Министерство образования и науки Калужской области

ГБПОУ КО «Калужский техникум электронных приборов

Исследовательская работа на тему:

# Создание ACCESS листов для локальной вычислительной сети при организации демонстрационного экзамена по стандартам WorldSkills в рамках государственной итоговой аттестации выпускников СПО

Работу выполнил:

Преподаватель ГБПОУ КО КТЭП

Федоров В.В.

Калуга, 2018

# Введение

На предыдущем этапе проектирования общей концепции сетевой модели для использования в процессе демонстрационного экзамена, была реализована модель VLAN, позволяющая изолировать участников друг от друга и от внешних сетей, а также модель коммутации и маршрутизации. Представленные модели были реализованы в сетевом эмуляторе Cisco Packet Tracer на языке описания для оборудования Cicso. Данная модель адаптировалась к структуре организации сети в ГБПОУ КО «Калужский техникум электронных приборов» и претерпела несущественные изменения, по сравнению с оригинальной версией. Для интеграции с существующими сетями было необходимо подключить дополнительный коммутатор Cisco (Коммутатор 0, рисунок 1), позволяющий полноценно использовать создаваемую структуру на основе VLAN, интегрировав ее в работающую на данный момент сетевую инфраструктуру организации. Модернизированная сетевая модель представлена на рисунке 1 и включает в себя 12 изолированных подсетей для участников, 1 изолированную подсеть для экспертов, 1 изолированную подсеть для доступа к глобальной сети Internet и одну серверную подсеть.

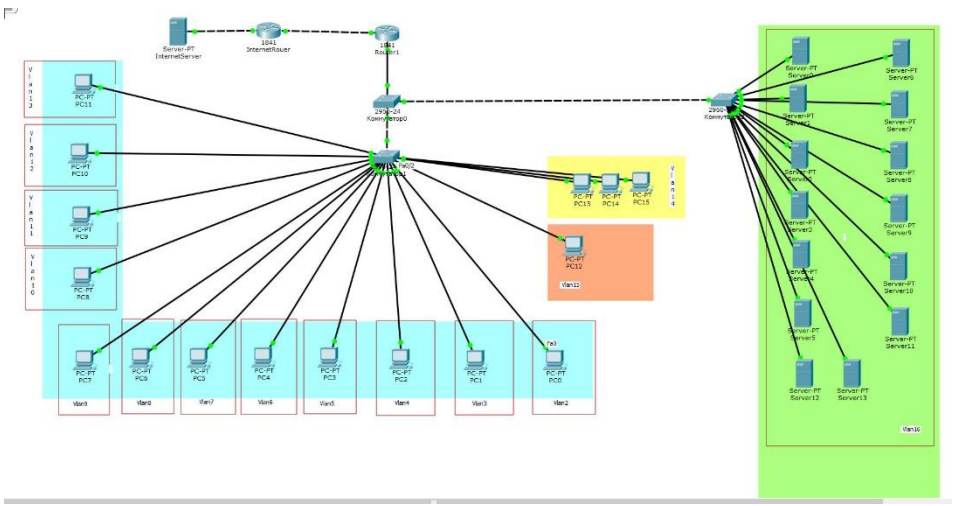


Рисунок 1 – Модернизированная сетевая модель

Настройки дополнительного коммутатора включают в себя существующие VLANы для полноценного соединения с прочим оборудованием посредством тегированного канала связи (рисунок 2).

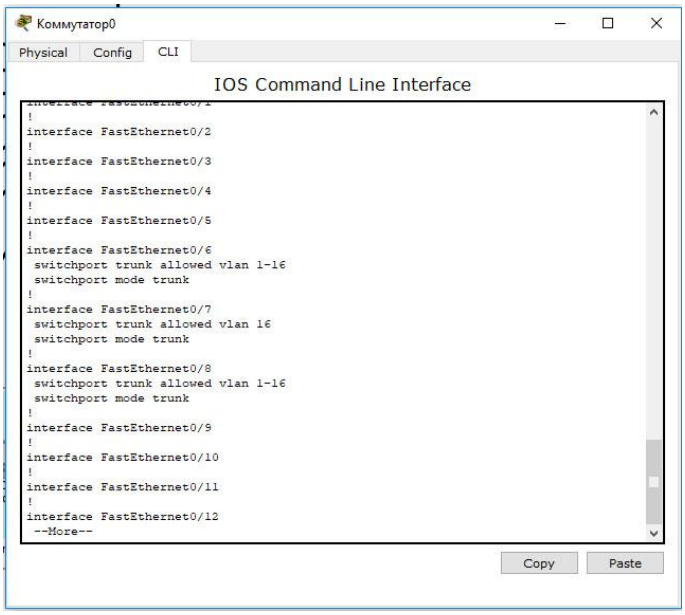



Рисунок 2 – Листинг настроек интерфейсов коммутатора 0

Для этого использовались 6-8 сетевые интерфейсы в режиме TRUNK, причем интерфейс на стороне сервера (Fa 0/7) включал в себя только один VLAN, в то время как 6 и 8 интерфейсы включали в себя весь перечень тегированного трафика, за исключением подсети по умолчанию, использующейся для коммуникации внутри организации. На данном этапе построения сети, вследствие создания внутренних маршрутов, изолированные подсети получают возможность взаимного доступа, что легко проверяется при помощи пингования различных сетевых сегментов (рисунок 3). Сам по себе факт успешного пиногования разных подсетей относительно друг друга говорит о правильной настройке маршрутизации, однако не позволяет использовать ее для проведения демонстрационного экзамена на данном этапе.

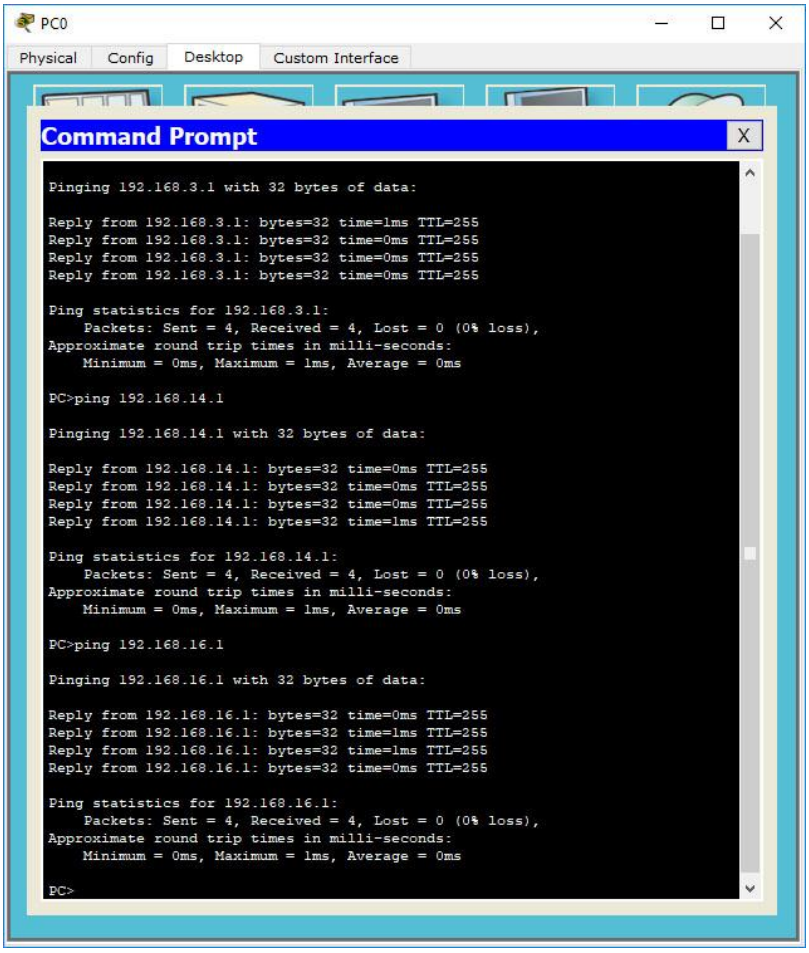



Рисунок 3 – Пинг с компьютра первого участника подсети второго участника, подсети экспертов и подсети серверов

Исходя из этого возникла необходимость создания блокирующего механизма для выборочного доступа подсетей и хостов, включаемых в указанные подсети друг к другу. Наиболее оптимальным, в данном случае является использование так называемых листов доступа (access lists), привязанных к интерфейсу маршрутизатора, и позволяющих выборочно ограничивать межсетевой трафик в соответсвии с требованиями, предъявляемыми к демонстрационному экзамену по стандартам Worldskills в рамках государственной итоговой аттестации выпускников СПО.

## Постановка целей и задач

Соответственно с проблематикой, указанной в предыдущей главе, была сформулирована цель настоящего исследования:

Обеспечить ограниченный механизм ограничения доступа межсетевого взаимодействия в моделируемой сети для демонстрационного экзамена.

В соответствии с требованиями, предъявляемыми для организации демонстрационного экзамена по стандартам WorldSkills в рамках государственной итоговой аттестации выпускников СПО, было выделено ряд задач:

- исследовать механизмы ограничения доступа при маршрутизации изолированных подсетей, выбрав наиболее оптимальные.
- обеспечить изоляцию участников друг от друга, а также изоляцию от остальных сегментов сети;
- обеспечить доступ для хостов подсети экспертов к любой другой подсети;
- обеспечить доступ хостов участников только к собственному выделенному серверу, находящемуся в 16 подсети, при этом исключить возможность доступа к серверам других участников.

# Глава 1. Исследование Access Control List (списков доступа) Cisco IOS

С целью защиты маршрутизаторов от различных рисков – случайных и злонамеренных – списки ACL (списки доступа) для защиты инфраструктуры необходимо определять на точках входа в сеть. Списки управления доступом IPv4 и IPv6 отказывают в доступе от внешних источников на все адреса инфраструктуры, например, интерфейсы маршрутизаторов. В то же время, списки ACL разрешают непрерывный поток транзитного трафика и предоставляют основные RFC 1918 , RFC 3330 , а также фильтрацию ложных IP-пакетов.

Данные, принимаемые маршрутизатором, можно разделить на две обширные категории:

- трафик, который проходит через маршрутизатор по пути пересылки
- трафик, предназначенный для маршрутизатора через путь приема, для обработки его процессором маршрутизации

При нормальной работе, основная часть трафика проходит через маршрутизатор по пути к конечному пункту назначения.[1] Технологии фильтрации предназначены для фильтрации данных, предназначенных для оборудования сетевой инфраструктуры. Следует различать фильтрацию инфраструктуры и общую фильтрацию. Единственной целью списков ACL для защиты инфраструктуры является ограничение на гранулярном уровне протоколов и источников, которые могут получить доступ к оборудованию инфраструктуры. Исходя из этого можно сказать, что списки доступа (access-lists) используются в целом ряде случаев и являются общим механизмом задания условий, которые роутер проверяет перед выполнением каких-либо действий. Ниже приведены некоторые примеры использования списков доступа:

- Управление передачей пакетов на интерфейсах

- Управление доступом к виртуальным терминалам роутера и управлению через SNMP
- Ограничение информации, передаваемой динамическими протоколами роутинга.[2]

Иными словами ACL — это набор текстовых выражений, которые что-то разрешают, либо что-то запрещают. Обычно ACL разрешает или запрещает IP-пакеты, но помимо всего прочего он может заглядывать внутрь IP-пакета, просматривать тип пакета, TCP и UDP порты. Также ACL существует для различных сетевых протоколов (IP, IPX, AppleTalk и так далее). В основном применение списков доступа рассматривают с точки зрения пакетной фильтрации.[3] Список доступа представляет собой набор строк вида условие-действие. Строка аксесс-листа называется access-control-entry (ACE). Условием может быть соответствие пакета определенному протоколу или набору параметров. Действием может быть разрешение пакета (permit), либо запрещение (deny). Для списков доступа справедливы следующие правила:

- созданный список доступа не действует, пока он не применен к конкретному интерфейсу.
- список доступа применяется на интерфейсе в конкретном направлении – для исходящего, либо входящего трафика (inbound/outbound).
- к интерфейсу можно применить только по одному аксесс-листу на протокол (ip), на направление (in/out).
- список доступа проверяется строка за строкой до первого совпадения. Оставшиеся строки игнорируются;
- в конце любого IP аксесс-листа подразумевается запрещающее правило (implicit deny). Пакет, не попавший ни под одно условие в списке, отбрасывается, в соответствии с правилом implicit deny;

- рекомендуется более специфические правила указывать в начале аксесс-листа, а более общие – в конце;
- новые строки по умолчанию дописываются в конец списка.
- Отдельную строку можно удалить из именованного аксесс-листа, другие ACL удаляются лишь целиком;
- список доступа должен иметь по крайней мере один permit, иначе он будет блокировать весь трафик;
- интерфейс, которому назначен несуществующий аксесс-лист не фильтрует трафик;
- IP Extended Access-lists применяются как можно ближе к источнику трафика.[4]

В cisco-устройствах Access Control List разделяют на два вида:

- Standard ACL – список правил, позволяющий выполнять фильтрацию по ip адресу источника в пакете;
- Extended ACL – список правил, позволяющий выполнять фильтрацию по ip адресу источника и получателя в пакете, а так же имеет возможность выполнять фильтрацию по портам tcp и udp.[5]

Расширенные списки управления доступом вводятся в действие применительно к интерфейсам для пакетов, либо входящих в интерфейс, либо исходящих из интерфейса. Система IOS проводит поиск в этом списке последовательно. Расширенные списки доступа также используют логику первого соответствия, поскольку маршрутизатор останавливает поиск по списку, как только обнаруживается первый соответствующий оператор, и предпринимает определенное в нем действие.[6]

# Глава 2. Применение списков доступа для Cisco IOS для разрабатываемой сетевой модели

Для изоляции подсетей участников применение стандартного access листа на исходящий трафик – наиболее целесообразно. Согласно методики проведения демоэкзамена, доступ к компьютерам участников может быть только из подсети экспертов и подсети серверов. Для первого участника, формирование access листа будет выглядеть следующим образом:

Router(config)#ip access-list standard TO_VLAN2

Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255

Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255

Все остальные подсети будут запрещены посредством неявного правила «deny ip any any», которое запрещает «все остальное».

Router(config-std-nacl)#exit

Далее необходимо привязать этот access лист к соответствующему исходящему интерфейсу. В нашем случае – это логический интерфейс fa 0/1.2

Router(config)#int fa 0/1.2

Router(config-subif)#ip access-group TO_VLAN2 out

Router(config-subif)#exit

Доступ к подсетям остальных участников ограничивается сходным образом (таблица 8).

Таблица 8. Создание стандартного листа доступа к внешней сети Internet

| Имя подсети | Описание подсети | Router(config)#ip access-list standard | Описание |
|---|---|---|---|
| Vlan1 | 192.168.1.0/24 | | |
| Vlan2 | 192.168.2.0/24 | Router(config)#ip access-list standard TO_VLAN2<br>Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit | Запрет доступа к подсети участника 1 для всех, кроме сегмента эксперта и серверов |

| Имя подсети | Описание подсети | Router(config)#ip access-list standard | Описание |
|---|---|---|---|
| | | Router(config)#int fa 0/1.2<br>Router(config-subif)#ip access-group TO_VLAN2 out<br>Router(config-subif)#exit | |
| Vlan3 | 192.168.3.0/24 | Router(config)#ip access-list standard TO_VLAN3<br>Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit<br>Router(config)#int fa 0/1.3<br>Router(config-subif)#ip access-group TO_VLAN3 out<br>Router(config-subif)#exit | Запрет доступа к подсети участника 2 для всех, кроме сегмента эксперта и серверов |
| Vlan4 | 192.168.4.0/24 | Router(config)#ip access-list standard TO_VLAN4<br>Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit<br>Router(config)#int fa 0/1.4<br>Router(config-subif)#ip access-group TO_VLAN4 out<br>Router(config-subif)#exit | Запрет доступа к подсети участника 3 для всех, кроме сегмента эксперта и серверов |
| Vlan5 | 192.168.5.0/24 | Router(config)#ip access-list standard TO_VLAN5<br>Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit<br>Router(config)#int fa 0/1.5<br>Router(config-subif)#ip access-group TO_VLAN5 out<br>Router(config-subif)#exit | Запрет доступа к подсети участника 4 для всех, кроме сегмента эксперта и серверов |
| Vlan6 | 192.168.6.0/24 | Router(config)#ip access-list standard TO_VLAN6<br>Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit<br>Router(config)#int fa 0/1.6<br>Router(config-subif)#ip access-group TO_VLAN6 out<br>Router(config-subif)#exit | Запрет доступа к подсети участника 5 для всех, кроме сегмента эксперта и серверов |
| Vlan7 | 192.168.7.0/24 | Router(config)#ip access-list standard TO_VLAN7<br>Router(config-std-nacl)#permit | Запрет доступа к подсети участника 6 для всех, кроме сегмента эксперта и серверов |

| Имя подсети | Описание подсети | Router(config)#ip access-list standard | Описание |
|---|---|---|---|
| | | 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit<br>Router(config)#int fa 0/1.7<br>Router(config-subif)#ip access-group TO_VLAN7 out<br>Router(config-subif)#exit | |
| Vlan8 | 192.168.8.0/24 | Router(config)#ip access-list standard TO_VLAN8<br>Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit<br>Router(config)#int fa 0/1.8<br>Router(config-subif)#ip access-group TO_VLAN8 out<br>Router(config-subif)#exit | Запрет доступа к подсети участника 7 для всех, кроме сегмента эксперта и серверов |
| Vlan9 | 192.168.9.0/24 | Router(config)#ip access-list standard TO_VLAN9<br>Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit<br>Router(config)#int fa 0/1.9<br>Router(config-subif)#ip access-group TO_VLAN9 out<br>Router(config-subif)#exit | Запрет доступа к подсети участника 8 для всех, кроме сегмента эксперта и серверов |
| Vlan10 | 192.168.10.0/24 | Router(config)#ip access-list standard TO_VLAN10<br>Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit<br>Router(config)#int fa 0/1.10<br>Router(config-subif)#ip access-group TO_VLAN10 out<br>Router(config-subif)#exit | Запрет доступа к подсети участника 9 для всех, кроме сегмента эксперта и серверов |
| Vlan11 | 192.168.11.0/24 | Router(config)#ip access-list standard TO_VLAN11<br>Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit<br>Router(config)#int fa 0/1.11<br>Router(config-subif)#ip access-group TO_VLAN11 out | Запрет доступа к подсети участника 10 для всех, кроме сегмента эксперта и серверов |

| Имя подсети | Описание подсети | Router(config)#ip access-list standard | Описание |
|---|---|---|---|
| | | Router(config-subif)#exit | |
| Vlan12 | 192.168.12.0/24 | Router(config)#ip access-list standard TO_VLAN12<br>Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit<br>Router(config)#int fa 0/1.12<br>Router(config-subif)#ip access-group TO_VLAN12 out<br>Router(config-subif)#exit | Запрет доступа к подсети участника 11 для всех, кроме сегмента эксперта и серверов |
| Vlan13 | 192.168.13.0/24 | Router(config)#ip access-list standard TO_VLAN13<br>Router(config-std-nacl)#permit 192.168.14.0 0.0.0.255<br>Router(config-std-nacl)#permit 192.168.16.0 0.0.0.255<br>Router(config-std-nacl)#exit<br>Router(config)#int fa 0/1.13<br>Router(config-subif)#ip access-group TO_VLAN13 out<br>Router(config-subif)#exit | Запрет доступа к подсети участника 12 для всех, кроме сегмента эксперта и серверов |
| Vlan14 | 192.168.14.0/24 | | |
| Vlan15 | 192.168.15.0/24 | | |
| Vlan16 | 192.168.16.0/24 | | |

Не менее важным моментов является ограничение доступа к виртуальным серверам участников, так как именно там хранятся выполняемые задания. Соответственно полный доступ к своему VDS должен иметь участник, находящийся в своей подсети и пользователи подсети экспертов (Vlan14). Созданный access лист, предназначенный для организации упорядоченного доступа к серверным ресурсам будет выглядеть следующим образом:

Router(config)#ip access-list extended TO_SERVERS

Router(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 host 192.168.16.2

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.2

Router(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 host 192.168.16.3

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.3

Router(config-ext-nacl)#permit ip 192.168.4.0 0.0.0.255 host 192.168.16.4

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.4

Router(config-ext-nacl)#permit ip 192.168.5.0 0.0.0.255 host 192.168.16.5

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.5

Router(config-ext-nacl)#permit ip 192.168.6.0 0.0.0.255 host 192.168.16.6

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.6

Router(config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 host 192.168.16.7

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.7

Router(config-ext-nacl)#permit ip 192.168.8.0 0.0.0.255 host 192.168.16.8

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.8

Router(config-ext-nacl)#permit ip 192.168.9.0 0.0.0.255 host 192.168.16.9

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.9

Router(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 host 192.168.16.10

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.10

Router(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 host 192.168.16.11

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.11

Router(config-ext-nacl)#permit ip 192.168.12.0 0.0.0.255 host 192.168.16.12

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.12

Router(config-ext-nacl)#permit ip 192.168.13.0 0.0.0.255 host 192.168.16.13

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.13

Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.14

Router(config-ext-nacl)#exit

Как и в предыдущем случае, все остальные подсети будут запрещены посредством неявного правила «deny ip any any».

Подробное описание структуры правил ограничения доступа к VDS сети представлено в таблице 9.

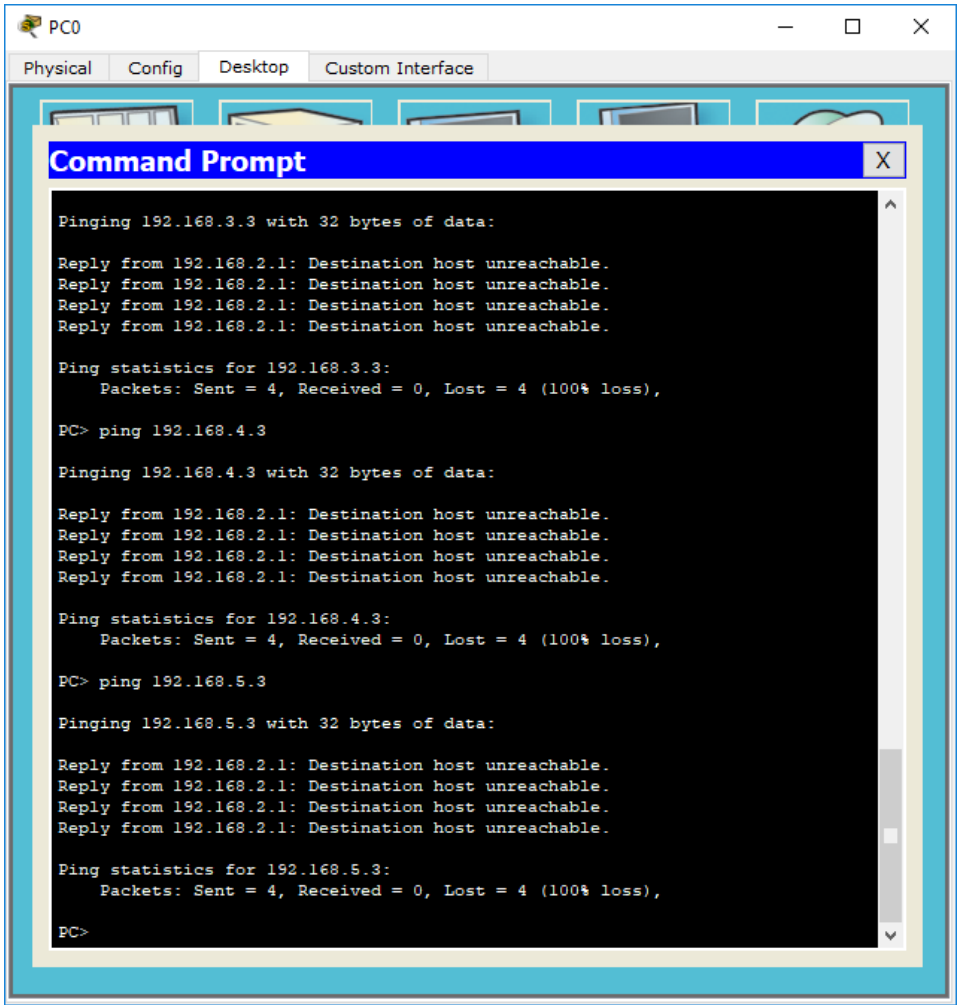
Таблица 9. Создание расширенного листа доступа на исходящий интерфейс fa 0/1.16 (интерфейс сегмента серверов)

| **Имя подсети** | **Описание подсети** | **Router(config)#ip access-list extended TO_SERVERS** | **Описание** |
|---|---|---|---|
| Vlan1 | 192.168.1.0/24 | | |
| Vlan2 | 192.168.2.0/24 | Router(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 host 192.168.16.2<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.2 | Доступ подсети участника 1 и экспертов к Server0 |
| Vlan3 | 192.168.3.0/24 | Router(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 host 192.168.16.3<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.3 | Доступ подсети участника 2 и экспертов к Server1 |
| Vlan4 | 192.168.4.0/24 | Router(config-ext-nacl)#permit ip 192.168.4.0 0.0.0.255 host 192.168.16.4<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.4 | Доступ подсети участника 3 и экспертов к Server2 |
| Vlan5 | 192.168.5.0/24 | Router(config-ext-nacl)#permit ip 192.168.5.0 0.0.0.255 host 192.168.16.5<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.5 | Доступ подсети участника 4 и экспертов к Server3 |
| Vlan6 | 192.168.6.0/24 | Router(config-ext-nacl)#permit ip 192.168.6.0 0.0.0.255 host 192.168.16.6<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.6 | Доступ подсети участника 5 и экспертов к Server4 |
| Vlan7 | 192.168.7.0/24 | Router(config-ext-nacl)#permit ip 192.168.7.0 0.0.0.255 host 192.168.16.7<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.7 | Доступ подсети участника 6 и экспертов к Server5 |
| Vlan8 | 192.168.8.0/24 | Router(config-ext-nacl)#permit ip 192.168.8.0 0.0.0.255 host 192.168.16.8<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.8 | Доступ подсети участника 7 и экспертов к Server6 |
| Vlan9 | 192.168.9.0/24 | Router(config-ext-nacl)#permit ip 192.168.9.0 0.0.0.255 host 192.168.16.9<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.9 | Доступ подсети участника 8 и экспертов к Server7 |
| Vlan10 | 192.168.10.0/24 | Router(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 host 192.168.16.10<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.10 | Доступ подсети участника 9 и экспертов к Server8 |
| Vlan11 | 192.168.11.0/24 | Router(config-ext-nacl)#permit ip 192.168.11.0 | Доступ подсети |

| Имя подсети | Описание подсети | Router(config)#ip access-list extended TO_SERVERS | Описание |
|---|---|---|---|
| | | 0.0.0.255 host 192.168.16.11<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.11 | участника 10 и экспертов к Server9 |
| Vlan12 | 192.168.12.0/24 | Router(config-ext-nacl)#permit ip 192.168.12.0 0.0.0.255 host 192.168.16.12<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.12 | Доступ подсети участника 11 и экспертов к Server10 |
| Vlan13 | 192.168.13.0/24 | Router(config-ext-nacl)#permit ip 192.168.13.0 0.0.0.255 host 192.168.16.13<br>Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.13 | Доступ подсети участника 12 и экспертов к Server11 |
| Vlan14 | 192.168.14.0/24 | Router(config-ext-nacl)#permit ip 192.168.14.0 0.0.0.255 host 192.168.16.14 | Доступ подсети экспертов к Server12 |

## Заключение

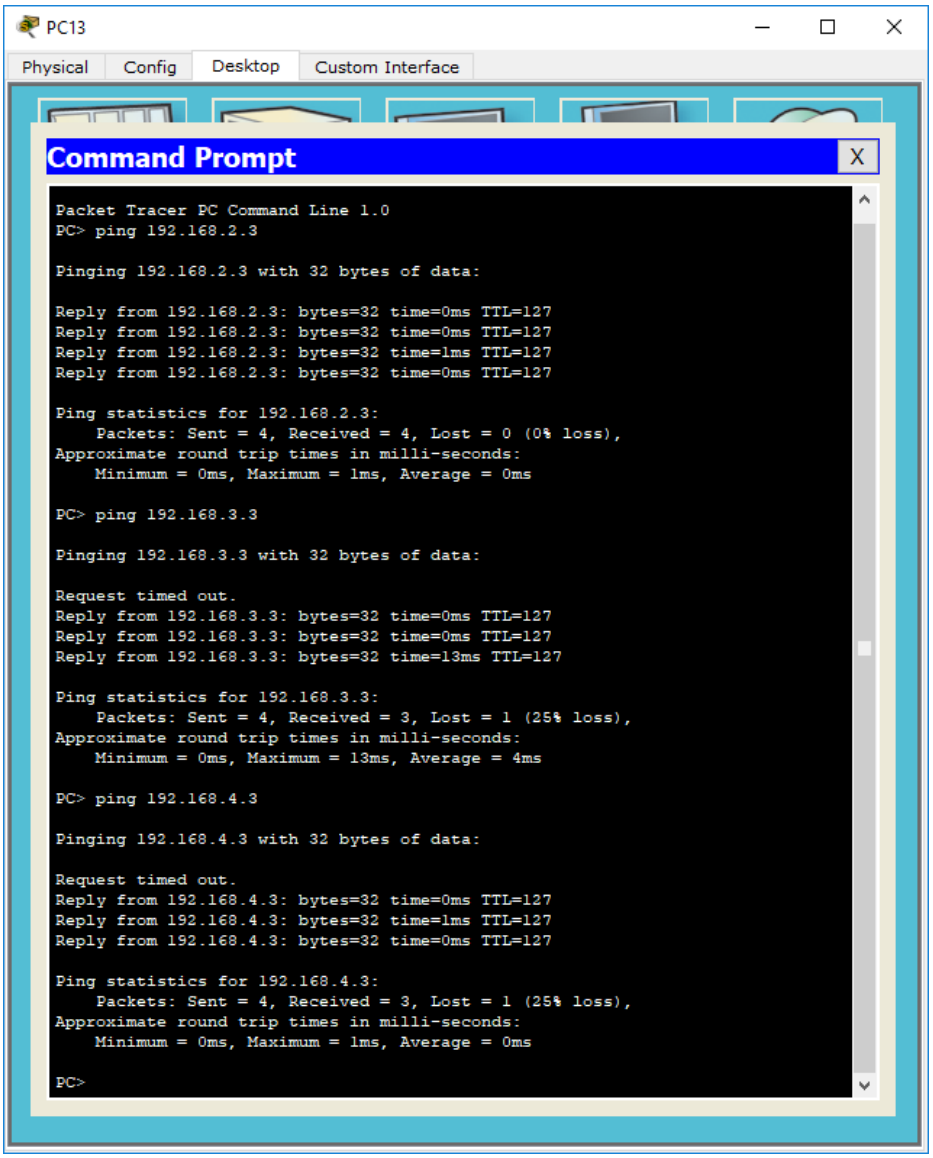
В результате применения созданных стандартных списков доступа, согласно общей схеме организации модели сети для демонстрационного экзамена по стандартам WorldSkills в рамках государственной итоговой аттестации выпускников СПО удалось добиться ограничения доступа хостов из подсетей участников к другим подсетям (рисунок 1), что исключает



возможность стороннего воздействия на процесс проведения демоэкзамена как из внешней сети, так и из внутренних подсетей.

Рисунок 4 – Результаты пинга подсети участника 2 и участника 3 из посети первого участника

При этом удалось сохранить доступ к подсетям участников из подсети экспертов (рисунок 5), что позволяет потенциальное использование программ, предназначенных для контроля за проводимыми участниками




действиями со стороны экспертной группы.

Рисунок 5 – результаты пинга хостом подсети экспертов хостов подсети участников 1, 2, 3

Использование расширенных ACCESS листов позволило организовать выборочный доступ участников к серверам 16 подсети (рисунок 6). Выборочный доступ к виртуальным серверам позволяет обезопасить VDS участника от негативного воздействия со стороны соседних и внешних подсетей. При этом доступ хостов из подсети экспертов так и остался неограниченным, что в свою очередь потенциально может привести к уязвимости системы в случае несанкционированной атаки со стороны компьютеров экспертов. Поэтому на время проведения демонстрационного экзамена принципиально важно уделять повышенное внимание доступу и проверке оборудования экспертов.

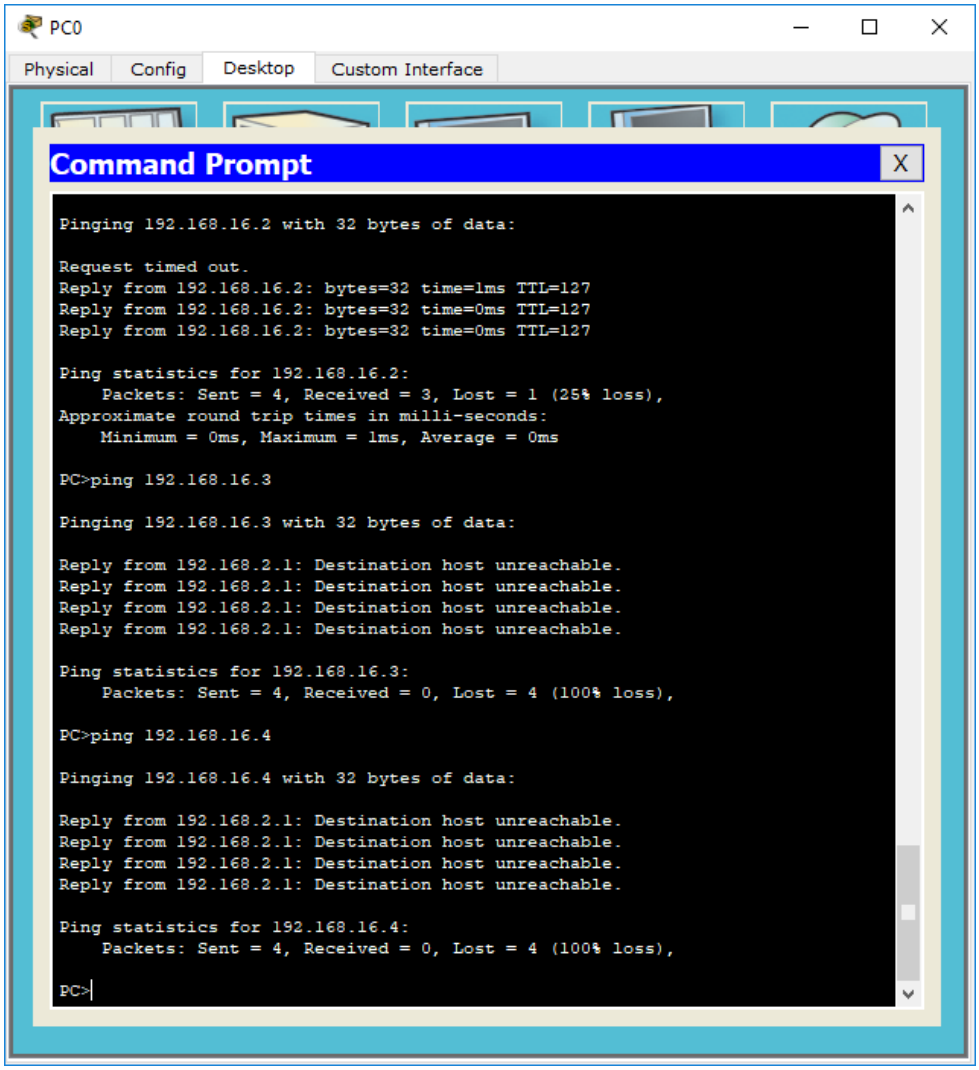



Рисунок 6 – Пинг VDS участника 1, пинг VDS участника 2, пинг VDS участника 3 из подсети первого участника

## Использованные источники:


1. Защита ядра: Списки управления доступом для защиты инфраструктуры. © 1992-2010 Cisco Systems, Inc.: [Электронный ресурс] http://www.cisco.com/support/RU/customer/content/10/107632/iacl.shtml
2. Списки доступа (Access Lists) в Cisco IOS (cisco acl firewall): [Электронный ресурс] http://www.opennet.ru/base/cisco/access_list_intro.txt.html
3. ACL: списки контроля доступа в Cisco IOS: [Электронный ресурс] https://habrahabr.ru/post/121806/
4. IP списки доступа Cisco IOS: [Электронный ресурс] https://k.psu.ru/wiki/IP_списки_доступа_Cisco_IOS
5. Access Control List: [Электронный ресурс] https://ciscolearning.ru/cisco-router/access-control-list/
6. Расширенные списки управления доступом: [Электронный ресурс] http://www.williamspublishing.com/PDF/978-5-8459-1811-6/part.pdf