Глава 7. IP-адресация

Материалы для инструктора

CCNA Routing and Switching

Введение в сетевые технологии (v6.0)

Материалы для инструкторов. Глава 7. Руководство по планированию

- Эта презентация PowerPoint состоит из двух частей:
- Руководство по планированию для инструкторов
  - Ознакомительная информация по главе
  - Методические пособия
- Презентация перед классом для инструктора
  - Дополнительные слайды, которые можно использовать в классе
  - Начало на слайде № 16

- **Примечание.** Перед предоставлением общего доступа удалите руководство по планированию из данной презентации.

Глава 7. IP-адресация

Introduction to Networks 6.0.
Руководство по планированию

Глава 7. Упражнения

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
7.0.1.2	Упражнение в аудитории	Моделирование всеобъемлющего Интернета (IoE)	Необязательно
7.1.1.2	Видео	Преобразование десятичных чисел в двоичный формат	Рекомендуется
7.1.1.4	Интерактивное упражнение	Преобразование двоичных чисел в десятичный формат	Рекомендуется
7.1.1.8	Интерактивное упражнение	Преобразование десятичных чисел в двоичный формат	Рекомендуется
7.1.1.9	Интерактивное упражнение	Игра «Двоичные числа»	Необязательно
7.1.2.4	Интерактивное упражнение	Использование операции И для определения сетевого адреса	Рекомендуется
7.1.2.7	Демонстрационный видеоролик	Сетевой адрес, адрес хоста и адрес трансляции	Рекомендуется
7.1.2.8	Лабораторная работа	Использование калькулятора Windows в работе с сетевыми адресами	Необязательно
7.1.2.9	Лабораторная работа	Преобразование IPv4-адресов в двоичный формат	Рекомендуется
7.1.3.7	Интерактивное упражнение	Индивидуальные, широковещательные и групповые адреса	Рекомендуется
7.1.3.8	Packet Tracer	Анализ трафика одноадресной, широковещательной и многоадресной рассылки	Необязательно

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

Глава 7. Упражнения (продолжение)

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
7.1.4.2	Интерактивное упражнение	Разрешение или блокировка адресов IPv4	Рекомендуется
7.1.4.5	Демонстрационный видеоролик	IP-адресация с использованием классов	Рекомендуется
7.1.4.8	Интерактивное упражнение	Общедоступные и частные адреса IPv4	Рекомендуется
7.1.4.9	Лабораторная работа	Определение IPv4-адресов	Необязательно
7.2.1.3	Интерактивное упражнение	Проблемы с IPv4-адресами и их решения	Рекомендуется
7.2.2.4	Интерактивное упражнение	Отработка представления IPv6-адресов	Рекомендуется
7.2.3.5	Интерактивное упражнение	Определение типов IPv6-адресов	Рекомендуется
7.2.4.2	Инструмент проверки синтаксиса	Настройка IPv6 на маршрутизаторе	Рекомендуется
7.2.4.8	Инструмент проверки синтаксиса	Проверка конфигурации IPv6-адреса	Рекомендуется
7.2.4.9	Packet Tracer	Настройка IPv6-адресов	Рекомендуется
7.2.5.3	Лабораторная работа	Определение IPv6-адресов	Необязательно

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

Глава 7. Упражнения (продолжение)

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
7.2.5.4	Лабораторная работа	Настройка IPv6-адресов на сетевых устройствах	Рекомендуется
7.3.2.5	Packet Tracer	Проверка адресации IPv4 и IPv6	Необязательно
7.3.2.6	Packet Tracer	Выполнение команды ping и трассировка маршрута для проверки пути	Необязательно
7.3.2.7	Лабораторная работа	Проверка подключения к сети с помощью команд ping и traceroute	Необязательно
7.3.2.8	Лабораторная работа	Составление карты сети Интернет	Рекомендуется
7.3.2.9	Packet Tracer	Устранение проблем с адресацией IPv4 и IPv6	Рекомендуется
7.4.1.1	Упражнение в аудитории	Всеобъемлющий Интернет... для вас!	Необязательно
7.4.1.2	Packet Tracer	Отработка комплексных практических навыков	Рекомендовано

В этой главе для выполнения упражнений с программой Packet Tracer используйте следующий пароль: **PT_ccna5**

Глава 7. Проверочная работа

- После прохождения главы 7 учащиеся должны выполнить проверочную работу по материалам главы 7.
- Для неформальной оценки успехов учащихся можно использовать контрольные работы, лабораторные работы, работу с симулятором Packet Tracer и другие упражнения.

Глава 7. Практические рекомендации

Прежде чем излагать материал главы 7, обратите внимание на следующее:

- Инструктор должен выполнить проверочную работу на знание материала главы 7.
- Цели этой главы:
  - Выполнить преобразование между двоичными и десятичным системами счисления
  - Описать структуру IPv4-адреса, в том числе сетевую часть, узловую часть и маску подсети
  - сопоставлять характеристики использования индивидуальных, многоадресных и широковещательных IPv4-адресов;
  - Объяснить суть частных, публичных и зарезервированных IPv4-адресов
  - Объяснить необходимость использования IPv6-адресации
  - Описать представление IPv6-адреса
  - Сравнить типы сетевых IPv6-адресов.
  - Настроить глобальные адреса одноадресной рассылки
  - Описать адреса многоадресной рассылки
  - Объяснить, как можно использовать протокол ICMP для проверки подключения к сети
  - Использовать утилиты ping и traceroute для проверки подключения к сети

Глава 7. Практические рекомендации (продолжение)

- Раздел 7.1.
  - Напомните студентам о позиционной нотации значения разряда в десятичном формате, чтобы помочь понять значения двоичных разрядов (см. видео 7.1.1.7).
  - Предложите студентам создать свою собственную диаграмму значений двоичных разрядов.
  - Студенты должны получить практические навыки в преобразовании, которые позволят им с легкостью выполнять этот процесс без использования калькуляторов. Преобразовывая значения вручную, студенты узнают, как можно манипулировать битами для создания двоичного эквивалента десятичного значения. Во время экзаменов для получения сертификата CCNA использование калькуляторов не допускается.
  - Чтобы проверить навыки студентов в преобразовании двоичных и десятичных значений, предложите им сыграть в бинарную игру.

Глава 7. Практические рекомендации (продолжение)

- Раздел 7.1. (продолжение)
  - Объясните иерархическую структуру IP-адреса с помощью различных аналогий, например, с почтовым адресом и телефонным номером.
  - Продемонстрируйте логическую операцию И (процесс логического умножения).
    - Рекомендуется упражнение 7.1.2.4. и видео 7.1.2.7.
  - Упражнение по преобразованиям — лабораторная работа 7.1.2.9
  - Студенты должны знать блоки частных адресов.
    - Рекомендуется выполнить упражнение 7.1.4.8.
    - Обсудите схему адресации на примере адреса их дома и вашего учебного заведения.
  - Традиционная классовая адресация.
    - Не потратьте много времени на это.
    - Это полезно для понимания основ адресации IPv4 и причины проблемы с исчерпанием адресов.

Глава 7. Практические рекомендации (продолжение)

- Раздел 7.2.
  - Объясните структуру IPv6-адреса.
    - Длина IPv6-адресов составляет 128 бит, и они представляются с помощью шестнадцатеричных значений.
    - Четыре бита могут быть представлены одним шестнадцатеричным значением. Четыре шестнадцатеричные цифры составляют гекстет.
    - Длина префикса используется для обозначения сетевой части адреса IPv6 в диапазоне от 0 до 128. Типичная длина префикса локальной сети: /64.
  - Предложите студентам с помощью упражнения 7.2.2.4. отработать сжатие IPv6-адресов.
  - Обратите внимание на важные функции локального IPv6-адреса.
    - Он позволяет устройству обмениваться данными с другими устройствами, поддерживающими адресацию IPv6, по одному и тому же каналу.
    - Каждый сетевой интерфейс с IPv6-адресом должен иметь локальный адрес канала.
    - Если такой адрес не был настроен на интерфейсе вручную, он будет создан автоматически.
    - Локальные адреса каналов находятся в диапазоне FE80::/10.

Глава 7. Практические рекомендации (продолжение)

- Раздел 7.2 (продолжение)
  - Объясните составные части глобального индивидуального адреса IPv6 и сравните его с адресом IPv4.
    - Префикс глобальной маршрутизации является сетевой частью адреса, который назначается интернет-провайдером.
    - Идентификатор подсети может использоваться организацией для определения подсетей в своем объекте.
    - Идентификатор интерфейса является эквивалентом части хоста в адресе IPv4.
  - Для закрепления знаний студенты должен выполнить интерактивное упражнение 7.2.3.5.
  - Обсудите три варианта объявления маршрутизатора.
    - Только SLAAC. «Я уже знаю все необходимое (префикс, длина префикса, шлюз по умолчанию)».
    - SLAAC и DHCPv6. «Вот моя информация, но вам нужно получить другие сведения, такие как DNS-адреса от DHCPv6-сервера».
    - Только DHCPv6. «Я не могу помочь вам. Всю информацию нужно получить от DHCPv6-сервера».

Глава 7. Практические рекомендации (продолжение)

- Раздел 7.3.
  - С помощью программы Packet Tracer продемонстрируйте проверку адресации IPv4 и IPv6 (раздел 7.3.2.5).
  - С помощью программы Packet Tracer продемонстрируйте использование команд ping и traceroute для проверки подключений (раздел 7.3.2.6).

Глава 7. Дополнительная помощь

- Дополнительные справочные материалы, содержащие различные стратегии обучения, в том числе планы занятий, описание аналогий для сложных понятий и темы обсуждений, доступны на веб-сайте сообщества сертифицированных сетевых специалистов (CCNA) по адресу https://www.netacad.com/group/communities/community-home.
- Практические рекомендации специалистов со всего мира для обучения по программе CCNA Routing and Switching. https://www.netacad.com/group/communities/ccna
- Если вы хотите поделиться с другими преподавателями планами занятий и другой полезной информацией, вы можете разместить ее на сайте сообщества сертифицированных компанией Cisco сетевых специалистов (CCNA).
- Студенты могут записаться на курс **Introduction to Packet Tracer** (Введение в Packet Tracer) (для самостоятельного изучения)

CISCO

Глава 7. IP-адресация

CCNA Routing and Switching

Введение в сетевые технологии (v6.0)

Глава 7. Разделы и задачи

- 7.1. Сетевые адреса IPv4
- Объяснить использование адресов IPv4 для обеспечения подключений в сетях предприятий малого и среднего бизнеса.
  - Выполнить преобразование между двоичными и десятичным системами счисления
  - Описать структуру IPv4-адреса, в том числе сетевую часть, узловую часть и маску подсети
  - сопоставлять характеристики использования индивидуальных, многоадресных и широковещательных IPv4-адресов;
  - Объяснить суть частных, публичных и зарезервированных IPv4-адресов
- 7.2. Сетевые адреса IPv6
- Выполнить настройку IPv6-адресов для обеспечения подключений в сети предприятий малого и среднего бизнеса
  - Объяснить необходимость использования IPv6-адресации
  - Описать представление IPv6-адреса
  - Сравнить типы сетевых IPv6-адресов.
  - Настроить глобальные адреса одноадресной рассылки
  - Описать адреса многоадресной рассылки

Глава 7. Разделы и цели (продолжение)

- 7.3. Проверка подключения
- Использовать типичные утилиты для проверки и тестирования сетевого подключения.
  - Объяснить, как можно использовать протокол ICMP для проверки подключения к сети
  - Использовать утилиты ping и traceroute для проверки подключения к сети

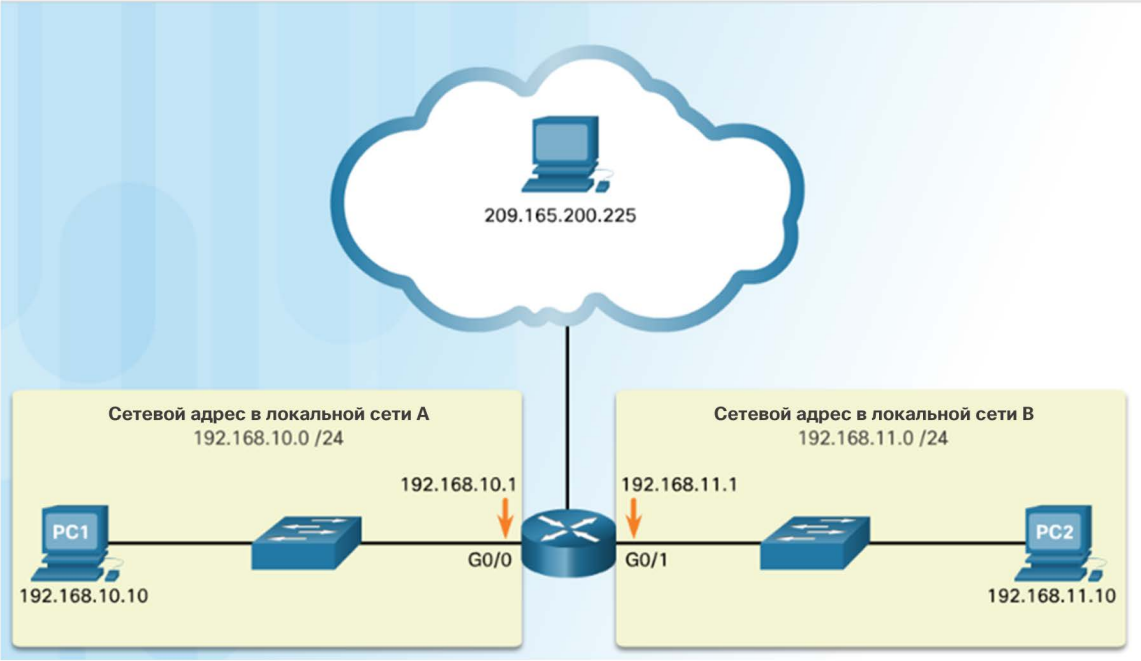
7.1. Сетевые адреса IPv4

Преобразование двоичных значений в десятичные
Адреса IPv4

- Двоичная система счисления состоит из цифр 0 и 1, называемых битами.
  - IPv4-адреса представляются в виде 32 двоичных битов, разделенных на 4 8-битных октета.

Преобразование двоичных значений в десятичные
Адреса IPv4 (продолжение)

- Для IPv4-адресов обычно используется десятичное представление с точками.



Демонстрационный видеоролик. Перевод чисел из двоичной в десятичную систему счисления

- В этом видеоролике рассматривается использование операции И для определения сетевого адреса, адресов хостов и широковещательного адреса в сети IPv4.

Позиционная система счисления

- В первой строке определяется основание («радикс») числа. Для десятичной системы счисления это 10. Двоичная система счисления — это система по основанию 2, поэтому радикс равен 2.
- Вторая строка определяет позицию числа, начиная с 0. Эти числа также представляют экспоненциальное значение, которое будет использоваться для расчета позиционного значения (4-я строка).
- В 3-й строке рассчитывается позиционное значение путем возведения основания в степень, равную экспоненциальному значению его позиции. Примечание. n^0 всегда = 1.
- Позиционное значение указано в четвертой строке.

Десятичная позиционная система счисления

Основание	10	10	10	10
Позиция в числе	3	2	1	0
Вычислите	(10^3)	(10^2)	(10^1)	(10^0)
Позиционное значение	1000	100	10	1

Применение десятичной позиционной системы счисления

	Тысячи	Сотни	Десятки	Единицы
Позиционное значение	1000	100	10	1
Двоичный номер (1234)	1	2	3	4
Вычислите	1 x 1000	2 x 100	3 x 10	4 x 1
Суммируйте...	1000	+ 200	+ 30	+ 4
Результат	1 234			

Преобразование двоичных значений в десятичные

Позиционная система счисления (продолжение)

Двоичная позиционная система счисления

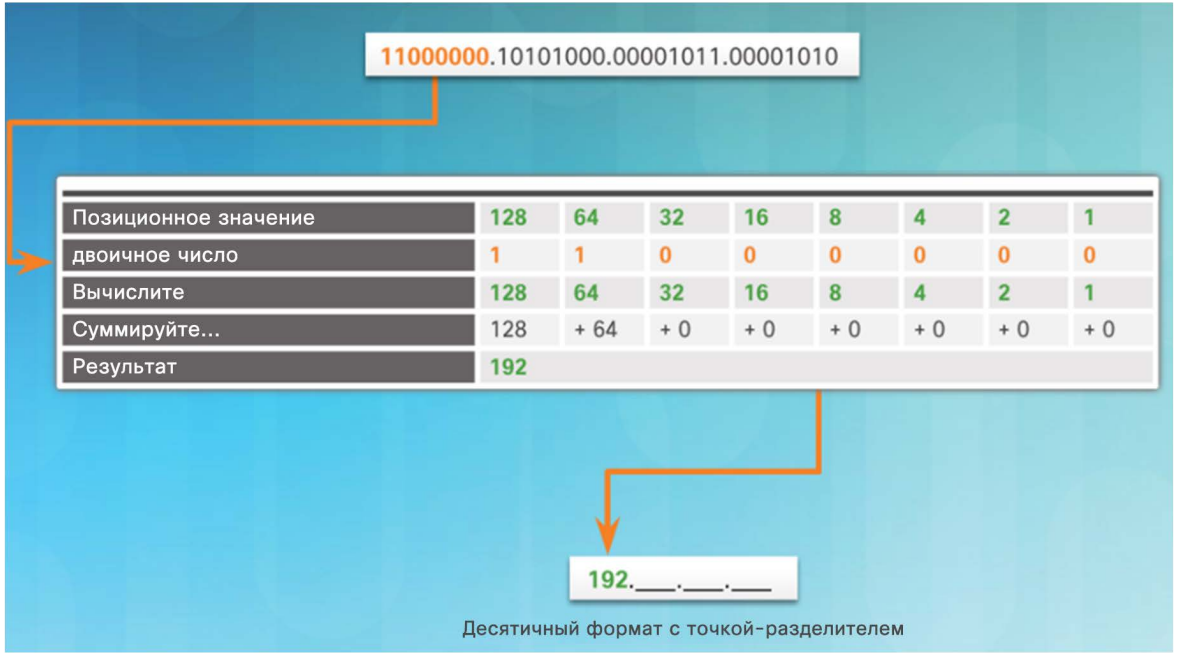
Основание	2	2	2	2	2	2	2	2
Позиция в числе	7	6	5	4	3	2	1	0
Вычислите	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)
Позиционное значение	128	64	32	16	8	4	2	1

- Применение двоичной позиционной системы счисления.

Позиционное значение	128	64	32	16	8	4	2	1
двоичное число (11000000)	1	1	0	0	0	0	0	0
Вычислите	1 x 128	1 x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	0 x 1
Суммируйте...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Результат	192							

Преобразование двоичных чисел в десятичный формат

- Для преобразования двоичного IPv4-адреса в десятичный формат введите 8-битное двоичное число для каждого октета под позиционным значением строки 1, а затем вычислите десятичное значение.



Позиционное значение	128	64	32	16	8	4	2	1
двоичное число	1	1	0	0	0	0	0	0
Вычислите	128	64	32	16	8	4	2	1
Суммируйте...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Результат	192							

Преобразование десятичных чисел в двоичный формат

- Для преобразования десятичного адреса IPv4 в двоичный формат используйте позиционную диаграмму и сначала проверьте, превышает ли число 128 бит. Если нет, поместите 0 в эту позицию. Если да, поместите 1 в эту позицию.
- 128 вычитается из исходного числа, и остаток затем сравнивается со следующей позицией (64). Если он меньше 64, в эту позицию помещается 0. Если больше, помещается 1 и вычитается 64.
- Процесс повторяется, пока не будут введены все позиционные значения.

Преобразование двоичных значений в десятичные

Примеры преобразования десятичных чисел в двоичный формат

Пример. 192.168.10.11

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

11000000 . _____ . _____ . _____

Пример. 192.168.10.11

Позиционное значение	128	64	32	16	8	4	2	1
	1	0	1	0	1	0	0	0

11000000 . 10101000 . _____ . _____

Пример. 192.168.10.11

Позиционное значение	128	64	32	16	8	4	2	1
	0	0	0	0	1	0	1	0

11000000 . 10101000 . 00001010 . _____

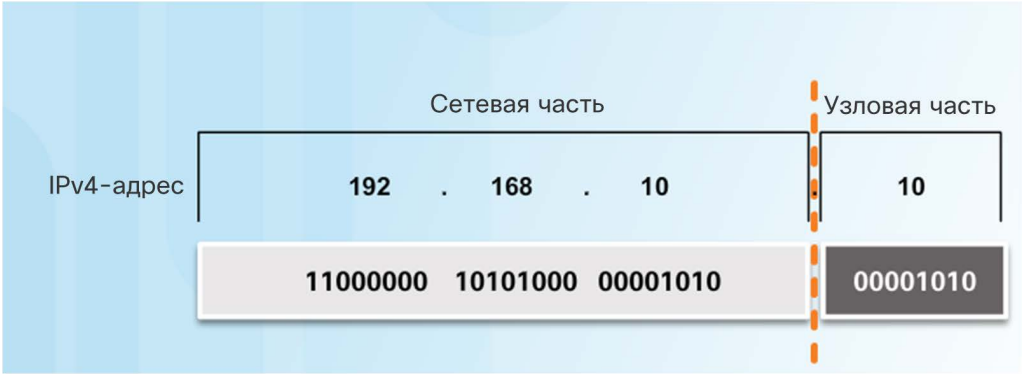
Пример. 192.168.10.11

Позиционное значение	128	64	32	16	8	4	2	1
	0	0	0	0	1	0	1	1

11000000 . 10101000 . 00001010 . 00001011

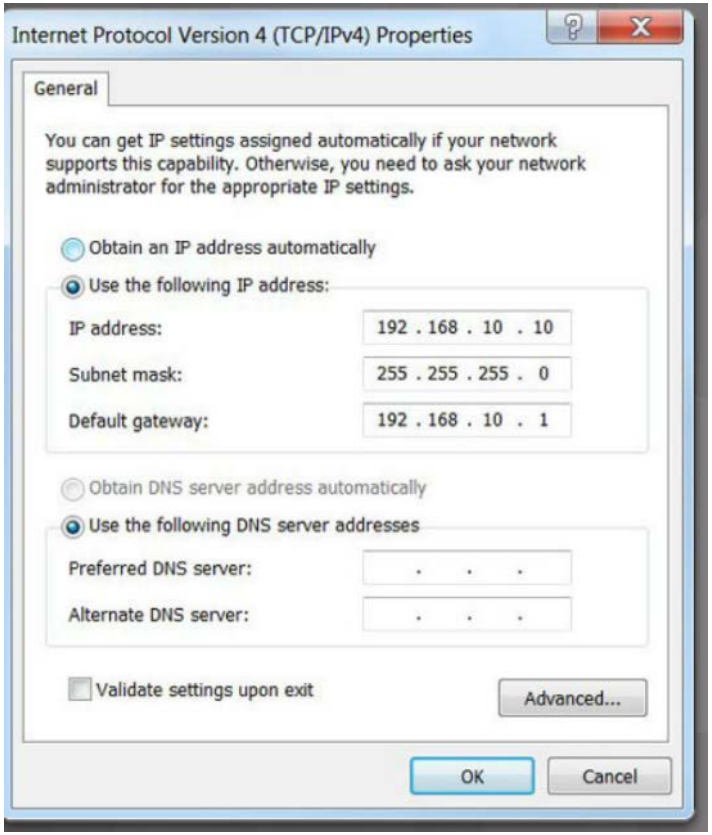
Разделы сети и хоста

- Адрес IPv4 имеет иерархическую структуру.
  - Он состоит из раздела сети и хоста.
- Все устройства в одной сети должны иметь одинаковый раздел сети.
- Маска подсети помогает устройствам определить раздел сети и хоста.



Маска подсети

- На хосте должны быть настроены три IPv4-адреса:
  - Уникальный IPv4-адрес хоста.
  - Маска подсети, которая определяет раздел IPv4-адреса, который относится к сети и хосту.
  - Шлюз по умолчанию — IP-адрес локального интерфейса маршрутизатора.



Маска подсети (продолжение)

- IPv4-адрес побитно сравнивается с маской подсети слева направо.
- 1 в маске подсети указывает, что соответствующий бит в адресе IPv4 является битом сети.

Логическая операция И

- Логическая операция И — одна из трех основных двоичных операций, используемых в дискретной логике.
- Используется для определения сетевого адреса.
- Применение логической операции И для двух битов дает следующие результаты.

1 И 1 = 1
0 И 1 = 0
0 И 0 = 0
1 И 0 = 0

IP-адрес	192 .	168 .	10 .	10
Двоичное	11000000	10101000	00001010	00001010
Маска подсети	255 .	255 .	255 .	0
	11111111	11111111	11111111	00000000
Результаты операции И	11000000	10101000	00001010	00000000
Сетевой адрес	192 .	168 .	10 .	0

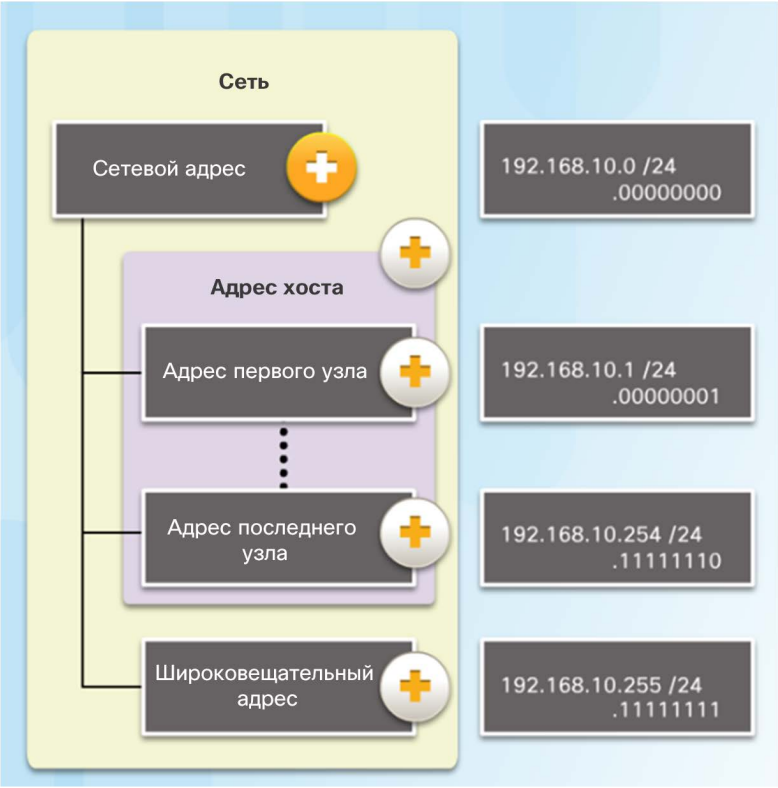
Длина префикса

Сопоставление маски подсети и длины префикса

Маска подсети	32-битный адрес	Длина префикса
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

- Длина префикса:
  - Сокращенный способ записи маски подсети.
  - Равна количеству битов в маске подсети, имеющих значение 1.
  - Записывается с использованием косой черты (/), за которой следует количество сетевых битов.

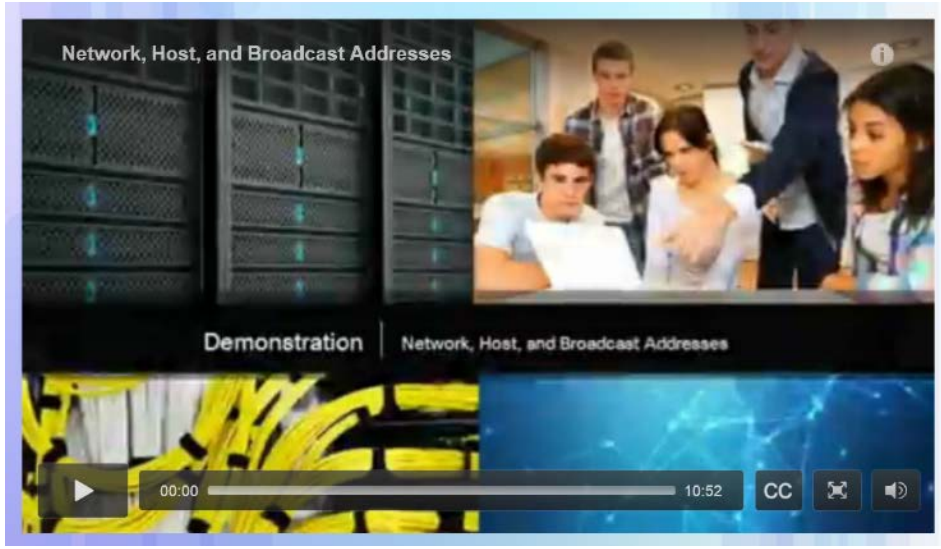
Сетевой адрес, адрес хоста и адрес трансляции



- Типы адресов в сети 192.168.10.0/24
  - Сетевой адрес — раздел хоста содержит только нули (.00000000)
  - Адрес первого хоста — раздел хоста содержит одни нули и заканчивается на 1 (.00000001)
  - Адрес последнего хоста — раздел хоста содержит одни единицы и заканчивается на 0 (.11111110)
  - Адрес трансляции — раздел хоста содержит только единицы (.11111111)

Демонстрационный видеоролик. Сетевой адрес, адрес хоста и адрес трансляции

- В этом видеоролике рассматривается использование операции И для определения сетевого адреса, адресов хостов и широковещательного адреса в сети IPv4.

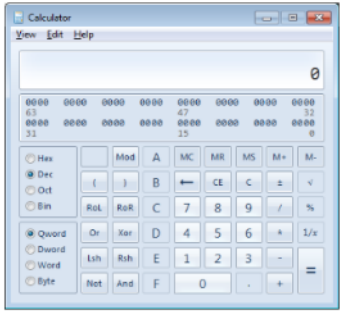


Лабораторная работа. Использование калькулятора Windows в работе с сетевыми адресами

Cisco Networking Academy®

Mind Wide Open®

Lab – Using the Windows Calculator with Network Addresses



Objectives

Part 1: Access the Windows Calculator

Part 2: Convert between Numbering Systems

Part 3: Convert Host IPv4 Addresses and Subnet Masks into Binary

Part 4: Determine the Number of Hosts in a Network Using Powers of 2

Part 5: Convert MAC Addresses and IPv6 Addresses to Binary

Background / Scenario

Network technicians use binary, decimal, and hexadecimal numbers when working with computers and networking devices. Microsoft provides a built-in Calculator application as part of the operating system. The Windows 7 version of Calculator includes a Standard view that can be used to perform basic arithmetic tasks such as addition, subtract, multiplication, and division. The Calculator application also has advanced programming, scientific, and statistical capabilities.

In this lab, you will use the Windows 7 Calculator application Programmer view to convert between the binary, decimal, and hexadecimal number systems. You will also use the Scientific view powers function to determine the number of hosts that can be addressed based on the number of host bits available.

Required Resources

- 1 PC (Windows 7 or 8)

Лабораторная работа. Преобразование IPv4-адреса в двоичный формат

Cisco Networking Academy® Mind Wide Open™

Lab – Converting IPv4 Addresses to Binary

Objectives

Part 1: Convert IPv4 Addresses from Dotted Decimal to Binary

Part 2: Use Bitwise ANDing Operation to Determine Network Addresses

Part 3: Apply Network Address Calculations

Background / Scenario

Every IPv4 address is comprised of two parts: a network portion and a host portion. The network portion of an address is the same for all devices that reside in the same network. The host portion identifies a specific host within a given network. The subnet mask is used to determine the network portion of an IP address. Devices on the same network can communicate directly; devices on different networks require an intermediary Layer 3 device, such as a router, to communicate.

To understand the operation of devices on a network, we need to look at addresses the way devices do—in binary notation. To do this, we must convert the dotted decimal form of an IP address and its subnet mask to binary notation. After this has been done, we can use the bitwise ANDing operation to determine the network address.

This lab provides instructions on how to determine the network and host portion of IP addresses by converting addresses and subnet masks from dotted decimal to binary, and then using the bitwise ANDing operation. You will then apply this information to identify addresses in the network.

Part 1: Convert IPv4 Addresses from Dotted Decimal to Binary

In Part 1, you will convert decimal numbers to their binary equivalent. After you have mastered this activity, you will convert IPv4 addresses and subnet masks from dotted decimal to their binary form.

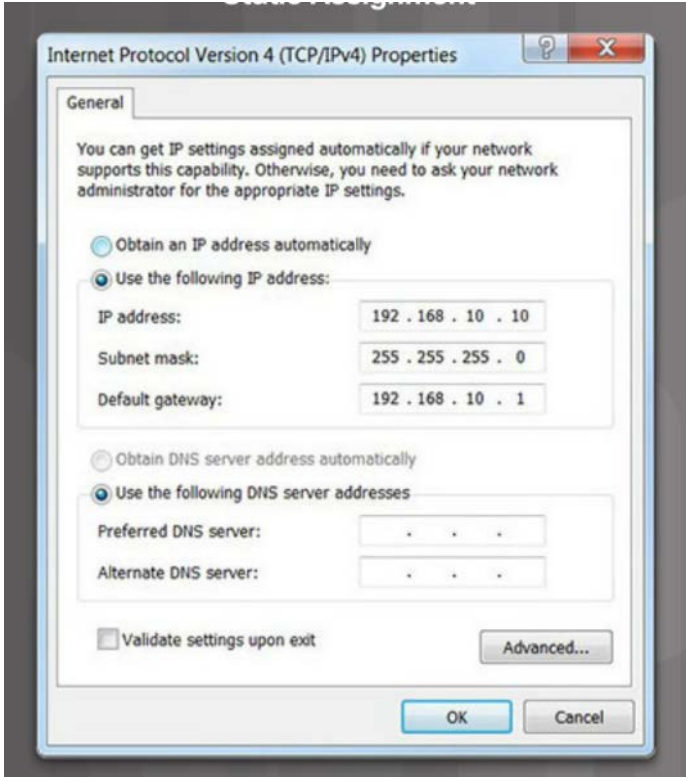
Step 1: Convert decimal numbers to their binary equivalent.

Fill in the following table by converting the decimal number to an 8-bit binary number. The first number has been completed for your reference. Recall that the eight binary bit values in an octet are based on the powers of 2, and from left to right are 128, 64, 32, 16, 8, 4, 2, and 1.

Decimal	Binary
192	11000000
168	

Присвоение хосту статического IPv4-адреса

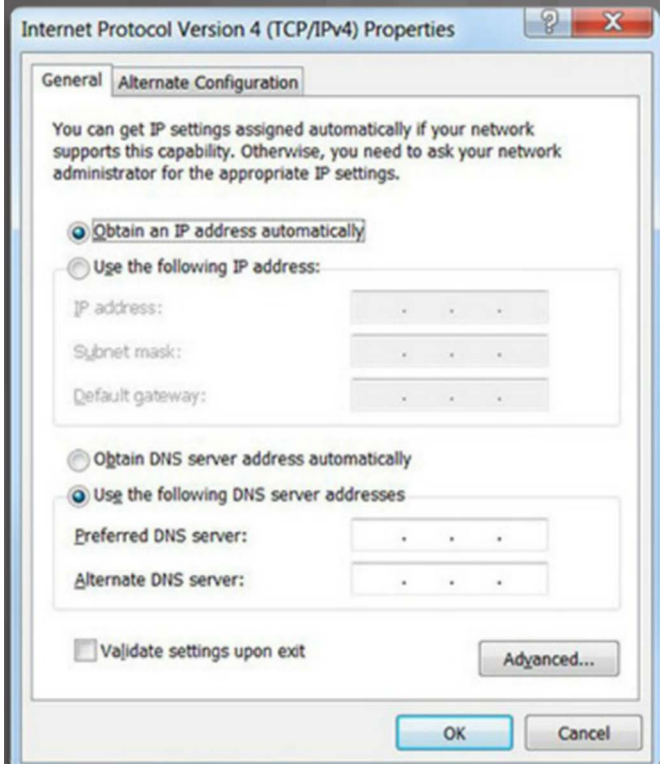
- Некоторым устройствам, например принтерам, серверам и сетевым устройствам, требуется фиксированный IP-адрес.
- Хосты в сети небольшого размера также можно настроить с использованием статических адресов.



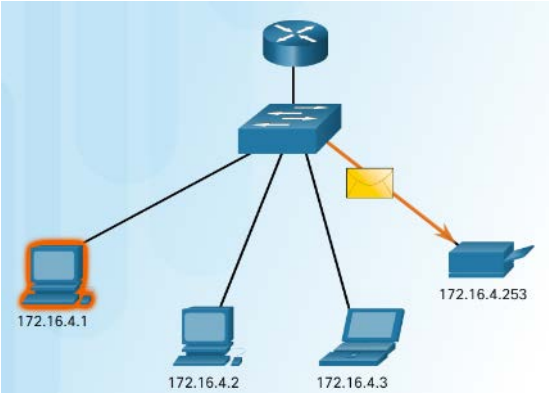
Динамическое назначение хосту IPv4-адреса

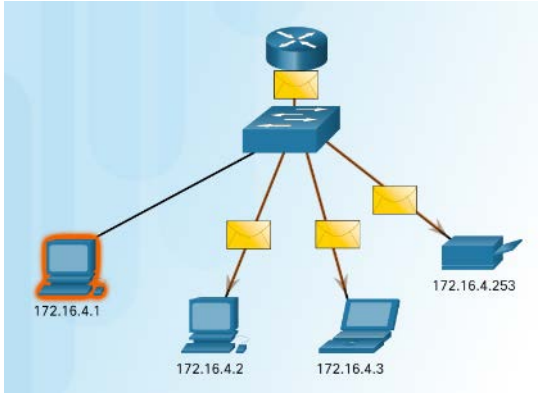
- В большинстве сетей используется протокол динамической настройки хоста (DHCP) для динамического назначения IPv4-адресов.
- DHCP-сервер предоставляет IPv4-адрес, маску подсети, шлюз по умолчанию и другие параметры конфигурации.
- DHCP назначает хостам адреса на определенный период времени.
- Если хост выключается или уходит из сети, его адрес возвращается в пул для повторного использования.

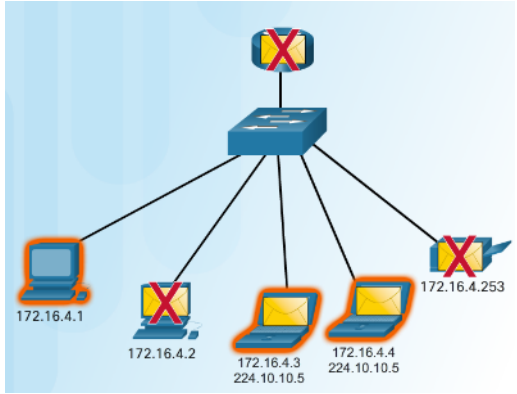
Назначение динамических адресов



Передача данных в IPv4-сети



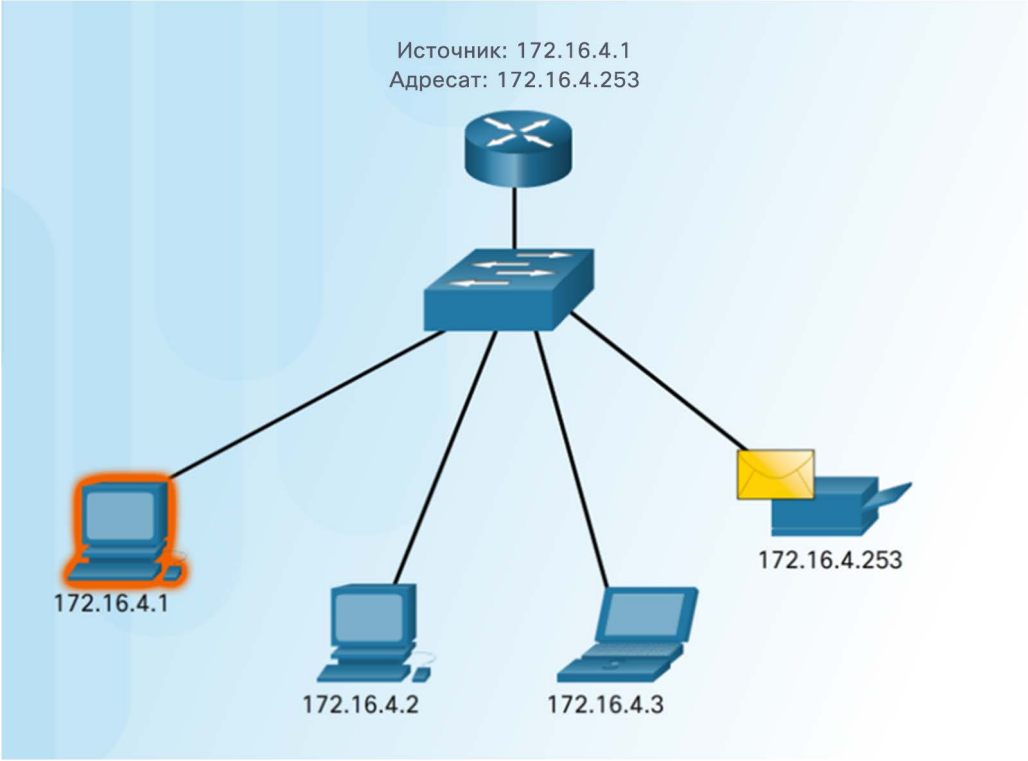




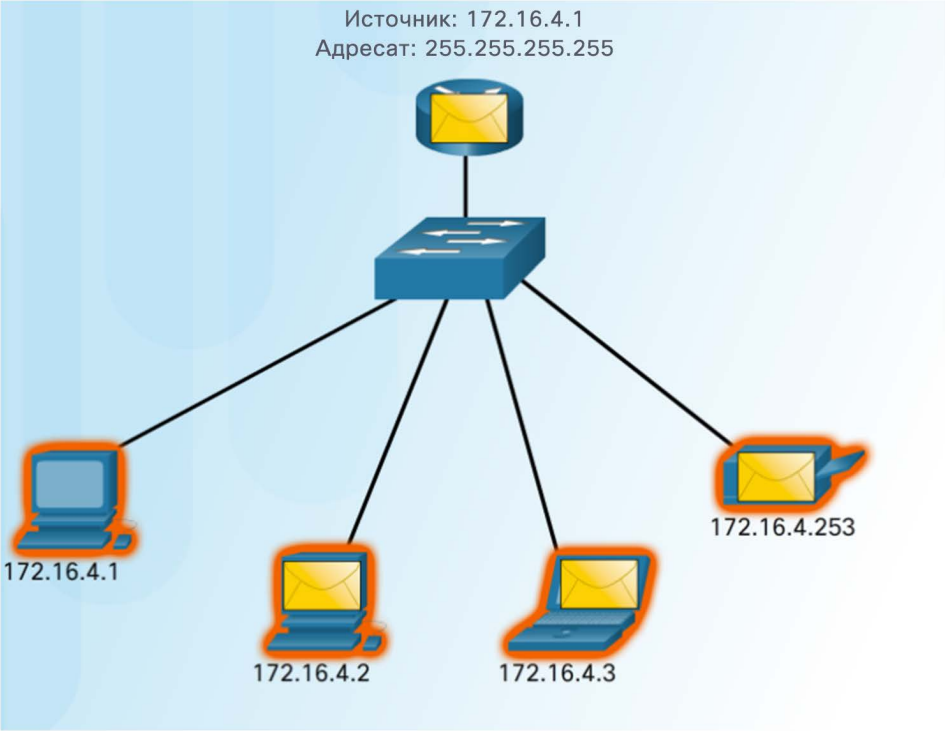
- Одноадресная передача — подключение «один к одному».
- Широковещательная рассылка — «один ко всем»
- Многоадресная рассылка — «один к выбранной группе».

Одноадресная передача

- Одноадресная передача — подключение «один к одному».
  - Используйте адрес устройства назначения в качестве адреса назначения.

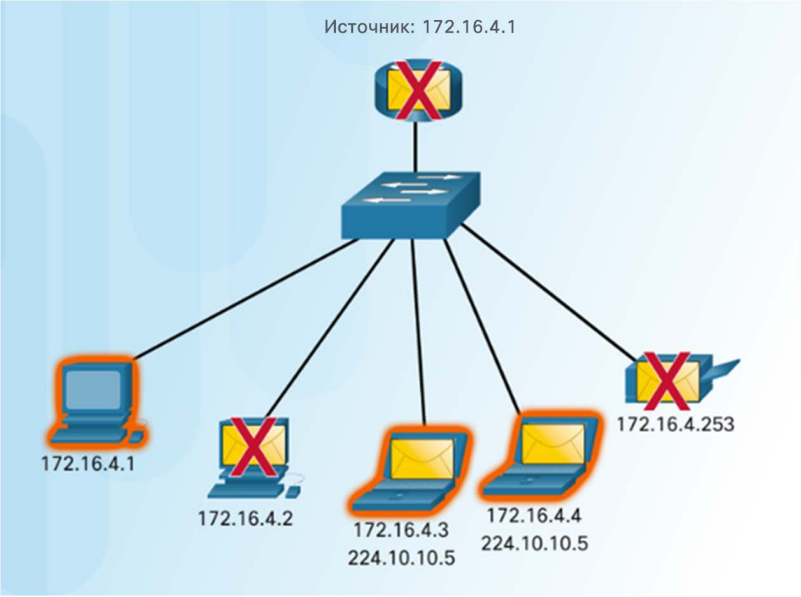


Широковещательная передача



- Широковещательная рассылка — «один ко всем»
  - Сообщение, отправленное для всех пользователей в локальной сети (домен широковещательной рассылки).
  - IPv4-адрес назначения в разделе хоста содержит только единицы (1).

Групповая передача



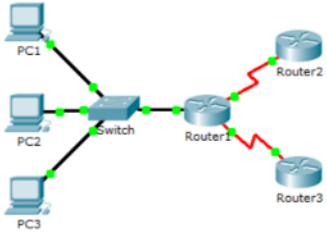
- Групповая рассылка — «один к выбранной группе».
  - Адреса от 224.0.0.0 до 239.255.255.255 зарезервированы для многоадресной рассылки.
  - Протоколы маршрутизации используют групповую рассылку для обмена данными маршрутизации.

Packet Tracer. Анализ трафика одноадресной, широковещательной и многоадресной рассылки

Cisco Networking Academy® Mind Wide Open®

Packet Tracer - Investigate Unicast, Broadcast, and Multicast Traffic

Topology



Objectives

Part 1: Generate Unicast Traffic

Part 2: Generate Broadcast Traffic

Part 3: Investigate Multicast Traffic

Background / Scenario

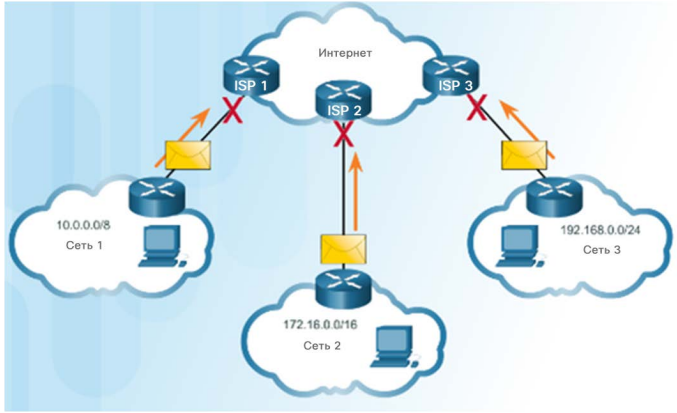
This activity will examine unicast, broadcast, and multicast behavior. Most traffic in a network is unicast. When a PC sends an ICMP echo request to a remote router, the source address in the IP packet header is the IP address of the sending PC. The destination address in the IP packet header is the IP address of the interface on the remote router. The packet is sent only to the intended destination.

Using the **ping** command or the Add Complex PDU feature of Packet Tracer, you can directly ping broadcast addresses to view broadcast traffic.

For multicast traffic, you will view EIGRP traffic. EIGRP is used by Cisco routers to exchange routing information between routers. Routers using EIGRP send packets to multicast address 224.0.0.10, which represents the group of EIGRP routers. Although these packets are received by other devices, they are dropped at Layer 3 by all devices except EIGRP routers, with no other processing required.

Публичные и частные IPv4-адреса

- Частные адреса
  - Немаршрутизируемые
  - Введены в середине 1990-х гг. из-за исчерпания IPv4-адресов.
  - Используются только во внутренних сетях.
  - Для маршрутизации должны быть преобразованы в публичный адрес IPv4.
  - Определяются RFC 1918.
- Блоки частных адресов
  - 10.0.0.0 /8 или от 10.0.0.0 до 10.255.255.255
  - 172.16.0.0 /12 или от 172.16.0.0 до 172.31.255.255192.168.0.0 /16
  - с 192.168.0.0 по 192.168.255.255.



IPv4-адреса специального назначения

Ping-запрос на интерфейс обратной петли

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\NetAcad> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad> ping 127.1.1.1

Pinging 127.1.1.1 with 32 bytes of data:
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Адреса loopback (127.0.0.0/8 или 127.0.0.1)
  - Используется на хосте для проверки работоспособности конфигурации TCP/IP.
- Адреса типа link-local (169.254.0.0/16 или 169.254.0.1)
  - Более известны как адреса автоматической частной IP-адресации (APIPA).
  - Используются клиентом с ОС Windows для автоматической настройки, если нет доступного DHCP-сервера.
- Адреса TEST-NET (192.0.2.0/24 или от 192.0.2.0 до 192.0.2.255)
  - Используются для обучения.

Традиционная классовая адресация

Специфика класса A	
Адреса	0.0.0.0 – 127.0.0.0
Маска подсети по умолчанию	/8 (255.0.0.0)
Максимальное количество сетей	128
Количество узлов в сети	16,777,214
Старший бит	0xxxxxxx.___.___.___

* Адреса 0.0.0.0 и 127.0.0.0 зарезервированы и не могут быть назначены

Специфика класса B	
Адреса	128.0.0.0 – 191.255.0.0
Маска подсети по умолчанию	/16 (255.255.0.0)
Максимальное количество сетей	16,384
Количество узлов в сети	65,534
Старший бит	10xxxxxx.___.___.___

Специфика класса C	
Адреса	192.0.0.0 – 223.255.255.0
Маска подсети по умолчанию	/24 (255.255.255.0)
Максимальное количество сетей	2,097,152
Количество узлов в сети	254
Старший бит	110xxxxx.___.___.___

- В 1981 году адреса IPv4 Интернета назначались при помощи классовой адресации (RFC 790).
- Сетевые адреса были основаны на 3 классах.
  - **Класс A** (от 0.0.0.0/8 до 127.0.0.0/8) разработан для очень крупных сетей с более чем 16 млн адресов хостов.
  - **Класс B** (от 128.0.0.0 /16 до 191.255.0.0 /16) разработан для поддержки потребностей небольших и крупных сетей, содержащих приблизительно до 65 000 адресов хостов.
  - **Класс C** (от 192.0.0.0 /24 до 223.255.255.0 /24) предназначен для небольших сетей с количеством хостов не более 254.

Демонстрационный видеоролик. Классовая IPv4-адресация

- Обсуждение классовой адресации
  - Определение классового адреса по IP-адресу и маске подсети

Бесклассовая адресация

- Классовая адресация растрачивала адреса и полностью истощила доступные IPv4-адреса.
- В 1990-х гг. была представлена бесклассовая адресация
  - Бесклассовая маршрутизация между доменами (CIDR, произносится как «сайдр»)
  - Позволила операторам связи назначать IPv4-адреса в любых битовых границах (имеется в виду длина префикса) вместо адресов класса A, B или C.

Назначение IP-адресов

- Ниже перечислены организации, которые контролируют и обслуживают адреса IPv4 и IPv6 для различных регионов.
  - Американский реестр номеров в сети Интернет (ARIN) — Северная Америка.
  - Réseaux IP Europeans (RIPE) — Европа, Ближний Восток и Центральная Азия.
  - Азиатско-Тихоокеанский сетевой информационный центр (APNIC) — Азиатско-Тихоокеанский регион
  - Африканский сетевой информационный центр (AfriNIC) — Африка
  - Региональный латиноамериканский и карибский реестр IP-адресов (LACNIC) — Латинская Америка и некоторые острова Карибского моря

Лабораторная работа. Определение IPv4-адресов

Cisco Networking Academy®

Mind Wide Open®

Lab– Identifying IPv4 Addresses

Objectives

Part 1: Identify IPv4 Addresses

Part 2: Classify IPv4 Addresses

Background / Scenario

In this lab, you will examine the structure of Internet Protocol version 4 (IPv4) addresses. You will identify the various types of IPv4 addresses and the components that help comprise the address, such as network portion, host portion, and subnet mask. Types of addresses covered include public, private, unicast, and multicast.

Required Resources

- Device with Internet access
- Optional: IPv4 address calculator

Part 1: Identify IPv4 Addresses

In Part 1, you will be given several examples of IPv4 addresses and will complete tables with appropriate information.

Step 1: Analyze the table shown below and identify the network portion and host portion of the given IPv4 addresses.

The first two rows show examples of how the table should be completed.

Key for table:

N = all 8 bits for an octet are in the network portion of the address

n = a bit in the network portion of the address

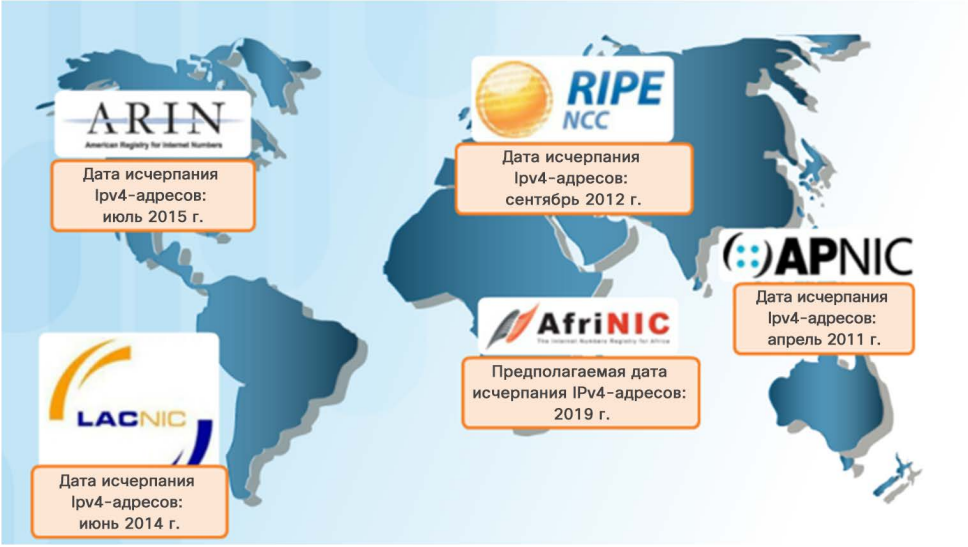
H = all 8 bits for an octet are in the host portion of the address

h = a bit in the host portion of the address

IP Address/Prefix	Network/Host N,n = Network, H,h = Host	Subnet Mask	Network Address
192.168.10.10/24	N.N.N.H	255.255.255.0	192.168.10.0
10.101.99.17/23	N.N.nnnnnnnh.H	255.255.254.0	10.101.98.0
209.165.200.227/27			
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
192.168.28.45/28			

7.2. Сетевые адреса IPv6

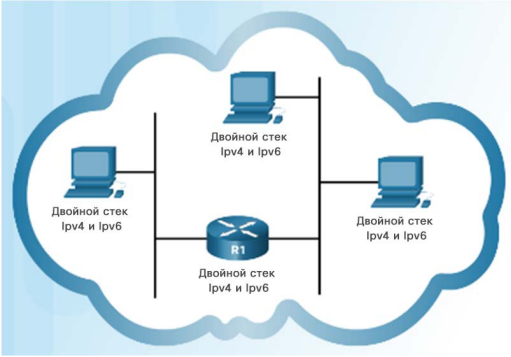
Потребность в протоколе IPv6



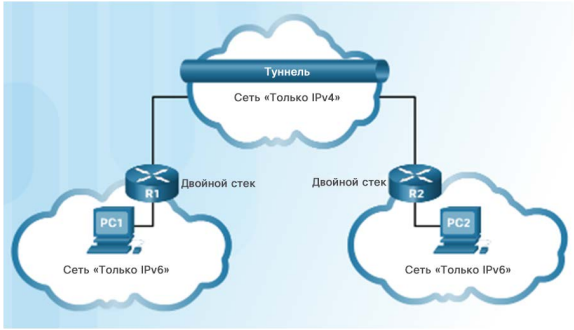
- Сравнение адресации IPv6 с IPv4:
  - Имеет более крупное 128-битное адресное пространство.
  - 340 ундециллионов адресов.
  - Устраняет ограничения, присущие адресации IPv4.
  - Добавляет усовершенствования, такие как автоматическая настройка адреса.
- Зачем нужна адресация IPv6:
  - Быстрый рост количества устройств в Интернете
  - Исчерпание IPv4-адресов
  - Проблемы, связанные с NAT
  - Интернет вещей

Параллельное использование протоколов IPv4 и IPv6

- Способы перехода от IPv4 к IPv6



Двойной стек. Устройства с двойным стеком одновременно работают с протокольными стеками IPv4 и IPv6.

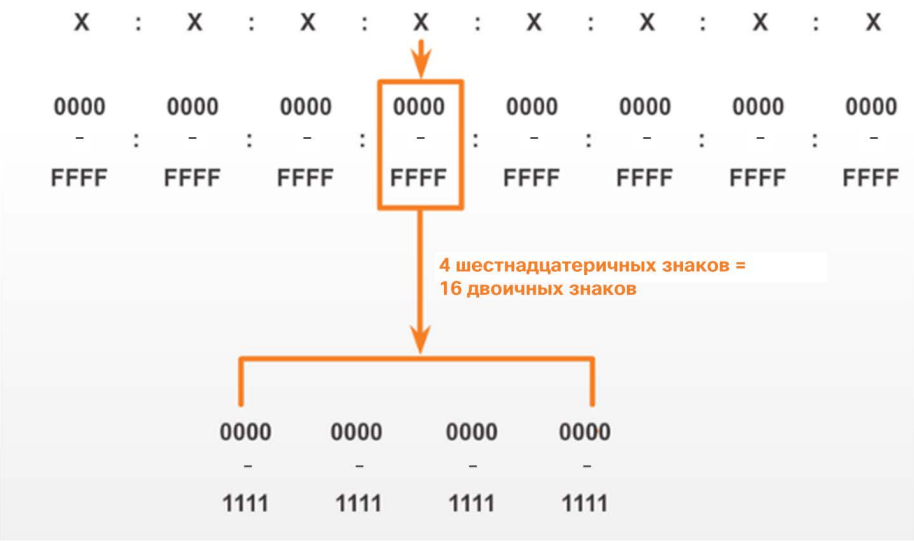


Туннелирование. Пакет IPv6 инкапсулируется внутри пакета IPv4.

Преобразование. Преобразование сетевых адресов версии 64 (NAT64) позволяет устройствам с поддержкой протокола IPv6 обмениваться данными с устройствами IPv4.

Представление IPv6-адресов

- IPv6-адреса:
  - Имеют длину 128 бит
  - Каждые 4 бита представляются одной шестнадцатеричной цифрой
  - Гекстет — неофициальный термин, обозначающий сегмент из 16 бит или четырех шестнадцатеричных значений.



Представление IPv6-адресов (продолжение)

- Предпочтительный формат представления IPv6-адресов

2001	:	0DB8	:	0000	:	1111	:	0000	:	0000	:	0000	:	0200
2001	:	0DB8	:	0000	:	00A3	:	ABCD	:	0000	:	0000	:	1234
2001	:	0DB8	:	000A	:	0001	:	0000	:	0000	:	0000	:	0100
2001	:	0DB8	:	AAAA	:	0001	:	0000	:	0000	:	0000	:	0200
FE80	:	0000	:	0000	:	0000	:	0123	:	4567	:	89AB	:	CDEF
FE80	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
FF02	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
FF02	:	0000	:	0000	:	0000	:	0000	:	0001	:	FF00	:	0200
0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000

Правило 1. Пропуск начальных нулей

- Чтобы сократить или сжать адрес IPv6
  - Первое правило — пропуск нулевых разрядов в любом гекстете.

Предпочитаемый формат	2001:0DB8:0000:1111:0000:0000:0000:0200
Без начальных нулей	2001: DB8: 0:1111: 0: 0: 0: 200

Предпочитаемый формат	2001:0DB8:000A:1000:0000:0000:0000:0100
Без начальных нулей	2001: DB8: A:1000: 0: 0: 0: 100

Предпочитаемый формат	0000:0000:0000:0000:0000:0000:0000:0000
Без начальных нулей	0: 0: 0: 0: 0: 0: 0: 0

Правило 2. Пропуск всех нулевых сегментов

- Правило 2. Пропуск всех нулевых сегментов
  - Двойное двоеточие (::) может заменять все единичные, непрерывные строки из одного или нескольких 16-битных сегментов (хекстетов), которые состоят только из нулей.

Предпочитаемый формат	2001:0DB8:0000:0000:ABCD:0000:0000:0100
Без начальных нулей	2001: DB8: 0: 0:ABCD: 0: 0: 100
Сжатый формат	2001:DB8::ABCD:0:0:100
или	
Сжатый формат	2001:DB8:0:0:ABCD::100

Можно использовать только одно сдвоенное двоеточие (::).

Правило 2. Пропуск всех нулевых сегментов (продолжение)

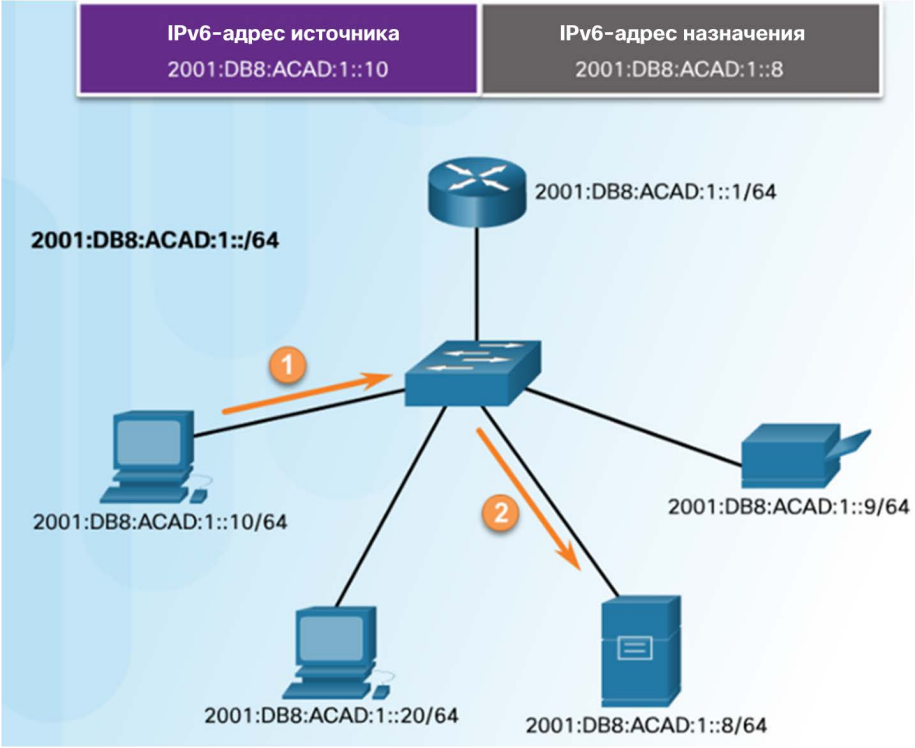
- Правило 2. Пропуск всех нулевых сегментов
  - Двойное двоеточие (::) может заменять все единичные, непрерывные строки из одного или нескольких 16-битных сегментов (хекстетов), которые состоят только из нулей.

Предпочитаемый формат	FF02:0000:0000:0000:0000:0000:0000:0001
Без начальных нулей	FF02:0:0:0:0:0:0:1
Сжатый формат	FF02::1

Предпочитаемый формат	0000:0000:0000:0000:0000:0000:0000:0000
Без начальных нулей	0:0:0:0:0:0:0:0
Сжатый формат	::

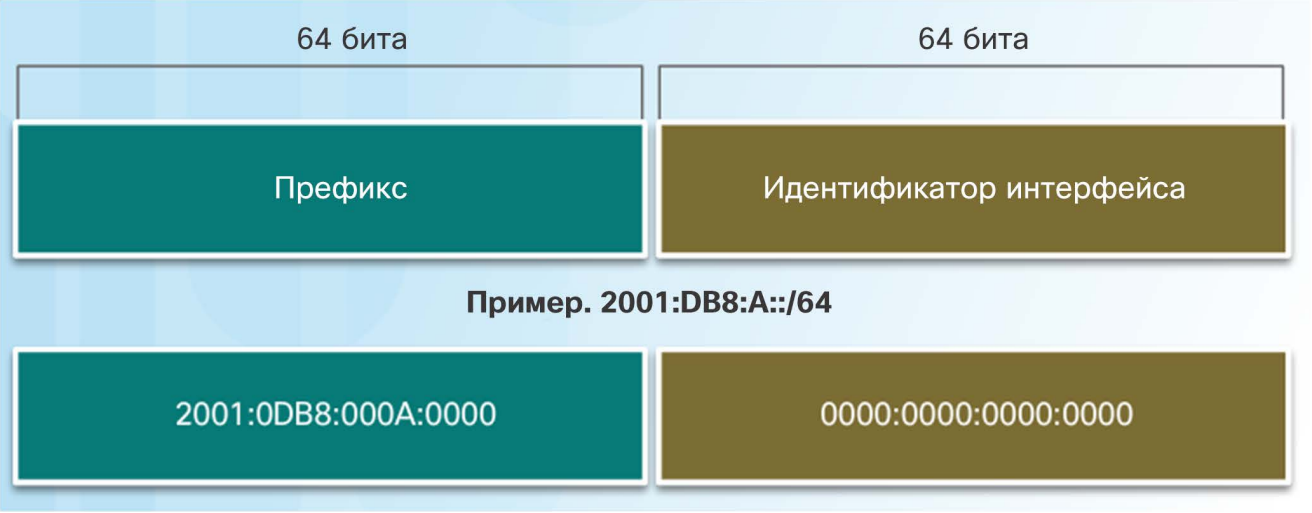
Типы адресов IPv6

- Существует три типа IPv6-адресов:
  - **Индивидуальный:** один IPv6-адрес источника.
  - **Групповой (или адрес многоадресной рассылки)**: используется для отправки одного IPv6-пакета на несколько адресов назначения.
  - **Произвольный (или адрес произвольной рассылки)**: любой индивидуальный IPv6-адрес, который может быть назначен нескольким устройствам.



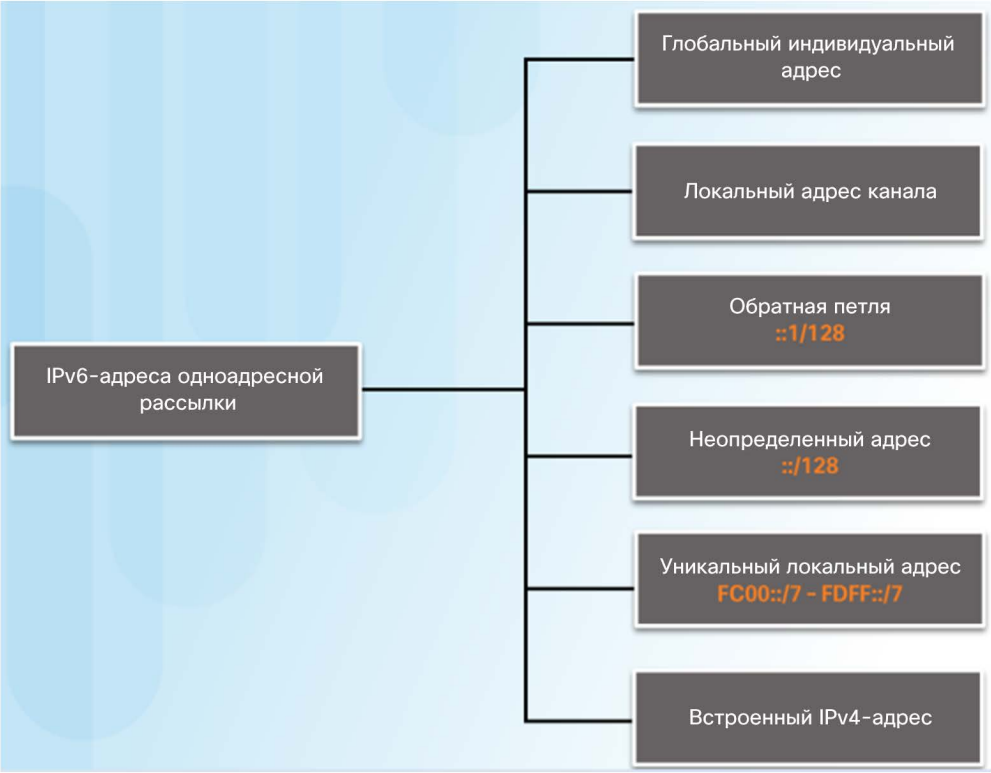
Длина префикса IPv6-адреса

- Длина префикса обозначает раздел сети IPv6-адреса.
  - Диапазон длины префикса может составлять от 0 до 128.
  - Типичная длина префикса IPv6 для большинства локальных сетей — /64.



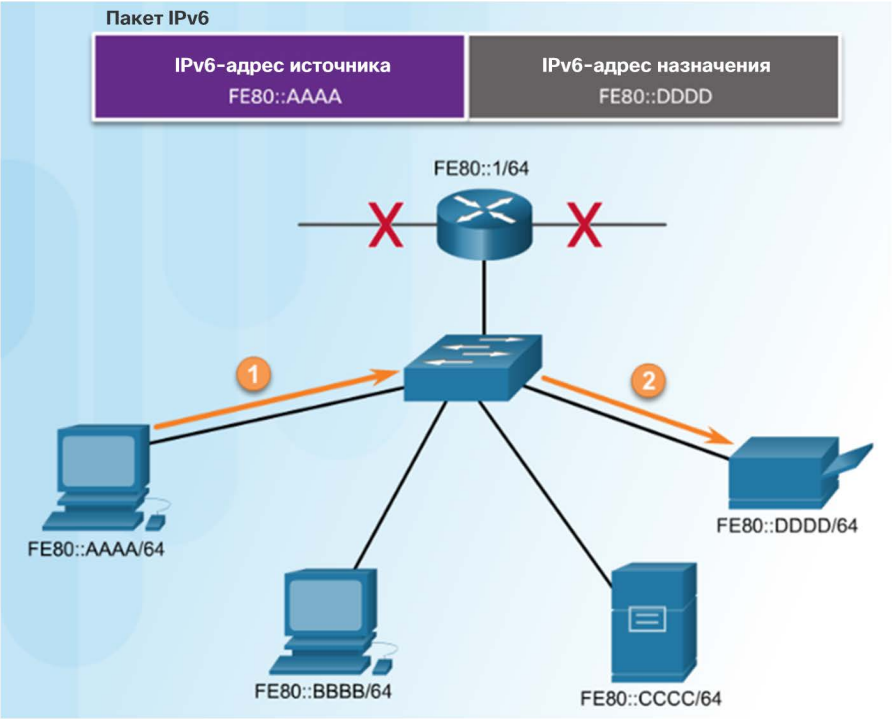
Индивидуальные IPv6-адреса

- **Глобальные индивидуальные адреса**. Эти адреса, к которым можно проложить маршрут по Интернету, являются уникальными по всему миру.
- **Локальные адреса канала** используются для обмена данными с другими устройствами по одному локальному каналу. Ограничены одним каналом.
- **Уникальные локальные адреса** используются для локальной адресации в пределах объекта или между ограниченным количеством объектов.



Локальные индивидуальные IPv6-адреса канала

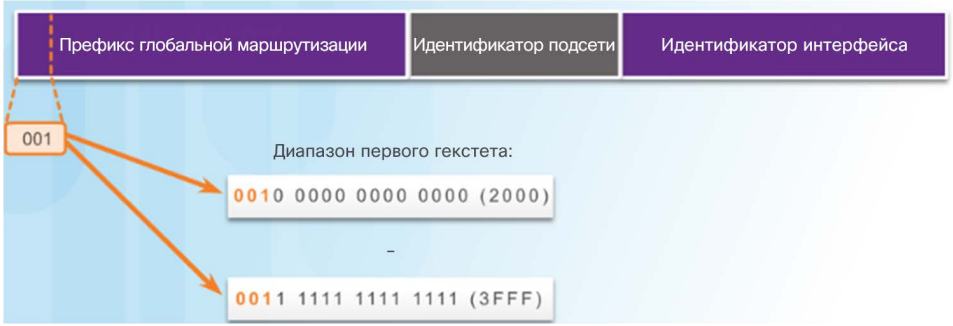
- IPv6-адреса типа link-local:
  - Позволяют устройству обмениваться данными с другими устройствами, поддерживающими адресацию IPv6, по одному и тому же каналу.
  - Создаются даже в том случае, если устройству не был назначен глобальный индивидуальный IPv6-адрес.
  - Находятся в диапазоне FE80::/10.

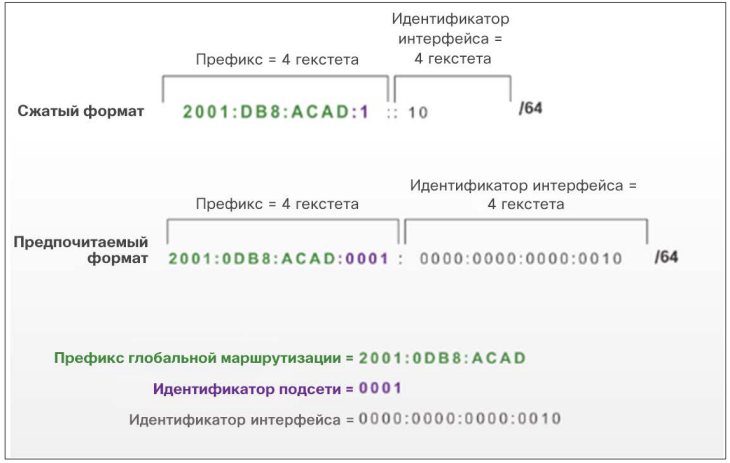


Примечание. Как правило, в качестве шлюза по умолчанию для других устройств в канале используется локальный адрес канала маршрутизатора.

Структура глобального индивидуального IPv6-адреса

- В настоящее время назначаются только глобальные индивидуальные адреса с первыми тремя битами 001 или 2000::/3.
- Глобальный индивидуальный адрес состоит из трех частей.
  - **Префикс глобальной маршрутизации.** Это сетевая часть адреса, которая назначается провайдером. Обычно это /48.
  - **Идентификатор подсети.** Используется для подсети в пределах организации.
  - **Идентификатор интерфейса** является эквивалентом раздела хоста в адресе IPv4.



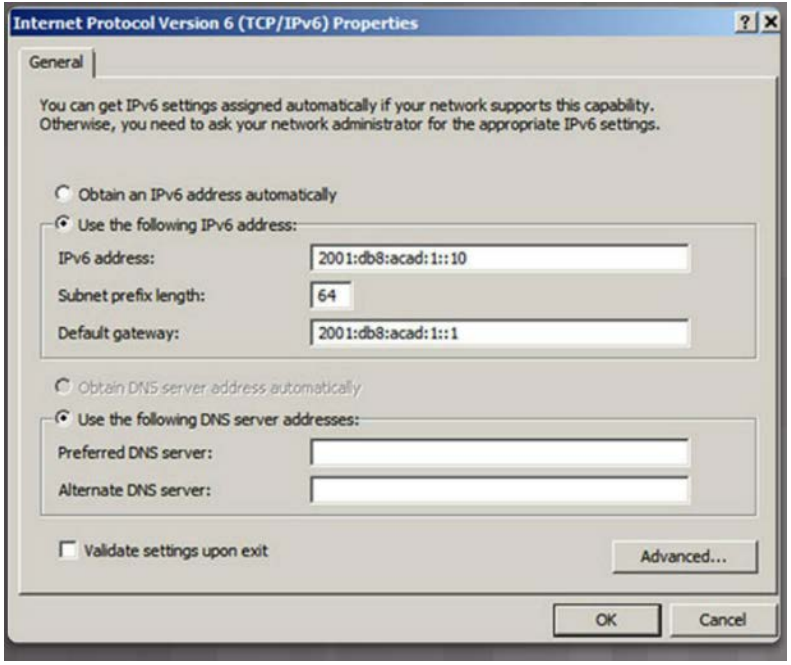


Статическая конфигурация глобального индивидуального адреса


```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# clock rate 56000
R1(config-if)# no shutdown
```

- Конфигурация маршрутизатора:
  - Команды аналогичны протоколу IPv4, замените IPv4 на IPv6.
  - Для настройки глобального индивидуального IPv6-адреса в интерфейсе используется команда **ipv6 address** *ipv6-address/prefix-length*.

Статическая конфигурация глобального индивидуального адреса (продолжение)



- Настройка узлов:
  - Ручная настройка IPv6-адреса на хосте аналогична настройке IPv4-адреса.
  - Адрес шлюза по умолчанию можно настроить в соответствии с локальным адресом канала или глобальным индивидуальным адресом интерфейса Gigabit Ethernet.
- Динамическое назначение IPv6-адресов:
  - Автоматическая конфигурация адреса без сохранения состояния (Stateless Address Autoconfiguration, SLAAC)
  - Адресация DHCPv6 с учётом состояний.

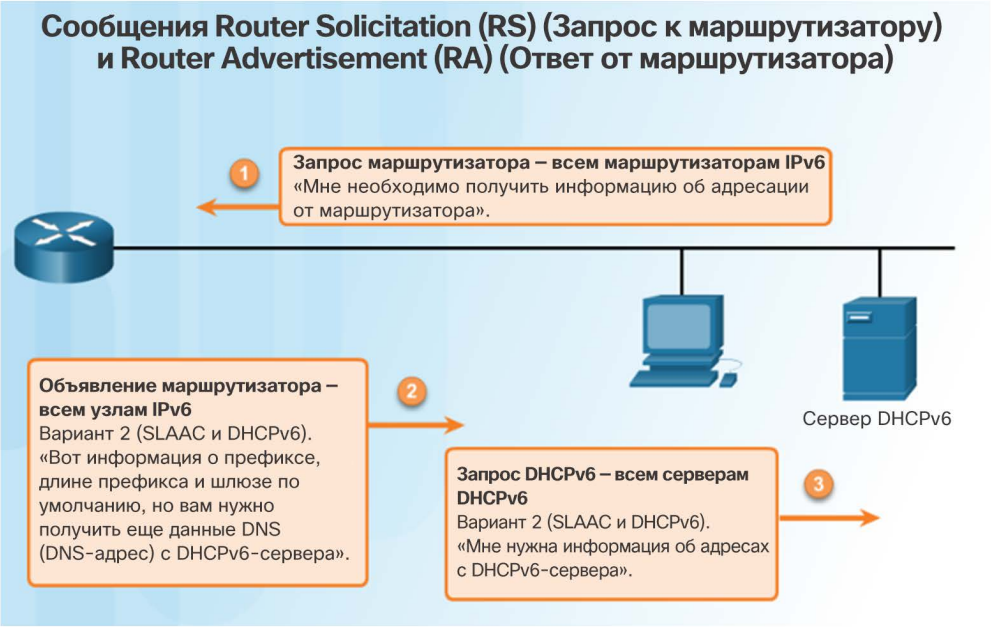
Динамическая конфигурация с помощью SLAAC

- Автоматическая конфигурация адреса без сохранения состояния (Stateless Address Autoconfiguration, SLAAC):
  - Устройство может получить префикс, длину префикса, адрес шлюза по умолчанию и другие сведения от IPv6-маршрутизатора.
  - Использует сообщения ICMPv6 Router Advertisement (RA) локального маршрутизатора.
- Сообщения RA ICMPv6 отправляются каждые 200 секунд всем устройствам в сети под управлением IPv6.

Вариант 1 (только SLAAC). «Я уже знаю все необходимое (префикс, длина префикса, шлюз по умолчанию)».
Вариант 2 (SLAAC и DHCPv6). «Вот моя информация, но вам нужно получить другие сведения, такие как DNS-адреса от DHCPv6-сервера».
Вариант 3 (только DHCPv6) — «Я не могу помочь вам. Всю информацию нужно получить от DHCPv6-сервера».

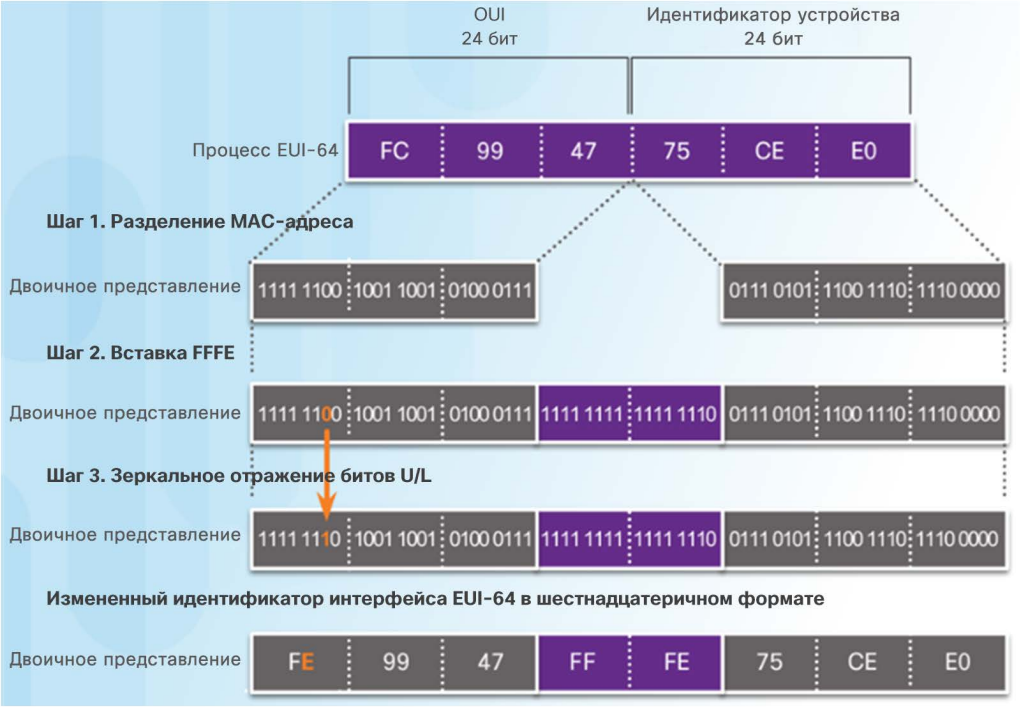
Динамическая конфигурация с помощью DHCPv6

- RA, вариант 1: только SLAAC (по умолчанию)
- RA, вариант 2: SLAAC и DHCPv6-сервер без сохранения состояния адресов:
  - Использует SLAAC для глобального индивидуального адреса IPv6 и шлюза по умолчанию.
  - Использует сервер DHCPv6 без отслеживания состояния для получения других сведений.
- RA, вариант 3: DHCPv6-сервер с сохранением состояния адресов
  - Использует локальные адреса канала маршрутизаторов для шлюза по умолчанию.
  - Использует DHCPv6 для получения других сведений.



Процесс EUI-64 и случайно созданный идентификатор интерфейса

- Если сообщение RA имеет тип SLAAC либо SLAAC и DHCPv6-сервер без сохранения состояния адресов, клиент должен создавать собственный идентификатор интерфейса.
  - Идентификатор интерфейса может быть создан с помощью EUI-64 или представлять собой случайно созданное 64-битное число.
- Идентификатор интерфейса EUI-64 имеет двоичный формат и состоит из трех частей.
  - 24-битный OUI на основе MAC-адреса клиента, в котором седьмой бит (универсально/локальный (U/L) бит) является обратным,
  - В середину вставляется 16-битное значение FFFE (в шестнадцатеричном формате).
  - 24-битный идентификатор устройства на основе MAC-адреса клиента.



Процесс EUI-64 и случайно созданный идентификатор интерфейса (продолжение)

- Случайно сгенерированные идентификаторы интерфейса
  - В Windows используется случайно созданный идентификатор интерфейса.

```
PCB> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  :
   IPv6 Address. . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway   . . . . . . . : fe80::1
```

Из сообщения RA

Случайное 64-битное число

Динамические адреса типа link-local

- Адрес типа link-local может быть создан динамически или настроен вручную.
- Маршрутизаторы Cisco IOS используют процесс EUI-64 для создания идентификатора интерфейса для всех локальных адресов канала в IPv6-интерфейсах.
- Недостатком использования динамически назначенного локального адреса канала является длинный идентификатор интерфейса, поэтому они часто настраиваются статически.

```
R1# show interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
<Output Omitted>

R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
R1#
```

Адреса типа link-local
с использованием EUI-64

Статические адреса типа link-local

- При ручной настройке локального адреса канала можно создавать простые и легко запоминающиеся адреса.

```
Router(config-if)#
ipv6 address link-local-address link-local
```

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#
```

Проверка конфигурации IPv6-адреса

- Команды для проверки конфигурации IPv6 аналогичны командам для IPv4.
  - show ipv6 interface brief
  - show ipv6 route
- Команда ping для IPv6 идентична команде, используемой для IPv4, за исключением того, что используется IPv6-адрес.

```
R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
R1#
```

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static


C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)
R1#
```

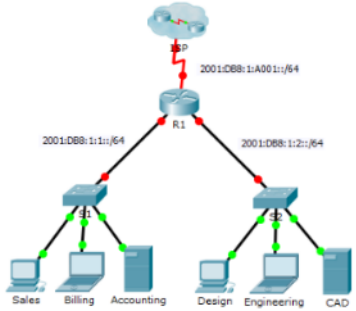
Packet Tracer. Настройка IPv6-адресации

Cisco Networking Academy®

Mind Wide Open®

Packet Tracer - Configuring IPv6 Addressing

Topology



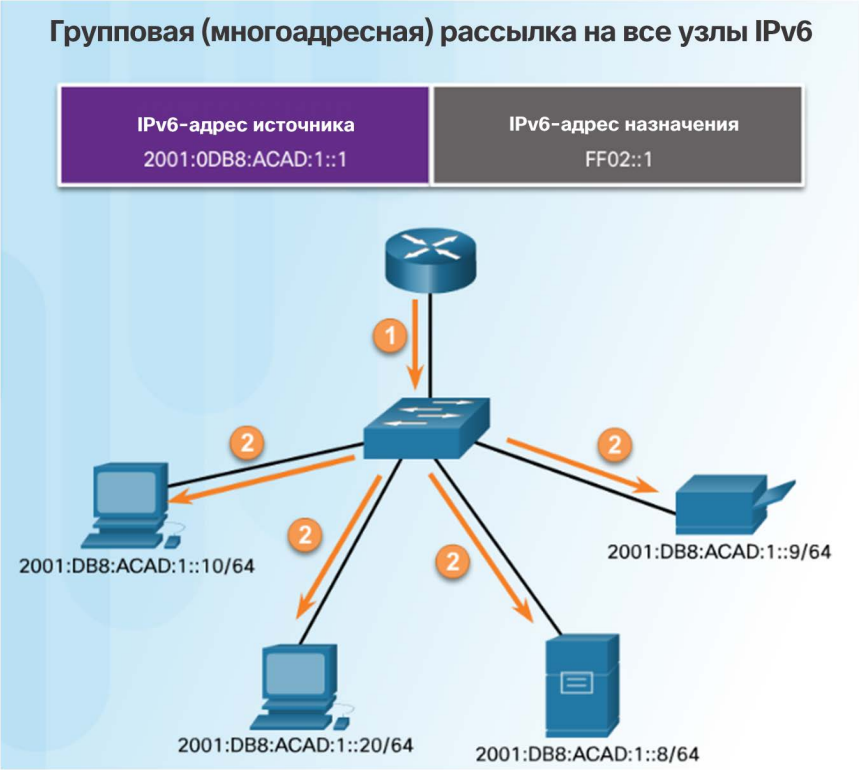
Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
R1	G0/0	2001:DB8:1:1::1/64	N/A
	G0/1	2001:DB8:1:2::1/64	N/A
	S0/0/0	2001:DB8:1:A001::2/64	N/A
	Link-local	FE80::1	N/A
Sales	NIC	2001:DB8:1:1::2/64	FE80::1
Billing	NIC	2001:DB8:1:1::3/64	FE80::1
Accounting	NIC	2001:DB8:1:1::4/64	FE80::1
Design	NIC	2001:DB8:1:2::2/64	FE80::1
Engineering	NIC	2001:DB8:1:2::3/64	FE80::1
CAD	NIC	2001:DB8:1:2::4/64	FE80::1

Objectives

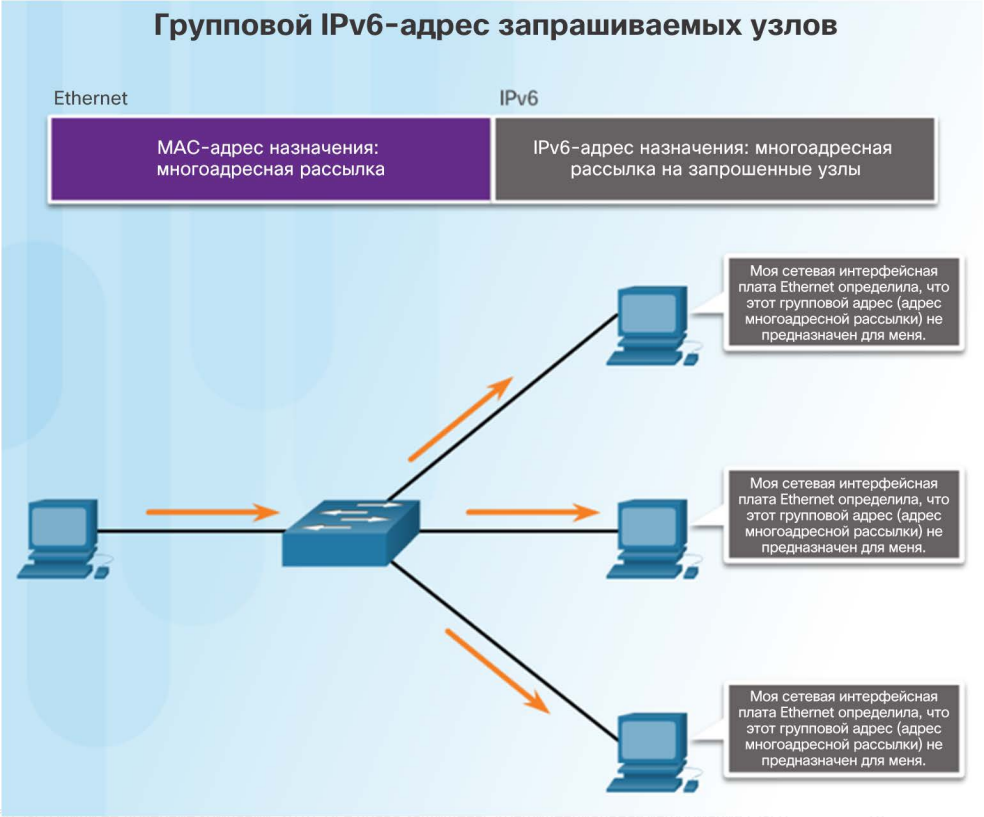
Присвоенные групповые IPv6-адреса

- Существует два типа групповых IPv6-адресов:
  - Присвоенные групповые адреса зарезервированы для заданных групп устройств.
  - Групповой адрес запрашиваемого узла
- Есть две распространенные группы присвоенных групповых IPv6-адресов:
  - Группа многоадресной рассылки для всех узлов FF02::1. Это группа многоадресной рассылки, в которую включены все устройства под управлением протокола IPv6. Аналогична широковещательной рассылке в IPv4.
  - Группа многоадресной рассылки для всех маршрутизаторов FF02::2. Это группа многоадресной рассылки, в которую включены все IPv6-маршрутизаторы.



Групповые IPv6-адреса запрашиваемых узлов

- Групповой адрес запрошенного узла:
  - сопоставляется с особым групповым адресом Ethernet;
  - позволяет сетевой интерфейсной плате Ethernet фильтровать кадры по MAC-адресу назначения.



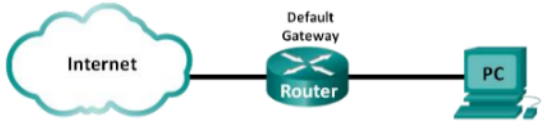
Лабораторная работа. Определение IPv6-адресов

Cisco Networking Academy

Mind Wide Open

Lab – Identifying IPv6 Addresses

Topology



Objectives

Part 1: Identify the Different Types of IPv6 Addresses

Part 2: Examine a Host IPv6 Network Interface and Address

Part 3: Practice IPv6 Address Abbreviation

Background / Scenario

With the depletion of the Internet Protocol version 4 (IPv4) network address space and the adoption and transition to IPv6, networking professionals must understand how both IPv4 and IPv6 networks function. Many devices and applications already support IPv6. This includes extensive Cisco device Internetwork Operating System (IOS) support and workstation/server operating system support, such as that found in Windows and Linux.

This lab focuses on IPv6 addresses and the components of the address. In Part 1, you will identify the IPv6 address types, and in Part 2, you will view the IPv6 settings on a PC. In Part 3, you will practice IPv6 address abbreviation.

Required Resources

- 1 PC (Windows 7 or 8 with Internet access)

Part 1: Identify the Different Types of IPv6 Addresses

In Part 1, you will review the characteristics of IPv6 addresses to identify the different types of IPv6 addresses.

Step 1: Review the different types of IPv6 addresses.

An IPv6 address is 128 bits long. It is most often presented as 32 hexadecimal characters. Each hexadecimal character is the equivalent of 4 bits (4 x 32 = 128). A non-abbreviated IPv6 host address is shown here:

2001:0DB8:0001:0000:0000:0000:0000:0001

A hextet is the hexadecimal, IPv6 version of an IPv4 octet. An IPv4 address is 4 octets long, separated by dots. An IPv6 address is 8 hextets long, separated by colons.

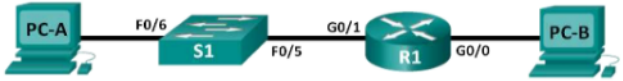
Лабораторная работа. Настройка IPv6-адресов на сетевых устройствах

Cisco Networking Academy

Mind Wide Open

Lab - Configuring IPv6 Addresses on Network Devices

Topology



Addressing Table

Device	Interface	IPv6 Address	Prefix Length	Default Gateway
R1	G0/0	2001:DB8:ACAD:A::1	64	N/A
	G0/1	2001:DB8:ACAD:1::1	64	N/A
S1	VLAN 1	2001:DB8:ACAD:1::B	64	N/A
PC-A	NIC	2001:DB8:ACAD:1::3	64	FE80::1
PC-B	NIC	2001:DB8:ACAD:A::3	64	FE80::1

Objectives

Part 1: Set Up Topology and Configure Basic Router and Switch Settings

Part 2: Configure IPv6 Addresses Manually

Part 3: Verify End-to-End Connectivity

Background / Scenario

Knowledge of the Internet Protocol version 6 (IPv6) multicast groups can be helpful when assigning IPv6 addresses manually. Understanding how the all-router multicast group is assigned and how to control address assignments for the Solicited Nodes multicast group can prevent IPv6 routing issues and help ensure best practices are implemented.

In this lab, you will configure hosts and device interfaces with IPv6 addresses and explore how the all-router multicast group is assigned to a router. You will use **show** commands to view IPv6 unicast and multicast addresses. You will also verify end-to-end connectivity using the **ping** and **traceroute** commands.

Note: The routers used with CCNA hands-on labs are Cisco 1941 ISRs with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

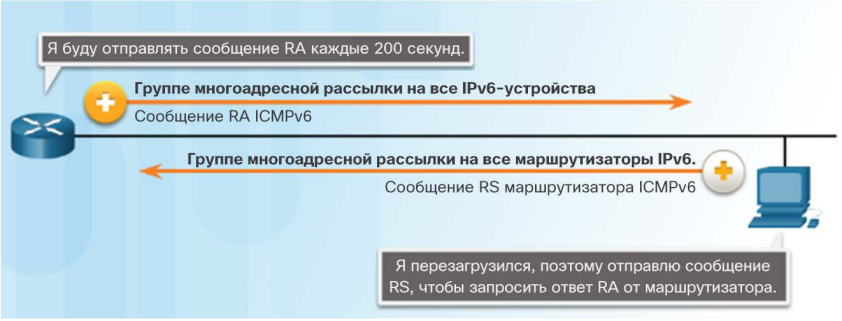
7.3. Проверка подключения

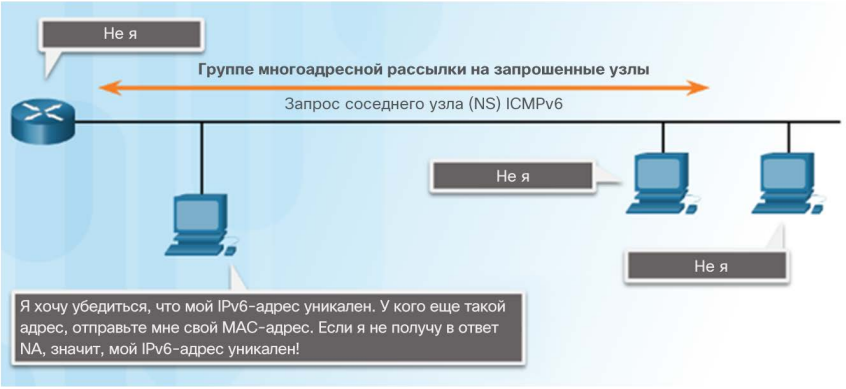
Протоколы ICMPv4 и ICMPv6

- ICMPv4 — это протокол обмена сообщениями для IPv4. Протокол ICMPv6 предоставляет такие же службы для IPv6.
- Следующие ICMP-сообщения являются одинаковыми для обеих версий:
  - Подтверждение узла
  - Узел назначения или сервис недоступны
  - Превышен интервал ожидания
  - Переадресация маршрута

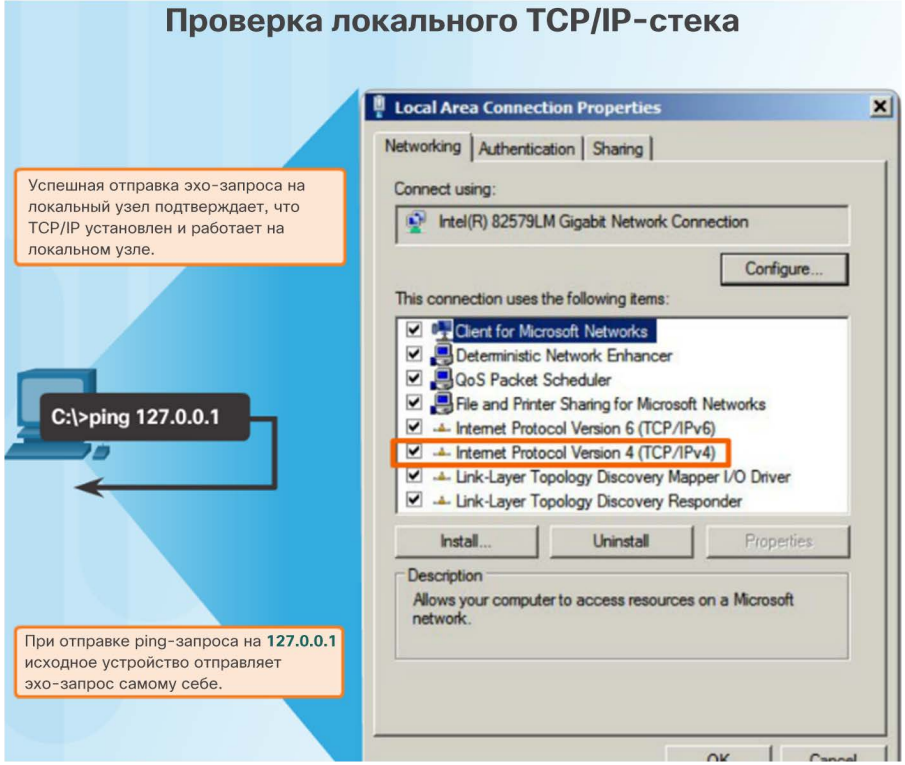
Сообщения ICMPv6 Router Solicitation (RS) (Запрос к маршрутизатору) и Router Advertisement (RA) (Ответ от маршрутизатора)

- ICMPv6 включает четыре новых протокола в составе протокола обнаружения соседа (ND или NDP)
  - Сообщение «Запрос к маршрутизатору» (Router Solicitation, RS)
  - Сообщение «Ответ маршрутизатора» (Router Advertisement, RA).
- Сообщения RA, используемые для предоставления хостам информации об адресации
  - Сообщение с запросом поиска соседей (NS)
  - Сообщение об объявлении соседних узлов (NA)
- Сообщения NS и NA используются для разрешения адресов и для обнаружения дублирующихся адресов (Duplicate Address Detection, DAD).



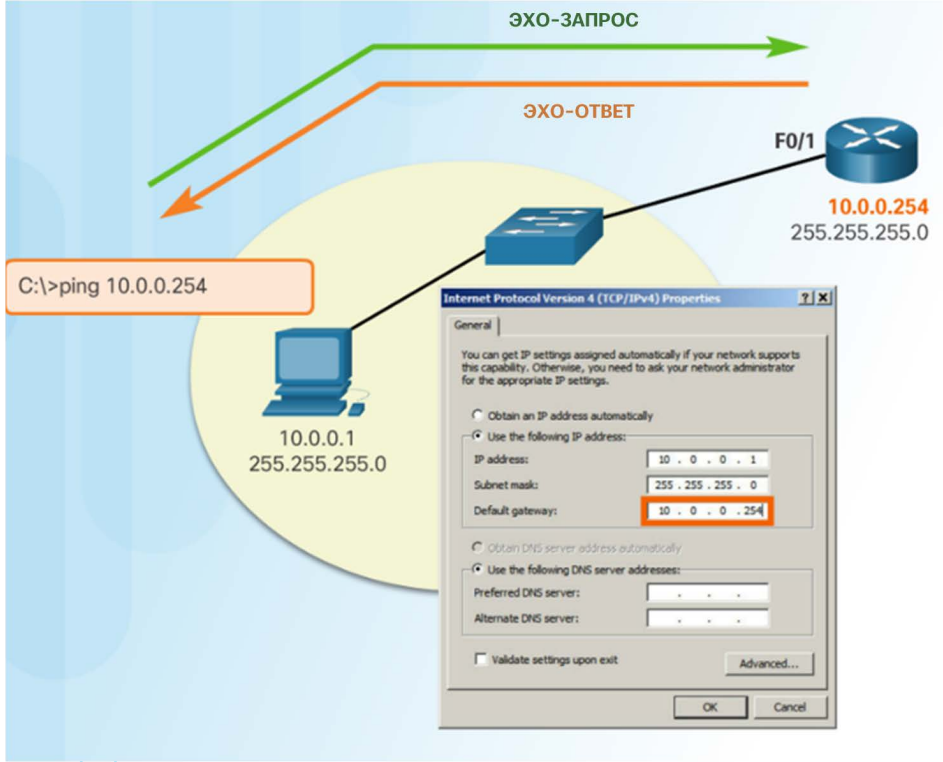


Выполнение команды ping. Тестирование локального стека



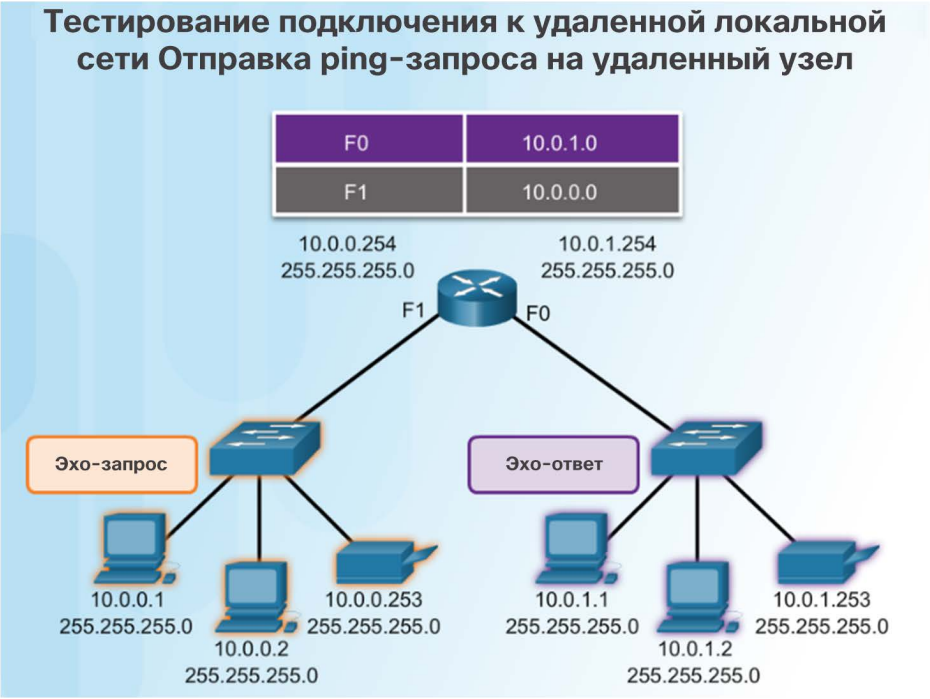
- Ping-запрос на локальный loopback-адрес 127.0.0.1 для IPv4 или ::1 для IPv6 позволяет проверить правильность настройки IP на хосте.

Выполнение команды ping. Тестирование подключения к локальной сети (LAN)



- Команду ping можно использовать для проверки способности хоста обмениваться данными по локальной сети.

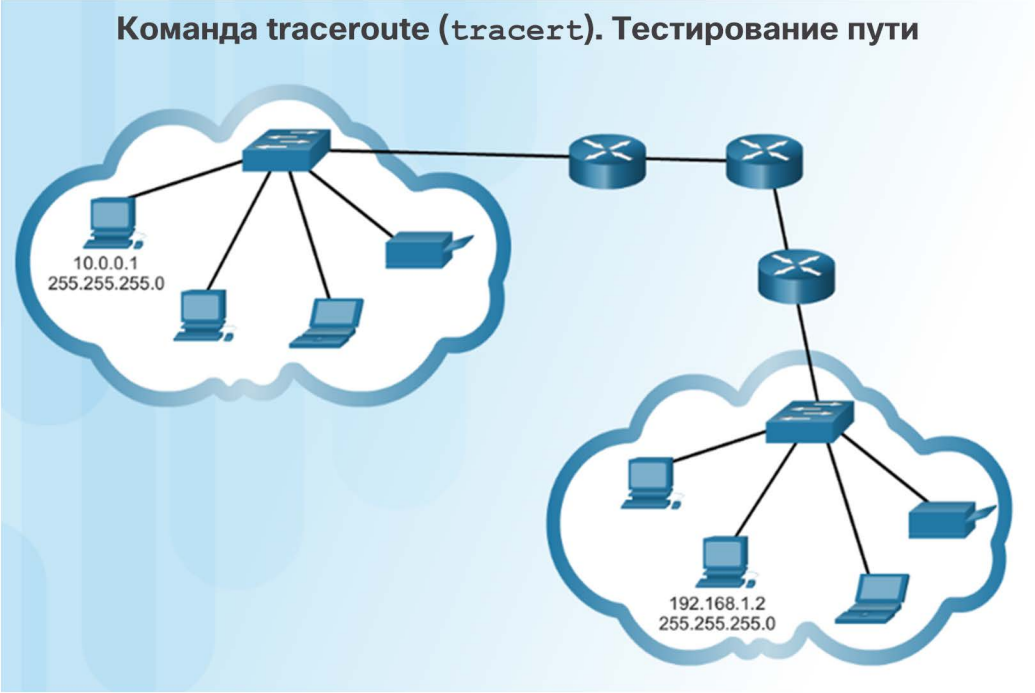
Выполнение команды ping. Тестирование подключения к удаленному узлу



- Команду ping можно использовать для проверки способности хоста обмениваться данными с другими сетями.

Команда traceroute. Тестирование пути

- Команда traceroute (tracert) — это утилита, позволяющая составить список переходов, по которым успешно проходит эхо-запрос на пути к узлу назначения.
  - Время прохождения сигнала в прямом и обратном направлениях (RTT) — это время, которое требуется на доставку пакета на удаленный хост и получения ответа это этого хоста.
  - Символ звездочки (*) используется для обозначения потерянного пакета.



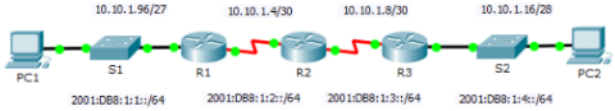
Packet Tracer. Проверка адресации IPv4 и IPv6

Cisco Networking Academy®

Mind Wide Open®

Packet Tracer - Verifying IPv4 and IPv6 Addressing

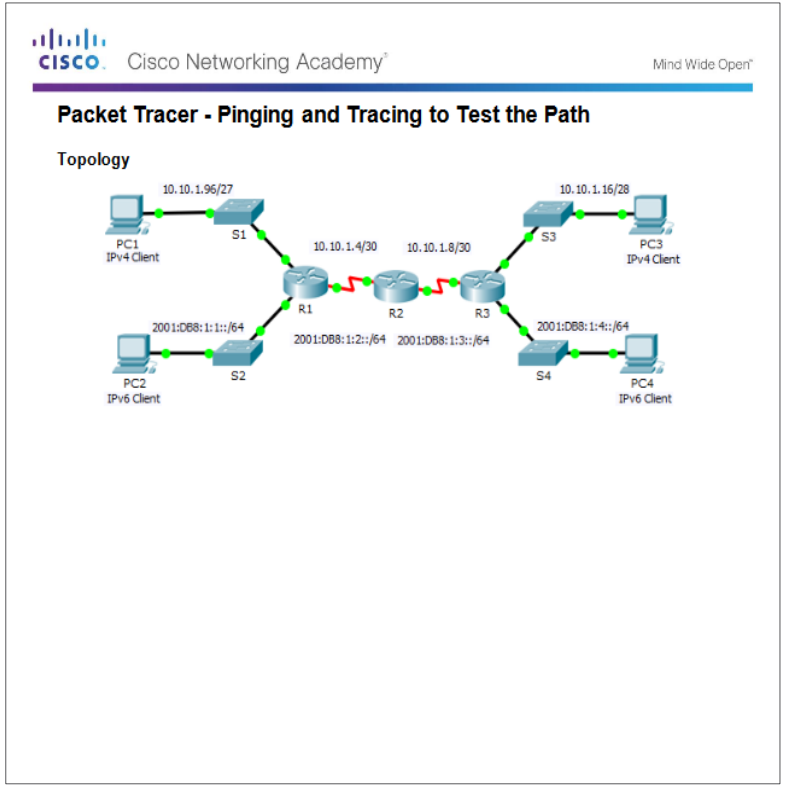
Topology



Addressing Table

Device	Interface	IPv4 Address / IPv6 Address/Prefix	Subnet Mask	Default Gateway
R1	G0/0	10.10.1.97	255.255.255.224	N/A
		2001:DB8:1:1::1/64		N/A
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:DB8:1:2::2/64		N/A
	Link-local	FE80::1		N/A
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:DB8:1:2::1/64		N/A
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:DB8:1:3::1/64		N/A
	Link-local	FE80::2		N/A
R3	G0/0	10.10.1.17	255.255.255.240	N/A
		2001:DB8:1:4::1/64		N/A
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:DB8:1:3::2/64		N/A

Packet Tracer. Выполнение команды ping и трассировка маршрута для проверки пути



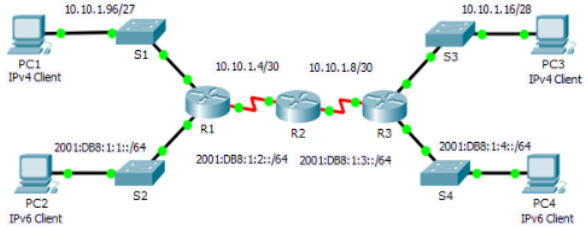
Лабораторная работа. Проверка сетевого подключения с помощью команд ping и traceroute

Cisco Networking Academy®

Mind Wide Open®

Packet Tracer - Pinging and Tracing to Test the Path

Topology



Лабораторная работа. Составление карты сети Интернет

Cisco Networking Academy®

Mind Wide Open™

Lab - Mapping the Internet

Objectives

Part 1: Test Network Connectivity Using Ping

Part 2: Trace a Route to a Remote Server Using Windows Tracert

Background

Route tracing computer software is a utility that lists the networks data has to traverse from the user's originating end device to a distant destination network.

This network tool is typically executed at the command line as:

```
tracert <destination network name or end device address>
```

(Microsoft Windows systems)

or

```
traceroute <destination network name or end device address>
```

(UNIX and similar systems)

Route tracing utilities allow a user to determine the path or routes as well as the delay across an IP network. Several tools exist to perform this function.

The **traceroute** (or **tracert**) tool is often used for network troubleshooting. By showing a list of routers traversed, it allows the user to identify the path taken to reach a particular destination on the network or across internetworks. Each router represents a point where one network connects to another network and through which the data packet was forwarded. The number of routers is known as the number of "hops" the data traveled from source to destination.

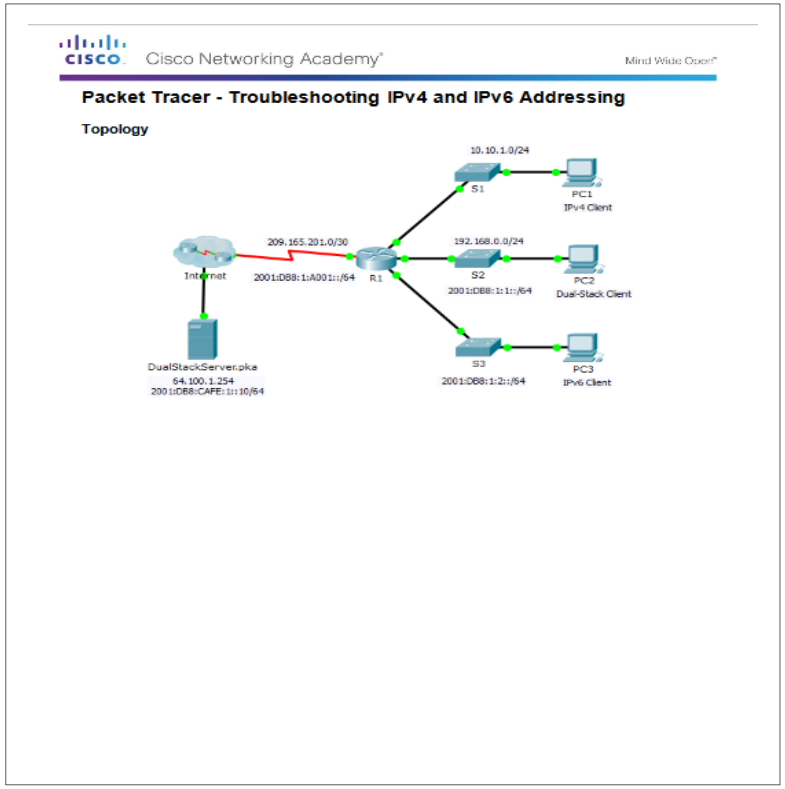
The displayed list can help identify data flow problems when trying to access a service such as a website. It can also be useful when performing tasks such as downloading data. If there are multiple websites (mirrors) available for the same data file, one can trace each mirror to get a good idea of which mirror would be the fastest to use.

Two trace routes between the same source and destination conducted some time apart may produce different results. This is due to the "meshed" nature of the interconnected networks that comprise the Internet and the Internet Protocols ability to select different pathways over which to send packets.

Command-line-based route tracing tools are usually embedded with the operating system of the end device.

Scenario

Packet Tracer. Поиск и устранение неполадок адресации IPv4 и IPv6


Cisco Networking Academy®

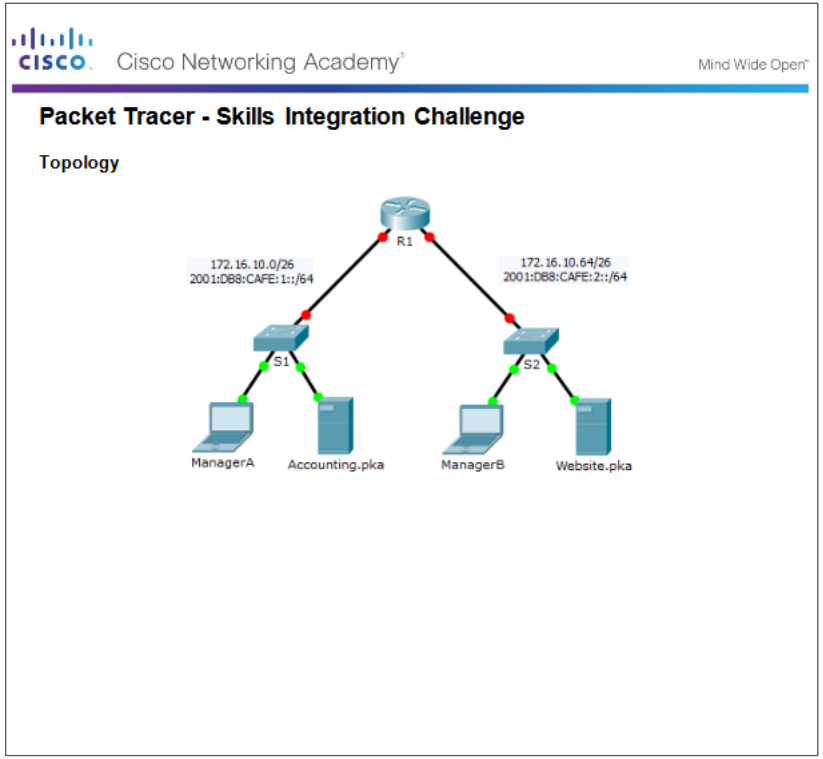
Mind Wide Open™

Packet Tracer - Troubleshooting IPv4 and IPv6 Addressing

Topology

7.4. Обзор главы

Packet Tracer. Отработка комплексных практических навыков



Глава 7. IP-адресация

- Объяснить использование адресов IPv4 для обеспечения подключений в сетях предприятий малого и среднего бизнеса.
- Выполнить настройку IPv6-адресов для обеспечения подключений в сети предприятий малого и среднего бизнеса
- Использовать типичные утилиты для проверки и тестирования сетевого подключения.

CISCO

Новые термины и команды

- октеты
- логическая операция И
- длина префикса
- представление с косой чертой
- сетевой адрес
- адрес узла
- широковещательный адрес
- направленная широковещательная рассылка
- ограниченная широковещательная рассылка
- группа многоадресной рассылки
- публичный адрес IPv4
- частные IPv4-адреса
- адрес типа link-local (IPv4)
- адреса TEST-NET
- классовая адресация
- Бесклассовый
- Администрация адресного пространства сети Интернет (IANA)
- Региональные интернет-регистраторы (RIR)
- двойной стек
- туннелирование
- преобразование сетевых адресов версии 64 (NAT64)
- предпочтительный глобальный индивидуальный адрес (GUA)
- адрес типа link-local (IPv6)
- уникальный локальный адрес
- глобальный префикс маршрутизации
- идентификатор подсети
- идентификатор интерфейса
- DHCPv6 без учета состояний
- DHCPv6 с учетом состояний
- расширенный уникальный идентификатор (EUI-64)
- присвоенный групповой адрес
- групповой адрес запрошенного узла
- сообщение «Запрос к маршрутизатору» (Router Solicitation, RS)
- объявление маршрутизатора (сообщение RA)
- сообщение о запросе соседних узлов (NS)
- объявление соседних узлов (NA)