OTUS

ОНЛАЙН ОБРАЗОВАНИЕ

Онлайн-образование

Не забыть включить запись!


Меня хорошо видно && слышно?
Ставьте +, если все хорошо
Напишите в чат, если есть проблемы

OTUS

ACL

Рукин Андрей
преподаватель
cisco@sk12.ru

Правила вебинара

Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Карта курса

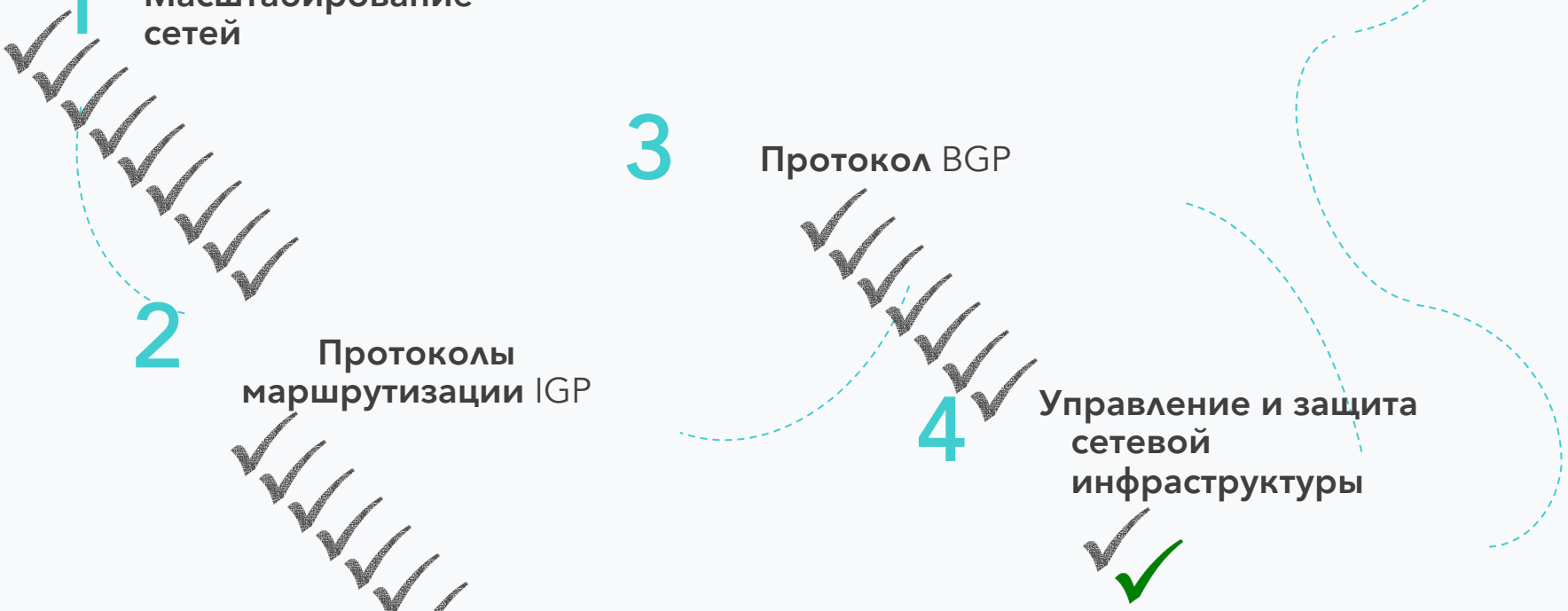
1 Масштабирование сетей

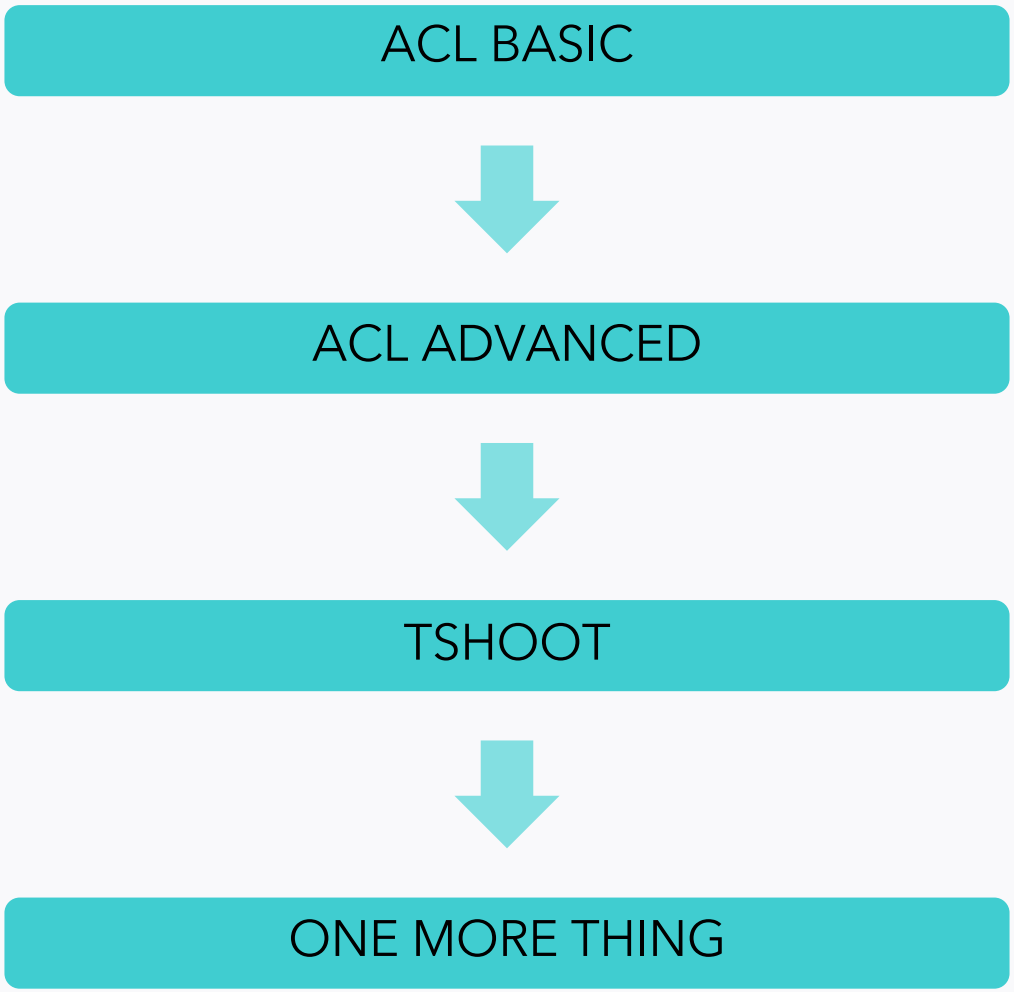
2 Протоколы маршрутизации IGP

3 Протокол BGP

4 Управление и защита сетевой инфраструктуры

5 Проектная работа



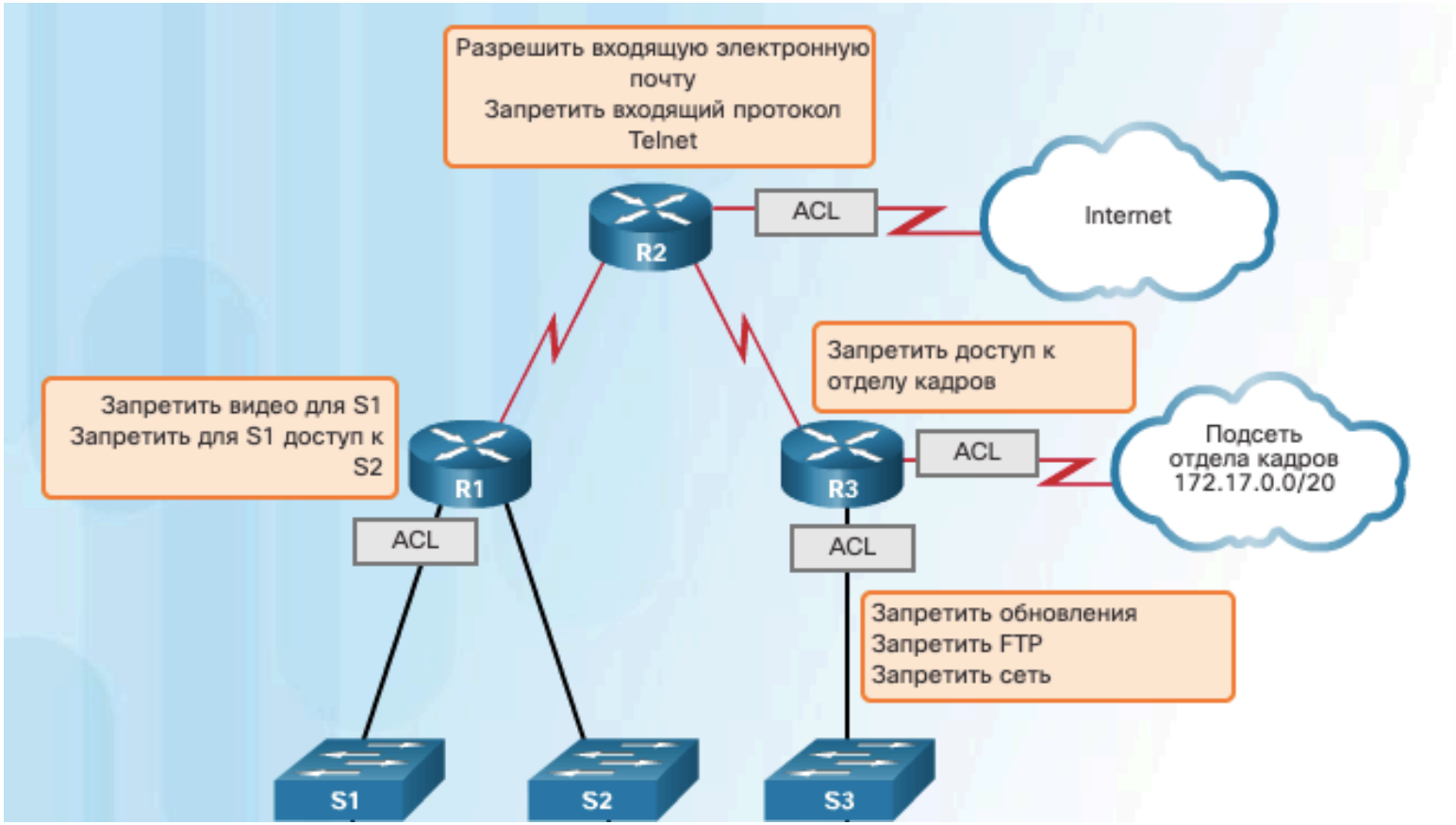

ACL BASIC
ACL ADVANCED
TSHOOT
ONE MORE THING

01

BASIC

ACL

ACL-список — это ряд команд IOS, определяющих, пересылает ли маршрутизатор пакеты или сбрасывает их, исходя из информации в заголовке пакета.



ACL-списки выполняют следующие задачи:

1. Ограничение сетевого трафика для повышения производительности сети
2. Управление потоком трафика (например, можно ограничить доставку маршрутных обновлений)
3. Обеспечивают базовый уровень безопасности в отношении доступа к сети
4. Осуществляют фильтрацию трафика на основе типа трафика
5. Осуществляют сортировку узлов в целях разрешения или запрета доступа к сетевым службам
6. Можно использовать для анализа, пересылки или обработки отдельных видов трафика
7. ……

По умолчанию ACL-списки не сконфигурированы на маршрутизаторе

Фильтрация пакетов

```
R1(config-ext-nacl)#do sh access-list OutBoundAccess
Extended IP access list OutBoundAccess
    10 permit ip 192.168.1.0 0.0.0.255 any
    11 deny tcp 192.168.2.0 0.0.0.127 any eq smtp
    12 deny tcp 192.168.2.0 0.0.0.127 any eq sunrpc
    13 deny tcp 192.168.2.0 0.0.0.127 any eq pop2
    14 deny tcp 192.168.2.0 0.0.0.127 any eq nntp
    15 deny tcp 192.168.2.0 0.0.0.127 any eq ftp
    16 deny tcp 192.168.2.0 0.0.0.127 any eq ftp-data
    17 deny tcp 192.168.2.0 0.0.0.127 any eq telnet
    18 deny tcp 192.168.2.0 0.0.0.127 any eq cmd
    19 deny tcp 192.168.2.0 0.0.0.127 any eq irc
    20 permit ip 192.168.2.0 0.0.0.255 any
    30 permit ip 192.168.3.0 0.0.0.255 any
    40 permit ip 192.168.4.0 0.0.0.255 any
    50 permit ip 192.168.5.0 0.0.0.255 any
```

Список контроля доступа ACL — это последовательный список разрешающих или запрещающих операторов, называемых записями контроля доступа — ACE (правила).

Фильтрация пакетов может происходить на уровнях 3 и 4 OSI

Входящий и исходящий ACL

Входящий ACL-список эффективен, поскольку он сохраняет ресурсы на поиск маршрута

Исходящие ACL-списки лучше всего использовать, когда одинаковые фильтры применяются к пакетам, поступающим с множества входящих интерфейсов

Шаблонная маска

ACL-списки IPv4 используют шаблонные маски

	Десятичные	Двоичные
IP-адрес	192.168.16.0	11000000.10101000.00010000.00000000
Групповая маска	0.0.15.255	00000000.00000000.00001111.11111111
Итоговый диапазон	От 192.168.16.0 до 192.168.31.255	От 11000000.10101000.00010000.00000000 до 11000000.10101000.00011111.11111111

	Десятичные	Двоичные
IP-адрес	192.168.1.0	11000000.10101000.00000001.00000000
Групповая маска	0.0.254.255	00000000.00000000.11111110.11111111
Результат	192.168.1.0	11000000.10101000.00000001.00000000
	Все нечётные подсети в основной сети 192.168.0.0	

Ключевые слова в шаблонной маске

HOST & ANY

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
!OR
R1(config)# access-list 1 permit any
```

```
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
!OR
R1(config)# access-list 1 permit host 192.168.10.10
```

Правила применения

По одному списку для интерфейса, направления и протокола

Имея два интерфейса и два работающих протокола, этот маршрутизатор в целом мог бы иметь восемь отдельных ACL-списков.

Правила применения списков ACL

У вас может быть только один ACL-список на один протокол, интерфейс и направление:

- Один ACL-список для одного протокола (например IPv4 или IPv6)
- Один ACL-список для одного направления (например IN или OUT)
- Один ACL-список для одного интерфейса (например, GigabitEthernet0/0)

Синтаксис стандартного ACL

Параметр	Описание
access-list-number	Номер ACL-списка. Это десятичное число от 1 до 99 или от 1300 до 1999 (для стандартного ACL-списка).
deny	Запрещает доступ при совпадении условий.
permit	Разрешает доступ при совпадении условий.
remark	Чтобы сделать список проще для понимания и прочтения, добавьте комментарий о записях в списке доступа IP.
source	Номер сети или узла, с которых отправляется пакет. Два способа определить адрес *источника*: • Используйте 32-битный адрес, записанный в виде четырех 8-битовых целых чисел, разделенных точками. • Используйте ключевое слово **any** как сокращение для адреса *источника* и *групповой маски источника* 0.0.0.0 255.255.255.255.
source-wildcard	(Опционально). 32-битная шаблонная маска должна применяться к адресу источника. Разряды в позиции битов, которые вы хотите игнорировать.
log	(Опционально). Вызывает информационное сообщение журнала о пакете, соответствующем записи, которая должна быть отправлена на консоль. (Уровень сообщений, регистрируемых на консоли, регулируется командой **logging console**).

Необходимо сначала создать стандартный ACL-список и затем активировать его на интерфейсе

Применение стандартных ACL

Нумерованного ACL

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0

R1(config-if)# ip access-group 1 out
```

Именованного ACL

```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

Редактирование стандартных ACL

Текстовый редактор

```
R1# show running-config | include access-list 1
access-list 1 deny host 192.168.10.99
access-list 1 permit 192.168.0.0 0.0.255.255
```

По порядковым номерам

```
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#
```

```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# 15 deny host 192.168.11.11
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    15 deny   192.168.11.11
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
```

Проверка стандартных списков контроля доступа

На интерфейсе

```
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<Данные опущены>
  Outgoing access list is NO_ACCESS
  Inbound access list is not set
```

Статистика

```
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10 (4 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Расширенные ACL

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Расширенные списки контроля доступа фильтруют IPv4-пакеты, исходя из нескольких признаков:

1. тип протокола;
2. IPv4-адрес источника;
3. IPv4-адрес назначения;
4. TCP или UDP порты источника;
5. TCP или UDP порты назначения;
6. дополнительная информация о типе протокола.

Нумерованные и именованные списки контроля доступа

Нумерованный список контроля доступа (ACL)

Номер присваивается в зависимости то того, какой протокол будет фильтроваться.

- (1–99) и (1300–1999): стандартный список контроля доступа IP
- (От 100 до 199) и (от 2000 до 2699): список контроля доступа расширенного протокола IP

Именованный список контроля доступа

Имя присваивается для определения списка контроля доступа.

- Имена могут содержать буквенно-цифровые символы.
- Рекомендуется вводить имя, используя ЗАГЛАВНЫЕ БУКВЫ.
- В именах не допускается наличие пробелов или знаков препинания.
- Записи списка контроля доступа можно добавлять или удалять.

Именованные списки контроля доступа

```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

```
R1(config)# ip access-list extended SURFING
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)# ip access-list extended BROWSING
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
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
```

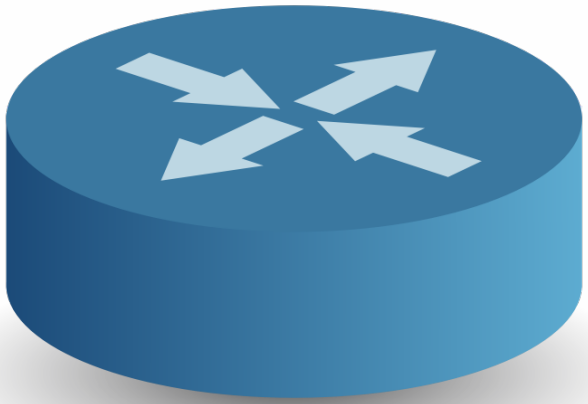
Настройка расширенных ACL

access-list *access-list-number* {deny | permit | remark} *protocol* {*source source-wildcard*} [operator port [port-number or name]] {*destination destination-wildcard*} [operator port [port-number or name]]

Параметр	Описание
access-list-number	Определяет список доступа с помощью числа в диапазоне от 100 до 199 (для расширенного списка контроля доступа по протоколу IP) и от 2000 до 2699 (для расширенного списка контроля доступа).
deny	Запрещает доступ при совпадении условий.
permit	Разрешает доступ при совпадении условий.
remark	Добавление примечаний к записям в списке контроля доступа IP для упрощения визуального восприятия и проверки.
protocol	Имя или номер протокола IP. Типичные ключевые слова: **icmp**, **ip**, **tcp** и **udp**. Для соответствия любому протоколу IP (включая ICMP, TCP и UDP) используйте ключевое слово **ip**.
source	Номер сети или узла, с которых отправляется пакет.
source-wildcard	Шаблонные биты должны применяться к источнику.
destination	Номер сети или хоста, к которому посылается пакет.
destination-wildcard	Шаблонные биты должны применяться к назначению.
operator	(Опционально). Сравнивает порты источника и назначения. Возможные операнды: **lt** (меньше чем), **gt** (больше чем), **eq** (равно), **neq** (не равно) и **range** (в диапазоне включительно).
port	(Опционально). Десятичный номер или имя порта TCP или UDP.
established	(Опционально). Только для протокола TCP: отображает установленное соединение.

Аналогично стандартным ACL

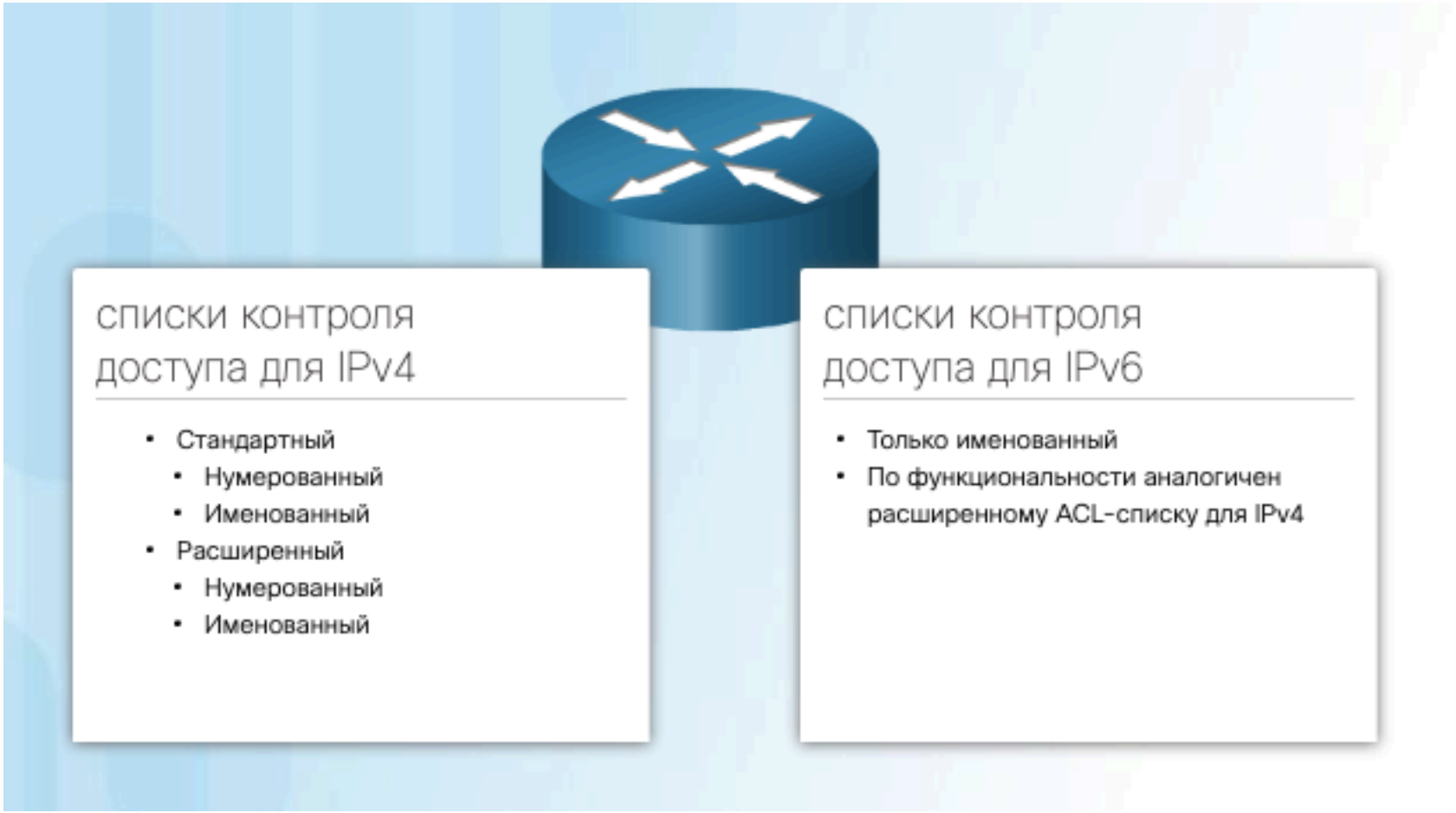
1. Проверка
2. Редактирование
   a. Текстовый редактор
   b. Номера строк
3. Статистика



02

ADVANCED

Типы списков контроля доступа IPv6



*ACL-список для IPv4 и ACL-список для IPv6 не могут иметь одно и то же имя

Важные различия ACL IPv4 & IPv6

1. IPv4 ACL использует шаблонные маски, а IPv6 - длину префикса

Важные различия ACL IPv4 & IPv6

1. IPv4 ACL использует шаблонные маски, а IPv6 - длину префикса
2. Для применения списка контроля доступа:
   - IPv4 использует команду ***ip access-group***
   - IPv6 использует команду ***ipv6 traffic-filter***

Важные различия ACL IPv4 & IPv6

1. IPv4 ACL использует шаблонные маски, а IPv6 - длину префикса
2. Для применения списка контроля доступа:
   - IPv4 использует команду ***ip access-group***
   - IPv6 использует команду ***ipv6 traffic-filter***
3. Скрытые записи:
   - IPv4 находится запись неявного отказа
     - ***deny ip any any***
   - IPv6 три правила:
     - ***permit icmp any any nd-na***
     - ***permit icmp any any nd-ns***
     - ***deny ipv6 any any***

Настройка IPv6 списков аналогична настройке расширенного именованного списка контроля доступа для IPv4.

```
R1(config)# ipv6 access-list access-list-name
R1(config-ipv6-acl)# deny | permit protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
[operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator
[port-number]]
```

Параметр	Описание
deny | permit	Определяет, следует ли принять или отклонить пакет.
protocol	Введите имя или номер протокола IP или целое число, отображающее номер протокола IPv6.
source-ipv6-prefix/prefix-length *destination-ipv6-address*	IPv6 сеть источника или назначения или класс сетей, для которых установлены условия разрешения или отклонения.
any	Введите **any** в качестве сокращения для префикса IPv6-адреса ::/0. Это соответствует всем адресам.
хост	Для **host** *source-ipv6-address* и *destination-ipv6-address* введите IPv6-адрес хоста источника или назначения, для которых установлены условия разрешения или отклонения.
operator	(Опционально). Операнд, в котором сравниваются порты источника или назначения конкретного протокола. Операнды включают варианты: lt (менее чем), gt (больше чем), eq (равно), neq (не равно) и диапазон.
port-number	(Опционально). Десятичное число или имя порта протокола TCP или UDP для фильтрации TCP или UDP соответственно.

ACL Advanced

Примеры и применение

```
R1(config)# ipv6 access-list NO-R3-LAN-ACCESS
R1(config-ipv6-acl)# deny ipv6 2001:db8:cafe:30::/64 any
R1(config-ipv6-acl)# permit ipv6 any any
R1(config-ipv6-acl)# end
R1#
```

```
R1(config)# interface s0/0/0
R1(config-if)# ipv6 traffic-filter NO-R3-LAN-ACCESS in
```

```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# remark Permit access only HTTP and HTTPS to Network 10
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 80
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 443
R3(config-ipv6-acl)# remark Deny all other traffic to Network 10
R3(config-ipv6-acl)# deny ipv6 any 2001:db8:cafe:10::/64
R3(config-ipv6-acl)# remark Permit PC3 telnet access to PC2
R3(config-ipv6-acl)# permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq 23
R3(config-ipv6-acl)# remark Deny telnet access to PC2 for all other devices
R3(config-ipv6-acl)# deny tcp any host 2001:db8:cafe:11::11 eq 23
R3(config-ipv6-acl)# remark Permit access to everything else
R3(config-ipv6-acl)# permit ipv6 any any
R3(config-ipv6-acl)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 traffic-filter RESTRICTED-ACCESS in
R3(config-if)#
```

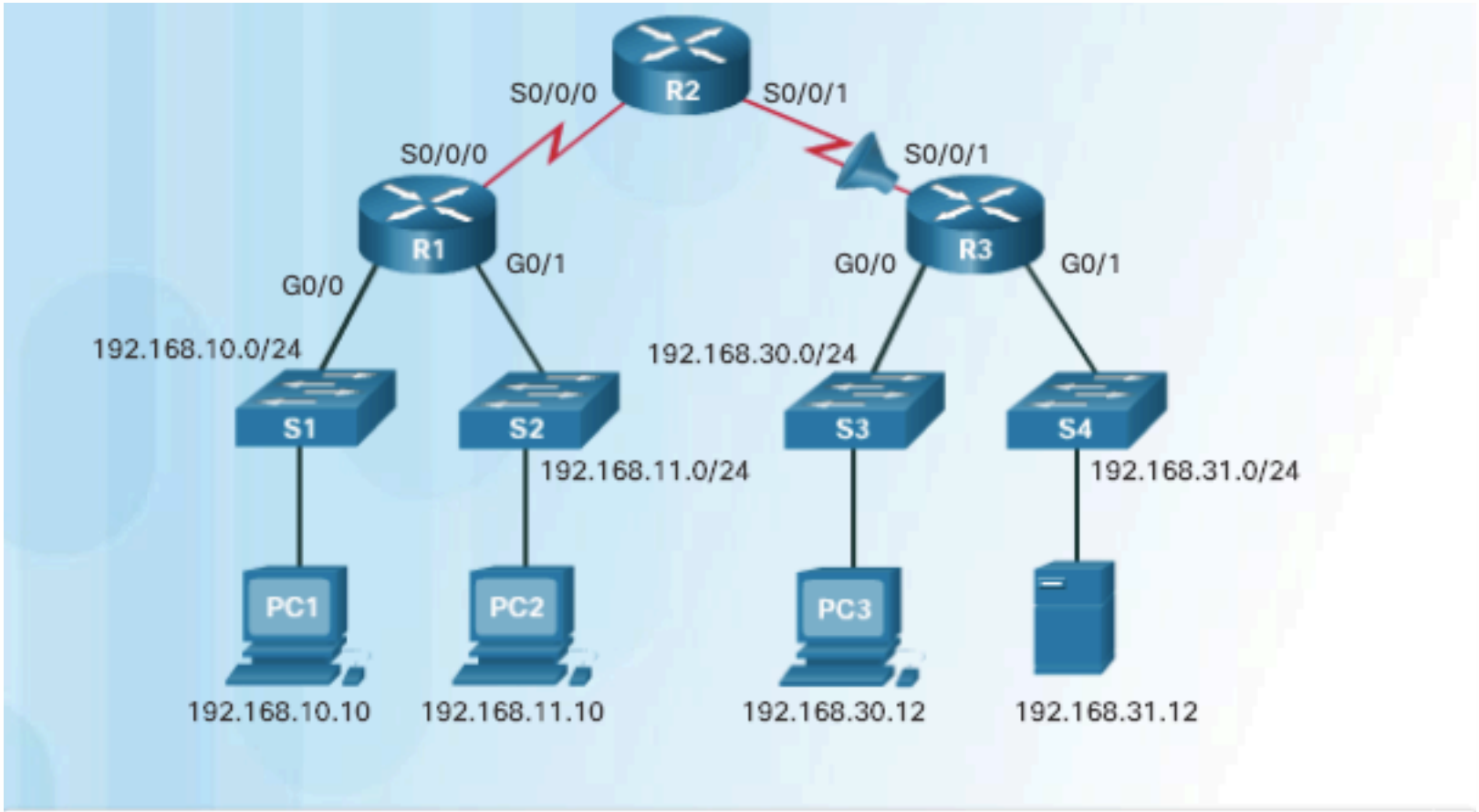
1
2
3
4
5
6

03

TSHOOT

ACL TSHOOT

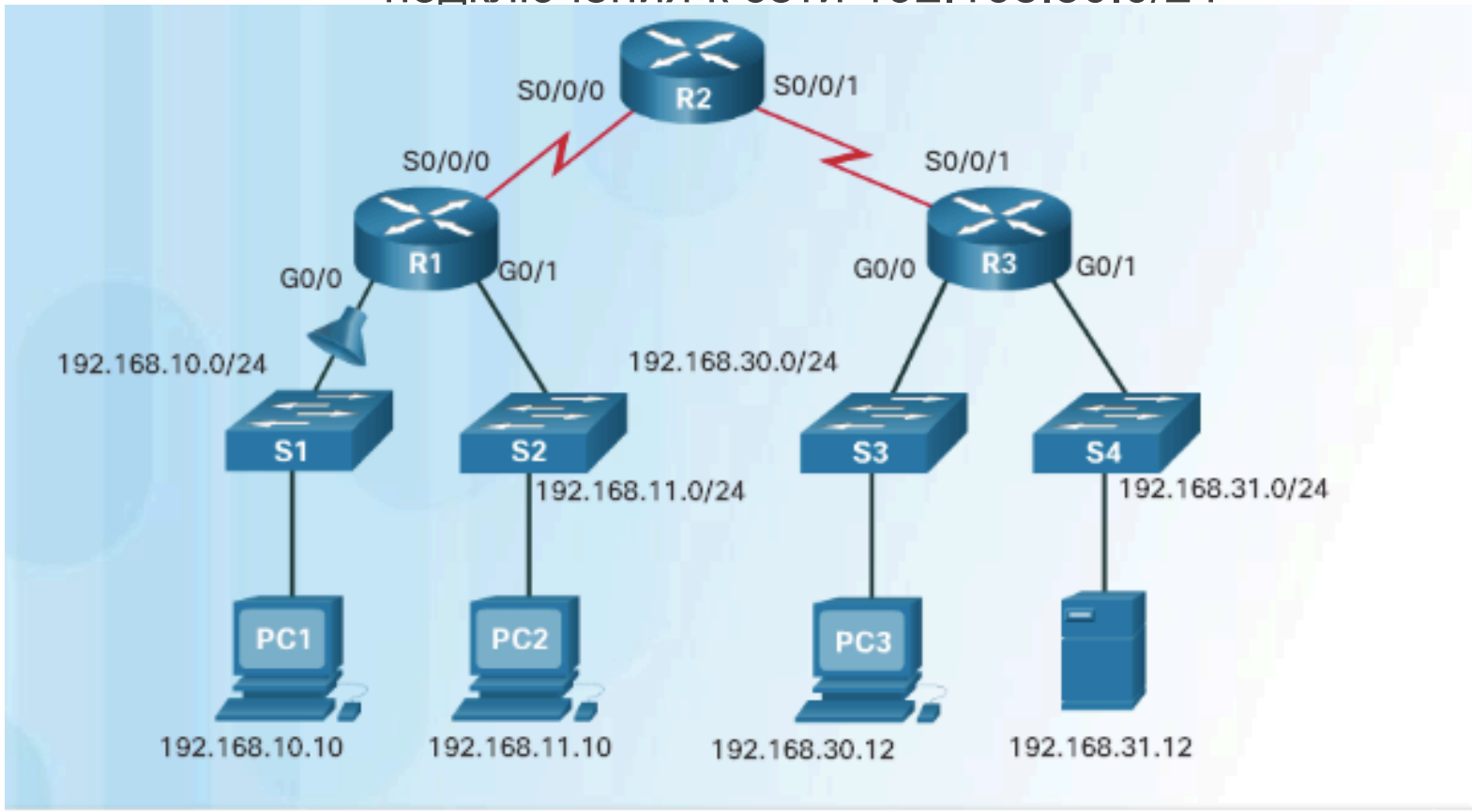
192.168.10.10 не может подключиться к 192.168.30.12 по Telnet




```
R3# show access-lists
Extended IP access list 110
    10 deny tcp 192.168.10.0 0.0.0.255 any (12 match(es))
    20 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
    30 permit ip any any
```

ACL TSHOOT

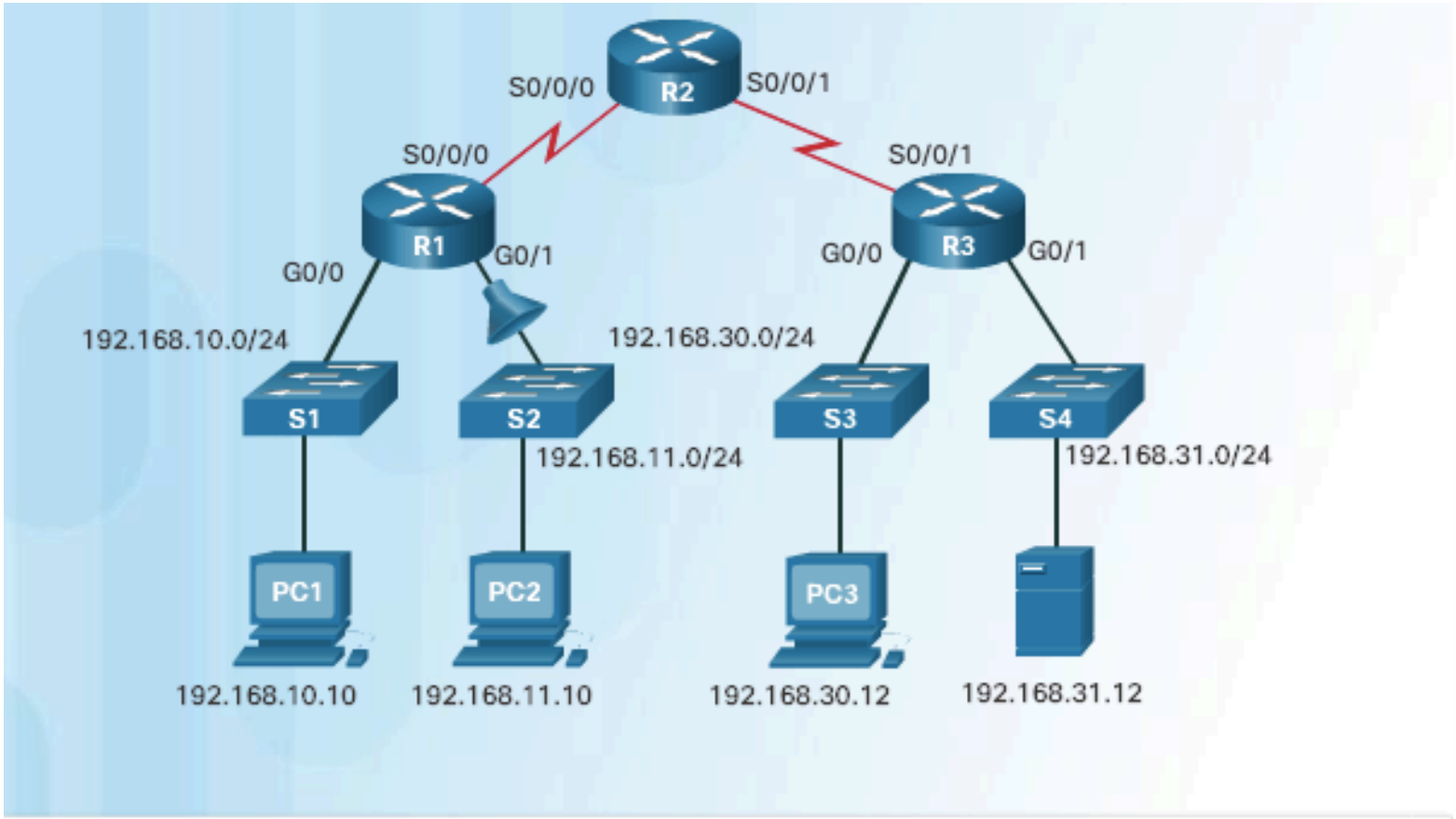
сеть 192.168.10.0/24 не может использовать протокол TFTP для подключения к сети 192.168.30.0/24




```
R3# show access-lists 120
Extended IP access list 120
    10 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
    20 deny tcp 192.168.10.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any
```

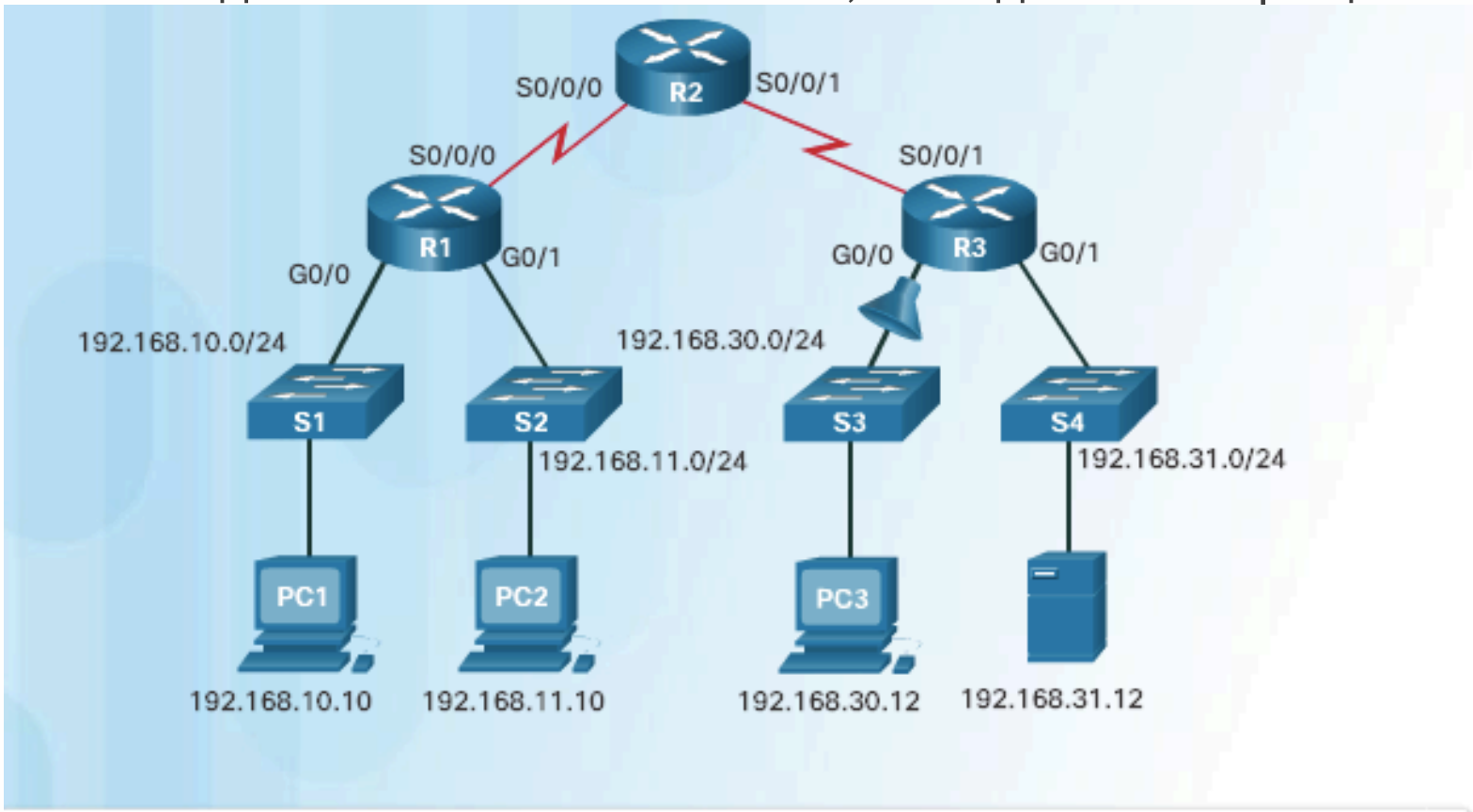
ACL TSHOOT

сеть 192.168.11.0/24 может использовать протокол Telnet для соединения с 192.168.30.0/24, но такое соединение запрещено



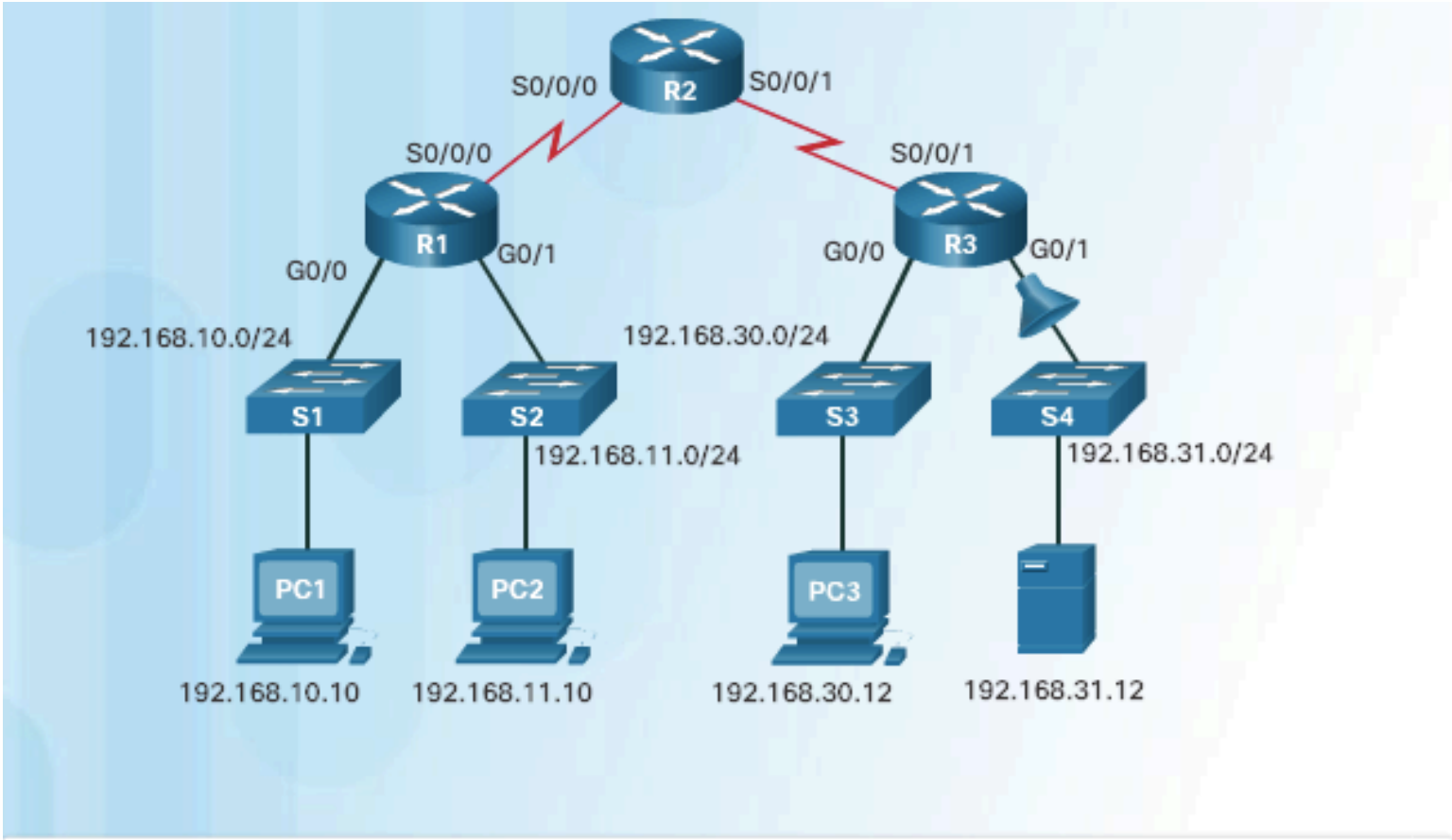

```
R1# show access-lists 130
Extended IP access list 130
  10 deny tcp any eq telnet any
  20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
  30 permit tcp any any (12 match(es))
```

узел 192.168.30.12 имеет возможность использовать Telnet для подключения к 192.168.31.12, но подобное запрещено




```
R3# show access-lists 140
Extended IP access list 140
    10 deny tcp host 192.168.30.1 any eq telnet
    20 permit ip any any (5 match(es))
```

Узел 192.168.30.12 может использовать Telnet для подключения к 192.168.31.12, но, данное подключение не может быть разрешено

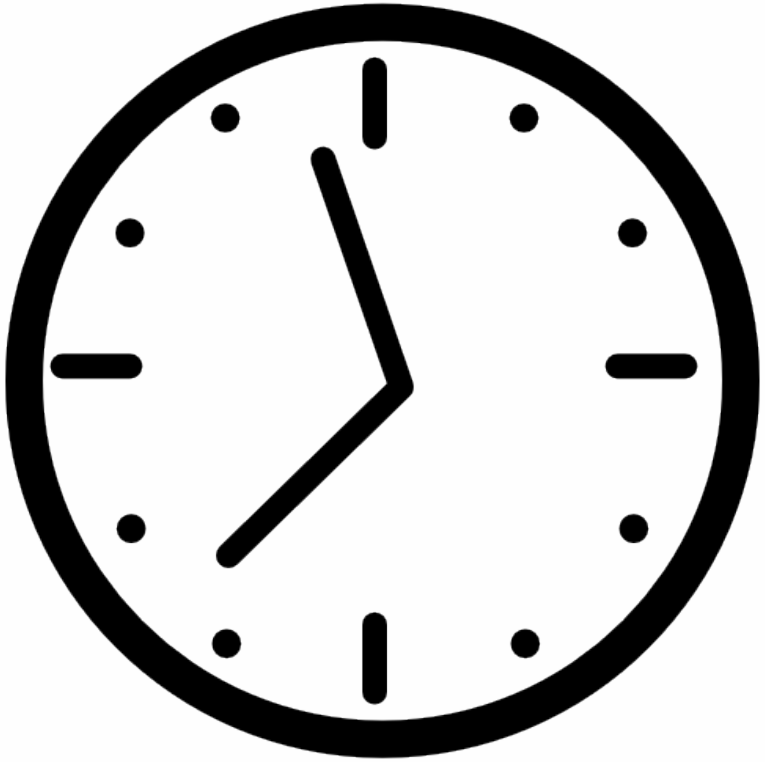



```
R2# show access-lists 150
Extended IP access list 150
        10 deny tcp any host 192.168.31.12 eq telnet
        20 permit ip any any
```

04

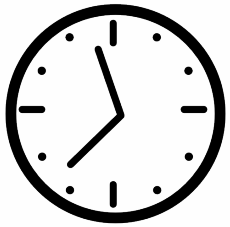
ONE MORE THING

ACL по времени (Time-based ACL)



ACL по времени (Time-based ACL)

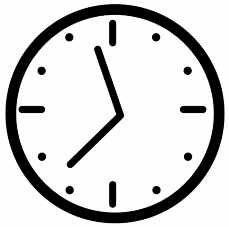
R1(config)#**time-range EVERYOTHERDAY**



ACL по времени (Time-based ACL)

R1(config)#**time-range EVERYOTHERDAY**

R1(config-time-range)#**periodic Monday Wednesday Friday 8:00 to 17:00** — создаем список времени, в котором добавляем дни недели и время

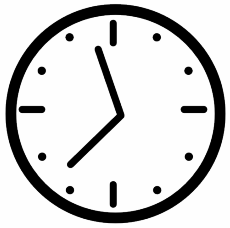


ACL по времени (Time-based ACL)

R1(config)#**time-range EVERYOTHERDAY**

R1(config-time-range)#**periodic Monday Wednesday Friday 8:00 to 17:00** — создаем список времени, в котором добавляем дни недели и время

R1(config)#**access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range EVERYOTHERDAY** — применяем time-range к ACL



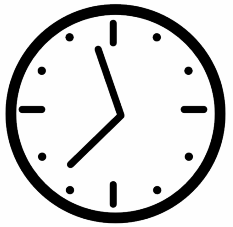
ACL по времени (Time-based ACL)

R1(config)#**time-range EVERYOTHERDAY**

R1(config-time-range)#**periodic Monday Wednesday Friday 8:00 to 17:00** — создаем список времени, в котором добавляем дни недели и время

R1(config)#**access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range EVERYOTHERDAY** — применяем time-range к ACL

R1(config)#**interface s0/0/0**
R1(config-if)#**ip access-group 101 out** — закрепляем ACL за интерфейсом



Ограничение доступа к оборудованию

Ограничение доступа к оборудованию

R1(config)#**access-list 21 permit host 192.168.10.1**

Ограничение доступа к оборудованию

R1(config)#**access-list 21 permit host 192.168.10.1**

R1(config)#**line vty 0 4** — переходим в режим настройки виртуальных линий

Ограничение доступа к оборудованию

R1(config)#**access-list 21 permit host 192.168.10.1**

R1(config)#**line vty 0 4** — переходим в режим настройки виртуальных линий

R1(config-line)#**password <*пароль*>**
R1(config-line)#**login** — настраиваем логин и пароль

Ограничение доступа к оборудованию

R1(config)#**access-list 21 permit host 192.168.10.1**

R1(config)#**line vty 0 4** — переходим в режим настройки виртуальных линий

R1(config-line)#**password <*пароль*>**
R1(config-line)#**login** — настраиваем логин и пароль

R1(config-line)#**access-class 21 in** закрепляем список доступа с разрешенным IP

Динамические списки доступа

Динамические списки доступа

R3(config)#**username *student* password 0 *otus*** — создаем пользователей для подключения через Telnet

Динамические списки доступа

R3(config)#**username *student* password 0 *otus*** — создаем пользователей для подключения через Telnet

R3(config)#**access-list 101 permit tcp any host 10.2.2.2 eq telnet**
R3(config)#access-list 101 dynamic testlist timeout 15 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 — разрешаем подключаться к серверу по Telnet всем узлам.

Динамические списки доступа

R3(config)#**username *student* password 0 *otus*** — создаем пользователей для подключения через Telnet

R3(config)#**access-list 101 permit tcp any host 10.2.2.2 eq telnet**
R3(config)#access-list 101 dynamic testlist timeout 15 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 — разрешаем подключаться к серверу по Telnet всем узлам.

R3(config)#**interface serial 0/0/1**
R3(config-if)#**ip access-group 101 in** — закрепляем 101 ACL за интерфейсом в входящем направлении.

Динамические списки доступа

R3(config)#**username *student* password 0 *otus*** — создаем пользователей для подключения через Telnet

R3(config)#**access-list 101 permit tcp any host 10.2.2.2 eq telnet**
R3(config)#**access-list 101 dynamic testlist timeout 15 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255** — разрешаем подключаться к серверу по Telnet всем узлам.

R3(config)#**interface serial 0/0/1**
R3(config-if)#**ip access-group 101 in** — закрепляем 101 ACL за интерфейсом в входящем направлении.

R3(config)#**line vty *0 4***
R3(config-line)#**login local**
R3(config-line)#**autocommand access-enable host timeout *5*** – как только пользователь аутентифицируется, сеть 192.168.30.0 будет доступна, через 5 минут бездействия сеанс закроется

Рефлексивные списки доступа

Рефлексивные списки доступа

R2(config)#**ip access-list extended OUTBOUNDFILTERS**
R2(config-ext-nacl)#**permit tcp 192.168.0.0 0.0.255.255 any reflect TCPTRAFFIC**
R2(config-ext-nacl)#**permit icmp 192.168.0.0 0.0.255.255 any reflect ICMPTRAFFIC** — заставляем маршрутизатор отслеживать трафик, который инициировался изнутри

Рефлексивные списки доступа

R2(config)#**ip access-list extended OUTBOUNDFILTERS**
R2(config-ext-nacl)#**permit tcp 192.168.0.0 0.0.255.255 any reflect TCPTRAFFIC**
R2(config-ext-nacl)#**permit icmp 192.168.0.0 0.0.255.255 any reflect ICMPTRAFFIC** — заставляем маршрутизатор отслеживать трафик, который инициировался изнутри

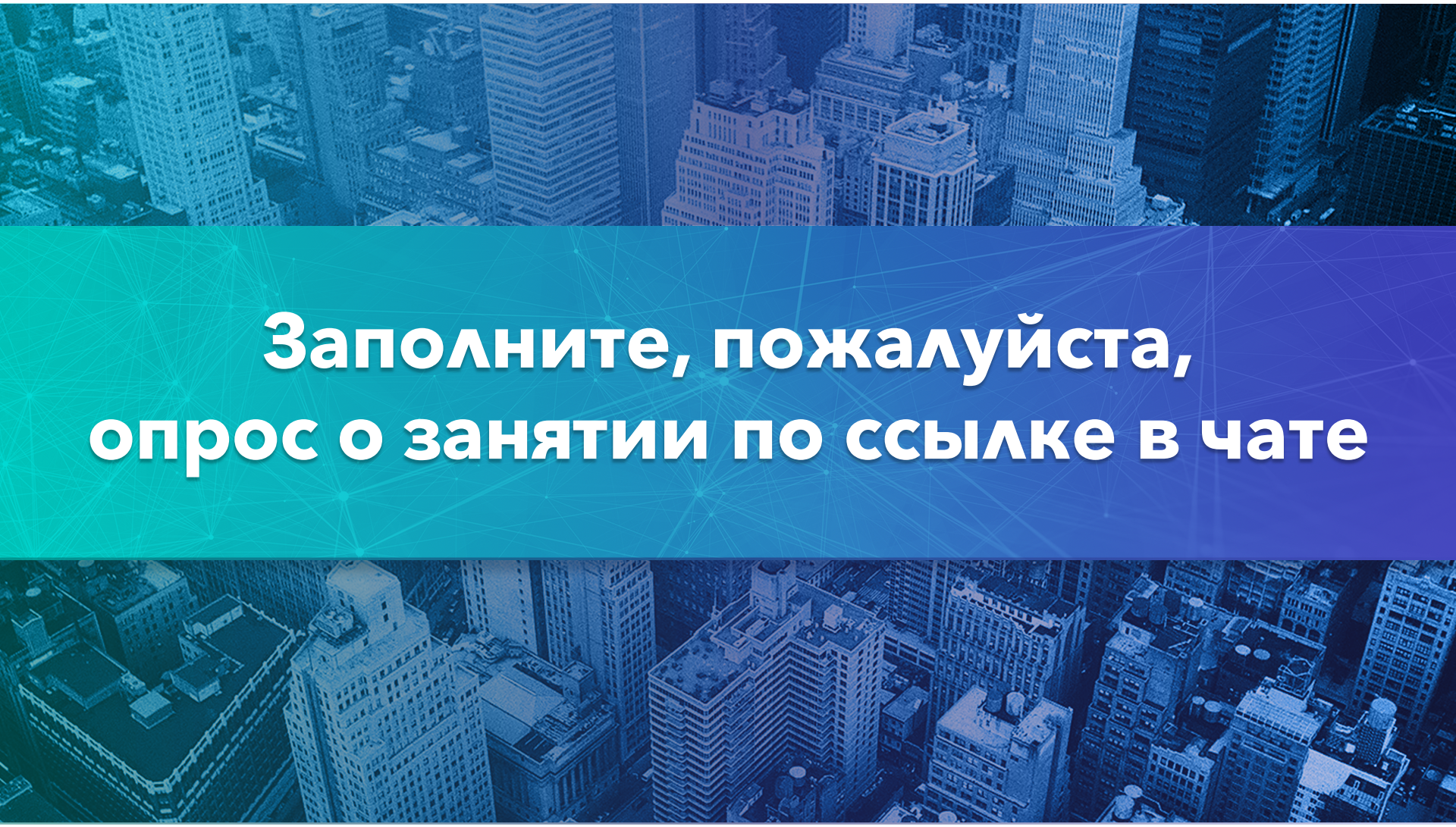
R2(config)#**ip access-list extended INBOUNDFILTERS**
R2(config-ext-nacl)#**evaluate TCPTRAFFIC**
R2(config-ext-nacl)#**evaluate ICMPTRAFFIC** — создаем входящую политику, которая требует, чтобы маршрутизатор проверял входящий трафик, чтобы видеть инициировался ли изнутри и связываем TCPTRAFFIC к INBOUNDFILTERS.

Рефлексивные списки доступа

R2(config)#**ip access-list extended OUTBOUNDFILTERS**
R2(config-ext-nacl)#**permit tcp 192.168.0.0 0.0.255.255 any reflect TCPTRAFFIC**
R2(config-ext-nacl)#**permit icmp 192.168.0.0 0.0.255.255 any reflect ICMPTRAFFIC** — заставляем маршрутизатор отслеживать трафик, который инициировался изнутри

R2(config)#**ip access-list extended INBOUNDFILTERS**
R2(config-ext-nacl)#**evaluate TCPTRAFFIC**
R2(config-ext-nacl)#**evaluate ICMPTRAFFIC** — создаем входящую политику, которая требует, чтобы маршрутизатор проверял входящий трафик, чтобы видеть инициировался ли изнутри и связываем TCPTRAFFIC к INBOUNDFILTERS.

R2(config)#**interface serial 0/1/0**
R2(config-if)#**ip access-group INBOUNDFILTERS in**
R2(config-if)#**ip access-group OUTBOUNDFILTERS out** — применяем входящий и исходящий ACL на интерфейс


Заполните, пожалуйста,
опрос о занятии по ссылке в чате


До новых встреч!
Приходите на следующие занятия
Рукин Андрей
преподаватель
cisco@sk12.ru