Лабораторная работа. Поиск и устранение неполадок в настройке и размещении ACL-списков

Топология

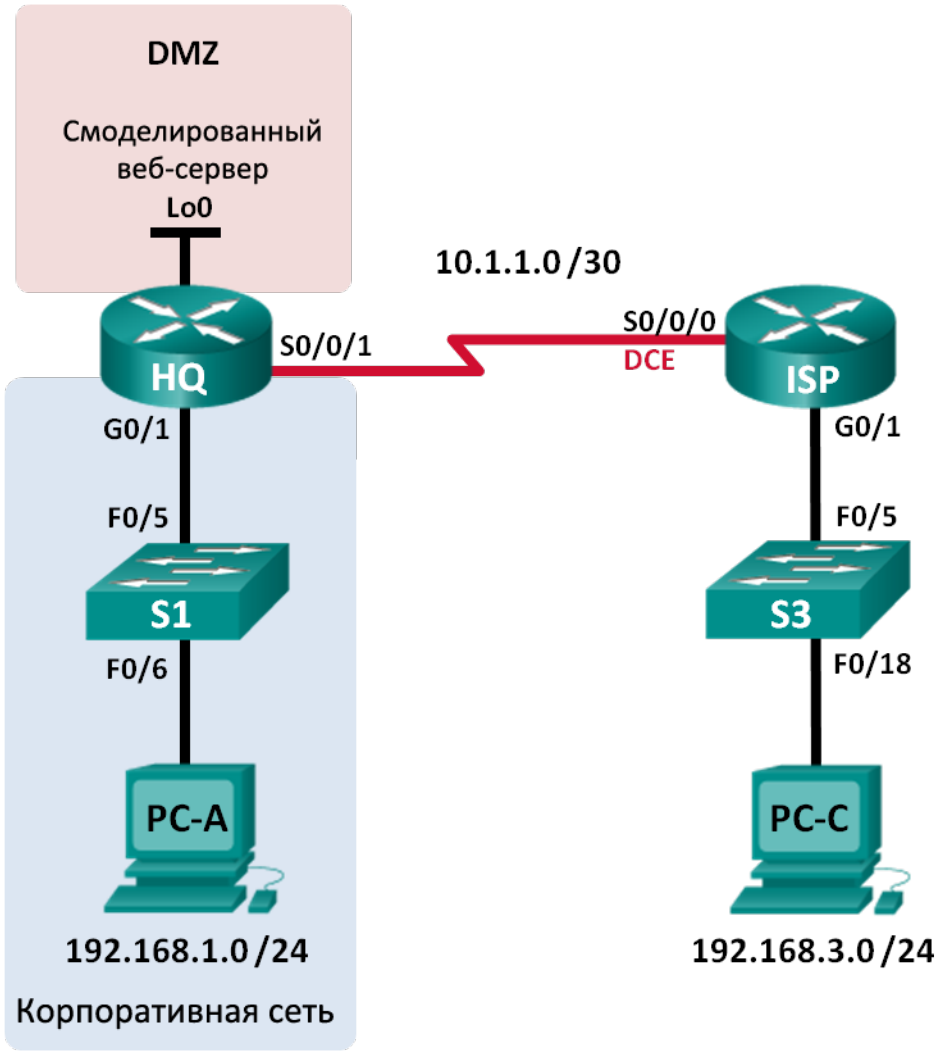

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
HQ	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	10.1.1.2	255.255.255.252	N/A
	Lo0	192.168.4.1	255.255.255.0	N/A
ISP	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
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. Построение сети и настройка базовых параметров устройства

Часть 2. Поиск и устранение неполадок внутреннего доступа

Часть 3. Поиск и устранение неполадок удалённого доступа

Исходные данные/сценарий

Список контроля доступа (ACL) — это последовательность команд IOS, обеспечивающая базовую фильтрацию трафика на маршрутизаторе Cisco. С помощью ACL-списков можно выбирать типы трафика, подлежащие обработке. Каждое отдельное выражение ACL-списка называют записью контроля доступа (ACE). Записи ACE в ACL-списках оцениваются сверху вниз. В конце списка стоит скрытая запись запрета deny all. Также ACL-списки контролируют тип трафика, входящего или исходящего из сети, используя узлы или сеть источника и назначения. Размещение ACL-списков имеет решающее значение для правильной обработки нужного трафика.

В контексте данной лабораторной работы небольшая компания только что добавила в сеть веб-сервер, чтобы клиенты могли получить доступ к конфиденциальной информации. Корпоративная сеть разделена на две зоны: зону корпоративной сети и демилитаризованную зону (DMZ). В зоне корпоративной сети будут размещены частные серверы и внутренние клиенты. В зоне DMZ содержится внешне доступный веб-сервер (смоделированный как интерфейс Lo0 в HQ). Поскольку компания может управлять только собственным маршрутизатором HQ, на нём необходимо применить все ACL-списки.

- ACL-список 101 реализован для ограничения трафика, выходящего из зоны корпоративной сети. Эта зона содержит частные сервера и внутренних клиентов (192.168.1.0/24). Доступ других сетей в корпоративную сеть должен быть закрыт.
- ACL-список 102 применяется для ограничения трафика, входящего в корпоративную сеть. Доступ в эту сеть разрешён только для ответов на запросы, созданные внутри корпоративной сети. К ним относятся TCP-запросы от внутренних узлов, например, на веб- или FTP-сервере. ICMP обладает доступом в сеть для устранения неполадок, чтобы входящие ICMP-сообщения, созданные в ответ на эхо-запросы, могли быть получены внутренними узлами.

- ACL-список 121 контролирует внешний трафик, входящий в зону DMZ и корпоративную сеть. Доступом к веб-серверу DMZ обладает только HTTP-трафик (смоделированный как интерфейс Lo0 на маршрутизаторе R1). Остальной трафик из внешних сетей, например EIGRP, разрешён. Кроме того, допустимым внутренним частным адресам, например, 192.168.1.0, loopback-адресам, например, 127.0.0.0 и групповым адресам доступ к корпоративной сети запрещён в целях предотвращения вредоносных атак со стороны внешних пользователей.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсе маршрутизатора в конце этой лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например 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 настройка базовых параметров устройства

В первой части лабораторной работы вам нужно создать топологию сети и настроить некоторые базовые параметры на маршрутизаторах и коммутаторах, например пароли и IP-адреса. В качестве исходных настроек маршрутизаторов также даны предварительные настройки. Также вам предстоит настроить параметры IP для компьютеров в приведённой топологии.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Настройте базовые параметры каждого коммутатора (дополнительно).

a. Отключите поиск DNS.

b. Настройте имена узлов в соответствии с топологией.

c. Настройте IP-адрес и шлюз по умолчанию в таблице адресации.

d. Назначьте **cisco** в качестве паролей консоли и VTY.

e. Назначьте **class** в качестве пароля привилегированного режима EXEC.

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

Шаг 5: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Настройте имена узлов в соответствии с топологией.

c. Назначьте **cisco** в качестве паролей консоли и VTY.

d. Назначьте **class** в качестве пароля привилегированного режима EXEC.

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

Шаг 6: Настройте HTTP-доступ и учётные данные пользователя на маршрутизаторе HQ.

Для получения доступа к смоделированному веб-серверу (192.168.4.1) необходимо настроить учётные данные пользователя.

```
HQ(config)# ip http server
HQ(config)# username admin privilege 15 secret adminpass
HQ(config)# ip http authentication local
```

Шаг 7: Загрузите настройки маршрутизатора.

В вашем распоряжении конфигурации для маршрутизаторов ISP и HQ. Эти настройки содержат ошибки. Ваша задача — найти ошибки и исправить их.

Маршрутизатор ISP

```
hostname ISP
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 no shutdown
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 128000
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.3.0
 no auto-summary
end
```

Маршрутизатор HQ

```
hostname HQ
interface Loopback0
 ip address 192.168.4.1 255.255.255.0
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group 101 out
 ip access-group 102 in
 no shutdown
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
```

```
 ip access-group 121 in
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0
 network 192.168.4.0
 no auto-summary
access-list 101 permit ip 192.168.11.0 0.0.0.255 any
access-list 101 deny ip any any
access-list 102 permit tcp any any established
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable
access-list 102 deny ip any any
access-list 121 permit tcp any host 192.168.4.1 eq 89
access-list 121 deny icmp any host 192.168.4.11
access-list 121 deny ip 192.168.1.0 0.0.0.255 any
access-list 121 deny ip 127.0.0.0 0.255.255.255 any
access-list 121 deny ip 224.0.0.0 31.255.255.255 any
access-list 121 permit ip any any
access-list 121 deny ip any any
end
```

Часть 2: Поиск и устранение неполадок внутреннего доступа

Во второй части нужно проверить ACL-списки на маршрутизаторе HQ, чтобы убедиться в правильности их настройки.

Шаг 1: Поиск и устранение неполадок в ACL-списке 101

ACL-список 101 реализован для ограничения трафика, выходящего из зоны корпоративной сети. В этой зоне содержатся только внутренние клиенты и частные сервера. Правом выхода из этой зоны корпоративной сети обладает только сеть 192.168.1.0/24.

a. Успешно ли проходит эхо-запрос от узла PC-A на его шлюз по умолчанию?

b. Убедившись в правильности настройки узла PC-A, просмотрите сводку ACL-списка 101, чтобы найти в конфигурации маршрутизатора HQ возможные ошибки. Введите команду **show access-lists 101.**

```
HQ# show access-lists 101
Extended IP access list 101
    10 permit ip 192.168.11.0 0.0.0.255 any
    20 deny ip any any
```

c. Удалось ли вам найти какие-либо ошибки в ACL-списке 101?

d. Проверьте интерфейс шлюза по умолчанию для сети 192.168.1.0 /24. Убедитесь, что ACL-список 101 применён на правильном направлении интерфейса G0/1. Введите **show ip interface g0/1**.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
```

```
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 101
  Inbound  access list is 102
```

Правильно ли настроено направление интерфейса G0/1 для ACL-списка 101?

e. Исправьте ошибки, найденные в ACL-списке 101, и убедитесь, что трафик из сети 192.168.1.0 /24 может покидать корпоративную сеть. Запишите команды, используемые для исправления ошибок.

f. Проверьте, успешно ли выполняется эхо-запрос с узла PC-A на интерфейс его шлюза по умолчанию.

Шаг 2: Поиск и устранение неполадок в ACL-списке 102

ACL-список 102 применяется для ограничения трафика, входящего в корпоративную сеть. Трафик, создаваемый во внешней сети, не допускается в корпоративную сеть. Удалённый трафик допускается в корпоративную сеть, если трафик был создан во внутренней сети. Ответные ICMP-сообщения допускаются в целях устранения неполадок.

a. Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-C?

b. Просмотрите сводку ACL-списка 102, чтобы найти возможные ошибки в конфигурации маршрутизатора HQ. Введите команду **show access-lists 102.**

```
HQ# show access-lists 102
Extended IP access list 102
    10 permit tcp any any established
    20 permit icmp any any echo-reply
    30 permit icmp any any unreachable
    40 deny ip any any (57 matches)
```

c. Удалось ли вам найти какие-либо ошибки в ACL-списке 102?

d. Убедитесь, что ACL-список 102 применён на правильном направлении интерфейса G0/1. Введите **show ip interface g0/1**.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
```

```
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 101
  Inbound  access list is 101
```

e. Удалось ли вам найти какие-либо ошибки в применении ACL-списка 102 на интерфейсе G0/1?

f. Устраните все ошибки в ACL-списке 102. Запишите команды, используемые для исправления ошибок.

g. Успешно ли теперь отправляется эхо-запрос от узла PC-A на узел PC-C?

Часть 3: Поиск и устранение неполадок удалённого доступа

В третьей части лабораторной работы ACL-список 121 настроен для предотвращения спуфинг-атак со стороны внешних сетей и разрешения только удалённого HTTP-доступа к веб-серверу (192.168.4.1) в зоне DMZ.

a. Проверьте настройки ACL-списка 121. Введите **show ip access-list 121**.

```
HQ# show ip access-lists 121
Extended IP access list 121
    10 permit tcp any host 192.168.4.1 eq 89
    20 deny icmp any host 192.168.4.11
    30 deny ip 192.168.1.0 0.0.0.255 any
    40 deny ip 127.0.0.0 0.255.255.255 any
    50 deny ip 224.0.0.0 31.255.255.255 any
    60 permit ip any any (354 matches)
    70 deny ip any any
```

Удалось ли вам найти какие-либо ошибки в этом ACL-списке?

b. Убедитесь, что ACL-список 121 применён на правильном направлении интерфейса S0/0/1 на маршрутизаторе R1. Введите команду **show ip interface s0/0/1**.

```
HQ# show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet address is 10.1.1.2/30
  Broadcast address is 255.255.255.255
<output omitted>
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is 121
```

Удалось ли вам найти какие-либо ошибки в применении этого ACL-списка?

c. При обнаружении ошибок внесите соответствующие изменения в конфигурацию ACL 121 и задокументируйте их.

d. Убедитесь, что через веб-браузер узел PC-C может получить доступ только к смоделированному веб-серверу на маршрутизаторе HQ. Для доступа к веб-серверу (192.168.4.1) используйте имя пользователя **admin** и пароль **adminpass**.

Вопросы на закрепление

1. В каком порядке следует указывать ACL-операторы? От общего к частному или наоборот?

2. Что произойдёт, если вы удалите ACL-список с помощью команды **no access-list**, а этот список будет по-прежнему применён на интерфейсе?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**Последовательный интерфейс №1**	**Последовательный интерфейс №2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.