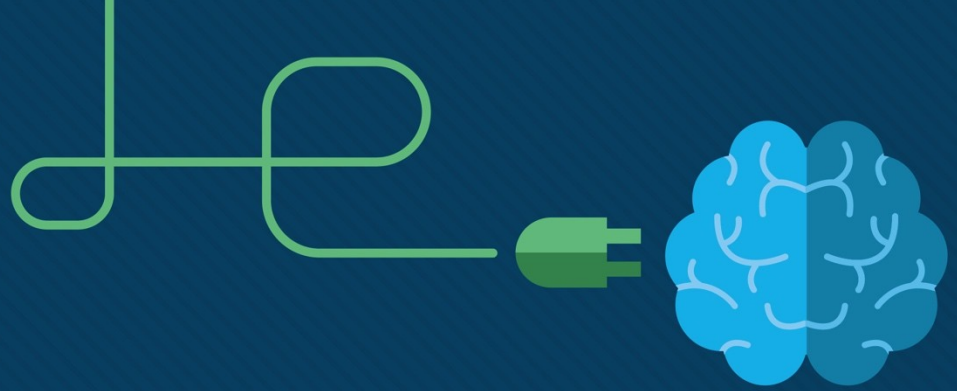


Модуль 13: ICMP

Введение в сетевые технологии v7.0 (ITN)

Задачи модуля

Название модуля: ICMP

Цель модуля: Выполнить проверку сетевых подключений с использованием различных инструментов.

Заголовок темы	Цель темы
Сообщения ICMP	Объяснить, как использовать протокол ICMP для проверки сетевых подключений.
Тестирование при помощи ping и traceroute	Выполнить проверку сетевых подключений при помощи ping и traceroute.

13.1 Сообщения ICMP

ICMPv4 и ICMPv6 сообщения

- Протокол ICMP обеспечивает обратную связь по вопросам, связанным с обработкой IP-пакетов при определенных условиях.
- ICMPv4 — это протокол обмена сообщениями для IPv4. ICMPv6 является протоколом обмена сообщениями для IPv6 и включает в себя дополнительные функции.
- Используются следующие ICMP-сообщения (одинаковые для ICMPv4 и ICMPv6).
  - Достижимость узла
  - Узел назначения или сервис недоступен
  - Превышен интервал ожидания

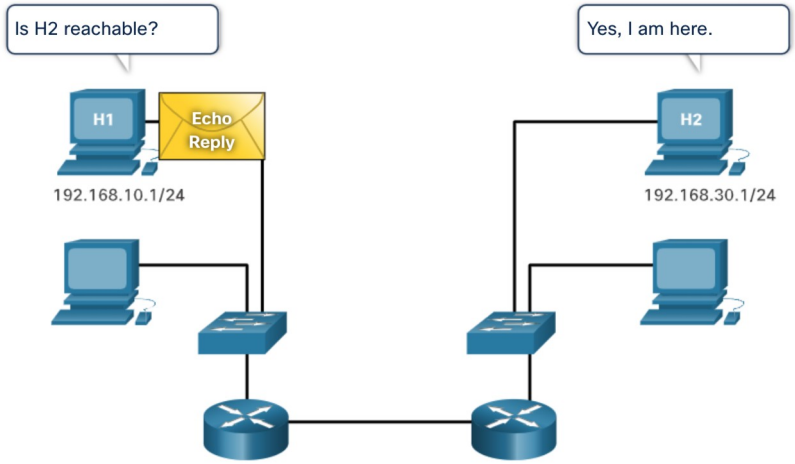
Из соображений безопасности сообщения ICMP не обязательны и часто даже не разрешены в сети.

Достижимость узла

Эхо-сообщение ICMP можно использовать для проверки доступности узла в IP-сети.

В примере:

- Локальный узел отправляет эхо-запрос ICMP.
- Если узел доступен, узел назначения отправляет эхо-ответ.



Назначение или служба недоступна

- Сообщение ICMP Destination Unreachable может использоваться для уведомления источника о недоступности места назначения или службы.
- Такое сообщение содержит код, определяющий причину, по которой пакет не может быть доставлен.

Примеры некоторых кодов сообщений о недоступном узле назначения для ICMPv4:

- 0 — сеть недоступна;
- 1 — узел недоступен;
- 2 — протокол недоступен;
- 3 — порт недоступен.

Ниже перечислены несколько кодов назначения недостижимых для ICMPv6:

- 0 - нет маршрута до пункта назначения
- 1 - Связь с пунктом назначения административно запрещена (например, брандмауэр)
- 2 — За пределами области адреса источника
- 3 - Адрес недоступен
- 4 — порт недоступен.

Примечание. Протокол ICMPv6 имеет практически такие же коды сообщений о недоступном узле назначения.

Время истекло

- Когда поле Time to Live (TTL) в пакете уменьшается до 0, в ICMPv4 будет отправлено сообщение ICMPv4 Time Exceeded.
- ICMPv6 также отправляет сообщение о превышении времени. В протоколе IPv6 поле TTL отсутствует; чтобы выяснить, не истек ли срок действия пакета, используется поле «предел переходов» (hop limit).

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Примечание. Сообщения о превышении времени используются инструментом traceroute.

ICMPv6 сообщения

ICMPv6 имеет новые функции и улучшенные функциональные возможности, отсутствующие в ICMPv4, включая 4 новых протокола в рамках протокола обнаружения соседей (ND или NDP).

Обмен сообщениями между маршрутизатором IPv6 и устройством IPv6, включая динамическое распределение адресов, осуществляется следующим образом:

- Сообщение «Запрос к маршрутизатору» (Router Solicitation, RS)
- Сообщение «Ответ маршрутизатора» (Router Advertisement, RA)

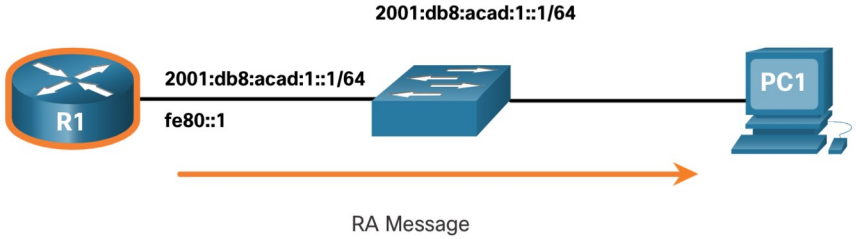
Обмен сообщениями между устройствами IPv6, включая обнаружение повторяющихся адресов и разрешение адресов, осуществляется следующим образом:

- Сообщение с запросом поиска соседей (NS)
- Сообщение об объявлении соседних узлов (NA)

Примечание. ND-протокол ICMPv6 также включает сообщение перенаправления, которое имеет аналогичную с сообщением перенаправления, используемым в ICMPv4, функцию.

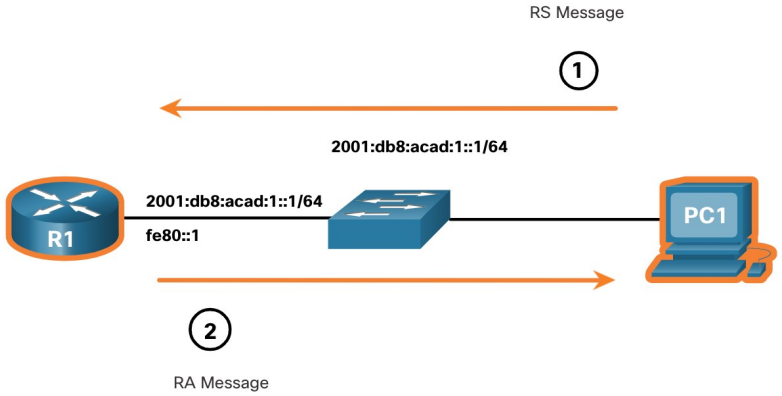
Сообщения ICMPv6 (продолжение)

- Сообщения RA отправляются маршрутизаторами с поддержкой IPv6 каждые 200 секунд для предоставления информации об адресации узлам с поддержкой IPv6.
- Сообщение RA может включать такие данные об адресах для хостов, как префикс, длина префикса, DNS-адрес и доменное имя.
- Узел, использующий SLAAC, установит в качестве своего шлюза по умолчанию локальный адрес канала маршрутизатора, отправившего RA.



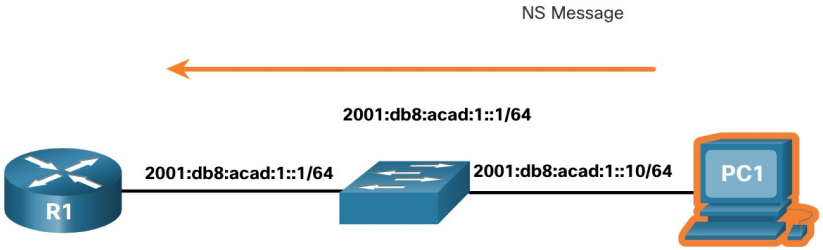
Сообщения ICMPv6 (продолжение)

- Маршрутизатор с поддержкой IPv6 также отправит сообщение RA в ответ на сообщение RS.
- На рисунке PC1 отправляет сообщение RS, чтобы определить, как получать информацию об адресах IPv6 динамически.
  - R1 отвечает PC с сообщением PA.
  - PC1 отправляет сообщение RS: «Привет, я только что загрузился. Есть ли IPv6 маршрутизатор в сети? Мне нужно знать, как динамически получать информацию об адресах IPv6».
  - R1 отвечает сообщением RA. "Привет всем устройствам с поддержкой IPv6. Я R1, и вы можете использовать SLAAC для создания глобального одноадресного адреса IPv6. Префикс: 2001:db8:acad:1::/64. Кстати, используйте мой локальный адрес связи fe80::1 в качестве шлюза по умолчанию"



Сообщения ICMPv6 (продолжение)

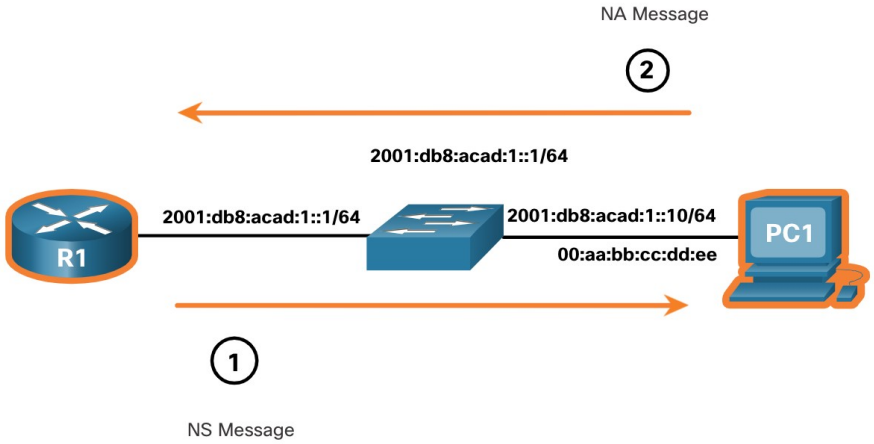
- Устройство, назначенное глобальный адрес одноадресной рассылки IPv6 или локальной одноадресной рассылки, может выполнять обнаружение дубликатов адресов (DAD), чтобы убедиться, что адрес IPv6 уникален.
- Для проверки уникальности адреса устройство отправляет сообщение NS с собственным IPv6-адресом в качестве целевого.
- Если другое устройство в сети имеет этот адрес, оно ответит сообщением NA, уведомляющим отправляющее устройство о том, что адрес используется.



Примечание. Процесс обнаружения дублирующихся адресов не обязателен, однако документ RFC 4861 рекомендует выполнять его для индивидуальных адресов.

Сообщения ICMPv6 (продолжение)

- Для того чтобы определить MAC-адрес назначения, устройство отправляет сообщение NS на адрес запрашиваемого узла.
- Сообщение включает известный (целевой) IPv6-адрес. Устройство с целевым IPv6-адресом отправляет в ответ сообщение NA, содержащее его MAC-адрес Ethernet.
- На рисунке R1 отправляет сообщение NS в 2001:db8:acad:1::10 с запросом его MAC-адреса.



13.2 Тестирование при помощи ping и traceroute

Ping — Тест подключения

- Команда **ping** — это утилита тестирования IPv4 и IPv6, которая использует сообщения эхо-запроса ICMP и эхо-ответа для проверки подключения между узлами и предоставляет сводную информацию, включающую в себя степень успеха и среднее время поездки туда и обратно до места назначения.
- Если в течение этого интервала ответ не получен, команда ping выдает сообщение об отсутствии ответа.
- Обычно для первого эхо-запроса требуется выполнить разрешение адреса (ARP или ND) перед отправкой эхо-запроса ICMP.

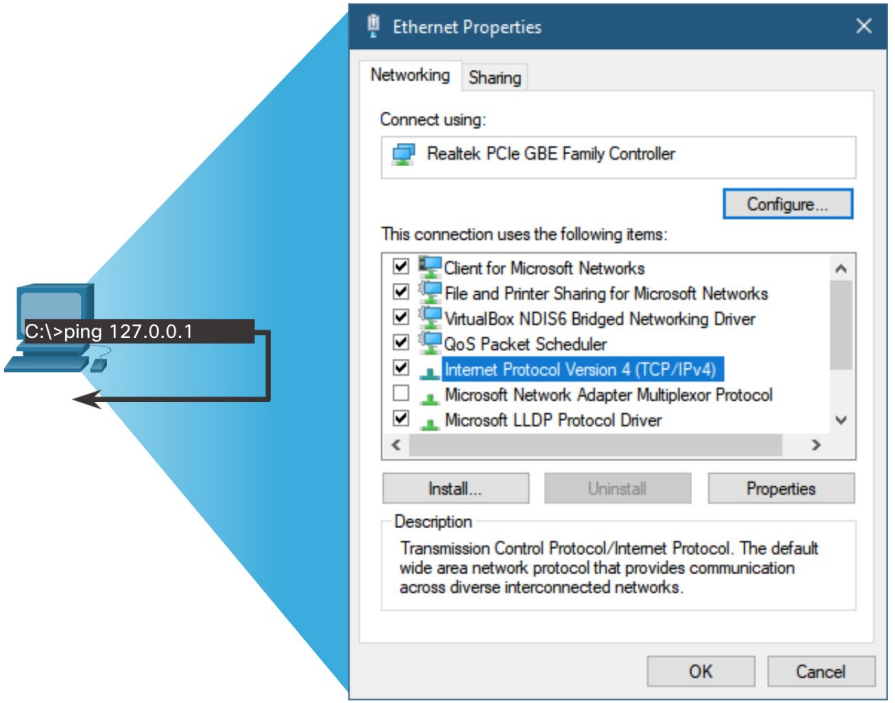
```
S1#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

```
R1#ping 2001:db8:acad:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Ping интерфейса loopback

Ping может использоваться для проверки внутренней конфигурации IPv4 или IPv6 на локальном хосте. Для выполнения этой проверки отправим **ping** на адрес loopback 127.0.0.1 для IPv4 (::1 для IPv6).

- Ответ от адреса 127.0.0.1 для IPv4 или :: 1 для IPv6 означает, что IP-сеть настроена на хосте правильно.
- Если мы получаем сообщение об ошибке, это означает, что протокол TCP/IP не работает на данном хосте.

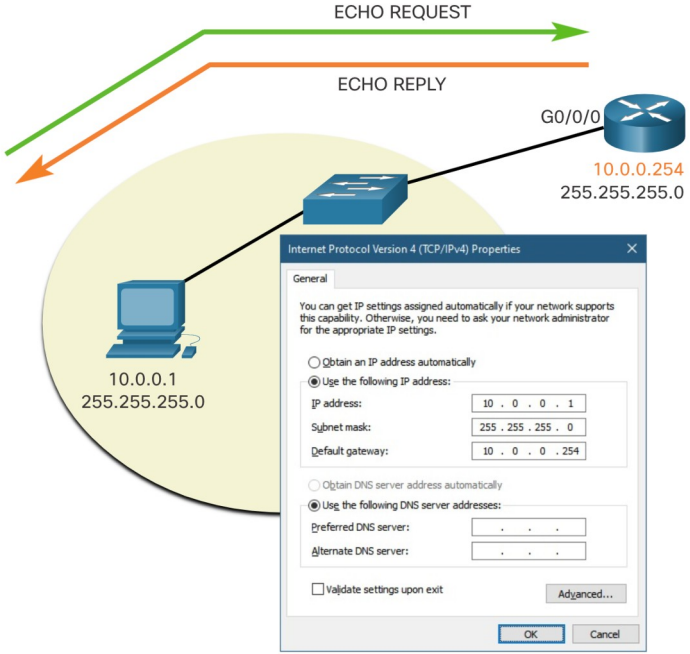


Ping шлюза по умолчанию

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

Для этой проверки чаще всего используется адрес шлюза, поскольку маршрутизатор практически всегда находится в рабочем состоянии.

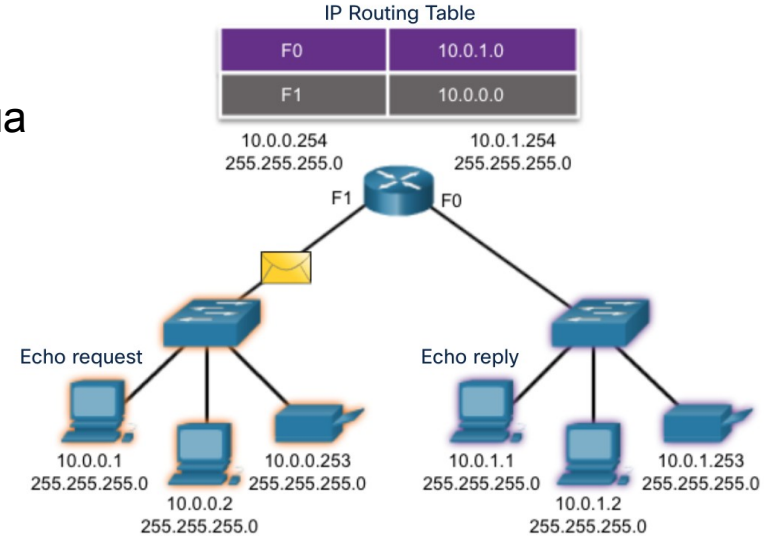
- Успешная отправка **ping** на шлюз позволяет убедиться, что хост и интерфейс маршрутизатора, выступающий в роли шлюза, нормально функционируют в данной локальной сети.
- Если адрес шлюза не отвечает, **ping** может быть отправлен на IP-адрес другого, заведомо рабочего хоста локальной сети.



Ping на удаленный узел

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

Локальный узел может выполнить эхо-запрос узла в удаленной сети. Успешное выполнение **ping-запроса** в объединенной сети подтверждает возможность обмена данными в локальной сети.



Примечание. Многие сетевые администраторы ограничивают или запрещают ввод ICMP-сообщений в корпоративную сеть; в связи с этим меры по обеспечению безопасности могут стать причиной отсутствия эхо-ответа.

Команда traceroute. Тестирование пути

- Команда **traceroute (tracert)** — это утилита, позволяющая составить список переходов, по которым успешно проходит эхо-запрос на пути к узлу назначения.

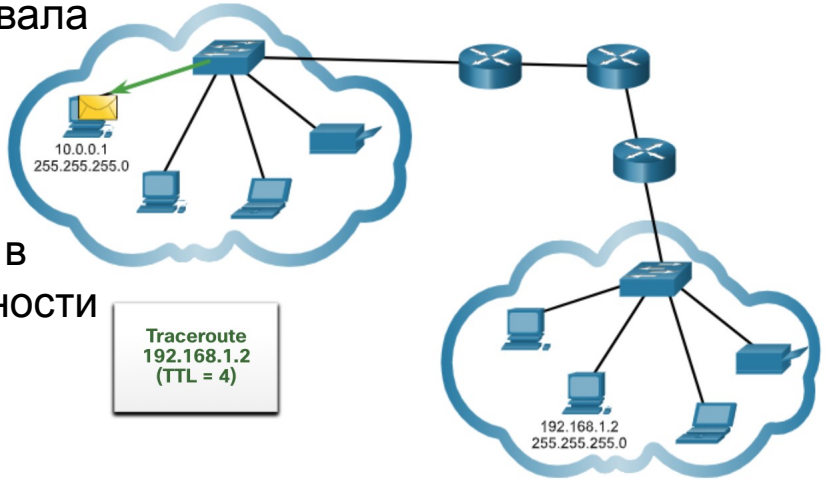
```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

  1   192.168.10.2    1 msec    0 msec    0 msec
  2   192.168.20.2    2 msec    1 msec    0 msec
  3   192.168.30.2    1 msec    0 msec    0 msec
  4   192.168.40.2    0 msec    0 msec    0 msec
```

- Утилита traceroute определяет суммарное время прохождения сигнала в прямом и обратном направлениях (RTT) для каждого перехода и сообщает о возможном отсутствии ответа на одном из переходов. Символ звездочки (*) используется для обозначения потерянного пакета или отсутствия ответа на пакет.
- Эта информация может использоваться для поиска проблемного маршрутизатора в пути или может указывать на то, что маршрутизатор настроен не отвечать на запросы.

Утилита traceroute использует значение в поле TTL в IPv4 и в поле предела переходов (Hop Limit) в IPv6 в заголовках 3-го уровня (вместе с сообщением ICMP о превышении интервала ожидания).

Команда traceroute. Тестирование пути

- Первая последовательность сообщений, отправленных командой traceroute, в поле TTL будет иметь значение 1. Данное значение TTL вызывает превышение интервала ожидания ответа на IPv4-пакет на первом маршрутизаторе. Затем маршрутизатор отвечает сообщением ICMPv4 Time Exceeded.
- Затем traceroute постепенно увеличивает значение в поле TTL (2, 3, 4 и т. д.) для каждой последовательности сообщений. Таким образом трассируются адреса каждого перехода, по мере того как превышение интервала ожидания ответа происходит дальше на маршруте.
- Значение в поле TTL продолжает увеличиваться до тех пор, пока не будет достигнут узел назначения, или до заранее установленного максимального уровня.



Packet Tracer - Ping и Traceroute — проверка адресации IPv4 и IPv6

В этом задании Packet Tracer вы будете делать следующее:

- Заполнение таблицы адресации
- Проверка подключения с помощью команды ping
- Определение пути путем отслеживания маршрута

Packet Tracer — использование Ping и Traceroute для проверки сетевого подключения

В этом задании Packet Tracer вы будете делать следующее:

- Проверка и восстановление IPv4-подключения
- Проверка и восстановление IPv6-подключения

13.3 Практика и контрольная работа модуля

Packet Tracer — использование ICMP для проверки и исправления сетевого подключения

В этом задании Packet Tracer вы будете делать следующее:

- Используйте ICMP для поиска проблем с подключением.
- Настройте сетевые устройства для устранения проблем с подключением.

Лабораторная работа — использование ICMP для проверки и исправления сетевого подключения

В этой лабораторной работе вы выполните следующие задачи:

- Создание и настройка сети
- Базовая проверка сети с помощью команды ping
- Базовая проверка сети с помощью команд tracert и traceroute
- Поиск и устранение проблем в топологии

Что я изучил в этом модуле?

- Назначение ICMP сообщений — предоставлять обратную связь о проблемах, связанных с обработкой IP-пакетов в определенных условиях, а не повышать надежность протокола IP.
- ICMP сообщения, общие для ICMPv4 и ICMPv6, являются: сообщения доступности узла, сообщение недостижимости хоста или службы, а также сообщение об истечении времени.
- Сообщения между маршрутизатором IPv6 и устройством IPv6, включая динамическое распределение адресов, включают RS и RA. Сообщения между устройствами IPv6 включают перенаправление (аналогично IPv4), NS и NA.
- Ping (используется IPv4 и IPv6) использует эхо-запрос ICMP и эхо-сообщения для проверки соединения между хостами.
- Ping может использоваться для проверки внутренней конфигурации IPv4 или IPv6 на локальном хосте.
- Команда traceroute (tracert) — это утилита, позволяющая составить список переходов, по которым успешно проходит эхо-запрос на пути к узлу назначения.


CISCO