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

Топология

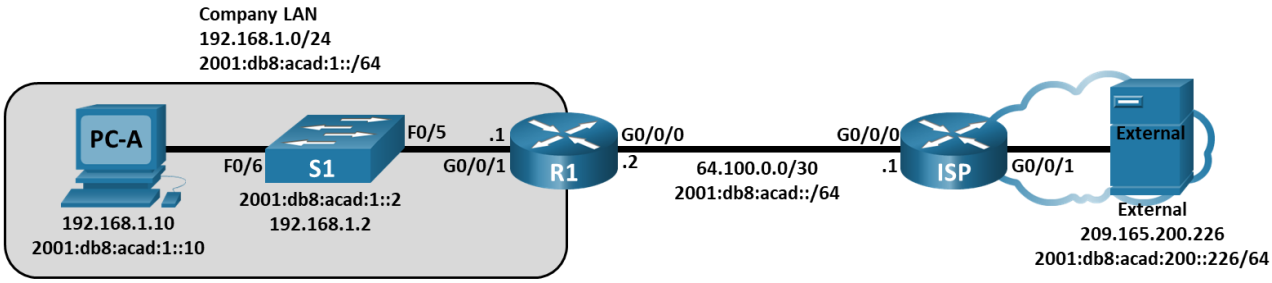


Таблица адресации

Устройство	Интерфейс	IP адрес/префикс	Шлюз по умолчанию
R1	G0/0/0	64.100.0.2 /30	—
		2001:db8:acad::2 /64	
		fe80::2	
R1	G0/0/1	192.168.1.1 /24	—
		2001:db8:acad:1::1 /64	
		fe80::1	
ISP	G0/0	64.100.0.1 /30	—
		2001:db8:acad::1 /64	
		fe80::1	
ISP	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
		2001db8:acad:1::2 /64	fe80::1
		fe80::10	
PC-A	NIC	2001:db8:acad:1::10 /64	fe80::1
		64.100.0.2 /30	Нет
Внешние	NIC	209.165.200.226 /27	209.165.200.225

Устройство	Интерфейс	IP адрес/префикс	Шлюз по умолчанию
		2001:DB8:ACAD:200::226 /64	FE80::225

Задачи

Часть 1. Создание и настройка сети

Часть 2. Базовая проверка сети с помощью команды ping

Часть 3. Базовая проверка сети с помощью команд tracert и traceroute

Часть 4. Поиск и устранение проблем в топологии

Общие сведения/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 ping доступна в ОС Windows, Unix-подобных ОС и операционной системе Cisco IOS.

Traceroute — это утилита сетевой диагностики, отображающая маршрут и измеряющая задержки при передаче пакетов в IP-сетях. Утилита tracert доступна в ОС Windows, а в Unix-подобных операционных системах (OS), а в операционной системе Cisco IOS используется ее аналог — утилита traceroute.

В этой лабораторной работе 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. В лабораторной работе даются необходимые конфигурации для устройств Cisco.

Примечание: Маршрутизаторы, используемые в практических лабораторных работах CCNA, - это Cisco 4221 с Cisco IOS XE Release 16.9.4 (образ universalk9). В лабораторных работах используются коммутаторы Cisco Catalyst 2960 с Cisco IOS версии 15.2(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание: Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

Шаблон **default bias**, по умолчанию используемый диспетчером базы данных коммутации Switch Database Manager (SDM), не предоставляет возможностей IPv6-адресации. Убедитесь, что SDM использует шаблон **dual-ipv4-and-ipv6** или **lanbase-routing**. Новый шаблон будет использоваться после перезагрузки даже в случае, если конфигурация не была сохранена.

```
S1# show sdm prefer
```

Чтобы назначить шаблон **dual-ipv4-and-ipv6** в качестве шаблона диспетчера базы данных коммутатора по умолчанию, используйте следующие команды:

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Необходимые ресурсы

- 2 маршрутизатора (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.4 или аналогичным)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.2(2) с образом lanbasek9 или аналогичная модель)
- 2 ПК (Windows и программа эмуляции терминала, такая как Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты.
- Кабели Ethernet и последовательные кабели согласно топологии.

Инструкции

Часть 1. Создание и настройка сети

В части 1 вы создадите сеть в топологии и настроите компьютеры и устройства Cisco. Для справки приводятся начальные конфигурации маршрутизаторов и коммутаторов. В этой топологии статическая маршрутизация используется для маршрутизации пакетов между сетями.

Шаг 1. Создайте сеть согласно топологии.

Шаг 2. Удалите настройки на маршрутизаторах и коммутаторах и перезагрузите устройства.

Шаг 3. Настройте IP-адреса и шлюзы по умолчанию для компьютеров в соответствии с таблицей адресации.

Шаг 4. Сконфигурируйте маршрутизаторы R1 и ISP и коммутатор S1, используя начальные конфигурации, представленные ниже.

Скопируйте и вставьте в окно командной строки режима общих настроек параметры конфигурации для каждого устройства. Сохраните конфигурацию в файл загрузочной конфигурации startup-config.

Начальная конфигурация для маршрутизатора R1:

```
hostname R1
no ip domain lookup
ipv6 unicast-routing
interface g0/0/0
 ip address 64.100.0.2 255.255.255.252
 IPv6 address  2001:db8:acad::2/64
 ipv6 address fe80::2 link-local
 ip nat outside
 no shutdown
interface g0/0/1
 ip add 192.168.1.1 255.255.255.0
 ipv6 address 2001:db8:acad:1::1/64
 ipv6 address fe80::1 link-local
 ip nat inside
 no shutdown
ip route 0.0.0.0 0.0.0.0 64.100.0.1
```

```
ipv6 route 0::/0 2001:db8:acad::1
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface g0/0/0 overload
```

Начальная конфигурация для маршрутизатора ISP:

```
hostname ISP
no ip domain lookup
ipv6 unicast-routing
interface g0/0/0
 ip address 64.100.0.1 255.255.255.252
 IPv6 address  2001:db8:acad::1/64
 ipv6 address fe80::1 link-local
 no shutdown
interface g0/0/1
 ip add 209.165.200.225 255.255.255.224
 ipv6 address 2001:db8:acad:200::225/64
 ipv6 address fe80::225 link-local
 no shutdown
ipv6 route ::/0 2001:db8:acad::2
```

Начальная конфигурация для коммутатора S1:

```
hostname S1
no ip domain-lookup
interface vlan 1
 ip add 192.168.1.2 255.255.255.0
 ipv6 address 2001:db8:acad:1::2/64
 ipv6 address fe80::2 link-local
 no shutdown
 exit
ip default-gateway 192.168.1.1
end
```

Шаг 5. Настройте таблицу IP-узлов на маршрутизаторе R1.

С помощью таблицы IP-узлов для подключения к удаленному устройству вместо IP-адреса можно использовать имя узла. В таблице узлов указано разрешение имен для устройства со следующими параметрами. Скопируйте и вставьте следующие конфигурации для маршрутизатора R1. Эти параметры позволят вводить команды **ping** и **traceroute** на маршрутизаторе R1, используя имена узлов.

```
ip host Externalv4 209.165.200.226
ip host Externalv6 2001:db8:acad:200::226
ip host ISPv4 64.100.0.1
ip host ISPv6 2001:db8:acad::1
ip host PC-Av4 192.168.1.10
ip host PC-Av6 2001:db8:acad:1::10
ip host R1v4 64.100.0.2
ip host R1v6 2001:db8:acad::2
```



```
ip host R1v6 2001:db8:acad::2
ip host R1v6 2001:db8:acad::2
end
```

Часть 2. Базовая проверка сети с помощью команды ping

В части 2 этой 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. IP-пакеты используют 8-битное значение поля заголовка Time to Live (IPv4) или Hop Limit (IPv6), которое определяет максимальное количество переходов уровня 3, которые могут быть пройдено по 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 с ОС Windows и устройствах Cisco.

Шаг 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 было отправлено 4 (четыре) ICMP-запроса по 32 байта каждый, ответы на которые 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: time=5ms
Reply from 2001:db8:acad:1::1: time=5ms
Reply from 2001:db8:acad:1::1: time=5ms
```

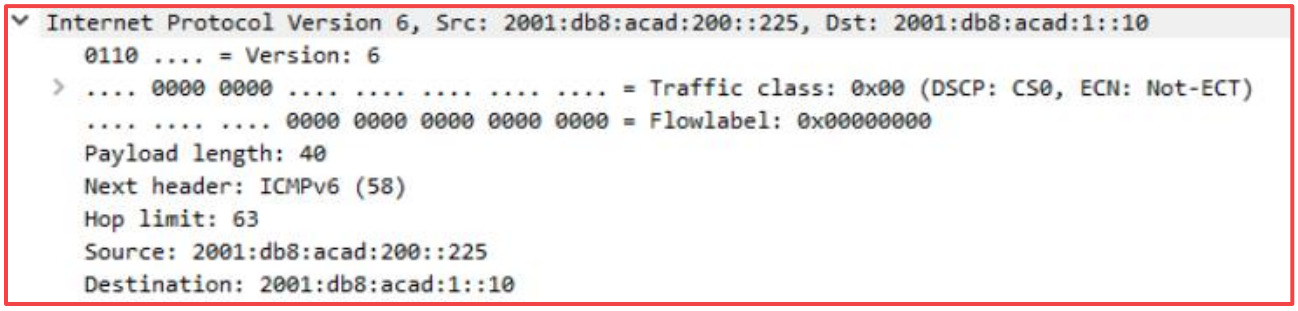


```
    from 2001:db8:acad:1::1: time=1ms

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 = 1ms, Maximum = 5ms, Average = 2ms
```

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). **Необязательно**: используйте WireShark, чтобы увидеть значение hop limit в IPv6.

Назначение	Среднее время прохождения сигнала в прямом и обратном направлениях (мс)	TTL/Hop Limit
192.168.1.10		
2001:db8:acad:1::10		
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 (Внешняя)		
2001:DB8:ACAD:200: :226 (внешний)		



Шаг 2. Отправьте расширенные эхо-запросы с ПК.

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.

```
C:\Users\User1>  ping –t 209.165.200.226
```

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.

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.

c. 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.

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

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

Какие сообщения об ошибках вы получили?

f. 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.

Шаг 3. 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. Ping External во внешней сети, используя IP-адрес 209.165.200.226 от маршрутизатора R1.

```
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 с маршрутизатора R1 на внешний. 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 PC-C в сети REMOTE, используя имя узла для маршрутизатора R1.

Примечание. Имя хоста не чувствительно к регистру. Вы можете заменить имя узла для IP-адреса, если это необходимо на R1 в этой лабораторной работе.

```
R1 # ping externalv4
```

Какой IP-адрес используется?

c. 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** для целевого адреса IPv6. Нажмите клавишу ввода, чтобы принять значение по умолчанию для других параметров.

```
R1# ping
Protocol [ip]: ipv6
Целевой адрес IPv6: 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 192.168.3.3 с числом повторов 50000. 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.

Когда вместо восклицательных знаков (!) появятся буква U и точки (.), снова подключите Ethernet-кабель или активируйте интерфейс GigabitEthernet на маршрутизаторе REMOTE. 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]: 10000
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. На маршрутизатор R1 поступила единица данных протокола (PDU) об ошибке. Каждый период (.) в выходных данных указывает, что время ожидания ответа от External истек. В этом примере 1% пакетов были потеряны во время имитируемого отключения сети.

Примечание. Такие же результаты позволит получить следующая команда:

```
R1# ping 209.165.200.226 repeat 10000
```

или

```
R1# ping 2001:db8:acad:200::226 repeat 10000
```

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

Часть 3. Базовая проверка сети с помощью команд tracert и traceroute

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 части 3 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.

Шаг 1. Отправьте команду tracert с PC-A на EXTERNAL.

a. Введите команду **tracert 209.165.200.226** в командной строке.

```
C:\> tracert 209.165.200.226
```

Результаты трассировки показывают, что путь от PC-A до EXTERNAL - от PC-A до R1 до ISP до EXTERNAL. Путь к EXTERNAL прошел через два перехода маршрутизатора к конечному месту назначения EXTERNAL.

Шаг 2. Изучите дополнительные параметры команды tracert.

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

```
C:\> tracert
```

b. Используйте параметр **-d**. Обратите внимание, что IP-адрес 209.165.200.226 не разрешен как ВНЕШНИЙ.

```
C:\> tracert –d 209.165.200.226
```

Шаг 3. Отправьте команду traceroute с маршрутизатора R1 на PC-C.

В командной строке введите **traceroute 209.165.200.226** или **traceroute 2001:db8:acad:200::226** на маршрутизаторе R1. Имена узлов будут определены, поскольку на маршрутизаторе R1 настроена таблица локальных IP-узлов.

```
R1# traceroute 209.165.200.226
R1# traceroute 2001:db8:acad:200::226
```

Шаг 4. Отправьте команду traceroute с коммутатора S1 на External.

На коммутаторе S1 введите **traceroute 209.165.200.226** или **traceroute 2001:db8:acad:200::226** . Имена узлов не отображаются в результатах команды traceroute, поскольку на данном коммутаторе таблица локальных IP-узлов не настроена.

```
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.

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

Часть 4. Поиск и устранение проблем в топологии

Шаг 1. Скопируйте и вставьте следующие параметры для маршрутизатора ISP.

```
hostname ISP
interface g0/0/0
 ip address 64.100.0.1 255.255.255.252
 IPv6 address  2001:db8:acad::1/64
 no shutdown
interface g0/0/1
  ip address 192.168.8.1 255.255.255.0
 no ipv6 address 2001:db8:acad:200::225/64
 IPv6 адрес 2001:db8:acad:201::225/64
 no shutdown
end
```

Шаг 2. Из сети R1 отправьте команды ping и tracert или traceroute, чтобы найти и устранить проблемы в сети ISP.

a. Введите команды **ping** и **tracert** на PC-A.

   С помощью команды **tracert** можно проверить сквозное соединение в пределах сети. Результат выполнения команды tracert показывает, что эхо-запросы от PC-A достигают шлюза по умолчанию 192.168.1.1, но не достигают External.

   Один из способов найти сетевую проблему — это пинг для каждого прыжка в сети во EXTERNAL. Сначала определите, может ли PC-A достичь интерфейса маршрутизатора ISP g0/0/0 с IP-адресом 64.100.0.1.

b. Компьютер PC-A может связаться с маршрутизатором ISP. Судя по успешной отправке эхо-запроса с компьютера PC-A на маршрутизатор ISP, проблема с подключением связана с сетью 192.168.3.0/24. Отправьте эхо-запрос на шлюз по умолчанию External, в качестве которого выступает интерфейс GigabitEthernet 0/1 маршрутизатора ISP.

   Как видно из результатов выполнения команды **ping**, компьютер PC-A не может подключиться к интерфейсу GigabitEthernet 0/1 маршрутизатора ISP.

   Результаты tracert и ping показывают, что PC-A может подключаться к маршрутизаторам R1 и ISP, но не к шлюзу External или шлюзу по умолчанию для External.

c. 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.

d. Исправьте найденные проблемы.

e. Убедитесь, что компьютер PC-A может отправлять команды ping и tracert на PC-C.

Примечание. Для этого также можно отправить команды ping и traceroute из интерфейса командной строки на маршрутизатор ISP и коммутатор S1, предварительно убедившись в отсутствии проблем подключения в сети 192.168.1.0/24.

f. Теперь повторите процесс подключения IPv6. **Примечание**. Если вы обнаружите неверный адрес IPv6, его необходимо удалить, так как он не заменен новой командой ipv6 address.

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?
4. Что такое значение TTL IPv4, установленное на хосте Windows? Что такое значение TTL IPv4, установленное на устройстве Cisco?
5. Что такое ограничение IPv6 Hop Limit, установленное на хосте Windows? Что такое предельное значение IPv6 Hop Limit, установленное на устройстве Cisco?

Сводная таблица по интерфейсам маршрутизаторов

Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet № 2	Последовательный интерфейс № 1	Последовательный интерфейс № 2
1 800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.

