя фильтрацию трафика по принципу шлюза сеансового уровня, данный класс межсетевых экранов не вмешивается в процесс установления соединения между узлами. Поэтому производительность инспектора состояний заметно выше, чем у посредника прикладного уровня и шлюза сеансового уровня, и сравнима с производительностью пакетных фильтров. Еще одно достоинство инспекторов состояния – прозрачность для пользователя: для клиентского программного обеспечения не потребуется дополнительная настройка. Данные межсетевые экраны имеют большие возможности расширения. При появлении новой службы или нового протокола прикладного уровня для его поддержки достаточно добавить несколько шаблонов. Однако инспекторам состояний по сравнению с посредниками прикладного уровня свойственна более низкая защищенность.

Термин «инспектор состояния» (англ. stateful inspection), внедренный компанией Check Point Software, полюбился производителям сетевого оборудования настолько, что сейчас практически каждый межсетевой экран причисляют к этой технологии, даже если он и не реализует ее полностью.

Реализация

Существует два варианта исполнения межсетевых экранов – программный и программно-аппаратный. В свою очередь, программно-аппаратный вариант имеет две разновидности: в виде отдельного модуля в коммутаторе или маршрутизаторе и в виде специализированного устройства.

В настоящее время чаще используется программное решение, которое на первый взгляд выглядит более привлекательным. Это вызвано тем, что для его применения достаточно, казалось бы, всего лишь приобрести программное обеспечение межсетевого экрана и установить на любой имеющийся в организации компьютер. Однако, как показывает практика, в организации далеко не всегда находится свободный компьютер, да еще и удовлетворяющий достаточно высоким требованиям по системным ресурсам. После того как компьютер все-таки найден (чаще всего – куплен), следует процесс установки и настройки операционной системы, а также непосредственно программного обеспечения межсетевого экрана. Нетрудно заметить, что использование обычного персонального компьютера далеко не так просто, как может показаться. Именно поэтому все большее распространение стали получать

специализированные программно-аппаратные комплексы, называемые security appliance, на основе, как правило, FreeBSD или Linux, «урезанные» для выполнения только необходимых функций. Достоинствами данных решений являются:

- простота внедрения: данные устройства имеют предустановленную и настроенную операционную систему и требуют минимум настроек после внедрения в сеть;
- простота управления: данными устройствами можно управлять откуда угодно по стандартным протоколам, таким как SNMP или Telnet, либо посредством защищенных протоколов, таких как SSH или SSL;
- производительность: данные устройства работают более эффективно, так как из их операционной системы исключены все неиспользуемые сервисы;
- отказоустойчивость и высокая доступность: данные устройства созданы выполнять конкретные задачи с высокой доступностью.

Ограниченность анализа межсетевого экрана

Межсетевой экран позволяет осуществлять фильтрацию только того трафика, который он способен «понимать». В противном случае он теряет свою эффективность, так как неспособен осознанно принять решение о том, что делать с нераспознанным трафиком. Существуют протоколы, такие как TLS, SSH, IPsec и SRTP, использующие криптографию для того, чтобы скрыть содержимое, из-за чего их трафик не может быть интерпретирован. Также некоторые протоколы, такие как OpenPGP и S/MIME, шифруют данные прикладного уровня, из-за чего фильтровать трафик на основании информации, содержащейся на данном сетевом уровне, становится невозможно. Еще одним примером ограниченности анализа межсетевых экранов является туннелированный трафик, так как его фильтрация является невозможной, если межсетевой экран «не понимает» используемый механизм туннелирования. Во всех этих случаях правила, сконфигурированные на межсетевом экране, должны явно определять, что делать с трафиком, который они не могут интерпретировать.

IDS и IPS

IDS

Intrusion Detection System (IDS) – система обнаружения вторжений (СОВ). Это программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими, в основном через Интернет. Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

IPS

Intrusion Prevention System (IPS, система предотвращения вторжений) – программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Системы IPS можно рассматривать как расширение систем обнаружения вторжений (IDS), так как задача отслеживания атак остается одинаковой. Однако они отличаются тем, что IPS-

системы должны отслеживать активность в реальном времени и быстро реализовывать действия по предотвращению атак.

Пакетные фильтры

Пакетные фильтры функционируют на сетевом уровне и контролируют прохождение трафика на основе информации, содержащейся в заголовке пакетов. Многие межсетевые экраны данного типа могут оперировать заголовками протоколов и более высокого, транспортного уровня (например, TCP или UDP). Пакетные фильтры одними из первых появились на рынке межсетевых экранов и по сей день остаются самым распространенным их типом. Данная технология реализована в подавляющем большинстве маршрутизаторов и даже в некоторых коммутаторах.

При анализе заголовка сетевого пакета могут использоваться следующие параметры:

- IP-адреса источника и получателя;
- тип транспортного протокола;
- поля служебных заголовков протоколов сетевого и транспортного уровней;
- порты источника и получателя.

Достаточно часто приходится фильтровать фрагментированные пакеты, что затрудняет определение некоторых атак. Многие сетевые атаки используют данную уязвимость межсетевых экранов, выдавая пакеты, содержащие запрещенные данные, за фрагменты другого, доверенного пакета. Одним из способов борьбы с данным типом атак является конфигурирование межсетевого экрана таким образом, чтобы блокировать фрагментированные пакеты. Некоторые межсетевые экраны могут дефрагментировать пакеты перед пересылкой во внутреннюю сеть, но это требует дополнительных ресурсов самого межсетевого экрана, особенно памяти. Дефрагментация должна использоваться очень обоснованно, иначе такой межсетевой экран легко может сам стать жертвой DoS-атаки.

Пакетные фильтры могут быть реализованы в следующих компонентах сетевой инфраструктуры:

- пограничных маршрутизаторах;
- операционных системах;
- персональных межсетевых экранах.

Так как пакетные фильтры обычно проверяют данные только в заголовках сетевого и транспортного уровней, они могут выполнять это достаточно быстро. Поэтому пакетные фильтры, встроенные в пограничные маршрутизаторы, идеальны для размещения на границе с сетью с низкой степенью доверия. Однако в пакетных фильтрах отсутствует возможность анализа протоколов более высоких уровней сетевой модели OSI. Кроме того, пакетные фильтры обычно уязвимы для атак, которые используют подделку сетевого адреса. Такие атаки обычно выполняются для обхода управления доступом, осуществляемого межсетевым экраном.

Принцип работы

1. Работают по принципу «если… то…» и, как результат, состоят из двух частей:
   а) условие (если…),
   б) действие (то…).
2. Могут содержать несколько условий. В таком случае должны быть выполнены все условия.

3. Обрабатываются по порядку. Обработка заканчивается после первого совпадения с правилом.

Существует два принципа обработки поступающего трафика:

1. Первый принцип гласит: «Что явно не запрещено, то разрешено». В данном случае если межсетевой экран получил пакет, не попадающий ни под одно правило, то он передается далее.
2. Противоположный принцип: «Что явно не разрешено, то запрещено» – гарантирует гораздо большую защищенность, так как он запрещает весь трафик, который явно не разрешен правилами.

В конечном счете межсетевые экраны выполняют над поступающим трафиком одну из двух операций: пропустить пакет далее (allow) или отбросить пакет (deny). Некоторые межсетевые экраны имеют еще одну операцию – reject, при которой пакет отбрасывается, но отправителю сообщается о недоступности сервиса, доступ к которому он пытался получить. В противовес этому при операции deny отправитель не информируется о недоступности сервиса, что является более безопасным.

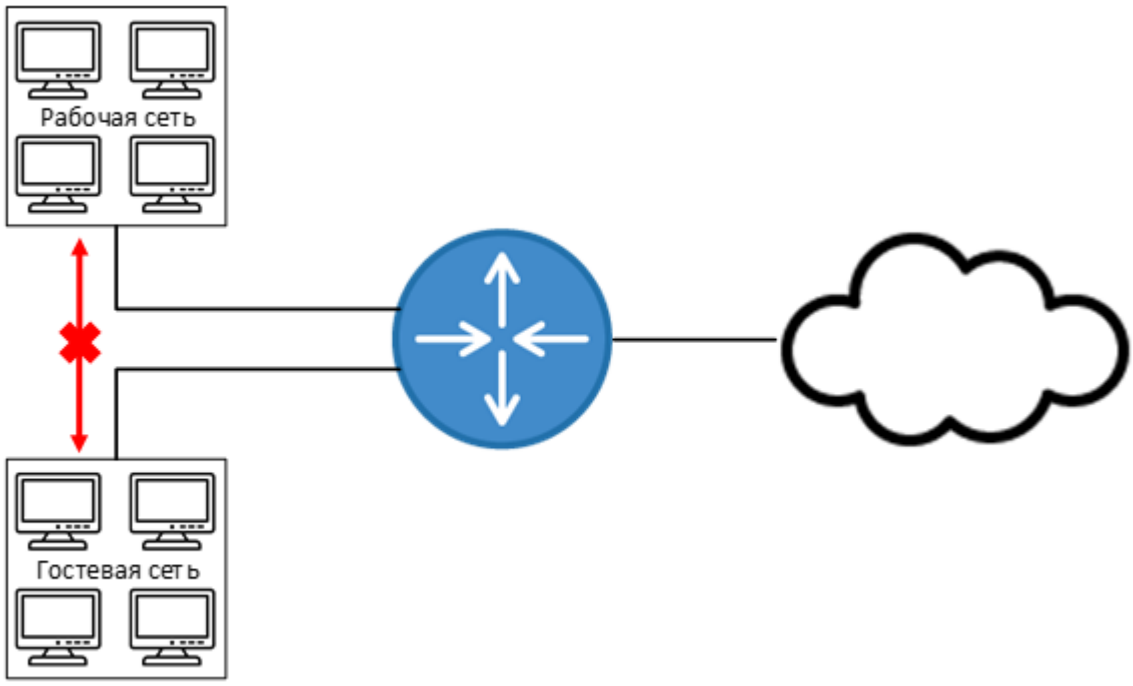
Последовательность правил в наборе существенно влияет на производительность межсетевого экрана. Межсетевые экраны последовательно сравнивают трафик с правилами до тех пор, пока не будет найдено соответствие. Для таких межсетевых экранов правила, которые соответствуют наибольшему количеству трафика, следует располагать как можно выше в списке, увеличивая тем самым производительность.

Гостевая сеть и DMZ

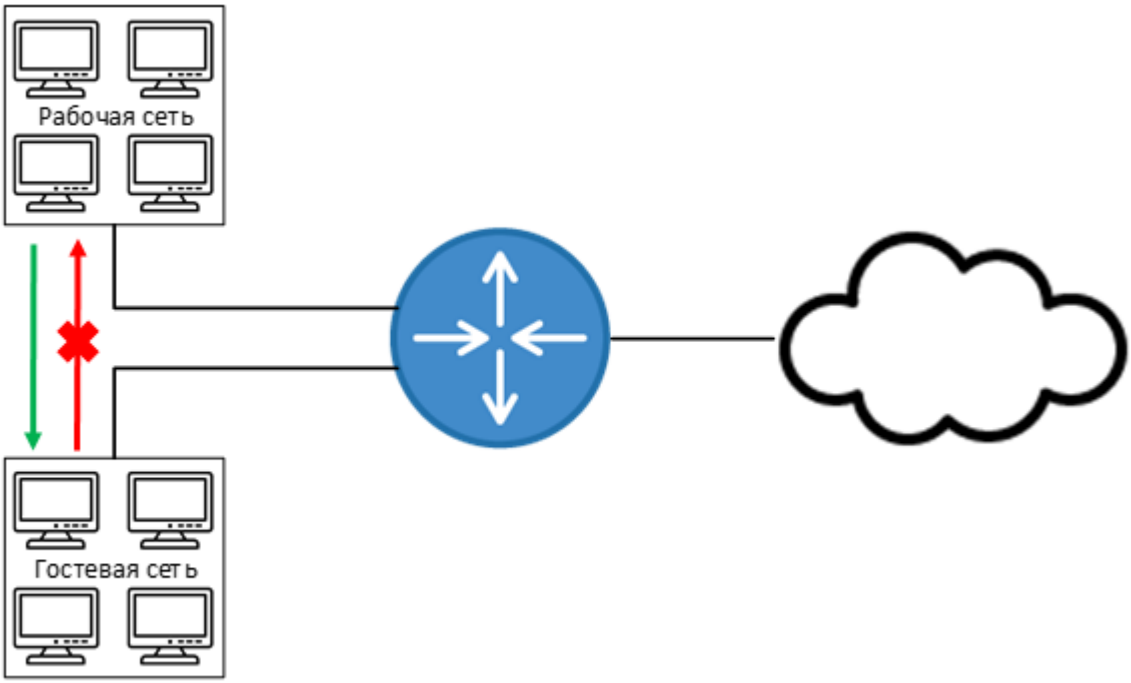
Гостевая сеть

Есть разные варианты организации гостевой сети.

Трафик из локальной сети в гостевую и наоборот запрещен



Трафик из локальной сети в гостевую разрешен, а из гостевой в локальную запрещен



DMZ

DMZ (англ. Demilitarized Zone «демилитаризованная зона» (ДМЗ)) – сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных. В качестве общедоступного может выступать, например, веб-сервис: обеспечивающий его сервер, который физически размещен в локальной сети (Интранете), должен отвечать на любые запросы из внешней сети (Интернета), при этом другие локальные ресурсы (например, файловые серверы, рабочие станции) необходимо изолировать от внешнего доступа.

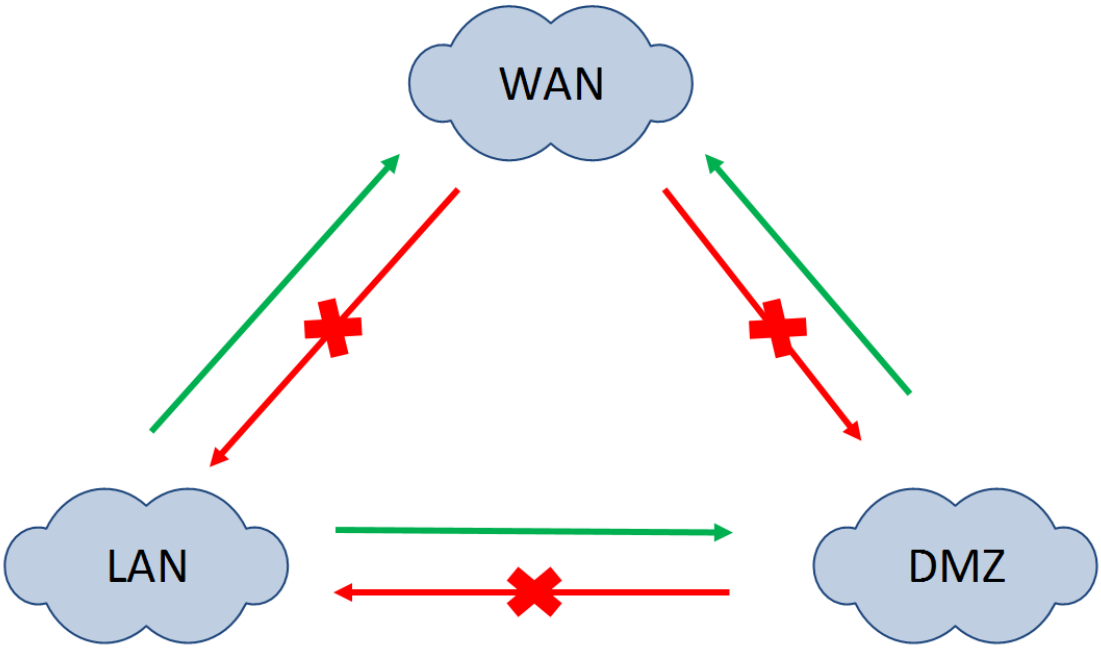
Цель DMZ – добавить дополнительный уровень безопасности в локальной сети, позволяющий минимизировать ущерб в случае атаки на один из общедоступных сервисов: внешний злоумышленник имеет прямой доступ только к оборудованию в DMZ.

Название происходит от военного термина «демилитаризованная зона» – территория между враждующими государствами, на которой не допускаются военные операции. Иными словами, доступ в DMZ открыт для обеих сторон при условии, что посетитель не имеет злого умысла. По аналогии, концепция DMZ (например, при построении шлюза в публичный Интернет) состоит в том, что в локальной сети выделяется область, которая не безопасна как оставшаяся часть сети (внутренняя) и не опасна как публичная (внешняя).

Системы, открытые для прямого доступа из внешних сетей, как правило, являются главными целями злоумышленников и потенциально подвержены проявлению угроз. Как следствие, эти системы не могут пользоваться полным доверием. Поэтому необходимо ограничить доступ этих систем к компьютерам, расположенным внутри сети.

Предоставляя защиту от внешних атак, ДМЗ, как правило, не имеет никакого отношения к атакам внутренним, таким как перехват трафика.

Схема прохождения трафика



Итого:

- LAN => WAN – разрешен;
- LAN => DMZ – разрешен;
- DMZ => LAN – запрещен;
- DMZ => WAN – разрешен;
- WAN => LAN – запрещен;
- WAN => DMZ – запрещен.

Распространенные сетевые атаки

Основы сетевой и информационной безопасности

Три концепции безопасности

Три основные концепции безопасности – это: конфиденциальность, целостность и доступность.

Конфиденциальность. Есть два вида данных: данные, которые перемещаются по сети, и данные, которые находятся на одном месте (файлы в файловом хранилище, в облаке и др.). Конфиденциальность значит, что только люди, имеющие на это полномочия, имеют доступ к важной или классифицированной информации. Как результат, неавторизованные люди не должны иметь никакого доступа к такой информации. Информация, которая перемещается по сети, должна быть зашифрована перед передачей. Также можно разделить сети, предназначенные для передачи разной конфиденциальной информации.

Целостность. Целостность данных значит, что изменения в информацию вносятся только авторизованными людьми или системами.

Доступность. Это понятие применяется к системам и информации. Может случиться, что информация будет недоступна авторизованному персоналу во время DoS-атаки или сбое на сетевом оборудовании.

Анализ эффективности затрат

Актив – это что-то, имеющее ценность для организации. Актив может быть материальным и нематериальным. К материальным активам относятся люди, компьютеры и т.д. К нематериальным активам относятся интеллектуальная собственность, база данных клиентов и др.

Уязвимость – это слабое место в системе или ее дизайне. Уязвимость может быть найдена в протоколах, операционных системах, приложениях и других объектах. Каждый день открываются новые уязвимости.

Угроза – это потенциальная опасность для актива. Если имеется уязвимость, которая до сих пор не была использована или до сих пор неизвестна, то такая уязвимость называется скрытой (латентной). Неизвестная уязвимость является более опасной, чем известная. Если кто-то успешно атаковал систему и получил доступ к чему-либо или скомпрометировал безопасность актива, то такая угроза является реализованной.

Риск – вероятность неавторизованного доступа, компрометации, повреждения или удаления актива.

Контрмера – это способ защиты, с помощью которого уменьшается потенциальный риск. Это может быть достигнуто с помощью уменьшения либо полного удаления уязвимости или хотя бы снижения вероятности использования уязвимости.

Классификация активов

Правительство:

- неклассифицированный;
- чувствительный, но неклассифицированный;
- конфиденциальный;
- секретный;
- сверхсекретный.

Частное применение:

- публичный;
- чувствительный;
- частный;
- конфиденциальный.

Критерии классификации:

- значение;
- возраст;
- стоимость замены;
- время полезного использования.

Роли классификации:

- владелец (например, топ-менеджеры компании);
- комендант (лица, ответственные за применение политик безопасности);
- пользователь.

Протокол Traffic Light

Протокол Traffic Light (англ. Traffic Light Protocol (TLP), дословно: «протокол Светофор») – набор обозначений для маркировки конфиденциальной информации с целью указать аудиторию ее дальнейшего распространения. Информация маркируется одним из четырех цветов, ее цвет обычно указывается в колонтитулах документа при помощи надписи вида: «TLP: цвет».

Всего используется 4 цвета:

КРАСНЫЙ – крайне конфиденциальная информация, только для конечного получателя. К примеру, информация должна быть доступна только участникам встречи или заседания. В большинстве случаев информация передается лично.

ЖЕЛТЫЙ – ограниченное распространение. Получатель может поделиться ЖЕЛТОЙ информацией только в рамках своей организации, при условии что этой информацией нужно поделиться. Автор конкретной информации может установить пределы, в которых разрешается ею делиться.

ЗЕЛЕНЫЙ – широкое распространение. Информация этой категории может быть широко распространена в пределах определенного сообщества. Тем не менее информация не может быть опубликована в СМИ, Интернете или где бы то ни было за пределами сообщества.

БЕЛЫЙ – неограниченное распространение. Распространяется свободно, но не должна нарушать авторские права.

Классификация уязвимостей

Понимание мест потенциальной угрозы – это большой шаг на пути к их устранению. Это могут быть:

- изъяны политик безопасности;
- ошибки дизайна;
- уязвимости протоколов;
- некорректная настройка;
- уязвимости в ПО;
- человеческий фактор;
- вредоносное ПО;
- уязвимости в аппаратной составляющей;
- физический доступ к активам.

Классификация контрмер

Административные контрмеры состоят из письменных политик (правил безопасности) процедур, стандартов и др.

Физические контрмеры – это обеспечение ограничения физического доступа к серверам, маршрутизаторам и другим активам. Использование источников бесперебойного питания или второго блока питания на устройствах также является контрмерой.

Логические контрмеры – это пароли, файрволы, списки доступа к VPN-туннелям.

Потенциальные атакующие

- Террористы.
- Преступники.
- Силовые структуры.
- Хакеры.
- Рассерженные сотрудники.
- Конкуренты.
- Любой, кто имеет доступ к ПК.

Методы атак

- Разведка.
- Социальный инжиниринг.
- Повышение полномочий.
- Задняя дверь (backdoor).
- Выполнение кода.

Направление атаки

- Извне.
- Изнутри (bring your own device (BYOD).

Распространенные атаки

Классификация атак

По характеру воздействия:

- пассивная,
- активная.

Пассивное воздействие на распределенную вычислительную систему (РВС) представляет собой некоторое воздействие, не оказывающее прямого влияния на работу системы, но в то же время способное нарушить ее политику безопасности. Отсутствие прямого влияния на работу РВС приводит именно к тому, что пассивное удаленное воздействие (ПУВ) трудно обнаружить. Возможным примером типового ПУВ в РВС служит прослушивание канала связи в сети.

Активное воздействие на РВС – воздействие, оказывающее прямое влияние на работу самой системы (нарушение работоспособности, изменение конфигурации РВС и т.д.), которое нарушает политику безопасности, принятую в ней. Активными воздействиями являются почти все типы удаленных атак. Связано это с тем, что в саму природу наносящего ущерб воздействия включается активное начало. Явное отличие активного воздействия от пассивного – принципиальная возможность его обнаружения, так как в результате его осуществления в системе происходят некоторые изменения. При пассивном же воздействии не остается совершенно никаких следов (из-за того, что атакующий просмотрит чужое сообщение в системе, в тот же момент не изменится, собственно, ничего).

По цели воздействия:

- нарушение функционирования системы (доступа к системе);
- нарушение целостности информационных ресурсов (ИР);
- нарушение конфиденциальности ИР.

Этот признак, по которому производится классификация, по сути есть прямая проекция трех базовых разновидностей угроз: отказа в обслуживании, раскрытия и нарушения целостности.

Главная цель, которую преследуют практически при любой атаке, – получение несанкционированного доступа к информации. Существуют два принципиальных варианта получения информации: искажение и перехват. Вариант перехвата информации означает получение к ней доступа без возможности ее изменения. Перехват информации приводит, следовательно, к нарушению ее конфиденциальности. Прослушивание канала в сети – пример перехвата информации. В этом случае имеется нелегитимный доступ к информации без возможных вариантов ее подмены. Очевидно, что нарушение конфиденциальности информации относится к пассивным воздействиям.

Возможность подмены информации следует понимать либо как полный контроль над потоком информации между объектами системы, либо возможность передачи различных сообщений от чужого имени. Следовательно, понятно, что подмена информации приводит к нарушению ее целостности. Такое информационное разрушающее воздействие есть характерный пример активного воздействия. Примером же удаленной атаки, предназначенной для нарушения целостности информации, может послужить удаленная атака (УА) «Ложный объект РВС».

По наличию обратной связи с атакуемым объектом:

- с обратной связью;
- без обратной связи (однонаправленная атака).

Атакующий отправляет некоторые запросы атакуемому объекту, на которые ожидает получить ответ. Следовательно, между атакующим и атакуемым появляется обратная связь, позволяющая первому адекватно реагировать на всяческие изменения на атакуемом объекте. В этом суть удаленной атаки, осуществляемой при наличии обратной связи с атакующим объектом. Подобные атаки наиболее характерны для РВС.

Атаки без обратной связи характерны тем, что им не требуется реагировать на изменения на атакуемом объекте. Такие атаки обычно осуществляются при помощи передачи на атакуемый объект одиночных запросов. Ответы на эти запросы атакующему не нужны. Подобную УА можно назвать также однонаправленной УА. Примером однонаправленных атак является типовая УА «DoS-атака».

По условию начала осуществления воздействия

Удаленное воздействие, так же как и любое другое, может начать осуществляться только при определенных условиях. В РВС существуют три вида таких условных атак:

- атака по запросу от атакуемого объекта;
- атака по наступлении ожидаемого события на атакуемом объекте;
- безусловная атака.

Воздействие со стороны атакующего начнется при условии, что потенциальная цель атаки передаст запрос определенного типа. Такую атаку можно назвать атакой по запросу от атакуемого объекта. Данный тип УА наиболее характерен для РВС. Примерами подобных запросов в сети Интернет могут служить DNS- и ARP-запросы, а в Novell NetWare – SAP-запрос.

Атака по наступлении ожидаемого события на атакуемом объекте. Атакующий непрерывно наблюдает за состоянием ОС удаленной цели атаки и начинает воздействие при происшествии конкретного события в этой системе. Атакуемый объект сам является инициатором начала атаки. Примером такого события может быть прерывание сеанса работы пользователя с сервером без выдачи команды LOGOUT в Novell NetWare.

Безусловная атака осуществляется немедленно и безотносительно к состоянию операционной системы и атакуемого объекта. Следовательно, атакующий является инициатором начала атаки в данном случае.

При нарушении нормальной работоспособности системы преследуются другие цели, и получение атакующим незаконного доступа к данным не предполагается. Его целью является вывод из строя ОС на атакуемом объекте и невозможность доступа для остальных объектов системы к ресурсам этого объекта. Примером атаки такого вида может служить DoS-атака.

По расположению субъекта атаки относительно атакуемого объекта

- межсегментная;
- внутрисегментная.

Приведем некоторые определения.

Источник атаки (субъект атаки) – программа (возможно, оператор), ведущая атаку и осуществляющая непосредственное воздействие.

Хост (host) – компьютер, являющийся элементом сети.

Маршрутизатор (router) – устройство, которое обеспечивает маршрутизацию пакетов в сети.

Подсетью (subnetwork) называется группа хостов, являющихся частью глобальной сети, отличающихся тем, что маршрутизатором для них выделена одна и та же подсеть. Также можно сказать, что подсеть есть логическое объединение хостов посредством маршрутизатора. Хосты внутри одной подсети могут непосредственно взаимодействовать между собой, не задействовав при этом маршрутизатор.

Сегмент сети – объединение хостов на физическом уровне.

С точки зрения удаленной атаки крайне важным является взаимное расположение субъекта и объекта атаки, то есть находятся ли они в разных или в одинаковых сегментах. Во время внутрисегментной атаки субъект и объект атаки располагаются в одном сегменте. В случае межсегментной атаки субъект и объект атаки находятся в разных сетевых сегментах. Этот классификационный признак дает возможность судить о так называемой степени удаленности атаки.

Далее будет показано, что практически внутрисегментную атаку осуществить намного проще, чем межсегментную. Отметим также, что межсегментная удаленная атака представляет куда большую опасность, чем внутрисегментная. Это связано с тем, что в случае межсегментной атаки объект ее и непосредственно атакующий могут находиться на расстоянии многих тысяч километров друг от друга, что может существенно воспрепятствовать мерам по отражению атаки.

По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие

- физический,
- канальный,
- сетевой,
- транспортный,
- сеансовый,
- представления,
- прикладной.

Международной организацией по стандартизации (ISO) был принят стандарт ISO 7498, который описывает взаимодействие открытых систем (OSI), к которым принадлежат также и РВС. Каждый сетевой протокол обмена, так же как и каждую сетевую программу, удается так или иначе спроецировать на эталонную 7-уровневую модель OSI. Такая многоуровневая проекция дает возможность описать в терминах модели OSI использующиеся в сетевом протоколе или программе функции. УА – сетевая программа, и логично рассматривать ее с точки зрения проекции на эталонную модель ISO/OSI.

Краткое описание некоторых сетевых атак

Фрагментация данных

При передаче пакета данных протокола IP по сети может осуществляться деление этого пакета на несколько фрагментов. Впоследствии, при достижении адресата, пакет восстанавливается из этих фрагментов. Злоумышленник может инициировать посылку большого числа фрагментов, что приводит к переполнению программных буферов на приемной стороне и в ряде случаев к аварийному завершению системы.

Атака Ping flooding

Данная атака требует от злоумышленника доступа к быстрым каналам в Интернете.

Программа ping посылает ICMP-пакет типа ECHO REQUEST, выставляя в нем время и его идентификатор. Ядро машины-получателя отвечает на подобный запрос пакетом ICMP ECHO REPLY. Получив его, ping выдает скорость прохождения пакета.

При стандартном режиме работы пакеты высылаются через некоторые промежутки времени, практически не нагружая сеть. Но в «агрессивном» режиме поток ICMP echo request/reply-пакетов может вызвать перегрузку небольшой линии, лишив ее способности передавать полезную информацию.

Нестандартные протоколы, инкапсулированные в IP

Пакет IP содержит поле, определяющее протокол инкапсулированного пакета (TCP, UDP, ICMP). Злоумышленники могут использовать нестандартное значение данного поля для передачи данных, которые не будут фиксироваться стандартными средствами контроля информационных потоков.

Атака smurf

Атака smurf заключается в передаче в сеть широковещательных ICMP-запросов от имени компьютера-жертвы. В результате компьютеры, принявшие такие широковещательные пакеты, отвечают компьютеру-жертве, что приводит к существенному снижению пропускной способности канала связи и в ряде случаев к полной изоляции атакуемой сети. Атака smurf исключительно эффективна и широко распространена.

Противодействие: для распознавания данной атаки необходимо анализировать загрузку канала и определять причины снижения пропускной способности.

Атака DNS spoofing

Другое название: атака Каминского.

Результатом данной атаки является внесение навязываемого соответствия между IP-адресом и доменным именем в кеш DNS-сервера. В результате успешного проведения такой атаки все пользователи DNS-сервера получат неверную информацию о доменных именах и IP-адресах. Данная атака характеризуется большим количеством DNS-пакетов с одним и тем же доменным именем. Это связано с необходимостью подбора некоторых параметров DNS-обмена.

Противодействие: для выявления такой атаки необходимо анализировать содержимое DNS-трафика либо использовать DNSSEC.

Атака IP spoofing

Большое количество атак в сети Интернет связано с подменой исходного IP-адреса. К таким атакам относится и syslog spoofing, которая заключается в передаче на компьютер-жертву сообщения от имени другого компьютера внутренней сети. Поскольку протокол syslog используется для ведения системных журналов, путем передачи ложных сообщений на компьютер-жертву можно навязать информацию или замести следы несанкционированного доступа.

Противодействие: выявление атак, связанных с подменой IP-адресов, возможно при контроле получения на одном из интерфейсов пакета с исходным адресом этого же интерфейса или при контроле получения на внешнем интерфейсе пакетов с IP-адресами внутренней сети.

Навязывание пакетов

Злоумышленник отправляет в сеть пакеты с ложным обратным адресом. С помощью этой атаки злоумышленник может переключать на свой компьютер соединения, установленные между другими компьютерами. При этом права доступа злоумышленника становятся равными правам того пользователя, чье соединение с сервером было переключено на компьютер злоумышленника.

Sniffing – прослушивание канала

Возможно только в сегменте локальной сети.

Практически все сетевые карты поддерживают возможность перехвата пакетов, передаваемых по общему каналу локальной сети. При этом рабочая станция может принимать пакеты, адресованные другим компьютерам того же сегмента сети. Таким образом, весь информационный обмен в сегменте сети становится доступным злоумышленнику. Для успешной реализации этой атаки компьютер злоумышленника должен располагаться в том же сегменте локальной сети, что и атакуемый компьютер.

Перехват пакетов на маршрутизаторе

Сетевое программное обеспечение маршрутизатора имеет доступ ко всем сетевым пакетам, передаваемым через данный маршрутизатор, что позволяет осуществлять перехват пакетов. Для реализации этой атаки злоумышленник должен иметь привилегированный доступ хотя бы к одному маршрутизатору сети. Поскольку через маршрутизатор обычно передается очень много пакетов, тотальный их перехват практически невозможен. Однако отдельные пакеты вполне могут быть перехвачены и сохранены для последующего анализа злоумышленником. Наиболее эффективен перехват пакетов FTP, содержащих пароли пользователей, а также электронной почты.

Навязывание хосту ложного маршрута с помощью протокола ICMP

В сети Интернет существует специальный протокол ICMP (Internet Control Message Protocol), одной из функций которого является информирование хостов о смене текущего маршрутизатора. Данное управляющее сообщение носит название «redirect». Существует возможность посылки с любого хоста в сегменте сети ложного redirect-сообщения от имени маршрутизатора на атакуемый хост. В результате у хоста изменяется текущая таблица маршрутизации, и в дальнейшем весь сетевой трафик данного хоста будет проходить, например, через хост, отославший ложное redirect-сообщение. Таким образом возможно осуществить активное навязывание ложного маршрута внутри одного сегмента сети Интернет.

WinNuke

Наряду с обычными данными, пересылаемыми по TCP-соединению, стандарт предусматривает также передачу срочных (Out Of Band) данных. На уровне форматов пакетов TCP это выражается в ненулевом urgent pointer. У большинства ПК с ОС Windows присутствует сетевой протокол NetBIOS, который использует для своих нужд три IP-порта: 137, 138, 139. Если соединиться с Windows-машиной по 139 порту и послать туда несколько байтов OutOfBand-данных, то реализация NetBIOS`a, не зная, что делать с этими данными, попросту «вешает» или перезагружает машину. Для Windows 95 это обычно выглядит как синий текстовый экран, сообщающий об ошибке в драйвере TCP/IP, и невозможность работы с сетью до перезагрузки ОС. NT 4.0 без сервис-паков перезагружается, NT 4.0 с ServicePack 2 паком выпадает в синий экран. Судя по информации из сети, подвержены такой атаке и Windows NT 3.51, и Windows 3.11 for Workgroups.

Посылка данных в 139-й порт приводит к перезагрузке NT 4.0 либо выводу синего «экрана смерти» с установленным Service Pack 2. Аналогичная посылка данных в 135-й и некоторые другие порты приводит к значительной загрузке процесса RPCSS.EXE. На Windows NT WorkStation это приводит к существенному замедлению работы, Windows NT Server практически замораживается.

Подмена доверенного хоста

Успешное осуществление удаленных атак этого типа позволит злоумышленнику вести сеанс работы с сервером от имени доверенного хоста (т.е. станции, легально подключившейся к серверу). Реализация данного вида атак обычно состоит в посылке пакетов обмена со станции злоумышленника от имени доверенной станции, находящейся под его контролем.

Syn-flood

SYN-флуд – одна из разновидностей сетевых атак типа отказа от обслуживания, которая заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий срок (RFC 4987).

Согласно процессу «трехкратного рукопожатия» TCP, клиент посылает пакет с установленным флагом SYN (synchronize). На него сервер должен ответить комбинацией флагов SYN+ACK (acknowledges). После этого клиент должен ответить пакетом с флагом ACK, после чего соединение считается установленным.

Принцип атаки заключается в том, что злоумышленник, посылая SYN-запросы, переполняет на сервере (цели атаки) очередь на подключения. При этом он игнорирует SYN+ACK-пакеты цели, не высылая ответные пакеты, либо подделывает заголовок пакета таким образом, что ответный SYN+ACK отправляется на несуществующий адрес. В очереди подключений появляются так называемые полуоткрытые соединения (англ. half-open connection), ожидающие подтверждения от клиента. По истечении определенного тайм-аута эти подключения отбрасываются. Задача злоумышленника заключается в том, чтобы поддерживать очередь заполненной таким образом, чтобы не допустить новых подключений. Из-за этого клиенты, не являющиеся злоумышленниками, не могут установить связь либо устанавливают ее с существенными задержками.

Технологии обнаружения атак

Сетевые и информационные технологии меняются настолько быстро, что статичные защитные механизмы, к которым относятся системы разграничения доступа, МЭ, системы аутентификации, во многих случаях не могут обеспечить эффективной защиты. Поэтому требуются динамические методы, позволяющие оперативно обнаруживать и предотвращать

нарушения безопасности. Одной из технологий, позволяющей обнаруживать нарушения, которые не могут быть идентифицированы при помощи традиционных моделей контроля доступа, является технология обнаружения атак.

По существу, процесс обнаружения атак является процессом оценки подозрительных действий, которые происходят в корпоративной сети. Иначе говоря, обнаружение атак (intrusion detection) – это процесс идентификации и реагирования на подозрительную деятельность, направленную на вычислительные или сетевые ресурсы.

Методы анализа сетевой информации

Эффективность системы обнаружения атак во многом зависит от применяемых методов анализа полученной информации. В первых системах обнаружения атак, разработанных в начале 1980-х годов, использовались статистические методы обнаружения атак. В настоящее время к статистическому анализу добавился ряд новых методик, начиная с экспертных систем и нечеткой логики и заканчивая использованием нейронных сетей.

Статистический метод

Основные преимущества статистического подхода – использование уже разработанного и зарекомендовавшего себя аппарата математической статистики и адаптация к поведению субъекта.

Сначала для всех субъектов анализируемой системы определяются профили. Любое отклонение используемого профиля от эталонного считается несанкционированной деятельностью. Статистические методы универсальны, поскольку для проведения анализа не требуется знания о возможных атаках и используемых ими уязвимостях. Однако при использовании этих методик возникают и проблемы:

1) статистические системы нечувствительны к порядку следования событий; в некоторых случаях одни и те же события в зависимости от порядка их следования могут характеризовать аномальную или нормальную деятельность;

2) трудно задать граничные (пороговые) значения отслеживаемых системой обнаружения атак характеристик, чтобы адекватно идентифицировать аномальную деятельность;

3) «статистические» системы могут быть с течением времени «обучены» нарушителями так, чтобы атакующие действия рассматривались как нормальные.

Следует также учитывать, что статистические методы неприменимы в тех случаях, когда для пользователя отсутствует шаблон типичного поведения или когда для пользователя типичны несанкционированные действия.

Экспертные системы

Экспертные системы состоят из набора правил, которые охватывают знания человека-эксперта. Использование экспертных систем представляет собой распространенный метод обнаружения атак, при котором информация об атаках формулируется в виде правил. Эти правила могут быть записаны, например, в виде последовательности действий или в виде сигнатуры. При выполнении любого из этих правил принимается решение о наличии несанкционированной деятельности. Важным достоинством такого подхода является практически полное отсутствие ложных тревог.

БД экспертной системы должна содержать сценарии большинства известных на сегодняшний день атак. Для того чтобы оставаться постоянно актуальными, экспертные системы требуют постоянного обновления БД. Хотя экспертные системы предлагают хорошую возможность для

просмотра данных в журналах регистрации, требуемые обновления могут либо игнорироваться, либо выполняться администратором вручную. Как минимум это приводит к экспертной системе с ослабленными возможностями. В худшем случае отсутствие надлежащего сопровождения снижает степень защищенности всей сети, вводя ее пользователей в заблуждение относительно действительного уровня защищенности.

Основным недостатком является невозможность отражения неизвестных атак. При этом даже небольшое изменение уже известной атаки может стать серьезным препятствием для функционирования системы обнаружения атак.

Нейронные сети

Большинство современных методов обнаружения атак используют некоторую форму анализа контролируемого пространства на основе правил или статистического подхода. В качестве контролируемого пространства могут выступать журналы регистрации или сетевой трафик. Анализ опирается на набор заранее определенных правил, которые создаются администратором или самой системой обнаружения атак.

Любое разделение атаки во времени или среди нескольких злоумышленников является трудным для обнаружения при помощи экспертных систем. Из-за большого разнообразия атак и хакеров даже специальные постоянные обновления БД правил экспертной системы никогда не дадут гарантии точной идентификации всего диапазона атак.

Использование нейронных сетей является одним из способов преодоления указанных проблем экспертных систем. В отличие от экспертных систем, которые могут дать пользователю определенный ответ о соответствии рассматриваемых характеристик заложенным в БД правилам, нейронная сеть проводит анализ информации и предоставляет возможность оценить, согласуются ли данные с характеристиками, которые она научена распознавать. В то время как степень соответствия нейросетевого представления может достигать 100 %, достоверность выбора полностью зависит от качества системы в анализе примеров поставленной задачи.

Сначала нейросеть обучают правильной идентификации на предварительно подобранной выборке примеров предметной области. Реакция нейросети анализируется, и система настраивается таким образом, чтобы достичь удовлетворительных результатов. В дополнение к начальному периоду обучения нейросеть набирается опыта с течением времени, по мере того как она проводит анализ данных, связанных с предметной областью.

Важным преимуществом нейронных сетей при обнаружении злоупотреблений является их способность «изучать» характеристики умышленных атак и идентифицировать элементы, которые не похожи на те, что наблюдались в сети прежде.

Каждый из описанных методов обладает рядом достоинств и недостатков, поэтому сейчас очень трудно встретить систему, реализующую только один из описанных методов. Как правило, эти методы используются в совокупности.

Социальная инженерия

Социальная инженерия – это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным. Зачастую социальную инженерию рассматривают как незаконный метод получения информации, однако это не совсем так. Социальную инженерию можно также использовать и в законных целях – не только для получения информации, но и для совершения действий конкретным человеком. Сегодня социальную инженерию зачастую

используют в Интернете для получения закрытой информации или информации, которая представляет большую ценность.

История

Сам термин «социальная инженерия» является социологическим и обозначает совокупность подходов прикладных социальных наук, которые ориентированы на целенаправленное изменение организационных структур, определяющих человеческое поведение и обеспечивающих контроль за ним. В сфере информационной безопасности данный термин был популяризован в начале XXI века бывшим компьютерным преступником, ныне консультантом по безопасности, Кевином Митником, который утверждал, что самое уязвимое место любой системы безопасности – человеческий фактор.

Методы социальной инженерии в смысле получения доступа к конфиденциальной информации либо мотивации к действию с помощью технических и нетехнических методов были известны задолго до популяризации термина Митника и вообще до компьютерной эры. Например, группа исследователей из врачей и медсестер трех больниц Среднего Запада проводила исследование, в котором психологи по телефону представлялись врачами и просили медсестер вколоть пациенту смертельную дозу лекарства. Несмотря на то что медсестры знали, что делали, в 95 % случаев они беспрекословно выполняли команду (разумеется, их останавливали ассистенты на входе в палату).

Техники

Все техники социальной инженерии основаны на когнитивных искажениях. Эти ошибки в поведении используются социальными инженерами для создания атак, направленных на получения конфиденциальной информации, часто с согласия жертвы.

Так, одним из простых примеров является ситуация, в которой некий человек входит в здание компании и вешает на информационном бюро объявление, выглядящее как официальное, с информацией об изменении телефона справочной службы интернет-провайдера. Когда сотрудники компании звонят по этому номеру, злоумышленник может запрашивать личные пароли и идентификаторы для получения доступа к конфиденциальной информации.

Фишинг

Фишинг (англ. phishing от fishing «рыбная ловля, выуживание») – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Это самая популярная схема социальной инженерии на сегодняшний день. Ни одна крупная утечка персональных данных не обходится без волны фишинговых рассылок, предшествующих ей. Целью фишинга является незаконное получение конфиденциальной информации. Наиболее ярким примером фишинговой атаки может служить сообщение, отправленное жертве по электронной почте и подделанное под официальное письмо – от банка или платежной системы, – требующее проверки определенной информации или совершения определенных действий. Причины могут называться самые различные. Это может быть утеря данных, поломка в системе и прочее. Такие письма обычно содержат ссылку на фальшивую веб-страницу, в точности похожую на официальную, и содержащую форму, требующую ввести конфиденциальную информацию.

Как распознать фишинг-атаку

Практически каждый день появляются новые схемы мошенничества. Большинство людей может самостоятельно научиться распознавать мошеннические сообщения, познакомившись с их некоторыми отличительными признаками. Чаще всего фишинговые сообщения содержат:

- сведения, вызывающие беспокойство, или угрозы, например, закрытия пользовательских банковских счетов;
- обещания огромного денежного приза с минимальными усилиями или вовсе без них;
- запросы о добровольных пожертвованиях от лица благотворительных организаций;
- непреднамеренные грамматические, пунктуационные и орфографические ошибки, выдающие подделку;
- умышленные грамматические, орфографические или фактологические ошибки в данных, касающихся пользователя, провоцирующие желание исправить их;
- имитацию поврежденного или неправильно перекодированного текста;
- адрес несуществующего почтового ящика, указанного в качестве адреса отправителя.

Несуществующие ссылки

Атака, которая заключается в отправлении письма с соблазнительной причиной посетить сайт и прямой ссылкой на него, которая лишь имеет сходство с ожидаемым сайтом, например, www.PayPai.com. Выглядит это, будто это ссылка на PayPal, мало кто заметит, что буква «l» заменена на «i». Таким образом, при переходе по ссылке жертва увидит сайт, максимально идентичный ожидаемому, и при вводе данных ее кредитной карты эта информация сразу отправляется к злоумышленнику.

Одним из наиболее известных примеров глобальной фишинговой рассылки может служить афера 2003 года, во время которой тысячи пользователей eBay получили электронные письма, в которых утверждалось, что их учетная запись была заблокирована и для ее разблокировки требуется обновить данные о кредитных картах. Во всех этих письмах присутствовала ссылка, ведущая на поддельную веб-страницу, в точности похожую на официальную. Впрочем, по подсчетам экспертов, убытки от этой аферы составили менее миллиона долларов (несколько сотен тысяч).

Мошенничество с использованием брендов известных корпораций

В таких фишинговых схемах используются поддельные сообщения электронной почты или веб-сайты, содержащие названия крупных или известных компаний. В сообщениях может быть поздравление с победой в каком-либо конкурсе, проводимом компанией, информация о том, что срочно требуется изменить учетные данные или пароль. Подобные мошеннические схемы от лица службы технической поддержки также могут производиться по телефону.

Подложные лотереи

Пользователь может получить сообщения, в которых говорится о том, что он выиграл в лотерею, которая проводилась какой-либо известной компанией. Внешне эти сообщения могут выглядеть так, как будто они были отправлены от лица одного из высокопоставленных сотрудников корпорации.

Ложные антивирусы и программы для обеспечения безопасности

Подобное мошенническое программное обеспечение, также известное под названием «scareware», – это программы, которые выглядят как антивирусы, хотя на самом деле все обстоит совсем наоборот. Такие программы генерируют ложные уведомления о различных угрозах, а также пытаются завлечь пользователя в мошеннические транзакции. Пользователь может столкнуться с ними в электронной почте, онлайн-объявлениях, в социальных сетях, в результатах поисковых систем и даже во всплывающих окнах на компьютере, которые имитируют системные сообщения.

IVR или телефонный фишинг

Телефонный фишинг – вишинг (англ. vishing – voice fishing). Назван так по аналогии с фишингом. Данная техника основана на использовании системы предварительно записанных голосовых сообщений с целью воссоздать «официальные звонки» банковских и других IVR-систем. Обычно жертва получает запрос (чаще всего через фишинг электронной почты) связаться с банком и подтвердить или обновить какую-либо информацию. Система требует аутентификации пользователя посредством ввода PIN-кода или пароля. Поэтому, предварительно записав ключевую фразу, можно выведать всю нужную информацию. Например, любой может записать типичную команду: «Нажмите единицу, чтобы сменить пароль. Нажмите двойку, чтобы получить ответ оператора» – и воспроизвести ее вручную в нужный момент времени, создав впечатление работающей в данный момент системы предварительно записанных голосовых сообщений.

Телефонный фрикинг

Телефонный фрикинг (англ. phreaking) – термин, описывающий эксперименты и взлом телефонных систем с помощью звуковых манипуляций с тоновым набором. Эта техника появилась в конце 1950-х в Америке. Телефонная корпорация Bell, которая тогда покрывала практически всю территорию Соединенных Штатов, использовала тоновый набор для передачи различных служебных сигналов. Энтузиасты, попытавшиеся повторить некоторые из этих сигналов, получали возможность бесплатно звонить, организовывать телефонные конференции и администрировать телефонную сеть.

Претекстинг

Претекстинг (англ. pretexting) – атака, в которой злоумышленник представляется другим человеком и по заранее подготовленному сценарию выуживает конфиденциальную информацию. Эта атака подразумевает должную подготовку: день рождения, ИНН, номер паспорта либо последние цифры счета, для того чтобы не вызвать подозрений у жертвы. Обычно реализуется через телефон или электронную почту.

Квид про кво

Квид про кво (от лат. Quid pro quo «то за это») – в английском языке это выражение обычно используется в значении «услуга за услугу». Данный вид атаки подразумевает обращение злоумышленника в компанию по корпоративному телефону (используя актерское мастерство) или электронной почте. Зачастую злоумышленник представляется сотрудником технической поддержки, который сообщает о возникновении технических проблем на рабочем месте сотрудника и предлагает помощь в их устранении. В процессе «решения» технических проблем злоумышленник вынуждает цель атаки совершать действия, позволяющие атакующему запускать команды или устанавливать различное программное обеспечение на компьютере жертвы.

Проведенное в 2003 году исследование в рамках программы «Информационная безопасность» показало, что 90 % офисных работников готовы разгласить конфиденциальную информацию, например свои пароли, за какую-либо услугу или вознаграждение.

«Дорожное яблоко»

Этот метод атаки представляет собой адаптацию троянского коня и состоит в использовании физических носителей. Злоумышленник подбрасывает «инфицированные» носители информации в местах общего доступа, где эти носители могут быть легко найдены, таких как туалеты, парковки, столовые, или на рабочем месте атакуемого сотрудника. Носители оформляются как официальные для компании, которую атакуют, или сопровождаются подписью, призванной вызвать любопытство. К примеру, злоумышленник может подбросить

CD, снабженный корпоративным логотипом и ссылкой на официальный сайт компании, снабдив его надписью: «Заработная плата руководящего состава». Диск может быть оставлен на полу лифта или в вестибюле. Сотрудник по незнанию может подобрать диск и вставить его в компьютер, чтобы удовлетворить свое любопытство.

Сбор информации из открытых источников

Применение техник социальной инженерии требует не только знания психологии, но и умения собирать о человеке необходимую информацию. Относительно новым способом получения такой информации стал ее сбор из открытых источников, главным образом из социальных сетей. К примеру, такие сайты, как livejournal, «Одноклассники», «ВКонтакте», содержат огромное количество данных, которые люди и не пытаются скрыть. Как правило, пользователи не уделяют должного внимания вопросам безопасности, оставляя в свободном доступе данные и сведения, которые могут быть использованы злоумышленником.

Показательным примером может стать история о похищении сына Евгения Касперского. В ходе следствия было установлено, что преступники узнали расписание дня и маршруты следования подростка из его записей на странице в социальной сети.

Даже ограничив доступ к информации на своей странице в социальной сети, пользователь не может быть точно уверен, что она никогда не попадет в руки мошенников. Например, бразильский исследователь по вопросам компьютерной безопасности показал, что существует возможность стать другом любого пользователя Facebook в течение 24 часов, используя методы социальной инженерии. В ходе эксперимента исследователь Нельсон Новаес Нето выбрал жертву и создал фальшивый аккаунт человека из ее окружения – ее начальника. Сначала Нето отправлял запросы на дружбу друзьям друзей начальника жертвы, а затем и непосредственно ее друзьям. Через 7,5 часа исследователь добился добавления в друзья от жертвы. Тем самым исследователь получил доступ к личной информации пользователя, которой тот делился только со своими друзьями.

Плечевой серфинг

Плечевой серфинг (англ. shoulder surfing) включает в себя наблюдение за личной информацией жертвы через ее плечо. Этот тип атаки распространен в общественных местах, таких как кафе, торговые центры, аэропорты, вокзалы, а также в общественном транспорте.

Опрос ИТ-специалистов в белой книге о безопасности показал, что:

- 85 % опрошенных признались, что видели конфиденциальную информацию, которую им не положено было знать;
- 82 % признались, что информацию, отображаемую на их экране, могли бы видеть посторонние лица;
- 82 % слабо уверены в том, что в их организации кто-либо будет защищать свой экран от посторонних лиц.

Обратная социальная инженерия

Об обратной социальной инженерии упоминают тогда, когда жертва сама предлагает злоумышленнику нужную ему информацию. Это может показаться абсурдным, но на самом деле лица, обладающие авторитетом в технической или социальной сфере, часто получают идентификаторы и пароли пользователей и другую важную личную информацию просто потому, что никто не сомневается в их порядочности. Например, сотрудники службы поддержки никогда не спрашивают у пользователей идентификатор или пароль; им не нужна эта информация для решения проблем. Однако многие пользователи ради скорейшего

устранения проблем добровольно сообщают эти конфиденциальные сведения. Получается, что злоумышленнику даже не нужно спрашивать об этом.

Примером обратной социальной инженерии может служить следующий простой сценарий. Злоумышленник, работающий вместе с жертвой, изменяет на ее компьютере имя файла или перемещает его в другой каталог. Когда жертва замечает пропажу файла, злоумышленник заявляет, что может все исправить. Желая быстрее завершить работу или избежать наказания за утрату информации, жертва соглашается на это предложение. Злоумышленник заявляет, что решить проблему можно, только войдя в систему с учетными данными жертвы. Теперь уже жертва просит злоумышленника войти в систему под ее именем, чтобы попытаться восстановить файл. Злоумышленник неохотно соглашается и восстанавливает файл, а по ходу дела крадет идентификатор и пароль жертвы. Успешно осуществив атаку, он даже улучшил свою репутацию, и вполне возможно, что после этого к нему будут обращаться за помощью и другие коллеги. Этот подход не пересекается с обычными процедурами оказания услуг поддержки и осложняет поимку злоумышленника.

Сетевое оборудование и его выбор

Существует огромное количество видов сетевого оборудования. Например, медиаконвертер, репитер, концентратор (хаб), коммутатор L2, коммутатор L3, беспроводная точка доступа, маршрутизатор, межсетевой экран и многое другое.

Одним из условных вариантов классификации является классификация по сложности настройки:

- домашнее оборудование (настраивать легче, но меньше возможностей настройки);
- профессиональное оборудование (настраивать сложнее, но больше возможностей настройки).

Также при выборе сетевого оборудования надо учитывать его производительность, которая может измеряться либо в пакетах в секунду (pps – packet per second), либо в битах в секунду (bps – bytes per second).

При выборе маршрутизатора необходимо учитывать:

- «домашнее» или профессиональное устройство;
- дополнительный функционал: Wi-Fi, шифрование и др.;
- производительность устройства;
- настольное или стоечное исполнение;
- пассивное или активное охлаждение.

При выборе коммутатора надо учитывать:

- скорость;
- количество портов;
- управляемое или неуправляемое устройство;
- L2 и L3;
- наличие аплинков (uplink);
- пассивное или активное охлаждение;
- настольное или стоечное исполнение;
- наличие PoE (Power over Ethernet);
- суммарную мощность PoE;

- производительность;
- поддержку STP;
- поддержку VLAN.

Командная строка Windows

Минимальный набор сетевых утилит из командной строки Windows, с которыми должен уметь работать системный администратор:

- **Ipconfig** – отобразить настройки сетевых подключений. Возможные ключи:
  - **/all** – отобразить все настройки,
  - **/release** – освободить аренду DHCP,
  - **/renew** – обновить аренду DHCP,
  - **/flushdns** – очистить кеш DNS;
- **ping** – диагностика сетевого соединения:
  - **–n** – количество отправляемых эхо-запросов,
  - **–t** – бесконечный ping;
- **tracert** – отобразить узлы на пути пакета и связь с ним;
- **pathping** – аналог tracert с более длительной проверкой связи с каждым узлом;
- **arp -a** – отобразить ARP-таблицу;
- **nslookup** – диагностика DNS.

Диагностика сетевых проблем

До появления проблемы надо иметь схему сети и порядок в сети. Также надо уметь различать предположения и факты, уметь пользоваться диагностическими утилитами командной строки и утилитами iperf, WinMTR и др.

Простой алгоритм диагностики:

1. Вспомнить схему сети.
2. Собрать все симптомы.
3. Определить, на каком уровне модели OSI находится проблема.
4. Выдвинуть теорию и проверить ее.

Идеология работы инженера

К идеологии работы инженера можно отнести клятву Гиппократа:

1. Обязательства перед учителями, коллегами и учениками.
2. Принцип непричинения вреда.
3. Обязательства оказания помощи больному (принцип милосердия).
4. Принцип заботы о пользе больного и доминанты интересов больного.
5. Принцип уважения к жизни.
6. Обязательство об отказе от хирургического вмешательства.
7. Обязательство об отказе от интимных связей с пациентами.
8. Обязательство личного совершенствования.
9. Врачебная тайна (принцип конфиденциальности).

Основные принципы

Основные принципы работы инженера:

1. Будь проактивным.
2. Надейся на лучшее, рассчитывай на худшее.
3. Делай резервное копирование.
4. Имей план отката.
5. Семь раз отмерь, один раз отрежь.
6. Любая теория должна быть проверена дважды.

Важно понимать, что работа может быть сделана хорошо, но клиент останется недоволен. И наоборот: работа может быть сделана плохо, но клиент останется доволен. Надо делать работу и хорошо, и так, чтобы клиент остался доволен. Если ты хочешь, чтобы тебя уважали, то ты должен сам уважать права и интересы других людей и стараться жить так, чтобы людям с тобой было хорошо.

Что дальше

Рекомендуемые книги:

- Таненбаум Э., Уэзеролл Д. Компьютерные сети.
- Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы.

Рекомендуемые видео:

- Созыкин А. Компьютерные сети.
- Семаев К. Видеокурсы по Linux.
- Курсы-по-ИТ.рф: Основы системного администрирования.
- Курсы-по-ИТ.рф: Диагностика сетевых проблем.
- Курсы-по-ИТ.рф: Беспроводные сети.
- Курсы-по-ИТ.рф: Видеокурсы по MikroTik.
- Курсы-по-ИТ.рф: Прочее.