1 Понятие системного администрирования

Системное администрирование призвано решать широкий круг задач, связанных с созданием и поддержкой в работоспособном состоянии сложной информационной системы, включающей различные аппаратные и программные средства. В настоящее время практически невозможно отделить сетевое администрирование от администрирования вообще. Системным администрированием занимается *системный администратор*

Существуют две базовые стратегии администрирования:

1. *Распределенное* – нет единого центра, регламентирующего политику администрирования
2. *Централизованное* – политика администрирования регламентируется единым центром

Так как основная часть повседневной работы системного администратора связана с ПО, нужно кратко оговорить ряд моментов, касающихся этого самого ПО. В первую очередь речь идет об установке и настройке (плюс удалении) ПО.

Установка ПО может происходить по -разному:

1. Просто копирование исполняемых и вспомогательных файлов «вручную» безо всяких проверок.
2. Компиляция исходных текстов, проверка зависимостей и копирование файлов с помощью стандартного набора специальных консольных команд.
3. Автоматическое, но контролируемое, выполнение проверок, копирование подготовленных файлов и осуществление других действий с помощью специальной программы, внешней по отношению к устанавливаемому ПО, – обычно называемой пакетным менеджером (packet manager).
4. Выполнение аналогичных действий с помощью специальной программы, частично или полностью интегрированной в устанавливаемое ПО, – называемой установщиком (installer).

Настройка, заключается в конфигурировании, то есть в изменении значений обязательных и опциональных параметров со значений по умолчанию на нужные значения. Часто есть возможность выполнять конфигурирование в режиме диалога – с помощью визарда или, по-другому, мастера (wizard).

2 Выбор программного обеспечения администратором

Базовая классификация ПО заключается в его разделении на:

1. Системное – реализует функционал различных подсистем ОС и позволяет контролировать ОС (само по себе «никому не нужно»).
2. Прикладное – позволяет решать конкретные прикладные задачи («интересно» пользователям).
3. Инструментальное – позволяет разрабатывать и тестировать другое ПО.
4. Встраиваемое (embedded) – позволяет управлять некоторым устройством («неотделимо» от устройства для которого предназначено).

Пять основных критериев выбора ПО:

1. Степень соответствия требованиям (сугубо техническим и другим).
2. Стоимость (приобретения, освоения, использования).
3. Доступность (сложность приобретения и освоения).
4. Эргономичность (сложность использования).
5. Качество технической поддержки (при возникновении проблем).

Также нужно понимать обобщённую цепь вызова подпрограмм, или «внутренний мир» ПО:

//////

При выборе сетевого программного обеспечения надо в первую очередь учитывать следующие факторы:

1. какую сеть оно поддерживает: одноранговую сеть, сеть на основе сервера или оба этих типа;
2. какое максимальное количество пользователей допускается (лучше брать с запасом не менее 20%);
3. какое количество серверов можно включить и какие типы серверов возможны;
4. какова совместимость с разными операционными системами и разными компьютерами, а также с другими сетевыми средствами;
5. каков уровень производительности программных средств в различных режимах работы;
6. какова степень надежности работы, каковы разрешенные режимы доступа и степень защиты данных;
7. и, возможно, главное - какова стоимость программного обеспечения.

Еще до установки сети необходимо решить вопрос об управлении сетью.

3 Установка программного обеспечения администратором

Установка ПО может происходить по-разному:

1. Просто копирование исполняемых и вспомогательных файлов «вручную» без всяких проверок.
2. Компиляция исходных текстов, проверка зависимостей и копирование файлов с помощью стандартного набора специальных консольных команд.
3. Автоматическое, но контролируемое, выполнение проверок, копирование подготовленных файлов и осуществление других действий с помощью пакетного менеджера (packet manager).
4. Выполнение аналогичных действий с помощью специальной программы, частично или полностью интегрированной в устанавливаемое ПО, – называемой установщиком (installer).

Некоторые компании разрабатывают более сложные программные средства для автоматизации масштабной установки ПО на большое количество компьютеров (automated software deployment). Примером может служить IBM Tivoli.

4 Сопровождение программного обеспечения администратором

Сопровождение ПО - это одна из фаз жизненного цикла программного обеспечения, следующая за фазой передачи ПО в эксплуатацию. В ходе сопровождения в программу вносятся изменения, с тем, чтобы исправить обнаруженные в процессе использования дефекты и недоработки, а также для добавления новой функциональности, с целью повысить удобство использования и применимость ПО.

Системный администратор сам должен владеть навыками тестирования ПО, аппаратного обеспечения и КС. В том числе оценивать их производительность. Правда таковое тестирование во многом отличается от тестирования, выполняемого разработчиками.

Три основные стратегии поиска и устранения неисправностей (troubleshooting):

1. Сверху вниз (top-down) – начинать с прикладного уровня и постепенно «спускаться» на физический.
2. Снизу-вверх (bottom-up) – начинать с физического уровня и постепенно «подниматься» на прикладной.
3. «Разделяй и властвуй» (divide-and-conquer) – начинать с наиболее вероятного уровня и «расширяться» в двух направлениях.

Эти стратегии можно применять не только к КС, а к любым информационным системам.

Также следует различать сборки (builds), версии (versions) и релизы (releases).

- Под сборкой понимают исполняемые файлы, полученные в результате очередной компиляции.
- Под версиями понимают сборки, которым присвоены номера (или названия).
- Под релизами понимают версии, предназначенные для распространения (distribution).

Системные администраторы часто сталкиваются с «недоработанными» релизами, относящимися к финальным этапам стадии разработки.

5. Маршрутизаторы Cisco как специализированное сетевое оборудование

На февраль 2022 маршрутизаторы CISCO делят на шесть основных целевых категорий:

1. Branch
2. WAN aggregation
3. Service provider
4. Industrial
5. Virtual
6. Small business

и множество серий.

В первом приближении маршрутизационные платформы от Cisco можно разделить на:

- менее производительные
- более производительные
- плюс появившиеся совсем недавно специализированные платформы.

Основу сегментов рынка SOHO (small office/home office) составляют различные серии ISRs (Integrated Services Routers). Аналогичные pre-ISR-серии обобщенно известны как access routers. Конечно же, такие маршрутизаторы массово применяют и на периферии корпоративных сетей.

Высокопроизводительные серии позиционируют как основу для наиболее требовательных к сетевым ресурсам сегментов рынка, а именно: компьютерных систем с большим числом сервисов, инфраструктуры провайдеров, центров обработки данных.

Многие серии представляют собой гибриды с коммутаторами. Примером может служить формально относящаяся к коммутаторам линейка Nexus.

В качестве лабораторной базы для первоначального обучения обычно используют относительно недорогие серии ISRs различных поколений.

Традиционно, программа CCNA ориентирована на «младшие» модели ISRs для сегмента рынка SMB (small/medium business) (или «старшие» модели ISRs для сегмента рынка SOHO).

Применительно к собственно ISRs это 2811, к ISRs G2 это 2901 (вроде стоят в лаборатории CISCO 5 корпуса), к ISRs 4K это 4331 (или 1841, 1941, 4221 соответственно).

6. Модули маршрутизаторов CISCO

Маршрутизаторы Cisco (исключая самые дешевые) изначально разрабатывают как модульные (modular). На так называемое шасси (chassis) с уже установленным базовым набором сетевых интерфейсов существует возможность доустанавливать различные количественно и качественно различающиеся модули. При этом, в первом приближении, выделяют пять групп модулей:

1. Интерфейсные карты (WIC – WAN interface card, HWIC – high-speed WIC, EHWIC – enhanced HWIC (усовершенствованный), NIM – network interface module. VWIC (voice WIC и т.д.).
2. Интерфейсные модули (NM – network module, NMD – NM double-wide (в два раза шире) и т.д.).
3. Внутренние модули (AIM – advanced integration module и т.д.).
4. DSP-сопроцессоры.
5. Порт-адаптеры и другие модули для высокопроизводительных платформ.

В названии модуля отражено его наполнение (HWIC-2FE – добавляет два сетевых интерфейса Fast Ethernet).
Разрабатывают и полностью программные модули, но маршрутизаторы (коммутаторы) это не затрагивает.

7. Учебные маршрутизаторы Cisco
// Не уверен в правильности

В качестве лабораторной базы для первоначального обучения обычно используют относительно недорогие серии ISRs различных поколений.
Традиционно, программа CCNA ориентирована на «младшие» модели ISRs для сегмента рынка SMB (или «старшие» модели ISRs для сегмента рынка SOHO).
Применительно к собственно ISRs это 2811, к ISRs G2 это 2901 (вроде стоят в лаборатории CISCO 5 корпуса), к ISRs 4K это 4331 (или 1841, 1941, 4221 соответственно).

Также стоит рассмотреть, что при рассмотрении любого сетевого устройства с точки зрения его функциональной организации можно выделить три так называемых плана (planes):

1. Management – административный – включает весь инструментарий, необходимый администратору для того чтобы он мог управлять сетевым устройством и отслеживать его состояние (например, протокол SSH).

2. Data – данных – включает все необходимое для выполнения сетевым устройством полезной нагрузки, то есть непосредственной пересылки пользовательского трафика (например, классическую таблицу маршрутизации – если не вдаваться в подробности о гибридных технологиях L2 – L3, таких как Cisco Express Forwarding).

3. Control – управляющий – представляет собой служебную надстройку над планом данных, с помощью которой сетевое устройство «разговаривает» с другими сетевыми устройствами и тем самым адаптирует структуры плана данных (например, протокол OSPF).

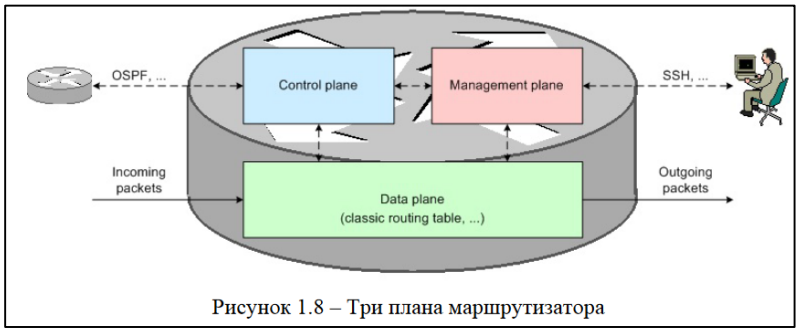


Рисунок 1.8 – Три плана маршрутизатора

Администрировать маршрутизатор (коммутатор) можно по-разному:
1. Подключение может быть локальным (local), то есть технологически без устройств посредников, или удаленным (remote), то есть технологически с возможным наличием устройств-посредников.
2. Административный трафик может быть изолирован от пользовательского (out-of-band) или совмещен с ним (in-band).
3. Не смотря на то, что все сетевые интерфейсы в КС имеют последовательную природу, обмен может быть посимвольным (character mode) или по-пакетным (packet mode).

8. Структура маршрутизаторов Cisco

В структуре маршрутизатора произвольной сложности, в конечном счете, можно выделить три «строительных» блока: процессор, память и устройства ввода-вывода.

В маршрутизаторах Cisco используют процессоры от ряда производителей с различными архитектурами – в большинстве случаев RISC. Так, в 2811 установлен процессор PMC-Sierra RM5261A, в 2901 – Cavium Octeon 17 Plus CN5220, в 4331 – Intel Atom C2718.

В маршрутизаторах (и коммутаторах) Cisco задействованы четыре традиционные подсистемы памяти:

1. BootROM (не путать с boot ROM при удаленной загрузке) – загрузочное ПЗУ (в современных моделях технологически это flash), в котором хранится собственно первичный загрузчик, коим в данном случае является ROMMON.

2. NVRAM (Non-Volatile RAM) – энергонезависимое ОЗУ (технологически это EEPROM либо, в современных моделях, flash), в котором хранится загрузочная конфигурация, глобальный конфигурационный регистр.

3. Flash – ПЗУ-накопитель (технологически это flash с различными вариантами подключения), основным назначением которого является хранение образов ОС IOS, но можно использовать и для хранения пользовательских файлов.

4. DRAM – обычное ОЗУ, в котором «удерживается» исполняющаяся ОС IOS со всеми своими подсистемами, рабочая конфигурация, таблица маршрутизации, буферы пакетов, таблицы адресов (логически разбивается на main processor memory и shared input/output memory).

Устройства ввода-вывода, в первую очередь, реализуют различные сетевые интерфейсы.
Безусловно, особо следует выделить flash-устройства.
Собственно подсистема памяти Flash в 2811 и 2901 представлена картами CompactFlash, а в 4331 – модулями eUSB со специфическими разъемами.

Кроме того, можно подключать (вставлять) другие flash-накопители: 2811, 2901 и 4331 – USB, 4331 – mSATA и NIM.

Официально поддерживаются только оригинальные flash-накопители (в отношении любых других компонентов политика аналогична).

9. Cisco IOS как встраиваемая операционная система

Cisco Internetwork Operating System (IOS) относят к специализированным встраиваемым ОС. Основное назначение IOS заключается в предоставлении возможности конфигурирования маршрутизаторов и коммутаторов производства Cisco.

Наряду с собственно IOS, существуют еще отдельные линейки для некоторых высокопроизводительных платформ: IOS XE (ASRs и другие), IOS XR (CRSes, NCSes, ASRs и другие) и NX-OS (Nexus и другие). А также более или менее подобные IOS: ASA OS и AsyncOS для аппаратных сетевых экранов, AireOS и ClickOS для беспроводного оборудования.

При изучении IOS можно использовать два основных эмулятора: Cisco Packet Tracer и GNS3.

Для получения доступа к возможностям IOS предусмотрены два основных средства и еще одно, которое считают перспективным:

1. Web-интерфейс.
2. Интерфейс командной строки.
3. ПО для устройств, поддерживающих архитектуру Cisco Digital Network Architecture (DNA)

Cisco имеет собственный интерфейс командной строки – Cisco Command Line Interface (CLI) (рисунок 2.4). Вплоть до 2018 г. именно CLI компания позиционировала как основное средство профессионального конфигурирования маршрутизаторов и коммутаторов.
С 2018 г. активно продвигает концепцию сетей на основе потребностей (intent-based) в связке с архитектурой DNA. Основные идеи: ориентация на автоматическое распределение ресурсов под потребности, визуальное проектирование, автоматизация конфигурирования, переход от децентрализованного администрирования к централизованному, максимальное применение виртуализации, ускорение «обратной связи» с сетью.

10. Загрузка IOS

Последовательность загрузки:

1. После включения питания в первую очередь отрабатывает загрузчик bootstrap в составе ROMMON, который инициализирует аппаратные структуры загрузочной среды (регистры процессора, UART CON-порта, глобальный конфигурационный регистр), выполняет POST, инициализирует аппаратные подсистемы, инициализирует программные структуры загрузочной среды (переменные окружения и так далее).

2. Загрузчик bootstrap пытается найти бинарный образ IOS исходя из значения специальной строки в загрузочной конфигурации либо значения специальной переменной загрузочной среды `BOOT` (при желании, IOS можно загрузить, например, с внешнего USB-накопителя). Далее если:
   Значение не задано/указанного образа не найдено -> загрузчик bootstrap пытается найти образ в подсистеме памяти Flash.
   Образов несколько -> выбирается первый обнаруженный.
   Образов нет вообще -> bootstrap запускает интерпретатор командной строки (собственно ROMMON), который можно использовать для копирования образа в Flash (например, с внешнего TFTP-сервера).
   Образ найден успешно -> загрузчик bootstrap загружает его в DRAM и передает ему управление.

3. Образ IOS распаковывается в DRAM и загружается, попутно инициализируя все необходимые программные и аппаратные структуры (например, назначает внутренние дескрипторы сетевым интерфейсам и распределяет буферы).

4. Выводится сообщение (только сообщение) о нажатии клавиши Enter (точнее, Return) для начала работы, загрузочная конфигурация переносится в рабочую, наконец, в случае нажатия клавиши Enter, появляется приглашение командной строки либо (если предусмотрено) запрос о входе в систему.
   Если загрузочная конфигурация по каким-либо причинам отсутствует, то, до сообщения о нажатии клавиши Enter для начала работы, появляется вопрос о том, стоит ли начинать конфигурационный диалог (автоустановку), на который всегда нужно отвечать отрицательно (вопрос может быть задан по-разному, даже перефразировано повторно), и загружается конфигурация по умолчанию (вместо загрузочной).

Процесс загрузки можно наблюдать только на основной консоли, если основная консоль подключена, что вовсе необязательно.

11. Режимы IOS

CLI может функционировать в одном из нескольких режимов, отличающихся назначением:

1. User EXEC (startup mode) – просмотр состояния системы, проверка связи, настройка
   терминала.
2. Privileged EXEC (“enable” mode) – просмотр конфигурации, просмотр состояния и отладка подсистем, работа с файлами, перезагрузка.
3. Global configuration (“configure terminal” mode) – конфигурирование устройства.
4. Конфигурирование интерфейса (“interface X” mode) – конфигурирование отдельного интерфейса.
5. Конфигурирование линии (“line” mode) – конфигурирование отдельной линии.
6. ПЗУ-монитор (“Ctrl-Break” mode) – диагностика и восстановление.

Исполнительские режимы, в отличие от конфигурационных, не предназначены для изменения каких-либо параметров.

Глобальный конфигурационный режим, в отличие от режима конфигурирования чего-либо, предназначен для изменения параметров всего устройства.

Переходы между режимами можно сравнить с подъемами и спусками по ступенькам шаг за шагом, начиная с момента входа в систему (один режим – одна ступенька). Но иногда переходы можно ускорять, прыгая через ступеньки вниз или перепрыгивая на ступеньки других лестниц (минуя exit – end – Ctrl-Z/C).
По приглашению (prompt) можно определить текущий режим
(например `Device(config-if)# someCommand`).

12. Система команд IOS и ее особенности

Команды IOS в большинстве своем комплексные, а значит требуют наличия аргументов при их вводе.

IOS не различает строчные и прописные буквы при вводе команд, но это правило не распространяется на значения некоторых аргументов (например, паролей).

Каждая команда предназначена для определенного режима (режимов), поэтому понимание смысла режимов позволяет легко соотносить с ними команды. Некоторые команды в разных режимах имеют разные наборы аргументов.

В любом из режимов командой `help` можно запросить помощь.

С помощью «`?`» можно запросить список всех доступных команд либо вариантов подстановки их аргументов (context sensitive help).

Команда-префикс `do` позволяет в конфигурационном режиме выполнить команду, предназначенную для исполнительского режима.

Аргумент-префикс `no` позволяет придать «инверсный» смысл некоторой команде в соответствующей ситуации (например, no shutdown).

Одним из востребованных удобств CLI является возможность сокращения команд при их вводе, но нужно помнить об однозначности интерпретации.

13. Файлы конфигурации и файловая система IOS
// Не уверен в целостности

Сразу следует отметить, что маршрутизаторы (и коммутаторы) Cisco хранят конфигурацию в двух специальных файлах:
1 `startup-config` – содержит загрузочную конфигурацию, то есть загружается при загрузке ОС.
2 `running-config` – содержит рабочую конфигурацию, то есть загрузочную конфигурацию с учетом текущих изменений вследствие введенных команд.

Также предусмотрен глобальный конфигурационный регистр, каждый бит которого «отвечает» за одну из глобальных настроек.

Для обеспечения возможности работы IOS с файловыми ресурсами разработана собственная файловая система Cisco IOS File System (IFS), включающая три подсистемы: network file systems, special file systems, storage file systems.

В основу современных IFSes положены FAT16 (IOS) и ext2 (IOS XE).

Для обращения к локальным или удаленным файловым ресурсам используют специальные префиксы.

На накопителях могут существовать и скрытые разделы специального назначения (например, может быть создан раздел с диагностическим образом, доступ к которому автоматически открывается после сбоя IOS).
Основные команды для работы с файлами:
- `cd` – сменить каталог;
- `copy` – скопировать файл либо каталог;
- `delete` – удалить файл;
- `dir` – вывести на экран содержимое текущего каталога;
- `erase` – удалить все файлы и каталоги из файловой системы;
- `format` – отформатировать файловую систему;
- `mkdir` – создать каталог);
- `more` – вывести на экран содержимое файла;
- `pwd` – вывести на экран название текущего каталога;
- `rename` – переименовать файл либо каталог;
- `rmdir` – удалить каталог.

14. Основные команды IOS для базовой настройки маршрутизатора и просмотра его состояния

При базовой настройке маршрутизатора либо коммутатора предполагается задание правильного времени. Время может быть «программным» (software clock) и «аппаратным» (hardware clock). Для работы со временем используют команды `clock` и `calendar` соответственно (`clock` с некоторыми аргументами и `calendar`, возможно не вполне логично, но целенаправленно отнесены к привилегированному исполнительскому режиму).

Название хоста можно изменить командой hostname (видно в приглашении командной строки). По умолчанию маршрутизаторы Cisco имеют название Router, коммутаторы – Switch.

Также можно перечислить команды interface, ip(v6) route, ip(v6) address, etc.

Не нужно забывать сохранять рабочую конфигурацию. `"Router#write"`

Для просмотра состояния различных подсистем IOS используют комплексную команду `show`. Основные варианты при знакомстве с IOS:
- `show running-config` / `show startup-config` – вывести на экран конфигурацию;
- `show interfaces` – вывести на экран подробное состояние всех сетевых интерфейсов (без аргументов) либо отдельно взятого интерфейса (если он указан);
- `show line` – вывести на экран состояние всех линий (без аргументов) либо подробное состояние отдельно взятой линии (если она указана);
- `show version` – вывести на экран общую информацию об IOS и маршрутизаторе либо коммутаторе;
- `show processes` – вывести на экран подробную информацию о процессах;
- `show diag`, `show platform` – вывести на экран подробную информацию об оборудовании;
- `show inventory` – вывести на экран подробную информацию о заменяемых частях (так называемых field replacement units).

15. Сетевые интерфейсы в IOS

Все сетевые интерфейсы (физические и логические, аппаратные и программные, реальные и виртуальные), применительно к которым возможно конфигурирование, Cisco разделяет на два типа: L2 и L3.

Одной из самых важных особенностей оборудования Cisco (даже относительно дешевого) является возможность преобразования L2 и L3-интерфейсов друг в друга.

Сетевые интерфейсы коммутаторов по умолчанию являются L2-интерфейсами и по умолчанию административно включены (administratively up), а сетевые интерфейсы маршрутизаторов по умолчанию являются L3-интерфейсами и по умолчанию административно выключены (administratively down).

Для конфигурирования L2-интерфейсов, точнее, всего что относится ко второму уровню в L2-интерфейсах, предназначена лишь одна команда, но очень «развесистая» – `switchport`

Cisco `Loopback` – это сугубо программный L3-интерфейс, как правило используемый для отладки. Создается автоматически при первом «обращении» (например, `interface lo0`) и может быть удален. После создания сразу административно включается, хотя может быть и административно выключен.

Cisco Null – это так же сугубо программный L3-интерфейс, как правило используемый для устранения маршрутизационных циклов. Никогда не принимает и не передает пакеты.

Названия интерфейсов при вводе обычно сокращают (по общим правилам), причем можно не вводить и разделяющие пробелы (например, `GigabitEthernet 0/0` равно `gi0/0`)

16 Сетевые интерфейсы и подсети

Физически Internet состоит из огромного количества самых разнообразных сегментов.

Логическая структуризация Internet заключается в разбиении на подсети.

Подсетью (subnet) называют определенное адресное пространство, предполагающее наличие некоторого количества станций.

Логическая структура может «накладываться» на физическую по-разному. Но минимальная подсеть должна соответствовать сегменту.

Cisco предлагает три основных критерия объединения станций в подсети:

1. Расположение.
2. Назначение.
3. Принадлежность.

Хотя, в конечном счете, все «завязано» на маршрутизацию.

С точки зрения IP-адресации выделяют два основных типа станций:

1. Пользовательские станции – User Nodes(UNs) – за ними работают рядовые пользователи сети.

2. Шлюзовые станции или просто шлюзы – GateWays(GWs) – предназначены для объединения подсетей (объединить подсети можно только объединив сегменты).

Сетевой интерфейс (network interface) – это минимально адресуемый в СПД компонент, входящий в состав какой-либо станции. Применительно к компьютерам, как правило, сетевой интерфейс физически выражен в виде сетевого адаптера – Network Interface Card (NIC).

Станция может содержать произвольное количество сетевых интерфейсов (пользовательская – обычно один, шлюзовая – минимум два). В одном сетевом адаптере обычно содержится один сетевой интерфейс, но может быть интегрировано и несколько. Каждый сетевой интерфейс обычно имеет одну точку подключения к СрПД, то есть физический порт.

IP-адрес ассоциируют с сетевым интерфейсом. Этот адрес нельзя однозначно приравнивать к адресу станции.

Каждый сетевой интерфейс должен иметь собственный IP-адрес. Причем сетевым интерфейсам можно присваивать не все адреса.

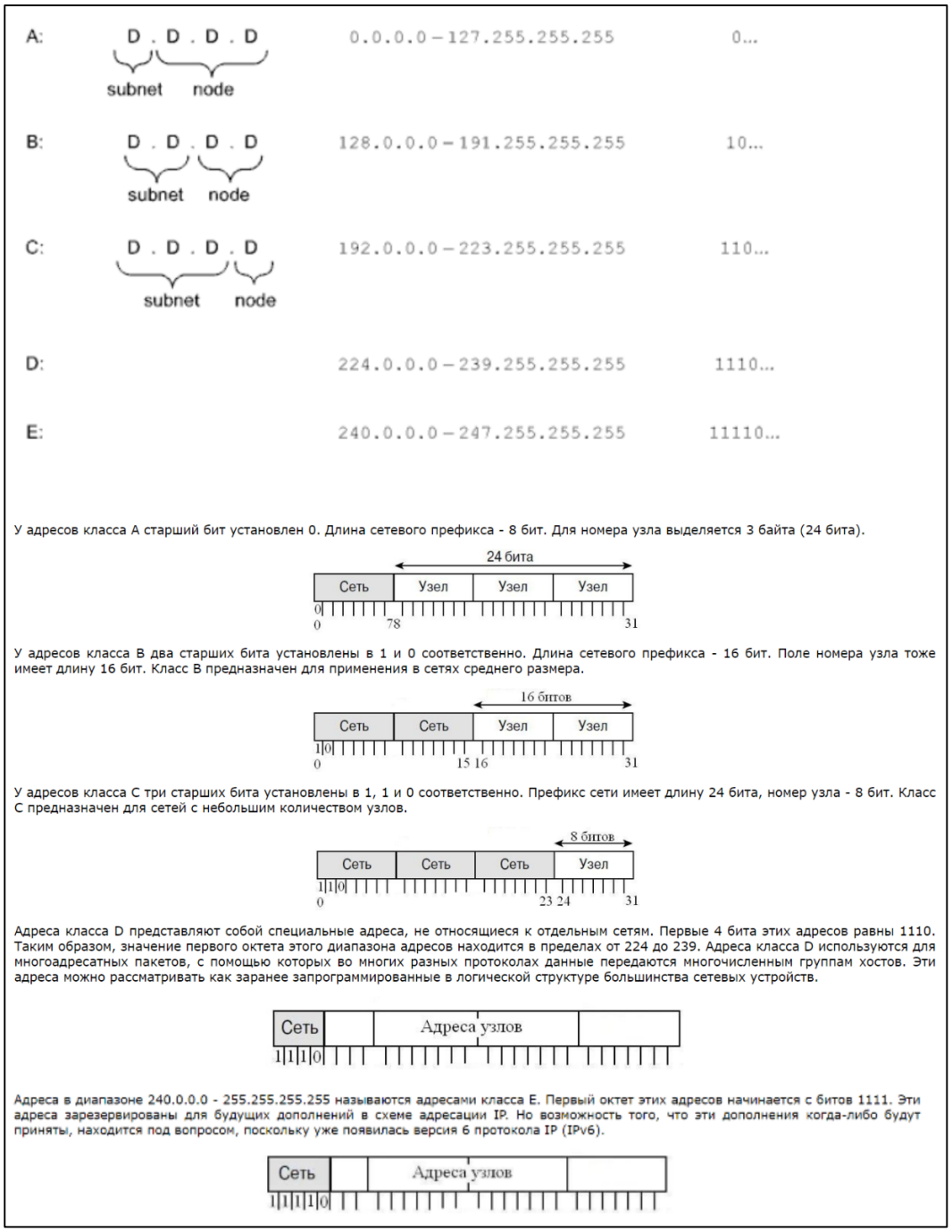
Если некоторая станция содержит два либо более сетевых интерфейсов, то среди них выделяется главный, ассоциированный с самой станцией. Обычно главный интерфейс «смотрит» в сторону Internet

17 Классы IPv4-адресов

Формально выделяют пять классов IP-адресов. Классы A, B и C являются основными, а классы D и E – дополнительными.

Класс D используется для адресации мультикаст-групп.

Класс E зарезервирован для будущего использования.
Есть и другие зарезервированные диапазоны.



Видно, что любой IP-адрес состоит из двух частей: подсетевой (subnet portion, subnet number, даже network number, и другие названия, но не network address) и станционной (node portion, local number, bits of host, и другие названия, но не host address).

18 Явные IPv4-параметры сетевого интерфейса

Для каждого сетевого интерфейса существует возможность задать 4 так называемых явных IP-параметра:

1. IP Address (IP)
2. Subnet Mask (SM)
3. Default Gateway (DG)
4. DNS Server (DNS)

Собственно, IP-адрес предназначен для адресации некоторой станции посредством соответствующего сетевого интерфейса. Должен быть уникален по крайней мере в пределах подсети. Если станция содержит несколько сетевых интерфейсов, то им нельзя присваивать адреса из перекрывающихся подсетей.

Маска подсети предназначена для выделения подсети исходя из IP-адреса. Маска подсети в двоичном виде представляет собой непрерывную последовательность единиц и следующую за ней непрерывную последовательность нулей согласно общей длине IP-адреса. Принято, что нули соответствуют станционной части, единицы – подсетевой:

Маски подсетей для стандартных классов:

1) 255.0.0.0 2) 255.255.0.0 3) 255.255.255.0

Маска подсети всегда четная. Маска одинакова для всех сетевых интерфейсов в пределах подсети.

Число адресов в диапазоне подсети всегда равно степени двойки (минимум 4).

Шлюз по умолчанию – адрес сетевого интерфейса из подсети, на который нужно направлять пакеты, которые предназначены станциям не из текущей подсети (пути к этим станциям неизвестны).

Принято в качестве шлюза по умолчанию назначать адрес первого сетевого интерфейса в подсети и использовать один шлюз по умолчанию. Кроме того, принято в пределах подсети использовать один шлюз по умолчанию

Адрес DNS-сервера необходим для обращения к службе DNS, позволяющей восстановить цифровое значение адреса станции-абонента, с которым работают компьютеры, исходя из символьного, с которым работают люди.

Минимально должны быть известны IP-адрес и маска подсети. Подсеть выделяется из IP-адреса всегда автоматически согласно введенной маске. Если маска подсети не указана, то используется стандартная

19 Неявные IPv4-параметры сетевого интерфейса

Определение явных IP-параметров подразумевает задание еще двух неявных:

5. Subnet Address (SA) – адрес подсети.
6. Broadcast Address (BA) – широковещательный адрес.

Адрес подсети используется для «поочередной» адресации всех возможных станций подсети. Адресом подсети является самый нижний адрес из диапазона адресов подсети, и он всегда четный.

Широковещательный адрес используется для одновременной адресации всех возможных станций подсети. Широковещательным адресом является самый верхний адрес из диапазона адресов подсети, и он всегда нечетный.

Более точно таковые широковещательные адреса называют directed broadcasts. Согласно последним рекомендациям RFCs (с целью повышения безопасности), если соответствующая подсеть занимает больше сегмента, то, по умолчанию, пакеты с такими адресами назначения все равно должны «подавляться» на границах сегментов, то есть на шлюзах. Но должна существовать возможность опционального отключения «подавления»

Количество адресов из диапазона подсети, которые можно присвоить сетевым интерфейсам, меньше общего количества адресов на два (минус адрес подсети и широковещательный адрес).

20 Классификация IPv4-адресов

С точки зрения строгости соответствия классам все IP-реализации можно разделить на два типа:

1. Classful – полноклассовые.
2. Classless – бесклассовые.

Подсети нестандартного размера (обычно меньше стандартных) позволяют гораздо более эффективно расходовать адресное пространство.
Cisco называет такой подход VLSM (Variable-Length Subnet Masking).
Часто используют альтернативную форму задания маски подсети – в нотации CIDR (Classless Inter-Domain Routing): 192.168.11.0/25 – число битов подсетевой части

С точки зрения «видимости» все IP-адреса делятся на:

1. Публичные (public).
2. Приватные (private).

В отличие от станции с публичным адресом, станция с приватным адресом «видна» только во внутренней сети предприятия или организации.

В каждом из классов существуют диапазоны адресов, специально зарезервированные для внутренних подсетей.

Диапазоны адресов, зарезервированные для внутренних подсетей:

A: 10.X.X.X

B: 172.16.0.0 - 172.31.255.255

C: 192.168.X.X

С точки зрения временного постоянства все IP-адреса делятся на:

1. Статические
2. Динамические

Статический адрес закрепляется за станцией администратором на более или менее продолжительное время.

Динамический адрес присваивается станции в процессе загрузки по некоторому критерию и действителен только в течение сеанса работы.

Динамический адрес может присваиваться по-разному:

1. Передаваться с сервера по определенному протоколу (например, DHCP) после выборки из:
   - статического пула
   - динамического пула
2. Случайно генерироваться - адреса Link Local: 169.254.X.X.

Имеется несколько специальных соглашений в области IP-адресации:

0.0.0.0 – формально адрес всей глобальной сети Internet, но имеет и другие смыслы.

255.255.255.255 – формально глобальный широковещательный адрес, но поскольку представляет большу'ю «опасность» уже давно интерпретируется как Limited Broadcast, то есть пакеты с такими адресами назначения должны «безоговорочно» подавляться шлюзами.

127.0.0.1 (как и любой адрес из диапазона 127.X.X.X) – ассоциирован со специальным сетевым интерфейсом-заглушкой (loopback), необходимым для обеспечения переносимости ПО, то есть пакеты с такими адресами назначения, переданные приложениями, тут же программно возвращаются на прикладной уровень.

21 Использование адресного пространства IPv4 и «правила хорошего тона»

С точки зрения строгости соответствия классам все IP-реализации можно разделить на два типа:

1. Classful – полноклассовые.
2. Classless – бесклассовые.

Подсети нестандартного размера (обычно меньше стандартных) позволяют гораздо более эффективно расходовать адресное пространство.
Cisco называет такой подход VLSM (Variable-Length Subnet Masking).

В настоящее время широко применяется практика последовательного деления адресного пространства. При этом возможны стратегии:

1. Новая подсеть включается в существующую бОльшую подсеть.
2. Новая подсеть добавляется к существующей как смежная.

Основная разница заключается в маршрутизации. Первая стратегия целесообразна для разноранговых подсетей, вторая – одноранговых.

С учетом абстракции, типовая оконечная подсеть физически выражена как совокупность станций, подключенных к одной СрПД. В пределах подсети, переданный одной станцией пакет принимается всеми остальными. Чтобы попасть в другие подсети, пакет должен пройти соответствующие шлюзы. В крайнем случае, подсеть может состоять, как только из станций, так и только из шлюзов.

“Правила хорошего тона” подразумевают использование только одного шлюза по умолчанию на одном маршрутизаторе.

Шлюз по умолчанию – адрес сетевого интерфейса из рассматриваемой подсети, на который нужно направлять пакеты, которые предназначены станциям не из текущей подсети, причем пути к этим станциям неизвестны.

Применяется в сетях с хорошо выраженными центральными маршрутизаторами, в малых сетях, в клиентских сегментах сетей. Шлюз по умолчанию задаётся записью в таблице маршрутизации вида «сеть 0.0.0.0 с маской сети 0.0.0.0».

22 Статическая IPv4-адресация в Windows

Назначение и просмотр статических ipv4 адресов в Windows возможен 3 методами:

1. Через панель управления

- Открыть настройки сети и Интернета.
- Связанные настройки -> Изменить параметры адаптера
- Откроется отдельное окно «Сетевые подключения» панели управления.
- сетевое соединение, для которого нужно установить статический IP-адрес, и выберите параметр Свойства.
- выберите Протокол Интернета версии 4 (TCP/IPv4) на вкладке Сеть и нажмите кнопку Свойства.
- Переключите селектор на «Использовать следующий IP-адрес».
- Теперь введите данные в следующие поля, соответствующие настройкам вашей сети: Ipv4 “адрес” “маска подсети” “Шлюз по умолчанию”

2. Через настройки

- Нажмите значок “Настройки” и выберите вкладку Сеть и Интернет.
- Выберите Wi-Fi> Текущее соединение, т.е. Сеть, к которой вы подключены.
- Прокрутите страницу вниз до раздела настроек IP и нажмите кнопку Изменить.
- Затем выберите параметр Вручную.
- Включите тумблер IPv4.
- Установите статический IP-адрес и маску подсети

3. Через PowerShell

Откройте Powershell от имени администратора и введите следующую команду, чтобы просмотреть текущую конфигурацию сети:

Get-NetIPConfiguration

После этого введите следующую команду, чтобы установить статический IP-адрес, и нажмите Enter.

New-NetIPAddress -InterfaceIndex 15 -IPAddress 192.168.29.34 -PrefixLength 24 –DefaultGateway 192.168.29.1 Set-DnsClientServerAddress -InterfaceIndex 4 -ServerAddresses 10.1.2.1

Для просмотра текущих параметров сетевых интерфейсов в Windows используется команда ipconfig.

23 Статическая IPv4-адресация в Linux

Обычно, стандартное ядро Linux распознает основные виды сетевых адаптеров. Если такого не происходит, то требуется установка драйвера от производителя, либо «ручная» настройка или перекомпиляция ядра.

В Linux, на примере Ethernet, традиционные специальные файлы устройств – сетевых интерфейсов – это `eth0`, `eth1` и так далее согласно их количеству. В последнее время широко используют новые, более сложные, схемы формирования названий (например, название `enp2s0` сформировано с учетом физического расположения).

IP-параметры каждого сетевого интерфейса хранятся в соответствующем файле в каталоге /etc/sysconfig/network-scripts (ветви Red Hat и SuSE) либо в файле /etc/network/interfaces (ветвь Debian).

Еще один важный файл – это /etc/sysconfig/network.

Список DNS-серверов хранится в файле - /etc/resolv.conf.

Для просмотра текущих параметров сетевых интерфейсов в Linux – ifconfig (позволяет менять параметры «на лету», но изменения хранятся до ближайшей перезагрузки).

Для проверки связи, как в Windows, так и в Linux, применяется команда ping. Для отслеживания пакетов в Linux широко применяется команда tcpdump.

24 Статическая IPv4-адресация в IOS

Для назначения IP-адреса сетевому интерфейсу используют команду ip address. IOS поддерживает подинтерфейсы, но на уровне сетевого интерфейса может быть только один IP-адрес. При попытке ввода второго IP-адреса первый вытесняется. Для административного включения сетевого интерфейса используют команду no shutdown, для выключения – соответственно shutdown.

```
Router>enable
Router#configure terminal
Router(config)#interface gi0/0
Router(config-if)#ip address 192.168.11.1 255.255.255.224 !Обязательно
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#disable
Router>
```

Для вывода на экран IP-информации о сетевом интерфейсе либо сетевых интерфейсах используют команду show ip interface.

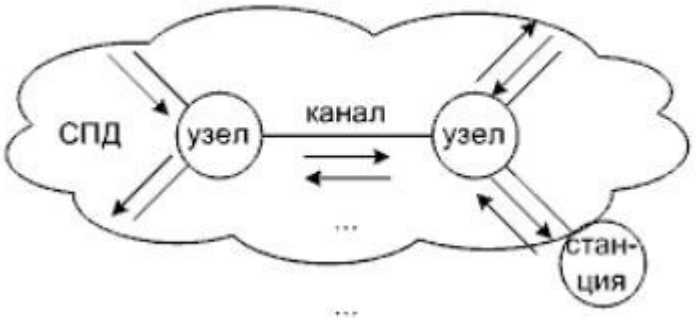
Для указания адреса DNS-сервера используют команду ip name-server. Для запрещения обращений к DNS-серверу используют команду no ip domain lookup

Как был назначен IP-адрес можно судить по методу:

- `manual` – данный статический адрес после загрузки введен вручную.
- `NVRAM` – данный статический адрес (либо факт отсутствия адреса) считан из загрузочной конфигурации.
- `TFTP` – данный статический адрес (либо факт отсутствия адреса) считан из конфигурации, полученной по протоколу TFTP.
- `DHCP` – данный динамический адрес получен по протоколу DHCP.
- `И т.д.`

Для проверки связи используют команды ping и traceroute. Эти команды в СПД с маршрутизаторами Cisco начинают «срабатывать» постепенно. Если команду ping либо команду traceroute ввести без аргументов, то ее можно «настроить» перед запуском.

25 Структура сети передачи данных



Канал представляет собой СрПД, через которую передаются пакеты. Узел представляет собой некоторое устройство, выполняющее прием, передачу или ретрансляцию пакетов. Узлами и станциями могут быть самые разные устройства.

Все узлы делят на два типа:

1. Пассивные
2. Активные

Пассивность узла означает, что он не выполняет анализ или обработку пакетов. Активность подразумевает, что пакеты анализируются или обрабатываются

Если соотносить узлы с моделью OSI, то можно выделить:

1. Повторители (repeaters) – аппаратно «сращивают» СПД на физическом уровне, типичными представителями являются оконечные концентраторы (hubs) (уже не производят).
2. Мосты (bridges) – аппаратно (но есть и «интеллектуальные») «сращивают» СПД на канальном уровне, типичными современными представителями являются коммутаторы (switches).
3. Шлюзы (gateways) – аппаратно и программно «сращивают» СПД на сетевом уровне, типичными представителями являются маршрутизаторы (routers).

Функция маршрутизации выполняется собственно маршрутизаторами. Но, нужно учитывать, что и все оконечные устройства должны иметь подсистему маршрутизации.

Физические порты маршрутизаторов ограничивают широковещательные домены. Физические порты коммутаторов ограничивают домены коллизий.

Оконечные концентраторы входят в домены коллизий и широковещательные домены.

26 Понятие маршрута и классификация маршрутов

Маршрут – это путь, по которому пакет передается от станции-отправителя к станции-получателю или составная часть этого пути.

Выделяются три вида маршрутов:

1. Маршрут к станции (сетевого интерфейса).
2. Маршрут к подсети.
3. Маршрут по умолчанию.

Каждый маршрутизатор принимает решения о направлении пересылки пакетов на основании таблицы маршрутизации. Таблица маршрутизации содержит набор правил. Каждое правило в наборе описывает шлюз или интерфейс, используемый маршрутизатором для доступа к определенной сети.

В IP-сетях реализованы два типа маршрутизации:

1. *Статическая*
2. *Динамическая*

При статической маршрутизации таблицы формируются «вручную» или автоматически на основе указанных IP-параметров и хранятся до их «ручной» модификации. При динамической маршрутизации таблицы и формируются, и модифицируются автоматически с задействованием специальных служебных протоколов, что не отменяет возможность вмешательства администратора.

В отношении протоколов динамической маршрутизации, все сетевые интерфейсы делятся на:

1. *Активные* – могут использоваться при обмене маршрутной информацией.
2. *Пассивные* – не могут использоваться при обмене маршрутной информацией.

В некоторых реализациях аналогично делятся маршруты. *Пассивные* маршруты, в отличие от *активных*, не могут «затрагиваться» (считываться и замещаться) протоколами динамической маршрутизации.

В некоторых реализациях (например, Windows) особо выделяются *персистентные* маршруты, которые должны сохраняться после перезагрузки.

27 Обобщенная структура таблицы маршрутизации

Маршруты хранятся в специальной таблице, называемой *таблицей маршрутизации*.

В обобщенном виде, с теми или иными вариациями, таблицу можно представить следующим образом.

	Destination	Netmask	Gateway	Interface	Metric	Options
Route						
Route						
...						
Route						

Назначение полей:

Destination – адрес назначения.

Netmask – маска подсети – дополняет адрес назначения с целью его правильной интерпретации.

Gateway – шлюз – IP-адрес шлюза-соседа, которому нужно передать пакет.

Interface – интерфейс – IP-адрес или другой параметр, однозначно определяющий сетевой интерфейс, который должен физически «выдать» пакет в канал.

Metric – метрика – определяет приоритетность маршрута (основное назначение), часто рассматривают в совокупности с так называемой административной дистанцией.

Options – опции – специфические опции данной реализации.

Специальные соглашения в области IP-маршрутизации:

Адрес назначения 0.0.0.0 – маршрут по умолчанию.

Маска подсети 255.255.255.255 – маршрут к одному сетевому интерфейсу.

28 Алгоритм применения таблицы маршрутизации для передачи пакета

Таблица маршрутизации определяет, что делать с уже принятым пакетом, подлежащим ретрансляции, или имеющимся пакетом, сформированным для передачи на вышестоящих уровнях. При наличии такого пакета, работа с таблицей маршрутизации протекает в две фазы:

1. Поиск маршрутной информации.
2. Применение маршрутной информации.

В настоящее время, как де-факто стандартный, применяется подход согласно принципу *наиболее точного соответствия* (best match, longest match), заключающийся в следующем:

1. Маршрут ищется путем последовательного сравнения IP-адреса назначения с диапазонами, считываемыми из строк таблицы маршрутизации.
2. При попадании (hit) маршрут считается подходящим.
3. Просматривается вся таблица маршрутизации. Конечно, этот процесс разными способами оптимизируется.
4. При наличии нескольких попаданий выбирается наиболее точный маршрут. Точность попадания определяется «размером мишени». Самым точным является маршрут к станции.
5. При одинаковой точности попадания маршрут выбирается исходя из дополнительного критерия – метрики.
6. Маршрут по умолчанию выбирается если не найдено ни одного более точного маршрута. «Промахнуться» невозможно.
7. При отсутствии попаданий пакет уничтожается (drop).
8. Маршрут ищется для того, чтобы его применить. Применение маршрута заключается в отправке по нему пакета. Пакет передается один раз.
9. На вопросы о том, куда и чем передавать, отвечают соответствующие поля в маршруте.

При наличии нескольких альтернативных маршрутов могут совпасть и их метрики, то есть маршруты оказываются абсолютно равноправными (надо отметить, что такое происходит довольно часто). В некоторых реализациях это считается недопустимым, а в некоторых возникает так называемая балансировка нагрузки, точнее, *эквивалентная балансировка нагрузки* – соответствующие пакеты поочередно передаются в разных направлениях. Существует еще и *неэквивалентная балансировка нагрузки* – отличается тем, что трафик распределяется пропорционально согласно метрикам.

29 Структура Internet

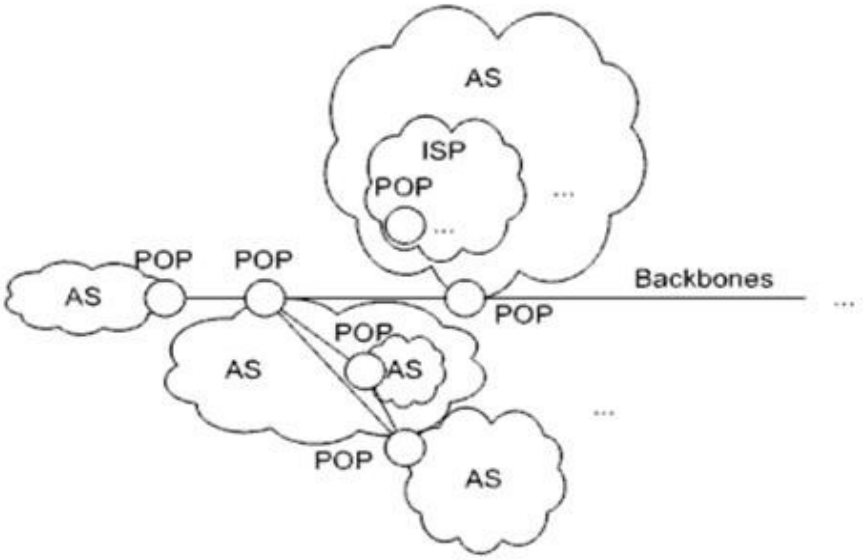


Рисунок -- Структура Internet

Основными структурными единицами Internet являются *автономные системы* - (AS). Каждая AS выделяется исходя из наличия собственной системы маршрутизации (возможно оригинальной), то есть состояние AS не должно зависеть от состояния других ASes.

Все ASes имеют уникальные 16-битные номера. Номера ASes поделены на:

1. Public: 1 – 64511.
2. Private: 64512 – 65535.

В связи с исчерпанием, не так давно были введены дополнительные 32-битные номера.

ASes связаны между собой посредством *базовых магистралей (backbones)*. Изначально в структуре Internet была задумана и реализована одна базовая магистраль, но сейчас это лишь условность. Поскольку на практике далеко не всегда удавалось осуществить непосредственное примыкание той или иной AS к базовой магистрали, к настоящему времени возникла очень сильная фрагментация. Реально, ASes соединены друг с другом через так называемые *пиринговые точки* или, по-другому, *точки присутствия* – Points-Of-Presence (POPs).

Внутри ASes работают *провайдеры* – Internet Service Providers (ISPs). Касательно POPs, следует уточнить, что терминологически это, в первую очередь, точки предоставления коммуникационных услуг пользователям Internet.

Также следует отметить, что крупные телекоммуникационные компании могут обладать несколькими ASes, а их СПД могут иметь межконтинентальную протяженность.

30 Назначение и классификация протоколов динамической маршрутизации

Суть всех протоколов динамической маршрутизации заключается в реализации тех или иных алгоритмов обмена маршрутами к подсетям, с целями как оптимизации трафика, так и вообще нахождения абонентов.

Обмен происходит именно маршрутами к подсетям. Основной смысл разбиения на подсети состоит в упрощении таблиц маршрутизации. Вместо того чтобы отслеживать станции и направлять пакет каждой из них «персонально», пакет направляется сразу в подсеть.

Также упрощение достигается за счет *агрегации маршрутов* – получение более общего маршрута из отдельных маршрутов к нескольким подсетям, если направления к этим подсетям совпадают.

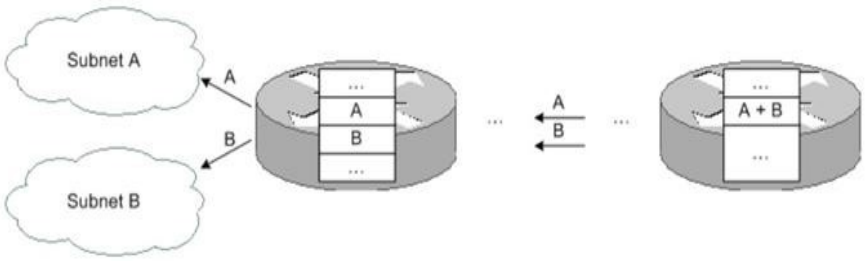


Рисунок -- Агрегация маршрутов

Реально агрегация происходит путем суммирования маршрутов (route summarization). Суммирование может быть:

1. «Ручным» (manual) – выполняется администратором (причем обычно выполняется оптимально).
2. Автоматическим (auto) – выполняется реализацией протокола динамической маршрутизации.

Как на уровне базовых магистралей, так и в пределах AS, допускается одновременное применение нескольких протоколов динамической маршрутизации. Шлюзы в пределах ASes называют внутренними, а шлюзы, через которые ASes подключены к базовым магистралям – внешними. Соответственно, протоколы для внутренних шлюзов называют IGPs (Interior Gateway Protocols), а для внешних – EGPs (Exterior Gateway Protocols).

Почти все используемые в IP-сетях протоколы динамической маршрутизации относят к группе адаптивных двух типов:

1. Distance Vector Algorithms – алгоритмы, основанные на анализе векторов расстояний.
2. Link State Algorithms – алгоритмы, основанные на анализе состояния связей.

DVAs при выборе маршрутов оценивают расстояние до подсетей. Касательно пересылки пакетов, расстояние в КС принято измерять в хопах. Один *хоп* (hop) – это изначальная передача либо одна последующая ретрансляция пакета.

LSAs при выборе маршрутов оценивают состояние связей, то есть каналов. Классическим примером состояния канала является его пропускная способность.

Поддержку подсетей нестандартного размера при IP-маршрутизации называют бесклассовой междоменной маршрутизацией – Classless Inter-Domain Routing (CIDR) (RFC 4632).

В случае бесклассового протокола, для учета нестандартных размеров подсетей при передаче IP-адресов подсетей дополнительно передаются и маски.

//////////////////

В отношении протоколов динамической маршрутизации, все сетевые интерфейсы делят на:

1. Активные (могут использоваться при обмене маршрутной информацией).
2. Пассивные (не могут использоваться при обмене маршрутной информацией)

31 Последовательность действий при передаче пакета в подсети и пересылка транзитных пакетов

Последовательность действий при передаче пакета в некоторой подсети заключается в следующем:

1. Пакет с известным IP-адресом назначения в заголовке передается на уровень MAC (например, Ethernet) и выполняется инкапсуляция.
2. В нормальной ситуации ядро сетевой ОС хранит таблицу соответствия MAC и IP-адресов. Если MAC-адрес назначения станции-абонента либо шлюза не известен, то для его восстановления используется протокол ARP.
3. Если пакет (теперь уже кадр) предназначен станции из текущей подсети, то, после передачи сетевым интерфейсом станции-передатчика, он будет сразу принят всеми станциями подсети.
4. Причем только на станции-абоненте, на основании анализа MAC-адреса назначения, кадр будет распознан как свой и его содержимое будет передано на уровень IP для дальнейшей обработки. Остальными станциями кадр будет отброшен.
5. Если пакет предназначен станции из другой подсети, то он будет передан, согласно таблице маршрутизации, соответствующему шлюзу с использованием MAC-адреса этого шлюза.

Если по каким-либо причинам необходимо принимать и обрабатывать все кадры, то включается специальный режим работы сетевого интерфейса – promiscuous.

Для того чтобы обеспечить передачу транзитных пакетов между подсетями через шлюз на нем должен быть разрешен IP Forwarding.

После включения IP Forwarding, каждый пакет, принятый одним из сетевых интерфейсов, может быть ретранслирован другими, то есть станция работает собственно, как шлюзовая.

Достижимость своих интерфейсов IP forwarding не затрагивает, то есть каждый интерфейс достижим через любой другой вне зависимости от состояния IP forwarding.

32 Структура таблицы ARP

Для просмотра ARP-таблицы используют команду show ip arp. Строки ARP-таблицы могут быть:

1. Статическими – вносятся администратором и, как правило, хранятся до перезагрузки или «ручного» удаления.
2. Динамическими – вносятся ОС автоматически и, как правило, удаляются по таймеру.

Строки с постоянными соответствиями сохраняются после перезагрузки.

2.0.9.29

```
C:\Users\Administrator>arp -a ;Вывести на экран ARP-таблицу

Interface: 192.168.11.214 --- 0xb
  Internet Address      Physical Address      Type
  192.168.11.193        b8-38-61-81-10-ca     dynamic
  192.168.11.223        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Administrator>arp -s 10.0.0.10 00-AA-00-4F-2A-9C

C:\Users\Administrator>netsh -c interface ipv4 add neighbors "Local Area
Connection" "192.168.10.10" "00-1d-71-83-6c-00" store=persistent
```

Структура таблицы ARP крайне простая. В первой колонке указывается IP адрес устройства, во второй соответствующий ему MAC адрес. В третей колонке указывается тип строки static/dynamic.

Для работы с ARP-таблицами, и в Windows, и в Linux, используют команду `arp`.

Чтобы сделать вводимые соответствия IP- и MAC-адресов постоянными, в Windows нужно использовать соответствующий вариант комплексной команды `netsh`, а в Linux – отредактировать стандартный конфигурационный файл `/etc/ethers`.

33 Использование протокола ARP

ARP — протокол разрешения адресов (Address Resolution Protocol) является протоколом третьего (сетевого) уровня модели OSI, используется для преобразования IP-адресов в MAC-адреса, играет важную функцию в множественном доступе сетей.

Непосредственно связь между IP адресом и MAC адресом осуществляется с помощью так называемых ARP-таблиц, где в каждой строке указывается соответствие IP адреса MAC адресу.

ARP-сообщения инкапсулируются в Ethernet-кадры. Существуют следующие типы сообщений ARP: запрос и ответ.

Request - широковещательный (адресован всем станциям в домене). Суть запроса: «компьютер с IP-адресом Y, сообщите свой MAC-адрес компьютеру с MAC-адресом X». В дополнение к запросу и ответу, предусмотрен еще один вид ARP-сообщений – ARP probe. Что позволяет, например, при загрузке ОС, обнаружить конфликты IP-адресов и параллельно оповестить все станции в подсети о «возникновении» у сетевого интерфейса нового IP-адреса. «Исчезновение» IP-адреса не анонсируется.

ARP proxy в связке с directed broadcast forwarding позволяет организовать прозрачный шлюз. Включение ARP proxy разрешает шлюзу отвечать на ARP-запрос из одной своей подсети в отношении IP-адреса из другой своей подсети (подставлять свой MAC-адрес). Такой запрос может возникнуть только если запрашивающая станция считает, что запрашиваемая станция находится в той же подсети.

34 Практические особенности IPv4-маршрутизации

Таблица маршрутизации определяет что делать с уже принятым пакетом, подлежащим ретрансляции, или имеющимся пакетом, сформированным для передачи на вышестоящих уровнях. При наличии такого пакета, работа с таблицей маршрутизации протекает в две фазы:

1. Поиск маршрутной информации.

2. Применение маршрутной информации

В настоящее время, как де факто стандартный, применяется подход согласно принципу наиболее точного соответствия (best match, longest match), заключающийся в следующем:

1. Маршрут ищется путем последовательного сравнения IP-адреса назначения, считанного из заголовка пакета, с диапазонами, задаваемыми адресами назначения в связке с масками подсетей, считываемыми из строк таблицы маршрутизации.

2. При попадании (hit) маршрут считается подходящим.

3. Просматривается вся таблица маршрутизации. Конечно, этот процесс разными способами оптимизируется.

4. При наличии нескольких попаданий выбирается наиболее точный маршрут. Точность попадания определяется «размером мишени». Самым точным является маршрут к станции.

5. При одинаковой точности попадания маршрут выбирается исходя из дополнительного критерия – метрики.

6. Маршрут по умолчанию выбирается если не найдено ни одного более точного маршрута. «Промахнуться» невозможно.

7. При отсутствии попаданий пакет уничтожается (drop).

8. Маршрут ищется для того, чтобы его применить. Применение маршрута заключается в отправке по нему пакета. Пакет передается один раз.

9. На вопросы о том, куда и чем передавать, отвечают соответствующие поля в маршруте

При наличии нескольких альтернативных маршрутов могут совпасть и их метрики, то есть маршруты оказываются абсолютно равноправными (надо отметить, что такое происходит довольно часто). В некоторых реализациях это считается недопустимым, а в некоторых возникает так называемая балансировка нагрузки, точнее, эквивалентная балансировка нагрузки (equal load balancing) – соответствующие пакеты поочередно передаются в разных направлениях. Существует еще и неэквивалентная балансировка нагрузки (unequal load balancing) – отличается тем, что трафик распределяется пропорционально согласно метрикам.

В IP-сетях реализованы два типа маршрутизации:

1. Статическая (static).

2. Динамическая (dynamic).

При статической маршрутизации таблицы формируются «вручную» или автоматически на основе указанных IP-параметров и хранятся до их «ручной» модификации. При динамической маршрутизации таблицы и формируются, и модифицируются автоматически с задействованием специальных служебных протоколов, что не отменяет возможность вмешательства администратора.

В отношении протоколов динамической маршрутизации, все сетевые интерфейсы делят на:

1. Активные (active) – могут использоваться при обмене маршрутной информацией.

2. Пассивные (passive) – не могут использоваться при обмене маршрутной информацией.

В некоторых реализациях (например, UNIX routed) аналогично делят маршруты. Пассивные маршруты, в отличие от активных, не могут быть «затронуты» (считаны или замещены) протоколами динамической маршрутизации. В реализациях особо выделяют постоянные или, по -другому, персистентные (persistent) маршруты, которые должны сохраняться после перезагрузки.

35 Структура таблицы IPv4-маршрутизации в Windows

Чтобы просмотреть текущую таблицу маршрутизации в Windows используют команду route с аргументом print. В первой колонке таблицы маршрутизации Windows указывается адрес подсети назначения, во второй - её маска, в третьей - шлюз, через который достижима эта подсеть, четвёртый - интерфейс, который должен физически «выдать» пакет в канал, пятый - метрика.

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.11.193   192.168.11.221     266
        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
    192.168.11.192  255.255.255.224         On-link   192.168.11.221     266
    192.168.11.221  255.255.255.255         On-link   192.168.11.221     266
    192.168.11.223  255.255.255.255         On-link   192.168.11.221     266
        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   192.168.11.221     266
  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   192.168.11.221     266
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0   192.168.11.193  Default
===========================================================================
...
```

Пример таблицы маршрутизации Windows на пользовательской станции

Постоянные маршруты: настраиваемые вручную маршруты статического лечени

//////////////////

3) Шлюз: При отправке пакетов данных IP шлюз определяет сервер следующего перехода, на который отправляются пакеты данных для определенного сетевого адреса назначения.

4) Интерфейс:. Интерфейс определяет конкретный сетевой адрес назначения, сетевой интерфейс, используемый локальным компьютером для отправки пакетов данных.

5) Метрика: количество переходов, счетчик переходов используется для обозначения стоимости маршрутизации, обычно представляет собой количество переходов, которые необходимо пройти, чтобы достичь адреса назначения, а счетчик переходов представляет маршрутизатор. Чем меньше количество переходов, тем ниже стоимость маршрутизации и выше приоритет.

36 Структура таблицы IPv4-маршрутизации в Linux

2.0.9.4

```
#netstat -r #Вывести на экран таблицу маршрутизации ядра

Kenel IP routing table
Destination     Gateway         Genmask         Flags    MSS window   irtt Iface
192.168.11.160  *               255.255.255.240 U          0 0          0 eth0
192.168.11.0    *               255.255.255.128 U          0 0          0 eth1
169.254.0.0     *               255.255.0.0     U          0 0          0 eth1
127.0.0.0       *               255.0.0.0       U          0 0          0 lo
default         192.168.11.1    0.0.0.0         UG         0 0          0 eth1
#
#Флаги: U -- route is Up, G -- use Gateway
#MSS, window, irtt -- параметры TCP (устарело)
#

#netstat -nr #Адреса отображать в цифровой форме (не делать DNS-запросы)

Destination     Gateway         Genmask         Flags    MSS window   irtt Iface
192.168.11.160  0.0.0.0         255.255.255.240 U          0 0          0 eth0
192.168.11.0    0.0.0.0         255.255.255.128 U          0 0          0 eth1
169.254.0.0     0.0.0.0         255.255.0.0     U          0 0          0 eth1
127.0.0.0       0.0.0.0         255.0.0.0       U          0 0          0 lo
0.0.0.0         192.168.11.1    0.0.0.0         UG         0 0          0 eth1
```

Пример таблицы маршрутизации Linux на шлюзе

Традиционная команда для просмотра таблицы маршрутизации в Linux: netstat -r (-nr). Также можно воспользоваться командой route. Сама таблица состоит из 8 столбцов:

- Destination - адрес подсети назначения,
- Gateway - шлюз,
- Genmask - маска подсети назначения,
- Flags - флаг, определяющий характеристики маршрута,
- Iface - название интерфейса.
- MSS - размер пакета
- Windows - TCP-окно
- irtt - время отклика для TCP-соединений
- Всё остальное - устаревшие параметры TCP.

37 Структура таблицы IPv4-маршрутизации в IOS

В первую очередь маршруты делят на:

1. Directly connected равно Connected (код C) – маршруты к своим подсетям (а не «к подключенным интерфейсам»).
1. Static (код S) – статические (собственно статические маршруты, которые вносят «вручную»)
2. Dynamic (коды R, B, O и другие) – динамические (автоматически вносятся процессами динамической маршрутизации)
3. + Local (код L) – локальные или, в данном контексте, маршруты к своим сетевым интерфейсам

В иерархии маршрутов выделяют два уровня:

1. L1 – маршруты к стандартным подсетям и подсетям, большим чем стандартные.
2. L2 – маршруты к подсетям, меньшим чем стандартные, и к сетевым интерфейсам.

С другой стороны, маршруты в иерархии можно рассматривать как:

1. Parent – родительские.
2. Child – дочерние.

Иерархия необходима для ускорения обработки таблицы маршрутизации. Сначала просматриваются маршруты первого уровня. В случае попадания происходит переход к просмотру соответствующих маршрутов второго уровня.

Маршруты первого уровня:

1. Default route – маршрут (маршруты) по умолчанию.
2. Supernet routes – маршруты к подсетям, большим чем стандартные.
3. Network routes – маршруты к стандартным подсетям.

Просмотреть содержимое таблицы маршрутизации в Cisco IOS можно с помощью команды show ip route.

При выборе маршрута для передачи пакета из имеющихся в таблице маршрутизации (равно как и выборе маршрута для внесения в таблицу маршрутизации при динамической маршрутизации) оцениваются:

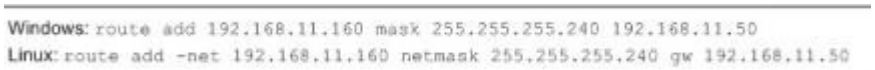
1. Prefix length – длина префикса – чем больше, тем маршрут приоритетнее.
2. Administrative distance (по-другому, external administrative distance) – административная дистанция – чем меньше, тем маршрут приоритетнее
3. Metric (по-другому, internal administrative distance) – метрика – так же чем меньше, тем маршрут приоритетнее.

38 Статическая IPv4-маршрутизация в Windows, Linux и IOS

Чтобы добавить статический маршрут в таблицу маршрутизации ядра, и в Windows, и в Linux, используют команду route с аргументом add.

Удалить в Windows: route delete.

Удалить в Linux: route del.



Постоянство вводимого статического маршрута в Windows достигают за счет аргумента -p. Постоянство статических маршрутов в Linux обеспечивают несколькими способами с возможностью комбинирования этих способов. Маршруты могут «привязываться» к конкретным сетевым интерфейсам (но необязательно использовать их).

Для внесения статического маршрута в таблицу маршрутизации используют команду `ip route`.

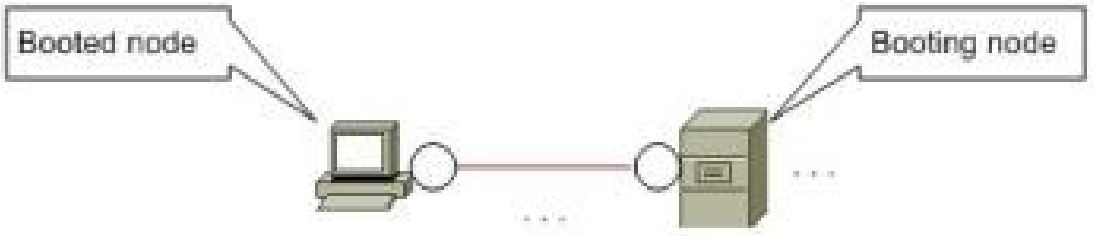
Отключение бесклассового выбора маршрутов, то есть включение полноклассового, осуществляют командой `no ip classless`.

Функционал IP forwarding по умолчанию включен и может быть выключен командой `no ip routing`.

При необходимости введения сравнительно большого количества статических маршрутов или при переходе к простейшей динамической маршрутизации (RIP) в Linux можно задействовать демон routed. При этом статические маршруты помещают в стандартный конфигурационный файл /etc/gateways. После настройки и запуска сервиса в течение некоторого времени сформируется таблица маршрутизации, которая затем может изменяться.

39 Структура системы удаленной загрузки

Термин удаленная загрузка означает, что по крайней мере ядро ОС некоторой станции загружается не с локальных накопителей, а по сети – с удаленной станции. Удаленная загрузка как правило используется для бездисковых пользовательских станций, не предназначенных для хранения информации. Каждый раз загружается «заготовка» ОС. Таким образом, в состав сети с удаленной загрузкой входит как минимум две станции, которые обычно расположены в одном сегменте.



Для решения проблемы эмуляции системного диска используют два подхода:

1. Поддержка виртуального диска в памяти (RAM Drive).
2. Поддержка сетевого виртуального диска.

40 Технологии удаленной загрузки

В настоящее время существуют несколько семейств технологий, связанных с удаленной загрузкой (используется клиент-серверная модель, включая поддержку со стороны BIOS/UEFI и загрузчиков Linux, в первую очередь выражены в соответствующих протоколах):

1. Для IPX (Internetwork Packet Exchange): RPL (Remote Program Load) плюс ПО от Novell, Microsoft и другое.
2. Для IPv4: BOOTP (BOOTstrap Protocol) -> DHCP (Dynamic Host Configuration Protocol) -> PXE (Preboot eXecution Environment) плюс ПО от 3COM, Intel, Citrix, Microsoft, IBM, HP и другое.
3. Для IPv6: DHCPv6 -> Netboot6 (PXE на базе IPv6) плюс ПО от Citrix и Microsoft.
4. Для IPv4/IPv6: iSCSI (internet SCSI) Boot и FCoE (Fibre Channel Over Ethernet) Boot и HTTP Boot плюс ПО от Cisco, Microsoft, Intel, IBM и другое.
5. Для IPv4/IPv6: HTTP Boot плюс ПО от HPE (для некоторых серверов), IBM (для некоторых серверов).
6. Для IPv4/IPv6: Прочие протоколы плюс как правило свободно распространяемое ПО, например, gPXE -> iPXE (развитие EtherBoot) (альтернатива PXE, но поддерживает PXE плюс другие протоколы).

41 Поддержка удаленной загрузки в BIOS

BIOS работает в реальном режиме с 16-ти разрядной адресацией и имеет совсем немного реализаций с разными модификациями и «обертками». В BIOS, еще при изначальной разработке, была заложена возможность включать сторонние дополнения – add-on BIOSes. Для обеспечения удаленной загрузки на стороне клиентской станции в состав add-on BIOSes необходимо включить boot ROM – специальное загрузочное ПЗУ.

1. После включения загружаемой станции выполняется так называемый POST (Power On Self Test).
   При этом BIOS сканирует память в диапазоне C0000h – EE000h (куда отображаются add-on BIOSes) с инкрементом, равным 2 kByte, в поисках сигнатуры 55AAh, которая свидетельствует о наличии add-on BIOS.
2. Если сигнатура найдена, то третий байт, содержащий размер add-on BIOS в 512-ти байтовых страницах, используется для проверки контрольной суммы.

   Если контрольная сумма равна нулю, то осуществляется вызов подпрограммы по адресу, расположенному со смещением +3 (четвертый байт). В случае с boot ROM, вызванный код используется для подмены обработчика прерывания 18h (ROM BASIC).
3. После просмотра всего диапазона, BIOS выполняет инструкцию INT 18h (перезагрузка).
4. Затем, вернув управление, новый обработчик копирует основное содержимое boot ROM (loader) в оперативную память и передает ему управление.
5. Затем, загрузчик loader с помощью подпрограмм boot ROM загружает простейший сетевой протокол, получает код загрузчика bootstrap от загружающей станции и передает ему управление.

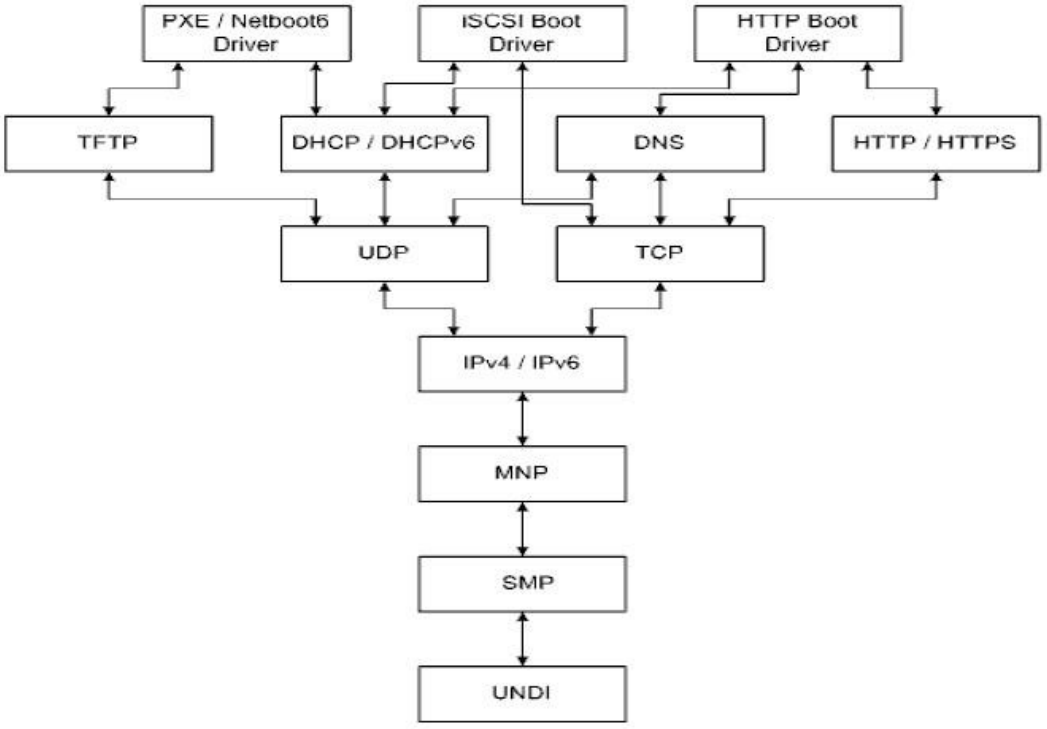
Дальнейшие действия зависят от реализации.

42 Поддержка удаленной загрузки в UEFI

UEFI имеет более сложную структуру и намного больше «оберток» в сравнении с BIOS. При этом подразумевается поддержка даже сложных сетевых протоколов, в том числе необходимых для удаленной загрузки. UEFI переходит в защищенный режим с 32-ух- либо 64-ех разрядной адресацией. Сложность требует наличия ПЗУ соответствующего объема, что во времена BIOS было «роскошью». Место add-on BIOSes заняли специальные UEFI-драйверы.

Для обеспечения удаленной загрузки от производителей сетевых контроллеров требуется только написание драйверов. Как правило это UNDI-драйверы, совместимые с UEFI API. Драйвер может быть, как «прошит» в ПЗУ на плате сетевого адаптера, так и интегрирован в UEFI. Типичные UEFI ориентированы на IPv4/IPv6 и поддерживает комплекс протоколов: PXE, Netboot6, iSCSI Boot, FCoE Boot, HTTP Boot, а также фильтрацию и аутентификацию.

//**Если есть возможность**

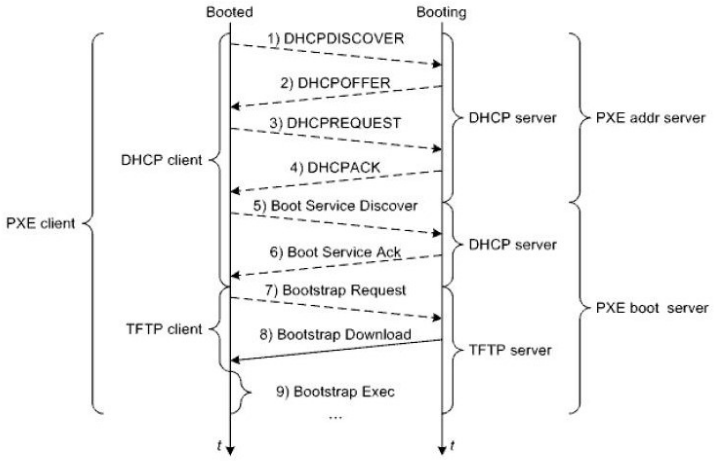


Где: MNP – Managed Network Protocol, SNP – Simple Network Protocol.

43 Взаимодействие по протоколу PXE

PXE представляет собой своеобразную надстройку над DHCP, формализующую три основные вещи:

1. Протокол взаимодействия клиентской станции с сервисами адресации и загрузочными сервисами.
2. Набор APIs, которые образуют «продвинутую» загрузочную среду на клиентской станции.
3. Структуру boot ROM.



1. DHCPDISCOVER – DHCP-клиент в составе PXE-клиента посылает броадкаст-запрос с целями анонсирования своего «возникновения» и поиска сервиса адресации, коим является DHCP-сервер.
   Если DHCP-клиент по каким-либо причинам еще не готов полноценно обрабатывать юникаст-пакеты, он должен установить флаг B – Broadcast Flag
2. DHCPOFFER – DHCP-сервер сразу выдает DHCP-клиенту IP-адрес и в юникаст- либо броадкаст-форме отвечает о своей готовности.
3. DHCPREQUEST – DHCP-клиент, по-прежнему в бродкаст-форме, подтверждает, что он выбрал определенный DHCP-сервер, и параллельно собственно запрашивает IP-адрес и требующиеся ему конфигурационные параметры.
4. DHCPACK – DHCP-сервер в юникаст- либо броадкаст-форме подтверждает подтверждение и параллельно предоставляет значения всех предварительно сконфигурированных параметров из тех, что были запрошены.
5. Boot Service Discover – PXE-клиент посредством DHCP посылает запрос о предоставлении загрузочного сервиса. (DHCPDISCOVER + DHCPREQUEST).
6. Boot Service Ack – DHCP-сервер, находящийся на стороне загрузочного сервиса, подтверждает предоставление услуг.
7. Bootstrap Request – TFTP-клиент в составе PXE-клиента посылает запрос о предоставлении файла – загрузчика bootstrap.
8. Bootstrap Download – TFTP-клиент скачивает файл – загрузчик bootstrap.
9. Bootstrap Exec – загрузчик bootstrap исполняется.

44 Протоколы BOOTP, DHCP, TFTP и их использование

Первым протоколом, который массово использовали для динамического назначения IP-адресов, является BOOTP.

Как альтернативу BOOTP, для нахождения IP-адресов по MAC-адресам, изредка использовали протокол RARP – в современных реализациях практически не поддерживается. DHCP представляет собой расширение BOOTP.

По большому счету, в DHCP-заголовке передается только пара конфигурационных параметров, в первую очередь, IP-адрес. Остальные параметры передаются в виде DHCP-опций. Тип DHCP-сообщения определяется из значения опции 53 – DHCP Message Type. Кроме уже упомянутых DHCPDISCOVER, DHCPOFFER, DHCPREQUEST и DHCPACK, есть еще:

DHCPDECLINE – отказ со стороны клиента от IP-адреса, если клиент выявил, что этот IP-адрес уже используется.

DHCPNAK – отказ со стороны сервера, если запрос DHCP_REQUEST неправильный.

DHCPRELEASE – сообщение от клиента к серверу об освобождении выделенных до этого DHCP-ресурсов, если эти ресурсы больше не нужны.

DHCPINFORM – запрос от клиента к серверу о некоторых конфигурационных параметрах, если собственно IP-адрес назначен «вручную».

DHCPFORCERENEW – сообщение от сервера к клиенту о принудительном начале повторного взаимодействия по DHCP.

Остальные типы имеют отношение к опциональному расширению DHCP, позволяющему сторонней станции (не клиенту и не серверу) запрашивать информацию о DHCP-конфигурации.

По истечении времени валидности IP-адрес обновляется посредством целенаправленных (юникаст) DHCP_REQUEST и DHCP_ACK!

Для пересылки файлов используется упрощенный и менее надежный вариант протокола FTP, называемый TFTP. Клиент посылает запрос о предоставлении файла, далее идёт процесс загрузки файлов.

Существуют также более или менее модифицированные версии TFTP от различных разработчиков с разной степенью стандартизации, например, MTFTP (Multicast TFTP)

BOOTP, DHCP и TFTP используют транспорт UDP.

45 Поддержка удаленной загрузки в Windows и Linux

DHCP-клиент в Windows запускается автоматически и активизируется при отсутствии статического IP-адреса. Интерфейс для явного конфигурирования не предусмотрен. Если назначить IP-адрес с помощью протокола DHCP не удалось, то назначается случайный IP-адрес – Link Local.

DHCP-клиент в Linux представлен демоном `dhclient`.

Для активизации `dhclient` (при загрузке) необходимо отредактировать соответствующую строку в соответствующем конфигурационном файле.

Для «тонкой» настройки дополнительно редактируют стандартный конфигурационный файл `etc/dhclient.conf`.

На загружающей станции должны быть установлены и настроены как минимум два сервиса:

1. DHCP либо ему подобный.
2. TFTP либо ему подобный.

В серверных редакциях Windows имеется возможность установить собственный сервис DHCP. Начиная с Server 2008, предусмотрена роль `DHCP Server`. В Server 2003 R2 был компонент `Dynamic Host Configuration Protocol (DHCP).` Для конфигурирования используют оснастку `DHCP` (`dhcpmgmt.msc`).

Однако, сервис TFTP как отдельный полноценный компонент не поддерживается. Поэтому для организации удаленной загрузки обычно используют стороннее, более «полноценное», ПО.

46 Динамическая IPv4-адресация в IOS

Запуск DHCP-клиента в Cisco IOS происходит с помощью соответствующего аргумента команды ip address (`ip address dhcp`). Перед запуском DHCP-клиента можно настроить:

1. Время истечения (expiration time) ip адреса – ip dhcp client lease DAY HOURS MINUTES
2. Tftp коммуникацию – ip dhcp client request tftp-server-address
3. И т.д.

На маршрутизаторах Cisco поддерживается сервис DHCP. По умолчанию этот сервис запущен, для остановки используют команду no service dhcp.

Для просмотра состояния сервиса DHCP используют команды группы show ip dhcp; show ip dhcp binding; show ip dhcp conflict, show ip dhcp pool, show ip dhcp server statistics и другие.

```
Router#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.11.195      0100.1b21.228e.72       Mar 31 2015 12:39 PM    Automatic


Router#show ip dhcp pool

Pool EXAMPLE-DHCP_DYNAMIC_POOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 30
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.11.193       192.168.11.193   - 192.168.11.222    1
```

47 Специальные соглашения при IPv4-адресации и IPv4-Маршрутизации

Имеется несколько специальных соглашений в области IP-адресации:

1. 0.0.0.0 – так называемый Unspecified IPv4-адрес, формально адрес всей глобальной сети Internet, но имеет и другие смыслы, которые будут описаны в дальнейшем.

2. 255.255.255.255 – формально глобальный широковещательный адрес, но поскольку представляет большу'ю «опасность» уже давно интерпретируется как Limited Broadcast, то есть пакеты с такими адресами назначения должны «безоговорочно» подавляться шлюзами.

3. 127.0.0.1 (как и любой адрес из диапазона 127.X.X.X) – ассоциирован со специальным сетевым интерфейсом-заглушкой (loopback), необходимым для обеспечения переносимости ПО, то есть пакеты с такими адресами назначения, переданные приложениями, тут же программно возвращаются на прикладной уровень.

Специальные соглашения в области IP-маршрутизации:

1. Адрес назначения 0.0.0.0 – маршрут по умолчанию.

2. Маска подсети 255.255.255.255 – маршрут к одному сетевому интерфейсу

48 Правила записи IPv6-адресов

Наряду с общим сохранением преемственности, технологии IPv6 все -таки существенно отличаются от технологий IPv4. Изменены как длина, так и формат адреса. Формат представления и примеры записи одного и того же адреса IPv6:

X:X:X:X:X:X:X:X или же 1234:5678:9ABC:def0:1234:5678:9AbC:DEF0

где X – шестнадцатеричное (любой регистр) шестнадцати-битное число. То есть общая длина адреса составляет 128 битов. Поскольку часто встречаются длинные последовательности нулей, одно либо более рядом стоящих нулевых чисел можно сокращать как два двоеточия. Но нужно помнить об однозначности интерпретации адреса. Также можно не писать лидирующие нули в тетрадах (fd:: равносилен 00fd::)

1. В записи используются латинские буквы ЛЮБОГО регистра. Однако, несмотря на то, что шестнадцатеричные цифры сравниваются по коду символа без учёта регистра, IETF предлагает использовать только строчные буквы.
2. Незначащие нули в каждом поле можно опустить, однако каждая группа должна иметь хотя бы один знак, даже если она состоит из одних нулей.
3. Самая длинная последовательность нулевых полей заменяется двумя двоеточиями ("::"). Если таких последовательностей несколько, для предотвращения неоднозначности сжимается крайняя левая. Кроме того, "::" может использоваться для сокращения последовательности из только одного нулевого поля.
4. При использовании IPv6-адреса в URL необходимо заключать адрес в квадратные скобки:
   `http://[2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d]`
   Если необходимо указать порт, то он пишется после скобок:
   `http://[2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d]:8080`

49 IPv6-терминология в сравнении с IPv4-терминологией

1. Изменен формат заголовка пакета. Вместо заголовка фиксированной длины с фиксированными полями применяется гибкий базовый заголовок плюс набор необязательных заголовков различного формата.
2. Изменена иерархия адресного пространства. Применительно к IPv6-адресации механизм классов упразднен. Вместо классов широко применяется механизм адресных префиксов. Имеются три базовых типа адресов:
    1. Юникаст.
    2. Мультикаст.
    3. Эникаст.
    4. Бродкаст -адресов нет вообще.
3. Базовые типы, как таковые, не используются. Их делят на виды согласно специфике применения. Принадлежность к тому либо иному виду определяется по адресному префиксу – фиксированным начальным битам адреса.
4. Изменен подход к назначению адресов сетевым интерфейсам. Одному и тому же сетевому интерфейсу могут быть назначены несколько адресов различных типов. Допускается даже назначение более одного адреса одного типа и это вполне нормально.
5. Модифицированы понятия сети и подсети. Если в случае с IPv4 предусматривалась только одна глобальная сеть, то на базе IPv6 предполагается возможность построения нескольких независимых глобальных сетей. Понятие подсети расширено. Особо следует выделить линк – подсеть размером в один сегмент.
6. Модифицировано понятие станции (узла). Для ссылки на любой из видов пользовательских станций в основном используют обобщенный термин хост. Вместо термина «шлюз» используют обобщенный термин маршрутизатор.
7. Введены новые правила задания размера подсети. Маска подсети, как таковая, аннулирована. Размер подсети определяется по префиксу подсети – фиксированным начальным битам адресов из диапазона описываемой подсети.

50 Локальные IPv6-адреса типа юникаст

При IPv6-адресации приватные адреса, как таковые, не выделяются. Обобщенно их заменяют локальные адреса.

Адрес вида Link-local Unicast (FE80::/10) предназначен для использования в пределах линка. Выход пакетов с адресами Link-local Unicast за пределы линков должен подавляться маршрутизаторами.

Рисунок – Формат адреса вида Link-local Unicast

Как и в других юникаст-адресах, имеется четкое разделение на топологическую и интерфейсную части.

Адреса Link-local Unicast автоматически генерируются на базе MAC-адресов следующим образом.

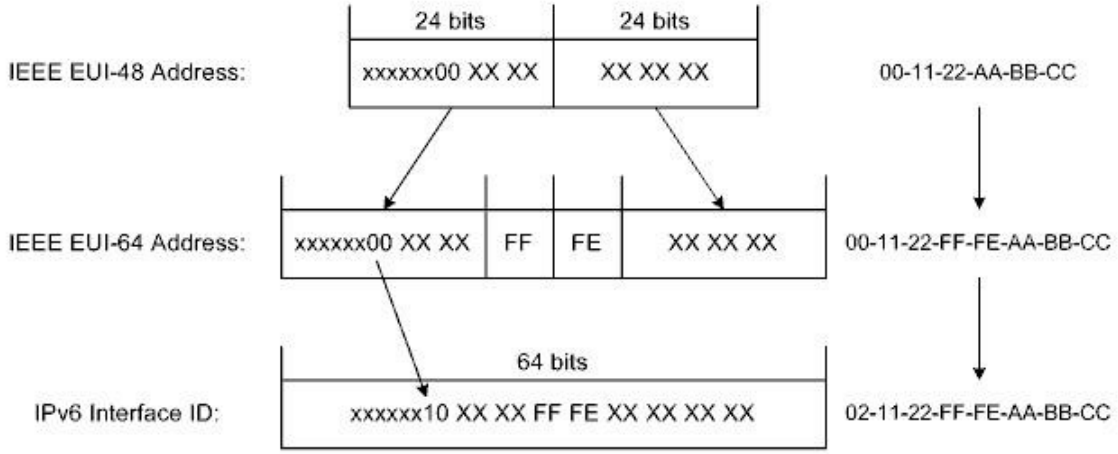


Рисунок – Алгоритм и пример вычисления значения поля IPv6 Interface ID

В результате, интерфейсная часть соответствует нотации EUI-64 (точнее, модифицированной нотации EUI-64). От приведенного правила можно отступать, но это не рекомендуется.

Для всех организаций, имеющих более или менее иерархическую подсетевую структуру и не испытывающих потребность во внешнем трафике, в качестве основной замены внутренних адресов IPv4 позиционируются адреса вида Unique Local Unicast (FC00::/7). Пакеты с адресами Unique Local Unicast должны подавляться всеми маршрутизаторами кроме внутренних.

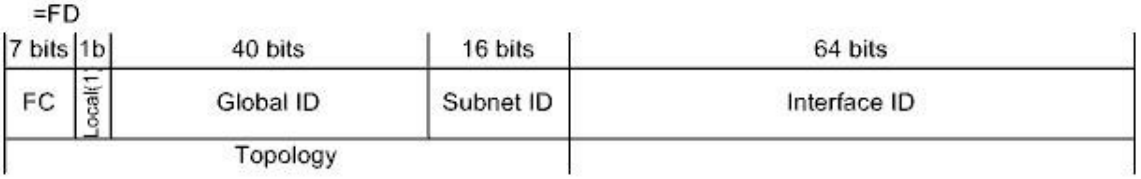


Рисунок – Формат адреса вида Unique Local Unicast

Для всех юникаст-адресов, в том числе Unique Local Unicast, приемлема (но не всегда удобна) EUI-64-нотация интерфейсной части.

51 Глобальные IPv6-адреса типа юникаст

Если в случае с IPv4 предусматривалась только одна глобальная сеть, то на базе IPv6 предполагается возможность построения нескольких независимых глобальных сетей.

В качестве основной замены реальных адресов IPv4 предлагаются адреса вида Global Unicast (2000::/3).

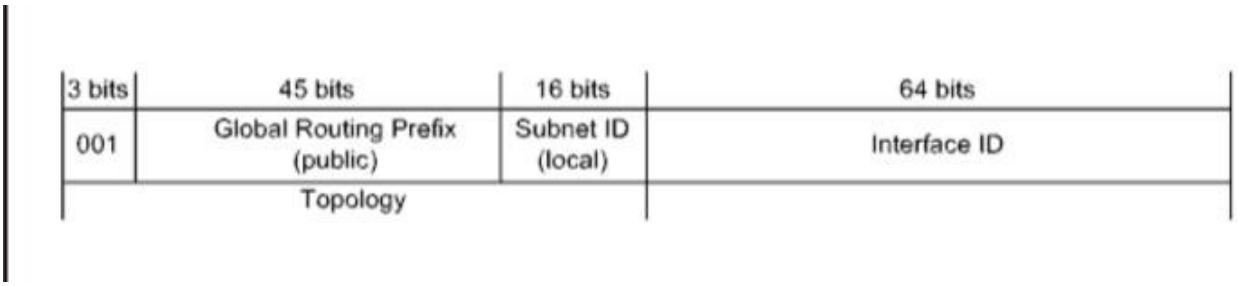


Рисунок – Формат адреса вида Global Unicast

Формат адресов Global Unicast претерпел эволюцию. Выше приведена современная трактовка – собственно Global Unicast (`2000::/3`). Непосредственными предшественниками были адреса Aggregatable Global Unicast (так же `2000::/3`), которые еще раньше сменили адреса Provider-based Unicast (`4000::/3`)

Наиболее значимые 48-разрядные обозначаются как префикс глобальной маршрутизации, который назначается конкретной автономной системе. Три наиболее значимых бита префикса глобальной маршрутизации всегда установлены на 001.

Соглашения в области IPv6-адресации:

1. Unspecified (`::/128`) – адрес всех глобальных сетей.

2. Loopback (`::1/128`) – адрес сетевого интерфейса – заглушки.

52 IPv6-адреса типа мультикаст и стандартные подсети

Адрес типа Multicast (FF00::/8) предназначен для использования в пределах подсети определенного вида и представляет собой уникальный в пределах таковой подсети групповой идентификатор.

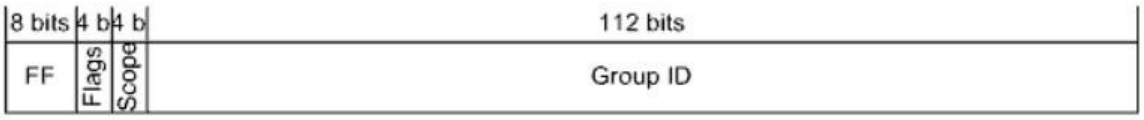


Рисунок -- Формат адреса типа Multicast

Применительно к линку, в качестве замены широковещательных адресов IPv4 позиционируются адреса вида Link-local Scope All-nodes Multicast.

Кроме того, при автоконфигурировании в пределах линка используются специальные адреса вида Solicited-node Multicast, строящиеся на основе адресов Link-local Unicast, из которых переносятся последние 24 бита.

Мультикаст-адреса могут присутствовать в пакетах только в поле Destination Address.

Понятие подсети расширено. Стандартизированы следующие виды подсетей, что, в частности, отражается в значениях специального для этого введенных четырехбитных полей Scope в форматах адресов некоторых видов: 0, F – Reserved.

1 – Interface-local.

2 – Link-local.

3 – Realm-local.

4 – Admin-local.

5 – Site-local.

6, 7, 9, A, B, C, D – Unassigned (по своему усмотрению).

8 – Organization-local.

E – Global.

Таким образом «очерчивается круг», в пределах которого адрес валиден и применяется.

Особо следует выделить линк (link) – подсеть размером в сегмент.

53 IPv6-адреса типа эникаст

Применительно к IPv6 эникаст-адреса обладают двумя специфическими свойствами (так задумывалось).

1. Во-первых, если юникаст-адрес присвоить более чем одному сетевому интерфейсу в подсети, то он превращается в эникаст-адрес.
2. Во-вторых, критерием выбора эникаст-адреса является кратчайшесть расстояния при маршрутизации.

Адрес типа Anycast предназначен для использования в пределах подсети и получается на основе префикса подсети.

Рисунок -- Один из форматов адреса типа Anycast

Соответствующие приведенному выше формату, одному из двух форматов Reserved Subnet Anycast, виды пока применения не нашли.

Единственным используемым на практике видом является Subnet-router Anycast.

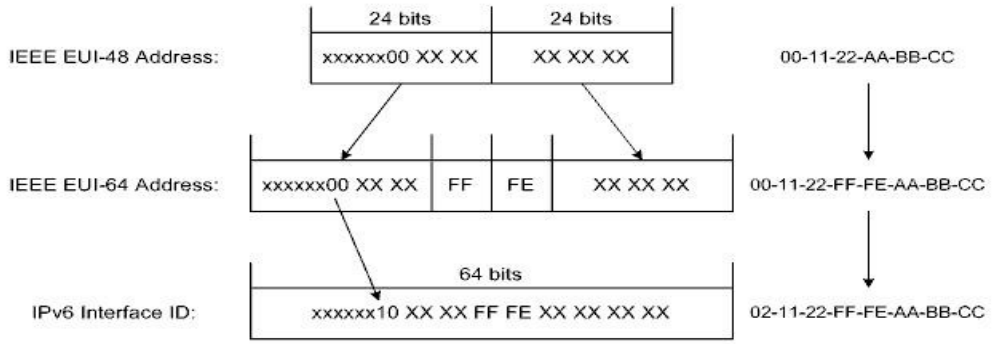
Рисунок -- Формат адреса вида Subnet-router Anycast

Такие адреса разрешено назначать только сетевым интерфейсам маршрутизаторов, и они могут присутствовать только в соответствующих служебных пакетах, причем только в поле Destination Address.

54 Нотация EUI-64 и инкапсуляция IPv6-адресов типа мультикаст

/// Информации о инкапсуляции нету в лекциях

Для всех юникаст-адресов, в том числе Unique Local Unicast, приемлема (но не всегда удобна) EUI-64-нотация интерфейсной части.



В результате, интерфейсная часть соответствует нотации EUI-64 (точнее, модифицированной нотации EUI-64). От приведенного правила можно отступать, но это не рекомендуется.

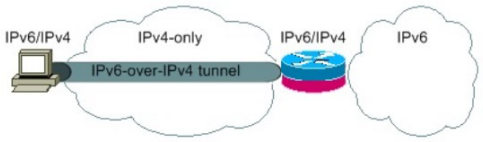
IPv6-пакеты, как и IPv4, обычно передаются с помощью протоколов канального уровня, таких как Ethernet, который инкапсулирует каждый пакет в кадр. Но IPv6-пакет может быть передан с помощью туннельного протокола более высокого уровня, например, в 6to4 или Teredo.

MAC-мультикаст адрес формируется на базе IPv6 мультикаст. Сначала идет два байта 33 33, а после - 32 младших бита IPv6 адреса.

55 Совместимость IPv6 с IPv4

В контексте совместимости IPv4 и IPv6, практический интерес представляет лишь возможность передавать трафик IPv6 посредством трафика IPv4, то есть организовывать туннели IPv6-over-IPv4. Таковые туннели делят на три типа:

1. Host-to-host.
2. Host-to-router и router-to-host.



3. Router-to-router.

Для обеспечения совместимости с IPv4 стандартизированы следующие виды адресов IPv6.

1. Адрес вида IPv4-compatible (::D.D.D.D/128). Включает публичный адрес IPv4. В настоящее время использование этих адресов не рекомендуется.
2. Адрес вида IPv4-mapped (::FFFF:D.D.D.D/128). Предназначен для использования при работе с виртуальной станцией IPv4 внутри станции IPv6. В физических пакетах эти адреса недопустимы и в основных реализациях не поддерживаются.
3. Адрес вида 6to4 Unicast

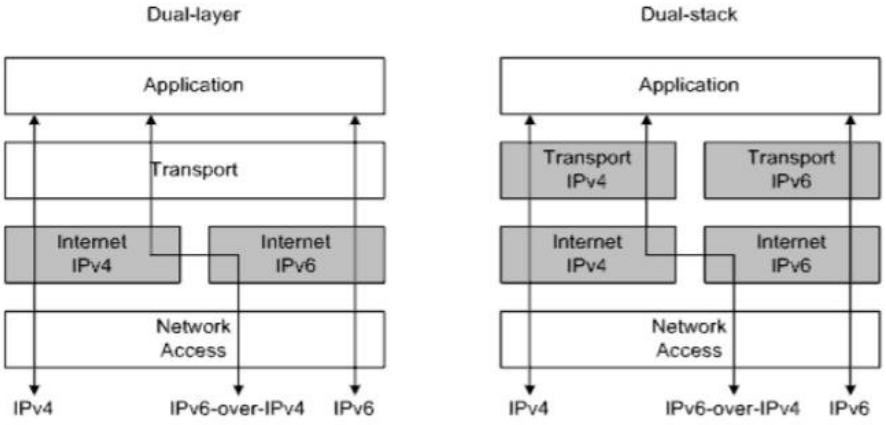
16 bits	32 bits	16 bits	64 bits
2002	Hex IPV4	Subnet ID	Interface ID
	Topology		

Включает шестнадцатеричное представление публичного адреса IPv4 и предназначен для формирования автоматических туннелей. Это один из видов туннельных адресов, поддерживаемый всеми основными реализациями.

Вопросы совместимости IPv4 и IPv6 затрагивают работу всего семейства протоколов TCP/IPv6. Выделяют две архитектуры:

1. Dual-layer – IPv4 и IPv6 разделены только на Internet-уровне модели TCP/IP.
2. Dual-stack – стеки TCP/IPv4 и TCP/IPv6 полноценны и независимы

В оптимальном случае трафик IPv6 полностью отделен от трафика IPv4.



56 Модели и задачи IPv6-автоконфигурирования

В сравнении с IPv4, возможности динамической IPv6-адресации значительно расширены и усовершенствованы, вплоть до полного автоконфигурирования.

Предусмотрены две базовых модели:

1. Stateless – распределенное управление, адреса и другие параметры конфигурируют с помощью служебных сообщений, базируется на ICMPv6 (Internet Control Message Protocol).
2. Stateful – централизованное управление, адреса и другие параметры передаются по специальному протоколу, базируется на DHCPv6.

Причем, в качестве приоритетной модели рассматривают первую, а не вторую.

ICMPv6, кроме всего прочего, включает в себя два мощных функционала:

1. Neighbor Discovery (ND) – граничное обнаружение.
2. Multicast Listener Discovery (MLD) – обнаружение мультикаст-станции-потребителя.

При разработке ND были четко сформулированы девять задач для решения в границах линка:

1. Обнаружение соседних маршрутизаторов.
2. Восстановление значений префиксов подсетей.
3. Восстановление значений некоторых других параметров.
4. Автоконфигурирование адресов.
5. Восстановление MAC-адресов соседних станций.
6. Обнаружение маршрутизаторов следующего звена.
7. Проверка достижимости соседних станций.
8. Проверка конфликтов адресов.
9. Оптимизация маршрутов.

Важно, что задачи ND решают именно в пределах линка.
Для обеспечения ND предусмотрены пять типов ICMPv6-сообщений:

1. RS (Router Solicitation).
2. RA (Router Advertisement).
3. NS (Neighbor Solicitation).
4. NA (Neighbor Advertisement).
5. Redirect.

Под адвертайзингом (advertising) понимают «предлагать услуги», а солиситингом (soliciting) – «спрашивать об услугах».

57 Обнаружение маршрутизаторов и оптимизация маршрутов при IPv6-автоконфигурировании

ICMPv6, кроме всего прочего, включает в себя два мощных функционала:

1. Neighbor Discovery (ND) – граничное обнаружение.
2. Multicast Listener Discovery (MLD) – обнаружение мультикаст-станции-потребителя.

При разработке ND были четко сформулированы девять задач для решения в границах линка:

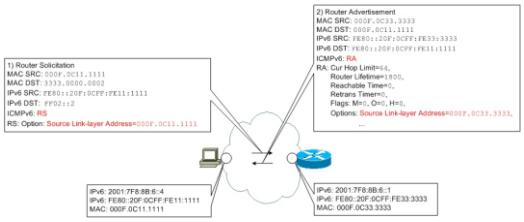
1. Обнаружение соседних маршрутизаторов.
2. Восстановление значений префиксов подсетей.
3. Восстановление значений некоторых других параметров.
4. Автоконфигурирование адресов.
5. Восстановление MAC-адресов соседних станций.
6. Обнаружение маршрутизаторов следующего звена.
7. Проверка достижимости соседних станций.
8. Проверка конфликтов адресов.
9. Оптимизация маршрутов.

Важно, что задачи ND решают именно в пределах линка.
Для обеспечения ND предусмотрены пять типов ICMPv6-сообщений:

1. RS (Router Solicitation).
2. RA (Router Advertisement).
3. NS (Neighbor Solicitation).
4. NA (Neighbor Advertisement).
5. Redirect

Под адвертайзингом (advertising) понимают «предлагать услуги», а солиситингом (soliciting) – «спрашивать об услугах».

Для решения первой задачи используется связка RS и RA (RS посылается маршрутизатором, ищущим другие, RA – ответ).



Согласно стандарту ND, маршрутизаторы должны не только отвечать на RSes, а и периодически передавать RAs «на упреждение», анонсируя свое присутствие в линке.

Важно, что задачи ND решают именно в пределах линка. ND – это механизм, вполне допускающий конфигурирование. Многие параметры могут быть заданы.

ND нельзя рассматривать как альтернативу динамической маршрутизации. ND работает в рамках линка и, по понятным причинам, на ND не возлагают обязанности автоматического нахождения маршрутов к внешним подсетям.

А вот автоматически назначать маршрут по умолчанию ND может. Более того, при автоконфигурировании все соседние маршрутизаторы автоматически рассматриваются как кандидаты в маршрутизаторы по умолчанию – создается специальный список.

Текущий маршрутизатор по умолчанию рекомендуется выбирать исходя из состояния связей (ND-кэша). А также исходя из значения специального поля в RA под названием Router Lifetime – время жизни маршрутизатора (нулевое значение запрещает использовать маршрутизатор как маршрутизатор по умолчанию).

Если же в линке оказывается несколько равноценных маршрутизаторов, то как правило, выбирается первый «попавшийся» маршрутизатор.

Для решения последней задачи используется специальное сообщение Redirect. Сообщение Redirect содержит следующие ключевые поля:

1. Target Address – адрес Link-local Unicast соседа, которому в дальнейшем нужно напрямую передавать пакеты с указанным адресом назначения;
2. Destination Address – адрес назначения;

и две ND-опции:

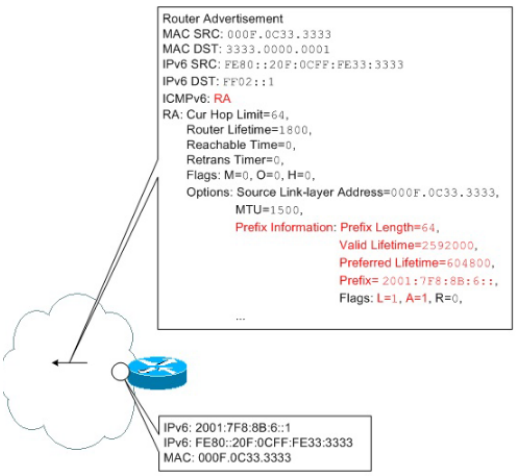
1. Target Link-layer Address - MAC-адрес соседа, которому в дальнейшем нужно напрямую передавать пакеты;
2. Redirected Header – фрагмент предварительно принятого пакета, который послужил причиной создания данного сообщения

58 Восстановление параметров при IPv6-автоконфигурировании

// + Общая часть про ND, MLD, задачи, ND-messages, etc.

Хост (маршрутизатор) восстанавливает значения префиксов подсетей путем анализа RA.

Отдельный префикс подсети анонсируется маршрутизатором в виде отдельной ND-опции Prefix Information



со следующими ключевыми полями:

1. Prefix Length – длина префикса;
2. Valid Lifetime – общее время жизни;
3. Preferred Lifetime – интервал времени, в течение которого адрес, сгенерированный на основе данного префикса подсети, будет считаться предпочтительным;
4. Prefix – собственно префикс подсети; включая флаги: L – данный префикс подсети относится к текущему линку; A – данный префикс подсети может быть использован для генерирования адресов.

RA вкладывается столько ND-опций, сколько нужно. Анонсируются все префиксы подсетей из привязанного к сетевому интерфейсу списка AdvPrefixList. Существует настоятельная рекомендация о том, что на маршрутизаторе в этот список по умолчанию вносятся префиксы всех подсетей, к которым относится сетевой интерфейс, исключая префиксы подсетей Link-local Unicast. При необходимости, список может быть дополнен «вручную».

В результате анализа RA, маршруты ко всем соответствующим подсетям автоматически вносятся в таблицу маршрутизации – как маршруты к своим подсетям. Хост (маршрутизатор) восстанавливает значение еще двух важных параметров, опять же, путем анализа RA.

1. Первым таковым параметром является Cur Hop Count. Значение будет вписываться в поле Hop Limit заголовка IPv6 каждого передаваемого маршрутизатору пакета.
2. Вторым параметром является MTU (maximum transmission unit). В линках с вариативным MTU, например, Ethernet, маршрутизатор обязан указывать (ND-опция).

59 Автоконфигурирование адресов и их жизненный цикл при IPv6-автоконфигурировании

// + Общая часть про ND, MLD, задачи, ND-messages, etc.

В контексте SLAAC (Stateless Address Autoconfiguration) под автоконфигурированием адресов понимают автоматическое назначение сетевому интерфейсу юникаст-адресов, не затрагивая адреса Link-local Unicast. Адреса Link-local Unicast также назначаются автоматически, но вне рамок автоконфигурирования.

Топологическая часть адреса берется из ND-опции Prefix Information в RA от маршрутизатора, а для интерфейсной части используется нотация EUI-64. При этом воспринимаются только префиксы подсети длиной 64 бита. Если маршрутизаторов несколько, то воспринимаются префиксы от всех маршрутизаторов.

Автоконфигурирование позиционируют прежде всего в отношении хостов, однако и сетевые интерфейсы маршрутизаторов могут быть подвержены автоконфигурированию. При этом соответствующие префиксы подсетей в RAs не включаются.

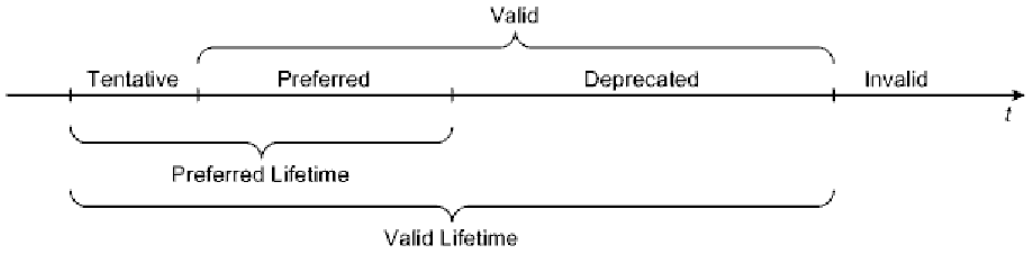
SLAAC и DHCPv6 вполне совместимы друг с другом. «Разделение обязанностей» контролируется двумя флагами в RA: M (managed address configuration) – адреса доступны посредством DHCPv6; O (other configuration) – другие параметры доступны посредством DHCPv6 (если флаг M установлен, то флаг O игнорируется).

Автоконфигурирование адресов подразумевает и автоматическое нахождение маршрутизатора по умолчанию.

Адреса DNS-серверов автоматически могут быть получены только посредством DHCPv6.

Состояния адреса, полученного в результате автоконфигурирования:

1. Tentative – уникальность адреса еще не проверена.
2. Preferred – адрес является предпочтительным.
3. Deprecated – использование адреса нежелательно.
4. Valid – адрес находится в состоянии Preferred либо Deprecated.
5. Invalid – время жизни адреса истекло.



Валидность сгенерированных адресов контролируется двумя таймерами:

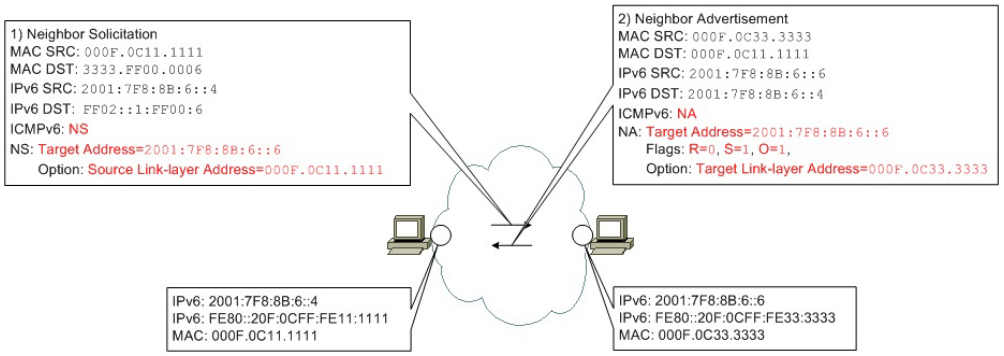
1. Preferred Lifetime – интервал времени, в течение которого адрес является предпочтительным;
2. Valid Lifetime – интервал времени, равный собственно времени жизни адреса.

Таймеры инициализируются исходя из значений соответствующих полей в сообщениях ND либо DHCPv6.

60 Восстановление адресов при IPv6-автоконфигурировании и проверка конфликтов адресов

// + Общая часть про ND, MLD, задачи, ND-messages, etc.

Для решения пятой задачи используется связка NS и NA.



NA содержит три флага: R (Router) – данное NA передано маршрутизатором (не хостом), S (Solicited) – данное NA передано в ответ на NS, O (Override) – данное NA содержит новый MAC-адрес.
Опять же, стандарт ND не запрещает передавать NA «на упреждение» (для анонсирования, без предшествующей просьбы).

Проверка конфликтов адресов является 8й задачей для решения в границах линка

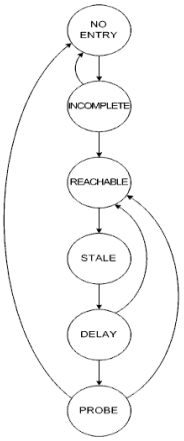
Не смотря на всю гибкость IPv6, проверку конфликта адресов никто не отменял – исключая эникаст-адреса. Задача DAD (Duplicate Address Detection) решается передачей специальным образом наполненного NS (с нулевым IPv6-адресом источника) и проверкой есть ли ответ.

61 Проверка достижимости при IPv6-автоконфигурировании

Задача NUD (Neighbor Unreachability Detection) является закономерным «продолжением» задачи восстановления MAC-адресов и так же решается использованием связки NS и NA.

Каждый сетевой интерфейс IPv6 должен иметь свой ND-кэш. ND-кэш напоминает ARP-таблицу. Каждому из соседей в ND-кэше соответствует строка и одно из состояний:

1. INCOMPLETE – сосед неизвестен, возникла необходимость передать ему пакет, идет восстановление его MAC-адреса.
2. REACHABLE – сосед известен и считается достижимым.
3. STALE – сосед известен, уже считается недостижимым, но нет необходимости передать ему пакет.
4. DELAY – сосед известен, считается недостижимым, возникла необходимость передать ему пакет, пакет передан, ожидается подтверждение от протоколов вышестоящих уровней (именно так).
5. PROBE – идет собственно проверка достижимости соседа.



В отличие от ARP, проверка достижимости соседа проводится, причем по мере надобности – упор сделан на то, что сетевые интерфейсы способны сообщать о своем состоянии. Одна проверка достижимости соседа, как и одно восстановление MAC-адреса подразумевает несколько попыток (согласно стандарту по умолчанию три и три попытки соответственно).

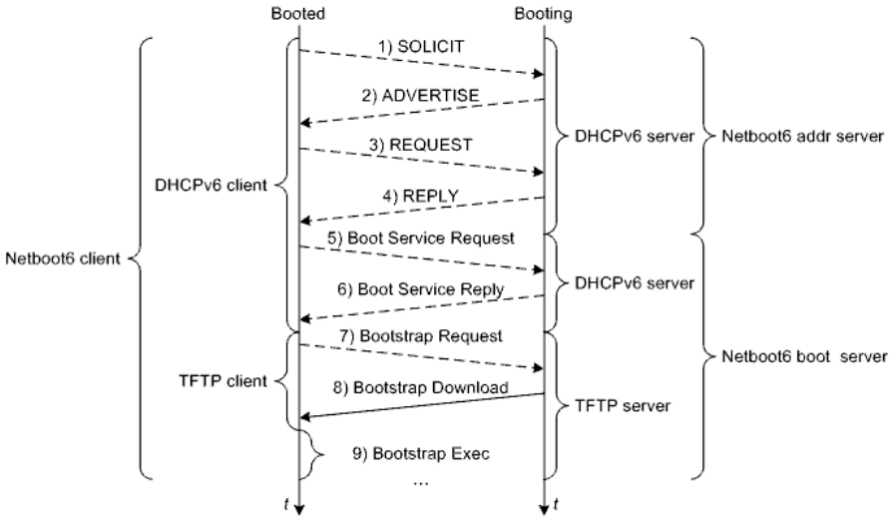
Алгоритм проверки достижимости опирается на два основных таймера:

1. Reachable Time – интервал времени после приема последнего сообщения NA от соседа, в течение которого этот сосед считается достижимым. Задаёт время «REACHABLE».
2. Retrans Timer – интервал между передачей NSes при переходе к следующей попытке.

Маршрутизаторы могут предлагать значения этих таймеров в отношении линка анонсируя RAs с ненулевыми значениями одноименных полей.

62 Взаимодействие по протоколу Netboot6

Netboot6 – аналог PXE для IPv6. В целом взаимодействие такое же, как и по PXE.



1. Клиент рассылает сообщение SOLICIT, в котором клиент описывает себя и потребность поиска сервиса адресации, коим является DHCPv6-сервер. Является аналогом DHCPDISCOVER. Рассылается в МУЛЬТИКАСТЕ. В IPv6 нету бродкаст! Содержит Identity Association Identifier, таймеры (renew, rebind) и т.д.
2. ADVERTISTE – Аналог DHCPOFFER. DHCP-сервер сразу выдает DHCP-клиенту IP-адрес и отвечает о своей готовности. Также содержит IAID, таймеры. Выдаёт IP address, preferred lifetime, valid lifetime адреса.
3. REQUEST – Аналог DHCPREQUEST. Клиент подтверждает, что выбрал определённый сервер и запрашивает IP адрес и требующиеся конфигурационные параметры. Содержит предоставленный выше IP, lifetime-ы, таймеры и т.д.
4. REPLY – Аналог DHCPACK - DHCP-сервер подтверждает подтверждение и параллельно предоставляет значения всех предварительно сконфигурированных параметров из тех, что были запрошены. Содержит адрес DNS сервера и Domain-name.

Далее идёт всё, как и в PXE:

5. Boot Service Request – аналог Boot Service Discover – клиент посредством DHCP посылает запрос о предоставлении загрузочного сервиса.
6. Boot Service Reply – аналог Boot Service ACK – DHCP-сервер, находящийся на стороне загрузочного сервиса, подтверждает предоставление услуг.
7. Bootstrap Request – TFTP-клиент в составе PXE-клиента посылает запрос о предоставлении файла – загрузчика bootstrap.
8. Bootstrap Download – TFTP-клиент скачивает файл – загрузчик bootstrap.
9. Bootstrap Exec – загрузчик bootstrap исполняется.

63 Протоколы DHCPv6 и его использование

/// Не уверен в правильности

DHCPv6 — это сетевой протокол для конфигурации узлов версии для IPv6.

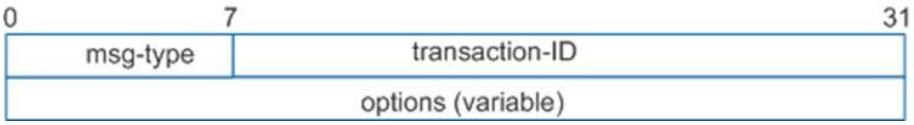
DHCPv6 использует номер порта 546 для клиентов и номер порта 547 для серверов. По сути, такой же DHCP, как и для IPv4.

Специально для обращения к DHCPv6-серверам и DHCPv6 relays стандартизированы два вида мультикаст-адресов:

1. Link-local All DHCP Relay Agents and Servers (FF02::1:2)
2. Site-local All DHCP Servers (FF05::1:3).

Современные реализации TFTP поддерживают IPv6

Формат сообщения DHCPv6:



1. msg-type - 1байт - Указывает тип сообщения в диапазоне от 1 до 13.
2. transaction-ID - 3 байта - Идентификатор взаимодействия DHCPv6, также называемый идентификатором транзакции, используется для идентификации обмена сообщениями DHCPv6 в обоих направлениях.
3. Options - Указывает поле параметра DHCPv6. Это поле содержит информацию о конфигурации, назначенную сервером DHCPv6 хосту IPv6, например, IPv6-адрес DNS-сервера.

Одни и те же DHCPv6-опции могут передаваться в обоих направлениях. В отличие от DHCPv4-опций, DHCPv6-опции имеют сложный формат с вариативным количеством полей и подопций. DHCPv6-клиент не обязан выполнять «предписания» DHCPv6-сервера, даже сам может «высказывать пожелания» о значениях некоторых параметров DHCPv6-серверу.

DHCPv6-клиент и DHCPv6-сервер должны иметь уникальные идентификаторы DUIDs (DHCP Unique IDentifiers), по которым они однозначно опознают друг друга.

DHCPv6-сервер способен выдавать как постоянные, так и врЕменные адреса. Постоянные адреса имеют Valid Lifetime и Preferred Lifetime. Для обеспечения выдачи и последующего сопровождения адресов, между DHCPv6-клиентом и DHCPv6-сервером создается ассоциация с уникальным идентификатором IAID (Identity Association IDentifier).

Валидность выданных адресов контролируется двумя таймерами:

1. T1 – интервал времени, начиная с приема REPLY, по истечении которого необходимо передать RENEW
2. T2 – интервал времени, начиная с приема REPLY, по истечении которого необходимо передать REBIND, если не поступило ответа на RENEW.

Если не поступило ответа на REBIND, то по истечении Valid Lifetime адрес становится недействительным. Кроме адресов, посредством DHCPv6 можно передавать префиксы подсетей.

64 Проблемы при IPv6-маршрутизации и их решения

1 проблема: Общее правило IP-адресации гласит, что подсети, к которым относятся разные сетевые интерфейсы маршрутизатора, не должны перекрываться.

Однако формат адресов LLU напрямую нарушает приведенное правило и порождает проблему выбора выходного сетевого интерфейса при передаче пакета, созданного на маршрутизаторе вне рамок ND. В таблице маршрутизации возникают несколько абсолютно равноправных маршрутов к подсети. Проблему решают явным указанием выходного сетевого интерфейса.

2 проблема: Согласно идеологии IPv4, в качестве адреса источника подставляется адрес выходного интерфейса. Наличие у одного сетевого интерфейса множества адресов разных видов создает проблему выбора адреса источника при инкапсуляции, когда пакет создан на самом маршрутизаторе и адрес источника явно не задан.

Сформулированы восемь единых правил для всех реализаций:

1. Приоритетнее адрес, совпадающий с адресом назначения.
2. Приоритетнее адрес из подсети, вид которой более приближен к виду подсети назначения.
3. Preferred-адрес приоритетнее deprecated-адреса.
4. Домашний адрес приоритетнее дорожного адреса (мобильность).
5. Приоритетнее адрес сетевого интерфейса, обращенного в сторону адреса назначения.
6. Приоритетнее адрес, чья метка равна метке адреса назначения.
7. Временный адрес приоритетнее постоянного.
8. Приоритетнее адрес из подсети, которая имеет наиболее длинный общий префикс с подсетью назначения

Адреса сравниваются попарно. Если текущее правило не выявило победителя, то выполняется переход к следующему правилу. Если в результате выявить одного победителя не удалось, то дальнейший выбор зависит от реализации.

3 проблема: Возникает и еще один закономерный вопрос – о том, адреса каких видов использовать для указания маршрутизаторов следующего звена при вводе статических маршрутов.

Согласно рекомендациям о применении IPv6, при настройке статической маршрутизации между маршрутизаторами, для ссылки на маршрутизаторы следующего звена рекомендуется использовать адреса Link-local Unicast, как это и делают протоколы динамической маршрутизации. А маршрутизатор по умолчанию для хостов рекомендуется назначать автоматически – посредством ND.

Имеет право на существование альтернативный подход, заключающийся в независимой настройке статической маршрутизации в отношении подсетей различных видов.

65 Поддержка мобильности в IPv6

Новой возможностью IPv6 является заложенная целенаправленная поддержка адресации мобильных станций.

Мобильный хост изначально «приписан» к своему домашнему линку. В домашнем линке мобильному хосту, как правило автоматически, назначается домашний адрес. В домашнем линке определен домашний префикс подсети. Любой доступный линк, в который мобильный хост может быть перемещен из домашнего, является для этого хоста чужим линком.

В чужом линке мобильному хосту также назначается адрес – дорожный адрес. В чужом линке определен чужой префикс подсети. Если мобильный хост находится в чужом линке, то он регистрируется у своего домашнего агента, который затем перенаправляет трафик с домашнего адреса на дорожный адрес через специально создаваемый туннель. Таким образом, мобильный хост всегда доступен по домашнему адресу, вне зависимости от места фактического подключения.

Поддержка мобильности реализуется посредством следующих составляющих:

1. Специальный заголовок Mobility header – заголовок для обеспечения мобильности.
   Этот заголовок используется для пересылки восьми типов mobility-сообщений. Все mobility-сообщения обеспечивают привязку мобильного хоста. Mobility-сообщения могут включать в себя различные mobility-опции.
2. Дополнительная опция: Home Address. С помощью этой опции мобильный хост указывает свой домашний адрес.
3. Специальный тип маршрутизационного заголовка. Используется для пересылки пакета от станции-корреспондента напрямую к мобильной станции и содержит домашний адрес.
4. Четыре вида ICMPv6-сообщений (Home Agent Address Discovery Request, Home Agent Address Discovery Reply, Mobile Prefix Solicitation, Mobile Prefix Advertisement). Используются при взаимодействии мобильного хоста и домашнего агента.
5. Дополнения ND. флаг в RA: H (Home Agent) – данный маршрутизатор является домашним агентом. Еще один флаг в ND-опции Prefix Information: R (Router Address) – данная ND-опция содержит полный адрес маршрутизатора

66 Специальные соглашения при IPv6-адресации и IPv6-Маршрутизации

Соглашения в области IPv6-адресации:

1. Unspecified (::/128) – адрес всех глобальных сетей.
2. Loopback (::1/128) – адрес сетевого интерфейса – заглушки.

Изменения в маршрутизации. Специальные соглашения:

1. ::/0 – маршрут по умолчанию.
2. X … X < 64 - маршрут к большей чем линк подсети.
3. X:X:X:X/64 – маршрут к подсети (в том числе и оконечной) размером с линк.
4. X:X:X:X:X:X:X:X/128 – маршрут к одному сетевому интерфейсу

67 Статическая и динамическая IPv6-адресация в Windows

В Linux- и Windows-станции с текущими реализациями IPv6 по умолчанию относятся к типу IPv4/IPv6 (можно скорректировать).

Как и в случае с другими реализациями IPv6, нужно соблюдать правила назначения адресов сетевым интерфейсам. Типовой хост имеет следующие адреса:

1. Адрес Link-local Unicast.
2. Дополнительные адреса Unicast (Unique Local Unicast и Global Unicast).
3. Адрес сетевого интерфейса – заглушки.
4. Адрес Link-local All Nodes Multicast.
5. Адреса Solicited-node Multicast для каждого из адресов Unicast.
6. Дополнительные групповые адреса Multicast.
7. Адреса туннелей IPv6-over-IPv4.

Типовой маршрутизатор, в дополнение к указанным адресам (применительно к каждому из сетевых интерфейсов), имеет следующие:

8. Адреса Link-local All Routers Multicast каждого из сетевых интерфейсов.
9. Адреса Site-local All Routers Multicast соответствующих сетевых интерфейсов.
10. Адреса Subnet-router Anycast для каждой из подсетей.

В Windows XP SP2 и Server 2003 поддержка IPv6 уже была интегрирована в составе Advanced Networking Pack и устанавливалась как опциональный компонент с помощью графического интерфейса (свойства сетевых интерфейсов) либо командой netsh interface ipv6 install. Для работы с адресами использовались только расширения команды netsh interface ipv6 (вместо отмененной команды ipv6).

Полноценная поддержка IPv6 доступна начиная с Windows Vista и Server 2008. Может быть задействован как графический интерфейс, так и различные варианты команды netsh interface ipv6.

Начиная с Windows 10 1607 по умолчанию запрещен туннельный интерфейс 6to4, Windows 10 1703 – ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), Windows 10 1803 – Teredo.

Следует обратить внимание на то, что по умолчанию автоконфигурирование работает даже при статическом конфигурировании адресов.

Конфигурирование IPv6 в Windows 10:

Можно через: Settings -> Internet and networks -> Choose network properties -> Edit -> static -> enable IPv6.

Можно через netsh:
Генерирование временных адресов:

```
>netsh interface ipv6 set privacy=enabled|disabled
```

Автоконфигурирование адресов:

```
>netsh interface ipv6 set interface Interface_Name_Or_Index routerdiscovery=enabled|disabled|dhcp
```

Можно через: панель управления –> сети –> выбрать сеть -> tcp/ip -> ipv6

Некоторые новые и обновленные команды:

- `ipconfig`
- `netsh interface ipv6 show interface`
- `ping`
- `netsh interface ipv6 show neighbors`

68 Статическая и динамическая IPv6-адресация в Linux

//+ общая часть про IPv6 из предыдущего вопроса

Linux поддержка IPv6 имеется в дистрибутивах с ядрами 2.2.x и последующими. Присвоение адресов IPv6 сводится к работе с соответствующими конфигурационными файлами.

Примеры IPv6-дополнений в конфигурационных файлах Linux:

`/etc/sysconfig/network`:

```
...
NETWORKING_IPV6=yes
...
```

– Общая информация, что IPv6 поддерживается

`/etc/network/interfaces` (ветвь Debian):

```
...
iface eth1 inet6 static
    address 2001:7f8:8b:6::4
    netmask 64
    gateway 2001:7f8:8b:6::1
iface eth1 inet6 static
    address fd00:0:0:6::4
    netmask 64
    gateway fd00:0:0:6::1
...
```

– Информация о сетевых интерфейсах

Примеры управления IPv6-автоконфигурированием в Linux:

Генерирование временных адресов:

```
#sysctl net.ipv6.conf.default.use_tempaddr=integer
```

либо

```
#echo "integer" > /proc/sys/net/ipv6/conf/default/use_tempaddr
```

где `integer`:
<= 0 -- запрет
= 1 -- разрешение, причем временные адреса менее приоритетны
> 1 -- разрешение, причем временные адреса более приоритетны

Автоконфигурирование, включая ND:

конфигурационный файл `/etc/sysconfig/network-scripts/ifcfg-<interface-name>`:

```
...
IPV6_AUTOCONF=yes|no
IPV6_ROUTER=yes|no
...
```

демон `radvd` со стандартным конфигурационным файлом `/etc/radvd.conf`

Примеры управления совместимостью с IPv4 в Linux с помощью RADVD (daemon):

6to4:

конфигурационный файл `/etc/sysconfig/network-scripts/ifcfg-<interface-name>`:

```
IPV6TO4INIT=yes
IPV6TO4_ROUTING="eth0-:1::1/64"
IPV6_CONTROL_RADVD=yes
```

С помощью Teredo: предоставляет пакет Miredo, предоставляющий одноименный сервис, со стандартным конфигурационным файлом /etc/miredo.conf

Обновленные команды для проверки информации и корректной работы ipv6 в Linux:

1. ifconfig;
2. ping6
3. ip -6 neigh show – просмотр информации о соседях.

69 Статическая и динамическая IPv6-адресация в IOS

На маршрутизаторах и коммутаторах Cisco IPv6-возможности по умолчанию находятся в административно выключенном состоянии. Для административного включения на сетевом интерфейсе IPv6 и автоматической генерации адреса Link-local Unicast используют команду `ipv6 enable`. Как альтернатива, позволяющая в добавок задействовать возможности ND, выступает команда `ipv6 address autoconfig`.

Для присвоения сетевому интерфейсу адреса Unique Local Unicast либо Global Unicast, и тем самым активации на нем IPv6, используют команду `ipv6 address`.
После ввода первого такого адреса автоматически генерируется и адрес Link-local Unicast.

Вариант с аргументом `eui-64` позволяет автоматически сгенерировать соответствующее значение интерфейсной части адреса. Вариант с аргументом `link-local` позволяет заменить автоматически сгенерированный адрес Link-local Unicast. Вариант с аргументом `anycast` позволяет добавить соответственно эникаст-адрес.

При вводе адресов можно использовать заранее подготовленные именованные префиксы, которые создают с помощью команды `ipv6 general-prefix`.

Для работы с мультикаст-группами используют различные варианты команды `ipv6 mld`, например, `ipv6 mld join-group`.

Для вывода на экран IPv6-информации о сетевом интерфейсе (в том числе информации о ND) используют команду `show ipv6 interface`.

Для просмотра информации о соседях используют команду `show ipv6 neighbors`.

Команды `ping` и `traceroute` совместимы с IPv6

Для просмотра таблицы IPv6-маршрутизации используют команду `show ipv6 route`.

В режим IPv6-маршрутизатора переключают командой `ipv6 unicast-routing`.

Шестнадцатеричные цифры в IPv6-адресах при выводе на экран и при переносе в конфигурационные файлы приводятся к верхнему регистру.

70 Поддержка совместимости IPv6 с IPv4 в Windows, Linux и IOS

В Windows нужно изменить ключ реестра или использовать команду `netsh interface ipv6`:

Ключ реестра:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters\DisabledComponents
```

где `DisabledComponents` (`DWORD`) формируется из битов:
бит 0 = 1 -- запрет всех туннельных интерфейсов IPv6-over-IPv4
бит 1 = 1 -- запрет туннельного интерфейса 6to4
бит 2 = 1 -- запрет туннельного интерфейса ISATAP
бит 3 = 1 -- запрет туннельного интерфейса Teredo
бит 4 = 1 -- разрешение IPv6 только посредством туннельных интерфейсов IPv6-over-IPv4
бит 5 = 1 -- IPv4 предпочтительнее IPv6

Варианты команды `netsh interface ipv6`:

```
>netsh interface ipv6 6to4 set state state=enabled|disabled|default
>netsh interface ipv6 isatap set state state=enabled|disabled|default
>netsh interface ipv6 set teredo type=disabled|client|enterpriseclient|server|default
```

В Linux можно использовать демонов `RADVD`, протокол `ISATAP`, пакет `Miredo`:

Возможности `radvd`

6to4:

конфигурационный файл `/etc/sysconfig/network-scripts/ifcfg-<interface-name>`:

```
IPV6TO4INIT=yes
IPV6TO4_ROUTING="eth0-:1::1/64"
IPV6_CONTROL_RADVD=yes
```

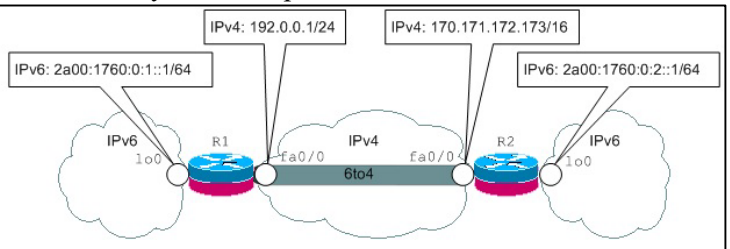
ISATAP:

```
#ip tunnel add is0 mode isatap local 192.168.11.216
#ip addr add fd00::6:0:5efe:192.168.11.216/64 dev is0
#ip link set is0 up
```

Teredo:

пакет Miredo, предоставляющий одноименный сервис, со стандартным конфигурационным файлом `/etc/miredo.conf`

В IOS для этого используется набор команд “tunnel”:



192.0.0.1 -> c000:1

```
R1(config)#interface tunnel 0
R1(config-if)#ipv6 address 2002:c000:1:1::1/16
R1(config-if)#tunnel source 192.0.0.1
R1(config-if)#tunnel mode ipv6ip 6to4
R1(config-if)#exit
R1(config)#ipv6 route 2a00:1760:0:2::/64 2002:aaab:acad:1::1
```

170.171.172.173 -> aaab:acad

```
R2(config)#interface tunnel 0
R2(config-if)#ipv6 address 2002:aaab:acad:1::1/16
R2(config-if)#tunnel source fa0/0
R2(config-if)#tunnel mode ipv6ip 6to4
R2(config-if)#exit
R2(config)#ipv6 route 2a00:1760:0:1::/64 2002:c000:1:1::1
```

В IOS передача между обычными пакетами и туннельными отличается:

1. Пакет «выкидывается» в интерфейс туннеля (IP интерфейса не требуется)
2. При инкапсуляции выполняется считывание параметров туннеля.
3. Адреса назначения задаются прикладными процессами, если не заданы в пакете до этого.
4. В качестве источника – IPv4 адрес второй точки туннеля.

71 Таблицы IPv6-маршрутизации в Windows, Linux и IOS

Основными отличиями в маршрутизации являются увеличение количества строк таблицы маршрутизации и изменение набора полей, что вполне адекватно ситуации.

В типовую таблицу маршрутизации включаются следующие маршруты:

1. К своим подсетям размером с линк.
2. К своим сетевым интерфейсам.
3. Маршрут по умолчанию.
4. Маршрут к сетевому интерфейсу – заглушке.
5. Маршруты, связанные с адресами Multicast.
6. Дополнительные статические и динамические маршруты.
7. Маршруты к туннелям IPv6-over-IPv4.

Как и в случае с IPv4, при выборе маршрута применяется правило наиболее точного соответствия. В первую очередь выбирается маршрут к сетевому интерфейсу, в последнюю – маршрут по умолчанию.

Таблица Windows:

```
C:\Users\Administrator>route print -6
===========================================================================
Interface List
 13...00 27 0e 1f a0 b9 ......Intel(R) 82567LF-2 Gigabit Network Connection
  1...........................Software Loopback Interface 1
 11...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 12...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 13    266 ::/0                     2001:7f8:8b:6::1
 13    266 ::/0                     fd00:0:0:6::1
  1    306 ::1/128                  On-link
 13    266 2001:7f8:8b:6::/64       On-link
 13    266 2001:7f8:8b:6::4/128     On-link
 13    266 fd00:0:0:6::/64          On-link
 13    266 fd00:0:0:6::4/128        On-link
 13    266 fe80::/64                On-link
 11    266 fe80::5efe:192.168.11.216/128
                                    On-link
 13    266 fe80::2978:fe81:4c15:df82/128
                                    On-link
  1    306 ff00::/8                 On-link
 13    266 ff00::/8                 On-link
===========================================================================
Persistent Routes:
 If Metric Network Destination      Gateway
  0 4294967295 ::/0                     2001:7f8:8b:6::1
  0 4294967295 ::/0                     fd00:0:0:6::1
===========================================================================
```

Таблица Linux:

```
#netstat -nr -A inet6
Kernel IPv6 routing table
Destination                    Next Hop                   Flags Metric Ref    Use Iface
2001:7f8:8b:1::/64             ::                         U     256    14       0 eth1
2001:7f8:8b:6::/64             ::                         U     256    0        0 eth0
fd00:0:0:1::/64                ::                         U     256    1        0 eth1
fd00:0:0:6::/64                ::                         U     256    0        0 eth0
fe80::/64                      ::                         U     256    0        0 eth1
fe80::/64                      ::                         U     256    0        0 eth0
::/0                           2001:7f8:8b:1::1           UG    1      32       0 eth1
::/0                           fd00:0:0:1::1              UG    1      0        0 eth1
::1/128                        ::                         U     0      3        1 lo
2001:7f8:8b:1::11/128          ::                         U     0      36       1 lo
2001:7f8:8b:6::1/128           ::                         U     0      0        1 lo
fd00:0:0:1::11/128             ::                         U     0      0        1 lo
fd00:0:0:6::1/128              ::                         U     0      0        1 lo
fe80::227:eff:fe1f:a0e2/128    ::                         U     0      6        1 lo
fe80::2c0:cff:fe72:6867/128    ::                         U     0      3        1 lo
ff00::/8                       ::                         U     256    72       0 eth1
ff00::/8                       ::                         U     256    33       0 eth0
#
#Ref -- количество ссылок (ядром не используется)
#Use -- количество попаданий
```

Таблица IOS (такая же, как и в IPv4, но можно назначать интерфейсы NextHop-ами):

```
Router#show ipv6 route
IPv6 Routing Table - Default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via FE80::1, FastEthernet0/1
C   2001:7F8:8B:1::/64 [0/0]
     via FastEthernet0/1, directly connected
L   2001:7F8:8B:1::11/128 [0/0]
     via FastEthernet0/1, receive
C   2001:7F8:8B:6::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2001:7F8:8B:6::1/128 [0/0]
     via FastEthernet0/0, receive
B   2001:ACAD:ACAD:A::/64 [20/0]
     via FE80::6FE:7FFF:FEEB:4B68, FastEthernet0/1
C   FD00:0:0:1::/64 [0/0]
     via FastEthernet0/1, directly connected
L   FD00:0:0:1::11/128 [0/0]
     via FastEthernet0/1, receive
C   FD00:0:0:6::/64 [0/0]
     via FastEthernet0/0, directly connected
L   FD00:0:0:6::1/128 [0/0]
     via FastEthernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

72 Статическая IPv6-маршрутизация в Windows, Linux и IOS

Основными отличиями в маршрутизации являются увеличение количества строк таблицы маршрутизации и изменение набора полей, что вполне адекватно ситуации.

В типовую таблицу маршрутизации включаются следующие маршруты:

1. К своим подсетям размером с линк.
2. К своим сетевым интерфейсам.
3. Маршрут по умолчанию.
4. Маршрут к сетевому интерфейсу – заглушке.
5. Маршруты, связанные с адресами Multicast.
6. Дополнительные статические и динамические маршруты.
7. Маршруты к туннелям IPv6-over-IPv4.

Как и в случае с IPv4, при выборе маршрута применяется правило наиболее точного соответствия. В первую очередь выбирается маршрут к сетевому интерфейсу, в последнюю – маршрут по умолчанию.

Некоторые новые и обновленные команды:

1. route print -6 (Windows)
2. netsh interface ipv6 show route (Windows)
3. netsh interface ipv6 add route (Windows)
4. tracert (Windows)
5. route -A inet6 add (Linux)
6. netstat -nr -A inet6 (Linux)
7. traceroute6 (Linux)

Включение IPv6 forwarding:

Windows:

```
>netsh interface ipv6 set interface Interface_Name_Or_Index forwarding=enabled
```

либо

сервис `Routing and Remote Access`

Linux:

конфигурационный файл `/etc/sysconfig/network`:

```
...
IPV6FORWARDING=yes
...
```

либо

IOS – добавление командами `ipv6 address`.
Просмотр `show ipv6 interfaces / route`

73 Понятие прокси и место прокси в компьютерной сети

Совокупность инструментальных средств (программного и аппаратного обеспечения), предназначенную для контроля доступа к сетевым ресурсам принято называть прокси.

Если прокси «не виден» для клиентского ПО, то он называется прозрачным.

Задачи, выполняемые прокси:

1. Аутентификация (идентификация/Аутентификация/авторизация) – определение круга пользователей, имеющих права доступа к сетевому ресурсу.
2. Фильтрация – запрет или разрешение прохождения входящих или исходящих пакетов по выбранным критериям.
3. Сетевой (межсетевой) экран – запрет или разрешение доступа к определенным категориям сетевых ресурсов.
4. Безопасность, или точнее, кибербезопасность – обеспечение защиты информации, передаваемой по открытым для прослушивания сетям.
5. Ведение журналов – протоколирование различных событий, связанных с доступом к сетевым ресурсам по разным критериям.
6. Отслеживание угроз (threat monitoring).
7. Акселерация – ускорение доступа к сетевым ресурсам за счет определенных оптимизаций (кэширование, многопоточность, поддержка «докачки»).
8. Формирование трафика – распределение приоритетов при доступе к сетевым ресурсам по определенным критериям (может быть программным или аппаратным).
9. Преобразование адресов – решение проблемы невидимости приватных адресов при выходе в Internet.
10. Прочие задачи, связанные с преобразованием передаваемой информации и, как правило, не требующие обеспечения конфиденциальности (например, прозрачное сжатие данных, балансировку нагрузки).

74 Аутентификация и ее проявления в компьютерных сетях

Аутентификация – определение круга пользователей, имеющих права доступа к сетевым ресурсам.

Если рассматривать более подробно, то в рамках аутентификации, можно выделить:

1. Идентификацию – назначение пользователям и ресурсам уникальных символьных или цифровых обозначений, то есть имен или идентификаторов в ОС.
2. Аутентификацию – обеспечение гарантии, что пользователи являются теми, за кого они себя выдают.
3. Авторизацию – назначение аутентифицированным пользователям прав, что обычно неотделимо от аутентификации.

Аутентификация обычно выполняется по учетной записи, то есть совокупности имени пользователя и пароля. В общем же случае, может выполняться как более сложно, например, по карте доступа или биометрически, так и по IP-адресу или MAC-адресу.

Аутентификация может проводиться:

1. Локально – запрос обрабатывается на том же устройстве, которое обеспечивает доступ, или к которому требуется доступ.
2. Удаленно – запрос перенаправляется на внешний выделенный для этого сервер по специальным протоколам (RADIUS - Remote Authentication Dial In User Services).

75 Сетевые экраны и фильтрация трафика

Фильтрация – запрет или разрешение прохождения входящих или исходящих пакетов по выбранным критериям.

В качестве объекта фильтрации выступает пакет. Может выполняться по IP-адресам, по портам, по содержимому и так далее.

Сетевой (межсетевой) экран – запрет или разрешение доступа к определенным категориям сетевых ресурсов (как правило централизованным или внешним).

Сетевой экран в основном выполняет фильтрацию, но это более общее понятие.

Классификация сетевых экранов:

1. Packet Firewalls – просто пропускают или отбрасывают пакеты. Работают на третьем уровне (очень редко на втором)
2. Stateful Firewalls – способны следить за состоянием TCP-соединений, то есть выполнять инспекцию трафика. Работают на третьем и четвертом уровнях.
3. Application Gateway Firewalls – способны следить за сообщениями протоколов прикладного уровня. Работают на третьем – седьмом уровнях.

76 Защита информации, передаваемой по открытым сетям

Безопасность (точнее кибербезопасность) – обеспечение защиты информации, передаваемой по открытым для прослушивания сетям.

Задачи, решаемые в рамках обеспечения безопасности:

1. *Аутентификация* – в данном контексте, обеспечение гарантии, что сообщение пришло от того, от кого оно ожидается. Как правило, заключается в манипулировании с ключами. (RSA)
2. *Целостность* – обеспечение гарантии, что при пересылке сообщение не было повреждено и не было подменено. Как правило, заключается в подсчете значений хэш-функций. (MD5, SHA-256)
3. *Конфиденциальность* – обеспечение гарантии, что перехваченное сообщение не может быть прочитано. Как правило, заключается в шифровании данных. (AES – advanced encryption standard)

Как вариант, возможна маскировка конфиденциальных данных под неконфиденциальные, выражающаяся в различных алгоритмах *стеганографии*.

Во многие алгоритмы для формирования доверительных отношений между абонентами заложено использование *цифровых подписей* или *цифровых сертификатов*.

Современные тенденции в области безопасности компьютерных сетей сводятся к формированию так называемых *виртуальных частных сетей* – VPN, охватывающих взаимодействующие станции.

При этом взаимодействие осуществляется по формируемым особым образом *виртуальным частным каналам* – VPC, которые на практике обычно представляют собой защищенные туннели, проложенные через открытые для прослушивания сети.

Все VPN можно разделить на два типа:

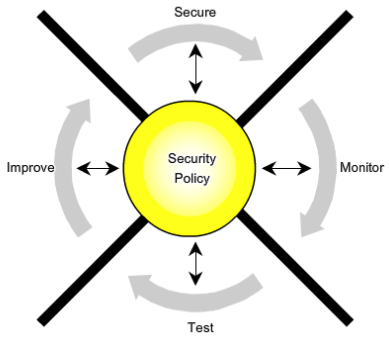
1. Site-to-site – связывают одноранговые шлюзы и являются статическими.
2. Remote-access – обеспечивают подключение удаленных пользователей, создаются динамически и базируются на клиент-серверной модели.

При администрировании, существуют две основополагающие политики обеспечения безопасности:

1. Разрешено всё, что не запрещено.
2. Запрещено все, что не разрешено.

В настоящее время наиболее оправданным признан второй вариант.

Также выделяют так называемое «Security wheel» от Cisco:

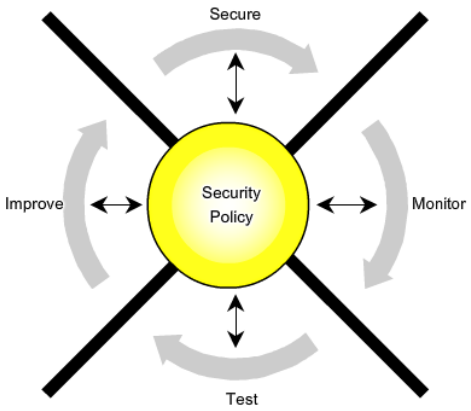


77 Отслеживание и подавление угроз в компьютерных сетях

Отслеживание угроз (threat monitoring) стоит немного особняком в отношении задач обеспечения защиты информации и ведения журналов. Если сделать упор на реакцию при возникновении угроз, то можно выделить два типа прокси:

1. IDSes (Intrusion Detection Systems) – своеобразные сенсоры, которые отслеживают вредоносный трафик по сигнатурам и различными способами оповещают при его обнаружении. Обычно трафик через них не «пропускается», а копируется в их сторону для параллельного анализа.
2. IPSes (Intrusion Prevention Systems) – не просто отслеживают вредоносный трафик, а и способны самостоятельно его заблокировать. Обычно трафик «пропускается» через них.

Выделяется Cisco security wheel:



Также Cisco выделяет следующие виды вредоносных атак:

1. Reconnaissance Attacks – разведывательные, целью которых является несанкционированный сбор информации.
2. Access Attacks – связанные с доступом, целью которых является получение несанкционированного доступа к информации или подмена информации.
3. DoS (Denial of Service) Attacks – связанные с сервисами, целью которых является отказ в обслуживании по тому или иному протоколу.

78 Примеры вредоносных атак в компьютерных сетях

Cisco выделяет следующие виды вредоносных атак:

1. Reconnaissance Attacks – разведывательные, целью которых является несанкционированный сбор информации.
   Примеры: просмотр содержимого пакетов сниферами (packet sniffing), сканирование адресов в поисках станций (ping sweeping), сканирование портов в поисках сервисов (port scanning), ловля на доверие (phishing), социальная инженерия (social engineering), поиск информации в Internet (Internet information queries).
2. Access Attacks – связанные с доступом, целью которых является получение несанкционированного доступа к информации или подмена информации.
   Примеры: подбор паролей методом «грубой силы» (brute-force password search), использование имеющихся прав не по назначению (trust exploitation), перенаправление пользовательских запросов на ложные серверы (port redirection), различные варианты подмены информации в каналах (man-in-the-middle), использование уязвимостей ПО (buffer overflow).
3. DoS (Denial of Service) Attacks – связанные с сервисами, целью которых является отказ в обслуживании по тому или иному протоколу.
   DDos (Distributed DoS) отличается тем, атаку проводят множество станций.
   Примеры: ping с длиной пакета 65535 Byte с целью «завешивания» некоторых старых ОС (ping of dead), порождение с помощью особенностей SNMP-запросов многочисленных станций-«зомби» с целью «забрасывания» SNMP-ответами выбранной станции-«жертвы» (smurf), последовательное создание многочисленных полуоткрытых TCP-соединений (TCP SYN flooding).

79 Примеры злоумышленников и вредоносных программ в компьютерных сетях

Cisco выделяет следующие типы компьютерных преступников:

1. Hackers – наиболее общий термин, но характерной чертой является наличие знаний в области компьютерных технологий.
2. Black Hats – злоумышленники, которые могут и не обладать больши'ми знаниями.
3. White Hats – выполняют несанкционированные атаки, но из благих побуждений (например, сообщают администратору об обнаруженных проблемах).
4. Crackers (взломщики) – специализируются на взломе защиты КС, или ПО, или еще чего-либо.
5. Spammers – массово рассылают электронную почту.
6. War Drivers – путешествуют в поисках «халявы» (обычно незащищенных беспроводных сетей).
7. Phishers (phone fishing) – пытаются под различными предлогами «выудить» конфиденциальную информацию.
8. Phrickers (phone freaks) – используют особенности телефонных сетей для совершения преступлений.

Cisco выделяет три типа вредоносных программ:

1. Viruses – наиболее общий термин, но характерной чертой является распространение с помощью внедрения вредоносного кода в пользовательские программы.
2. Worms – характерной чертой является самостоятельное распространение посредством СПД, протекающее в три фазы: поиск или создание известных вирусу заранее уязвимостей, внедрение путем копирования через сеть, вредоносное проявление.
3. Trojan horses – характерной чертой является маскировка под «безобидные» программы.

80 Задачи прокси, непосредственно не связанные с безопасностью

Акселерация – ускорение доступа к сетевым ресурсам за счет определенных оптимизаций.

Основные способы:

1. Кэширование.
2. Многопоточность.
3. Поддержка «докачки».

Формирование трафика – распределение приоритетов при доступе к сетевым ресурсам по определенным критериям.

Может быть программным или аппаратным, статическим или динамическим.
Может осуществляться по разным критериям, например, по времени.

Преобразование адресов.

Особую проблему при организации коллективного доступа в Internet представляет собой «невидимость» внутренних адресов.

Первоначально задачу можно сформулировать так: требуется, чтобы несколько пользовательских станций из внутренней подсети могли совместно пользоваться одним реальным адресом. NAT (Network Address Translation) – наиболее общий стандарт, решающий задачу путем прозрачной подмены адресов на маршрутизаторах

Также можно упомянуть прозрачное сжатие данных, балансировку нагрузки и вполне легальное перенаправление прикладных сервисов.

81 NAT и другие манипуляции адресами

Особую проблему при организации коллективного доступа в Internet представляет собой «невидимость» внутренних адресов.

Первоначально задачу можно сформулировать так: требуется, чтобы несколько пользовательских станций из внутренней подсети могли совместно пользоваться одним реальным адресом. NAT (Network Address Translation) – наиболее общий стандарт, решающий задачу путем прозрачной подмены адресов на маршрутизаторах

Обобщенный алгоритм работы IP NAT:

1. Клиент передает пакет прокси с поддержкой NAT.
2. Прокси запоминает IP-адрес назначения, IP-адрес источника, подставляет в качестве IP-адреса источника свой адрес и передает пакет серверу, запрашиваемому клиентом.
3. После получения ответного пакета от сервера выполняются обратные преобразования на основе запомненной информации.
4. Ответный пакет передается клиенту.

Для обеспечения правильности выполнения преобразований строится таблица, то есть NAT работает по табличному принципу.

Все реализации NAT, в первую очередь, делятся на два типа:

1. Статические – преобразования осуществляется исходя из строгого соответствия пар адресов.
2. Динамические – при преобразованиях адреса по мере надобности выделяются из пула по определенному критерию.

Наиболее сложной, но и наиболее полноценной формой NAT, позволяющей различать L4-соединения, является PAT (Port Address Translation) – в дополнение к IP-адресам запоминаются номера программных портов. Согласно терминологии RFCs это называют NAPT (Network Address Port Translation), у Cisco это NAT Overload, но обычно используют аббревиатуру PAT. PAT-дополнение совместимо и со статическим, и с динамическим вариантами NAT.

Первоначальная постановка задачи предполагает, что подменяется IP-адрес источника (source NAT), но возможна подмена IP-адреса назначения (destination NAT) либо обоих адресов (twice NAT).

Первоначальная постановка так же предполагает, что приватный IP-адрес замещается публичным, но, в общем случае, возможна произвольная комбинация. Наконец, первоначальная постановка задачи предполагает, что запросы порождаются клиентами во внутренней сети, но, поскольку «правильная» NAT-таблица работает в двух направлениях (преобразуются и IP-адреса назначения в ответных пакетах), открыта возможность обслуживания запросов со стороны внешних клиентов (two-way NAT).

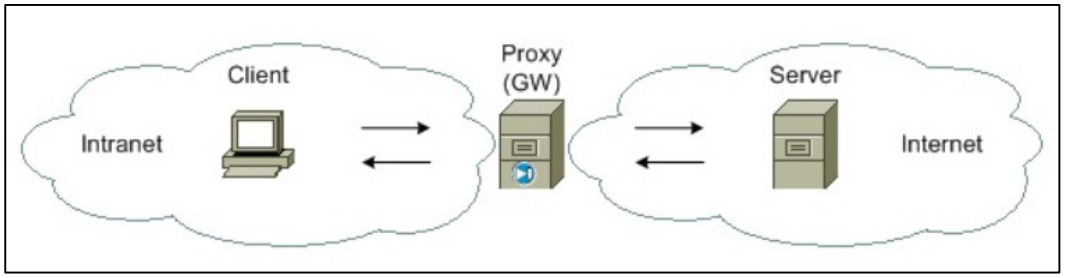
Так, статический вариант NAT позволяет разместить во внутренней сети сервер и адресовать его из Internet.

Более того, статический вариант PAT позволяет перенаправлять запросы из Internet об определенных сервисах на соответствующие отдельные внутренние серверы.

Все варианты NAT совместимы с туннелированием. NAT полностью противоречит идеологии IPv6, поэтому, касательно IPv6, его поддержка не рекомендуется.

82 Пример взаимодействия через прокси

Типичное место расположения прокси – это граница между внутренней сетью и сетью публичного доступа.



Задачи, связанные с обеспечением безопасности обычно решают во внутренней сети. Провайдеры, в идеале, обеспечивают беспрепятственное прохождение трафика.

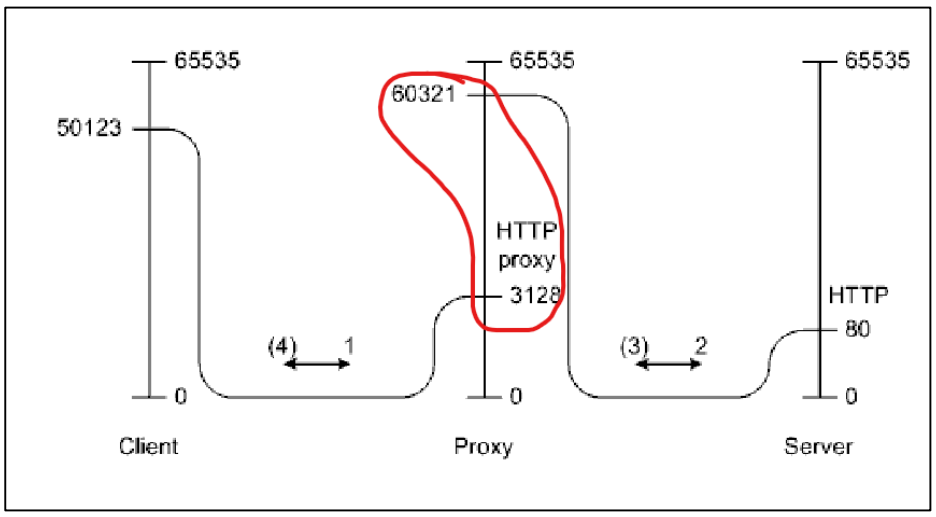
Две основные проблемы прокси: при использовании следует избегать каскадирования большого числа прокси, а также перегрузки ядра ОС.

Касательно протоколов прикладного уровня, подавляющее большинство прокси – это HTTP-прокси, причем двух вариантов:

1. Get Method.
2. Connect Method.

На втором месте находятся прокси электронной почты. Все остальные встречаются крайне редко.

Обобщенная последовательность действий при взаимодействии клиента и сервера на примере HTTP-прокси выглядит примерно так (красным цветом обозначена подмена ID):

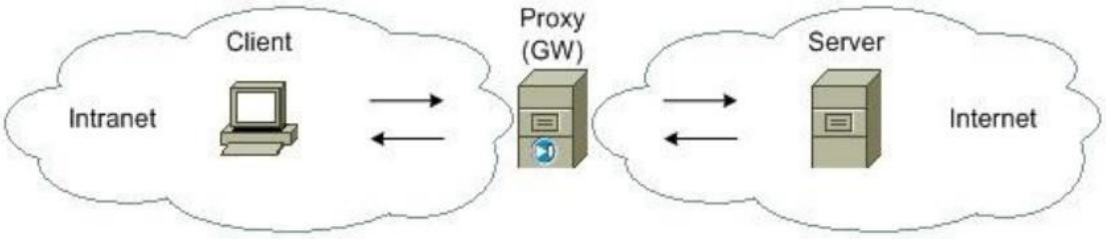


83 Классификация инструментальных средств, реализующих прокси

Все задачи, выполняемые прокси, могут решаться самыми разными устройствами на различных уровнях модели OSI. Все способы можно объединить в три направления:

1. Host-based (Server-based + Personal) – сугубо программные решения на базе универсальных серверных и настольных ОС, таких как Windows и Linux. Эти ОС, в свою очередь, «крутятся» на обычных серверах и пользовательских станциях. Здесь можно сразу выделить два уровня, на которых можно решать упомянутые задачи: ядро ОС и прикладное ПО.
2. Integrated – программно-аппаратные решения на базе специализированных сетевых ОС, таких как IOS и Junos OS, которые «крутятся» на маршрутизаторах и другом сетевом оборудовании. Эти ОС хоть и специализированы как сетевые, но в своей области универсальны, то есть не полностью адаптированы к упомянутым задачам. Степень адаптации повышается за счет специальных аппаратных модулей.
3. Appliance-based – полностью специализированные аппаратные решения, такие как Cisco ASA и SafeNet eSafe. Такие устройства «сосредоточены» на обеспечении безопасности и называются аппаратными сетевыми экранами (security appliances). Аппаратные сетевые экраны, которые «заточены» для контроля доступа по протоколам прикладного уровня, известны как NACs (Network Admission Controls). Примером может служить Cisco Ironport.

Типичное место расположения прокси — это граница между внутренней сетью и сетью публичного доступа.



84 Фильтрация и NAT в Windows

Фильтры строятся на основе правил (rules)

Каждое правило – это строка, содержащая в себе условия, определяющие подпадает ли пакет под правило, и действие, которое необходимо осуществить в случае выполнения условий.
Правила могут объединяться в цепочки (chains) и образовывать сложную иерархию.

Начиная с Windows XP SP2 и Server 2003 SP1, в ядро интегрирован `Windows Firewall`, который позиционируют как базовый персональный сетевой экран.

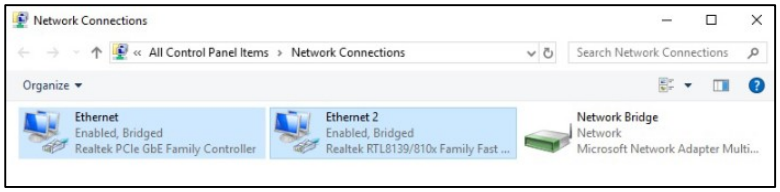
В Windows 10 (Server 2016, Server 2019, ...) `Windows Firewall`, в связке с `Windows Defender` и `Windows Action Center`, постепенно «переносят» в отдельное системное приложение под названием `Windows Security`.

Настроить Firewall можно через Firewall & network protection или же через сервис «Windows Security»

Упрощенными для удобства пользователя специфическими формами NAT являются Network Bridge и Internet Connection Sharing («вытесняют» сервис `Routing and Remote Access`).

Network Bridge позволяет объединить два возможно разнородных сегмента с целью эмуляции одного сегмента.

Internet Connection Sharing позволяет нескольким пользователям из одной подсети совместно использовать (в режиме разделения времени) один сетевой интерфейс из другой подсети, обычно с целью доступа в Internet.



– Пример бриджа

Полноценная поддержка NAT с графическим интерфейсом доступна в серверных редакциях – в составе Routing and Remote Access.

В Server 2003 R2 был интегрированный компонент `Routing and Remote Access`, в Server 2008 R2 – опциональная роль с тем же названием. Начиная с Server 2012, роль имеет название `Remote Access`.

Рассказать, как можно настроить бриджы и шеринг (всё так же через network connections)

85 Пакет IP Tables

В большинстве систем UNIX широко применяют пакет IP Filter – в основном для целей фильтрации и NAT. В Linux эту роль выполняет пакет IP Tables.

Для нормальной работы IP Tables должны быть включены некоторые опции ядра. Для обеспечения возможности управления введен одноименный сервис `iptables`.

Фильтры строятся на основе правил (rules)

Каждое правило – это строка, содержащая в себе условия, определяющие подпадает ли пакет под правило, и действие, которое необходимо осуществить в случае выполнения условий.
Правила могут объединяться в цепочки (chains) и образовывать сложную иерархию.

Следовательно, при работе с IP Tables необходимо внимательно проверять содержимое и последовательность правил.

– стандартные цепочки IP Table

Примеры таблиц:

1. `filter` -- нужна для фильтрации пакетов;
2. `mangle` -- нужна для внесения изменений в заголовки пакетов (например, в поле TTL);
3. `nat` -- нужна для преобразования адресов

Общий формат правила:

```
iptables [-t table] command [match] [target/jump]
```

Примеры команд:
`-A (--append)` -- добавить новое правило в конец цепочки;
`-D (--delete)` -- удалить правило из цепочки;
`-F (--flush)` -- удалить все правила из цепочки;
`-I (--insert)` -- вставить новое правило в цепочку;
`-L (--list)` -- вывести на экран список правил в цепочке;
`-N (--new-chain)` -- создать новую цепочку с названием в таблице;
`-P (--policy)` -- определить политику по умолчанию для цепочки;
`-R (--replace)` -- заменить одно правило другим в цепочке;
`-X (--delete-chain)` -- удалить цепочку из таблицы.

Примеры критериев (matches):
`-d (--destination)` -- нужен для указания адреса назначения;

`-f (--fragment)` -- нужен для включения поддержки фрагментации;
`-p (--protocol)` -- нужен для указания протокола;
`-s (--source)` -- нужен для указания адреса источника.

Примеры действий (targets) :

`ACCEPT` -- пакет прекращает движение по цепочке и считается пропущенным, но он может быть отброшен следующими цепочками;
`DNAT` -- подмена адреса назначения;
`DROP` -- пакет отбрасывается;
`LOG` -- протоколирование пакета или связанных с его прохождением событий;
`MASQUERADE` -- подмена адреса источника без явного указания заменяющего адреса;
`REJECT` -- равно DROP плюс посылка ответного ICMP-сообщения о недостижимости;
`SNAT` -- подмена адреса источника.

Переходы (jumps) позволяют передавать пакет другим цепочкам.

86 Полнофункциональные прокси на базе Windows и Linux

/// + рассказать всё, что знаю про прокси)

Linux: Де факто стандартным прокси-сервером для систем UNIX, в том числе и Linux, является пакет Squid со стандартным конфигурационным файлом: `/etc/squid/squid.conf`.

Windows: Начиная с Windows XP SP2 и Server 2003 SP1, в ядро интегрирован `Windows Firewall`, который позиционируют как базовый персональный сетевой экран.

В Windows 10 (Server 2016, Server 2019, ...) `Windows Firewall`, в связке с `Windows Defender` и `Windows Action Center`, постепенно «переносят» в отдельное системное приложение под названием `Windows Security`.

Кроме того, очень широко применяют пакеты сторонних производителей, среди которых следует выделить Qbik WinGate и Kerio (GFI Software) KerioControl.

Настроить Firewall можно через Firewall & network protection или же через сервис «Windows Security»

87 Поддержка NAT в IOS

Cisco IOS поддерживает все теоретические варианты NAT. Статические и динамические преобразования совместимы (даже в одном направлении), но статические нужно конфигурировать раньше динамических.

Отдельно взятое правило преобразований задают командой `ip nat`.

Если правило относится к динамическим преобразованиям, аргумент `overload` разрешает совместное использование пула адресов и включает PAT. Если правило относится к статическим преобразованиям, PAT включает аргумент `extendable`.

Обязательно нужно «привязать» сетевые интерфейсы к внутренней сети (inside) и сети публичного доступа (outside) командами `ip nat inside` и `ip nat outside` соответственно (можно и не по одному).

Важно правильно понимать Cisco-терминологию, связанную с адресацией при NAT-преобразованиях:

1. Inside local -- адрес расположенной в сети inside станции как он «виден» в сети inside.
2. Inside global -- адрес расположенной в inside-сети станции как он «виден» в сети outside.
3. Outside local --а адрес расположенной в сети outside станции как он «виден» в сети inside.
4. Outside global -- адрес расположенной в сети outside станции как он «виден» в сети outside.

Cisco-варианты NAT:

1. `ip nat inside source static` -- в направлении из сети inside в сеть outside подменяется IP-адрес источника (и IP-адрес назначения в обратном направлении), то есть адрес inside local заменяется адресом inside global (классический статический source NAT).
2. `ip nat inside source list` -- замены аналогично `ip nat inside source static`, плюс позволяет задействовать список адресов inside local и пул адресов inside global (динамический source NAT).
3. `ip nat inside destination list` -- в направлении из сети outside в сеть inside подменяется IP-адрес назначения, то есть адрес inside global заменяется адресом inside local -- фактически то же самое, что и `ip nat inside source`, но позволяет задействовать список адресов inside global и пул адресов inside local. (используется редко)
4. `ip nat outside source static` -- в направлении из сети outside в сеть inside подменяется IP-адрес источника, то есть адрес outside global заменяется адресом outside local. (статический destination NAT, используется редко)
5. `ip nat outside source list` -- замены аналогично `ip nat outside source static`, плюс позволяет задействовать список адресов outside global и пул адресов outside local (динамический destination NAT, используется редко).

По умолчанию строка NAT-таблицы считается валидной 24 часа – TCP, 5 минут – UDP, 1 минуту – ICMP.