Packet Tracer - Использование Ping и Traceroute для проверки сетевого подключения - Режим симуляции физического оборудования

Топология

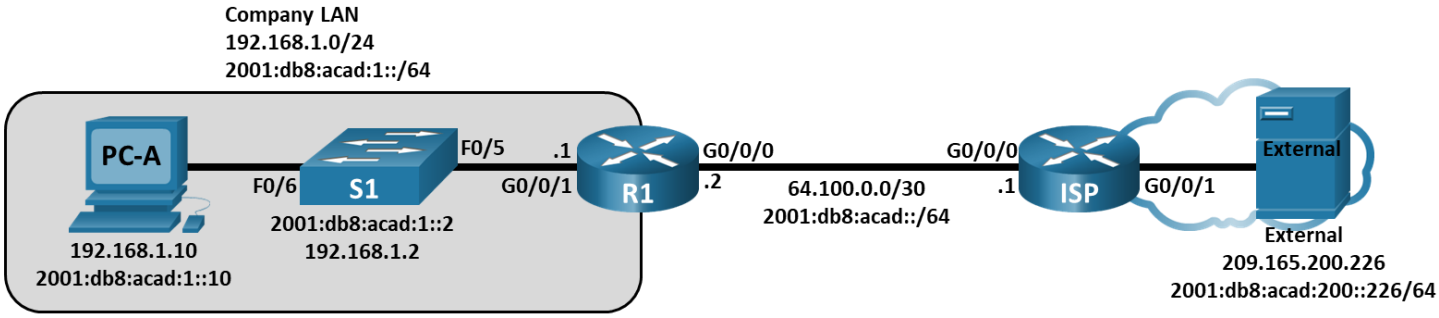

Таблица адресации

Устройство	Интерфейс	IP адрес/префикс	Шлюз по умолчанию
R1	G0/0/0	64.100.0.2 /30	—
		2001:db8:acad::2 /64	
		fe80::2	
	G0/0/1	192.168.1.1 /24	
		2001:db8:acad:1::1 /64	
		fe80::1	
ISP	G0/0/0	64.100.0.1 /30	—
		2001:db8:acad::1 /64	
		fe80::1	
	G0/0/1	209.165.200.225 /27	
		2001:db8:acad:200::225 /64	
		fe80::225	
S1	VLAN 1	192.168.1.2 /24	192.168.1.1
		2001:db8:acad:1:: 2 /64	fe80::1
		fe80::2	
PC-A	NIC	2001:db8:acad:1::10 /64	fe80::1

Устройство	Интерфейс	IP адрес/префикс	Шлюз по умолчанию
		192.168.1.10 /24	192.168.1.1
External	NIC	209.165.200.226 /27	209.165.200.225
		2001:db8:acad:200::226 /64	fe80::225

Цели

Часть 1. Базовая проверка сети с помощью команды ping

Часть 2. Базовая проверка сети с помощью команд tracert и traceroute

Часть 3. Поиск и устранение проблем в топологии

Общие сведения и сценарий

Ping и tracerout — это две незаменимые команды для проверки TCP/IP-соединения. Ping — это утилита сетевого администрирования, которая используется для проверки доступности устройства в IP-сети. Кроме того, она определяет суммарное время прохождения сигнала для сообщений, отправленных с узла источника на компьютер назначения.

Утилита traceroute - это инструмент сетевой диагностики для отображения пути или маршрута пакета, а также для измерения задержек передачи пакетов, проходящих по IP-сети.

В этой лабораторной работе в режиме симуляции физического оборудования рассматриваются команды **ping** и **traceroute** и изучаются параметры командной строки, влияющие на ход выполнения команд. Для изучения команд в лабораторной работе используются компьютеры и устройства Cisco. Доступные параметры команд **ping** и **tracert** ограничены в Packet Tracer В лабораторной работе даются необходимые конфигурации для устройств Cisco.

Инструкции

Part 1: Базовая проверка сети с помощью команды ping

В этой части лабораторной работы вы будете проверять сквозное соединение с помощью команды **ping**. Утилита ping отправляет на целевой узел пакеты с эхо-запросом протокола управления сообщениями в сети Интернет (Internet Control Message Protocol, ICMP) и ждет ответа ICMP. Утилита фиксирует как суммарное время прохождения сигнала в прямом и обратном направлениях, так и потерю пакета.

IP-пакеты имеют ограниченный срок службы в сети. Пакеты IPv4 используют 8-битное время жизни (TTL). Пакеты IPv6 используют значение поля заголовка Hop Limit. TTL и Hop Limit определяют максимальное количество переходов уровня 3, которые могут быть пройдены на пути к месту назначения. Узлы в сети будут устанавливать собственное 8-битное значение с максимальным значением 255.

Таким образом, каждый раз, когда IP-пакет поступает на сетевое устройство третьего уровня, это значение уменьшается на единицу, прежде чем он будет перенаправлен к месту назначения. Поэтому, если это значение в конечном итоге достигнет нуля, IP-пакет отбрасывается.

Вы проанализируете результаты выполнения команды **ping** и другие параметры утилиты, доступные на ПК в Packet Tracer и устройствах Cisco.

Step 1: Проверьте сетевые подключения из сети R1, используя компьютер PC-A.

Все эхо-запросы с **PC-A** на другие устройства в топологии должны быть успешными. Если это не так, проверьте топологию и кабельные соединения, а также настройки устройств Cisco и ПК.

a. Отправьте эхо-запрос с **PC-A** на шлюз по умолчанию, используя адрес IPv4 (интерфейс R1 GigabitEthernet 0/0/1).

```
C:\> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0 % loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

В этом примере были отправлены четыре запроса ICMP по 32 байта каждый. Ответы были получены менее чем за одну миллисекунду без потери пакетов. Время передачи запросов и получения ответов растет по мере увеличения количества устройств, обрабатывающих запросы и ответы ICMP в процессе их передачи на узел назначения и обратно.

Это также можно сделать с помощью IPv6-адреса шлюза по умолчанию (интерфейс GigabitEthernet 0/0/1 R1).

```
C:\> ping 2001:db8:acad:1::1

Pinging 2001:db8:acad:1::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0 % loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

b. Отправьте с компьютера **PC-A** эхо-запросы с помощью команды ping на адреса, указанные в следующей таблице, и запишите среднее время прохождения сигнала в прямом и обратном направлениях и время его существования (Time to Live, TTL).

Назначение	Среднее время прохождения сигнала в прямом и обратном направлениях (мс)	TTL/Hop Limit
192.168.1.10		
2001:db8:acad:1::10		

Назначение	Среднее время прохождения сигнала в прямом и обратном направлениях (мс)	TTL/Hop Limit
192.168.1.1 (**R1**)		
2001:db8:acad:1::1 (**R1**)		
192.168.1.2 (**S1**)		
2001:db8:acad:1::2(**S1**)		
64.100.0.2 (**R1**)		
2001:db8:acad::2 (**R1**)		
64.100.0.1 (**ISP**)		
2001:db8:acad::1 (**ISP**)		
209.165.200.225 (**ISP** G0/0/1)		
2001:db8:acad:200::225 (**ISP** G0/0/1)		
209.165.200.226 (**External**)		
2001:db8:acad:200::226 (**External**)		

Step 2: Выполните эхо-запрос от S1 до External.

От **S1**попытайтесь выполнить эхо-запрос до **ISP** и **External**. с помощью адресов IPv4 и IPv6.

Каковы результаты эхо-запросов от S1 до ISP и External?

ISPISPExternal

Part 2: Использование команды tracert и traceroute для базовой проверки сети

Команды для отслеживания маршрутов доступны на компьютерах и сетевых устройствах. На компьютере под управлением ОС Windows команда **tracert** отслеживает путь к узлу назначения, используя сообщения ICMP. Команда **traceroute** отслеживает маршруты к узлам назначения на устройствах Cisco и компьютерах под управлением Unix-подобных операционных систем, используя датаграммы UDP (User Datagram Protocol).

В этой части вы изучите команды traceroute и выполните трассировку пути, который проходит пакет до узла назначения. Вы будете использовать команду **tracert** на ПК Windows и команду **traceroute** на устройствах Cisco. Вы также познакомитесь с параметрами точной настройки этих команд.

Step 1: На PC-A используйте команду tracert до External.

a. Введите команду **tracert 209.165.200.226** в командной строке **PC-A**.

```
C:\> tracert 209.165.200.226

Tracing route to 209.165.200.226 over a maximum of 30 hops:

  1 * * 1 ms 192.168.1.1
  2 * 0 ms 0 ms 64.100.0.1
  3 0 ms * 0 ms 64.100.0.1
  4 * 11 ms * Request timed out.
```



```
  5 0 ms * 0 ms 64.100.0.1
Control-C
^C
C:\ >
```

Примечание.Вы можете остановить трассировку, нажав **Ctrl-C**.

Результаты **Tracert**показывают, что путь от PC-A к External таков, от PC-A к маршрутизатору R1, а от него к провайдеру и не может достичь External. Результаты **tracert** указывают на проблему на маршрутизаторе поставщика услуг Интернета.

b. Повторите команду tracert, используя адрес IPv6. В командной строке введите **tracert 2001:db8:acad:200::226**.

Step 2: Запустите команду traceroute с коммутатора S1 на External.

На коммутаторе S1 введите **traceroute 209.165.200.226** или **traceroute 2001:db8:acad:200::226**.

Примечание.Чтобы остановить **traceroute**, нажмите клавишу **Ctrl-Shift-6**.

```
S1# traceroute 209.165.200.226
S1# traceroute 2001:db8:acad:200::226
```

Команда **traceroute** имеет дополнительные параметры. Чтобы их посмотреть, после ввода команды **traceroute** в командной строке введите знак вопроса **?** или просто нажмите клавишу **ввода**.

Примечание. Доступные опции ограничены в Packet Tracer.

Дополнительную информацию о командах **ping** и **traceroute** для устройств Cisco можно найти на странице

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml

Part 3: Исправьте проблему с сетевым подключением у ISP.

Step 1: Доступ к сетевому расположению, в котором возникает проблема с подключением.

На основе предыдущих шагов вы определили, что существует проблема на маршрутизаторе **ISP** с помощью команд **ping** и **traceroute**. У вас есть удаленный SSH доступ ко всем сетевым устройствам, используя имя пользователя **admin** и пароль **class**.

a. Из терминала коммутатора **S1** выполниет SSH до маршрутизатора **ISP**, используя интерфейс G0/0/0 для устранения проблемы.

```
C:\> ssh -l admin 64.100.0.1
```

b. Проверьте текущую конфигурацию маршрутизатора **ISP** с помощью команды **show**.

Результаты команд **show run** и **show ip interface brief** показывают, что интерфейс GigabitEthernet 0/1 работает нормально, но IP-адрес в нем указан неправильно.

c. Исправьте найденные проблемы. Из командной строки на **PC-A**скопируйте и вставьте следующую конфигурацию в маршрутизатор **ISP**, чтобы устранить проблему в сеансе SSH на маршрутизаторе **ISP** .

```
configure terminal
interface g0/0/1
 no ip address 192.168.8.1 255.255.255.0
 ip address 209.165.200.225 255.255.255.224
 no ipv6 address 2001:db8:acad:201::225/64
 ipv6 address 2001:db8:acad:200::225/64
```



```
 ipv6 address fe80::225 link-local
no shutdown
```

d. Закройте сеанс SSH по завершении.

Step 2: Проверьте наличие сквозного подключения.

В командной строке **PC-A** используйте команды **ping** и **tracert** для проверки сквозного подключения к внешнему серверу в 209.165.200.226 и 2001:db8:acad:200:: 226.

Part 4: Использование расширенной команды Ping

Step 1: Отправьте расширенные эхо-запросы с PC-A.

Стандартная команда **ping** отправляет 4 запроса по 32 байта каждый. Ответ на каждый запрос ожидается в течение 4 000 мс (4 с), после чего отображается сообщение Request timed out (Превышен интервал ожидания для запроса). Для устранения неполадок сети параметры команды **ping** можно настроить более точно.

a. Введите **ping** в командной строке и нажмите клавишу **ввода**.

```
C:\> ping
```

b. С помощью параметра **–t** попробуйте установить соединение с PC-C, чтобы убедиться, что PC-C доступен. Параметр **-t** будет непрерывно отпралять эхо-эхо-запрос на цель пока вы сами не остановите исполнение этой команды. Используйте сочетание клавиш **Ctrl + C**, чтобы остановить эхо-запрос.

```
C:\> ping 209.165.200.226
```

c. Чтобы увидеть, какие результаты будут в случае недоступности узла, отсоедините кабель, соединяющий маршрутизатор ISP и коммутатор S3, или отключите интерфейс GigabitEthernet 0/1 на маршрутизаторе **ISP**. От коммутатора **S1**, SSH до интерфейса **ISP** G0/0/0. Используйте пароль **class**.

```
S1# ssh -l admin 64.100.0.1
```

d. Используйте команду **shutdown**, чтобы отключить интерфейс GigabiteThernet 0/0/1 на маршрутизаторе **ISP**.

При нормальной работе сети с помощью команды **ping** можно определить, ответил ли узел назначения и через какое время. В случае проблем с сетевым подключением команда **ping** выдает сообщение об ошибке.

e. Прежде чем перейти к следующему шагу, снова подключите кабель Ethernet или активируйте интерфейс GigabitEthernet на маршрутизаторе **ISP** (с помощью команды **no shutdown**). Примерно через 30 секунд команда ping должна быть выполнена успешно.

f. Чтобы остановить выполнение команды **ping**, нажмите **Ctrl+C**.

g. Вышеуказанные шаги могут быть повторены для IPv6 адрес для получения сообщения об ошибке ICMP.

Какие сообщения об ошибках вы получили?

h. Прежде чем перейти к следующему шагу, снова подключите кабель Ethernet или активируйте интерфейс GigabitEthernet0/0/1 на маршрутизаторе **ISP** (с помощью команды **no shutdown**). Примерно через 30 секунд команда ping должна быть выполнена успешно.

Step 2: Проверьте сетевые подключения из сети R1, используя устройства Cisco.

Команду **ping** можно использовать и на устройствах Cisco. В этом шаге вы изучите, как выполнять команду **ping** на маршрутизаторе **R1** и коммутатора **S1**.

a. От **R1** запустите эхо-запрос до **External**во внешней сети используя IP вдрес 209.165.200.226.

```
R1# ping 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Восклицательный знак (**!**) указывает, что эхо-запрос был успешным от маршрутизатора **R1** до **External**. Поездка туда и обратно занимает в среднем 1 мс без потери пакетов, о чем свидетельствует 100% коэффициент успеха.

b. Поскольку на маршрутизаторе **R1** настроена таблица локальных узлов, можно отправить эхо-запрос на **Externalv4** во внешней, используя имя узла для маршрутизатора **R1**.

```
R1# ping Externalv4
```

Какой IP-адрес используется?

c. В привилегированном режиме EXEC для команды **ping** доступны дополнительные параметры. Введите **ping** в командной строке и нажмите клавишу **ввода**. Используйте **ipv6** в качестве протокола. Введите **2001:DB8:ACAD:200: :226** или **external** как IPv6-адрес назначения. Нажмите клавишу **ввода**, чтобы принять значение по умолчанию для других параметров.

```
R1# ping
Protocol [ip]: ipv6
Target IPv6 address: 2001:db8:acad:200::226
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:200::226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

d. Если в сети возникают проблемы, можно отправить расширенный эхо-запрос. Отправьте команду **ping** на адрес 209.165.200.226 с числом повторов 50000. Затем выключите интерфейс GigabitEthernet 0/0/1 на маршрутизаторе **ISP**.

Из сеанса SSH к **ISP** на коммутаторе **S1** отключите интерфейс GigabitEthernet 0/0/1 на **ISP**.

e. В сеансе SSH включите интерфейс GigabitEthernet 0/0/1 на **ISP** после замены восклицательных знаков (**!**) Буквой **U** и точками (**.**). Примерно через 30 секунд команда ping должна быть выполнена успешно. Чтобы остановить выполнение команды **ping**, нажмите **Ctrl+Shift+6**.

```
R1# ping
Protocol [ip]:
Target IP address: 209.165.200.226
Repeat count [5]: 50000
Datagram size [100]:
```



```
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Sending 500, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
UU...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 99 percent (9970/10000), round-trip min/avg/max = 1/1/10 ms
```

Буква **U** в результатах означает, что узел назначения недостижим. **R1**получил сообщение об сообщение ошибке . Каждая точка (**.**) В выходных данных указывает, что время ожидания ответа от **External** истекло. В этом примере 1% пакетов были потеряны во время имитируемого отключения сети.

Команда **ping** очень полезна для устранения неполадок сетевого подключения. Тем не менее, если команду **ping** выполнить нельзя, то определить место возникновения сбоя с **ee** помощью невозможно. Отобразить информацию о маршруте и задержках в сети позволяет команда **tracert** (или **traceroute**).

f. В окне задания PT нажмите **Check Results**, чтобы проверить правильность всех элементов оценки и тестов подключения.

Вопросы для повторения

1. По какой причине, кроме проблем с сетевым соединением, ответ на команды **ping** и **traceroute** может не доходить на исходное устройство?
2. Какое сообщение выдаст команда **ping**, если отправить эхо-запрос с помощью команды **ping** на несуществующий адрес в удаленной сети, например 209.165.200.227? Что это означает? Если вы отправите **эхо-запрос** на действительный узел и получите такой ответ, что нужно будет проверить?
3. .Какое сообщение выдаст команда **ping**, если с компьютера под управлением ОС Windows отправить эхо-запрос с помощью команды **ping** на адрес, который не существует ни в одной из сетей вашей топологии, например 192.168.5.3? Что означает данное сообщение?

