Гвоздков И.В.
Хорошенко С.В

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ СЕТЕВЫХ ИНФРАСТРУКТУР

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

САНКТ-ПЕТЕРБУРГ
2016

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»

Гвоздков И.В.
Хорошенко С.В

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ СЕТЕВЫХ ИНФРАСТРУКТУР

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

СПб ГУТ)))

САНКТ-ПЕТЕРБУРГ
2016

УДК 621.391.24(77)
ББК 3287я73
И20

Рецензент

Рекомендовано к печати
Редакционно-издательским советом СПбГУТ

Гвоздков И.В. Хорошенко С.В

И 20 Технологии безопасности сетевых инфраструктур: лабораторный практикум / Гвоздков И.В. Хорошенко С.В – СПб. : СПбГУТ, 2016. – 55с

Написаны в соответствии с рабочими учебными программами дисциплины «Технологии безопасности сетевых инфраструктур».

Данный курс лабораторных работ посвящен практическому изучению, настройке и работе с сетевым оборудованием локальных сетей.

Предназначен для студентов обучающихся по направлению подготовки 09.03.02 «Информационные системы и технологии»

УДК 621.391.24(77)
ББК 3287я73

СОДЕРЖАНИЕ

Лабораторная работа 1

НАСТРОЙКА БАЗОВОГО PPP С АУТЕНТИФИКАЦИЕЙ

Топология

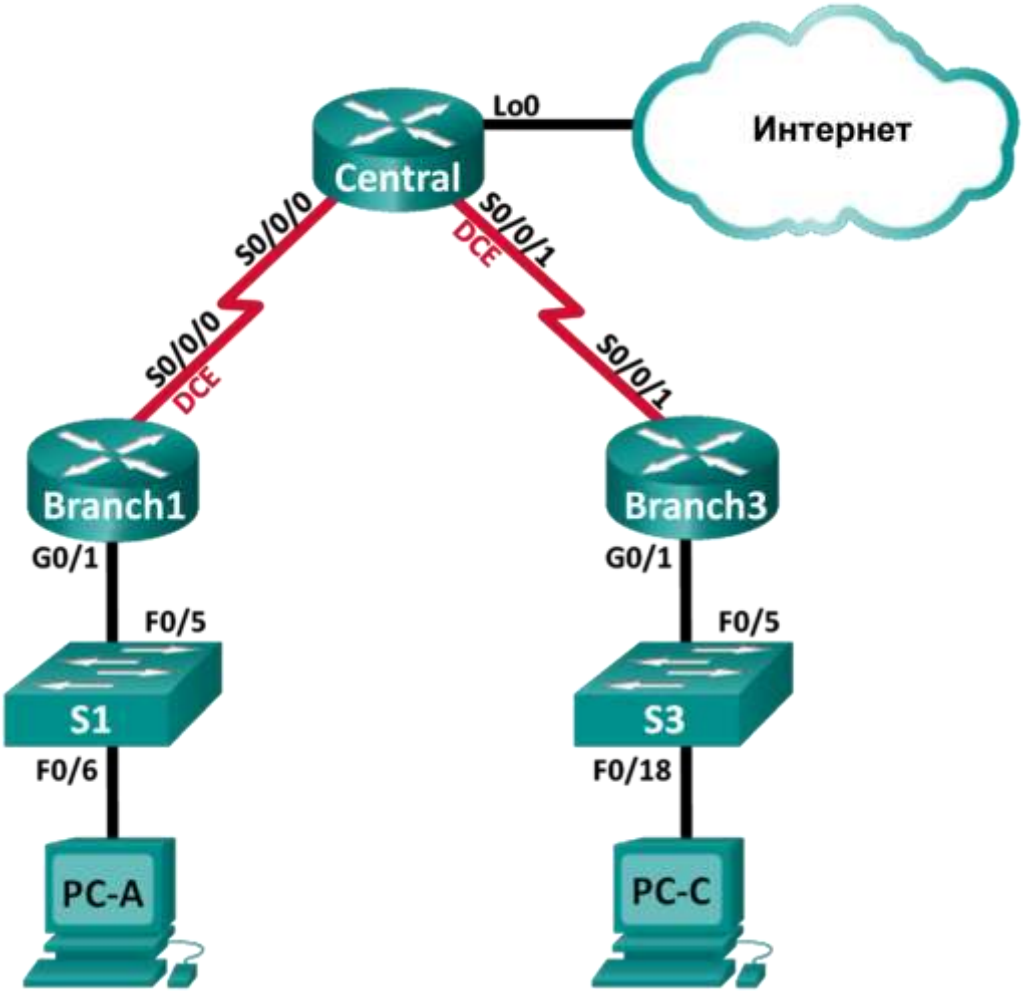


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Branch1	G0/1	192.168.1.1	255.255.255.0	—
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	—
Central	S0/0/0	10.1.1.2	255.255.255.252	—
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	—
	Lo0	209.165.200.225	255.255.255.224	—
Branch3	G0/1	192.168.3.1	255.255.255.0	—
	S0/0/1	10.2.2.1	255.255.255.252	—
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Задачи

Часть 1. Настройка базовых параметров устройства

Часть 2. Настройка инкапсуляции PPP

Часть 3. Настройка аутентификации PPP CHAP

Общие сведения/сценарий

PPP часто используется в качестве протокола WAN уровня 2. PPP можно использовать для подключения из локальной сети к WAN-провайдеру и для подключения сегментов LAN в рамках корпоративной сети.

В этой лабораторной работе требуется настроить инкапсуляцию PPP на выделенных последовательных каналах между маршрутизаторами филиалов и центральным маршрутизатором. Требуется настроить протокол аутентификации по квитированию вызова (CHAP) PPP на последовательных каналах PPP. Вы также изучите влияние, оказываемое изменениями инкапсуляции и аутентификации на состояние последовательного канала.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(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. Точные идентификаторы интерфейсов 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.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ 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

Часть 1: Настройка основных параметров устройств

В части 1 вам предстоит настроить топологию сети и базовые параметры маршрутизатора, например, IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели сети согласно приведенной топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите DNS-поиск.

b. Настройте имя устройства.

c. Зашифруйте открытые пароли.

d. Создайте баннерное сообщение дня (MOTD) для предупреждения пользователей о запрете несанкционированного доступа.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.

f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте ведение журнала консоли в синхронном режиме.

h. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и включите физические интерфейсы.

i. Настройте тактовую частоту **128 000** для всех последовательных интерфейсов DCE.

j. На маршрутизаторе Central создайте **Loopback 0** для имитации доступа в Интернет и назначьте IP-адрес согласно таблице адресации.

Шаг 4: Настройте маршрутизацию.

a. Включите на маршрутизаторах использование протокола OSPF для одной области и используйте в качестве идентификатора процесса значение 1. Добавьте в процесс OSPF все сети, за исключением 209.165.200.224/27.

b. На маршрутизаторе Central настройте маршрут по умолчанию к моделируемому Интернету, используя Lo0 в качестве выходного интерфейса, и перераспределите этот маршрут в процесс OSPF.

c. На всех маршрутизаторах выполните команды **show ip route ospf**, **show ip ospf interface brief** и **show ip ospf neighbor**, чтобы проверить правильность настройки OSPF. Обратите внимание на идентификатор каждого маршрутизатора.

Шаг 5: Настройте компьютеры.

Назначьте компьютерам IP-адреса и шлюзы по умолчанию в соответствии с таблицей адресации.

Шаг 6: Проверьте наличие сквозного подключения.

Все устройства должны успешно получать ответы на ping-запросы ко всем остальным устройствам, указанным в данной топологии. Если это не так, ищите и устраняйте неполадки, пока не удастся установить сквозное соединение.

Примечание. Чтобы успешно получать ответы на ping-запросы между ПК, может потребоваться отключить межсетевой экран.

Шаг 7: Сохраните настройки.

Часть 2: Настройте инкапсуляцию PPP.

Шаг 1: Отобразите инкапсуляцию, используемую в последовательном интерфейсе по умолчанию.

На маршрутизаторах выполните команду **show interfaces serial** *идентификатор_интерфейса* для отображения текущей инкапсуляции, используемой в последовательном интерфейсе.

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:05, output hang never
  Last clearing of show interface counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   1003 packets input, 78348 bytes, 0 no buffer
   Received 527 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   1090 packets output, 80262 bytes, 0 underruns
   0 output errors, 0 collisions, 3 interface resets
   0 unknown protocol drops
   0 output buffer failures, 0 output buffers swapped out
   2 carrier transitions
   DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Укажите тип инкапсуляции, используемой в последовательном интерфейсе по умолчанию, для маршрутизатора Cisco. _____

Шаг 2: Измените инкапсуляцию на PPP.

a. Для изменения инкапсуляции HDLC на PPP введите команду **encapsulation ppp** на интерфейсе S0/0/0 маршрутизатора Branch1.

```
Branch1(config)# interface s0/0/0
Branch1(config-if)# encapsulation ppp
Branch1(config-if)#
Jun 19 06:02:33.687: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
Branch1(config-if)#
Jun 19 06:02:35.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
```

b. Введите команду для отображения состояния и протокола линии связи для интерфейса S0/0/0 маршрутизатора Branch1. Задокументируйте выполненную команду. Укажите текущее состояние интерфейса S0/0/0.

Для исправления разночтений в настройках инкапсуляции для последовательного интерфейса ведите команду **encapsulation ppp** на интерфейсе S0/0/0 для маршрутизатора Central.

```
Central(config)# interface s0/0/0
Central(config-if)# encapsulation ppp
Central(config-if)#
.Jun 19 06:03:41.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
.Jun 19 06:03:41.274: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done
```

c. Убедитесь, что интерфейс S0/0/0 как на маршрутизаторе Branch1, так и на маршрутизаторе Central переведен в активное состояние и на нем настроена инкапсуляция PPP.

Укажите состояние протокола управления каналом PPP. _____

Укажите, согласование каких протоколов NCP было выполнено.

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
```

```
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:03:58
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     77 packets input, 4636 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     117 packets output, 5800 bytes, 0 underruns
     0 output errors, 0 collisions, 8 interface resets
     22 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     18 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

Central# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:03, output hang never
  Last clearing of "show interface" counters 00:01:20
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     41 packets input, 2811 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     40 packets output, 2739 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Шаг 3: Намеренно разорвите последовательное подключение.

a. Выполните команды **debug ppp**, чтобы понаблюдать за влиянием изменения настройки PPP на маршрутизаторы Branch1 и Central.

```
Branch1# debug ppp negotiation
PPP protocol negotiation debugging is on
Branch1# debug ppp packet
PPP packet display debugging is on
```

```
Central# debug ppp negotiation
PPP protocol negotiation debugging is on
Central# debug ppp packet
PPP packet display debugging is on
```

b. Наблюдайте за сообщениями команды debug PPP при проходе трафика по последовательному каналу между маршрутизаторами Branch1 и Central.

```
Branch1#
Jun 20 02:20:45.795: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 02:20:49.639: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic
0x73885AF2
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic
0x8CE1F65F
Jun 20 02:20:50.159: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic
0x8CE1F65F
Jun 20 02:20:50.159: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic
0x73885AF2
Jun 20 02:20:50.159: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Central#
Jun 20 02:20:49.636: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 02:20:50.148: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic
0x73885AF2
Jun 20 02:20:50.148: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic
0x8CE1F65F
Jun 20 02:20:50.148: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up
Jun 20 02:20:50.160: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic
0x8CE1F65F
Jun 20 02:20:50.160: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic
0x73885AF2
Jun 20 02:20:55.552: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
```

c. Разорвите последовательное подключение путем возвращения HDLC в качестве инкапсуляции для последовательного интерфейса S0/0/0 маршрутизатора Branch1. Запишите команду, использованную для изменения инкапсуляции на HDLC.

_____

Наблюдайте за сообщениями команды debug PPP на маршрутизаторе Branch1. Последовательное подключение разорвано, и протокол линии связи не функционирует. Маршрут к маршрутизатору 10.1.1.2 (Central) удален из таблицы маршрутизации.

```
Jun 20 02:29:50.295: Se0/0/0 PPP DISC: Lower Layer disconnected
Jun 20 02:29:50.295: PPP: NET STOP send to AAA.
Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.29
Branch1(config-if)#9: Se0/0/0 LCP: O TERMREQ [Open] id 7 len 4
Jun 20 02:29:50.299: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]
Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is TERMINATING
Jun 20 02:29:50.299: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0,
address 10.1.1.2
Jun 20 02:29:50.299: Se0/0/0 IPCP: Remove route to 10.1.1.2
Jun 20 02:29:50.299: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is DOWN
Branch1(config-if)#
Jun 20 02:30:17.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
```

```
Jun 20 02:30:17.083: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
```

d. Наблюдайте за сообщениями команды debug PPP на маршрутизаторе Central. Маршрутизатор Central продолжает попытки установить подключение к маршрутизатору Branch1, как видно из сообщений команды debug. Если интерфейсы не могут установить подключение, они снова отключаются. Кроме того, OSPF не может сформировать отношения смежности с соседним с ним устройством вследствие несоответствия инкапсуляции для последовательного канала.

```
Jun 20 02:29:50.296: Se0/0/0 PPP: Sending cstate DOWN notification
Jun 20 02:29:50.296: Se0/0/0 PPP: Processing CstateDown message
Jun 20 02:29:50.296: Se0/0/0 PPP DISC: Lower Layer disconnected
Jun 20 02:29:50.296: PPP: NET STOP send to AAA.
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 LCP: O TERMREQ [Open] id 2 len 4
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is TERMINATING
Jun 20 02:29:50.296: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0,
address 10.1.1.1
Jun 20 02:29:50.296: Se0/0/0 IPCP: Remove route to 10.1.1.1
Jun 20 02:29:50.296: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is DOWN
Jun 20 02:29:52.296: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
.Jun 20 02:29:52.296: Se0/0/0 PPP: Sending cstate UP notification
.Jun 20 02:29:52.296: Se0/0/0 PPP: Processing CstateUp message
.Jun 20 02:29:52.296: PPP: Alloc Context [29F9F32C]
.Jun 20 02:29:52.296: ppp3 PPP: Phase is ESTABLISHING
.Jun 20 02:29:52.296: Se0/0/0 PPP: Using default call direction
.Jun 20 02:29:52.296: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:29:52.296: Se0/0/0 PPP: Session handle[60000003] Session id[3]
.Jun 20 02:29:52.296: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 02:29:52.296: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 02:29:52.296: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:29:52.296: Se0/0/0 LCP:Event[UP] State[Starting to REQsent]
.Jun 20 02:29:54.308: Se0/0/0 LCP: O CONFREQ [REQsent] id 2 len 10
.Jun 20 02:29:54.308: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:29:54.308: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:29:56.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24
link[illegal]
.Jun 20 02:29:56.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding
<Данные опущены>
.Jun 20 02:30:10.436: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10
.Jun 20 02:30:10.436: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:30:10.436: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:30:12.452: Se0/0/0 PPP DISC: LCP failed to negotiate
.Jun 20 02:30:12.452: PPP: NET STOP send to AAA.
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:12.452: Se0/0/0 PPP: Phase is DOWN
.Jun 20 02:30:14.452: PPP: Alloc Context [29F9F32C]
.Jun 20 02:30:14.452: ppp4 PPP: Phase is ESTABLISHING
```

```
.Jun 20 02:30:14.452: Se0/0/0 PPP: Using default call direction
.Jun 20 02:30:14.452: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:30:14.452: Se0/0/0 PPP: Session handle[6E000004] Session id[4]
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 02:30:14.452: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 02:30:14.452: Se0/0/0 LCP:    MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
.Jun 20 02:30:16.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24
link[illegal]
.Jun 20 02:30:16.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding
<Данные опущены>
.Jun 20 02:30:32.580: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10
.Jun 20 02:30:32.580: Se0/0/0 LCP:    MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:32.580: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:30:34.596: Se0/0/0 PPP DISC: LCP failed to negotiate
.Jun 20 02:30:34.596: PPP: NET STOP send to AAA.
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:34.596: Se0/0/0 PPP: Phase is DOWN
.Jun 20 02:30:36.080: Se0/0/0 PPP: I pkt type 0x008F, discarded, PPP not
running
.Jun 20 02:30:36.596: PPP: Alloc Context [29F9F32C]
.Jun 20 02:30:36.596: ppp5 PPP: Phase is ESTABLISHING
.Jun 20 02:30:36.596: Se0/0/0 PPP: Using default call direction
.Jun 20 02:30:36.596: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:30:36.596: Se0/0/0 PPP: Session handle[34000005] Session id[5]
.Jun 20 02:30:36.596: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
```

Что происходит в случае, если на одном конце последовательного канала используется инкапсуляция PPP, а на другом — HDLC?

Введите команду **encapsulation ppp** на интерфейсе S0/0/0 маршрутизатора Branch1, чтобы исправить несоответствующую инкапсуляцию.

```
Branch1(config)# interface s0/0/0
Branch1(config-if)# encapsulation ppp
```

e. Наблюдайте за сообщениями команды debug PPP от маршрутизатора Branch1 при установке подключения между маршрутизаторами Branch1 и Central.

```
Branch1(config-if)#
Jun 20 03:01:57.399: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:01:59.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
Jun 20 03:01:59.399: Se0/0/0 PPP: Sending cstate UP notification
Jun 20 03:01:59.399: Se0/0/0 PPP: Processing CstateUp message
Jun 20 03:01:59.399: PPP: Alloc Context [30F8D4F0]
Jun 20 03:01:59.399: ppp9 PPP: Phase is ESTABLISHING
Jun 20 03:01:59.399: Se0/0/0 PPP: Using default call direction
Jun 20 03:01:59.399: Se0/0/0 PPP: Treating connection as a dedicated line
Jun 20 03:01:59.399: Se0/0/0 PPP: Session handle[BA000009] Session id[9]
Jun 20 03:01:59.399: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.399: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.399: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.399: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
```

```
Jun 20 03:01:59.407: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to
ACKsent]
Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
Jun 20 03:01:59.439: Se0/0/0 LCP: State is Open
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
Jun 20 03:01:59.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
Jun 20 03:01:59.439: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol
not up
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is UP
Jun 20 03:01:59.439: Se0/0/0 IPCP: Protocol configured, start CP.
state[Initial]
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.439: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.439: Se0/0/0 IPCP:    Address 10.1.1.1 (0x03060A010101)
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.439: Se0/0/0 CDPCP: Protocol configured, start CP.
state[Initial]
<Данные опущены>
Jun 20 03:01:59.471: Se0/0/0 Added to neighbor route AVL tree: topoid 0,
address 10.1.1.2
Jun 20 03:01:59.471: Se0/0/0 IPCP: Install route to 10.1.1.2
Jun 20 03:01:59.471: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:01:59.479: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:01:59.479: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 03:01:59.483: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
Jun 20 03:01:59.483: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:01:59.491: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
Jun 20 03:01:59.491: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148
Jun 20 03:01:59.511: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
Jun 20 03:01:59.511: %OSPF-5-ADJCHG:Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from LOADING to FULL, Loading Done
Jun 20 03:01:59.511: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:01:59.519: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 60 link[ip]
```

f. Наблюдайте за сообщениями команды debug PPP от маршрутизатора Central при установке подключения между маршрутизаторами Branch1 и Central.

```
Jun 20 03:01:59.393: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.393: Se0/0/0 LCP: I CONFREQ [Open] id 1 len 10
Jun 20 03:01:59.393: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.393: Se0/0/0 PPP DISC: PPP Renegotiating
Jun 20 03:01:59.393: PPP: NET STOP send to AAA.
Jun 20 03:01:59.393: Se0/0/0 LCP: Event[LCP Reneg] State[Open to Open]
Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 03:01:59.393: Se0/0/0 LCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
```

```
Jun 20 03:01:59.393: Se0/0/0 PPP: Outbound cdp packet dropped, NCP not
negotiated
.Jun 20 03:01:59.393: Se0/0/0 PPP: Phase is DOWN
.Jun 20 03:01:59.393: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0,
address 10.1.1.1
.Jun 20 03:01:59.393: Se0/0/0 IPCP: Remove route to 10.1.1.1
.Jun 20 03:01:59.393: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 03:01:59.397: PPP: Alloc Context [29F9F32C]
.Jun 20 03:01:59.397: ppp38 PPP: Phase is ESTABLISHING
.Jun 20 03:01:59.397: Se0/0/0 PPP: Using default call direction
.Jun 20 03:01:59.397: Se0/0/0 PPP: Treating connection as a dedicated line
<Данные опущены>
.Jun 20 03:01:59.401: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
.Jun 20 03:01:59.401: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to
Open]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 03:01:59.433: Se0/0/0 LCP: State is Open
.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14 link[ip]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Queue IPCP code[1] id[1]
.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Discarded CDPCP code[1] id[1]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
.Jun 20 03:01:59.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
.Jun 20 03:01:59.433: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol
not up
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is UP
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Protocol configured, start CP.
state[Initial]
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 03:01:59.433: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 03:01:59.433: Se0/0/0 IPCP:    Address 10.1.1.2 (0x03060A010102)
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Protocol configured, start CP.
state[Initial]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: O CONFREQ [Starting] id 1 len 4
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[UP] State[Starting to REQsent]
<Данные опущены>
.Jun 20 03:01:59.465: Se0/0/0 IPCP: State is Open
.Jun 20 03:01:59.465: Se0/0/0 Added to neighbor route AVL tree: topoid 0,
address 10.1.1.1
.Jun 20 03:01:59.465: Se0/0/0 IPCP: Install route to 10.1.1.1
.Jun 20 03:01:59.465: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 03:01:59.465: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
.Jun 20 03:01:59.469: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
.Jun 20 03:01:59.477: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
.Jun 20 03:01:59.477: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 03:01:59.481: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 03:01:59.489: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
.Jun 20 03:01:59.493: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148
.Jun 20 03:01:59.505: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 03:01:59.505: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 60
.Jun 20 03:01:59.517: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 88 link[ip]
.Jun 20 03:01:59.517: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done
```

```
.Jun 20 03:01:59.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 03:01:59.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:01.445: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]
Jun 20 03:02:01.445: Se0/0/0 CDPCP: I CONFREQ [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: O CONFACK [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: Event[Receive ConfReq+] State[ACKrcvd to
Open]
Jun 20 03:02:01.449: Se0/0/0 CDPCP: State is Open
Jun 20 03:02:01.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:02:01.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:02.017: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:02:02.897: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 112 link[ip]
Jun 20 03:02:03.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
```

Основываясь на сообщениях команды debug для PPP, укажите, какие этапы проходит PPP при настройке инкапсуляции PPP на другом конце последовательного канала, на маршрутизаторе Central.

Что произойдет, если инкапсуляция PPP настроена на обоих концах последовательного канала?

g. Выполните команду **undebug all** (или **u all**) на маршрутизаторах Branch1 и Central, чтобы отключить отладку на обоих маршрутизаторах.

h. Выполните команду **show ip interface brief** на маршрутизаторах Branch1 и Central после конвергенции сети. Укажите состояние интерфейса S0/0/0 на обоих маршрутизаторах.

i. Убедитесь, что интерфейс S0/0/0 как на маршрутизаторе Branch1, так и на маршрутизаторе Central настроен на инкапсуляцию PPP.

Ниже запишите команду для проверки инкапсуляции PPP.

j. Инкапсуляцию в последовательном интерфейсе для связи между маршрутизаторами Central и Branch3 измените на инкапсуляцию PPP.

```
Central(config)# interface s0/0/1
Central(config-if)# encapsulation ppp
Central(config-if)#
Jun 20 03:17:15.933: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:17:17.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
Jun 20 03:17:23.741: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
Jun 20 03:17:23.825: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1
from LOADING to FULL, Loading Done


Branch3(config)# interface s0/0/1
Branch3(config-if)# encapsulation ppp
Branch3(config-if)#
Jun 20 03:17:21.744: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:17:21.948: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
.Jun 20 03:17:21.964: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
.Jun 20 03:17:23.812: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
```

k. Перед переходом к части 3 убедитесь в том, что сквозное подключение восстановлено.

Часть 3: Настройка аутентификации CHAP PPP

Шаг 1: Убедитесь, что инкапсуляция PPP настроена на всех последовательных интерфейсах.

Запишите команды, используемые для подтверждения того, что настроена инкапсуляция PPP.

Шаг 2: Настройте аутентификацию CHAP PPP для канала между маршрутизатором Central и маршрутизатором Branch3.

a. Настройте имя пользователя для аутентификации CHAP.

```
Central(config)# username Branch3 password cisco
Branch3(config)# username Central password cisco
```

b. Выполните команды **debug ppp** на маршрутизаторе Branch3 для наблюдения за процессом, который связан с аутентификацией.

```
Branch3# debug ppp negotiation
PPP protocol negotiation debugging is on
Branch3# debug ppp packet
PPP packet display debugging is on
```

c. Настройте интерфейс S0/0/1 на маршрутизаторе Branch3 для аутентификации CHAP.

```
Branch3(config)# interface s0/0/1
Branch3(config-if)# ppp authentication chap
```

d. Изучите сообщения команды debug PPP на маршрутизаторе Branch3, выдаваемые во время согласования с маршрутизатором Central.

```
Branch3(config-if)#
Jun 20 04:25:02.079: Se0/0/1 PPP DISC: Authentication configuration changed
Jun 20 04:25:02.079: PPP: NET STOP send to AAA.
Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 04:25:02.079: Se0/0/1 LCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
Jun 20 04:25:02.079: Se0/0/1 PPP: Outbound cdp packet dropped, NCP not
negotiated
.Jun 20 04:25:02.079: Se0/0/1 PPP: Phase is DOWN
.Jun 20 04:25:02.079: Se0/0/1 Deleted neighbor route from AVL tree: topoid 0,
address 10.2.2.2
.Jun 20 04:25:02.079: Se0/0/1 IPCP: Remove route to 10.2.2.2
.Jun 20 04:25:02.079: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 04:25:02.083: PPP: Alloc Context [29F4DA8C]
.Jun 20 04:25:02.083: ppp73 PPP: Phase is ESTABLISHING
.Jun 20 04:25:02.083: Se0/0/1 PPP: Using default call direction
.Jun 20 04:25:02.083: Se0/0/1 PPP: Treating connection as a dedicated line
.Jun 20 04:25:02.083: Se0/0/1 PPP: Session handle[2700004D] Session id[73]
<Данные опущены>
.Jun 20 04:25:02.091: Se0/0/1 PPP: I pkt type 0xC021, datagramsize 19 link[ppp]
.Jun 20 04:25:02.091: Se0/0/1 LCP: I CONFACK [ACKsent] id 1 len 15
.Jun 20 04:25:02.091: Se0/0/1 LCP:    AuthProto CHAP (0x0305C22305)
.Jun 20 04:25:02.091: Se0/0/1 LCP:    MagicNumber 0xF7B20F10 (0x0506F7B20F10)
.Jun 20 04:25:02.091: Se0/0/1 LCP: Event[Receive ConfAck] State[ACKsent to
Open]
```

```
.Jun 20 04:25:02.123: Se0/0/1 PPP: Phase is AUTHENTICATING, by this end
.Jun 20 04:25:02.123: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Branch3"
.Jun 20 04:25:02.123: Se0/0/1 LCP: State is Open
.Jun 20 04:25:02.127: Se0/0/1 PPP: I pkt type 0xC223, datagramsize 32 link[ppp]
.Jun 20 04:25:02.127: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Central"
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is AUTHENTICATING, Unauthenticated
User
.Jun 20 04:25:02.127: Se0/0/1 PPP: Sent CHAP LOGIN Request
.Jun 20 04:25:02.127: Se0/0/1 PPP: Received LOGIN Response PASS
.Jun 20 04:25:02.127: Se0/0/1 IPCP: Authorizing CP
.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP stalled on event[Authorize CP]
.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP unstall
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is AUTHENTICATING, Authenticated User
.Jun 20 04:25:02.135: Se0/0/1 CHAP: O SUCCESS id 1 len 4
.Jun 20 04:25:02.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
.Jun 20 04:25:02.135: Se0/0/1 PPP: Outbound cdp packet dropped, line protocol
not up
.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is UP
.Jun 20 04:25:02.135: Se0/0/1 IPCP: Protocol configured, start CP.
state[Initial]
.Jun 20 04:25:02.135: Se0/0/1 IPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 04:25:02.135: Se0/0/1 IPCP: O CONFREQ [Starting] id 1 len 10
<Данные опущены>
.Jun 20 04:25:02.143: Se0/0/1 CDPCP: I CONFACK [ACKsent] id 1 len 4
.Jun 20 04:25:02.143: Se0/0/1 CDPCP: Event[Receive ConfAck] State[ACKsent to
Open]
.Jun 20 04:25:02.155: Se0/0/1 IPCP: State is Open
.Jun 20 04:25:02.155: Se0/0/1 CDPCP: State is Open
.Jun 20 04:25:02.155: Se0/0/1 Added to neighbor route AVL tree: topoid 0,
address 10.2.2.2
.Jun 20 04:25:02.155: Se0/0/1 IPCP: Install route to 10.2.2.2
.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 04:25:02.155: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 84
.Jun 20 04:25:02.167: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
.Jun 20 04:25:02.167: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 04:25:02.171: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 04:25:02.171: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 148
.Jun 20 04:25:02.191: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
.Jun 20 04:25:02.191: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
.Jun 20 04:25:02.191: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 04:25:02.571: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 04:25:03.155: Se0/0/1 PPP: I pkt type 0x0207, datagramsize 333
link[cdp]
.Jun 20 04:25:03.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339
.Jun 20 04:25:04.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339
```

Основываясь на сообщениях команды debug для PPP, укажите, какие этапы проходит маршрутизатор Branch3, прежде чем будет установлена связь с маршрутизатором Central.

e. Выполните команду **debug ppp authentication** для просмотра сообщений аутентификации CHAP на маршрутизаторе Central.

```
Central# debug ppp authentication
PPP authentication debugging is on
```

f. Настройте аутентификацию CHAP на интерфейсе S0/0/1 на маршрутизаторе Central.

```
Central(config)# interface s0/0/1
Central(config-if)# ppp authentication chap
```

g. Наблюдайте за сообщениями команд debug PPP, относящихся к аутентификации CHAP на маршрутизаторе Central.

```
Central(config-if)#
.Jun 20 05:05:16.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
.Jun 20 05:05:16.061: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 05:05:16.061: Se0/0/1 PPP: Using default call direction
.Jun 20 05:05:16.061: Se0/0/1 PPP: Treating connection as a dedicated line
.Jun 20 05:05:16.061: Se0/0/1 PPP: Session handle[12000078] Session id[112]
.Jun 20 05:05:16.081: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Central"
.Jun 20 05:05:16.089: Se0/0/1 CHAP: I CHALLENGE id 1 len 28 from "Branch3"
.Jun 20 05:05:16.089: Se0/0/1 PPP: Sent CHAP SENDAUTH Request
.Jun 20 05:05:16.089: Se0/0/1 PPP: Received SENDAUTH Response PASS
.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using hostname from configured hostname
.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using password from AAA
.Jun 20 05:05:16.089: Se0/0/1 CHAP: O RESPONSE id 1 len 28 from "Central"
.Jun 20 05:05:16.093: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Branch3"
.Jun 20 05:05:16.093: Se0/0/1 PPP: Sent CHAP LOGIN Request
.Jun 20 05:05:16.093: Se0/0/1 PPP: Received LOGIN Response PASS
.Jun 20 05:05:16.093: Se0/0/1 CHAP: O SUCCESS id 1 len 4
.Jun 20 05:05:16.097: Se0/0/1 CHAP: I SUCCESS id 1 len 4
.Jun 20 05:05:16.097: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
.Jun 20 05:05:16.165: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1
from LOADING to FULL, Loading Done
```

h. Выполните команду **undebug all** (или **u all**) на маршрутизаторах Central и Branch3, чтобы полностью отключить отладку.

```
Central# undebug all
All possible debugging has been turned off
```

Шаг 3: Намеренно разорвите последовательный канал, настроенный с использованием аутентификации.

a. На маршрутизаторе Central настройте имя пользователя для маршрутизатора Branch1. Назначьте **cisco** в качестве пароля.

```
Central(config)# username Branch1 password cisco
```

b. На маршрутизаторах Central и Branch1 настройте аутентификацию CHAP на интерфейсе S0/0/0. Что происходит с интерфейсом?

Примечание. Для ускорения процесса выключите интерфейс и снова его включите.

c. Используйте команду **debug ppp negotiation**, чтобы посмотреть, что происходит.

```
Central# debug ppp negotiation
PPP protocol negotiation debugging is on
Central(config-if)#
.Jun 20 05:25:26.229: Se0/0/0 PPP: Missed a Link-Up transition, starting PPP
.Jun 20 05:25:26.229: Se0/0/0 PPP: Processing FastStart message
.Jun 20 05:25:26.229: PPP: Alloc Context [29F9F32C]
.Jun 20 05:25:26.229: ppp145 PPP: Phase is ESTABLISHING
.Jun 20 05:25:26.229: Se0/0/0 PPP: Using default call direction
.Jun 20 05:25:26.229: Se0/0/0 PPP: Treating connection as a dedicated line
```

```
.Jun 20 05:25:26.229: Se0/0/0 PPP: Session handle[6000009C] Session id[145]
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 15
.Jun 20 05:25:26.229: Se0/0/0 LCP:    AuthProto CHAP (0x0305C22305)
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x74385C31 (0x050674385C31)
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
.Jun 20 05:25:26.229: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x8D920101 (0x05068D920101)
.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x8D920101 (0x05068D920101)
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to
ACKsent]
.Jun 20 05:25:26.233: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 15
.Jun 20 05:25:26.233: Se0/0/0 LCP:    AuthProto CHAP (0x0305C22305)
.Jun 20 05:25:26.233: Se0/0/0 LCP:    MagicNumber 0x74385C31 (0x050674385C31)
.Jun 20 05:25:26.233: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to
Open]
.Jun 20 05:25:26.261: Se0/0/0 PPP: Phase is AUTHENTICATING, by this end
.Jun 20 05:25:26.261: Se0/0/0 CHAP: O CHALLENGE id 1 len 28 from "Central"
.Jun 20 05:25:26.261: Se0/0/0 LCP: State is Open
.Jun 20 05:25:26.265: Se0/0/0 LCP: I TERMREQ [Open] id 2 len 4
.Jun 20 05:25:26.265: Se0/0/0 PPP DISC: Received LCP TERMREQ from peer
.Jun 20 05:25:26.265: PPP: NET STOP send to AAA.
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is TERMINATING
.Jun 20 05:25:26.265: Se0/0/0 LCP: O TERMACK [Open] id 2 len 4
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[Receive TermReq] State[Open to
Stopping]
.Jun 20 05:25:26.265: Se0/0/0 PPP: Sending cstate DOWN notification
.Jun 20 05:25:26.265: Se0/0/0 PPP: Processing CstateDown message
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[CLOSE] State[Stopping to Closing]
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is DOWN
```

Объясните, что приводит к окончательному завершению канала. Запишите ниже команду, выполненную для устранения неполадки.

d. Выполните команду **undebug all** на всех маршрутизаторах, чтобы отключить отладку.

e. Проверьте наличие сквозного подключения.

Вопросы для повторения

1. Каковы признаки того, что на канале последовательной связи настроена несоответствующая инкапсуляция?

   Каковы признаки того, что на канале последовательной связи настроена несоответствующая аутентификация?

Лабораторная работа 2

Настройка маршрутизатора как клиента PPPoE для DSL-подключения

Топология

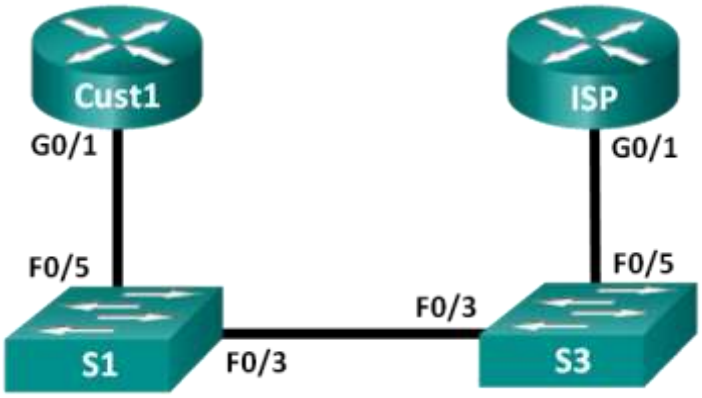


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Cust1	G0/1	Получен с помощью PPP	Получен с помощью PPP	Получен с помощью PPP
ISP	G0/1	Н/Д (недоступно)	Н/Д (недоступно)	Н/Д (недоступно)

Задачи

Часть 1. Развертывание сети

Часть 2. Настройка маршрутизатора интернет-провайдера

Часть 3. Настройка маршрутизатора Cust1

Общие сведения/сценарий

Интернет-провайдеры часто используют протокол PPPoE для передачи данных по каналам DSL своим заказчикам. PPP поддерживает назначение IP-адреса устройству на удаленном терминале канала PPP. Что еще более важно, PPP поддерживает аутентификацию по протоколу CHAP. Интернет-провайдеры могут проверять данные учета, чтобы узнать, был ли оплачен счет клиента, прежде чем позволить ему подключиться к Интернету.

В этой лабораторной работе выполняется настройка подключения на стороне клиента и интернет-провайдера для настройки PPPoE. В большинстве случаев достаточно выполнить настройку на стороне клиента.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4)M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(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. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

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

Необходимые ресурсы

2 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)

2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)

Консольные кабели для настройки устройств на базе Cisco IOS через консольные порты

Кабели Ethernet, расположенные в соответствии с топологией

Построение сети

- **Подключите кабели сети согласно приведенной топологии.**

- **Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.**

- **Произведите базовую настройку маршрутизаторов.**

Отключите DNS-поиск.

Настройте имена устройств в соответствии с топологией.

Зашифруйте открытые пароли.

Создайте объявление дня (MOTD), предупреждающее пользователей, что несанкционированный доступ запрещен.

Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

Настройте ведение журнала консоли в синхронном режиме.

Сохраните конфигурацию.

Настройка маршрутизатора интернет-провайдера

В части 2 необходимо настроить маршрутизатор интернет-провайдера с использованием параметров PPPoE для приема подключений от маршрутизатора Cust1.

Примечание. Многие из команд настройки PPPoE для маршрутизатора интернет-провайдера выходят за рамки курса; однако они необходимы для выполнения лабораторной работы. Их можно скопировать и вставить в маршрутизатор интернет-провайдера в командной строке режима глобальной настройки.

Создайте в локальной базе данных учетных записей имя пользователя **Cust1** с паролем **ciscopppoe**.

```
ISP(config)# username Cust1 password ciscopppoe
```

Создайте пул адресов, которые будут назначены пользователям.

```
ISP(config)# ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
```

Создайте виртуальный шаблон Virtual Template и свяжите с ним IP-адрес G0/1. Свяжите виртуальный шаблон с пулом адресов. Настройте CHAP для аутентификации клиентов.

```
ISP(config)# interface virtual-template 1
ISP(config-if)# ip address 10.0.0.254 255.255.255.0
ISP(config-if)# mtu 1492
ISP(config-if)# peer default ip address pool PPPoEPOOL
ISP(config-if)# ppp authentication chap callin
ISP(config-if)# exit
```

Назначьте шаблон группе PPPoE.

```
ISP(config)# bba-group pppoe global
ISP(config-bba-group)# virtual-template 1
ISP(config-bba-group)# exit
```

Свяжите группу bba-group с физическим интерфейсом G0/1.

```
ISP(config)# interface g0/1
ISP(config-if# pppoe enable group global
ISP(config-if)# no shutdown
```

Настройка маршрутизатора Cust1

В части 3 необходимо настроить маршрутизатор Cust1 с использованием параметров PPPoE.

Настройте интерфейс G0/1 для подключения по протоколу PPPoE.

```
Cust1(config)# interface g0/1
Cust1(config-if)# pppoe enable
Cust1(config-if)# pppoe-client dial-pool-number 1
Cust1(config-if)# exit
```

Свяжите интерфейс G0/1 с интерфейсом номеронабирателя. Используйте имя пользователя **Cust1** и пароль **ciscopppoe**, настроенные в части 2.

```
Cust1(config)# interface dialer 1
Cust1(config-if)# mtu 1492
Cust1(config-if)# ip address negotiated
Cust1(config-if)# encapsulation ppp
Cust1(config-if)# dialer pool 1
Cust1(config-if)# ppp authentication chap callin
Cust1(config-if)# ppp chap hostname Cust1
Cust1(config-if)# ppp chap password ciscopppoe
Cust1(config-if)# exit
```

Настройте статический маршрут по умолчанию на интерфейс номеронабирателя.

```
Cust1(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
```

Настройте отладку на маршрутизаторе Cust1 для отображения согласования PPP и PPPoE.

```
Cust1# debug ppp authentication
Cust1# debug pppoe events
```

Включите интерфейс G0/1 на маршрутизаторе Cust1 и проверьте выходные данные отладки при установлении сеанса номеронабирателя PPPoE и во время аутентификации CHAP.

```
*Jul 30 19:28:42.427: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed
state to down
*Jul 30 19:28:46.175: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed
state to up
*Jul 30 19:28:47.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
*Jul 30 19:29:03.839:  padi timer expired
*Jul 30 19:29:03.839:  Sending PADI: Interface = GigabitEthernet0/1
*Jul 30 19:29:03.839: PPPoE 0: I PADO  R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.887:  PPPOE: we've got our pado and the pado timer went off
*Jul 30 19:29:05.887: OUT PADR from PPPoE Session
*Jul 30 19:29:05.895: PPPoE 1: I PADS  R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.895: IN PADS from PPPoE Session
*Jul 30 19:29:05.899: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Jul 30 19:29:05.899: PPPoE: Virtual Access interface obtained.
*Jul 30 19:29:05.899: PPPoE : encap string prepared
*Jul 30 19:29:05.899: [0]PPPoE 1: data path set to PPPoE Client
```

```
*Jul 30 19:29:05.903: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state
to up
*Jul 30 19:29:05.911: Vi2 PPP: Using dialer call direction
*Jul 30 19:29:05.911: Vi2 PPP: Treating connection as a callout
*Jul 30 19:29:05.911: Vi2 PPP: Session handle[C6000001] Session id[1]
*Jul 30 19:29:05.919: Vi2 PPP: No authorization without authentication
*Jul 30 19:29:05.939: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Jul 30 19:29:05.939: Vi2 PPP: Sent CHAP SENDAUTH Request
*Jul 30 19:29:05.939: Vi2 PPP: Received SENDAUTH Response FAIL
*Jul 30 19:29:05.939: Vi2 CHAP: Using hostname from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: Using password from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: O RESPONSE id 1 len 26 from "Cust1"
*Jul 30 19:29:05.955: Vi2 CHAP: I SUCCESS id 1 len 4
*Jul 30 19:29:05.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-
Access2, changed state to up
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr  prepared
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr  prepared
```

Введите команду **show ip interface brief** на маршрутизаторе Cust1, чтобы узнать IP-адрес, назначенный маршрутизатором интернет-провайдера. Выходные данные приведены ниже. Каким способом был получен этот IP-адрес? _____

```
Cust1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down
down
GigabitEthernet0/0         unassigned      YES unset  administratively down
down
GigabitEthernet0/1         unassigned      YES unset  up                    up
Serial0/0/0                unassigned      YES unset  administratively down
down
Serial0/0/1                unassigned      YES unset  administratively down
down
Dialer1                    10.0.0.1        YES IPCP   up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  up                    up
```

Введите команду **show ip route** на маршрутизаторе Cust1. Выходные данные приведены ниже.

```
Cust1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Dialer1
      10.0.0.0/32 is subnetted, 2 subnets
C        10.0.0.1 is directly connected, Dialer1
C        10.0.0.254 is directly connected, Dialer1
```

Введите команду **show pppoe session** на маршрутизаторе Cust1. Выходные данные приведены ниже.

```
Cust1# show pppoe session
```

```
     1 client session

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st      Type
    N/A      1  30f7.0da3.0b01  Gi0/1                   Di1 Vi2        UP
                30f7.0da3.0bc1                              UP
```

Отправьте ping-запрос на адрес 10.0.0.254 с маршрутизатора Cust1. На эти ping-запросы должны приходить ответы. Если это не так, ищите и устраняйте неполадки, пока не удастся установить подключение.

```
Cust1# ping 10.0.0.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Вопросы для повторения

Почему интернет-провайдеры, использующие технологию DSL, главным образом используют протокол PPPoE?

Лабораторная работа. Настройка туннеля GRE «точка-точка» в сети VPN

Топология

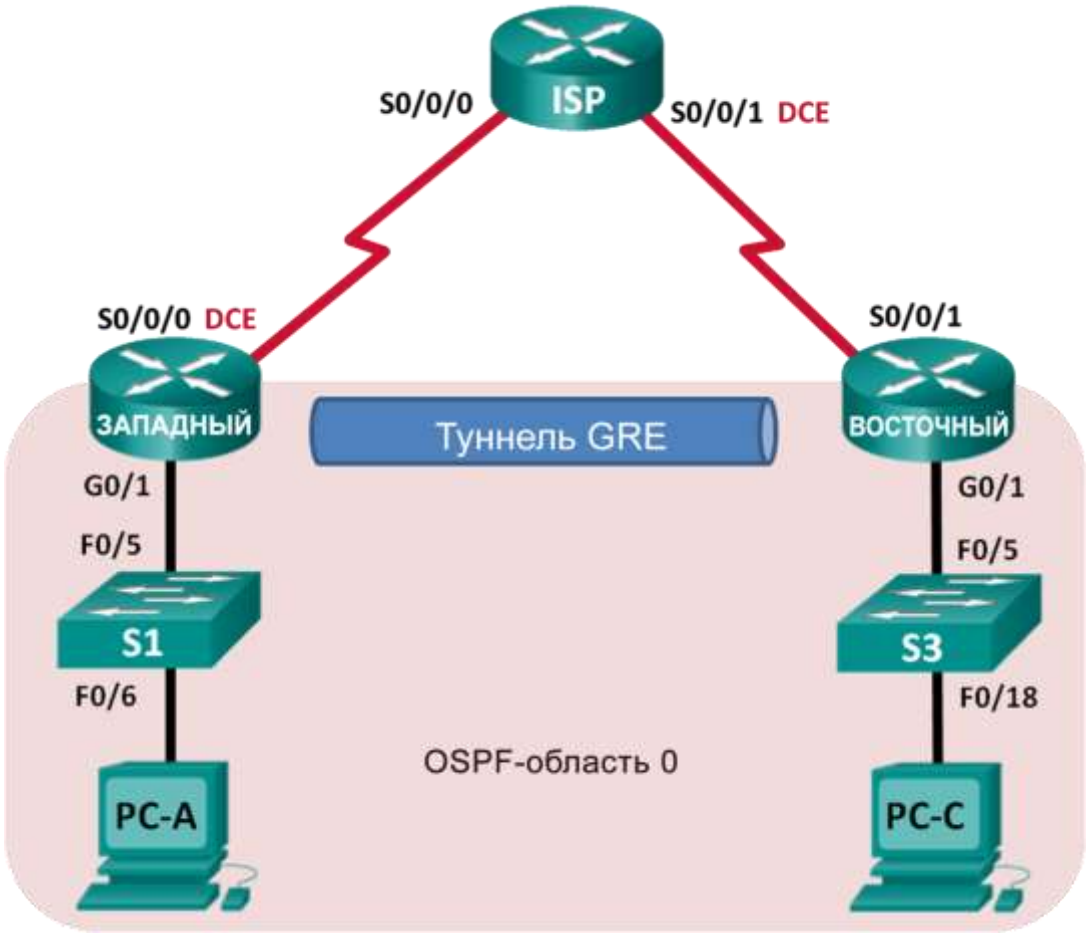


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
WEST	G0/1	172.16.1.1	255.255.255.0	Н/Д (недоступно)
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/Д (недоступно)
	Tunnel0	172.16.12.1	255.255.255.252	Н/Д (недоступно)
ISP	S0/0/0	10.1.1.2	255.255.255.252	Н/Д (недоступно)
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/Д (недоступно)
EAST	G0/1	172.16.2.1	255.255.255.0	Н/Д (недоступно)
	S0/0/1	10.2.2.1	255.255.255.252	Н/Д (недоступно)
	Tunnel0	172.16.12.2	255.255.255.252	Н/Д (недоступно)
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка туннеля GRE

Часть 3. Организация маршрутизации по туннелю GRE

Общие сведения/сценарий

Универсальная инкапсуляция при маршрутизации (GRE) — это протокол туннелирования, способный инкапсулировать различные протоколы сетевого уровня между двумя объектами по общедоступной сети, например, в Интернете.

GRE можно использовать в следующих ситуациях:

- подключение сети IPv6 по сетям IPv4;
- многоадресная рассылка пакетов, например OSPF и EIGRP, а также потоковая передача данных.

В этой лабораторной работе необходимо настроить незашифрованный туннель GRE VPN «точка-точка» и убедиться, что сетевой трафик использует туннель. Также будет нужно настроить протокол маршрутизации OSPF внутри туннеля GRE VPN. Туннель GRE существует между маршрутизаторами WEST и EAST в области 0 OSPF. Интернет-провайдер не знает о туннеле GRE. Для связи между маршрутизаторами WEST и EAST и интернет-провайдером применяются статические маршруты по умолчанию.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4)M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(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. Точные идентификаторы интерфейсов 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.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)

- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (Windows и программа эмуляции терминала, такая как Tera Term)
- Консольные кабели для настройки устройств на базе Cisco IOS через консольные порты
- Кабели Ethernet и последовательные кабели в соответствии с топологией

Часть 1: Настройка основных параметров устройств

В части 1 вам предстоит настроить топологию сети и базовые параметры маршрутизатора, например, IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели сети согласно приведенной топологии.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите DNS-поиск.

b. Назначьте имена устройств.

c. Зашифруйте незашифрованные пароли.

d. Создайте объявление дня (MOTD), предупреждающее пользователей, что несанкционированный доступ запрещен.

e. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте ведение журнала консоли в синхронном режиме.

h. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и включите физические интерфейсы. На данном этапе не настраивайте интерфейсы Tunnel0.

i. Настройте тактовую частоту **128 000** для всех последовательных интерфейсов DCE.

Шаг 4: Настройте маршруты по умолчанию к маршрутизатору интернет-провайдера.

```
WEST(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

EAST(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

Шаг 5: Настройте компьютеры.

Назначьте компьютерам IP-адреса и шлюзы по умолчанию в соответствии с таблицей адресации.

Шаг 6: Проверьте подключение.

На данный момент компьютеры не могут отправлять друг другу ping-запросы. Каждый ПК должен получать ответ на ping-запрос от своего шлюза по умолчанию. Маршрутизаторы могут получать ответы на ping-запросы на последовательные интерфейсы других маршрутизаторов в топологии. Если это не так, найдите и устраните все неполадки и убедитесь в наличии подключения.

Шаг 7: Сохраните текущую конфигурацию.

Часть 2: Настройка туннеля GRE

В части 2 необходимо настроить туннель GRE между маршрутизаторами WEST и EAST.

Шаг 1: Настройка интерфейса туннеля GRE.

a. Настройте интерфейс туннеля на маршрутизаторе WEST. В качестве интерфейса источника туннеля используйте S0/0/0 на маршрутизаторе WEST, а в качестве адреса назначения туннеля используйте 10.2.2.1 на маршрутизаторе EAST.

```
WEST(config)# interface tunnel 0
WEST(config-if)# ip address 172.16.12.1 255.255.255.252
WEST(config-if)# tunnel source s0/0/0
WEST(config-if)# tunnel destination 10.2.2.1
```

b. Настройте интерфейс туннеля на маршрутизаторе EAST. В качестве интерфейса источника туннеля используйте S0/0/1 на маршрутизаторе EAST, а в качестве адреса назначения туннеля используйте 10.1.1.1 на маршрутизаторе WEST.

```
EAST(config)# interface tunnel 0
EAST(config-if)# ip address 172.16.12.2 255.255.255.252
EAST(config-if)# tunnel source 10.2.2.1
EAST(config-if)# tunnel destination 10.1.1.1
```

Примечание. Для команды **tunnel source** в качестве источника можно использовать имя интерфейса или IP-адрес.

Шаг 2: Убедитесь, что туннель GRE работает.

a. Проверьте состояние интерфейса туннеля на маршрутизаторах WEST и EAST.

```
WEST# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down
down
GigabitEthernet0/0         unassigned      YES unset  administratively down
down
GigabitEthernet0/1         172.16.1.1      YES manual up                    up
Serial0/0/0                10.1.1.1        YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down
down
Tunnel0                    172.16.12.1     YES manual up                    up

EAST# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down
down
GigabitEthernet0/0         unassigned      YES unset  administratively down
down
GigabitEthernet0/1         172.16.2.1      YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down
down
Serial0/0/1                10.2.2.1        YES manual up                    up
Tunnel0                    172.16.12.2     YES manual up                    up
```

b. С помощью команды **show interfaces tunnel 0** проверьте протокол туннелирования, источник туннеля и назначение туннеля, используемые в этом туннеле.

Какой протокол туннелирования используется? Какие IP-адреса источника и назначения туннеля связаны с туннелем GRE на каждом маршрутизаторе?

c. Отправьте ping-запрос по туннелю из маршрутизатора WEST на маршрутизатор EAST с использованием IP-адреса интерфейса туннеля.

```
WEST# ping 172.16.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms
```

d. С помощью команды **traceroute** на маршрутизаторе WEST определите путь к интерфейсу туннеля на маршрутизаторе EAST. Укажите путь до маршрутизатора EAST.

e. Отправьте ping-запрос и выполните трассировку маршрута через туннель от маршрутизатора EAST к маршрутизатору WEST с использованием IP-адреса интерфейса туннеля.

Укажите путь от маршрутизатора EAST до маршрутизатора WEST.

С какими интерфейсами связаны эти IP-адреса? Поясните ответ.

f. Команды **ping** и **traceroute** должны успешно выполняться. Если это не так, устраните неполадки и перейдите к следующей части.

Часть 3: Включение маршрутизации через туннель GRE

В части 3 необходимо настроить протокол маршрутизации OSPF таким образом, чтобы локальные сети (LAN) на маршрутизаторах WEST и EAST могли обмениваться данными с помощью туннеля GRE.

После установления туннеля GRE можно реализовать протокол маршрутизации. Для туннелирования GRE вместо сети, связанной с последовательным интерфейсом, сетевая инструкция будет включать IP-сеть туннеля, так же как в случае с другими интерфейсами, например Serial и Ethernet. Следует помнить, что маршрутизатор ISP в этом процессе маршрутизации не участвует.

Шаг 1: Настройка маршрутизации по протоколу OSPF для области 0 по туннелю.

a. Настройте процесс протокола OSPF с идентификатором 1 в области 0 на маршрутизаторе WEST для сетей 172.16.1.0/24 и 172.16.12.0/24.

```
WEST(config)# router ospf 1
WEST(config-router)# network 172.16.1.0 0.0.0.255 area 0
WEST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

b. Настройте процесс протокола OSPF с идентификатором 1 в области 0 на маршрутизаторе EAST для сетей 172.16.2.0/24 и 172.16.12.0/24.

```
EAST(config)# router ospf 1
EAST(config-router)# network 172.16.2.0 0.0.0.255 area 0
EAST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

Шаг 2: Проверка маршрутизации OSPF.

a. Выполните команду **show ip route** на маршрутизаторе WEST, чтобы проверить маршрут к 172.16.2.0/24 LAN на маршрутизаторе EAST.

```
WEST# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

```
Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.1.1.2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/1
L        172.16.1.1/32 is directly connected, GigabitEthernet0/1
O        172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0
C        172.16.12.0/30 is directly connected, Tunnel0
L        172.16.12.1/32 is directly connected, Tunnel0
```

Какой выходной интерфейс и IP-адрес используются для перехода в сеть 172.16.2.0/24?

b. Отправьте с маршрутизатора EAST команду для проверки маршрута к локальной сети 172.16.1.0/24 на маршрутизаторе WEST.

Какой выходной интерфейс и IP-адрес используются для перехода в сеть 172.16.1.0/24?

Шаг 3: Проверьте наличие сквозного соединения.

a. Выполните ping-запрос от PC-A к PC-C. Ответы должны приходить успешно. Если это не так, найдите и устраните неполадки и убедитесь в наличии подключения между конечными узлами.

Примечание. Чтобы успешно получать ответы на ping-запросы между ПК, может потребоваться отключить межсетевой экран.

b. Выполните трассировку маршрута от PC-A к PC-C. Укажите путь от PC-A до PC-C.

Вопросы для повторения

1. Какие еще настройки необходимы для создания защищенного туннеля GRE?
2. Если вы добавили дополнительные локальные сети к маршрутизатору WEST или EAST, то что нужно сделать, чтобы сеть для передачи трафика использовала туннель GRE?

Лабораторная работа 4

Лабораторная работа. Настройка и проверка eBGP

Топология

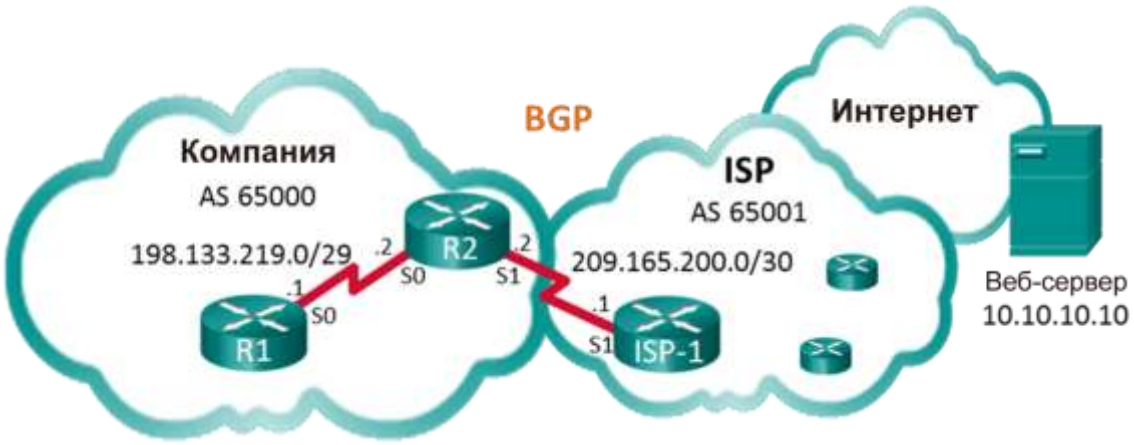


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
R1	S0/0/0 (DCE)	198.133.219.1	255.255.255.248
R2	S0/0/0	198.133.219.2	255.255.255.248
	S0/0/1 (DCE)	209.165.200.2	255.255.255.252
Провайдер 1	S0/0/1	209.165.200.1	255.255.255.252
Веб-сервер		10.10.10.10	255.255.255.255

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Настройка eBGP на маршрутизаторе R1

Часть 3. Проверка конфигурации eBGP

Общие сведения/сценарий

В этой лабораторной работе вы настроите протокол eBGP для сети вашей компании. Маршрут в Интернет по умолчанию предоставит интернет-провайдер. После завершения настройки вы будете использовать различные команды **show**, чтобы убедиться, что конфигурация eBGP работает должным образом.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)
- Консольные кабели для настройки устройств на базе Cisco IOS через консольные порты
- последовательные кабели в соответствии с топологией.

Часть 1: Создание сети и настройка основных параметров устройства

В части 1 вам предстоит настроить топологию сети и базовые параметры маршрутизаторов R1 и R2. Вы также скопируете предоставленную конфигурацию для Провайдер 1 на этот маршрутизатор.

Шаг 1: Подключите кабели сети согласно приведенной топологии.

Шаг 2: При необходимости инициализируйте и перезагрузите сетевые устройства.

Шаг 3: Настройте базовые параметры на R1 и R2.

a. Отключите DNS-поиск, чтобы предотвратить попытки маршрутизаторов неверно преобразовывать введенные команды таким образом, будто они являются именами хостов.

b. Настройте имена хостов в соответствии с топологией.

c. Настройте интерфейсы в соответствии с таблицей адресации.

d. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Скопируйте конфигурацию на Провайдер 1.

Скопируйте и вставьте следующую конфигурацию на Провайдер 1.

```
hostname Провайдер 1
no ip domain-lookup
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
interface Serial0/0/1
 ip address 209.165.200.1 255.255.255.252
 no shut
ip route 0.0.0.0 0.0.0.0 lo0
router bgp 65001
 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 209.165.200.2 remote-as 65000
end
```

Часть 2: Настройка eBGP на маршрутизаторе R2

Настройте маршрутизатор R2 таким образом, чтобы он стал одноранговым узлом eBGP для маршрутизатора Провайдер 1. Сведения о номерах автономной системы BGP см. в разделе «Топология».

Шаг 1: Включите BGP и укажите номер автономной системы компании.

```
R2(config)# router bgp 65000
```

Шаг 2: Используйте команду neighbor для идентификации Провайдер 1 как однорангового узла BGP.

```
R2(config-router)# neighbor 209.165.200.1 remote-as 65001
```

Шаг 3: Добавьте сеть компании в таблицу BGP, чтобы объявить ее для маршрутизатора Провайдер 1.

```
R2(config-router)# network 198.133.219.0 mask 255.255.255.248
```

Часть 3: Проверка конфигурации eBGP

В части 3 используйте команды проверки BGP, чтобы убедиться, что конфигурация BGP работает должным образом.

Шаг 1: Выведите на экран таблицу маршрутизации IPv4 на маршрутизаторе R2.

```
R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 209.165.200.1 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 209.165.200.1, 00:00:07
      198.133.219.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.133.219.0/29 is directly connected, Serial0/0/0
L        198.133.219.2/32 is directly connected, Serial0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/30 is directly connected, Serial0/0/1
L        209.165.200.2/32 is directly connected, Serial0/0/1
```

Шаг 2: Выведите на экран таблицу BGP на маршрутизаторе R2.

```
R2# show ip bgp
BGP table version is 4, local router ID is 209.165.200.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  0.0.0.0          209.165.200.1            0             0 65001 i
 *>  198.133.219.0/29 0.0.0.0                  0         32768 i
```

Шаг 3: Выведите состояние подключения BGP на маршрутизаторе R2.

```
R2# show ip bgp summary
BGP router identifier 209.165.200.2, local AS number 65000
BGP table version is 4, main routing table version 4
2 network entries using 288 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 320 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 792 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs
```

```
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
209.165.200.1   4        65001      12      11        4    0    0 00:06:56
1
```

Шаг 4: Выведите на экран таблицу маршрутизации IPv4 на маршрутизаторе Провайдер 1.

Убедитесь, что сеть 198.133.218.0/29 объявлена на маршрутизаторе Провайдер 1.

```
Провайдер 1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Loopback0
      10.0.0.0/32 is subnetted, 1 subnets
C        10.10.10.10 is directly connected, Loopback0
      198.133.219.0/29 is subnetted, 1 subnets
B        198.133.219.0 [20/0] via 209.165.200.2, 00:00:25
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/30 is directly connected, Serial0/0/1
L        209.165.200.1/32 is directly connected, Serial0/0/1
```

Выполните ping-запрос к веб-серверу с R1. Успешно ли выполнена проверка связи?

Вопросы для повторения

Топология, используемая в этой лабораторной работе, была создана, чтобы продемонстрировать, как настроить протокол маршрутизации BGP. В реальных сетях протокол BGP для такой топологии обычно не настраивается. Поясните ответ.

Лабораторная работа. 5

Лабораторная работа. Настройка подключения к филиалу

Топология

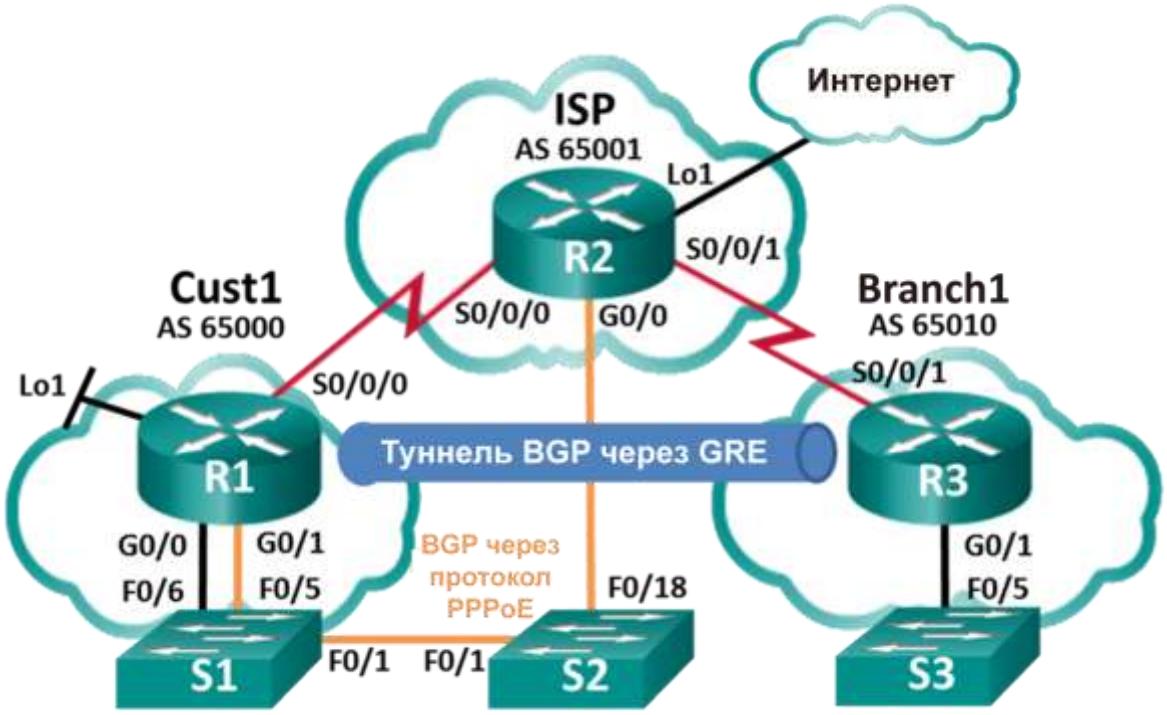


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
R1	G0/0	192.168.1.1	255.255.255.0
	G0/1	PPPoE Client	
	Lo1	209.165.200.49	255.255.255.240
	S0/0/0 (DCE)	209.165.200.81	255.255.255.252
R2	G0/0	PPPoE Provider	
	Lo1	209.165.200.65	255.255.255.240
	S0/0/0	209.165.200.82	255.255.255.252
	S0/0/1 (DCE)	209.165.200.85	255.255.255.252
R3	G0/1	192.168.3.1	255.255.255.0
	S0/0/1 (DCE)	209.165.200.86	255.255.255.252

Задачи

Часть 1. Построение сети и загрузка настроек устройств

Часть 2. Настройка подключения клиента по протоколу PPPoE

Часть 3. Настройка туннеля GRE

Часть 4. Настройка BGP по протоколу PPPoE и BGP по туннелю GRE

Общие сведения/сценарий

В этой лабораторной работе вы будете настраивать два отдельных WAN-соединения: маршрут BGP через соединение по протоколу PPPoE и маршрут BGP по туннелю GRE. Эта лабораторная работа является тестовым сценарием и не соответствует реальным реализациям BGP.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (образ universalk9). Допускается использование маршрутизаторов других моделей, а также других версий операционной системы 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. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов удалены, и на них отсутствуют файлы загрузочной конфигурации. Если вы не уверены, обратитесь к инструктору.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 3 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet и последовательные кабели, как указано в топологии

Часть 1: Построение сети и загрузка настроек устройств

Шаг 1: Создайте сеть согласно топологии.

Шаг 2: Загрузите настройки маршрутизатора.

Скопируйте и вставьте следующие конфигурации на соответствующие маршрутизаторы и коммутатор.

Конфигурация Cust 1 (R1):

```
conf t
hostname Cust1
no cdp run
interface Loopback1
 ip address 209.165.200.49 255.255.255.240
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shut
interface Serial0/0/0
 ip address 209.165.200.81 255.255.255.252
 no shut
ip route 0.0.0.0 0.0.0.0 s0/0/0 25
end
```

Примечание. В конфигурации Cust1 выше CDP отключен командой **cdp run**. Статический маршрут по умолчанию с административной дистанцией вручную изменяется на 25 вместо 1 по умолчанию. Значение этих конфигураций будет объяснено далее в лабораторной работе.

Конфигурация ISP (R2):

```
conf t
hostname ISP
username Cust1 password 0 ciscopppoe
```

```
bba-group pppoe global
 virtual-template 1
interface Loopback 1
 ip address 209.165.200.65 255.255.255.240
interface GigabitEthernet0/0
 ip tcp adjust-mss 1452
 pppoe enable group global
 no shut
interface Serial0/0/0
 ip address 209.165.200.82 255.255.255.252
 no shut
interface Serial0/0/1
 ip address 209.165.200.85 255.255.255.252
 no shut
interface Virtual-Template1
 mtu 1492
 ip address 209.165.200.30 255.255.255.224
 peer default ip address pool PPPoEPOOL
 ppp authentication chap callin
router bgp 65001
 network 0.0.0.0
 neighbor 209.165.200.1 remote-as 65000
ip local pool PPPoEPOOL 209.165.200.1 209.165.200.20
ip route 0.0.0.0 0.0.0.0 Loopback1
end
```

Конфигурация Branch1 (R3):

```
conf t
hostname Branch1
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 no shut
interface Serial0/0/1
 ip address 209.165.200.86 255.255.255.252
 no shut
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
end
```

Конфигурация S1:

```
conf t
hostname S1
vlan 111
interface f0/6
 switchport mode access
 switchport access vlan 111
end
```

Примечание. Поскольку S1 подключается к двум отдельным сетям, G0/0 и G0/1 на маршрутизаторе Cust1, необходимо сегментировать коммутатор на две отдельные сети VLAN — в этом случае VLAN111 и VLAN1.

Шаг 3: Сохраните конфигурацию на всех настроенных маршрутизаторах и коммутаторах.

Часть 2: Настройка подключения клиента по протоколу PPPoE

В части 2 вы будете настраивать маршрутизатор Cust1 как клиент с протоколом PPPoE, следуя требованиям протокола PPPoE, указанным ниже. Конфигурация маршрутизатора интернет-провайдера уже настроена.

Требования протокола PPPoE для маршрутизатора Cust1:

- Настройте следующие параметры для **интерфейса Dialer1**:
  - **a negotiated ip address**
  - **mtu 1492**
  - **ppp encapsulation**
  - **dialer pool 1**
  - **ppp chap callin authentication**
  - **ppp chap hostname Cust1**
  - **ppp chap password ciscopppoe (unencrypted)**
- Настройте следующие параметры для **G0/1**:
  - **разрешите использование протокола pppoe по всей сети**
  - **установите максимальный размер сегмента TCP как 1452**
  - **установите пул dialer pool 1 для клиента pppoe**

Перечислите команды для настройки Cust1 как клиента с протоколом PPPoE:

Если маршрутизатор Cust1 настроен правильно, он должен получить IP-адрес от маршрутизатора интернет-провайдера. Какой IP-адрес получил Cust1 и на какой интерфейсе? Какую команду вы использовали для проверки IP-адреса и интерфейса?

Примечание. Если на интерфейсе dialer1 маршрутизатора Cust1 используется протокол CDP, может появляться следующее повторяющееся сообщение журнала: *PPP: Outbound cdp packet dropped, NCP not negotiated*. Для предотвращения этого CDP отключен по всей сети.

Часть 3: Настройка туннеля GRE

В части 3 вы будете настраивать туннель GRE между маршрутизаторами Cust1 и Branch1, следуя требованиям протокола GRE, указанным ниже.

Требования к туннелю GRE:

- Настройте следующие параметры для **интерфейса туннеля 0** на маршрутизаторах Cust1 и Branch1:
  - **IP-адреса 192.168.2.1/24 и 192.168.2.2/24 соответственно**
  - **Режим туннеля GRE по протоколу IP**
  - **Интерфейс источника туннеля и адрес назначения, используя последовательные интерфейсы**

Перечислите команды для настройки туннеля GRE между Cust1 и Branch1:

Как можно определить, что туннель создан успешно? Какую команду можно использовать для проверки настройки туннеля?

Что бы изменилось, если бы на Cust1 не был настроен статический маршрут по умолчанию? Проверьте это, удалив статический маршрут по умолчанию. Расскажите о полученном результате. Перед выполнением следующего задания замените статический маршрут по умолчанию, как показано в конфигурации Cust1 в части 1, шаг 2.

Часть 4: Настройка BGP по протоколу PPPoE и BGP по туннелю GRE

В части 4 вы будете настраивать протокол BGP между маршрутизаторами Cust1 и Branch1, следуя требованиям BGP, указанным ниже. Конфигурация маршрутизатора интернет-провайдера уже настроена.

Требования BGP

- На Cust1 сделайте следующее.
  - **Создайте процесс маршрутизации AS 65000 по протоколу BGP.**
  - **Объявите сети, подключенные к Loopback 1 и G0/0.**
  - **Настройте соседние устройства BGP для соединения с маршрутизаторами ISP и Branch1.**
- На Branch1:
  - **Создайте процесс маршрутизации AS 65000 по протоколу BGP.**
  - **Объявите сеть, подключенную к G0/1.**
  - **Настройте соседнее устройство BGP только для соединения с Cust1.**

Перечислите команды для настройки BGP на Cust1 и Branch1.

Вы получили консольные сообщения на маршрутизаторе Cust1 о соединении соседнего устройства BGP с ISP и Branch1?

Можно ли с маршрутизатора Cust1 отправить эхо-запрос на адрес 209.165.200.30 маршрутизатора ISP по протоколу PPPoE? Проходит ли эхо-запрос на адрес 192.168.3.1 локальной сети Branch1?

Посмотрите таблицу маршрутизации для маршрутизатора Cust1. Какие маршруты принадлежат BGP? Должен присутствовать маршрут, полученный как от ISP, так и от Branch1.

В таблице маршрутизации Cust1 найдите два маршрута, полученные по протоколу BGP. Какую информацию они сообщают о текущих маршрутах сети?

Лабораторная работа 6

Настройка и проверка расширенных списков контроля доступа

Топология

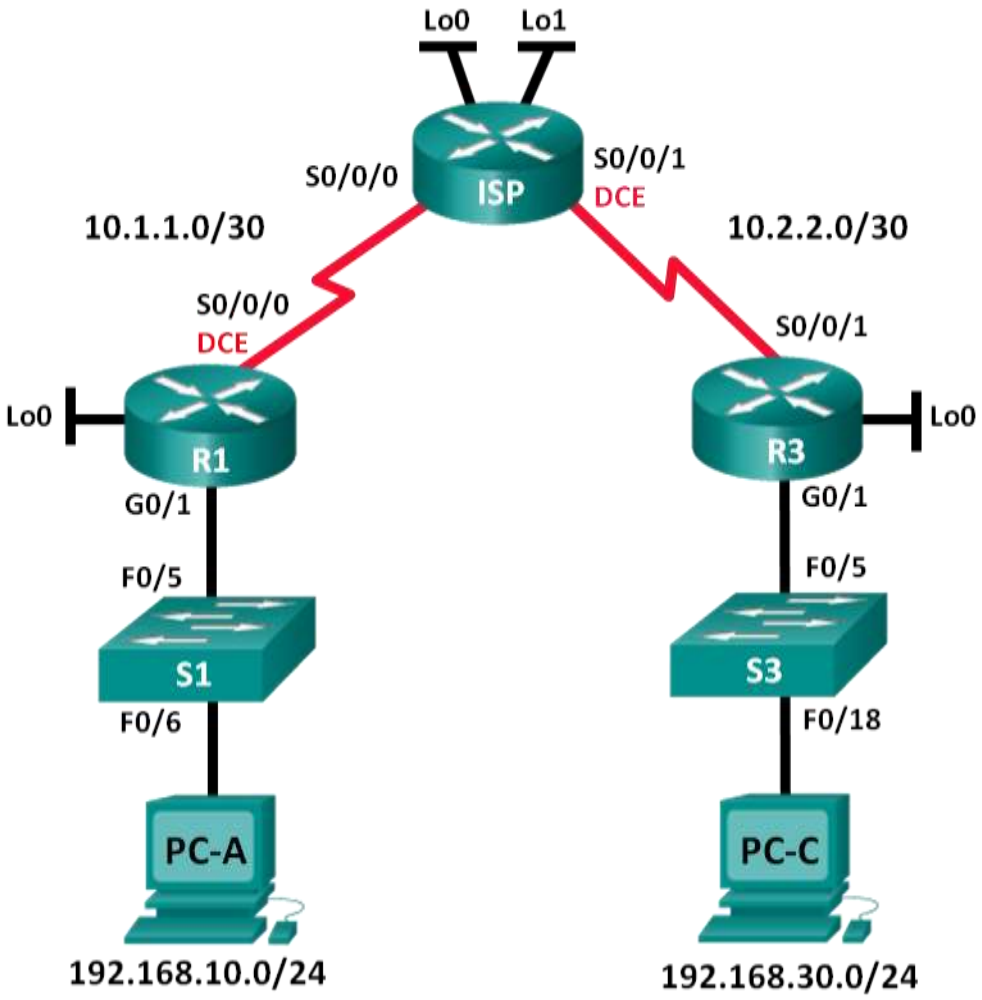


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.10.1	255.255.255.0	Н/Д (недоступно)
	Lo0	192.168.20.1	255.255.255.0	Н/Д (недоступно)
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/Д (недоступно)
ISP	S0/0/0	10.1.1.2	255.255.255.252	Н/Д (недоступно)
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/Д (недоступно)
	Lo0	209.165.200.225	255.255.255.224	Н/Д (недоступно)
	Lo1	209.165.201.1	255.255.255.224	Н/Д (недоступно)
R3	G0/1	192.168.30.1	255.255.255.0	Н/Д (недоступно)
	Lo0	192.168.40.1	255.255.255.0	Н/Д (недоступно)
	S0/0/1	10.2.2.1	255.255.255.252	Н/Д (недоступно)
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Задачи

Часть 1. Настройка топологии и инициализация устройств

Часть 2. Настройка устройств и проверка подключения

- Настройте базовые параметры на компьютерах, маршрутизаторах и коммутаторах.
- Настройте маршрутизацию протокола OSPF на R1, ISP и R3.

Часть 3. Настройка и проверка расширенных нумерованных и именованных списков контроля доступа

- Настройте, примените и проверьте нумерованные расширенные списки контроля доступа.
- Настройте, примените и проверьте именованные расширенные списки контроля доступа.

Часть 4. Изменение и проверка расширенных списков контроля доступа

Общие сведения/сценарий

Расширенные списки контроля доступа (ACL) очень эффективны. Они предлагают более высокий уровень управления, чем стандартные списки контроля доступа, как по отношению к типам фильтруемого трафика, так и к тому, где трафик создан и куда он направлен.

В данной лабораторной работе вы настроите правила фильтрации для двух офисов, представленных маршрутизаторами R1 и R3. Руководство определило некоторые правила в рамках политики безопасности для сетей LAN, расположенных на маршрутизаторах R1 и R3, которые вы должны реализовать. На маршрутизаторе интернет-провайдера, расположенном между R1 и R3, не настроены списки контроля доступа. У вас не будет прав административного доступа к маршрутизатору ISP, поскольку вы можете управлять только собственным оборудованием.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4)M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(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.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (Windows 7, Vista или XP с программой эмуляции терминала, например, Tera Term)
- Консольные кабели для настройки устройств на базе Cisco IOS через консольные порты
- Кабели Ethernet и последовательные кабели в соответствии с топологией

Часть 1: Настройка топологии и инициализация устройств

В первой части вам предстоит создать топологию сети и при необходимости удалить все конфигурации.

Шаг 1: Подключите кабели сети согласно приведенной топологии.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Часть 2: Настройка устройств и проверка подключения

Во второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров. Имена и адреса устройств указаны в топологии и таблице адресации.

Шаг 1: Настройте IP-адреса на PC-A и PC-C.

Шаг 2: Настройте базовые параметры на маршрутизаторе R1.

a. Отключите DNS-поиск.

b. Настройте имена устройств в соответствии с приведенной топологией.

c. Создайте интерфейс loopback на маршрутизаторе R1.

d. Настройте IP-адреса интерфейса в соответствии с таблицей «Топология и адресация».

e. Установите пароль **class** для доступа к привилегированному режиму EXEC.

f. Назначьте интерфейсу S0/0/0 тактовую частоту **128 000**.

g. Назначьте **cisco** в качестве пароля консоли и VTY и включите доступ по протоколу Telnet. Настройте **logging synchronous** для консоли и каналов vty.

h. Включите доступ в Интернет на маршрутизаторе R1, чтобы смоделировать веб-сервер с локальной аутентификацией для пользователя **admin**.

```
R1(config)# ip http server
R1(config)# ip http authentication local
R1(config)# username admin privilege 15 secret class
```

Шаг 3: Настройте базовые параметры на ISP.

a. Настройте имена устройств в соответствии с приведенной топологией.

b. Создайте интерфейсы loopback на ISP.

c. Настройте IP-адреса интерфейса в соответствии с таблицей «Топология и адресация».

d. Отключите DNS-поиск.

e. Назначьте **class** в качестве пароля доступа к привилегированному режиму EXEC.

f. Назначьте интерфейсу S0/0/1 тактовую частоту **128 000**.

g. Назначьте **cisco** в качестве пароля консоли и VTY и включите доступ по протоколу Telnet. Настройте **logging synchronous** для консоли и каналов vty.

h. Включите доступ в Интернет на ISP. Используйте те же параметры, что и на шаге 2h.

Шаг 4: Настройте базовые параметры на маршрутизаторе R3.

a. Настройте имена устройств в соответствии с приведенной топологией.

b. Создайте интерфейс loopback на маршрутизаторе R3.

c. Настройте IP-адреса интерфейса в соответствии с таблицей «Топология и адресация».

d. Отключите DNS-поиск.

e. Назначьте **class** в качестве пароля доступа к привилегированному режиму EXEC.

f. Назначьте **cisco** в качестве пароля консоли и настройте **logging synchronous** на канале консоли.

g. Включите SSH на S3.

```
R3(config)# ip domain-name cisco.com
R3(config)# crypto key generate rsa modulus 1024
R3(config)# line vty 0 4
R3(config-line)# login local
R3(config-line)# transport input ssh
```

h. Включите доступ в Интернет на R3. Используйте те же параметры, что и на шаге 2h.

Шаг 5: Настройте базовые параметры на коммутаторах S1 и S3 (дополнительно).

a. Настройте имена хостов в соответствии с топологией.

b. Настройте IP-адреса интерфейса управления в соответствии с таблицей «Топология и адресация».

c. Отключите DNS-поиск.

d. Установите пароль **class** для доступа к привилегированному режиму EXEC.

e. Настройте адрес основного шлюза.

Шаг 6: Настройте маршрутизацию протокола OSPF на R1, ISP и R3.

a. Назначьте 1 в качестве идентификатора процесса OSPF и объявите все сети на маршрутизаторах R1, ISP и R3. Конфигурация OSPF для R1 включена для справки.

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.10.0 0.0.0.255 area 0
R1(config-router)# network 192.168.20.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

b. После настройки OSPF на маршрутизаторах R1, ISP и R3 убедитесь, что их таблицы маршрутизации включают все сети. В случае необходимости выполните поиск и устранение неполадок.

Шаг 7: Проверьте наличие подключения между всеми устройствами.

Примечание. Наличие соединения важно проверять **перед** настройкой и применением списков контроля доступа! Прежде чем приступить к фильтрации трафика, проверьте работоспособность сети.

a. От узла PC-A отправьте ping-запросы на PC-C, интерфейс loopback и последовательные интерфейсы на маршрутизаторе R3.

   Успешно ли выполнена проверка связи? _____

b. От маршрутизатора R1 отправьте ping-запросы на PC-C, интерфейс loopback и последовательный интерфейс на маршрутизаторе R3.

   Успешно ли выполнена проверка связи? _____

c. От узла PC-C отправьте ping-запросы на PC-A, интерфейс loopback и последовательный интерфейс на маршрутизаторе R1.

   Успешно ли выполнена проверка связи? _____

d. От маршрутизатора R3 отправьте ping-запросы на PC-A, интерфейс loopback и последовательный интерфейс на маршрутизаторе R1.

e. Успешно ли выполнена проверка связи? _____

f. От узла PC-A отправьте ping-запросы на интерфейсы loopback на маршрутизаторе интернет-провайдера.

g. Успешно ли выполнена проверка связи? _____

h. От узла PC-C отправьте ping-запросы на интерфейсы loopback на маршрутизаторе интернет-провайдера.

i. Успешно ли выполнена проверка связи? _____

j. Откройте веб-браузер на узле PC-A и перейдите по адресу http://209.165.200.225 на маршрутизаторе ISP. Появится окно с запросом имени пользователя и пароля. Используйте имя пользователя admin и пароль class. Если будет предложено принять подпись, сделайте это. В отдельном окне маршрутизатор загрузит приложение Cisco Configuration Professional (CCP) Express. Возможно, появится запрос на ввод имени пользователя и пароля. Используйте имя пользователя admin и пароль class.

k. Откройте веб-браузер на узле PC-C и перейдите по адресу http://10.1.1.1 на маршрутизаторе R1. Появится окно с запросом имени пользователя и пароля. Используйте admin как имя пользователя и class как пароль. Если будет предложено принять подпись, сделайте это. В отдельном окне маршрутизатор загрузит приложение CCP Express. Возможно, появится запрос на ввод имени пользователя и пароля. Используйте имя пользователя admin и пароль class.

Часть 3: Настройка и проверка расширенных нумерованных и именованных списков контроля доступа

Расширенные списки контроля доступа позволяют фильтровать трафик различными способами. Расширенные списки контроля доступа позволяют фильтровать трафик на основе IP-адреса отправителя, порта отправителя, IP-адреса назначения, порта назначения, а также на основе различных протоколов и сервисов.

Данные списки контроля доступа работают в соответствии со следующими политиками безопасности:

1. Разрешать доступ веб-трафика из сети 192.168.10.0/24 в любую сеть.
2. Разрешать подключение SSH к последовательному интерфейсу R3 от узла PC-A.
3. Разрешать пользователям в сети 192.168.10.0/24 сетевой доступ к сети 192.168.20.0/24.
4. Разрешать доступ веб-трафика из сети 192.168.30.0/24 к маршрутизатору R1 через веб-интерфейс и сеть интернет-провайдера 209.165.200.224/27. Доступ сети 192.168.30.0/24 к какой-либо другой сети должен быть ЗАПРЕЩЕН.

Для выполнения этих политик безопасности вам потребуется как минимум два списка контроля доступа. Рекомендуется размещать расширенные списки контроля доступа как можно ближе к источнику. Мы последуем этой рекомендации для соблюдения вышеупомянутых политик безопасности.

Шаг 1: Для расширенных нумерованных списков контроля доступа на маршрутизаторе R1 настройте политики безопасности под номерами 1 и 2.

На маршрутизаторе R1 вы будете использовать нумерованный расширенный список. Укажите диапазоны для расширенных списков контроля доступа.

a. Настройте список контроля доступа на маршрутизаторе R1. В качестве номера этого списка контроля доступа используйте 100.

```
R1(config)# access-list 100 remark Allow Web & SSH Access
R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1
eq 22
R1(config)# access-list 100 permit tcp any any eq 80
```

Что означает 80 в вышеуказанных выходных данных?

На каких интерфейсах должен быть применен список контроля доступа под номером 100?

На каком направлении следует применить список контроля доступа 100?

b. Примените список контроля доступа 100 на интерфейсе S0/0/0.

```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 100 out
```

c. Проверьте работу списка контроля доступа 100.

1) Откройте веб-браузер на узле PC-A и проверьте доступ к http://209.165.200.225 (маршрутизатор ISP). Вход должен быть выполнен успешно. В ином случае выполните поиск и устранение неполадок.

2) Установите SSH-подключение от узла PC-A к маршрутизатору R3, используя 10.2.2.1 в качестве IP-адреса. Войдите в систему, используя учетные данные **admin** и **class**. Вход должен быть выполнен успешно. В ином случае выполните поиск и устранение неполадок.

3) Из командной строки привилегированного режима EXEC на маршрутизаторе R1 выполните команду **show access-lists**.

```
R1# show access-lists
Extended IP access list 100
    10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)
    20 permit tcp any any eq www (111 matches)
```

4) Из командной строки узла PC-A выполните ping-запрос на адрес 10.2.2.1. Объясните полученные результаты.

Шаг 2: Настройте именованный расширенный список контроля доступа на маршрутизаторе R3 для соблюдения политики безопасности под номером 3.

a. Настройте политику безопасности на маршрутизаторе R3. Присвойте списку контроля доступа имя WEB-POLICY.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq
80
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224
0.0.0.31 eq 80
```

b. Примените список контроля доступа WEB-POLICY на интерфейсе S0/0/1.

```
R3(config-ext-nacl)# interface S0/0/1
R3(config-if)# ip access-group WEB-POLICY out
```

c. Проверьте работу списка контроля доступа WEB-POLICY.

1) Из командной строки привилегированного режима EXEC маршрутизатора R3 выполните команду **show ip interface s0/0/1**.

Укажите имя списка контроля доступа (если имеется).

На каком направлении применен список контроля доступа? Откройте веб-браузер на узле PC-C и получите доступ к http://209.165.200.225 (маршрутизатор ISP). Вход должен быть выполнен успешно. В ином случае выполните поиск и устранение неполадок.

2) На узле PC-C откройте веб-сеанс на адрес http://10.1.1.1 (R1). Вход должен быть выполнен успешно. В ином случае выполните поиск и устранение неполадок.

3) На узле PC-C откройте веб-сеанс на адрес http://209.165.201.1 (маршрутизатор ISP). Вход не должен быть выполнен. В ином случае выполните поиск и устранение неполадок.

4) Из командной строки узла PC-C отправьте ping-запрос к PC-A. Какой получен результат и почему?

Часть 4: Изменение и проверка расширенных списков контроля доступа

Вследствие применения списков контроля доступа на маршрутизаторах R1 и R3 ни ping-запросы, ни какие-либо другие виды трафика не могут проходить между локальными сетями на маршрутизаторах R1 и R3. Руководство решило разрешить весь трафик между сетями 192.168.10.0/24 и 192.168.30.0/24. Необходимо внести изменения в списки контроля доступа на маршрутизаторах R1 и R3.

Шаг 1: Измените список контроля доступа 100 на маршрутизаторе R1.

a. В привилегированном режиме EXEC на маршрутизаторе R1 введите команду **show access-lists**.

Сколько строк в этом списке контроля доступа? _____

b. Перейдите в режим глобальной конфигурации и измените список контроля доступа на маршрутизаторе R1.

```
R1(config)# ip access-list extended 100
R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0
0.0.0.255
R1(config-ext-nacl)# end
```

c. Введите команду **show access-lists**.

Где именно в списке контроля доступа 100 появился только что добавленный канал?

Шаг 2: Измените список контроля доступа WEB-POLICY на маршрутизаторе R3.

a. В привилегированном режиме EXEC на маршрутизаторе R3 введите команду **show access-lists**.

Сколько строк в этом списке контроля доступа? _____

b. Перейдите в режим глобальной конфигурации и измените список контроля доступа на маршрутизаторе R3.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0
0.0.0.255
R3(config-ext-nacl)# end
```

c. Выполните команду **show access-lists**, чтобы убедиться, что в конце списка контроля доступа была добавлена новая строка.

Шаг 3: Проверьте работу измененных списков контроля доступа.

a. Из узла PC-A отправьте ping-запрос на IP-адрес PC-C. Получены ли ответы на ping-запросы? _____

b. Из узла PC-C отправьте ping-запрос на IP-адрес узла PC-A. Получены ли ответы на ping-запросы? _____

Почему изменения списков контроля доступа незамедлительно подействовали на ping-запросы?

Вопросы для повторения

1. Почему необходимо тщательно планировать и проверять работу списков контроля доступа?
2. Какой тип списка контроля доступа лучше — стандартный или расширенный?
3. Почему пакеты приветствия OSPF и обновления маршрутизации не блокируются неявной записью контроля доступа (ACE) **deny any** или выражением контроля доступа в списках контроля доступа, примененных на маршрутизаторах R1 и R3?

Лабораторная работа 7

Реализация локального анализатора коммутируемых портов

Топология

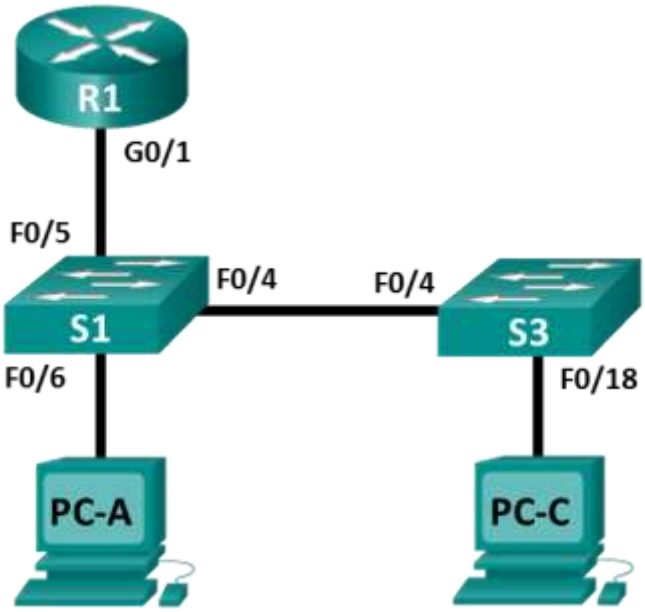


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.3	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.254	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Задачи

Часть 1. Построение сети и проверка соединения

Часть 2. Настройка локального анализатора коммутируемых портов и сбор копируемого трафика с помощью ПО Wireshark

Общие сведения/сценарий

Как сетевой администратор, вы хотите анализировать входящий и исходящий трафик локальной сети. Для этого вы настроите зеркалирование портов на коммутационном порте, подключенном к маршрутизатору, и зеркально скопируете весь трафик на другой коммутационный порт. Цель состоит в отправке зеркалированного трафика в систему обнаружения вторжений (IDS) для анализа. В этой первоначальной реализации вы будете отправлять весь зеркалированный трафик на ПК, который будет перехватывать трафик для анализа, используя программу прослушивания портов. Для настройки зеркалирования портов будет использоваться функция анализатора коммутируемых портов (SPAN) на коммутаторе Cisco. Анализатор коммутируемых портов — это тип зеркалирования портов, в котором копии кадров, поступающих на порт, отправляются на другой порт того же коммутатора. Очень часто

можно найти устройство, на котором работает анализатор трафика пакетов или система обнаружения вторжений (IDS), подключенные к зеркалированному порту.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сетевыми сервисами (ISR) Cisco 1941 с операционной системой Cisco IOS версии 15.4(3) (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, а также других версий операционной системы 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. Точные идентификаторы интерфейсов 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.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.4(3) (универсальный образ) или аналогичная модель)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ 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 в соответствии с топологией.

Часть 1: Построение сети и проверка связи

В первой части вам предстоит настроить топологию сети и выполнить базовую настройку, например, IP-адреса интерфейсов, статическую маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Настройте базовые параметры этого маршрутизатора.

a. Отключите DNS-поиск.

b. Присвойте имена устройствам в соответствии с топологией.

c. Настройте IP-адрес для маршрутизатора, указанный в таблице адресации.

d. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

e. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

f. Установите режим **transport input telnet** для линий VTY.

g. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 5: Настройте базовые параметры каждого коммутатора.

a. Отключите DNS-поиск.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

d. Настройте IP-адреса для коммутаторов, указанных в таблице адресации.

e. На каждом коммутаторе настройте шлюз по умолчанию.

f. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.

g. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 6: Проверьте подключение.

a. Необходимо получать ответ на ping-запросы с компьютера PC-A от каждого интерфейса маршрутизаторов R1, S1 и S3, а также от компьютера PC-C. Удалось ли получить все ответы? _____

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

b. Необходимо получать ответ на ping-запросы с компьютера PC-C от каждого интерфейса маршрутизаторов R1, S1 и S3, а также от компьютера PC-A. Удалось ли получить все ответы? _____

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

Часть 2: Настройка локального анализатора коммутируемых портов и сбор копируемого трафика с помощью ПО Wireshark

Для настройки локального анализатора коммутируемых портов необходимо настроить один или несколько исходных зеркалированных портов и один зеркалированный порт назначения для копирования или зеркалирования трафика. Исходные порты анализатора коммутируемых портов можно настроить для мониторинга трафика на входе, на выходе или в обоих направлениях (по умолчанию).

Исходный порт анализатора коммутируемых портов необходимо настроить на порту, который подключается к маршрутизатору через порт F0/5 коммутатора S1. Таким образом будет контролироваться весь входящий и исходящий трафик локальной сети. Порт назначения анализатора коммутируемых портов будет настроен на порту F0/6 коммутатора S1, подключенном к узлу PC-A, на котором работает Wireshark.

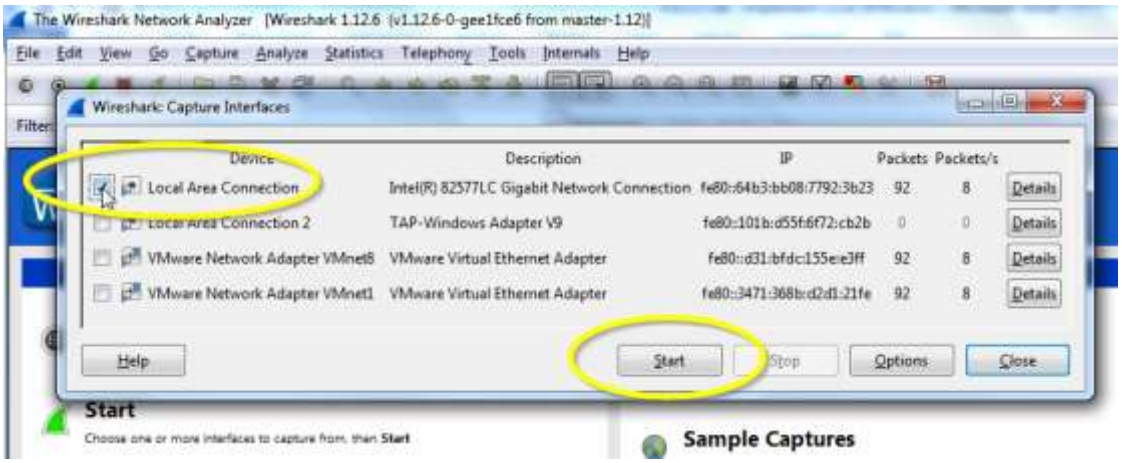
Шаг 1: Настройте анализатор коммутируемых портов на коммутаторе S1.

a. Подключитесь с консоли к S1 и настройте исходный и целевой порты мониторинга на коммутаторе S1. Теперь весь входящий и исходящий трафик на порту F0/5 будет копироваться и перенаправляться на порт F0/6.

```
S1(config)# monitor session 1 source interface f0/5
S1(config)# monitor session 1 destination interface f0/6
```

Шаг 2: Запустите сбор трафика с помощью ПО Wireshark на компьютере PC-A.

a. Откройте ПО Wireshark на компьютере PC-A, настройте для интерфейса сбора трафика подключение по локальной сети и щелкните **Start** (Начать).



Шаг 3: Подключитесь к маршрутизатору R1 по Telnet и создайте трафик ICMP в локальной сети.

a. Установите подключение по Telnet от S1 к R1.

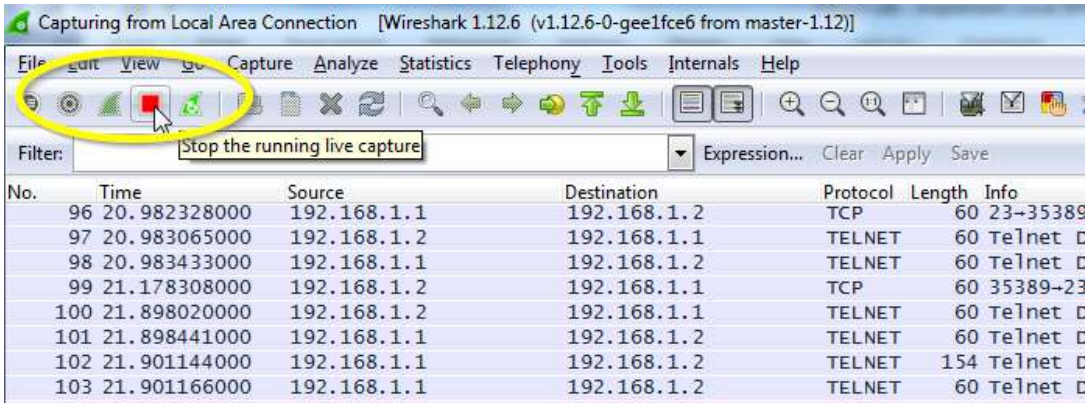
```
S1# Telnet 192.168.1.1
Trying 192.168.1.1. . . Open

User Access Verification

Password:
R1>
```

b. В привилегированном режиме отправьте эхо-запросы к PC-C, S1 и S3.

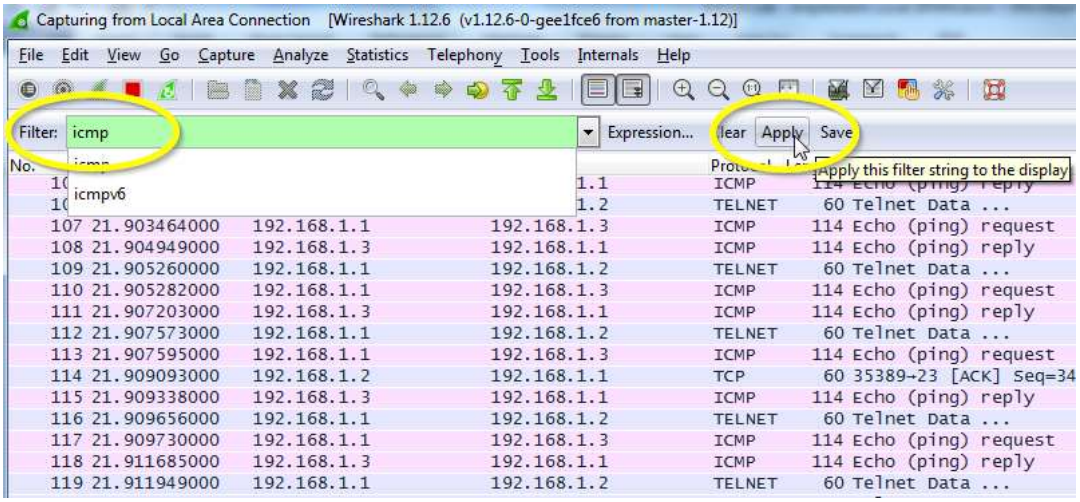
```
R1> enable
Password:
R1# ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1# ping 192.168.1.2
<Выходные данные опущены>
R1# ping 192.168.1.3
<Выходные данные опущены>
```

Шаг 4: Остановите сбор трафика с помощью Wireshark на PC-A и выполните фильтрацию трафика ICMP.

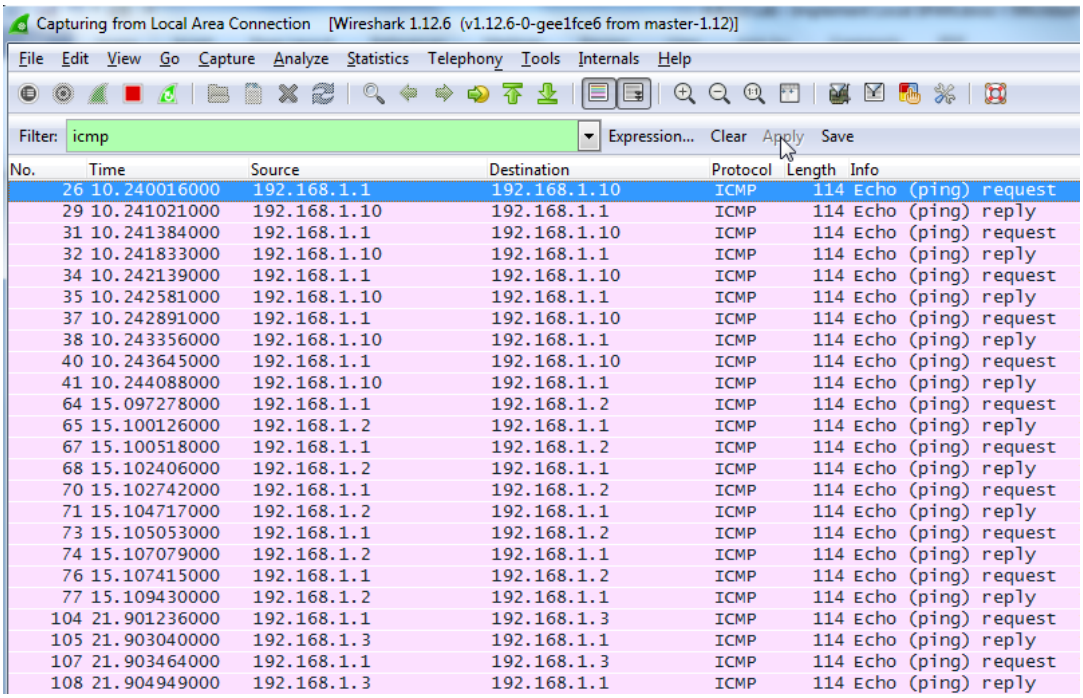
a. Вернитесь на компьютер PC-A и остановите захват трафика программой Wireshark.



b. Отфильтруйте ICMP-пакеты в трафике, собранном Wireshark.



c. Изучите отфильтрованные ICMP-пакеты в трафике, собранном Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
26	10.240016000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
29	10.241021000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
31	10.241384000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
32	10.241833000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
34	10.242139000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
35	10.242581000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
37	10.242891000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
38	10.243356000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
40	10.243645000	192.168.1.1	192.168.1.10	ICMP	114	Echo (ping) request
41	10.244088000	192.168.1.10	192.168.1.1	ICMP	114	Echo (ping) reply
64	15.097278000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
65	15.100126000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
67	15.100518000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
68	15.102406000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
70	15.102742000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
71	15.104717000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
73	15.105053000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
74	15.107079000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
76	15.107415000	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) request
77	15.109430000	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) reply
104	21.901236000	192.168.1.1	192.168.1.3	ICMP	114	Echo (ping) request
105	21.903040000	192.168.1.3	192.168.1.1	ICMP	114	Echo (ping) reply
107	21.903464000	192.168.1.1	192.168.1.3	ICMP	114	Echo (ping) request
108	21.904949000	192.168.1.3	192.168.1.1	ICMP	114	Echo (ping) reply

d. Были ли ping-запросы от R1 к PC-C, S1 и S3 успешно скопированы и перенаправлены с порта F0/6 на PC-A?

e. Выполнялся ли мониторинг и копирование трафика в обоих направлениях? Вопросы для повторения

В данном сценарии не лучше ли было использовать систему обнаружения (IDS) или предотвращения (IPS) вторжений вместо PC-A и анализатора трафика пакетов?

Приложение

СБРОС КОММУТАТОРА CISCO 2960

1. Подключиться терминалом к консольному порту со скоростью 9600
2. Выключить свитч. Отсоединить кабель питания на 15 секунд, затем включить кабель обратно и зажать на передней панели свитча кнопку "Mode" пока светодиод System мигает зеленым. Продолжать нажимать кнопку "Mode" когда светодиод System загорелся янтарным. Когда светодиод престал гореть кнопку "Mode" можно отпустить.
3. Инициализируем файловую систему на флэше командой flash_init
4. Смотрим контент флэша с помощью команды dir flash:
5. Удаляем конфигурационный файл config.text командой delete flash:config.text
6. Загружаем IOS с помощью команды boot

СБРОС МАРШРУТИЗАТОРА CISCO

1. Подключитесь к устройству
2. Включите электропитание устройства. На экране консоли вы увидите процесс начала загрузки IOS;
3. В начальный момент загрузки устройства, желательно до момента распаковки с flesh-памяти операционной системы, вам следует послать устройству сигнал Break, нажав на клавиатуре одновременно две клавиши Ctrl+Break;
4. Устройство войдет в режим ROM Monitor, о чем будет свидетельствовать приглашение:

```
rommon 1>
```

5. В этом режиме установите значение конфигурационного регистра 0x2142, при котором устройство не будет использовать при загрузке конфиг, записанный во flesh-память:

```
rommon 1> confreg 0x2142
Yuo mast reset or power cycle for new config to take effect
rommon 2>
```

6. Перезагрузите устройство:

```
rommon 2> reset
rommon 3>
```

7. После перезагрузки вашего устройства Cisco на вопрос IOS о начальном конфигурировании вам следует ответить No:

```
Would you like to enter the initial configuration dialog? [yes/no]: No
Press RETURN to get started!
Router>
```

8. Теперь Cisco позволит войти в привилегированный режим без пароля:

```
Router> enable
Router#
```

СПИСОК ЛИТЕРАТУРЫ

1. Олифер, В. Г. Компьютерные сети : принципы, технологии, протоколы: учебник для вузов/ В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб.: Питер, 2010

2. Олифер В., Олифер Н.: "Компьютерные сети", Спб: Издательство "Питер", 2010.

3. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-издание, исправленное 1168 стр., с ил.; ISBN 978-5-8459-0842-1, 1-58713-150-1; формат 70x100/16; твердый переплетCD-ROM; серия Cisco Press; 2009, 1 кв.; Вильямс

4. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство944 стр., с ил.; ISBN 978-5-8459-1120-9, 1-58-713113-7; формат 70x100/16; твердый переплет CD-ROM; 2009, 2 кв.; Вильямс.

5. Полный справочник по Cisco1088 стр., с ил.; ISBN 5-8459-0589-3, 0-07-219280-1; формат 70x100/16; твердый переплет серия Полный справочник; 2009, 1 кв.; Вильямс.

6. Руководство по Cisco IOS Питер, Русская Редакция, 2009 г.Твердый переплет, 784 стр. ISBN 978-5-469-01413-3, 5-469-01413-4, 978-5-7502-0309-3 Тираж: 2000 экз.