Лабораторная работа 5
Списки контроля доступа

Цель работы – изучение технологий и протоколов обеспечения информационной безопасности на границе сетей на основе списков контроля доступа и представляет собой сценарий для Cisco Packet Tracer. Для успешного выполнения лабораторной работы студентам необходимо выполнить задание сценария и подготовить отчет (по своему варианту), а также защитить его в форме собеседования.

5.1. Теоретическая часть

5.1.1. Списки контроля доступа – назначение

Список контроля доступа (англ. access control list, ACL) — это последовательность команд IOS, определяющих порядок обработки пакетов маршрутизатором, а именно: должен ли маршрутизатор пропустить или заблокировать тот или иной пакет, исходя из информации в заголовке пакета. Списки контроля доступа являются основой обеспечения информационной безопасности на границе сетей и одной из наиболее используемых функций операционной системы Cisco IOS.

ACL предназначены для решения следующих классов задач:

- Ограничение сетевого трафика для повышения производительности сети. Например, если корпоративная политика запрещает видеотрафик в сети, необходимо настроить и применить ACL, блокирующие данный тип трафика. Подобные меры значительно снижают нагрузку на сеть и повышают её производительность.
- Ограничение служебного трафика. Например, ACL могут ограничивать доставку обновлений маршрутизации на отдельных участках сети, что позволяет сократить излишний служебный трафик.
- Ограничение доступа извне к отдельным сетевым расположениям. ACL обеспечивают базовый уровень информационной безопасности периметра сети, выборочно разрешая и запрещая внешний доступ к отдельным устройствам, сетевым ресурсам или участкам сети.
- Ограничение доступа по отдельным протоколам. ACL позволяют осуществлять фильтрацию трафика на основе типа трафика, например, разрешить трафик http или электронной почты, но при этом блокировать весь трафик протоколов telnet и ssh.

– Ограничение доступа отдельным пользователям к внешним ресурсам. ACL допускают сортировку пользователей и устройств в целях разрешения или запрета доступа к отдельным сетевым службам. Например, можно разрешить или запретить доступ из различных VLAN к определённым ресурсам или сетевым службам.

Маршрутизатор (или иное сетевое устройство, поддерживающее ACL) работает как фильтр пакетов, пропускает или отбрасывает пакеты на основе правил фильтрации. Для этого из заголовков каждого пакета, поступившего на интерфейсы маршрутизатора, извлекается служебная информация, необходимая для принятия решения о продвижении или блокировке пакета.

Из заголовков третьего (сетевого) уровня:

– IP-адрес источника;
– IP-адрес назначения.

Дополнительно может извлекаться из заголовков четвертого (транспортного) уровня:

– порт источника TCP/UDP;
– порт назначения TCP/UDP.

5.1.2. Порядок применения ACL

Создание ACL не дает команды маршрутизатору на его использование. Созданный ACL – это просто некий список в глобальной конфигурации маршрутизатора. Для того, чтобы ACL начал работать, его необходимо применить к определенном типу трафика. Например, ACL можно прикрепить:

– к интерфейсу (пакетная фильтрация);
– к линии telnet (ограничения доступа к маршрутизатору);
– к каналу VPN (какой трафик нужно шифровать);
– к сортировщику QoS (какой трафик обрабатывать приоритетнее);
– к преобразованию NAT (какие адреса транслировать).

Применительно к пакетной фильтрации, ACL размещаются на интерфейсах. При прикреплении ACL к интерфейсу маршрутизатор начинает просматривать входящий (поступающий на маршрутизатор) и исходящий (покидающий маршрутизатор) трафик. Соответственно ACL могут быть размещены на входящем или на исходящем направлении.

Рассмотрим пример. Пусть из внутренней сети поступает пакет на интерфейс маршрутизатора fa0/1. Маршрутизатор проверяет наличие ACL на интерфейсе. Если он есть, дальнейшая обработка ведется по правилам списка строго в том порядке, в котором записаны правила. Если ACL разрешает продвижение, пакет передается на выходной интерфейс (допустим, fa0/0); если

ACL запрещает продвижение пакета, пакет уничтожается. Если ACL на интерфейсе нет, пакет проходит без всяких ограничений. Перед отправкой пакета с выходного интерфейса, маршрутизатор проверяет интерфейс fa0/0 на наличие исходящего ACL (ACL может быть прикреплен на интерфейсе как входящий или исходящий).

При применении ACL к интерфейсам следует руководствоваться следующим правилом: **расширенные ACL следует размещать как можно ближе к источнику, стандартные же как можно ближе к получателю**. Это обеспечивает максимальную эффективность ACL. Вернемся к рассмотренному примеру. Прикрепление исходящего ACL на интерфейс fa0/1 будет неэффективным, хотя и ACL работать будет. Допустим, на маршрутизатор приходит tcp echo запрос (ping) для какого-то узла во внутренней сети. Маршрутизатор проверяет наличие ACL на внешнем интерфейсе fa0/0 – его нет, пакет проходит; далее проверяется внутренний интерфейс fa0/1, на данном интерфейсе есть ACL, настроенный как исходящий. Такая конфигурация не позволяет запрещенному пакету проникнуть во внутреннюю сеть, но прикрепление этого ACL к интерфейсу fa0/0 как входящего позволило бы уничтожить запрещенный пакет сразу при поступлении на маршрутизатор, сэкономив его вычислительные ресурсы.

При этом **нельзя разместить более 1 ACL на интерфейс, на протокол, на направление**. Другими словами, на одном интерфейсе одного маршрутизатора на входящем направлении для IP-протокола может быть назначен олько один ACL.

Ещё одно правило, касающееся самих маршрутизаторов, ACL не действуют на трафик, сгенерированный самим маршрутизатором.

5.1.3. Структура ACL

ACL представляет собой последовательность текстовых команд, начинающихся с ключевого слова permit (разрешить) либо deny (запретить). Чтение правил происходит строго в том порядке в котором они записаны в конфигурационном файле. Соответственно, когда пакет поступает на интерфейс, проверяется первое условие. Если пакет удовлетворяет первому условию, дальнейшая его обработка прекращается: он либо проходит через ACL дальше, либо уничтожается. В противном случае проверяется второе условие, и т.д. пока не будут проверены все условия. **Если пакет не удовлетворяет ни одному условию, он будет уничтожен**, т.к. в конце каждого списка стоит неявное правило deny any (запретить всё).

Рассмотрим пример (рис. 5.1). У пакетов, поступающих на маршрутизатор через интерфейс G0/0, проверяются адреса их источника на основе следующих записей стандартного ACL:

```
access-list 2 deny 192.168.10.10
access-list 2 permit 192.168.10.0 0.0.0.255
access-list 2 deny 192.168.0.0 0.0.255.255
access-list 2 permit 192.0.0.0 0.255.255.255
```

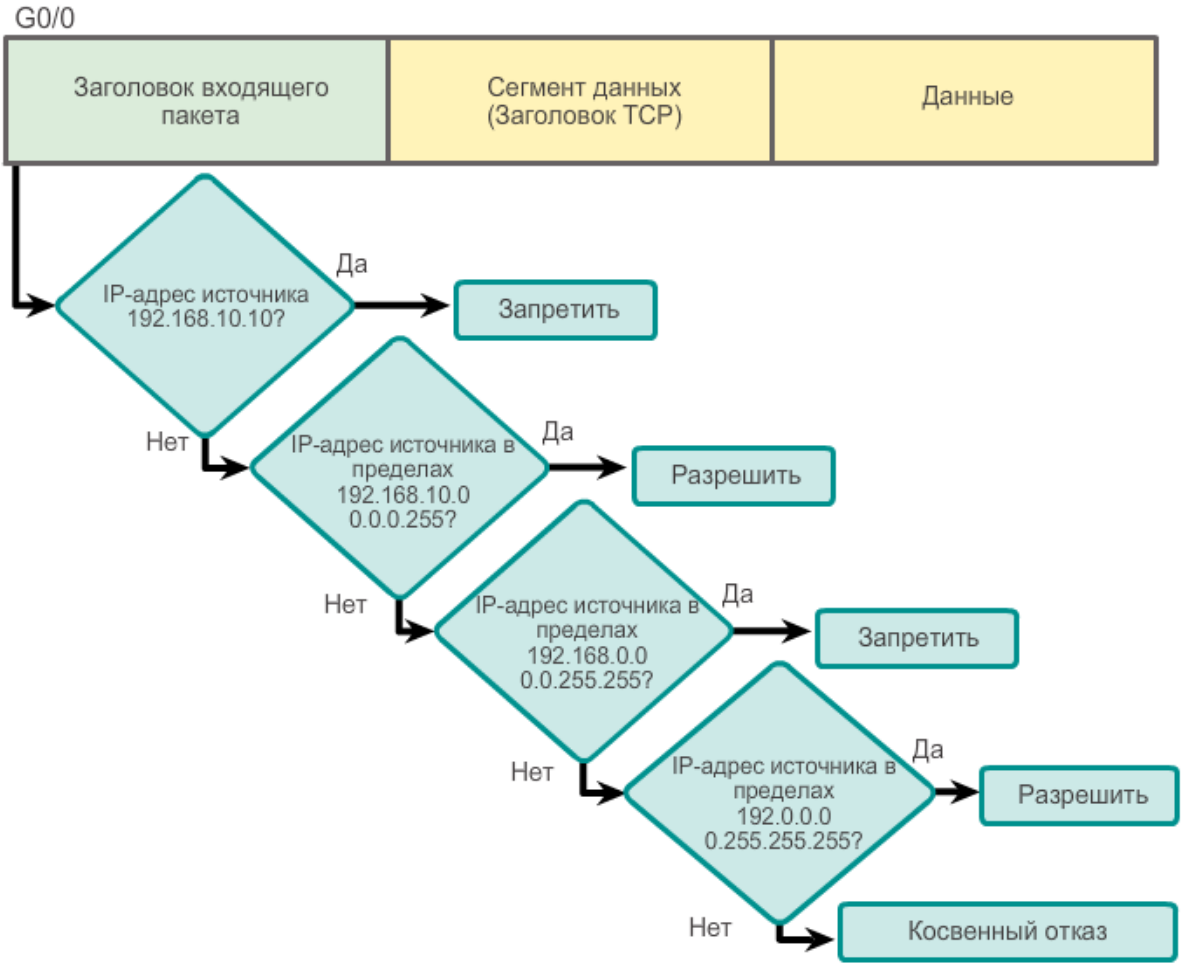

Рис. 5.2. Логика работы ACL

Напомним: когда трафик поступает на маршрутизатор, он сравнивается с записями в порядке, заданном в ACL-списке. Маршрутизатор продолжает обработку пакетов, пока не обнаружит совпадение. Маршрутизатор обрабатывает пакет на основе первого найденного совпадения, остальные записи маршрутизатором не учитываются.

Если к концу списка совпадения не найдены, маршрутизатор отклоняет трафик. Это объясняется тем, что по умолчанию в конце каждого ACL-списка содержится команда запрета для трафика, который не совпали ни с одной записью списка.

При создании ACL каждая его строка явно или неявно обозначается порядковым номером, по умолчанию в рамках десяти (10, 20, 30 и т.д). Такая нумерация облегчает удаление конкретных записей, в т.ч. из середины списка, и на её место вставить другую.

5.1.4. Стандартные и расширенные ACL

В Cisco IOS предусмотрено два типа ACL для IPv4: стандартные и расширенные.

Стандартные (англ. standard) ACL используются для принятия решения о разрешении или блокировке пакета на основе единственного параметра: IPv4-адреса источника, например:

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Данный список разрешает весь трафик из сети 192.168.30.0/24. Из-за неявного правила «deny any (запретить все, что не разрешено)» в конце списка данный ACL блокирует весь остальной трафик.

Расширенные (англ. extended) ACL фильтруют IPv4-пакеты, руководствуясь несколькими признаками:

- тип протокола;
- IPv4-адрес источника;
- IPv4-адрес назначения;
- TCP или UDP порт источника;
- TCP или UDP порт назначения.

Пример расширенного ACL:

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

Данный ACL разрешает трафику с любого адреса сети 192.168.30.0/24 идти в любую IPv4-сеть, если порт назначения — 80 (протокол http).

Стандартные и расширенные списки контроля доступа могут быть созданы с помощью номера или имени. Номер присваивается в зависимости то того, какой протокол будет фильтроваться:

- (от 1 до 99) и (от 1300 до 1999) – стандартные ACL протокола IP;
- (от 100 до 199) и (от 2000 до 2699) – расширенные ACL протокола IP.

Создание именованных ACL гораздо более удобно. При работе с именованными ACL используется собственный конфигурационный режим, упрощающий просмотр и редактирование ACL. Кроме этого, присвоение ACL имён упрощает понимание функции того или иного списка. Так, ACL,

настроенному для запрета протокола ftp, рекомендуется присвоить имя, по смыслу которого будет понятно его назначение, например, «no_ftp». Именованные ACL также разделяются на стандартные и расширенные.

Расширенные ACL могут проверять гораздо больше параметров, нежели стандартные, но и работают они медленнее, так как маршрутизатору приходится проводить более глубокий анализ пакета, в отличие от стандартных ACL, где проверяется единственный параметр – IP-адрес отправителя.

Кроме указанных типов ACL в Cisco IOS предусмотрены временные (англ. time-based), «зеркальные» (англ. reflexive) и динамические (англ. dynamic, lock-and-key) ACL. Временные ACL позволяют применять различные правила в различные дни и часы, например, ограничивать доступ к определенным ресурсам в рабочее время. Зеркальные ACL позволяют отслеживать состояние сессий, открытых из внутренней сети компании, и создавать соответствующие возвратные правила. Динамические ACL применяют те или иные правила в зависимости от набора прав, полученных пользователем в результате аутентификации. Отметим, что последние три типа списков контроля доступа не будут рассмотрены в настоящем курсе.

5.1.5. Команды IOS

Рассмотрим список новых команд IOS, необходимых и достаточных для выполнения лабораторной работы 5. Более простые команды см. в описании лабораторных работ 1-4, а также в контекстной справке Cisco IOS (команда ?).

Команды привилегированного режима

`router#`

```
show access-lists [номер или имя ACL]
```

Выводит указанный ACL или все ACL, если конкретный не указан.

Команды режима глобального конфигурирования

`router(config)#`

```
access-list <номер списка от 1 до 99> {permit | deny | remark}
{<адрес сети> <wildcard-маска> | any | host <IP-адрес узла>}
[log]
```

Создает стандартный нумерованный ACL и/или добавляет в него команду: разрешить или запретить трафик с данного источника.

Параметры команды:

- действие: permit – разрешить, deny – запретить, remark – добавить комментарий (текстовое пояснение, не является правилом фильтрации);
- источник трафика: сеть с данной wildcard-маской, any – любой источник; host [IP-адрес] – конкретный узел;
- ключевое слово log (опционально) включает логирование пакетов, удовлетворяющих текущему правилу.

```
access-list <номер списка от 100 до 199> {permit | deny |
remark} <протокол> {<адрес сети> <wildcard-маска> | any | host
<IP-адрес узла>} [<operator> <порт или название протокола>]
{<адрес сети> <wildcard-маска> | any | host <IP-адрес узла>}
[<operator> <порт или название протокола>] [established]
```

Создает расширенный нумерованный ACL и/или добавляет в него команду: разрешить или запретить трафик указанного протокола от указанного источника (можно указать номера портов источника) к данному получателю (можно указать номера портов назначения).

Параметры команды:

- действие: permit/deny/remark – см. выше;
- протокол: какой протокол разрешаем/запрещаем (например: icmp, ip, tcp, udp, ospf и т.д.);
- источник трафика: сеть/any/host – см. выше;
- назначение трафика: сеть/any/host – аналогично источнику;

– operator: фильтр портов источника/назначения; принимает значения: eq [port] – точное совпадение (конкретный номер порта); gt [port] – номера портов, больше указанного; lt [port] – номера портов, меньше указанного; neq [port] – любые номера портов, кроме указанного; range [port1 port2] – все номера портов в указанном промежутке;
– ключевое слово established разрешает прохождение TCP-сегментов, которые являются частью уже созданной TCP-сессии.

```
access-list {standard | extended} <имя ACL>
```

Создает стандартный или расширенный именованный ACL и/или переводит консоль в режим конфигурирования ACL.

```
access-list resequence <имя ACL> <номер0> <шаг>
```

Выполняет перенумерацию строк в указанном списке контроля доступа; новые порядковые номера правил начинаются с указанного номера и следуют с указанным шагом.

Команды конфигурирования ACL

```
router(config-ext-nacl)#
router(config-std-nacl)#
```

```
[номер строки] {permit | deny | remark} ...
```

Добавляет строку в текущий ACL и присваивает ей указанный порядковый номер (если параметр указан – иначе правило помещается в конец списка). Формат строки зависит от типа ACL: стандартный или расширенный.

Команды конфигурирования интерфейса

```
router(config-if)#
```

```
ip access-group <номер или имя ACL> {in | out}
```

Прикрепляет указанный ACL к текущему интерфейсу в указанном направлении – включает фильтрацию трафика.

5.2. Задание к лабораторной работе

Лабораторная работа выполняется в среде Cisco Packet Tracer в предложенном Вам файле-сценарии формата pka. Сценарий содержит созданную заранее логическую топологию в виде составной сети, моделирующей

корпоративную сеть условного предприятия, подключенную к сети Интернет (рис. 5.2). Устройства не настроены.

Необходимо выполнить расчет IP-адресов локальных сетей и устройств, настроить все устройства (компьютеры и маршрутизаторы), маршрутизацию и списки контроля доступа.

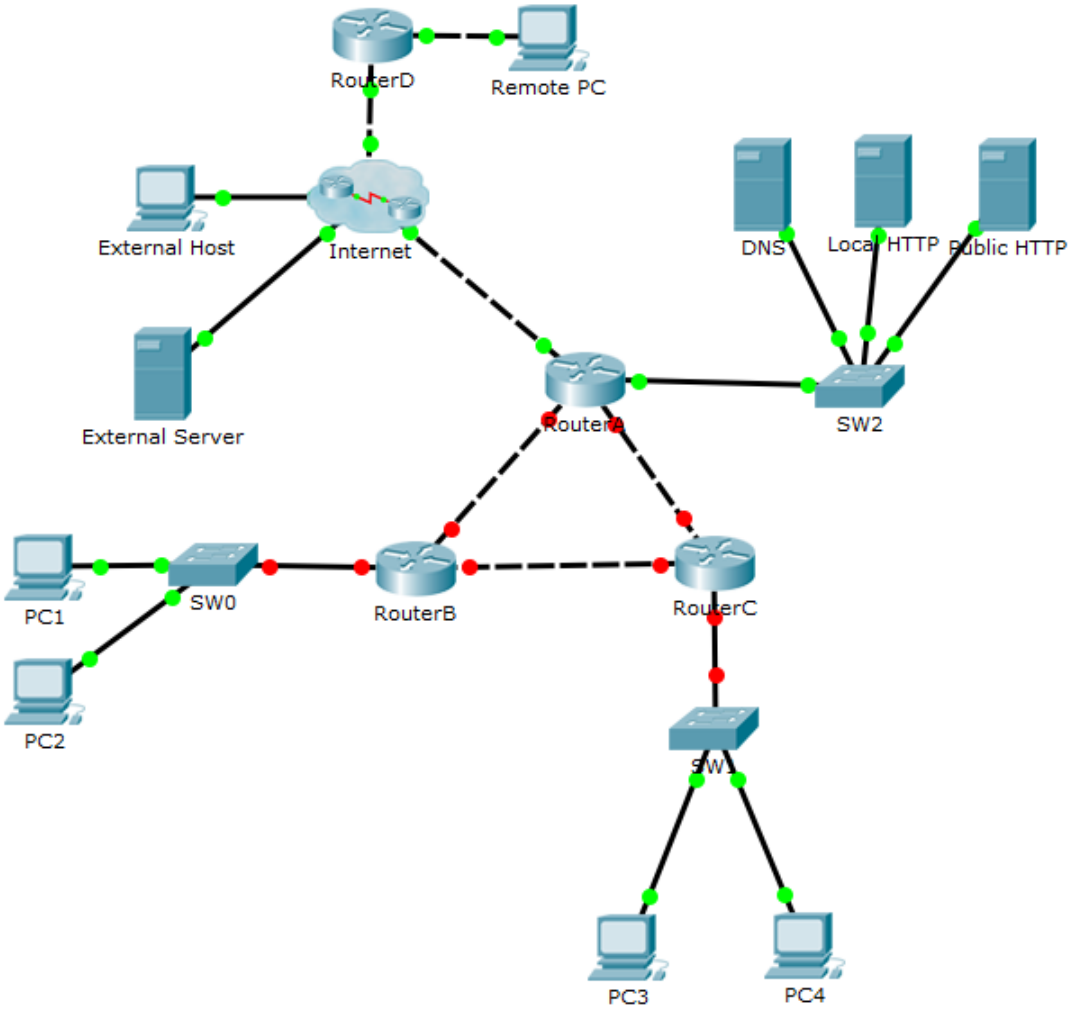

Рис. 5.2. Топология сети

Напомним ряд важных правил создания ACL:

- Для применения ACL его необходимо связать с интерфейсом.
- Обработка пакета ACL ведется строго в том порядке, в котором записаны правила.
- Если пакет удовлетворяет правилу, оно применяется, и обработка пакета прекращается – правила ниже прочитаны не будут.
- В конце каждого ACL стоит неявное правило «deny any (запретить всё)».

– Расширенные ACL следует размещать как можно ближе к источнику, стандартные – как можно ближе к получателю.
– Нельзя применить более 1 списка доступа на интерфейс, на протокол, на направление.
– ACL не действует на трафик, сгенерированный самим маршрутизатором.
– Адреса сетей записываются в ACL с wildcard маской.

5.2.1. Расчёт IP-адресов и настройка локальных сетей

Выполнить расчет основных сетевых параметров для сетей VLAN A, VLAN B, VLAN C и VLAN D исходя из известного количества узлов в каждой из них (согласно Вашему варианту), а также известного диапазона адресов для внутренней сети (где X – номер Вашего варианта): 10.X.0.0/16. Для служебных сетей, соединяющих между собой маршрутизаторы, использовать любые подсети из того же диапазона, размеры данных подсетей выбрать минимально возможными. Для сети с серверами использовать сеть 192.168.0.0/16.

Присвоить номера и наименования виртуальным сетям. Наименование VLAN задать в формате #Фамилия. Номера виртуальных сетей:

– для сети VLAN A = 2X+10;
– для сети VLAN B = 2X+11;
– для сети VLAN C = 2X+12;
– для сети VLAN D = 2X+13.

Пример: Студент с номером 34 Василий Пупкин создает виртуальную сеть VLAN A номер 78 с именем 78pupkin.

Рассчитанные адреса занести в отчет.

Выполнить настройку компьютеров (настроить IP-адрес, маску подсети и шлюз по умолчанию). Задать компьютерам IP-адреса из соответствующих диапазонов. Как и ранее, использовать для компьютеров максимальные IP-адреса из доступных. Компьютеры распределить по виртуальным сетям следующим образом: PC1 – Vlan A, PC2 – Vlan B, PC3 – Vlan C, PC4 – Vlan D.

Выполнить настройку серверов:

– DNS: 192.168.1.2;
– HTTP local: 192.168.X.254 (http://local.com);
– HTTP public: 192.168.X+1.254 (http://public.com).

Используя вкладку Services, убедиться, что на серверах настроены необходимые службы: dns и веб-сервер.

На вкладке Services/DNS добавить dns-записи для серверов public, local и external, установив соответствие между их IP-адресами и доменными именами.

На вкладке Services/HTTP произвольно отредактировать веб-страницы серверов public и local. Обязательное требование к веб-страницам: должны отображаться ФИО студента, номер группы и варианта. *Не используйте кириллицу!*

5.2.2. Настройка устройств

Выполнить первоначальную настройку маршрутизаторов (присвоить символьные имена, задать пароли для доступа к консоли, привилегированному режиму и виртуальному терминалу, включить шифрование всех паролей и добавить баннер). *Подробнее о первоначальной настройке устройств см. методические рекомендации к лабораторной работе 1.*

Настроить виртуальные локальные сети. Обратите внимание, что виртуальные сети в этом сценарии создаются на коммутаторах отдельно, протокол vtp работать не будет, т.к. коммутаторы разделены маршрутизатором Router B.

Настроить интерфейсы и суб-интерфейсы на маршрутизаторах. В локальных сетях использовать **минимальные** IP-адреса из доступных. В остальных подсетях использовать минимальный адрес для маршрутизатора с меньшим порядковым номером.

Используя команды проверки конфигурации (show), убедиться в правильности введенных настроек. Присвоенные адреса занести в отчет.

5.2.3. Настройка маршрутизации

Настроить маршрутизацию любым способом (статическая, RIP, OSPF; **обязательно** отключить автосуммирование маршрутов).

Подробнее о настройке маршрутизации см. методические рекомендации к лабораторным работам 3 и 4.

Используя команды проверки конфигурации (show), tcp echo запросы (ping) и веб-браузеры на компьютерах, убедиться в правильности введенных настроек. Основной критерий: на этом этапе веб-страницы серверов public и local должны быть доступны с любого компьютера в сети (включая internet user) как по IP-адресу, так и по доменному имени.

5.2.4. Настройка ACL

Руководствуясь правилами, приведенными в начале раздела 5.3, настроить на маршрутизаторах списки контроля доступа, ограничив трафик следующим образом:

- ДЛЯ VLAN A:

    - Дать доступ ко всем узлам сети по любом протоколу, в том числе к сети интернет. Исключение: удаленный пк.
- ДЛЯ VLAN B:
    - Доступ к интернету по протоколу HTTP и dns;
    - Доступ к серверу PUBLIC по протоколу HTTP и dns.
- ДЛЯ VLANC:
    - Доступ к серверу LOCAL по протоколу HTTP.
- ДЛЯ VLAND:
    - Доступ к сети интернет по всем протоколам;
    - Доступ к удаленному пк по протоколу icmp.
- ДЛЯ сети интернет:
    - Доступ по протоколам dns и http к серверу PUBLIC;
- ДЛЯ связи между виртуальными сетями (VLAN):
    - Открытый доступ по протоколу icmp.
- ДЛЯ удаленного хоста:
    - Разрешить получение icmp пакетов только от VLAND;
    - Дать доступ к серверу LOCAL по dns и http;
    - В сегменте сети с удаленным пк разрешается использовать только стандартные ACL.

ПОЛЕЗНАЯ ИНФОРМАЦИЯ:

Remote PC = Удаленный ПК.

tcp 80 – http трафик.

udp 53 – dns трафик.

Удаленный ПК является частью корпоративной сети и его адрес можно использовать при постановке ограничений.

permit tcp any any established – команда для разрешения ответных сообщений для протокола tcp. Если у устройства A есть доступ к устройству B, а у устройства B нет доступа к устройству A, то данная команда позволит, при обращении устройства A к устройству B, получить ответ от устройства B, который дойдет до устройства A, несмотря на отсутствие явного доступа.

permit icmp any any echo-reply – команда для разрешения ответов по ICMP. Any может быть заменено на адрес сети с маской или ip конкретного узла.

Для того, чтобы дать доступ устройству к серверу по протоколу DNS необходимо:

- *Разрешить доступ этому устройству к DNS-серверу по протоколу dns (udp 53);*
- *Разрешить доступ устройству к конечному серверу по протоколу http (tcp 80).*

ВНИМАНИЕ! Сеть Интернет не имеет конкретного адреса. В моделируемой топологии сегмент Internet условно обозначает отдельный участок сети Интернет. В связи с этим адрес сети, в которой находятся internet user и internet server, не должен использоваться в конфигурации маршрутизаторов. Вместо этого при настройке ACL необходимо использовать ключевое слово any, а при настройке маршрутизации – маршруты по умолчанию.

Контрольные вопросы

1. Какие существуют способы обеспечения информационной безопасности на границе сетей?
2. Что такое список контроля доступа?
3. Какие бывают списки контроля доступа?
4. Какова структура списка контроля доступа?
5. На каких типах устройств применяются списки контроля доступа?
6. Как осуществляется фильтрация пакетов на основании списка контроля доступа?
7. Приведите пример списка контроля доступа. Расскажите, как он работает.
8. Что происходит с пакетом, для которого не найдено совпадений в списке контроля доступа?
9. Что происходит с пакетом, для которого в списке контроля доступа более одного совпадения?
10. Как правильно применять различные виды списков контроля доступа?

5.3. Варианты индивидуальных заданий

Номер варианта	Количество узлов в сети			
	VLAN A	VLAN B	VLAN C	VLAN D
1	45	5	1765	156
2	12	643	125	1531
3	156	23	1235	786
4	32	1843	100	23
5	63	342	75	5
6	276	75	167	1832
7	754	34	175	1353
8	53	15	1634	259
9	434	43	179	1256

Номер варианта	Количество узлов в сети			
	VLAN A	VLAN B	VLAN C	VLAN D
10	564	342	57	134
11	8	194	45	785
12	87	115	1023	5
13	543	75	79	87
14	130	54	743	250
15	76	5	1026	356

5.4. Форма отчета

Отчет о выполнении лабораторной работы оформляется в соответствии с индивидуальным вариантом задания и является обязательным требованием для допуска к защите наряду с правильно настроенным сценарием работы в программе Packet Tracer.

Отчет должен включать титульный лист, схему сети, а также заполненные таблицы, приведенные ниже.

5.4.1. Расчет адресов сетей

Параметр	VLAN A	VLAN B	VLAN C	VLAN D
Количество узлов				
Маска (префикс)				
Маска (десятичн.)				
Маска (инверсная)				
SUBNET				
BROADCAST				

5.4.2. Расчет адресов служебных сетей

Сеть	Адрес / маска (префиксная)
RA – RB	
RA – RC	
RB – RC	

5.4.3. Сведения о конфигурации устройств

Устр-во	Интерфейс		IP-адрес/ VLAN	Маска подсети	**Шлюз** (где необходимо)
Router A					
Router B					

Устр-во	Интерфейс	IP-адрес/ VLAN	Маска подсети	**Шлюз** (где необходимо)
Router C				
Internet				
Switch0				
SW1				
SW3				
PC 1	NIC			
PC 2	NIC			
PC 3	NIC			
PC 4	NIC			
DNS	NIC			
Local http	NIC			
Public http	NIC			

5.4.4. Сведения о настроенных ACL

(добавить необходимое количество строк)

Устр-во	Интер-фейс	Напр. трафика (in/out)	Правила