**Packet Tracer. Настройка и модификация стандартных списков контроля доступа для IPv4**

**Таблица адресации**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| R1 | G0/0/0 | 192.168.10.1 | 255.255.255.0 | — |
| *R1* | G0/0/1 | 192.168.20.1 | 255.255.255.0 | *—* |
| *R1* | S0/1/0 (DCE) | 10.1.1.1 | 255.255.255.252 | *—* |
| Edge | S0/1/0 | 10.1.1.2 | 255.255.255.252 | — |
| *Edge* | S0/1/1 (DCE) | 10.2.2.2 | 255.255.255.252 | *—* |
| *Edge* | S0/2/1 | 209.165.200.225 | 255.255.255.224 | *—* |
| R3 | G0/0/0 | 192.168.30.1 | 255.255.255.0 | — |
| *R3* | G0/0/1 | 192.168.40.1 | 255.255.255.0 | *—* |
| *R3* | S0/1/1 | 10.2.2.1 | 255.255.255.252 | *—* |
| S1 | VLAN 1 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 |
| S2 | VLAN 1 | 192.168.20.11 | 255.255.255.0 | 192.168.20.1 |
| S3 | VLAN 1 | 192.168.30.11 | 255.255.255.0 | 192.168.30.1 |
| S4 | VLAN 1 | 192.168.40.11 | 255.255.255.0 | 192.168.40.1 |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-B | NIC | 192.168.20.3 | 255.255.255.0 | 192.168.20.1 |
| PC-C | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |
| PC-D | NIC | 192.168.40.3 | 255.255.255.0 | 192.168.40.1 |

**Задачи**

**Часть 1. Проверка связи**

**Часть 2. Настройка и проверка стандартных нумерованных списков ACL и стандартных именованных ACL-списков**

**Часть 3. Изменение стандартного ACL-списка**

**Общие сведения и сценарий**

Обеспечение сетевой безопасности является важным аспектом при разработке и управлении IP-сетями. Ценным навыком является умение применять соответствующие правила для фильтрации пакетов на основе установленной политики безопасности.

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 Edge, расположенном между R1 и R3, ACL-списки не будут использоваться. У вас не будет прав административного доступа к маршрутизатору ISP, поскольку вы можете управлять только собственным оборудованием.

**Инструкция**

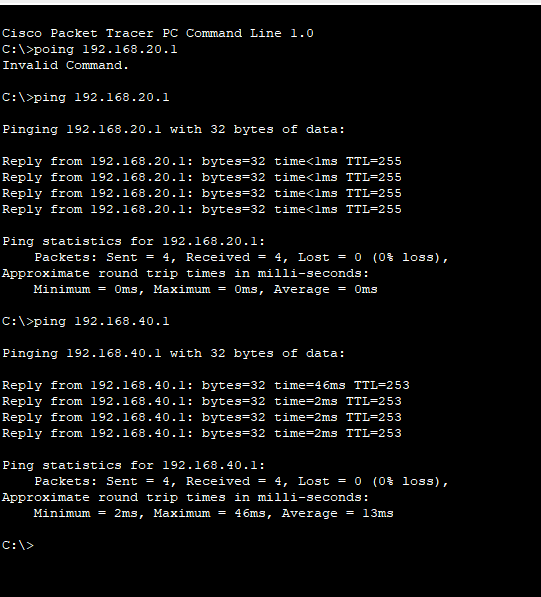
**Часть 1. Проверка связи**

В части 1 выполняется проверка соединения между устройствами.

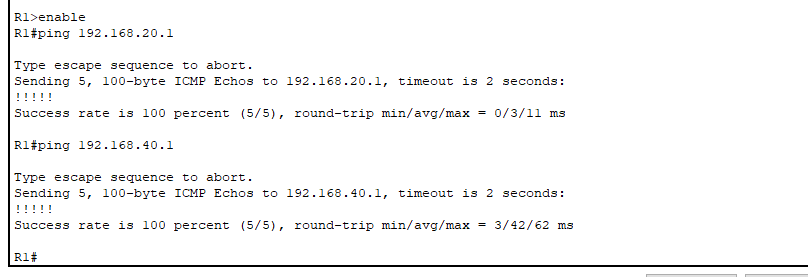
**Примечание.** Соединение важно проверять **перед** настройкой и применением списков доступа! Удостовериться в правильной работе сети необходимо до начала фильтрации трафика.

Вопросы:

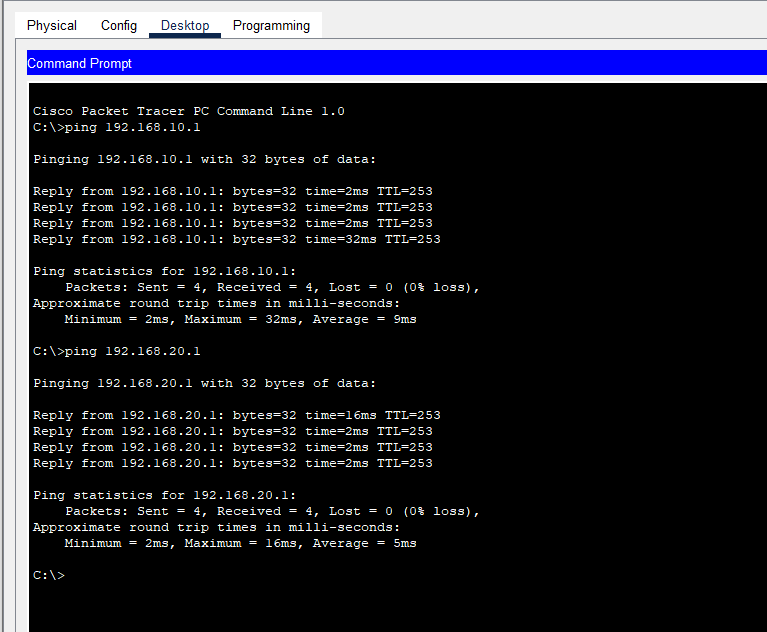
От PC-A, запустите ping до PC-C и PC-D. Ваши пинги были успешными?



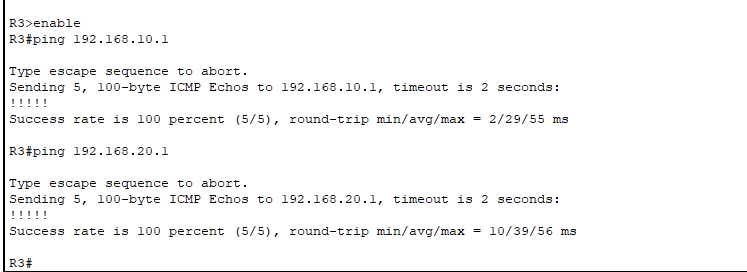
От R1, запустите ping до PC-C и PC-D. Ваши пинги были успешными?



От PC-C, запустите ping до PC-A и PC-B. Ваши пинги были успешными?



От R3, запустите ping до PC-A и PC-B. Ваши пинги были успешными?



Могут ли все ПК выполнить ping запрос на сервер в 209.165.200.254? Да

**Часть 2. Настройка и проверка стандартных нумерованных и именованных списков управления доступом**

**Шаг 1: Настройка нумерованного стандартного списка управления доступом.**

Стандартные ACL-списки фильтруют трафик, исходя только из адреса источника. Согласно принятой рекомендации стандартные ACL-списки следует настраивать и применять как можно ближе к назначению. Для первого списка доступа создайте стандартный нумерованный ACL-список, который пропускает трафик от всех узлов в сети 192.168.10.0/24 и всех узлов в сети 192.168.20.0/24 ко всем узлам в сети 192.168.30.0/24. Согласно политике безопасности в конце всех ACL-списков должна содержаться запрещающая запись контроля доступа **deny any** (ACE), которую также называют оператором ACL-списка.

Вопросы:

Какую шаблонную маску вы будете использовать, чтобы разрешить всем узлам из сети 192.168.10.0/24 доступ к сети 192.168.30.0/24? 0.0.0.255

Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список? R3

На каком интерфейсе вы разместите этот список? В каком направлении вы его примените? G0/0/0 out

a.     Настройте ACL на R3. В качестве номера списка доступа используйте 1.

*Откройте окно конфигурации*

R3(config)# **access-list 1 remark Allow R1 LANs Access**

R3(config)# **access-list 1 permit 192.168.10.0 0.0.0.255**

R3(config)# **access-list 1 permit 192.168.20.0 0.0.0.255**

R3(config)# **access-list 1 deny any**

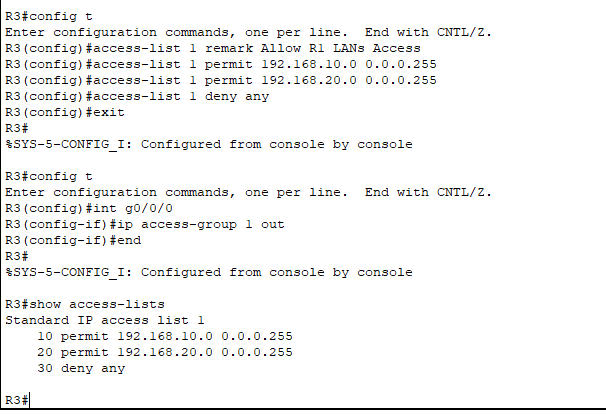
б.     Примените ACL-список к подходящему интерфейсу в нужном направлении.

R3(config)# **interface g0/0/0**

R3(config-if)# **ip access-group 1 out**

в.     Проверьте нумерованный ACL-список.

Использование команды **show**поможет вам при проверке синтаксиса и размещении списков ACL в вашем маршрутизаторе.



Вопросы:

Какую команду вы будете использовать для просмотра полного списка доступа 1 со всеми записями ACE? Show access-lists

Какую команду вы будете использовать, чтобы просмотреть, где и в каком направлении был применен список доступа? Show ip interface g0/0/0

1)    На маршрутизаторе R3 выполните команду **show access-lists 1**.

R3# **show** **access-list 1**

Standard IP access list 1

permit 192.168.10.0, wildcard bits 0.0.0.255

permit 192.168.20.0, wildcard bits 0.0.0.255

deny any

2)    На маршрутизаторе R1 выполните команду **show ip interface brief**.

R3# **show ip interface g0/0/0**

GigabitEthernet0/0/0 is up, line protocol is up (connected)

Internet address is 192.168.30.1/24

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

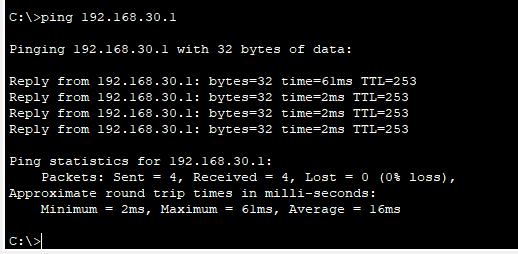
Outgoing access list is 1

Inbound access list is not set

<Вывод пропущен >Вопросы:

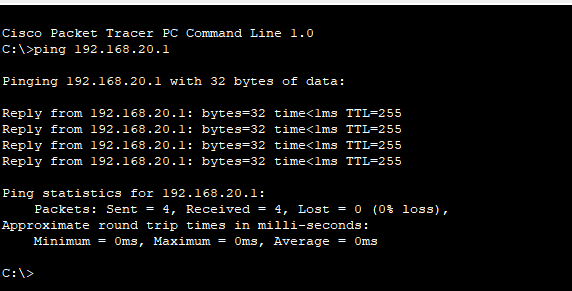
3)    Проверьте, пропускает ли ACL-список трафик из сети 192.168.10.0/24 в сеть 192.168.30.0/24.

Из командной строки узла PC-A отправьте эхо-запрос на IP-адрес PC-C. Успешно ли выполнена проверка связи?

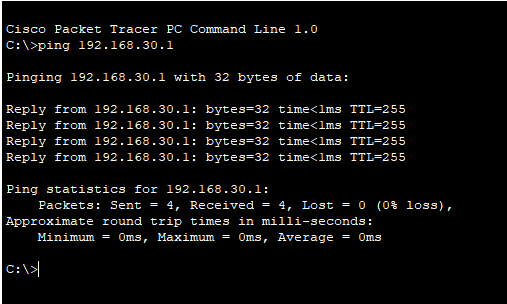


4)    Проверьте, пропускает ли ACL-список трафик из сети 192.168.20.0/24 в сеть 192.168.30.0/24.

Из командной строки узла PC-B отправьте эхо-запрос на IP-адрес PC-C. Успешно ли выполнена проверка связи?

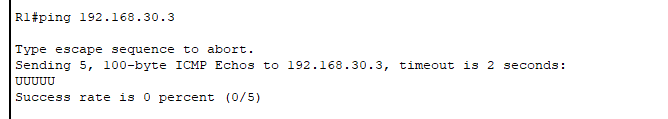


5) Должны ли запросы ping от PC-D до PC-C быть успешными? Запустите Ping от PC-D до PC-C, чтобы проверить ваш ответ.



г.     Из командной строки маршрутизатора R1 снова отправьте эхо-запрос на IP-адрес узла PC-C.

R1# **ping 192.168.30.3**



Вопрос:

Успешно ли выполнен эхо-запрос? Дайте пояснение. Access list не пропускает пакет

д.     На маршрутизаторе R3 выполните команду **show access-lists 1**. Обратите внимание, что в выходных данных команды отображается информация о количестве раз, когда каждый ACE был сопоставлен трафиком, достигающим интерфейса Gigabit Ethernet 0/0/0.

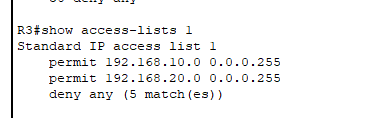
R3# **show access-lists 1**

Standard IP access list 1

permit 192.168.10.0 0.0.0.255 (4 match(es))

permit 192.168.20.0 0.0.0.255 (4 match(es))

deny any (4 match(es))\



**Шаг 2. Настройте стандартный именованный список контроля доступа.**

Создайте стандартный именованный ACL-список, который соответствует следующему правилу: список должен разрешать доступ для трафика со всех узлов из сети 192.168.40.0/24 ко всем узлам в сети 192.168.10.0/24. Кроме того, доступ в сеть 192.168.10.0/24 должен быть разрешен только для узла PC-C. Этот список доступа должен быть назван BRANCH-OFFICE-POLICY.

Вопросы:

Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список? R1

На каком интерфейсе вы разместите этот список? В каком направлении вы его примените? G0/0/0 OUT

a.     Создайте стандартный ACL-список под именем BRANCH-OFFICE-POLICY на маршрутизаторе R1.

R1(config)# **ip access-list standard BRANCH-OFFICE-POLICY**

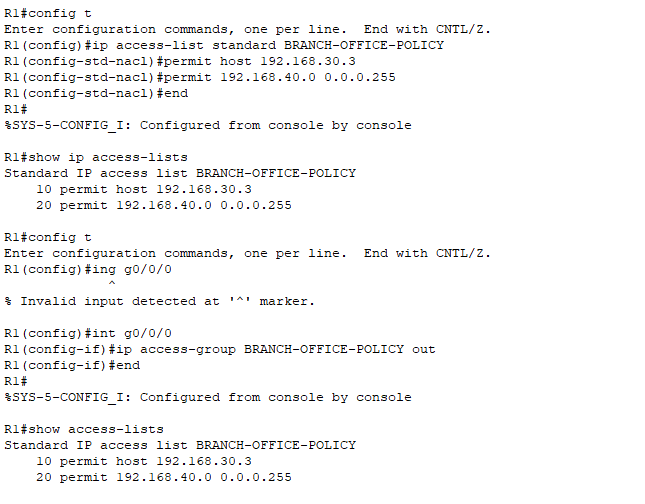
R1(config-std-nacl)# **permit host 192.168.30.3**

R1(config-std-nacl)# **permit 192.168.40.0 0.0.0.255**

R1(config-std-nacl)# **end**

R1#

\*Feb 15 15:56:55.707: %SYS-5-CONFIG\_I: Configured from console by console



Вопрос:

Посмотрите на первый ACE в списке доступа. Каков еще один способ написать это?

б.     Примените ACL-список к подходящему интерфейсу в нужном направлении.

R1# **config t**

R1(config)# **interface g0/0/0**

R1(config-if)# **ip access-group BRANCH-OFFICE-POLICY out**

в.     Проверьте именованный ACL-список.

1)    На R1 выполните команду show access-lists.

R1# **show** **access-lists**

Standard IP access list BRANCH-OFFICE-POLICY

10 permit host 192.168.30.3

20 permit 192.168.40.0 0.0.0.255

Вопрос:

Существуют ли различия между ACL-списком на маршрутизаторе R1 и ACL-списком на маршрутизаторе R3? Если да, в чем они заключаются?

2)    На R1 выполните команду **show ip interface g0/0/0**, чтобы проверить, что ACL настроен на интерфейсе.

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 BRANCH-OFFICE-POLICY

Inbound access list is not set

Вопрос:

Проверьте работу ACL-списка. Из узла PC-C отправьте эхо-запрос на IP-адрес узла PC-A. Получены ли ответы на ping-запросы?

3)    Проверьте ACL-список, чтобы удостовериться, что доступ к сети 192.168.10.0/24 настроен только на узле PC-C. Вам нужно выполнить расширенный эхо-запрос и использовать адрес G0/0/0 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A.

R3# **ping**

Protocol [ip]:

Target IP address: **192.168.10.3**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 192.168.30.1

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:

Packet sent with a source address of 192.168.30.1

U.U.U

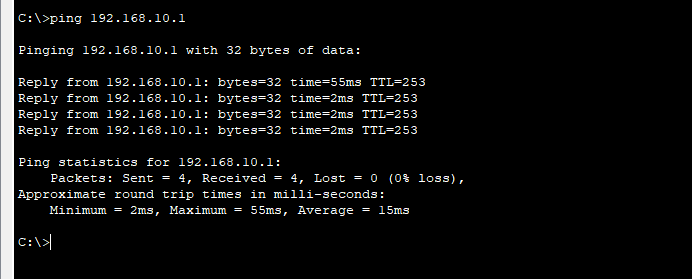
Вопрос:

Успешно ли выполнена проверка связи?

4)    Проверьте, пропускает ли ACL-список трафик из сети 192.168.40.0/24 в сеть 192.168.10.0/24. Из командной строки узла PC-D отправьте эхо-запрос на IP-адрес PC-A.

Вопрос:

Успешно ли выполнена проверка связи?



*Закройте окно настройки.*

**Часть 3. Изменение стандартного ACL-списка**

Политика безопасности нередко претерпевает изменения. По этой причине ACL-списки тоже необходимо изменять. В части 3 необходимо изменить один из ранее настроенных списков контроля доступа для соответствия новой политике безопасности.

Попытка выполнить эхо-запрос сервера на 209.165.200.254 с PC-A. Обратите внимание на то, что эхо-запрос не прошел. ACL на R1 блокирует возврат интернет-трафика на PC-A. Это связано с тем, что адрес источника в возвращаемых пакетах не входит в диапазон разрешенных адресов.

Руководство решило, что пользователи из сети 209.165.200.224/27 должны получить полный доступ к сети 192.168.10.0/24. Также руководство хочет, чтобы правила в ACL-списках на всех их маршрутизаторах выполнялись последовательно. В конце всех ACL-списков должна быть внесена запись ACE **deny any**. Вам необходимо изменить ACL-список с именем BRANCH-OFFICE-POLICY.

Также вам предстоит добавить в этот список ACL две дополнительные строки. Это можно сделать двумя способами:

**Вариант 1**: Выполните команду **no access-list standard BRANCH-OFFICE-POLICY** в режиме глобальной конфигурации. Это приведет к удалению ACL с маршрутизатора. В зависимости от IOS маршрутизатора, произойдет один из следующих вариантов: вся фильтрация пакетов будет отменена, и все пакеты будут пропускаться через маршрутизатор; либо, поскольку команда **ip access-group в интерфейс G0/1** активна, фильтрация останется прежней. В любом случае, когда ACL-список будет удален, вы сможете заново ввести весь ACL-список или вырезать и вставить записи из текстового редактора.

**Вариант 2**: ACL-списки можно изменить, не удаляя, добавив или удалив конкретные строки из ACL-списка. Этот вариант наиболее удобен, особенно в случае если ACL-список содержит много записей. При повторном вводе всего ACL-списка или при вырезании и копировании могут возникнуть ошибки. В изменении определенных строк в списках ACL нет ничего сложного.

Для этого задания используйте вариант 2.

**Шаг 1: Изменение стандартного именованного ACL-списка.**

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

*Откройте окно конфигурации*

R1# **show access-lists**

Standard IP access list BRANCH-OFFICE-POLICY

10 permit 192.168.30.3 (8 matches)

20 permit 192.168.40.0 0.0.0.255 (5 matches)

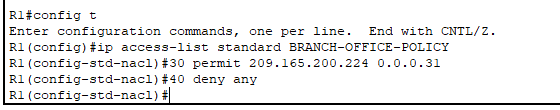
б.     Добавьте две дополнительные строки в конец ACL-списка. В режиме глобальной конфигурации измените ACL-список с именем BRANCH-OFFICE-POLICY.

R1#(config)# **ip access-list standard BRANCH-OFFICE-POLICY**

R1(config-std-nacl)# **30 permit 209.165.200.224 0.0.0.31**

R1(config-std-nacl)# **40 deny any**

R1(config-std-nacl)# **end**



в.     Проверьте ACL-список.

1)    На R1 выполните команду **show access-lists**.

R1# **show access-lists**

Standard IP access list BRANCH-OFFICE-POLICY

10 permit 192.168.30.3 (8 matches)

20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)

30 permit 209.165.200.224, wildcard bits 0.0.0.31

40 deny any

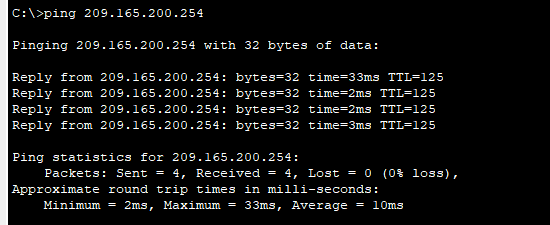
Вопрос:

Нужно ли вам применить список под именем BRANCH-OFFICE-POLICY на интерфейсе G0/1 маршрутизатора R1? Нет

2)    Проверьте, пропускает ли список ACL трафик из сети 209.165.200.224/27 в сеть 192.168.10.0/24. С PC-A выполните эхо-запрос сервера на 209.165.200.254.

Вопрос:

Успешно ли выполнена проверка связи?



*Закройте окно настройки.*

**Вопросы для повторения**

1.     Как вы видите, стандартные ACL-списки достаточно эффективны и полезны. Зачем вам когда-либо понадобилось использовать расширенные списки ACL? Для фильтрации пакетов не только по IP

2.     В большинстве случаев при использовании именованного ACL-списка требуется введение большего количества строк, нежели при использовании нумерованного ACL-списка. Почему вы бы предпочли использовать именованный ACL-список, а не нумерованный?  
С именованным списком легче работать, т.к его имя отражает его назначение, а номер ничего не означает

*Конец документа*