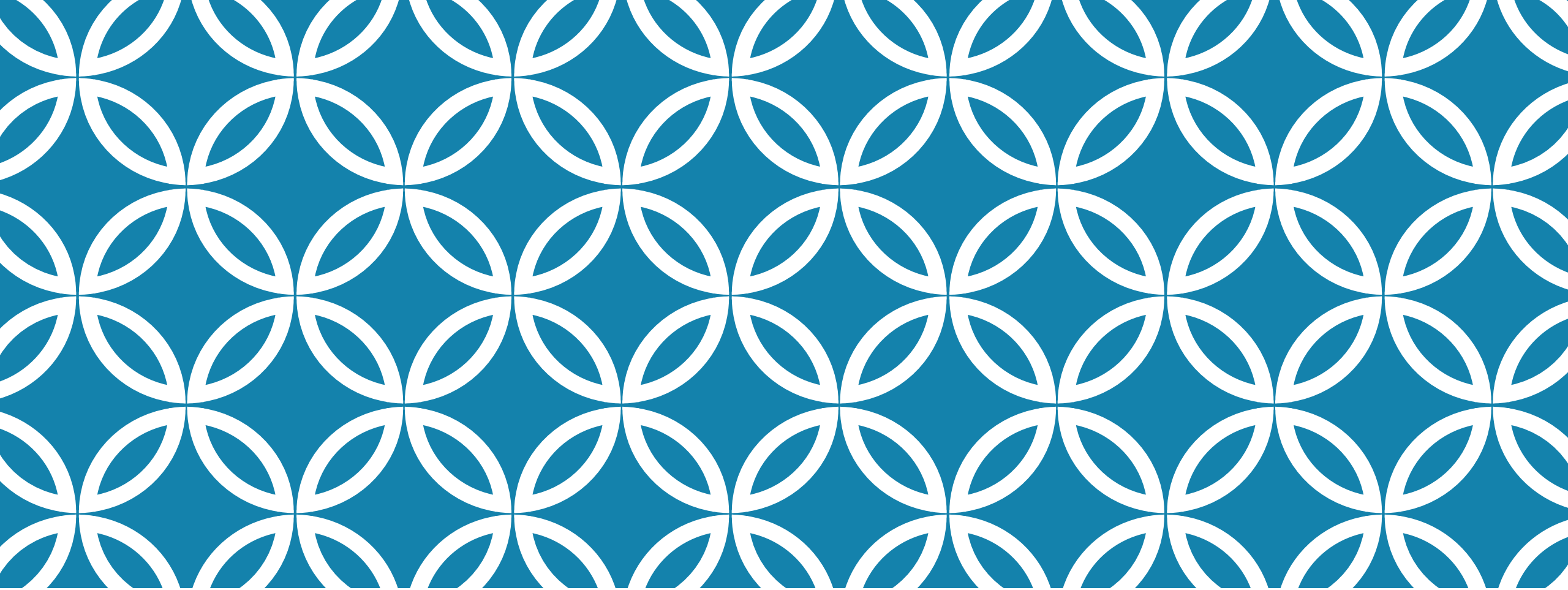


МОДУЛЬ 5. ACL ДЛЯ КОНФИГУРАЦИИ IPV4

КАФЕДРА ТЕЛЕКОММУНИКАЦИЙ

5.1 НАСТРОЙКА СТАНДАРТНЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА ДЛЯ IPV4

5.1.1 СОЗДАНИЕ ACL

Все списки управления доступом (ACL) должны быть запланированы. При настройке сложного списка ACL рекомендуется:

1. Использовать текстовый редактор и записать определенную политику, которая будет реализована.

2. Добавить команды конфигурации IOS для выполнения этих задач.

3. Включить комментарии для документирования списка ACL.

4. Скопировать и вставить команды на устройство.

5. Всегда тщательно тестировать ACL, чтобы убедиться, что он правильно применяет требуемую политику.

5.1.2 СИНТАКСИС СТАНДАРТНЫХ НУМЕРОВАННЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА IPV4

Для создания нумерованного стандартного списка управления доступом используйте команду **access-list**.

```
Router(config)# access-list access-list-number {deny | permit | remark text} source [source-wildcard]
[log]
```

Параметр	Описание
access-list-number	Диапазон значений: от 1 до 99 или от 1300 до 1999 года
deny	Запрещает доступ при совпадении условий.
permit	Разрешает доступ при совпадении условий.
remark *text*	(Необязательно) текстовая запись для целей документации.
source	Определяет адрес источника сети или узла для фильтрации.
source-wildcard	(Опционально) 32-битная шаблонная маска должна применяться к адресу источника.
log	(Необязательно) Создает и отправляет информационное сообщение при сопоставлении ACE.

Примечание. Используйте команду глобальной конфигурации **no access-list access-list-number** для удаления нумерованного стандартного списка ACL.

5.1.3 СИНТАКСИС ИМЕНОВАННЫХ СТАНДАРТНЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА IPV4

Чтобы создать именованный стандартный ACL, используйте стандартную команду **ip access-list standard**.

Имена ACL-списков состоят из буквенно-цифровых символов, они чувствительны к регистру и должны быть уникальными.

Указывать имена ACL-списков заглавными буквами не обязательно, но это делает их более заметными при просмотре выходных данных текущей конфигурации.

```
Router(config)# ip access-list standard access-list-name
```

```
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# ?
Standard Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
R1(config-std-nacl)#
```

5.1.4 ПРИМЕНЕНИЕ СТАНДАРТНОГО СПИСКА КОНТРОЛЯ ДОСТУПА IPV4

После настройки стандартного списка ACL IPv4 он должен быть связан с интерфейсом или сервисом.

Команда **ip access-group** используется для привязки нумерованного или именованного стандартного ACL IPv4 к интерфейсу.

Чтобы удалить список ACL из интерфейса, сначала введите команду конфигурации интерфейса **no ip access-group**.

```
Router(config-if) # ip access-group {access-list-number | access-list-name} {in | out}
```

5.1.5 ПРИМЕР СТАНДАРТНЫХ НУМЕРОВАННЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА

Пример: ACL разрешает трафик от хоста 192.168.10.10 и всех хостов в последовательном интерфейсе сети 192.168.20.0/24 0/1/0 на маршрутизаторе R1.

```
R1(config)# access-list 10 remark ACE permits ONLY host 192.168.10.10 to the internet
R1(config)# access-list 10 permit host 192.168.10.10
R1(config)# do show access-lists
Standard IP access list 10
    10 permit 192.168.10.10
R1(config)#
```

```
R1(config)# access-list 10 remark ACE permits all host in LAN 2
R1(config)# access-list 10 permit 192.168.20.0 0.0.0.255
R1(config)# do show access-lists
Standard IP access list 10
    10 permit 192.168.10.10
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
R1(config)#
```

```
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group 10 out
R1(config-if)# end
R1#
```

5.1.5 ПРИМЕР СТАНДАРТНЫХ НУМЕРОВАННЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА

Для просмотра конфигурации ACL используйте команду **show running-config**.

Для проверки правильности применения списка контроля доступа к интерфейсу используйте команду **show ip interface**.

```
R1# show run | section access-list
access-list 10 remark ACE permits host 192.168.10.10
access-list 10 permit 192.168.10.10
access-list 10 remark ACE permits all host in LAN 2
access-list 10 permit 192.168.20.0 0.0.0.255
R1#
```

```
R1# show ip int Serial 0/1/0 | include access list
  Outgoing Common access list is not set
  Outgoing access list is 10
  Inbound Common access list is not set
  Inbound  access list is not set
R1#
```

5.1.5 ПРИМЕР СТАНДАРТНЫХ НУМЕРОВАННЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА

Пример: ACL разрешает трафик от хоста 192.168.10.10 и всех хостов в последовательном интерфейсе сети 192.168.20.0/24 0/1/0 на маршрутизаторе R1.

```
R1(config)# no access-list 10
R1(config)# ip access-list standard PERMIT-ACCESS
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)#
```

```
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)# remark ACE permits all hosts in LAN 2
R1(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)#
```

```
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group PERMIT-ACCESS out
R1(config-if)# end
R1#
```

5.1.5 ПРИМЕР СТАНДАРТНЫХ НУМЕРОВАННЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА

Для просмотра конфигурации ACL используйте команду **show access-list**.

Для проверки правильности применения списка контроля доступа к интерфейсу используйте команду **show ip interface**.

```
R1# show access-lists
Standard IP access list PERMIT-ACCESS
    10 permit 192.168.10.10
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
R1# show run | section ip access-list
ip access-list standard PERMIT-ACCESS
 remark ACE permits host 192.168.10.10
 permit 192.168.10.10
 remark ACE permits all hosts in LAN 2
 permit 192.168.20.0 0.0.0.255
R1#
```

```
R1# show ip int Serial 0/1/0 | include access list
  Outgoing Common access list is not set
  Outgoing access list is PERMIT-ACCESS
  Inbound Common access list is not set
  Inbound  access list is not set
R1#
```

5.2 ВНЕСЕНИЕ ИЗМЕНЕНИЙ В ACL-СПИСКИ ДЛЯ IPV4

5.2.1 ДВА МЕТОДА ИЗМЕНЕНИЯ ACL

После настройки списка управления доступом, возможно, потребуется изменить его. Списки ACL с большим количеством ACE могут быть сложными для настройки. Иногда настроенные ACE не дают ожидаемого поведения.

Существует два метода, которые следует использовать при изменении списка управления доступом:

1. Использование текстового редактора.

2. Использование порядковых номеров.

5.2.2 МЕТОД ТЕКСТОВОГО РЕДАКТОРА

ACL с несколькими ACE следует создавать в текстовом редакторе. Таким образом можно создать или отредактировать список контроля доступа (ACL), после чего вставить его в интерфейс маршрутизатора. Это также упрощает задачи редактирования и исправления ACL.

Чтобы исправить ошибку в ACL:

1. Скопируйте список ACL из текущей конфигурации и вставьте его в текстовый редактор.

2. Внесите необходимые изменения или изменения.

3. Удалите ранее настроенный список ACL на маршрутизаторе.

4. Скопируйте и вставьте отредактированный список ACL обратно в маршрутизатор.

```
R1# show run | section access-list
access-list 1 deny   19.168.10.10
access-list 1 permit 192.168.10.0 0.0.0.255
R1#
```

```
R1(config)# no access-list 1
R1(config)#
R1(config)# access-list 1 deny 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#
```

5.2.3 МЕТОД ПОРЯДКОВЫХ НОМЕРОВ

ACL ACE можно удалить или добавить с помощью порядкового номера ACL.

Используйте команду **ip access-list standard** для редактирования списка ACL.

Записи нельзя перезаписать с теми же порядковыми номерами, что и у существующих записей. Текущий оператор должен быть удален сначала с помощью команды **no 10**. Затем правильный ACE можно добавить с помощью порядкового номера.

```
R1# show access-lists
Standard IP access list 1
    10 deny   19.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

```
R1# conf t
R1(config)# ip access-list standard 1
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 deny host 192.168.10.10
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

5.2.4 ПРИМЕР ИЗМЕНЕНИЯ ИМЕНОВАННОГО ACL

Именованные ACL также могут использовать порядковые номера для удаления и добавления ACE. В примере добавлен ACE для запрета хостов 192.168.10.11.

```
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
```

```
R1# configure terminal
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# 15 deny 192.168.10.5
R1(config-std-nacl)# end
R1#
R1# show access-lists
Standard IP access list NO-ACCESS
    15 deny   192.168.10.5
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

5.2.5 СТАТИСТИКА ПО ACL

Команда **show access-lists** в примере показывает статистику для каждой инструкции, которые сработали.

Запрещающий ACE сработал 20 раз, а разрешающий ACE - 64 раза.

Обратите внимание, что подразумеваемое утверждение **deny any** не отображает никакой статистики. Чтобы отслеживать, сколько неявных отклоненных пакетов было сопоставлено, необходимо вручную настроить команду **deny any**.

Используйте команду **clear access-list counters** для очистки статистики ACL.

```
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10  (20 matches)
    20 permit 192.168.10.0, wildcard bits 0.0.0.255  (64 matches)
R1# clear access-list counters NO-ACCESS
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

5.3 ЗАЩИТА ПОРТОВ VTY С ПОМОЩЬЮ СТАНДАРТНОГО ACL ДЛЯ IPV4

5.3.1 КОМАНДА ACCESS-CLASS

Стандартный ACL-список может обеспечить удаленный административный доступ к устройству с помощью линий vty, выполняя следующие два шага:

Создайте список ACL, чтобы определить, каким административным узлам должен быть разрешен удаленный доступ.

Примените ACL к входящему трафику на линиях vty.

```
R1(config-line)# access-class {access-list-number | access-list-name} { in | out }
```

5.3.2 ПРИМЕР БЕЗОПАСНОГО ДОСТУПА VTY

В этом примере показано, как настроить ACL для фильтрации трафика vty.

Сначала настраивается запись локальной базы данных для пользователя ADMIN и пароля class.

Строки vty на R1 настроены на использование локальной базы данных для проверки подлинности, разрешение трафика SSH и использование ADMIN-HOST ACL для ограничения трафика.

```
R1(config)# username ADMIN secret class
R1(config)# ip access-list standard ADMIN-HOST
R1(config-std-nacl)# remark This ACL secures incoming vty lines
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet
R1(config-line)# access-class ADMIN-HOST in
R1(config-line)# end
R1#
```

5.3.3 ПРОВЕРКА БЕЗОПАСНОСТИ ПОРТА VTY

После настройки ACL-списка для ограничения доступа к линиям VTY важно убедиться в его надлежащем функционировании.

Чтобы проверить статистику ACL, выполните команду **show access-lists**.

Совпадение в строке разрешения выходных данных является результатом успешного SSH-соединения хоста с IP-адресом 192.168.10.10.

Соответствие в операторе deny связано с неудачной попыткой создать соединение SSH с устройства в другой сети.

```
R1#
Oct  9 15:11:19.544: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 192.168.10.10]
[localport: 23] at 15:11:19 UTC Wed Oct 9 2019
R1# show access-lists
Standard IP access list ADMIN-HOST
    10 permit 192.168.10.10  (2 matches)
    20 deny   any  (2 matches)
R1#
```

5.4 НАСТРОЙКА РАСШИРЕННЫХ ACL ДЛЯ IPV4

5.4.1 РАСШИРЕННЫЕ ACL

Расширенные списки ACL обеспечивают большую степень контроля. Они могут фильтровать по адресу источника, адресу назначения, протоколу (например, IP, TCP, UDP, ICMP) и номеру порта.

Расширенные списки ACL могут быть созданы как:

1. Нумерованный расширенный список управления доступом - создается с помощью команды глобальной конфигурации **access-list [access-list-number]**.

2. Именованный расширенный список управления доступом - создается с помощью команды **ip access-list extended [access-list-name]**.

5.4.2 ПРОТОКОЛЫ И ПОРТЫ

Расширенные списки ACL могут фильтровать множество различных типов интернет-протоколов и портов. Используйте **?** , чтобы получить помощь при вводе сложного ACE. Четыре выделенных протокола являются наиболее популярными.

```
R1(config)# access-list 100 permit ?
  <0-255>        An IP protocol number
  ahp            Authentication Header Protocol
  dvmrp          dvmrp
  eigrp          Cisco's EIGRP routing protocol
  esp            Encapsulation Security Payload
  gre            Cisco's GRE tunneling
  icmp           Internet Control Message Protocol
  igmp           Internet Gateway Message Protocol
  ip             Any Internet Protocol
  ipinip         IP in IP tunneling
  nos            KA9Q NOS compatible IP over IP tunneling
  object-group   Service object group
  ospf           OSPF routing protocol
  pcp            Payload Compression Protocol
  pim            Protocol Independent Multicast
  tcp            Transmission Control Protocol
  udp            User Datagram Protocol
R1(config)# access-list 100 permit
```

5.4.2 ПРОТОКОЛЫ И ПОРТЫ

Выбор протокола влияет на параметры порта. Доступны многие параметры порта TCP, как показано на выходных данных.

```
R1(config)# access-list 100 permit tcp any any eq ?
  <0-65535>    Port number
  bgp          Border Gateway Protocol (179)
  chargen      Character generator (19)
  cmd          Remote commands (rcmd, 514)
  daytime      Daytime (13)
  discard      Discard (9)
  domain       Domain Name Service (53)
  echo         Echo (7)
  exec         Exec (rsh, 512)
  finger       Finger (79)
  ftp          File Transfer Protocol (21)
  ftp-data     FTP data connections (20)
  gopher       Gopher (70)
  hostname     NIC hostname server (101)
  ident        Ident Protocol (113)
  irc          Internet Relay Chat (194)
  klogin       Kerberos login (543)
  kshell       Kerberos shell (544)
  login        Login (rlogin, 513)
  lpd          Printer service (515)
  msrpc        MS Remote Procedure Call (135)
  nntp         Network News Transport Protocol (119)
  onep-plain   Onep Cleartext (15001)
  onep-tls     Onep TLS (15002)
  pim-auto-rp  PIM Auto-RP (496)
  pop2         Post Office Protocol v2 (109)
  pop3         Post Office Protocol v3 (110)
  smtp         Simple Mail Transport Protocol (25)
  sunrpc       Sun Remote Procedure Call (111)
  syslog       Syslog (514)
  tacacs       TAC Access Control System (49)
  talk         Talk (517)
  telnet       Telnet (23)
  time         Time (37)
  uucp         Unix-to-Unix Copy Program (540)
  whois        Nicname (43)
  www          World Wide Web (HTTP, 80)
```

5.4.3 ПРИМЕРЫ КОНФИГУРАЦИИ ПРОТОКОЛОВ И НОМЕРОВ ПОРТОВ

Расширенные списки ACL могут фильтровать различные номера порта и параметры имени порта.

В этом примере настраивается расширенный список ACL 100 для фильтрации HTTP-трафика. Первый ACE использует имя порта **www**. Второй ACE использует номер порта **80**. Оба ACE достигают абсолютно одинакового результата.

```
R1(config)# access-list 100 permit tcp any any eq www
!or...
R1(config)# access-list 100 permit tcp any any eq 80
```

Настройка номера порта требуется, если в списке нет конкретного имени протокола, например SSH (номер порта 22) или HTTPS (номер порта 443), как показано в следующем примере.

```
R1(config)# access-list 100 permit tcp any any eq 22
R1(config)# access-list 100 permit tcp any any eq 443
R1(config)#
```

5.4.4 ПРИМЕРЫ КОНФИГУРАЦИИ ПРОТОКОЛОВ И НОМЕРОВ ПОРТОВ

В этом примере ACL разрешает трафик HTTP и HTTPS из сети 192.168.10.0 в любой пункт назначения.

Расширенные списки ACL могут применяться в различных местах. Однако они обычно применяются близко к источнику. Здесь ACL 110 применяется входящий на интерфейсе R1 G0/0/0.

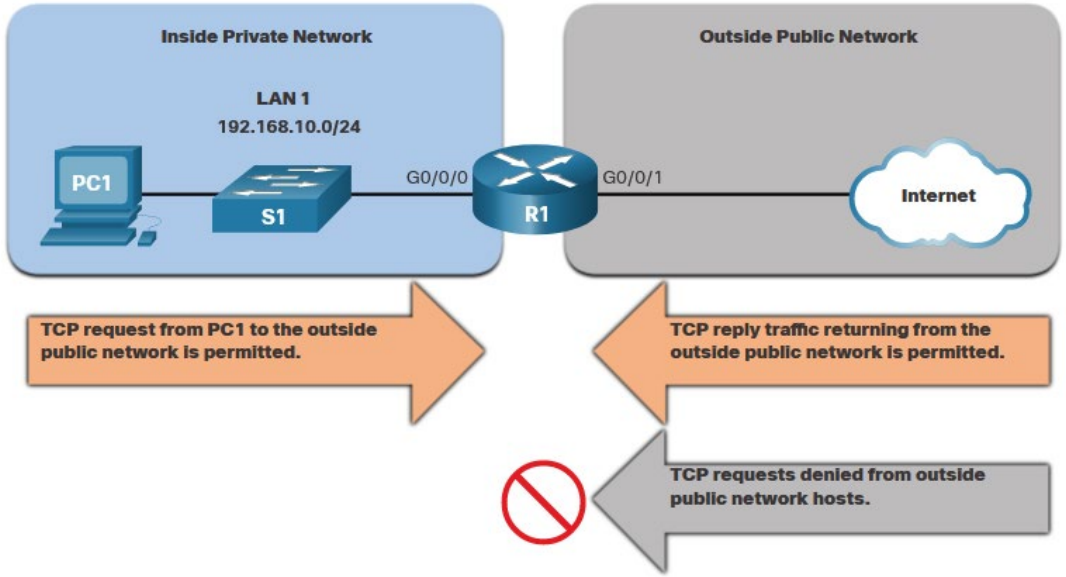
```
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 110 in
R1(config-if)# exit
R1(config)#
```

5.4.5 РАСШИРЕННЫЙ СПИСОК КОНТРОЛЯ ДОСТУПА TCP

TCP также может выполнять основные службы брандмауэра с сохранением состояния, используя ключевое слово TCP **established**.

Ключевое слово established позволяет внутреннему трафику выйти из внутренней частной сети и позволяет возвращенному ответному трафику войти во внутреннюю частную сеть.

TCP-трафик, генерируемый внешним узлом и пытающийся связаться с внутренним узлом, отклоняется.



5.4.5 РАСШИРЕННЫЙ СПИСОК КОНТРОЛЯ ДОСТУПА TCP

ACL 120 настроен так, чтобы разрешить возврат веб-трафика только на внутренние узлы. ACL затем применяется исходящий на интерфейсе R1 G0/0/0.

Команда **show access-lists** показывает, что внутренние узлы получают доступ к защищенным веб-ресурсам из Интернета.

Примечание. Соответствие происходит, если в возвращающемся сегменте TCP установлены биты флага ACK или RST, указывающие, что пакет принадлежит существующему соединению.

```
R1(config)# access-list 120 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 120 out
R1(config-if)# end
R1# show access-lists
Extended IP access list 110
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (657 matches)
Extended IP access list 120
    10 permit tcp any 192.168.10.0 0.0.0.255 established (1166 matches)
R1#
```

5.4.6 СИНТАКСИС НУМЕРОВАННОГО РАСШИРЕННОГО ACL IPV4

Присвоение имен ACL-спискам упрощает понимание функции того или иного списка. Чтобы создать именованный расширенный список ACL, используйте команду конфигурации **ip access-list extended**.

В этом примере создается именованный расширенный ACL с именем NO-FTP-ACCESS, и приглашение командной строки изменяется на именованный расширенный режим конфигурации ACL. Инструкции ACE вводятся в именованном расширенном режиме конфигурации ACL.

```
Router(config)# ip access-list extended access-list-name
```

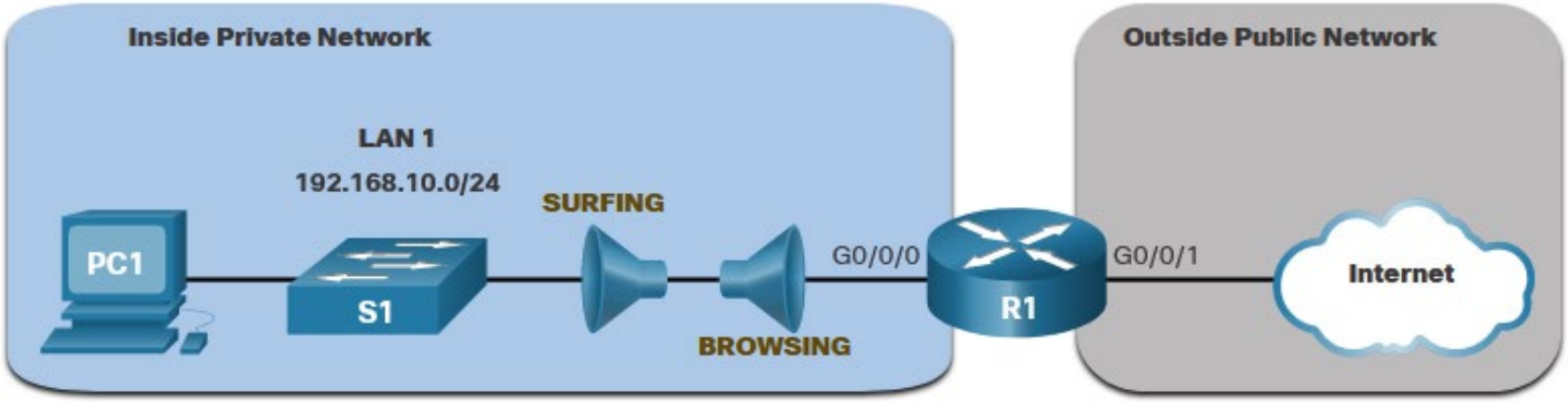
```
R1(config)# ip access-list extended NO-FTP-ACCESS
R1(config-ext-nacl)#
```

5.4.7 ПРИМЕР НУМЕРОВАННОГО РАСШИРЕННОГО ACL IPV4

Топология на рисунке используется для демонстрации настройки и применения двух именованных расширенных списков ACL IPv4 к интерфейсу:

SURFING - это позволит внутреннему HTTP и HTTPS трафику выйти в Интернет.

BROWSING - это позволит веб-трафику вернуться только на внутренние узлы, в то время как весь остальной трафик, выходящий из интерфейса R1 G0/0/0, неявно запрещен.



5.4.8 ПРИМЕР НУМЕРОВАННОГО РАСШИРЕННОГО ACL IPV4

ACL SURFING разрешает трафик HTTP и HTTPS от внутренних пользователей для выхода из интерфейса G0/0/1, подключенного к Интернету. Веб-трафик, возвращаемый из Интернета, разрешен обратно во внутреннюю частную сеть списком ACL BROWSING.

ACL SURFING применяется на входящий трафик, а ACL BROWSING применяется на исходящий трафик на R1 G0/0/0.

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# Remark Permits inside HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)#
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# Remark Only permit returning HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
R1(config-if)# end
R1# show access-lists
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (124 matches)
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established (369 matches)
R1#
```

5.4.8 ПРИМЕР НУМЕРОВАННОГО РАСШИРЕННОГО ACL IPV4

Команда **show access-lists**, используется чтобы проверить статистику ACL. Обратите внимание, что разрешенные безопасные счетчики HTTPS (например 443) в ACL SURFING и установленные счетчики возврата в ACL BROWSING увеличились.

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 19.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

5.4.9 РЕДАКТИРОВАНИЕ РАСШИРЕННЫХ ACL

Расширенный список ACL можно редактировать с помощью текстового редактора, когда требуется много изменений. Если редактирование применяется к одному или двум ACE, можно использовать порядковые номера.

Например:

Номер последовательности ACE 10 в SURFING ACL имеет неверный IP-адрес сети источника.

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 19.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

5.4.9 РЕДАКТИРОВАНИЕ РАСШИРЕННЫХ ACL

Для исправления этой ошибки исходный оператор удаляется командой **no sequence_#** , а исправленный оператор добавляется заменяющий исходный оператор.

Выходные данные проверяют изменение конфигурации с помощью команды **show access-lists**.

```
R1# configure terminal
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# no 10
R1(config-ext-nacl)# 10 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config-ext-nacl)# end
```

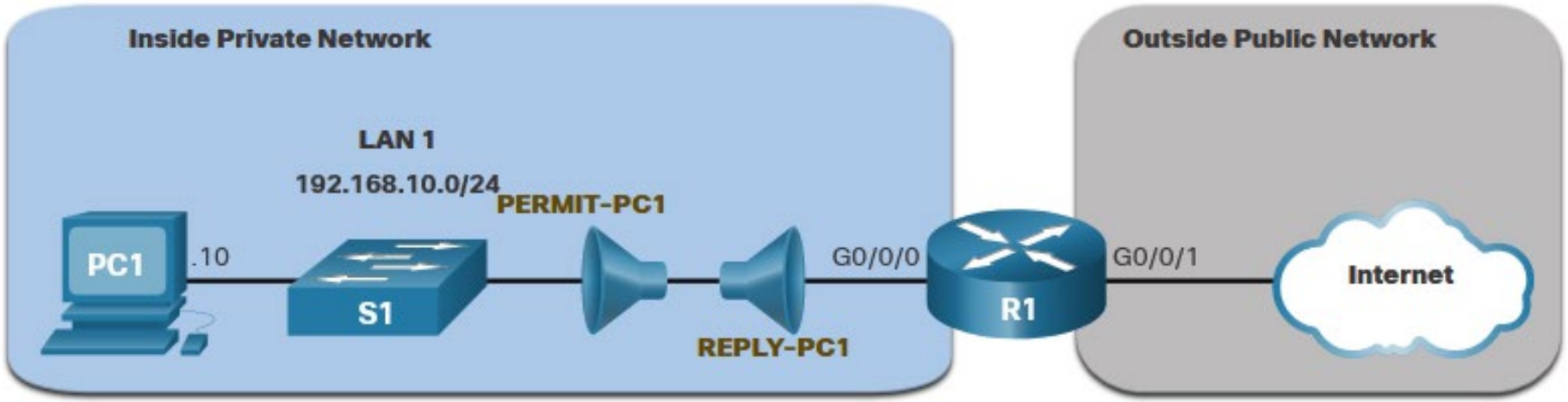
```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

5.4.10 ДРУГОЙ ПРИМЕР РАСШИРЕННОГО ACL IPV4

Будут созданы два именованных расширенных списка ACL:

PERMIT-PC1 - это позволит только PC1 TCP доступ к Интернету и запретить все остальные хосты в частной сети.

REPLY-PC1 - это позволит только указанному возвращаемому TCP-трафику на PC1 неявно запрещать весь остальной трафик.



5.4.10 ДРУГОЙ ПРИМЕР РАСШИРЕННОГО ACL IPV4

ACL PERMIT-PC1 разрешает PC1 (192.168.10.10) TCP-доступ трафику по протоколам FTP, SSH, Telnet, DNS, HTTP и HTTPS.

ACL REPLY-PC1 разрешает обратный трафик на PC1.

ACL PERMIT-PC1 применяется для входящего трафика, а ACL REPLY-PC1 применяется для исходящего трафика на R1 G0/0/0.

```
R1(config)# ip access-list extended PERMIT-PC1
R1(config-ext-nacl)# Remark Permit PC1 TCP access to internet
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 20
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 21
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 22
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 23
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 53
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 80
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 443
R1(config-ext-nacl)# deny ip 192.168.10.0 0.0.0.255 any
R1(config-ext-nacl)# exit
R1(config)#
R1(config)# ip access-list extended REPLY-PC1
R1(config-ext-nacl)# Remark Only permit returning traffic to PC1
R1(config-ext-nacl)# permit tcp any host 192.168.10.10 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0/0
R1(config-if)# ip access-group PERMIT-PC1 in
R1(config-if)# ip access-group REPLY-PC1 out
R1(config-if)# end
R1#
```

5.4.11 ПРОВЕРКА РАСШИРЕННЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА

Команда **show ip interface** используется для проверки списка контроля доступа на интерфейсе и направления, к которому был привязан список.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  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
  Outgoing access list is REPLY-PC1
  Inbound  access list is PERMIT-PC1
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
R1#
R1# show ip interface g0/0/0 | include access list
Outgoing access list is REPLY-PC1
Inbound access list is PERMIT-PC1
R1#
```

5.4.11 ПРОВЕРКА РАСШИРЕННЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА

Команда **show access-lists** может использоваться для подтверждения того, что списки ACL работают должным образом. Команда отображает счетчики статистики, которые увеличиваются при сопоставлении ACE.

Примечание. Трафик должен быть создан для проверки работы ACL.

```
R1# show access-lists
Extended IP access list PERMIT-PC1
10 permit tcp host 192.168.10.10 any eq 20
20 permit tcp host 192.168.10.10 any eq ftp
30 permit tcp host 192.168.10.10 any eq 22
40 permit tcp host 192.168.10.10 any eq telnet
50 permit tcp host 192.168.10.10 any eq domain
60 permit tcp host 192.168.10.10 any eq www
70 permit tcp host 192.168.10.10 any eq 443
80 deny ip 192.168.10.0 0.0.0.255 any
Extended IP access list REPLY-PC1
10 permit tcp any host 192.168.10.10 established
R1#
```

5.4.11 ПРОВЕРКА РАСШИРЕННЫХ СПИСКОВ КОНТРОЛЯ ДОСТУПА

Команда **show running-config** может использоваться для проверки настроенных параметров. Команда также отображает настроенные примечания.

```
R1# show running-config | begin ip access-list
ip access-list extended PERMIT-PC1
remark Permit PC1 TCP access to internet
permit tcp host 192.168.10.10 any eq 20
permit tcp host 192.168.10.10 any eq ftp
permit tcp host 192.168.10.10 any eq 22
permit tcp host 192.168.10.10 any eq telnet
permit tcp host 192.168.10.10 any eq domain
permit tcp host 192.168.10.10 any eq www
permit tcp host 192.168.10.10 any eq 443
deny ip 192.168.10.0 0.0.0.255 any
ip access-list extended REPLY-PC1
remark Only permit returning traffic to PC1
permit tcp any host 192.168.10.10 established
!
```