МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

Настройка расширенных ACL-списков

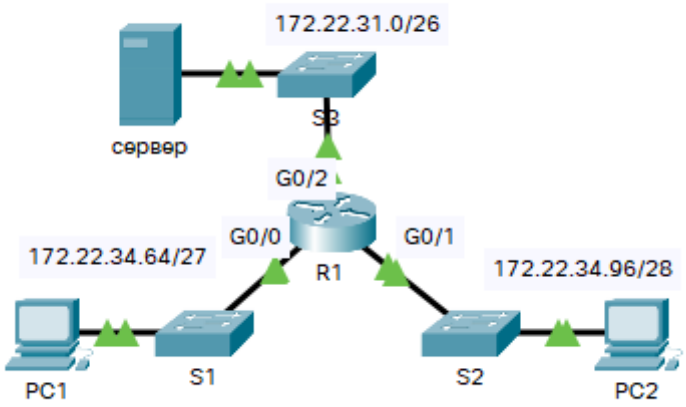
Отчет по лабораторной работе № 8
по дисциплине «Компьютерные сети»
студента 2 курса группы ИВТ-б-о-202(1)
Шор Константина Александровича

Направления подготовки 09.03.01«Информатика и вычислительная техника»

Симферополь, 2022

Сценарий_1

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	172.22.34.65	255.255.255.224	Недоступно
	G0/1	172.22.34.97	255.255.255.240	Недоступно
	G0/2	172.22.34.1	255.255.255.192	Недоступно
Сервер	Сетевой адаптер	172.22.34.62	255.255.255.192	172.22.34.1
PC1	Сетевой адаптер	172.22.34.66	255.255.255.224	172.22.34.65
PC2	Сетевой адаптер	172.22.34.98	255.255.255.240	172.22.34.97



Часть 1. Настройка, применение и проверка расширенного нумерованного ACL-списка

Шаг 1. Настройте ACL-список на разрешение FTP и ICMP.

a. В режиме глобальной конфигурации маршрутизатора **R1** введите следующую команду, чтобы определить первый допустимый номер для расширенного списка доступа.

b. Добавьте **100,** а затем поставьте вопросительный знак.

c. Чтобы разрешить FTP-трафик, введите **permit**, после которого поставьте вопросительный знак.

d. Данный ACL-список разрешает FTP и ICMP. ICMP включён в список, указанный выше, в отличие от FTP, который использует протокол TCP. Таким образом, необходимо ввести TCP. Введите **tcp**, чтобы дальше уточнить справку по ACL-спискам.

e. Обратите внимание, что мы можем настроить фильтрацию только для **PC1** с помощью ключевого слова **host**, а также можем разрешить доступ для любого узла с помощью ключевого слова **any**. В этом случае доступ разрешён любому устройству с адресом, принадлежащим сети 172.22.34.64/27. Введите сетевой адрес, а после него — знак вопроса.

f. Рассчитайте шаблонную маску, определяющую двоичную противоположность маски подсети.

g. Введите сетевой адрес, а после него — знак вопроса.

h. Настройте адрес узла-назначения. В этом сценарии мы фильтруем трафик в пользу только одного адресата — сервера. Введите ключевое слово **host**, а после него — IP-адрес сервера.

i. Обратите внимание, что одним из параметров является **<cr>** (возврат каретки). Другими словами, вы можете нажать клавишу **ВВОД**, и согласно правилу будет разрешён весь трафик TCP. Однако мы хотим разрешить только трафик FTP. Поэтому введите ключевое слово **eq**, после которого поставьте вопросительный знак, чтобы отобразить доступные параметры. Затем введите **ftp** и нажмите клавишу **ВВОД**.

j. Создайте второе правило списка доступа, разрешающее передачу трафика ICMP (эхо-запрос и др.) от **PC1** на сервер **Server**. Обратите внимание на то, что номер списка доступа остается неизменным, а конкретный тип трафика ICMP не требует определения.

k. Остальной трафик запрещён по умолчанию.

```
R1>ena
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
R1(config)#access-list 100?
<100-199>
R1(config)#access-list 100 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
R1(config)#access-list 100 permit ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
R1(config)#access-list 100 permit tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
R1(config)#access-list 100 permit tcp 172.22.34.64 ?
  A.B.C.D  Source wildcard bits
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
  A.B.C.D  Destination address
  any      Any destination host
  eq       Match only packets on a given port number
  gt       Match only packets with a greater port number
  host     A single destination host
  lt       Match only packets with a lower port number
  neq      Match only packets not on a given port number
  range    Match only packets in the range of port numbers
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?
  dscp         Match packets with given dscp value
  eq           Match only packets on a given port number
  established  established
  gt           Match only packets with a greater port number
  lt           Match only packets with a lower port number
  neq          Match only packets not on a given port number
  precedence   Match packets with given precedence value
  range        Match only packets in the range of port numbers
  <cr>
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?
  <0-65535>  Port number
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp ?
  dscp         Match packets with given dscp value
  established  established
  precedence   Match packets with given precedence value
  <cr>
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
R1(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
R1(config)#
```

Шаг 2. Примените ACL-список на соответствующему интерфейсе для фильтрации трафика.

С точки зрения маршрутизатора **R1**, трафик, к которому применяется список ACL 100, поступает от сети, подключённой к интерфейсу Gigabit Ethernet 0/0. Войдите в режим настройки интерфейса и примените ACL-список.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int
R1(config)#interface gig
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#
```

Шаг 3. Проверьте работу применённого ACL-списка.

a. Отправьте эхо-запрос от **PC1** на сервер **Server**. В случае неудачных эхо-запросов проверьте IP-адреса перед тем, как продолжить работу.

b. Выполните FTP-подключение от **PC1** к серверу **Server**. В качестве имени пользователя и пароля используется **cisco**.

```
PC> ftp 172.22.34.62
```

c. Выйдите из FTP-службы сервера **Server**.

```
ftp> quit
```

г. Отправьте эхо-запрос от **PC1** на **PC2**. Узел назначения должен быть недоступен, поскольку отсутствует явное разрешение трафика.

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>ping 172.22.34.98

Pinging 172.22.34.98 with 32 bytes of data:

Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.

Ping statistics for 172.22.34.98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Часть 2. Настройка, применение и проверка расширенного именованного ACL-списка

Шаг 1. Настройте ACL-список на разрешение FTP и ICMP.

a. Именованные ACL-списки начинаются с ключевого слова **ip**. В режиме глобальной конфигурации **R1** введите следующую команду, закончив её вопросительным знаком.

b. Можно настроить именованные стандартные и расширенные ACL-списки. Посредством этого списка доступа фильтруются как IP-адреса источника, так и IP-адреса узла-назначения; таким образом, список должен быть расширенным. Введите в качестве имени **HTTP_ONLY**. (Для получения большего количество баллов при работе в Packet Tracer необходимо задавать имя, чувствительное к регистру).

c. Командная строка изменится. Теперь активирован режим настройки именованного расширенного ACL-списка. Всем устройствам локальной сети **PC2** требуется TCP-доступ. Введите сетевой адрес со знаком вопроса в конце.

d. Другой способ расчёта шаблонной маски заключается в вычитании маски подсети из 255.255.255.255.

```
  255.255.255.255
- 255.255.255.240
-----------------
=   0.  0.  0. 15
```

e. Допишите правило, определив адрес сервера как в части 1, и настроив фильтрацию трафика **www**.

f. Создайте второе правило списка доступа, разрешающее передачу трафика ICMP (эхо-запрос и др.) от **PC2** на **Сервер**. Примечание. Командная строка не меняется, задавать конкретный тип трафика ICMP не нужно.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list ?
  extended  Extended Access List
  standard  Standard Access List
R1(config)#ip access-list extended HTTP_ONLY
R1(config-ext-nacl)#permit tcp 172.22.34.96 ?
  A.B.C.D  Source wildcard bits
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 ?
  A.B.C.D  Destination address
  any      Any destination host
  eq       Match only packets on a given port number
  gt       Match only packets with a greater port number
  host     A single destination host
  lt       Match only packets with a lower port number
  neq      Match only packets not on a given port number
  range    Match only packets in the range of port numbers
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 ?
  eq           Match only packets on a given port number
  established  established
  gt           Match only packets with a greater port number
  lt           Match only packets with a lower port number
  neq          Match only packets not on a given port number
  range        Match only packets in the range of port numbers
  <cr>
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq ?
  <0-65535>  Port number
  domain     Domain Name Service (DNS, 53)
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
R1(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
R1(config-ext-nacl)#
```

Шаг 2. Примените ACL-список на соответствующем интерфейсе для фильтрации трафика.

С точки зрения маршрутизатора **R1**, трафик, к которому применяется список **HTTP_ONLY**, поступает от сети, подключённой к интерфейсу Gigabit Ethernet 0/1. Войдите в режим настройки интерфейса и примените ACL-список.

```
R1(config)#int
R1(config)#interface gig
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#ip access
R1(config-if)#ip access-group HTTP_ONLY in
R1(config-if)#
```

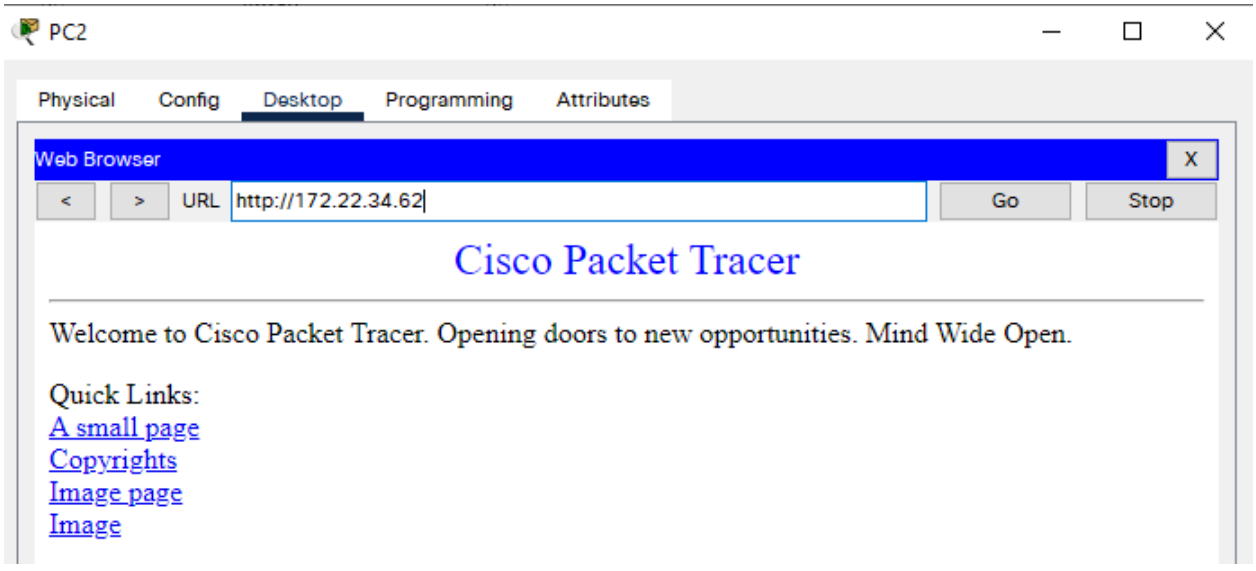
Шаг 3. Проверьте работу ACL-списка

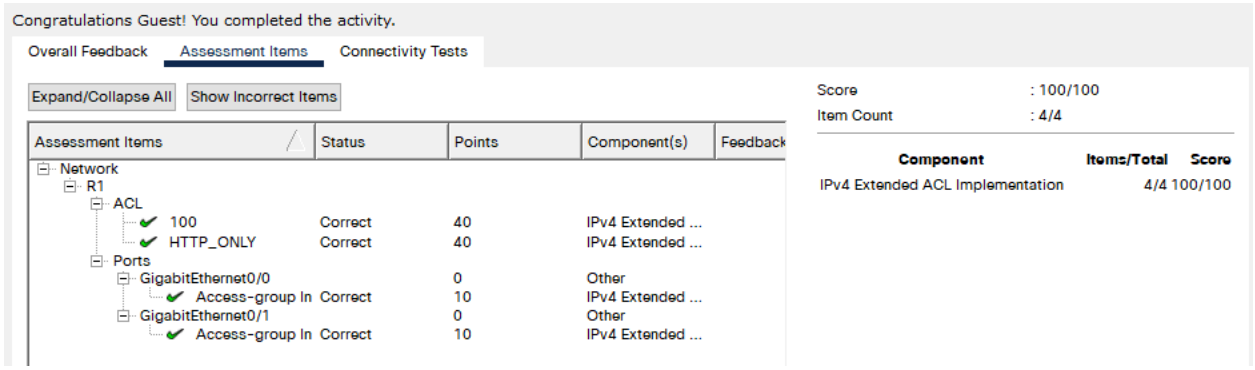
a. Отправьте эхо-запрос от **PC2** на сервер **Server**. В случае неудачных эхо-запросов проверьте IP-адреса перед тем, как продолжить работу.

b. Выполните FTP-подключение от **PC2** к серверу **Server**. Подключение не должно быть успешным.

c. Откройте веб-браузер на **PC2** и введите IP-адрес сервера **Server** в виде URL-адреса. Подключение должно быть успешным.

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62

%Error opening ftp://172.22.34.62/ (Timed out)
.



(Disconnecting from ftp server)
```

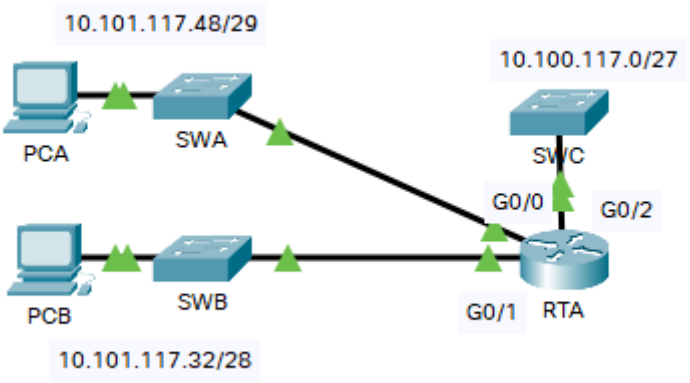



Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items
Assessment Items
Status
Points
Component(s)
Feedback
Network
R1
ACL
100
Correct
40
IPv4 Extended ...
HTTP_ONLY
Correct
40
IPv4 Extended ...
Ports
GigabitEthernet0/0
0
Other
Access-group In
Correct
10
IPv4 Extended ...
GigabitEthernet0/1
0
Other
Access-group In
Correct
10
IPv4 Extended ...
Score
: 100/100
Item Count
: 4/4
Component
Items/Total
Score
IPv4 Extended ACL Implementation
4/4
100/100

Сценарий_2

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
RTA	G0/0	10.101.117.49	255.255.255.248	Недоступно
	G0/1	10.101.117.33	255.255.255.240	Недоступно
	G0/2	10.101.117.1	255.255.255.224	Недоступно
PCA	Сетевой адаптер	10.101.117.51	255.255.255.248	10.101.117.49
PCB	Сетевой адаптер	10.101.117.35	255.255.255.240	10.101.117.33
SWC	VLAN1	10.101.117.2	255.255.255.224	10.101.117.1



Assessment Items	Status	Points	Component(s)	Feedback
Network				
RTA				
ACL		0	ACL	
199	Incorrect	60	IPv4 Extended ...	
Ports		0	Other	
GigabitEthernet0/2		0	Other	
Access-group Out	Incorrect	20	IPv4 Extended ...	

Перед выполнением лабы надо настроить коммутаторы, для этого задания на всех коммутаторах нужно прописать шлюз по умолчанию на интерфейс маршрутизатора

```
  ssh               Configure ssh options
SWC(config)#ip add
SWC(config)#ip addre
SWC(config)#ip address
SWC(config)#ip defa
SWC(config)#ip default-gateway ?
  A.B.C.D  IP address of default gateway
SWC(config)#ip default-gateway 10.101.117.1 ?
  <cr>
SWC(config)#ip default-gateway 10.101.117.1
SWC(config)#
```

SWA

```
!
ip default-gateway 10.101.117.49
!
```

SWB

```
!
ip default-gateway 10.101.117.33
!
```

Часть 1. Настройка, применение и проверка расширенного нумерованного ACL-списка

Настройте и примените ACL-список, а затем убедитесь, что он удовлетворяет следующим правилам безопасности:

- Трафик по протоколу Telnet в сети 10.101.117.32/28 разрешён для передачи на устройства в сетях 10.100.117.0/27.
- Трафик ICMP разрешён от любого устройства и в любом направлении.
- Весь остальной трафик запрещён.

Шаг 1. Настройте расширенный ACL-список.

a. Находясь в соответствующем режиме конфигурации на **RTA**, используйте последний допустимый номер расширенного списка доступа, чтобы настроить ACL-список. Используйте следующие операции для создания первой записи в ACL-списке:

1) Последним номером расширенного списка является 199.

2) Используемым протоколом является TCP.

3) Сетью-источником является 10.101.117.32.

4) Шаблонную маску можно определить путём вычитания 255.255.255.240 из 255.255.255.255.

5) Сетью назначения является 10.101.117.0.

6) Шаблонную маску можно определить путём вычитания 255.255.255.224 из 255.255.255.255.

7) Используемым протоколом является протокол Telnet.

Каково первое правило ACL-списка?

b. Трафик ICMP разрешён, требуется второе правило ACL-списка. Используйте список с одним и тем же номером для разрешения трафика ICPM, независимо от адреса источника или назначения. Какой будет второе правило ACL-списка? (Совет. Используйте ключевое слово any.)

c. Остальной IP-трафик запрещён по умолчанию.

```
RTA(config)#access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq
telnet
```

telnet сети 10.101.117.32/28 разрешен для 10.100.117.0/27

```
  <cr>
RTA(config)#access-list 199 permit icmp any any
RTA(config)#
```

Icmp разрешен от всех для всех

Шаг 2. Примените расширенный ACL-список.

Общим правилом является размещение расширенных ACL-списков как можно ближе к источнику. При этом, поскольку список доступа 199 влияет на трафик, исходящий от сетей 10.101.117.48/29 и 10.101.117.32/28, наиболее оптимальным местом размещения этого ACL-списка является интерфейс Gigabit Ethernet 0/2 в исходящем направлении. С помощью какой команды ACL-список 199 применяется на интерфейсе Gigabit Ethernet 0/2?

```
RTA(config)#int
RTA(config)#interface gig
RTA(config)#interface gigabitEthernet 0/2
RTA(config-if)#ip a
RTA(config-if)#ip acce
RTA(config-if)#ip access-group 199 out
```

Шаг 3. Проверьте работу расширенного ACL-списка.

a. Отправьте эхо-запросы от компьютера **PCB** на все остальные IP-адреса в сети. В случае неудачных эхо-запросов проверьте IP-адреса перед тем, как продолжить работу.

b. Выполните подключение по Telnet от **PCB** к **SWC**. Пароль: **cisco**.

c. Выйдите из службы Telnet на **SWC**.

d. Отправьте эхо-запросы от компьютера **PCA** на все остальные IP-адреса в сети. В случае неудачных эхо-запросов проверьте IP-адреса перед тем, как продолжить работу.

e. Выполните подключение по Telnet от **PCA** к **SWC**. В результате применения списка доступа маршрутизатор отклоняет соединение.

f. Выполните подключение по Telnet от **PCA** к **SWB**. Список доступа размещен на интерфейсе **G0/2** и не влияет на это подключение.

g. Войдите в систему **SWB** и оставайтесь в ней. Выполните подключение по Telnet к **SWC**.

a.

```
Ping statistics for 10.101.117.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 4ms

C:\>telnet 10.101.117.2
Trying 10.101.117.2 ...Open


User Access Verification

Password:
SWC>
```

b.

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.101.117.49

Pinging 10.101.117.49 with 32 bytes of data:

Reply from 10.101.117.49: bytes=32 time<1ms TTL=255
Reply from 10.101.117.49: bytes=32 time<1ms TTL=255
Reply from 10.101.117.49: bytes=32 time<1ms TTL=255
Reply from 10.101.117.49: bytes=32 time<1ms TTL=255

Ping statistics for 10.101.117.49:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.101.117.33

Pinging 10.101.117.33 with 32 bytes of data:

Reply from 10.101.117.33: bytes=32 time<1ms TTL=255
Reply from 10.101.117.33: bytes=32 time<1ms TTL=255
Reply from 10.101.117.33: bytes=32 time=1ms TTL=255
Reply from 10.101.117.33: bytes=32 time=1ms TTL=255

Ping statistics for 10.101.117.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.101.117.1

Pinging 10.101.117.1 with 32 bytes of data:

Reply from 10.101.117.1: bytes=32 time<1ms TTL=255
Reply from 10.101.117.1: bytes=32 time<1ms TTL=255
Reply from 10.101.117.1: bytes=32 time<1ms TTL=255
Reply from 10.101.117.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.101.117.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.101.117.51

Pinging 10.101.117.51 with 32 bytes of data:

Reply from 10.101.117.51: bytes=32 time=5ms TTL=128
Reply from 10.101.117.51: bytes=32 time=6ms TTL=128
Reply from 10.101.117.51: bytes=32 time=10ms TTL=128
Reply from 10.101.117.51: bytes=32 time=6ms TTL=128
```

```
Ping statistics for 10.101.117.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.101.117.51

Pinging 10.101.117.51 with 32 bytes of data:

Reply from 10.101.117.51: bytes=32 time=5ms TTL=128
Reply from 10.101.117.51: bytes=32 time=6ms TTL=128
Reply from 10.101.117.51: bytes=32 time=10ms TTL=128
Reply from 10.101.117.51: bytes=32 time=6ms TTL=128

Ping statistics for 10.101.117.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 10ms, Average = 6ms

C:\>ping 10.101.117.35

Pinging 10.101.117.35 with 32 bytes of data:

Reply from 10.101.117.35: bytes=32 time<1ms TTL=127
Reply from 10.101.117.35: bytes=32 time<1ms TTL=127
Reply from 10.101.117.35: bytes=32 time<1ms TTL=127
Reply from 10.101.117.35: bytes=32 time<1ms TTL=127

Ping statistics for 10.101.117.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.101.117.2

Pinging 10.101.117.2 with 32 bytes of data:

Reply from 10.101.117.2: bytes=32 time<1ms TTL=254
Reply from 10.101.117.2: bytes=32 time<1ms TTL=254
Reply from 10.101.117.2: bytes=32 time<1ms TTL=254
Reply from 10.101.117.2: bytes=32 time<1ms TTL=254

Ping statistics for 10.101.117.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

e.

```
C:\>telnet 10.101.117.2
Trying 10.101.117.2 ...
% Connection timed out; remote host not responding
C:\>
```

f.

```
C:\>telnet 10.101.117.34
Trying 10.101.117.34 ...Open


User Access Verification

Password:
SWB>
```

g.

```
SWB#telnet 10.101.117.2
Trying 10.101.117.2 ...Open


User Access Verification

Password:
SWC>
```

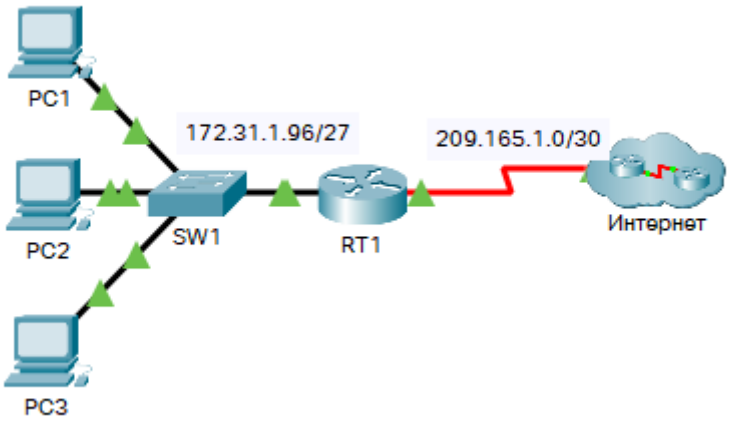
Часть 2. Вопросы на закрепление

1. Каким образом компьютер PCA «обошёл» список доступа 199 и подключился к коммутатору SWC через Telnet?
2. Что можно было сделать, чтобы запретить прямой доступ компьютера PCA к SWC, разрешив при этом доступ PCB к SWC через Telnet?

Сценарий_3

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
RT1	G0/0	172.31.1.126	255.255.255.224	Недоступно
	S0/0/0	209.165.1.2	255.255.255.252	Недоступно
PC1	Сетевой адаптер	172.31.1.101	255.255.255.224	172.31.1.126
PC2	Сетевой адаптер	172.31.1.102	255.255.255.224	172.31.1.126
PC3	Сетевой адаптер	172.31.1.103	255.255.255.224	172.31.1.126
Server1	Сетевой адаптер	64.101.255.254		
Server2	Сетевой адаптер	64.103.255.254		



Assessment Items	Status	Points	Component(s)	Feedback
Network				
RT1				
ACL		0	ACL	
ACL	Incorrect	80	IPv4 Extended ...	
Ports		0	Other	
GigabitEthernet0/0		0	Other	
Access-group In	Incorrect	20	IPv4 Extended ...	

Часть 1. Настройка расширенного именованного ACL-списка

Используйте один именованный ACL-список для реализации следующих правил:

- Запретите доступ через протоколы HTTP и HTTPS с **PC1** на серверы **Server1** и **Server2.** Эти серверы находятся внутри облака, известны только их IP-адреса.
- Заблокируйте FTP-доступ с **PC2** к серверам **Server1** и **Server2**.
- Заблокируйте ICMP-доступ с **PC3** к серверам **Server1** и **Server2**.

Примечание. Чтобы получить больше баллов, вы должны создать записи ACL-списка в порядке, указанном ниже.

Шаг 1. Запретите PC1 доступ к службам HTTP и HTTPS на серверах Server1 и Server2.

a. Создайте расширенный именованный ACL-список, который запретит **PC1** доступ к службам HTTP и HTTPS на серверах **Server1** и **Server2**. Поскольку невозможно напрямую наблюдать за подсетями серверов в сети Интернет, требуется использование четырёх правил.

   С какой команды начинается именованный ACL-список?

b. Создайте правило, запрещающее доступ с **PC1** к серверу **Server1**, только для HTTP (порт 80).

c. Создайте правило, запрещающее доступ с **PC1** к серверу **Server1**, только для HTTPS (порт 443).

d. Создайте правило, запрещающее доступ с **PC1** к серверу **Server2**, только для HTTP.

e. Создайте правило, запрещающее доступ с **PC1** к серверу **Server2**, только для HTTPS.

Deny /permit

```
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.101.255.254 eq www
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.101.255.254 eq 443

RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.103.255.254 eq 80
RT1(config-ext-nacl)#deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
```

Шаг 2. Запретите PC2 доступ к службам FTP на серверах Server1 и Server2.

a. Создайте правило, запрещающее доступ с **PC2** к серверу **Server1**, только для FTP (порт 21).

b. Создайте правило, запрещающее доступ с **PC2** к серверу **Server2**, только для FTP (порт 21).

```
  www         World Wide Web (HTTP, 80)
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
RT1(config-ext-nacl)#deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
RT1(config-ext-nacl)#deny icmp ?
```

Шаг 3. Запретите PC3 отправлять эхо-запросы на серверы Server1 и Server2.

a. Создайте правило, запрещающее ICMP-доступ с **PC3** к серверу **Server1**.

b. Создайте правило, запрещающее ICMP-доступ с **PC3** к серверу **Server2**.

```
  <cr>
RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.101.255.254
RT1(config-ext-nacl)#deny icmp host 172.31.1.103 host 64.103.255.254
```

Шаг 4. Разрешите весь остальной IP-трафик.

По умолчанию список доступа отклоняет весь трафик, который не соответствует любому правилу, указанному в списке. С помощью какой команды разрешается весь остальной трафик?

```
  <cr>
RT1(config-ext-nacl)#permit ip any any
```

Часть 2. Применение и проверка расширенного ACL-списка

Трафик, который должен фильтроваться, поступает от сети 172.31.1.96/27 и предназначен для удалённых сетей. Правильное размещение ACL-списка также зависит от направления трафика по отношению к **RT1**.

Шаг 1. Примените ACL-список на соответствующем интерфейсе и направлении.

a. С помощью каких команд ACL-список применяется на правильном интерфейсе и правильном направлении?

```
RTl(config)#int
RTl(config)#interface gig
RTl(config)#interface gigabitEthernet 0/0
RTl(config-if)#ip acc
RTl(config-if)#ip access-group ACL ?
  in   inbound packets
  out  outbound packets
RTl(config-if)#ip access-group ACL in
RTl(config-if)#
```

Шаг 2. Проверьте доступ для каждого компьютера.

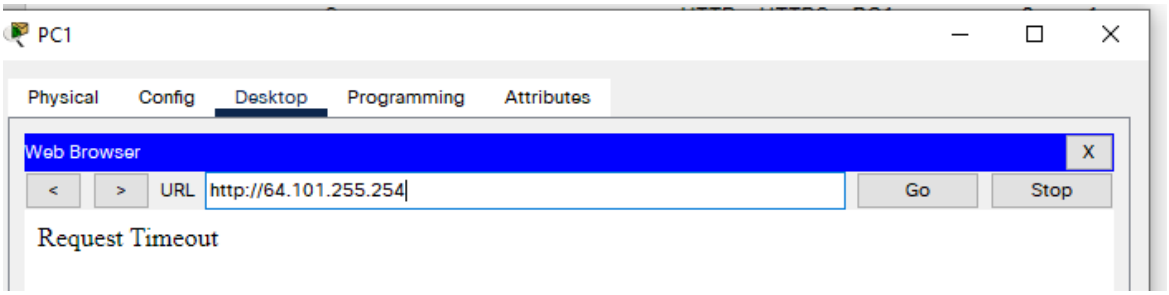
a. Попробуйте получить доступ к веб-сайтам на серверах **Server1** и **Server2**, используя веб-браузер **PC1**, а также протоколы HTTP и HTTPS.

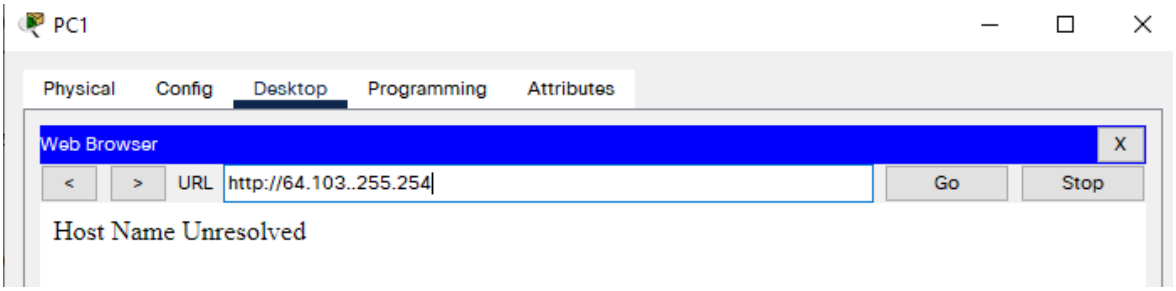
b. Попробуйте получить FTP-доступ к серверам **Server1** и **Server2** с компьютера **PC1**. Имя пользователя и пароль: **cisco**.

c. Выполните эхо-запросы на серверы **Server1** и **Server2** от **PC1**.

d Повторите шаги 2a-2c для компьютеров **PC2** и **PC3**, чтобы проверить правильность работы списков доступа.

PC1



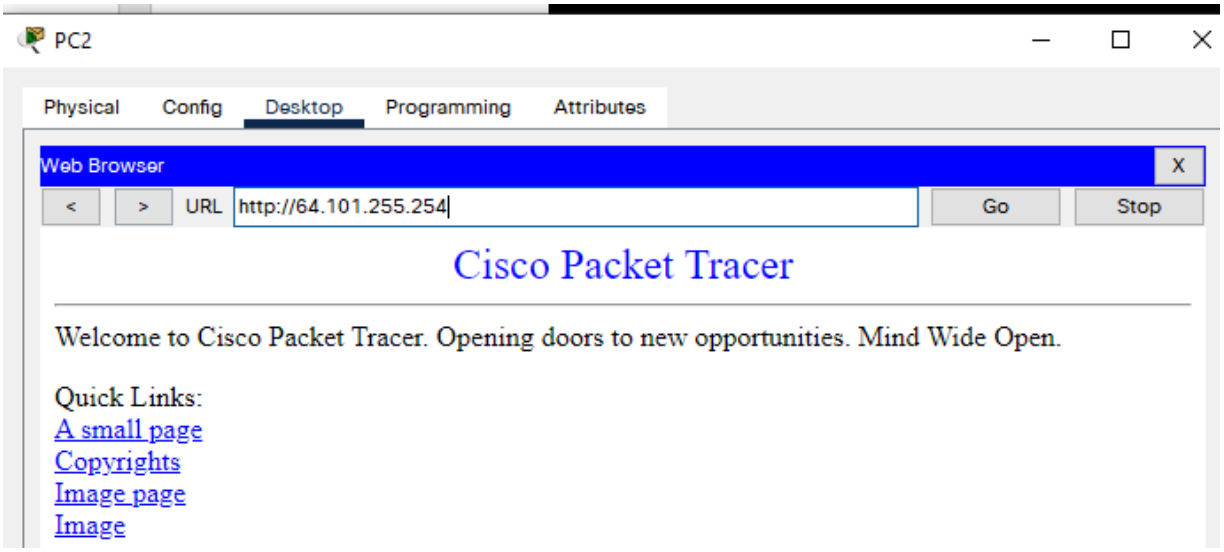


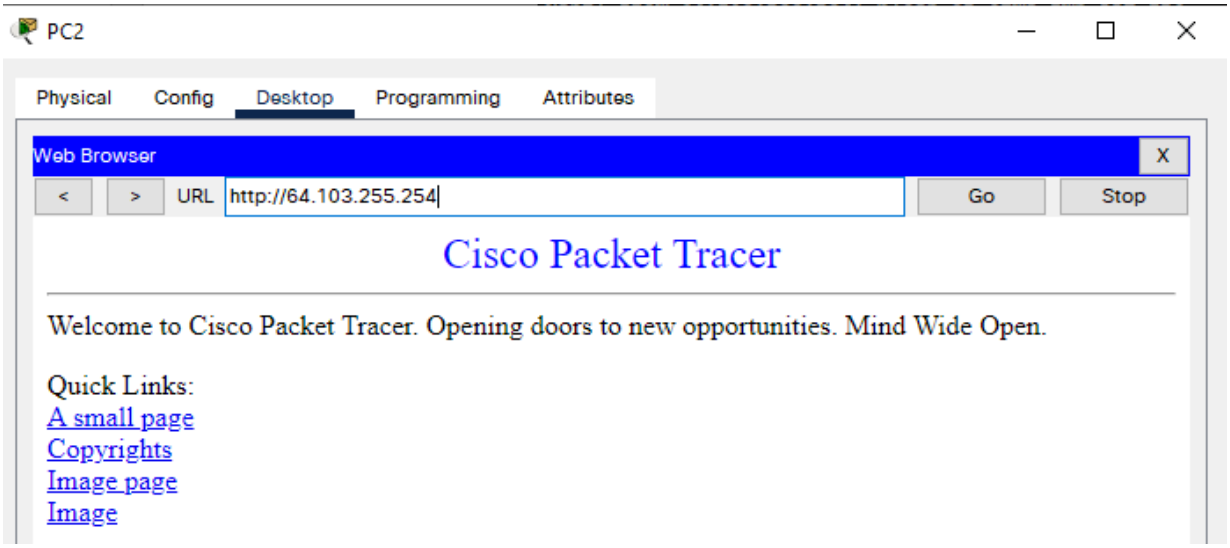

```
C:\>ftp 64.101.255.254
Trying to connect...64.101.255.254
Connected to 64.101.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>ftp 64.103.255.254
 Invalid or non supported command.
ftp>
```

```
C:\>ftp 64.103.255.254
Trying to connect...64.103.255.254
Connected to 64.103.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

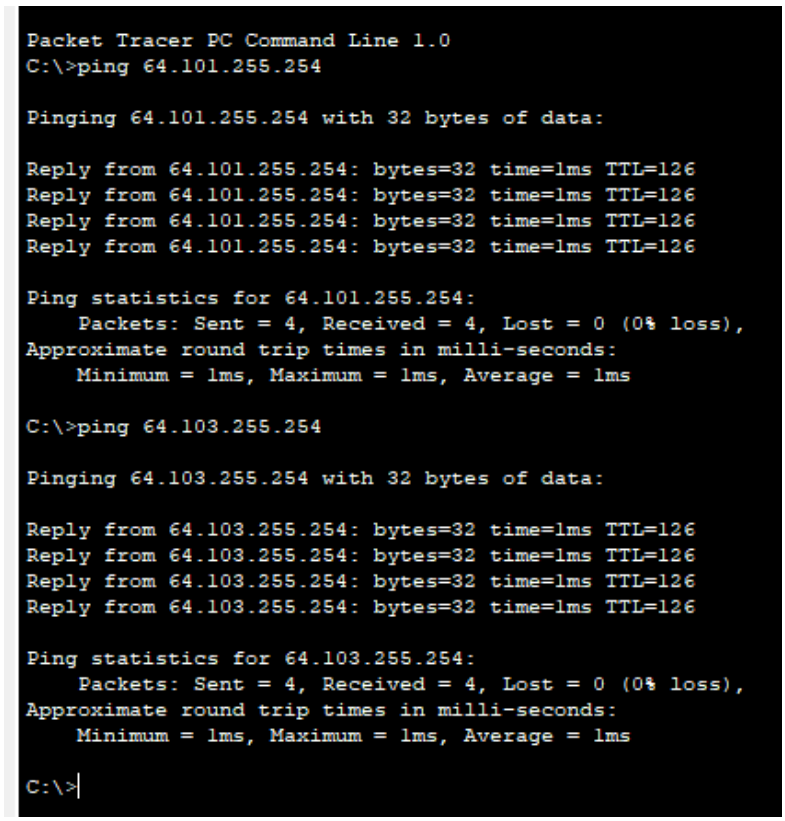
```
C:\>ping 64.101.255.254

Pinging 64.101.255.254 with 32 bytes of data:

Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126

Ping statistics for 64.101.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 64.103.255.254

Pinging 64.103.255.254 with 32 bytes of data:

Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=2ms TTL=126

Ping statistics for 64.103.255.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

PC2

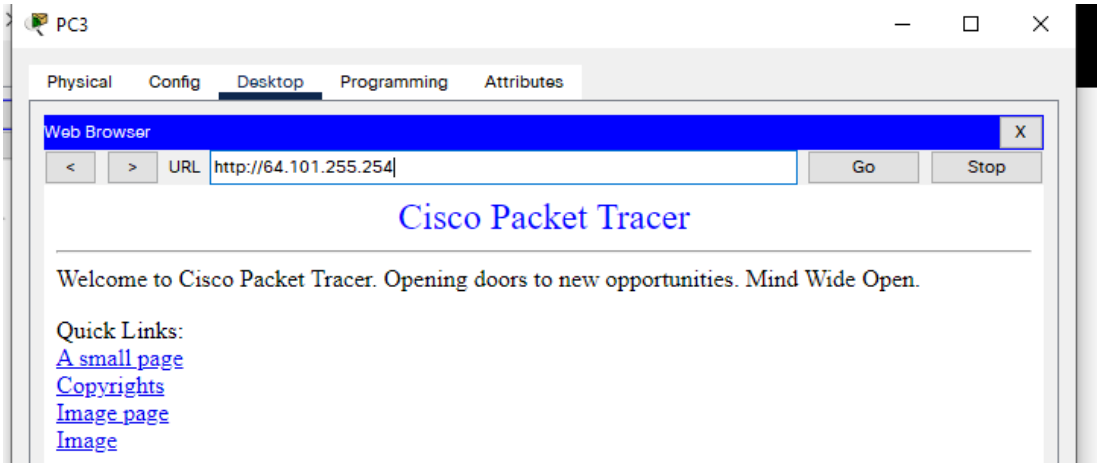


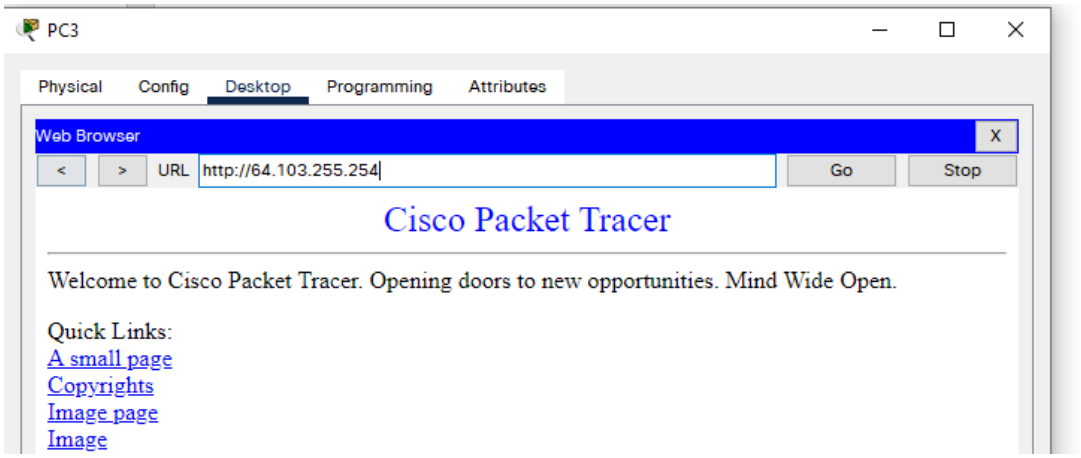


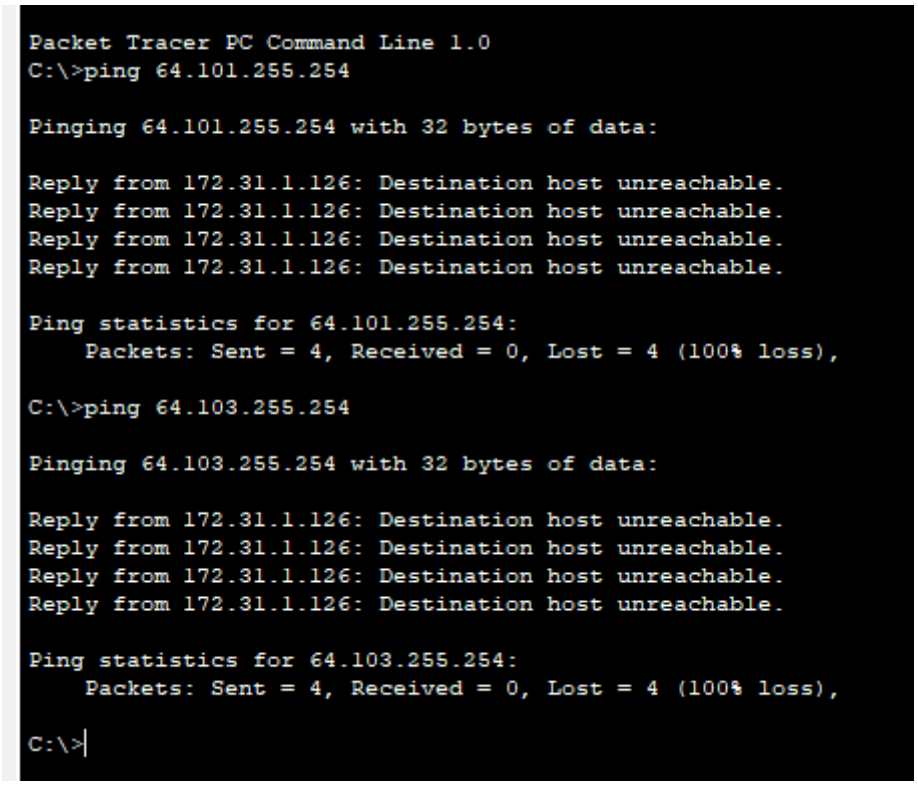

```
C:\>ftp 64.101.255.254
Trying to connect...64.101.255.254

%Error opening ftp://64.101.255.254/ (Timed out)
.



(Disconnecting from ftp server)



ftp 64.103.255.254
Trying to connect...64.103.255.254

%Error opening ftp://64.103.255.254/ (Timed out)
.



(Disconnecting from ftp server)
```

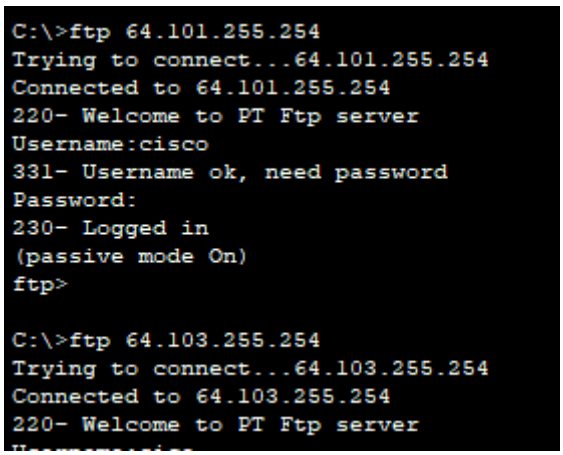

Packet Tracer PC Command Line 1.0
C:\>ping 64.101.255.254
Pinging 64.101.255.254 with 32 bytes of data:
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Reply from 64.101.255.254: bytes=32 time=1ms TTL=126
Ping statistics for 64.101.255.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>ping 64.103.255.254
Pinging 64.103.255.254 with 32 bytes of data:
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Reply from 64.103.255.254: bytes=32 time=1ms TTL=126
Ping statistics for 64.103.255.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>

PC3


PC3
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://64.101.255.254
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image


PC3
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://64.103.255.254
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image


Packet Tracer PC Command Line 1.0
C:\>ping 64.101.255.254
Pinging 64.101.255.254 with 32 bytes of data:
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Ping statistics for 64.101.255.254:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 64.103.255.254
Pinging 64.103.255.254 with 32 bytes of data:
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Reply from 172.31.1.126: Destination host unreachable.
Ping statistics for 64.103.255.254:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>


C:\>ftp 64.101.255.254
Trying to connect...64.101.255.254
Connected to 64.101.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
C:\>ftp 64.103.255.254
Trying to connect...64.103.255.254
Connected to 64.103.255.254
220- Welcome to PT Ftp server

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All | Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedb
Network				
RT1				
ACL		0	ACL	
✔ ACL	Correct	80	IPv4 Extended ...	
Ports		0	Other	
GigabitEthernet0/0		0	Other	
✔ Access-group In	Correct	20	IPv4 Extended ...	