Лабораторная работа №7

Списки контроля доступа

Цель: научиться использовать технологию access control list (ACL) для ограничение доступа к сетевым ресурсам.

1. Теоретические сведения

Списки контроля доступа (Access Control List - ACL) - это фильтры, которые обеспечивают базовый уровень безопасности сети. Посредством ACL администратор управляет сетевым трафиком, обеспечивая доступ к требуемым ресурсам зарегистрированным легальным пользователям и запрещая несанкционированный доступ к сети.

Списки доступа представляют собой последовательность команд, **разрешающих (permit)** или **запрещающих (deny)** продвижение пакетов через маршрутизатор, т.е. разрешающих или запрещающих доступ из других локальных сетей или из Интернета в защищаемую сеть, а также удаленный доступ по протоколам Telnet, SSH. При конфигурировании списков доступа маршрутизатор не только создает пути передачи пакетов, но и фильтрует проходящий через него трафик.

Списки доступа ACL могут быть созданы для всех сетевых протоколов, функционирующих на маршрутизаторе, например, IPv4, IPv6 или IPX, и устанавливаются на интерфейсах маршрутизаторов. Запрет или разрешение сетевого трафика через интерфейс маршрутизатора реализуется на основании анализа совпадения определенных условий (правил). Для этого списки доступа представляются в виде последовательных записей, в которых анализируются используемые адреса и протоколы.

Списки доступа создаются как для **входящих**, так и для **исходящих** пакетов на основании анализируемых параметров (адреса источника, адреса назначения, используемого протокола и номера порта верхнего уровня), указанных в списке доступа ACL (рис. 1).

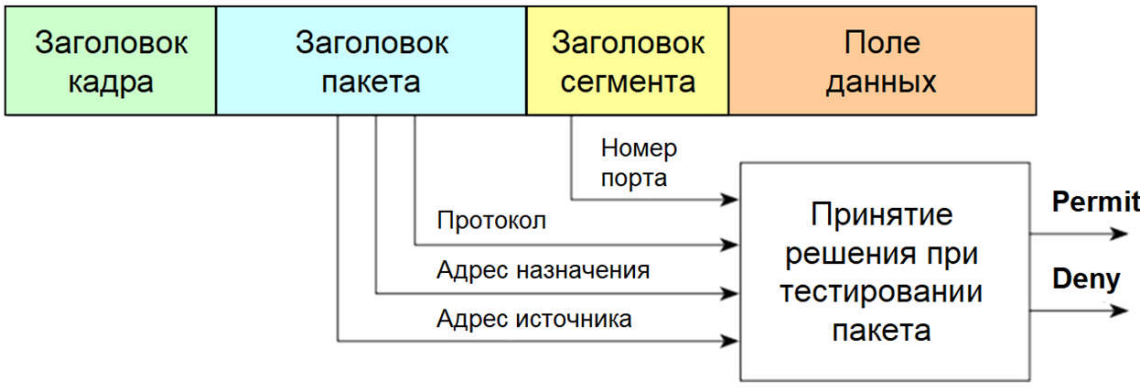

Рис. 1. Извлечение данных для принятие решения при тестировании пакета

Отдельные списки доступа могут быть созданы на каждом интерфейсе маршрутизатора для каждого направления сетевого трафика (исходящего и входящего) и для каждого сетевого протокола, установленного на интерфейсе.

Функционирование маршрутизатора по проверке соответствия принятого пакета требованиям списка доступа производится следующим образом. Когда кадр поступает на интерфейс, маршрутизатор извлекает (декапсулирует) из кадра пакет и проверяет его на соответствие условиям списка ACL входного интерфейса. При отсутствии запрета или отсутствии списка доступа пакет маршрутизируется и продвигается на выходной интерфейс, где вновь проверяется, затем инкапсулируется в новый кадр и отправляется интерфейсу следующего устройства.

Проверка условий (утверждений) списка доступа производится последовательно. Если текущее утверждение верно, пакет обрабатывается в соответствие с командами **permit** или **deny** списка доступа. В конце каждого списка присутствует неявно заданная по умолчанию команда

deny any (запретить все остальное). Поэтому если в списке доступа нет ни одного разрешающего условия, то весь трафик будет заблокирован.

По функциональным возможностям можно выделить два типы списков доступа:

1. **Стандартные (standard ACLs):** проверяют только IP-адрес источника и не могут анализировать данные, вложенные в IP-пакет.
2. **Расширенные (extended ACLs):** способны проверять не только адрес источника, но и адрес узла назначения. Кроме, того для продвижения или фильтрации пакетов extended ACLs могут использовать данные, вложенные в IP-пакет.

При этом списки доступа обеих типов могут быть либо **нумерованными**, либо **именованными**, т.е. когда список доступа конфигурируются на маршрутизаторе, каждый список должен иметь уникальный идентификационный номер или имя. Идентификационный номер созданного списка доступа должен находиться в пределах определенного диапазона, заданного для этого типа списка (табл. 1).

Табл. 1. Диапазоны идентификационных номеров списков доступа

Диапазон номеров	Тип списка доступа
1-99	IP standard access-list
100-199	IP extended access-list
1300-1999	IP standard access-list (extended range)
2000-2699	IP extended access-list (extended range)
600-699	AppleTalk access-list
800-899	IPX standard access-list
900-999	IPX extended access-list

Для каждого протокола, для каждого направления трафика и для каждого интерфейса может быть создан свой список доступа. Однако исходящие фильтры не затрагивают трафик, который идет из местного маршрутизатора.

Стандартные списки доступа рекомендуется устанавливать по возможности ближе к адресату назначения, а расширенные - ближе к источнику. То есть стандартные списки доступа должны блокировать устройство или сеть назначения и располагаться поближе к защищаемой сети, а расширенные списки устанавливаются ближе к возможному источнику нежелательного трафика.

Список доступа производит фильтрацию пакетов по порядку, поэтому в строках списков следует задавать **условия фильтрации**, начиная со специфических и заканчивая общими. Условия списка доступа обрабатываются последовательно от вершины списка к основанию, пока не будет найдено соответствующее условие. Если никакое условие не найдено, то тогда пакет отклоняется и уничтожается, поскольку неявное условие deny any (запретить все остальное) есть неявно в конце любого списка доступа. Не удовлетворяющий списку доступа пакет протокола IP будет отклонен и уничтожен, при этом отправителю будет послано сообщение протокола ICMP. Новые записи (линии) всегда добавляются в конце списка доступа.

2. Задание

2.1. Обучающая часть с индивидуальными параметрами

Проект 1 «Настройка нумерованных access-lists»

1. Для реализации проекта студент должен использовать индивидуальные параметры, варианты которых приведены в **Приложении**.
2. В CPT создайте новый проект и постройте сеть, показанную на рисунке 2. Определите маску подсети таким образом, чтобы выделенный Вам в варианте индивидуальных параметров диапазон частных IP-адресов дробился на заданное количество подсетей. Компьютерам локальной сети и соответствующему интерфейсу маршрутизатора назначьте IP-адреса, принадлежащие одной из подсетей. Серверы должны получить IP-

адреса из публичного диапазона. На одном сервере должен быть запущен HTTP-сервис, а его Web-страница должна отображать ФИО студента и название группы. На другом сервере должны работать DNS- и FTP-серверы.

3. Серверам дайте полные доменные имена и псевдонимы. В качестве названия домена второго уровня используйте аббревиатуру, построенную из первых букв ваших: фамилии, имени и отчества. Название домена первого уровня определено вариантом индивидуальных параметров.

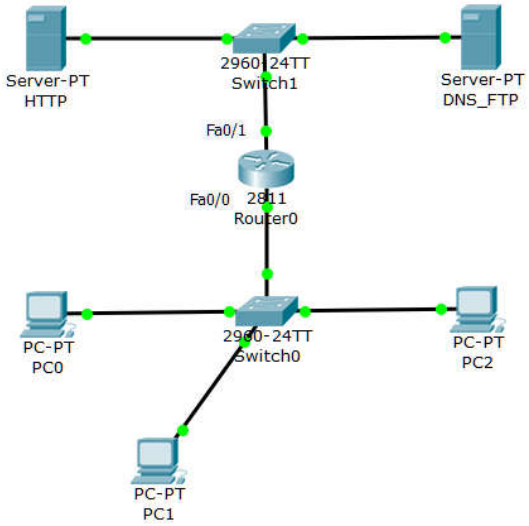

Рис. 2. Топология сети в Проекте 1

4. Проверьте доступность сетевых ресурсов со всех рабочих станций сети.
5. Запретить с помощью ACL доступ компьютеру PC1 к сетевым ресурсам за пределами его подсети. Если компьютер имеет IP-адрес 192.168.0.3, то для реализации этого правила необходимо на маршрутизаторе в режиме глобального конфигурирования ввести команду *access-list 10 deny host 192.168.0.3*. Номер **10** выбран произвольно. Однако его принадлежность диапазону 1-99 (см. табл. 1) говорит о том, что создаваемый список доступа будет **стандартным**. Команда **deny** запрещает продвижение пакетов от хоста с IP-адресом 192.168.0.3.
6. После создания списка доступа его необходимо прикрепить к интерфейсу маршрутизатора. В нашем случае можно выбрать либо интерфейс (Fa0/0), принадлежащий подсети рабочих станций, либо интерфейс (Fa0/1), принадлежащий подсети серверов. В первом случае пакет от 192.168.0.3 будет уничтожаться на входе в маршрутизатор и процедура маршрутизации для него выполняться не будет, что уменьшит нагрузку на процессор маршрутизатора. Во втором случае пакет будет от 192.168.0.3 уничтожаться после процедуры маршрутизации. Установим список доступа для входящих пакетов на интерфейсе Fa0/0. Для этого необходимо в режиме конфигурирования интерфейса Fa0/0 ввести команду: *ip access-group 10 in*.
7. Проверьте доступность сетевых ресурсов для компьютера PC1. Доступны ли сервисы HTTP и FTP? Действует ли разрешение DNS-имен? Какой ответ дает ping шлюзов подсетей рабочих станций и серверов? Есть ли взаимодействие с рабочими станциями?
8. Выполните проверки аналогичные п. 6 для компьютеров PC0 и PC2.
9. Результат выполнения п. 7 должен показать недоступность ресурсов подсети серверов. Чтобы разобраться, почему так происходит, выполните на маршрутизаторе команду *show running-config* и найдите записи, соответствующие списку доступа с номером 10. В рабочей конфигурации маршрутизатора вы найдете только одну запись: *access-list 10 deny host 192.168.0.3*, которая должна фильтровать на интерфейсе маршрутизатора Fa0/0 входящие пакеты от только хоста *192.168.0.3*. Пакеты от других хостов из подсети *192.168.0.0* под условия фильтрации этой записи не попадают. Однако в конце любого списка контроля доступа неявно имеется записи, которая в нашем случае примет вид:

access-list 10 deny any. Она запрещает продвижение пакетов от всех источников не разрешенных явным образом. Поэтому пакеты от компьютеров PC0 и PC2 также не смогут пройти входной интерфейс маршрутизатора.

10. Исправить это положение позволяет запись списка контроля доступа, разрешающая продвигать на маршрутизатор пакеты от хостов подсети 192.168.0.0. Для ее создания в режиме глобального конфигурирования на маршрутизаторе введите команду:

    access-list 10 permit 192.168.0.0 0.0.0.255

    В данной команде используется **wildcard**-маска. По своей структуре она является инверсной по отношению к маске подсети. Алгоритм ее использования также отличается от методики применения маски подсети. Так маска подсети накладывается на IP-адрес с помощью операции конъюнкции (логическое "И") и позволяет выделить из него номер подсети, который используется маршрутизаторами для продвижения пакетов в составной сети. Wildcard-маска накладывается на IP-адрес с помощью операции дизъюнкции (логическое "ИЛИ"), что позволяет превратить IP-адрес с произвольным номером хоста в подсети в широковещательный IP-адрес. Это дает возможность определить принадлежность номера хоста в IP-адресе источника к заданному wildcard-маской диапазону хостов. В нашем случае, если

    (192.168.0.0) | (0.0.0.255) **равно** (IP-адрес источника) | (0.0.0.255),

    где | - операция дизъюнкции,

    то условие списка доступа считается выполненным и к пакету применяется правило, указанное в соответствующей записи. Когда необходимо проверить IP-адрес единственного хоста, то в команде access-list вместо слова host можно использовать его IP-адрес и wildcard-маску 0.0.0.0.
11. Проверьте теперь доступность сетевых ресурсов для компьютера PC0 и PC2. Доступны ли сервисы HTTP и FTP? Действует ли разрешение DNS-имен? Какой ответ дает ping шлюзов подсетей рабочих станций и серверов? Есть ли взаимодействие с рабочими станциями?
12. Важно отметить, что как только в списке контроля доступа обнаруживается запись с выполненным условием, проверка следующих записей не производится. Поэтому при составлении списка контроля доступа нужно идти от частных условий проверки к наиболее общим. Удалите список контроля доступа с номером 10, введя команду:

    no access-list 10

    Постройте новый список доступа с этим же номером, но измените порядок команд следующим образом:

    access-list 10 permit 192.168.0.0 0.0.0.255

    access-list 10 deny 192.168.0.3 0.0.0.0 (эквивалентна: *access-list deny host 192.168.0.3*).
13. Проверьте теперь доступность сетевых ресурсов для всех рабочих станций. Запрет доступа для хоста 192.168.0.3 должен перестать работать. Это связано с тем, что IP-адреса всех рабочих станций попадают под условие первой записи списка, и проверка условия второй записи никогда не будет выполнена для компьютеров указанной подсети. Тоже самое касается неявной записи с правилом *deny any* в конце списка.
14. Удалите неправильный access-list с номером 10 и создайте список заново с правильным порядком записей в нем.
15. Запретить доступ компьютеру PC0 на FTP-сервер. Для решения такой задачи необходимо анализировать IP-адрес узла назначения и номер порта сетевой службы, который инкапсулирован в данные транспортного уровня модели OSI. С помощью стандартных списков доступа выполнить эту проверку невозможно. Поэтому используем расширенные списки контроля доступа. Пусть компьютер PC0 имеет IP-адрес 192.168.0.2. Тогда для решения поставленной задачи в режиме глобального конфигурирования маршрутизатора следует выполнить две такие команды:

    access-list 110 deny tcp host 192.168.0.2 host 205.10.10.3 eq 21

    access-list 110 permit ip any any

Переформатируйте указанные выше команды для IP-адресов Вашей рабочей станции и сервера. Номер списка выбран произвольно, но принадлежность к диапазону 100-199 относит его к типу extended (расширенный). В расширенных списках контроля доступа необходимо указывать пакеты какого протокола будут анализироваться. Т.к. в качестве транспортного протокола для службы FTP используется tcp, то в первой записи ACL(110) для запрета доступа хоста 192.168.0.2 к данному сервису следует просматривать такие пакеты. Далее в первой команде указываются IP-адреса источника и узла назначения tcp-пакетов. Причем в заголовке этих пакетов должен быть указан номер порта сетевой службы равный (eq) 21. Порт 21 стандартно закреплен за службой FTP. Вторая запись ACL(110) разрешает продвижение любых IP-пакетов от любых источников к любым узлам назначения. Протокол IP инкапсулирует данные других протоколов, анализируемых в технологии ACL. Поэтому условие проверки пакетов, указанное во второй записи ACL(110) будет наиболее общим и блокирует выполнение неявного *deny ip any any* в конце списка.

16. Прикрепите список контроля доступа к интерфейсу Fa0/0 для обработки входящих пакетов.
17. Проверьте доступность FTP-сервера для рабочих станций сети.
18. Проверьте доступность сетевых ресурсов (FTP, WWW) для компьютера PC1. Ресурсы должны стать доступными, потому что привязка на интерфейс Fa0/0 списка контроля доступа с номером 110 для анализа входящих пакетов вытеснила оттуда стандартный список с номером 10. Одновременно несколько списков контроля доступа для обработки входящих пакетов на одном интерфейсе установить невозможно. Рекомендуется стандартные списки контроля доступа привязывать на интерфейс, ближайший к узлу назначения, а расширенные - на интерфейс, ближайший к источнику. В нашем случае стандартный access-list следует привязать на интерфейс Fa0/1 для обработки исходящих из маршрутизатора пакетов. Для этого в режиме конфигурирования данного интерфейса введите команду: *ip access-group 10 out*.
19. Протестируйте работоспособность сети: для PC1 должен быть запрещен доступ в подсеть серверов; для PC0 должен быть запрещен доступ к FTP-серверу; взаимодействие рабочих станций (PC0, PC1, PC2) не должно быть ограничено; для PC0 должны быть доступны службы HTTP и DNS.
20. В привилегированном режиме Cisco IOS с помощью команды:

    show access-lists

    просмотрите состав списков контроля доступа, которые были созданы Вами на маршрутизаторе. В конце каждой записи списка в скобках указывается количество пакетов, обработанных с помощью ее правила.
21. С помощью команды *show running-config* проверьте правильность привязки списков контроля доступа к интерфейсам маршрутизатора.
22. Настройте удаленное управление маршрутизатором по протоколу telnet.
23. Подключите к коммутатору подсети серверов новый компьютер и назначьте ему статический IP-адрес.
24. С помощью режима симуляции CPT проследите, как происходит продвижение пакетов, посылаемых утилитой ping, между новым компьютером и различными рабочими станциями. Дайте свое объяснение.
25. Проверьте подключение с нового компьютера по протоколу telnet к маршрутизатору.
26. Профильтруйте трафик направленный из посети серверов на маршрутизатор и сетевые устройства за ним.

    Замечание: Стандартные порты сетевых служб. Службы HTTP, FTP и telnet в работе опираются на протокол TCP и порты: 80, 21, 23 соответственно. Служба DNS использует протокол UDP и порт 53.

    Создайте новые нумерованные стандартный и расширенный списки контроля доступа, с помощью которых:

- запретите доступ из подсети серверов на маршрутизатор и коммутатор Sw2 по протоколу telnet;
- запретите продвижение в подсеть рабочих станций любых пакетов из подсети серверов, если их источниками не выступают HTTP- или DNS_FTP-серверы.

Привязка созданных Вами списка(ов) контроля доступа к интерфейсам маршрутизатора **не должна** вытеснить оттуда ALC(10) и ACL(110), и нарушить их работоспособность.

27. Модифицируйте ACL(110) так, чтобы доступ к маршрутизатору по протоколу telnet был возможен только с компьютера PC1.
28. Протестируйте и отладьте работу сети.
29. Продемонстрируйте работоспособную модель сети преподавателю и сохраните ее в файле с именем **LabNet-7(Family_group)-task-1.pkt** для последующего отчета по лабораторной работе.

2.2. Самостоятельная работа

Проект 2 «Настройка именованных access-lists»

1. Дополните сетевую модель, построенную Вами в первом задании, локальной сетью на основе L3-коммутатора (рис. 3).

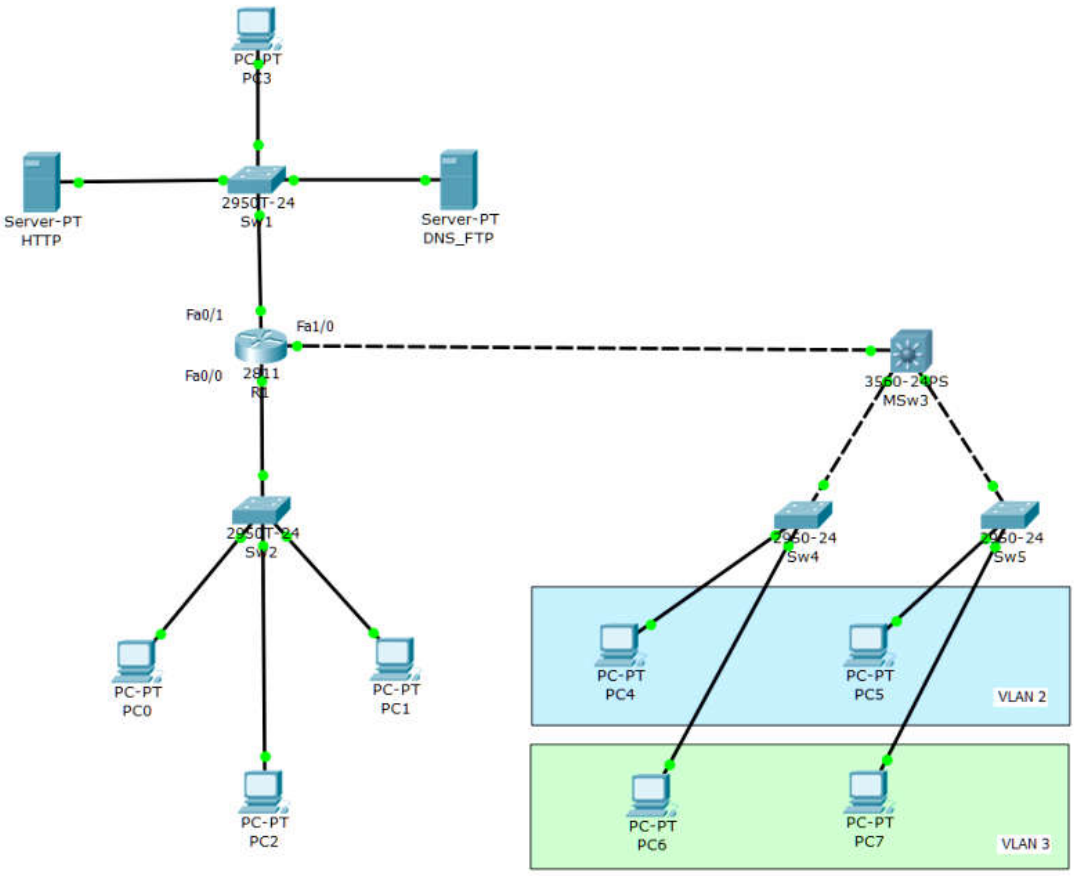

Рис. 3. Топология сети в Задании 2

2. На маршрутизатор добавьте еще один сетевой модуль с интерфейсом FastEthernet для подключения L3-коммутатора и назначьте ему статический IP-адрес.
3. Настройте коммутаторы Sw4 и Sw5 для обеспечения работы двух виртуальных локальных сетей и подключите их магистральными каналами к L3-коммутатору.
4. Сконфигурируйте L3-коммутатор следующим образом:

- создайте логические интерфейсы виртуальных локальный сетей (SVI) и назначьте им статические IP-адреса;
- настройте удаленное управление по протоколу telnet;
- настройте DHCP-сервер для выдачи IP-адресов компьютерам, входящим во VLAN 2 и VLAN 3 (в качестве IP DNS-сервиса укажите адрес DNS_FTP-сервера);
- переключите интерфейс соединения с маршрутизатором в режим маршрутизируемого порта и назначьте ему статический IP-адрес;
- задайте маршрут по умолчанию.

5. У компьютеров PC4 - PC7 включите протокол DHCP.
6. На маршрутизаторе создайте статический агрегирующий маршрут для перенаправления трафика в подсети VLANs.
7. С помощью **именованных стандартных ACL** запретим передачу трафика между VLAN 2 и 3. Для этого сконфигурируем L3-коммутатор следующим образом:
   - в режиме глобального конфигурирования войдите в режим конфигурирования именованного стандартного списка контроля доступа с названием **aclVLAN3** командой: *ip access-list standard aclVLAN3*. Приглашение командной строки Cisco IOS примет вид: **MSw3(config-std-nacl)#**
   - дальше последовательно введите строки (записи) с правилами обработки пакетов (пусть VLAN2 относится к подсети 192.168.2.0 255.255.255.0):
     MSw3(config-std-nacl)#deny 192.168.2.0 0.0.0.255
     MSw3(config-std-nacl)#permit any
     MSw3(config-std-nacl)#exit (завершаем редактирование ACL с именем aclVLAN3).
   - войдите в режим конфигурирования логического интерфейса VLAN 3 и привяжите список контроля доступа для обработки **исходящих** пакетов командой:
     ip access-group aclVLAN3 out
   - в режиме симуляции CPT с компьютера PC4 командой ping протестируйте связь с компьютером PC7. На каком этапе прерывается прохождение ICMP-пакета? Какой пакет возвращается на PC4?
   - использование команды ping на компьютере PC7 для проверки связи с PC4 в режиме симуляции даст другой результат. Можно увидеть, что ICMP-пакет пройдет до узла назначения, однако эхо-пакет в обратном направлении пройти не сможет. Чтобы полностью заблокировать трафик между VLAN 2 и 3 нужно на логический интерфейс VLAN 2 для обработки исходящих пакетов прикрепить ACL с фильтрацией трафика из подсети VLAN 3. Самостоятельно проделайте эту работу по аналогии с показанным выше примером.
   - После монтирования обеих списков контроля доступа трафики VLAN 2 и 3 должны быть разделены на L3-коммутаторе. При этом компьютеры PC4 - PC7 должны иметь доступ к сервисам подсети серверов (HTTP-, FTP- и DNS-сервисам).
8. С помощью **именованного расширенного ACL** отфильтруем трафик из подсети серверов, продвигая на L3-коммутаторе только пакеты от HTTP- и FTP_DNS-серверов. При этом блокируя доступ к FTP-сервису. Для этого сконфигурируем L3-коммутатор следующим образом:
   - в режиме глобального конфигурирования войдите в режим конфигурирования именованного расширенного списка контроля доступа с названием **aclOutNet** командой: *ip access-list extended aclOutNet*.
   - дальше последовательно введите строки (записи) с правилами обработки пакетов:
     deny tcp 205.10.10.0 0.0.0.255 eq ftp any
     permit ip host 205.10.10.2 any
     permit ip host 205.10.10.3 any

- войдите в режим конфигурирования маршрутизируемого интерфейса L3-коммутатора и привяжите список контроля доступа для обработки **входящих** пакетов командой:

ip access-group aclOutNet in

- протестируйте доступность Web-ресурсов;
- проверьте доступность FTP-сервиса;
- с разных компьютеров подсети серверов командой ping протестируйте связь с PC4 - PC7.

9. С помощью именованных стандартных и расширенных списков контроля доступа самостоятельно решите следующие задачи:
   - запретите по протоколу telnet удаленно конфигурировать маршрутизатор и L3-коммутатор с любых компьютеров кроме PC1;
   - запретите обмен данными между PC2 и компьютерами подсетей VLAN 2 и 3.
10. Продемонстрируйте работоспособную модель сети преподавателю и сохраните ее в файле с именем **LabNet-7(Family_group)-task-7.pkt** для последующего отчета по лабораторной работе.

3. Подготовка отчета, представление и оценка работы

Структура отчета

В качестве отчета по заданию необходимо предоставить готовый проект Cisco Packet Tracer. В рабочей области проекта нужно текстовыми метками указать логины и пароли, которые были задействован при настройке или требуются для использования какого-либо устройства или сетевой службы. В отчете (файлах, направляемых на Eluniver) оценивается точность названий, для которых в задании определен шаблон или уникальное значение, параметры настройки сетевого оборудования.

Загрузку проектов на сайт Eluniver следует выполнять после демонстрации задания преподавателю. Желательно загружать все файлы одновременно.

Представление и защита работы

Представлением работы является ее демонстрация преподавателю. В ходе представления преподаватель может задать вопрос по любому пункту задания или попросить выполнить какие-либо построения на основе навыков, полученных при разработке проекта. Оценка за представление задания выставляется на основе работоспособности проекта, правильности ответа студента на вопросы по проекту и готовности выполнить дополнительное задание без использования методического материала.

Защита работы заключается в ответе на два контрольных вопроса, выбранных произвольно преподавателем из списка контрольных вопросов (п. 4). Оценивается детальность и точность ответа. Во время ответа пользоваться методическим материалом нельзя. Возможность ответа на контрольные вопросы дается студенту после представления задания.

Структура оценки лабораторной работы

№	Вид оценки	Максимальный балл
1.	Выполнение задания по Проекту 1	25
2.	Выполнение задания по Проекту 2	25
3.	Отчет по Проекту 1	10
4.	Отчет по Проекту 2	10
5.	Контрольный вопрос 1	15
6.	Контрольный вопрос 2	15
	Итого:	**100**

4. Контрольные вопросы

1. Дайте расшифровку аббревиатуры ACL.
2. На каком уровне модели OSI работают списки контроля доступа?
3. Какая команда в ACL разрешает доступ к сетевому ресурсу?
4. Какая команда используется для фильтрации трафика в технологии ACL?
5. Какие параметры определяют количество списков контроля доступа на интерфейсе сетевого устройства?
6. Дайте определения для входящих и исходящих пакетов сетевого интерфейса. Имеются ли различия при обработке этих пакетов с помощью ACL?
7. Какие поля пакета данных используются в технологии?
8. Какие поля сегмента данных применяются при фильтрации трафика с помощью списков контроля доступа?
9. Как называется операция извлечения сегмента из пакета данных?
10. Трафик каких транспортных протоколов стека TCP\IP может контролировать технология ACL?
11. Какое неявное правило всегда имеется в конце списка контроля доступа?
12. Какие параметры пакетов используются в стандартных списках контроля доступа?
13. В чем различие нумерованных и именованных списков контроля доступа?
14. Как называются списки, в которых в качестве параметров указывается номер порта сетевой службы?
15. С помощью какого типа списков контроля доступа можно анализировать адрес источника пакетов?
16. Как по номеру списка контроля доступа определить является ли он стандартным?
17. Можно ли по имени списка контроля доступа определить его тип?
18. Какой синтаксис команд используется в стандартных списках контроля доступа?
19. Для принятия решения о продвижении или фильтрации пакета просматривается весь список контроля доступа?
20. Влияет ли расположение команд списка контроля доступа на результат фильтрации пакетов?
21. Какого правила следует придерживаться при составлении списка контроля доступа?
22. Где наиболее рационально размещать стандартные списки контроля доступа?
23. Приведите пример построения расширенного списка контроля доступа с ключевым словом *any?* Объясните его назначение.
24. Какой тип списков контроля доступа является наиболее подходящим для установки на входной порт сетевого интерфейса маршрутизатора?
25. Для чего используется ключевое слово *extended* при построении команд ACL?
26. Какие команды на L3-коммутаторе Cisco позволят блокировать трафик между VLAN при включенной маршрутизации?
27. Как заблокировать доступ к управлению коммутаторами и маршрутизаторами сети всем узлам, кроме компьютера администратора? Приведите пример команд.
28. Как с помощью технологии ACL можно защитить сетевые ресурсы предприятия? Приведите пример набора команд, который позволит пользователям работать только с http-сервисом на сервере.
29. Каким образом на Cisco-маршрутизаторах реализуется обновление списка контроля доступа?
30. Можно ли с помощью команд Cisco IOS вставлять новые строки между существующими в списке доступа? Приведите пример такой команды.

Приложение. Варианты индивидуальных параметров к заданиям

Вариант	Номер локальной сети	Количество подсетей	Диапазон публичных адресов		Название домена первого уровня
1.	192.168.63.0	8	4.23.176.0	255.255.255.0	lab
2.	176.25.0.0	16	203.167.18.0	255.255.255.0	mon
3.	10.0.0.0	128	170.89.204.128	255.255.255.192	cu
4.	192.168.27.0	4	209.0.0.0	255.255.0.0	ger
5.	100.64.0.0	32	2.78.45.0	255.255.255.0	met
6.	192.168.0.0	64	65.12.78.0	255.255.255.128	pow
7.	10.0.56.0	8	112.35.36.0	255.255.255.0	jor
8.	192.168.224.0	12	36.96.158.0	255.255.255.192	sig
9.	10.26.100.0	5	98.12.0.0	255.255.224.0	lot
10.	187.56.26.128	4	211.25.0.0	255.255.0.0	got
11.	192.168.5.0	8	2.158.39.0	255.255.255.192	ric
12.	192.168.1.192	6	9.5.193.0	255.255.255.128	pol
13.	10.229.35.0	27	181.169.28.192	255.255.255.224	she
14.	10.85.157.0	11	148.25.221.0	255.255.255.0	tar
15.	175.26.192.0	17	116.0.56.128	255.255.255.240	hi
16.	192.168.0.0	74	22.38.192.0	255.255.240.0	vot
17.	10.153.34.192	6	95.33.208.0	255.255.248.0	iz
18.	10.92.64.0	12	92.37.54.0	255.255.255.0	nur
19.	192.168.128.0	65	43.228.14.224	255.255.255.224	foi
20.	192.168.26.128	3	3.21.199.0	255.255.0.0	kod
21.	10.220.35.0	6	49.27.162.0	255.255.255.128	bot
22.	10.38.184.128	5	75.0.28.0	255.255.255.0	sok
23.	192.168.30.0	18	5.11.67.224	255.255.255.224	tau
24.	192.168.35.0	9	40.28.26.0	255.0.0.0	lic
25.	10.92.138.192	7	71.29.6.128	255.255.255.192	end