Основы DevOps

КОДЕБАЙ
АКАДЕМИЯ

КОМПЬЮТЕРНЫЕ СЕТИ

ОГЛАВЛЕНИЕ

ОСНОВЫ КОМПЬЮТЕРНЫХ СЕТЕЙ

ОПРЕДЕЛЕНИЯ

Компьютерная сеть – это взаимосвязанные вычислительные устройства, которые могут обмениваться данными и совместно использовать ресурсы. Эти сетевые устройства используют систему правил, называемых *сетевыми протоколами*, для передачи информации посредством физических или беспроводных технологий. Разные протоколы зачастую описывают лишь разные стороны одного типа связи; взятые вместе, они образуют *стек протоколов*.

Сетевым узлом может быть оборудование передачи данных, такое как модем, коммутатор, маршрутизатор или терминальное оборудование, такое как два или более компьютеров и принтеров. Канал относится к среде передачи, соединяющей два узла. Связи могут быть физическими, такими как кабели или оптические волокна, или беспроводными, такими как Wi-Fi, 5G.

В работающей компьютерной сети узлы следуют набору правил или протоколов, которые определяют, как отправлять и получать данные. Архитектура компьютерной сети определяет конструкцию этих физических и логических компонентов. Он предоставляет спецификации для физических компонентов сети, функциональной организации, протоколов и процедур.

ИСТОРИЯ

Компьютерные сети были впервые созданы в конце 1950-х годов для использования в вооруженных силах и обороне. Первоначально они использовались для передачи данных по телефонным линиям и имели ограниченное коммерческое и научное применение.

Прорыв в области производства компьютерных компонентов и успехи в разработке передачи данных между персональными компьютерами привели к созданию глобальной сети Интернет.

В середине 80-х годов положение дел в локальных сетях стало кардинально меняться. Утвердились стандартные технологии объединения компьютеров в сеть — Ethernet, Arcnet, Token Ring.

Современные сетевые решения обеспечивают больше, чем возможность подключения. Сегодня они имеют решающее значение для цифровой трансформации и успеха бизнеса.

Базовые сетевые возможности стали более программируемыми, автоматизированными и безопасными.

КЛАССИФИКАЦИЯ

Существуют варианты классификации сетей по назначению и характеристикам.

ПО ТЕРРИТОРИАЛЬНОЙ РАСПРОСТРАНЁННОСТИ

LAN (ЛВС, Local Area Network) — локальная сеть, имеющая замкнутую инфраструктуру до выхода на поставщиков услуг; может описывать и маленькую офисную сеть, и сеть уровня большого завода, занимающего несколько сотен гектаров; иногда определяется как сеть «около шести миль (10 км) в радиусе»; локальные сети являются сетями закрытого типа, доступ к ним разрешён только ограниченному кругу пользователей, для которых работа в такой сети непосредственно связана с их профессиональной деятельностью;

CAN (Campus Area Network) — кампусная сеть, объединяет локальные сети близко расположенных зданий;

WAN (Wide Area Network) — глобальная сеть, покрывающая большие географические регионы, включающие в себя как локальные сети, так и прочие телекоммуникационные сети и устройства. Глобальные сети являются открытыми и ориентированы на обслуживание любых пользователей.

ПО АРХИТЕКТУРЕ

Клиент-серверная - в этом типе компьютерной сети узлы могут быть серверами или клиентами. Серверные узлы предоставляют клиентским узлам какие-то сервисы, а также могут управлять поведением клиентских узлов. Например, некоторые компьютерные устройства в корпоративных сетях хранят данные и параметры конфигурации. Эти устройства являются серверами в сети. Клиенты могут получить доступ к этим данным, отправив запрос на серверную машину.

Пиринговая - в пиринговой архитектуре подключенные компьютеры имеют равные полномочия и привилегии. Нет центрального сервера для координации. Каждое устройство в компьютерной сети может действовать как клиент или сервер

ПО ТИПУ СЕТЕВОЙ ТОПОЛОГИИ

Расположение узлов и связей называется топологией сети. Их можно настроить по-разному, чтобы получить разные результаты.

Шина - каждый узел связан только с одним другим узлом. Передача данных по сетевым соединениям происходит в одном направлении.

Кольцо - каждый узел связан с двумя другими узлами, образуя кольцо. Данные могут передаваться в двух направлениях. Однако отказ одного узла может вывести из строя всю сеть.

Звезда - узел центрального сервера связан с несколькими клиентскими сетевыми устройствами. Эта топология работает лучше, поскольку данные не должны проходить через каждый узел. Это также более надежно.

Ячейки - каждый узел связан со многими другими узлами. В полностью ячеистой топологии каждый узел соединен с каждым другим узлом в сети.

ПО ТИПУ СРЕДЫ ПЕРЕДАЧИ

Проводная - телефонный провод, коаксиальный кабель, витая пара, волоконно-оптический кабель.

Беспроводная - передача информации по радиоволнам в определённом частотном диапазоне.

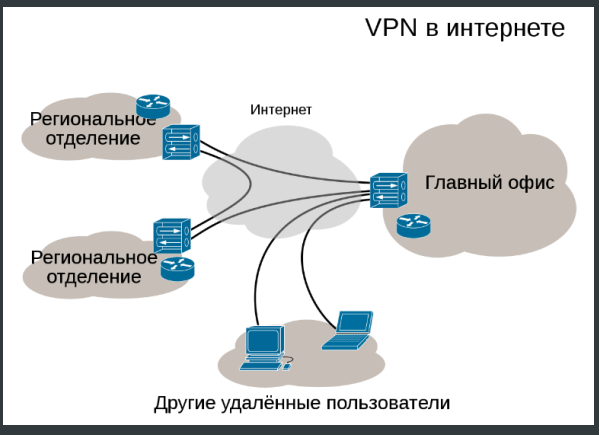
ПО СКОРОСТИ ПЕРЕДАЧИ

Низкоскоростная (до 10 Мбит/с),

Среднескоростная (до 100 Мбит/с),

Высокоскоростная (свыше 100 Мбит/с);

ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ



VPN (англ. Virtual Private Network «виртуальная частная сеть») — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например Интернет) или сети провайдера.

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 (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

ОБЛАЧНЫЕ СЕТИ

Сети поставщиков услуг позволяют клиентам арендовать сетевые мощности и функциональные возможности у поставщика. Поставщики сетевых услуг могут состоять из телекоммуникационных компаний, операторов данных, провайдеров беспроводной связи, интернет-провайдеров и операторов кабельного телевидения, предлагающих высокоскоростной доступ в Интернет.

Концептуально облачную сеть можно рассматривать как глобальную сеть, инфраструктура которой предоставляется облачной службой. Некоторые или все сетевые возможности и ресурсы организации размещаются на общедоступной или частной облачной платформе и предоставляются по запросу. Эти сетевые ресурсы могут включать в себя виртуальные маршрутизаторы, брандмауэры, полосу пропускания и ПО для управления сетью, а также другие инструменты и функции, доступные по мере необходимости.

Сегодня предприятия используют облачные сети для ускорения выхода на рынок, увеличения масштаба и эффективного управления затратами. Модель облачной сети стала стандартным подходом к созданию и развертыванию приложений для современных предприятий.

МОДЕЛИ OSI И TCP/IP

Открытой системой может быть названа любая система (компьютер, вычислительная сеть, ОС, программный пакет, другие аппаратные и программные продукты), которая построена в соответствии с открытыми спецификациями.

Сети поддерживают концепцию открытой системы – они построены на основе открытых спецификаций, открыты для расширения и взаимодействия (IETF RFC).

МОДЕЛЬ OSI

Модель взаимодействия открытых систем OSI (Open Systems Interconnection) — базовая основополагающая модель, описывающая структуру передачи данных от одного приложения другому.

Посредством данной модели различные сетевые устройства могут взаимодействовать друг с другом.

Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определённые функции при таком взаимодействии.

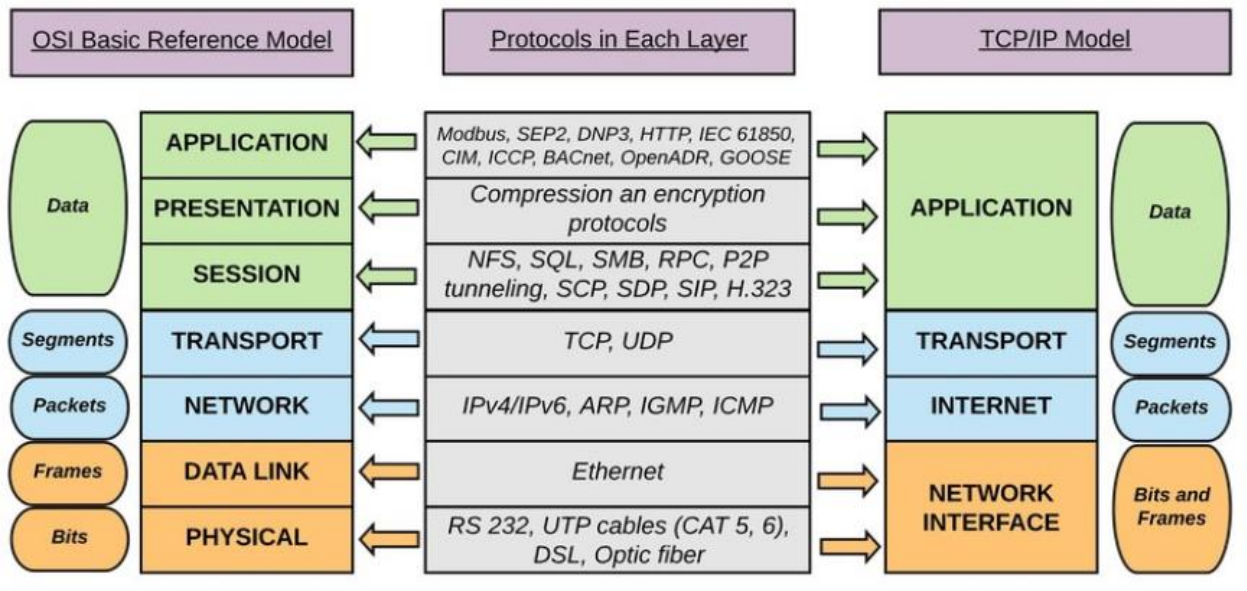
Уровень (layer)		Тип данных (PDU)	Функции	Примеры	Оборудование
Host	**7. Прикладной (application)**	Данные	Доступ к сетевым службам	HTTP, FTP, WebSocket	Хосты (клиенты сети), Межсетевой экран
	6. Представления (presentation)		Представление и шифрование данных	ASCII, JPEG, MIDI	
	5. Сеансовый (session)		Управление сеансом связи	RPC, PAP, L2TP	
	4. Транспортный (transport)	Сегменты Датаграммы	Прямая связь между конечными пунктами и надёжность	TCP, UDP	
Media	**3. Сетевой (network)**	Пакеты	Определение маршрута и логическая адресация	IPv4, IPv6, IPsec, ICMP	Маршрутизатор, Межсетевой экран
	2. Канальный (data link)	Кадры (frame)	Физическая адресация	Ethernet, PPP	Коммутатор, точка доступа

	1. Физический (physical)	Биты	Работа со средой передачи, сигналами и двоичными данными	Витая пара коаксиал, оптоволокно, радиоканал, USB	Концентратор, Повторитель

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 протоколом передачи. Наборы правил, решающих задачу по передаче данных, составляют стек протоколов передачи данных.



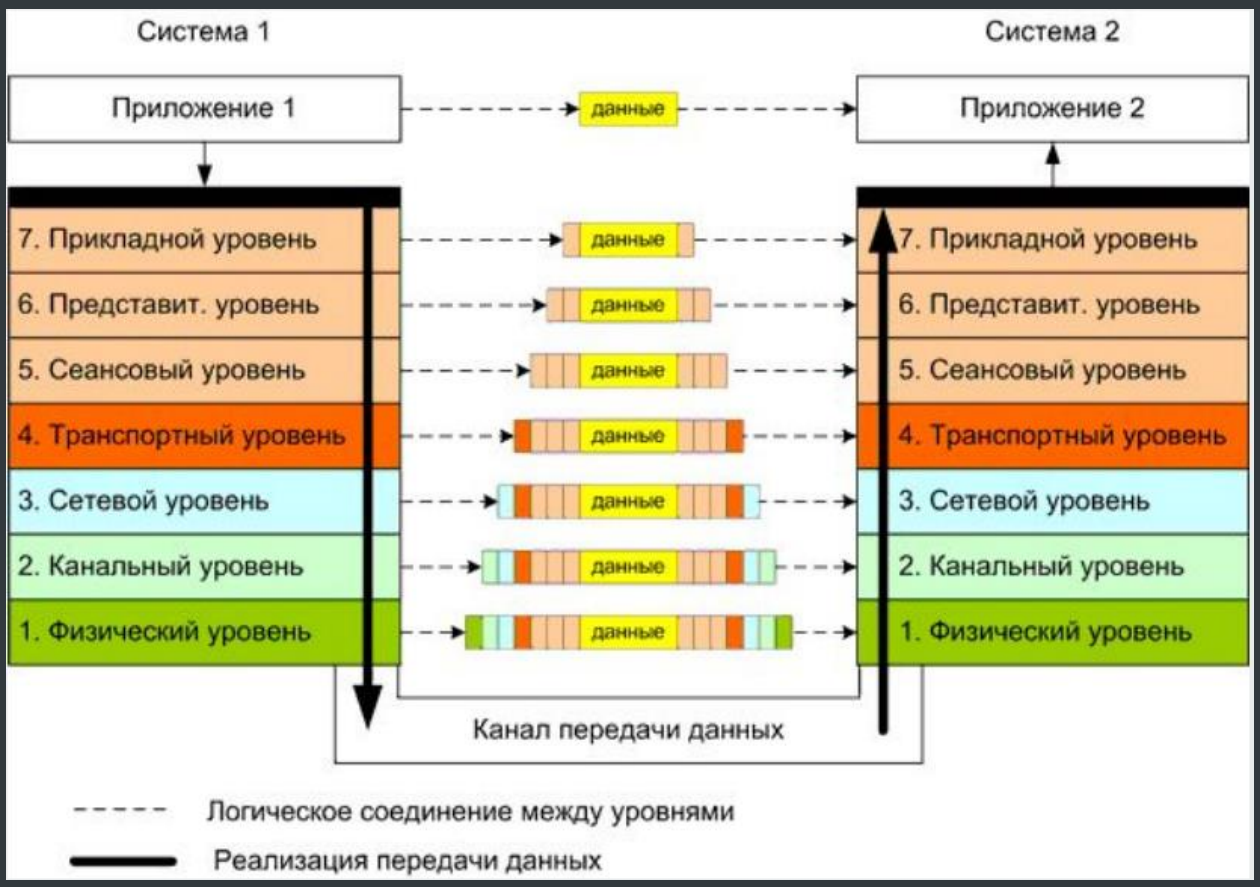
ИНКАПСУЛЯЦИЯ

OSI состоит из двух основных частей:

- абстрактная модель сетевого взаимодействия (семиуровневая модель)
- набор специализированных протоколов взаимодействия.

Протоколы работают в стеке – протокол, располагающийся на уровне выше, работает «поверх» нижнего, используя механизмы инкапсуляции(вложения).

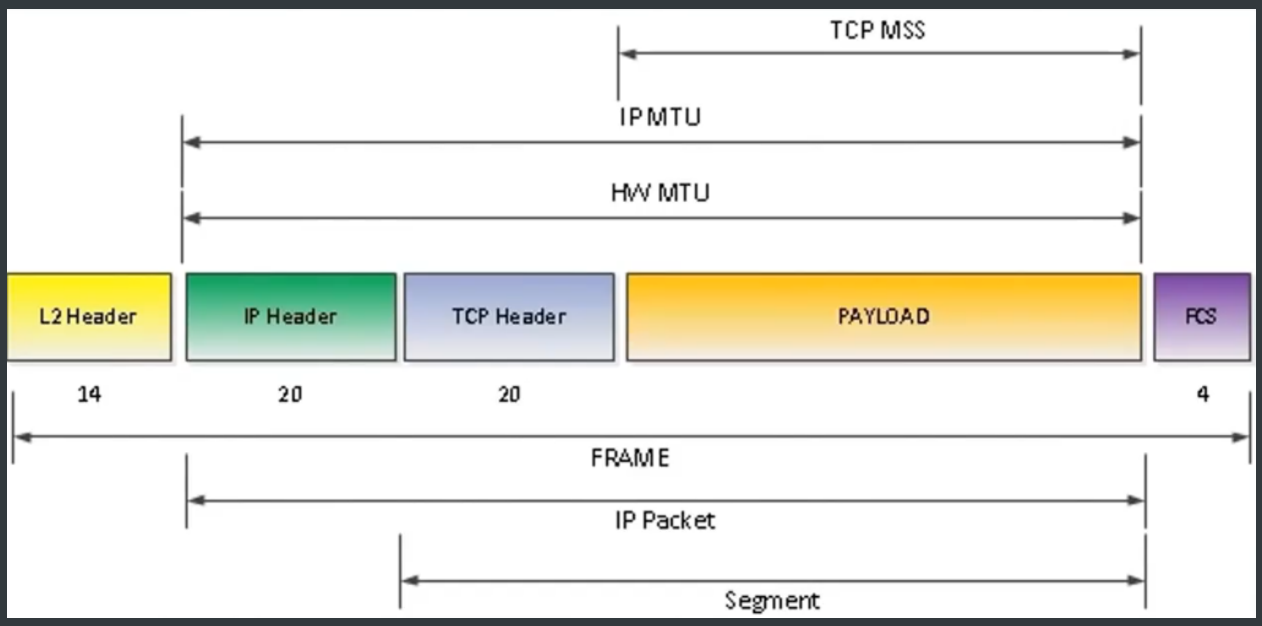
Интерфейсы – правила и процедуры, которые отвечают за взаимодействие между соседними уровнями.



MTU (MAXIMUM TRANSMISSION UNIT)

Максимальный размер полезного блока данных, который может быть передан протоколом без фрагментации. 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 — mtu, hw mtu, system mtu
L3 — ip mtu (ip заголовок учитывается), mtu routing
L4 — tcp mss



В Linux hw mtu и ip mtu как правило совпадают. В Cisco в hw mtu входят заголовки и суффикс, поэтому он больше.

АДРЕСАЦИЯ В СЕТИ

ТИПЫ АДРЕСОВ СТЕКА TCP/IP

В стеке TCP/IP используется три типа адресов:

- Локальные (аппаратные) адреса;
- Сетевые адреса (IP-адреса);
- Символьные (доменные)имена;

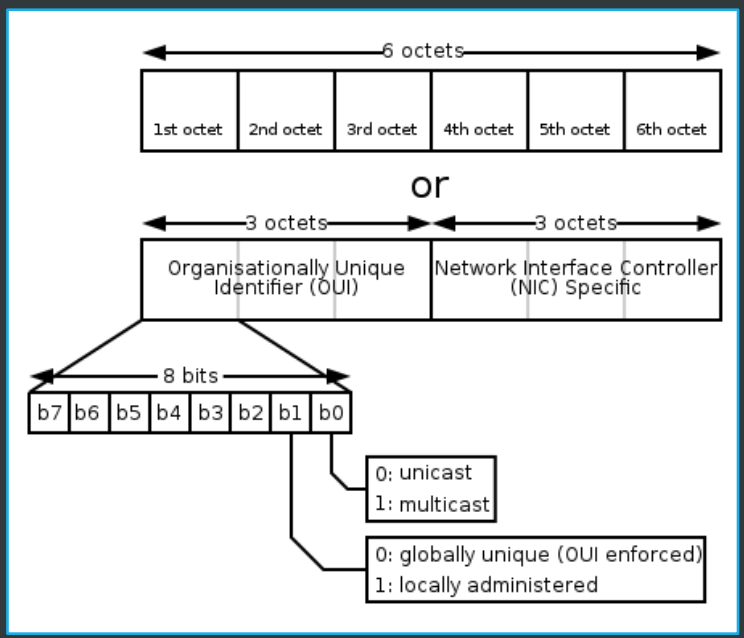
Все эти типы адресов присваиваются узлами составной сети независимо друг от друга.

MAC-АДРЕС

MAC-адрес – уникальный идентификатор, присваиваемый каждой единице сетевого оборудования или некоторым их интерфейсам.

MAC-адреса назначаются производителями оборудования и являются уникальными, так как управляются централизованно.

Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байт, например 11-A0-17-3D-BC-01.



IP АДРЕС

IP-адрес (IP от англ. Internet Protocol) — цифровой идентификатор, присваиваемый устройству, которое работает в условиях публичной или локальной сети на основе стека протоколов TCP/IP

IP-адрес IPv4 имеет 32-битную (4 байта) структуру.

Он разделён на 4 части, каждая из которых состоит из 8 бит (1 байт) и называется октетом. Каждый бит IP-адреса – цифра двоичной системы.

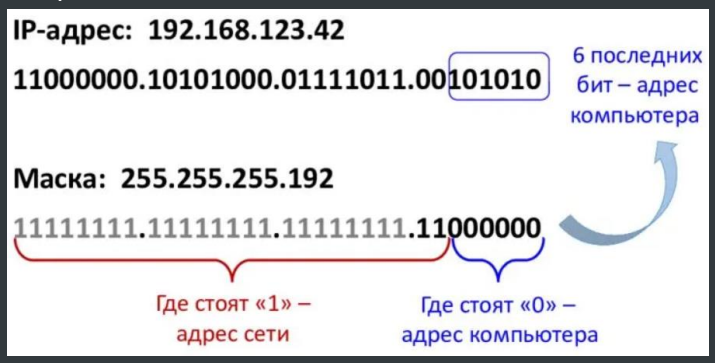
При преобразовании октета с двоичной системы в десятеричную получается одно число со значением от 0 до 255.

МАСКА СЕТИ

Устройства различают части IP-адреса при помощи маски подсети – 32-битной строки, разделённой на 4 октета, как и IP-адрес.

При установке соединения каждый октет IP-адреса сопоставляется с октетом маски подсети.

По умолчанию в стандартной домашней сети маска подсети имеет вид: 255.255.255.0.



В примере маска IP-адреса указана в десятичном представлении и содержит числа «255» и «0». Первое отвечает за идентификацию сети, а второе за обозначение конечного узла.

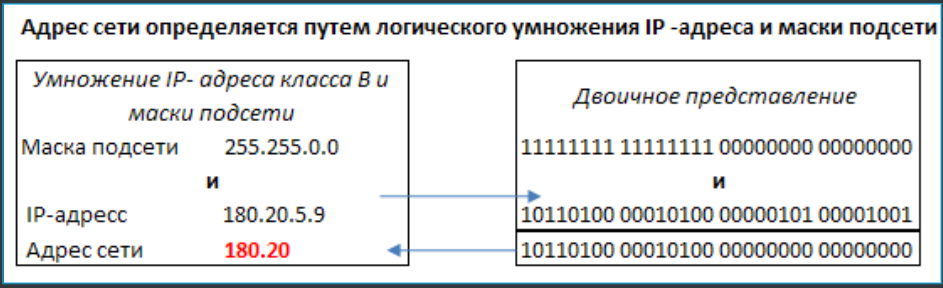
ПРИМЕР НАХОЖДЕНИЯ СЕТИ

Устройства в сети использует маску подсети для нахождения адреса сети по адресу IP при помощи особого метода, который называется логическим умножением.

Логическое умножение производится так: маршрутизатор просматривает адрес IP и маску подсети в двоичном коде.

Затем биты в маске подсети умножаются на соответствующие биты в адресе IP, после чего определяется адрес сети.

Логическое умножение	
Комбинация битов	Результат
1 и 1	1
1 и 0	0
0 и 0	0



КЛАССОВАЯ АДРЕСАЦИЯ

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

Класс	Первые биты	Распределение байт (C - сеть, X-хост)	Число возможных адресов сетей	Число возможных адресов хостов	Маска подсети
A	0	C.X.X.X	128	16 777 216	255.0.0.0
B	10	C.C.X.X	16 386	65 536	255.255.0.0
C	110	C.C.C.X	2 097 154	256	255.255.255.0
D	1110	Групповой адрес			
E	1111	Зарезервировано			

Применение этого метода не позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку невозможно применение различных масок подсетей к различным подсетям.

ПРИВАТНЫЕ IP СЕТИ

В каждом классе выделен диапазон для приватных IP адресов. Такие адреса предназначены для применения в локальных сетях, распределение таких адресов никем не контролируется.

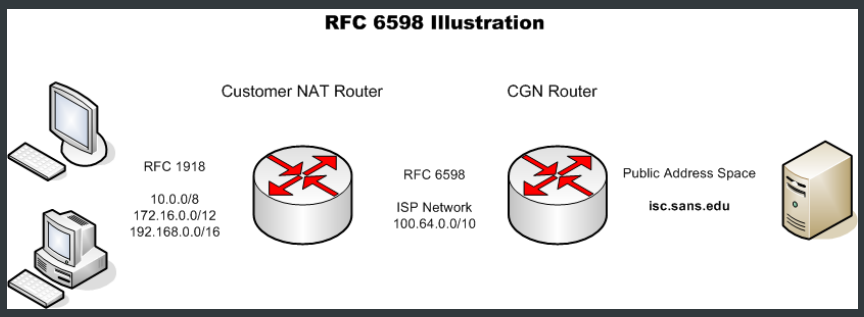
Диапазоны частных (private) IP-адресов:

10.0.0.0—10.255.255.255
172.16.0.0—172.31.255.255
192.168.0.0—192.168.255.255

В связи с дефицитом свободных IP-адресов, провайдеры могут раздавать своим абонентам внутрисетевые адреса.

Трансляция сетевых адресов (NAT) - технология, позволяющая маршрутизатору, пропуская идущий из локальной сети пакет, заменять адрес отправителя своим. Когда маршрутизатор получает ответ от сервера, он по таблице открытых соединений восстанавливает адресата и ретранслирует ему ответ.

CGNAT – отвечает за ретрансляцию сетевых адресов и портов, позволяя работать с одним «белым» адресом формата IPv4 сразу нескольким пользователям.



СПЕЦИАЛЬНЫЕ IP-АДРЕСА

Специальные IP-адреса

0.0.0.0 – текущий хост (сеть)

255.255.255.255 – все хосты в текущей сети (ограниченный широковещательный адрес)

127.0.0.0 – обратная петля (loopback)
- Сеть для тестирования
- Данные не передаются в сеть, а приходят обратно
- 127.0.0.1 – localhost (текущий компьютер)

169.254.0.0 – Link-local адреса
- Назначаются ОС хоста автоматически, если недоступна другаяIP конфигурация
- Могут использоваться в пределах локальной сети

IPV6

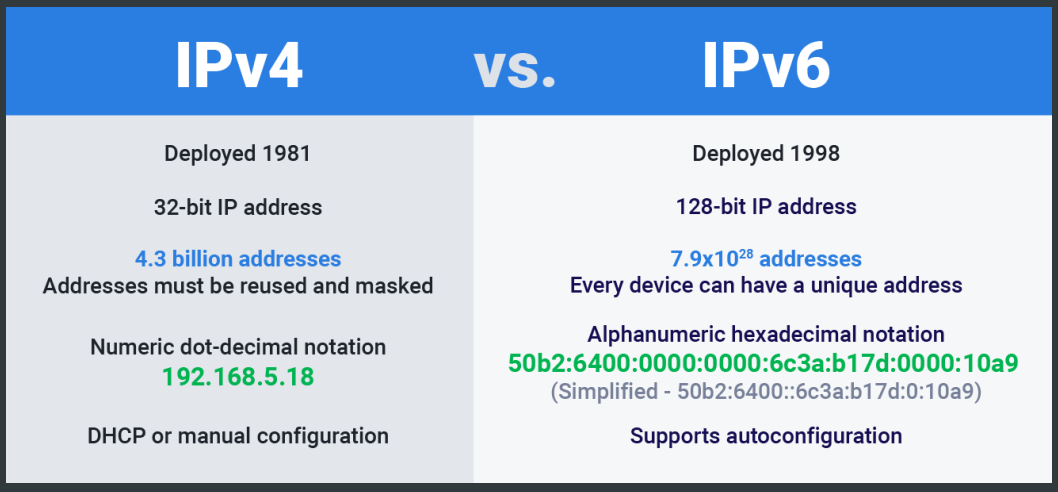
IPv6 (англ. Internet Protocol version 6) — новая версия интернет-протокола (IP), призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при её использовании в Интернете, за счёт целого ряда принципиальных изменений. Протокол был разработан IETF. Длина адреса IPv6 составляет 128 бит, в отличие от адреса IPv4, длина которого равна 32 битам.

СРАВНЕНИЕ С IPV4

Большое адресное пространство было введено ради иерархичности адресов (это упрощает маршрутизацию). Тем не менее, 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 и указанием величины MTU следующего канала, в который этому пакету не удалось войти. В IPv4 размер MTU в ICMP-пакете не указывался, и отправителю требовалось осуществлять подбор MTU техникой Path MTU discovery.
- Из IP-заголовка исключена контрольная сумма. С учётом того, что канальные (Ethernet) и транспортные (TCP и UDP) протоколы имеют свои контрольные суммы, ещё одна контрольная сумма на уровне IP воспринимается как излишняя.



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.

Автоконфигурация - при инициализации сетевого интерфейса ему назначается локальный IPv6-адрес, состоящий из префикса fe80::/10 и идентификатора интерфейса, размещённого в младшей части адреса. В качестве идентификатора интерфейса часто используется 64-битный расширенный уникальный идентификатор EUI-64, часто ассоциируемый с MAC-адресом. Локальный адрес действителен только в пределах сетевого сегмента канального уровня и используется для обмена информационными ICMPv6-пакетами.

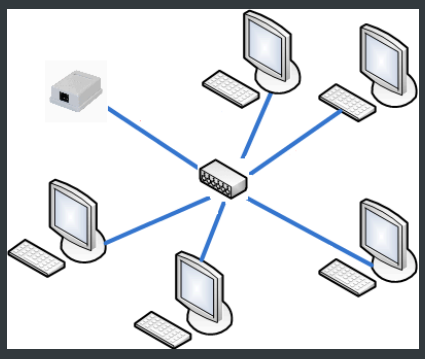
Для настройки других адресов узел может запросить информацию о настройках сети у маршрутизаторов, отправив ICMPv6-сообщение «Router Solicitation» на групповой адрес маршрутизаторов. Маршрутизаторы, получившие это сообщение, отвечают ICMPv6-сообщением «Router Advertisement», в котором может содержаться информация о сетевом префиксе, адресе шлюза, адресах рекурсивных DNS серверов[9], MTU и множестве других параметров. Объединяя сетевой префикс и идентификатор интерфейса, узел получает новый адрес. Для защиты персональных данных идентификатор интерфейса может быть заменён на псевдослучайное число.

Для большего административного контроля может быть использован DHCPv6, позволяющий администратору маршрутизатора назначать узлу конкретный адрес.

Для провайдеров может использоваться функция делегирования префиксов клиенту, что позволяет клиенту просто переходить от провайдера к провайдеру, без изменения каких-либо настроек.

КОММУТАЦИЯ ПАКЕТОВ

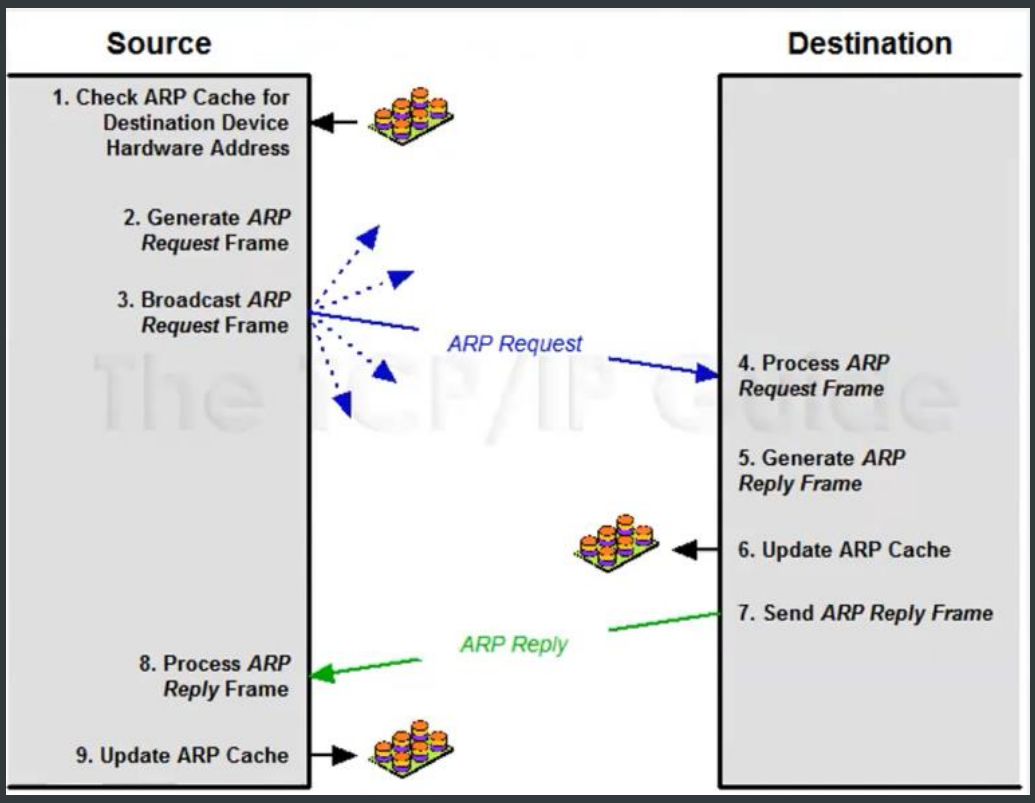
Сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами. Сообщения могут иметь произвольную длину, от нескольких байт до многих мегабайт. Напротив, пакеты обычно тоже могут иметь переменную длину, но в узких пределах, например от 46 до 1500 байт (EtherNet).



Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета узлу назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения.

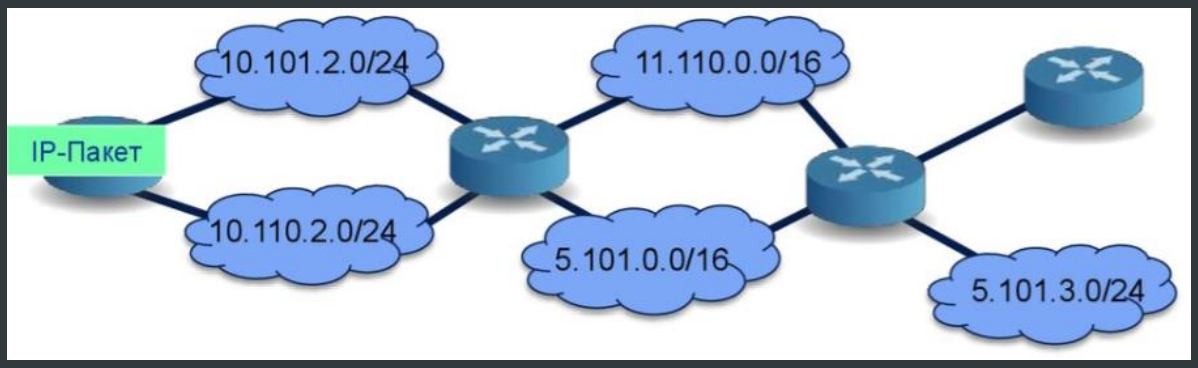
РАЗРЕШЕНИЕ АДРЕСОВ

Протокол ARP (Address Resolution Protocol) служит для разрешения адресов (поиска соответствия mac-адресов и IP-адресов) в пределах одного L2-сегмента (L2- домена).



IP МАРШРУТИЗАЦИЯ

Процесс выбора пути для передачи сообщения в IP сети.



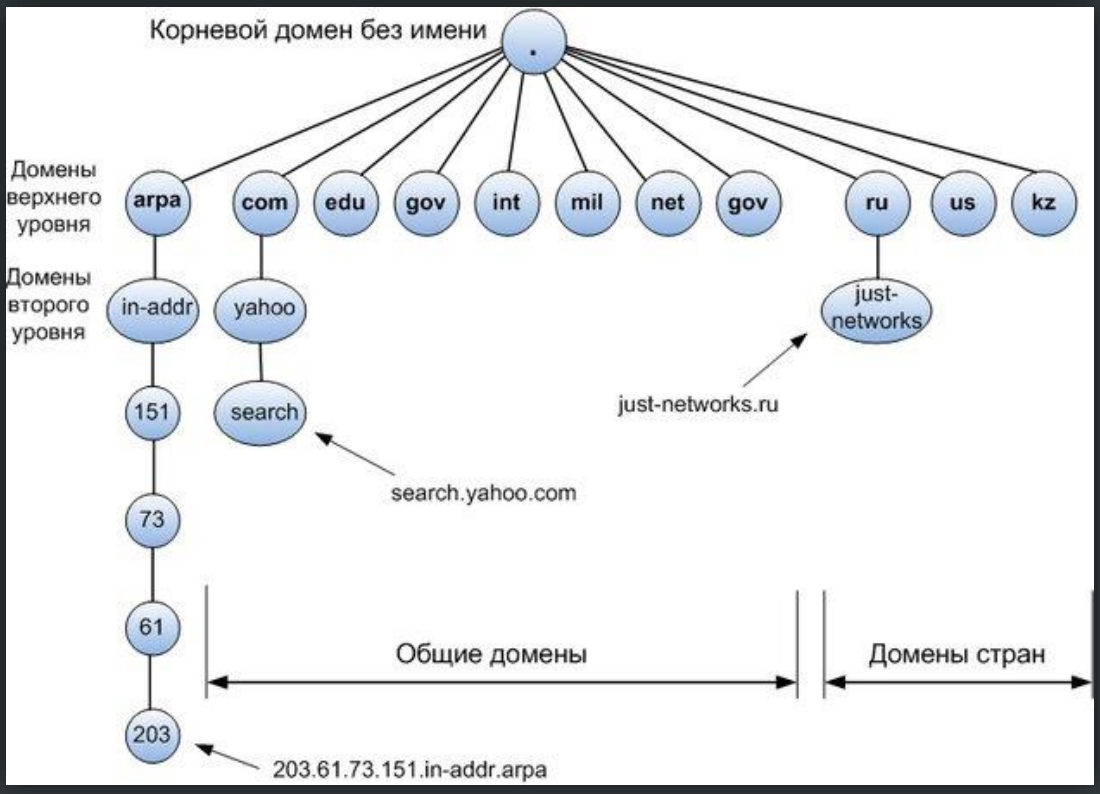
Статическая маршрутизация — вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора.

Динамическая маршрутизация — вид маршрутизации, при котором таблица маршрутизации редактируется служебными программами.

Протоколы ДМ: RIP, OSPF, IS-IS, EIGRP, BGP

DOMAIN NAME SYSTEM

Domain Name System («система доменных имён») — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста, получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене (SRV-запись).



Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу.

DNS обладает следующими характеристиками:

Распределённость администрирования. Ответственность за разные части иерархической структуры несут разные люди или организации.

Распределённость 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.

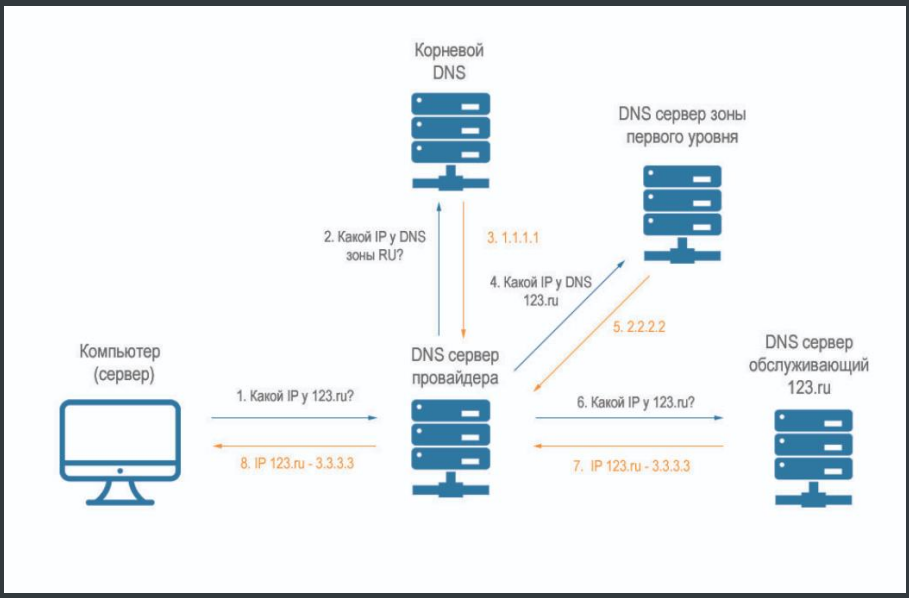
Кэширование информации. Узел может хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.

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, разделённые как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

РАБОТА DNS

Рекурсивный запрос — в ответ на такой тип запроса сервер обязан вернуть «готовый результат», то есть IP-адрес, либо пустой ответ и код ошибки NXDOMAIN



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

НАИБОЛЕЕ ВАЖНЫЕ ТИПЫ DNS-ЗАПИСЕЙ

A (address record) связывает имя хоста с адресом протокола IPv4.

AAAA (IPv6 address record) связывает имя хоста с адресом протокола IPv6.

CNAME (canonical name record) или каноническая запись имени (псевдоним) используется для перенаправления на другое имя.

MX (mail exchange) или почтовый обменник указывает сервер(ы) обмена почтой для данного домена.

NS (name server) указывает на DNS-сервер для данного домена.

PTR (pointer) обратная DNS-запись, связывает IP-адрес хоста с его каноническим именем.

SOA (Start of Authority) или начальная запись зоны указывает, на каком сервере хранится эталонная информация о данном домене, содержит контактную информацию лица, ответственного за зону, тайминги (параметры времени) кеширования зонной информации и взаимодействия DNS-серверов.

SRV (server selection) указывает на серверы для сервисов.

УТИЛИТЫ LINUX ДЛЯ РАБОТЫ С СЕТЬЮ

СЕТЕВЫЕ УТИЛИТЫ PING, TELNET, TRACEROUTE

ping - простой инструмент для диагностики сети. Она позволяет проверить доступен удаленный хост или нет. Проверяет, может ли хост отвечать на сетевые запросы с помощью протокола ICMP

```
$ ping опции адрес_узла
```

Telnet - позволяет соединиться с удаленным портом любого компьютера и установить интерактивный канал связи, например, для передачи команд или получения информации. Можно сказать, что это универсальный браузер в терминале, который умеет работать со множеством сетевых протоколов

```
$ telnet опции хост порт
```

Traceroute - утилита, для отслеживания маршрута пакетов. Пакет отправляет сообщение на компьютер-отправитель со всех шлюзов между источником и пунктом назначения.

Команда traceroute использует UDP пакеты. Она отправляет пакет с TTL=1 и смотрит адрес ответившего узла, дальше TTL=2, TTL=3 и так пока не достигнет цели. Каждый раз отправляется по три пакета и для каждого из них измеряется время прохождения. Пакет отправляется на случайный порт, который, скорее всего, не занят. Когда утилита traceroute получает сообщение от целевого узла о том, что порт недоступен трассировка считается завершенной

УТИЛИТА IP

ip - популярная современная утилита для просмотра сетевых подключений в системе Linux. Позволяет посмотреть сетевые интерфейсы, IP адреса, маску сети, таблицу маршрутизации и многое другое

```
$ ip [опции] объект команда [параметры]
```

`Объект` - тип данных, с которым надо будет работать, например: адреса, устройства, таблица arp, таблица маршрутизации и так далее;

`Команды` - какое-либо действие с объектом;

`Параметры` - параметры для команды

Опции:

`-v, -Version` - только вывод информации об утилите и ее версии.

`-h, -human` - выводить данные в удобном для человека виде.

`-s, -stats` - включает вывод статистической информации.

`-d , details` - показывать ещё больше подробностей.

`-r, -resolve` - определять имена хостов с помощью DNS.

`-br, -brief` - выводить только базовую информацию для удобства чтения

Объекты:

`Address` или `a` - сетевые адреса.

`Link` или `l` - физическое сетевое устройство.

`Neighbour` или `neigh` - просмотр и управление ARP.

`Route` или `r` - управление маршрутизацией.

`Rule` или `ru` - правила маршрутизации.

`Tunnel` или `t` - настройка туннелирования

Команды:

```
add, change, del или delete, flush, get, list или show, monitor,
replace, restore, save, set и update
```

Если команда не задана, по умолчанию используется `show` показать

```
ip -br a show
ip link show
ip link set dev интерфейс down/up
ip link set mtu 4000 dev enp0s3
ip neigh show
ip neigh flush
ip route show
ip route add подсеть/маска via шлюз
```

СЕТЕВЫЕ УТИЛИТЫ NETSTAT/SS

netstat - устаревший аналог ss, вместо подсистемы ядра здесь используется файловая система proc, а также данные выводятся немного в другом формате.

ss - позволяет вывести все открытые локальные сокеты и проанализировать какие программы их используют. Можно отдельно выводить UDP, TCP и Unix сокеты, а также смотреть к каким удалённым сокетам подключены программы компьютера.

```
$ ss опции [фильтр_состояния] [фильтр_адреса]
```

Опции:

`-r` - Resolve определять сетевые имена адресов с помощью DNS.

`-a` - All отобразить все сокеты (открытые соединения).

`-l` - Listening показать только прослушиваемые сокеты.

`-p` - Processes, показать процессы, использующие сокет.

`-i` - Internal, посмотреть внутреннюю информацию TCP.

`-0, --packet` - только PACKET сокеты.

`-t, --tcp` - TCP сокеты.

`-u, --udp` - UDP сокеты.

`-d, --dhcp` - DHCP сокеты.

`-x, --unix` - UNIX сокеты.

УТИЛИТА TCPDUMP

tcpdump - консольный сетевой анализатор, позволяющий посмотреть трафик, проходящий через сетевой интерфейс. Можно анализировать содержимое сетевых пакетов и их тип.

```
$ tcpdump опции -i интерфейс фильтры
```

`Фильтры`:

`host` - имя хоста;

`ip` - ip адрес;

`proto` - протокол;

`net` - адрес сети или подсети;

`port` - адрес порта;

`src` - параметр, касающийся отправителя;

`dst` - параметр, касающейся получателя;

Доступны такие протоколы: `ether, fddi, tr, wlan, ip, ip6, arp, rarp, decnet, tcp` и `udp`.

УТИЛИТА NC

nc - утилита позволяет создавать новые сетевые сокеты и подключаться к существующим по сети. Это может понадобиться для тестирования работы сети или приложений.

```
$ nc -параметры адрес порт(ы)
```

Параметры:

`-i` задержка – добавить задержку между отправкой строк или сканированием портов. Задаётся в секундах;

`-l` – режим прослушивания. Используется с указанием порта;

`-n` – Работать с IP-адресами напрямую, не задействуя DNS, также отключить поиск портов;

`-P` имя_пользователя – указать имя пользователя для подключения к прокси;

`-x` адрес:порт – указать адрес и порт для подключения к прокси;

`-p` порт – указать номер порта. В большинстве случаев порт считывается без указания параметра;

`-U` – использовать сокет домена UNIX (для межпроцессного взаимодействия);

`-u` – использовать протокол UDP, по умолчанию используется TCP;

`-v` – подробный режим. Используется при сканировании портов;

`-W` количество_пакетов – закрыть соединение после получения определённого количества пакетов;

`-w` таймер – включить таймер для ограничения времени соединения. Задаётся в секундах;

`-z` – отключить отправку данных. Используется при сканировании портов.