МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

По выполнению лабораторных работ по дисциплине
«Вычислительные системы и компьютерные сети»
для бакалавров направления подготовки
09.03.01 «Информатика и вычислительная техника»
направленность (профиль) «Программное обеспечение средств вычислительной техники и автоматизированных систем»

Ставрополь,
2026 г.

Содержание

Лабораторная работа №1

Исследование технологий создания виртуальных процессоров ЦОД.

Цель работы: Изучить и создать систему виртуальнуых процессоров ЦОД.

1 Теоретическая часть

VLAN (Virtual Local Area Network) – группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN'ax, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях.

В современных сетях VLAN – главный механизм для создания логической топологии сети, не зависящей от её физической топологии. VLAN'ы используются для сокращения широковещательного трафика в сети. Имеют большое значение с точки зрения безопасности, в частности, как средство борьбы с ARP-spoofing'ом.

Зачем нужен VLAN

- Гибкое разделение устройств на группы

Как правило, одному VLAN соответствует одна подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных подсетях. Но в то же время VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения

- Уменьшение количества широковещательного трафика в сети

Каждый VLAN – это отдельный широковещательный домен. Например, коммутатор – это устройство 2 уровня модели OSI. Все порты на коммутаторе с лишь одним VLAN находятся в одном широковещательном домене. Создание дополнительных VLAN на коммутаторе означает разбиение коммутатора на несколько широковещательных доменов. Если один и тот же VLAN настроен на разных коммутаторах, то порты разных коммутаторов будут образовывать один широковещательный домен.

- Увеличение безопасности и управляемости сети

Когда сеть разбита на VLAN, упрощается задача применения политик и правил безопасности. С VLAN политики можно применять к целым подсетям, а не к отдельному устройству. Кроме того, переход из одного VLAN в другой предполагает прохождение через устройство 3 уровня, на котором, как правило, применяются политики, разрешающие или запрещающие доступ из VLAN в VLAN.

1.2 Тегирование трафика VLAN

Компьютер при отправке трафика в сеть даже не догадывается, в каком VLAN'е он размещён. Коммутатор принимает решения в соответствии с таблицей комутации. Коммутатор знает, что компьютер, который подключен к определённому порту, находится в соответствующем VLAN'е. Трафик, приходящий на порт определённого VLAN'а, ничем особенным не отличается от трафика другого VLAN'а. Другими словами, никакой информации о принадлежности трафика определённому VLAN'у в нём нет.

Однако, если через порт может прийти трафик разных VLAN'ов, коммутатор должен его как-то различать. Для этого каждый кадр (frame) трафика должен быть помечен каким-то особым образом. Пометка должна говорить о том, какому VLAN'у трафик принадлежит.

Наиболее распространённый сейчас способ ставить такую пометку описан в открытом стандарте IEEE 802.1Q. Существуют проприетарные протоколы, решающие похожие задачи, например, протокол ISL от Cisco Systems, но их популярность значительно ниже (и снижается).

Коммутатор и VLAN'ы

VLAN'ы могут быть настроены на коммутаторах, маршрутизаторах, других сетевых устройствах и на хостах. Однако, для объяснения VLAN лучше всего подойдет коммутатор.

Коммутатор – устройство 2го уровня и изначально все порты коммутатора находятся, как правило, в VLAN 1 и, следовательно, в одном широковещательном сегменте.

Это значит, что если одно из устройств, которое подключено к порту коммутатора, отправит широковещательный фрейм, то коммутатор перенаправит этот фрейм на все остальные порты, к которым подключены устройства, и они получат этот фрейм.

1.3 Механизмы передачи фреймов

Для того, чтобы передавать фреймы, коммутатор использует три базовых механизма:

1 Flooding – фрейм, полученный на один из портов, передается на остальные порты коммутатора. Коммутатор выполняет эту операцию в двух случаях:

- при получении широковещательного или multicast (если не настроена поддержка multicast) фрейма,
- при получении unknown unicast фрейма. Это позволяет коммутатору доставить фрейм хосту (при условии, что хост достижим и существует), даже когда он не знает, где хост находится.

2 Forwarding – передача фрейма, полученного на одном порту, через другой порт в соответствии с записью в таблице коммутации.

3 Filtering– если коммутатор получает фрейм через определенный порт, и MAC-адрес получателя доступен через этот же порт (это указано в таблице коммутации), то коммутатор отбрасывает фрейм. То есть, коммутатор считает, что в этом случае хост уже получил этот фрейм, и не дублирует его.

1.4 VLAN Trunking Protocol (VTP) – проприетарный протокол компании Cisco Systems, предназначенный для создания, удаления и переименования VLANов на сетевых устройствах. Передавать информацию о том, какой порт находится в каком VLANe, он не может.

1.4.1 Сообщения VTP

- Summary advertisements
- Subset advertisements
- Advertisement requests
- VTP Join messages (используются для pruning)

1.4.2 Режимы работы протокола

На коммутаторе VTP может работать в трёх режимах:

1. Server (режим по умолчанию):

- Можно создавать, изменять и удалять VLAN из командной строки коммутатора,
- Генерирует объявления VTP и передает объявления от других коммутаторов,
- Может обновлять свою базу данных VLAN при получении информации не только от других VTP серверов но и от других VTP клиентов в одном домене, с более высоким номером ревизии.
- Сохраняет информацию о настройках VLAN в файле vlan.dat во flash.

2. Client:

- Нельзя создавать, изменять и удалять VLAN из командной строки коммутатора,
- Передает объявления от других коммутаторов,
- Синхронизирует свою базу данных VLAN при получении информации VTP,
- Сохраняет информацию о настройках VLAN в файле vlan.dat во flash.

3. Transparent:

- Можно создавать, изменять и удалять VLAN из командной строки коммутатора, но только для локального коммутатора,
- Не генерирует объявления VTP,
- Передает объявления от других коммутаторов,
- Не обновляет свою базу данных VLAN при получении информации по VTP,
- Сохраняет информацию о настройках VLAN в NVRAM,
- Всегда использует configuration revision number 0.

В версии 3 VTP добавился новый режим работы и изменились некоторые режимы работы, по сравнению с предыдущими версиями:

1 Server:

- Добавилась поддержка Private VLAN
- Могут анонсироваться VLAN из расширенного диапазона

2 Client:

- Настройки VLAN сохраняются в NVRAM и в режиме клиента
- Добавилась поддержка Private VLAN
- Могут анонсироваться VLAN из расширенного диапазона

3 Transparent:

- без изменений

4 Off:

- Новый режим работы VTP, который добавился в 3 версии.
- Не передает объявления VTP.

- В остальном аналогичен режиму Transparent

1.4.3 Диапазоны VLAN

Диапазоны VLAN:

1. VTP версии 1 и 2 не анонсирует эти VLAN, они не могут быть исключены (pruned):

1) 1 – нормальный (normal) диапазон,

2) 1002-1005 – нормальный (normal) диапазон,

3) 1006-4094 – расширенный (extended) диапазон,

2. VTP версии 1 и 2 анонсирует эти VLAN, они могут быть исключены (pruned)

1) 2-1001 – нормальный (normal) диапазон.

1.4.4 VLAN database

Сервера VTP должны иметь возможность сохранять информацию, полученную в обновлениях VTP от других серверов, без участия администратора. Для этого в коммутаторах Cisco под управлением IOS используется VLAN database. Это отдельный файл, который хранится во флеш и называется vlan.dat.

При обнулении конфигурации коммутатора, VLAN database не затрагивается, поэтому зачастую получается, что информация о VLAN и настройках VTP сохраняется после обнуления и перезагрузки коммутатора. Для того чтобы удалить VLAN database необходимо удалить файл vlan.dat.

Можно изменить название файла в котором хранится VLAN database:

```
sw(config)# vtp file <filename>
```

2 Практическая часть

2.1 Настройка VLAN на коммутаторах

Рисунок 2.1 – Настройка Vlan на коммутаторах

Терминология Cisco:

1) access port – порт принадлежащий одному VLAN'у и передающий нетегированный трафик

2) trunk port – порт передающий тегированный трафик одного или нескольких VLAN'ов

Коммутаторы Cisco ранее поддерживали два протокола 802.1Qи ISL. ISL – проприетарный протокол использующийся в оборудовании Cisco. ISL полностью инкапсулирует фрейм для передачи информации о принадлежности к VLAN'у.

В современных моделях коммутаторов Cisco ISL не поддерживается.

Создание VLAN'а с идентификатором 2 и задание имени для него:

```
sw1(config)# vlan 2
```

```
sw1(config-vlan)# name test
```

Удаление VLAN'a с идентификатором 2:

```
sw1(config)# no vlan 2
```

2.2 Настройка транка (trunk)

Для того чтобы передать через порт трафик нескольких VLAN, порт переводится в режим транка.

Режимы интерфейса (режим по умолчанию зависит от модели коммутатора):

1) auto – Порт находится в автоматическом режиме и будет переведён в состояние trunk, только если порт на другом конце находится в режиме on или desirable. Т.е. если порты на обоих концах находятся в режиме "auto", то trunk применяться не будет.

2) desirable – Порт находится в режиме "готов перейти в состояние trunk"; периодически передает DTP-кадры порту на другом конце, запрашивая удаленный порт перейти в состояние trunk (состояние trunk будет установлено, если порт на другом конце находится в режиме on, desirable, или auto).

3) trunk – Порт постоянно находится в состоянии trunk, даже если порт на другом конце не поддерживает этот режим.

4) nonegotiate – Порт готов перейти в режим trunk, но при этом не передает DTP-кадры порту на другом конце. Этот режим используется для предотвращения конфликтов с другим "не-cisco" оборудованием. В этом случае коммутатор на другом конце должен быть вручную настроен на использование trunk'a.

По умолчанию в транке разрешены все VLAN. Для того чтобы через соответствующий VLAN в транке передавались данные, как минимум, необходимо чтобы VLAN был активным. Активным VLAN становится тогда, когда он создан на коммутаторе и в нём есть хотя бы один порт в состоянии up/up.

VLAN можно создать на коммутаторе с помощью команды vlan. Кроме того, VLAN автоматически создается на коммутаторе в момент добавления в него интерфейсов в режиме access.

В схеме, которая используется для демонстрации настроек, на коммутаторах sw1 и sw2, нужные VLAN будут созданы в момент добавления access-портов в соответствующие VLAN:

```
sw1(config)# interface fa0/3
sw1(config-if)# switchport mode access
sw1(config-if)# switchport access vlan 15
% Access VLAN does not exist. Creating vlan 15
```

На коммутаторе sw3 access-портов нет. Поэтому необходимо явно создать все необходимые VLAN:

```
sw3(config)# vlan 2,10,15
```

Для автоматического создания VLAN на коммутаторах, может использоваться протокол VTP.

2.3 Настройка VTP на коммутаторах Cisco

2.3.1 Настройка VTP версии 2

Имя VTP-домена (от 1 до 32 символов):

```
sw(config)# vtp domain <domain-name>
```

Настройка пароля, который будет использоваться для аутентификации в VTP-домене (от 1 до 32 символов):

```
sw(config)# vtp password <password>
```

Настройка второй версии протокола VTP:

```
sw(config)# vtp version 2
```

Настройка режима VTP:

```
sw(config)# vtp mode <client | server | transparent>
```

2.3.2 Настройка VTP версии 3

Имя VTP-домена (от 1 до 32 символов):

```
sw(config)# vtp domain <domain-name>
```

Настройка пароля, который будет использоваться для аутентификации в VTP-домене (от 1 до 32 символов):

```
sw(config)# vtp password <password> [hidden | secret]
```

1) hidden - означает, что пароль будет показан в show vtp password в зашифрованном формате (не clear text);

3) secret - чтобы указать пароль в зашифрованном формате.

Настройка версии протокола VTP:

```
sw(config)# vtp version 3
```

Если настроены VLAN расширенного (extended) диапазона, переводить VTP обратно в версию 2 или 1 из третьей запрещается.

Настройка режима VTP:

```
sw(config)# vtp mode <client | server | transparent | off> [vlan | mst | unknown]
```

VTP Primary Server

```
sw# vtp primary-server [vlan | mst] [force]
```

Включение/отключение VTP на интерфейсах

Отключить VTP на интерфейсе:

```
sw(config-if)# no vtp
```

Просмотр информации о настройках VTP

```
sw# show vtp status
sw# show vtp added counters
sw# show vtp password
```

Для 3 версии VTP:

```
sw# show vtp devices [conflict]
```

Информация об интерфейсах (для 3 версии):

```
sw# show vtp interface [int-id]
```

2.4 Настройка статического транка

Создание статического транка:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport mode trunk
```

На некоторых моделях коммутаторов (на которых поддерживается ISL) после попытки перевести интерфейс в режим статического транка, может появится такая ошибка:

```
sw1(config-if)# switchport mode trunk
Command rejected: An interface whose trunk encapsulation is “Auto” can not be configured to “trunk” mode.
```

Это происходит из-за того, что динамическое определение инкапсуляции (ISL или 802.1Q) работает только с динамическими режимами транка. И для того, чтобы настроить статический транк, необходимо инкапсуляцию также настроить статически.

Для таких коммутаторов необходимо явно указать тип инкапсуляции для интерфейса:

```
sw1(config-if)# switchport trunk encapsulation dot1q
```

И после этого снова повторить команду настройки статического транка (switchport mode trunk).

2.5 Динамическое создание транков (DTP)

Dynamic Trunk Protocol (DTP) – проприетарный протокол Cisco, который позволяет коммутаторам динамически распознавать настроен ли соседний коммутатор для поднятия транка и какой протокол использовать (802.1Q или ISL). Включен по умолчанию.

Режимы DTP на интерфейсе:

1) auto – Порт находится в автоматическом режиме и будет переведён в состояние trunk, только если порт на другом конце находится в режиме on или desirable. Т.е. если порты на обоих концах находятся в режиме "auto", то trunk применяться не будет.

2) desirable – Порт находится в режиме "готов перейти в состояние trunk"; периодически передает DTP-кадры порту на другом конце, запрашивая удаленный порт перейти в состояние trunk (состояние trunk будет установлено, если порт на другом конце находится в режиме on, desirable, или auto).

3) nonegotiate – Порт готов перейти в режим trunk, но при этом не передает DTP-кадры порту на другом конце. Этот режим используется для предотвращения конфликтов с другим "не-cisco" оборудованием. В этом случае коммутатор на другом конце должен быть вручную настроен на использование trunk'a.

Перевести интерфейс в режим auto:

```
sw1(config-if)# switchport mode dynamic auto
```

Перевести интерфейс в режим desirable:

```
sw1(config-if)# switchport mode dynamic desirable
```

Перевести интерфейс в режим nonegotiate:

```
sw1(config-if)# switchport nonegotiate
```

Проверить текущий режим DTP:

```
sw# show dtp interface
```

2.6 Разрешенные VLAN’ы

По умолчанию в транке разрешены все VLAN. Можно ограничить перечень VLAN, которые могут передаваться через конкретный транк.

Указать перечень разрешенных VLAN для транкового порта fa0/22:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan 1-2,10,15
```

Добавление ещё одного разрешенного VLAN:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan add 160
```

Удаление VLAN из списка разрешенных:

```
sw1(config)# interface fa0/22
sw1(config-if)# switchport trunk allowed vlan remove 160
```

2.7 Native VLAN

В стандарте 802.1Q существует понятие native VLAN. Трафик этого VLAN передается нетегированным. По умолчанию это VLAN 1. Однако можно изменить это и указать другой VLAN как native.

Настройка VLAN 5 как native:

```
sw1(config-if)# switchport trunk native vlan 5
```

Теперь весь трафик принадлежащий VLAN'у 5 будет передаваться через транковый интерфейс нетегированным, а весь пришедший на транковый интерфейс нетегированный трафик будет промаркирован как принадлежащий VLAN'у 5 (по умолчанию VLAN 1).

2.8 Настройка маршрутизации между VLAN

Рисунок 2.2 – Настройка маршрутизации между Vlan

Передача трафика между VLANами с помощью коммутатора Cisco

Все настройки по назначению портов в VLAN, сделанные ранее для sw1, sw2 и sw3, сохраняются. Дальнейшие настройки подразумевают использование sw3 как коммутатора 3 уровня.

При такой схеме работы никаких дополнительных настроек на маршрутизаторе не требуется. Коммутатор осуществляет маршрутизацию между сетями разных VLAN, а на маршрутизатор отправляет трафик предназначенный в другие сети.

Включение маршрутизации на коммутаторе:

sw3(config)# ip routing

Задание адреса в VLAN. Этот адрес будет маршрутом по умолчанию для компьютеров в VLAN 2:

```
sw3(config)# interface Vlan2
sw3(config-if)# ip address 10.0.2.1 255.255.255.0
sw3(config-if)# no shutdown
```

Задание адреса в VLAN 10:

```
sw3(config)# interface Vlan10
sw3(config-if)# ip address 10.0.10.1 255.255.255.0
sw3(config-if)# no shutdown
```

Контрольные вопросы

1. Что такое VLAN?
2. Какие проблемы локальных сетей решает VLAN?
3. Как в локальной сети организовать обмен информацией о VLAN?
4. В каких режимах работают порты коммутатора?
5. Какой VLAN принадлежит магистральный порт?
6. Как распространить одну VLAN на несколько коммутаторов?
7. Можно ли организовать несколько VLAN на нескольких коммутаторах без использования магистралей?
8. Зачем нужны протоколы ISL и IEEE 802.1Q?
9. Зачем нужны магистрали в локальной сети?
10. Какие задачи решает VTP?
11. Какие задачи решает STP?
12. Какими командами можно организовать VLAN?

13. Какой командой перевести порт в режим доступа и в режим магистрали?
14. Какой командой можно получить информацию о VLAN?

В локальной сети имеется одиннадцать VLAN. Сколько маршрутизаторов надо для объединения всех 11 VLAN в единое целое?

Задание для самостоятельной работы

Собрать схему изображенную на рисунке 1 и выполнить индивидуальное задание согласно варианту, все Vlan'ы должны получать пакет из другого Vlan'а.

Рисунок1.1 – Топология сети

Таблица 1 – задание для самостоятельной работы

Вариант	VLAN100	VLAN200	VLAN300	Вариант	VLAN100	VLAN200	VLAN300
1	11.1.0.0/16	5.1.0.0/16	11.1.0.0/16	6	6.1.0.0/16	7.1.0.0/16	8.1.0.0/16
2	3.1.0.0/16	10.10.0.0/16	8.1.0.0/16	7	8.1.0.0/16	10.1.0.0/16	2.1.0.0/16
3	8.1.0.0/16	11.1.0.0/16	12.1.0.0/16	8	8.1.0.0/16	11.1.0.0/16	2.1.0.0/16
4	2.1.0.0/16	3.1.0.0/16	11.1.0.0/16	9	12.1.0.0/16	13.1.0.0/16	10.10.0.0/16
5	4.1.0.0/16	5.1.0.0/16	8.1.0.0/16	10	3.1.0.0/16	5.1.0.0/16	11.1.0.0/16

Лабораторная работа №2

Статическая маршрутизация

Цель работы: Научиться настраивать статическую маршрутизацию.

1 Теоретическая часть

1.1.1 Маршрутизация

Протоколы маршрутизации - это правила, по которым осуществляется обмен информации о путях передачи пакетов между маршрутизаторами. Протоколы характеризуются временем сходимости, потерями и

масштабируемостью. В настоящее время используется несколько протоколов маршрутизации. Каждый протокол имеет сильные и слабые стороны.

Одна из главных задач маршрутизатора состоит в определении наилучшего пути к заданному адресату. Маршрутизатор определяет пути (маршруты) к адресатам или из статической конфигурации, введённой администратором, или динамически на основании маршрутной информации, полученной от других маршрутизаторов. Маршрутизаторы обмениваются маршрутной информацией с помощью протоколов маршрутизации. Маршрутизатор хранит таблицы маршрутов в оперативной памяти. Таблица маршрутов это список наилучших известных доступных маршрутов. Маршрутизатор использует эту таблицу для принятия решения куда направлять пакет. Для просмотра таблицы маршрутов следует использовать команду show ip route. Даже, если на некотором маршрутизаторе X не задавались никакие команды маршрутизации, тогда он всё равно строит таблицу маршрутов для непосредственно подсоединённых к нему сетей, например:

. . .

C192.168.4.0/24 is directly connected, Ethernet0 10.0.0.0/16 is subnetted, 3 subnets

C10.3.0.0 is directly connected, Serial0 C10.4.0.0 is directly connected, Serial1

C10.5.0.0 is directly connected, Ethernet1

Маршрут на непосредственно подсоединённые сети отображается на интерфейс маршрутизатора, к которому они присоединены. Здесь /24 обозначает маску 255.255. 255.0, а /16 - 255.255.0.0.

Таблица маршрутов отображает сетевые префиксы (адреса сетей) на выходные интерфейсы. Когда X получает пакет, предназначенный для 192.168.4.46, он ищет префикс 192.168.4.0/24 в таблице маршрутов. Согласно таблице пакет будет направлен на интерфейс Ethernet0. Если X получит пакет для 10.3.21.5, он направит его на Serial0.

Эта таблица показывает четыре маршрута для непосредственно подсоединённых сетей. Они имеют метку C. Маршрутизатор X отбрасывает все пакеты, направляемые к сетям, не указанным в таблице маршрутов. Для направления пакетам к другим адресатам необходимо в таблицу включить дополнительные маршруты. Новые маршруты могут быть добавлены двумя методами:

Статическая маршрутизация – администратор вручную определяет маршруты к сетям назначения.

Динамическая маршрутизация – маршрутизаторы следуют правилам, определяемым протоколами маршрутизации для обмена информацией о маршрутах и выбора лучшего пути.

Статические маршруты не меняются самим маршрутизатором. Динамические маршруты изменяются самим маршрутизатором автоматически при получении информации о смене маршрутов от соседних маршрутизаторов. Статическая маршрутизация потребляет мало вычислительных ресурсов и полезна в сетях, которые не имеют нескольких путей к адресату назначения. Если от маршрутизатора к маршрутизатору есть только один путь, то часто используют статическую маршрутизацию.

Для конфигурации статической маршрутизации в маршрутизаторах Cisco используют две версии команды ip route.

Первая версия

ip route АдресСетиНазначения МаскаСетиНазначения Интерфейс

Команда указывает маршрутизатору, что все пакеты, предназначенные для АдресСетиНазначения-МаскаСетиНазначения следует направлять на свой интерфейс Интерфейс. Если интерфейс Интерфейс - типа Ethernet, то физические (MAC) адреса исходящих пакетов будут широковещательными.

Вторая версия

ip route АдресСетиНазначения МаскаСетиНазначения Адрес

Команда указывает маршрутизатору, что все пакеты, предназначенные для АдресСетиНазначения-МаскаСетиНазначения, следует направлять на тот свой интерфейс, из которого достижим IP адрес Адрес. Как правило, Адрес это адрес следующего хопа по пути к АдресСетиНазначения. Выходной интерфейс и физические адреса исходящих пакетов определяются маршрутизатором по своим ARP таблицам на основании IP адреса Адрес. Например

ip route 10.6.0.0 255.255.0.0 Serial1 (1)

ip route 10.7.0.0 255.255.0.0 10.4.0.2 (2)

Первый пример отображает сетевой префикс 10.6.0.0/16 на локальный интерфейс маршрутизатора Serial1. Следующий пример отображает сетевой префикс 10.7.0.0/16 на IP адрес 10.4.0.2 следующего хопа по пути к 10.7.0.0/16. Обе эти команды добавят статические маршруты в таблицу маршрутизации (метка S):

S 10.6.0.0 via Serial1

S 10.7.0.0 [1/0] via 10.4.0.2

Когда интерфейс падает, все статические маршруты, отображаемые на этот интерфейс, удаляются из таблицы маршрутов. Если маршрутизатор не может больше найти адрес следующего хопа по пути к адресу, указанному в статическом маршруте, то маршрут исключается из таблицы.

Заметим, что для сетей типа Ethernet рекомендуется всегда использовать форму (2) команды ip route. Ethernet интерфейс на маршрутизаторе, как правило, соединён с несколькими Ethernet интерфейсами других устройств в сети. Указание в команде ip route IP адреса позволит маршрутизатору правильно сформировать физический адрес выходного пакета по своим ARP таблицам.

1.2 Маршрут по умолчанию.

Совсем не обязательно, чтобы каждый маршрутизатор обслуживал маршруты ко всем возможным сетям назначения. Вместо этого маршрутизатор хранит маршрут по умолчанию или шлюз последнего пристанища (last resort). Маршруты по умолчанию используются, когда маршрутизатор не может поставить в соответствие сети назначения строку в таблице маршрутов. Маршрутизатор должен использовать маршрут по умолчанию для отсылки пакетов другому маршрутизатору. Следующий маршрутизатор будет иметь маршрут к этой сети назначения или иметь свой маршрут по умолчанию к третьему маршрутизатору и т.д. В конечном счёте, пакет будет маршрутизирован на маршрутизатор, имеющий маршрут к сети назначения.

Маршрут по умолчанию может быть статически введен администратором или динамически получен из протокола маршрутизации.

Так как все IP адреса принадлежат сети 0.0.0.0 с маской 0.0.0.0, то в простейшем случае надо использовать команду

ip route 0.0.0.0 0.0.0.0 [адрес следующего хопа | выходной интерфейс]

Ручное задание маршрута по умолчанию на каждом маршрутизаторе подходит для простых сетей. В сложных сетях необходимо организовать динамический обмен маршрутами по умолчанию.

1.3 Команда trace

Команда trace является идеальным способом для выяснения того, куда отправляются данные в сети. Эта команда использует ту же технологию протокола ICMP, что и команда ping, только вместо проверки сквозной связи между отправителем и получателем, она проверяет каждый шаг на пути. Команда trace использует способность маршрутизаторов генерировать сообщения об ошибке при превышении пакетом своего установленного времени жизни (Time To Live, TTL). Эта команда посылает несколько пакетов и выводит на экран данные про время прохождения туда и назад для каждого из них. Преимущество команды

trace заключается в том, что она показывает очередной достигнутый маршрутизатор на пути к пункту назначения. Это очень мощное средство для локализации отказов на пути от отправителя к получателю.

Таблица 3.1 - Варианты ответов утилиты trace

Символ	Значение
!H	Зондирующий пакет был принят маршрутизатором, но не переадресован, что обычно бывает из-за списка доступа
P	Протокол недосягаем
N	Сеть недосягаема
U	Порт недосягаем
*	Превышение границы ожидания

2 Практическая часть

Статические маршруты

Рисунок 2.1 – Схема сети.

1. Собрать схему сети, представленную на рисунке 2.1 в части расстановки устройств в области рабочего стола, подключения рабочих станций к коммутаторам. Дальнейшее подключение выполнять по мере настройки оборудования.

2. Настроить на обоих коммутаторах в режиме access vlan 100 на интерфейсе FastEthernet 0/1 и vlan 200 на интерфейсе FastEthernet 0/2. Интерфейс FastEthernet 0/24 настроить в режиме передачи и приема тегированных пакетов 100 и 200 vlan.

3. Настроить на PC0, подключенного к FastEthernet 0/1 коммутатора Switch0, ip address 192.168.0.2/24, шлюз 192.168.0.1

4. Настроить на PC1, подключенного к FastEthernet 0/2 коммутатора Switch0, ip address 192.168.1.2/24, шлюз 192.168.1.1

5. Настроить на PC2, подключенного к FastEthernet 0/1 коммутатора Switch1, ip address 192.168.101.2/24, шлюз 192.168.101.1

6. Настроить на PC1, подключенного к FastEthernet 0/2 коммутатора Switch1, ip address 192.168.102.2/24, шлюз 192.168.102.1

7. Настроить маршрутизатор Router 3 следующим образом:

7.1. Интерфейс GigabitEthernet 0/1, подключенный к порту FastEthernet 0/24 коммутатора Switch 0, в режиме субинтерфейсов настроить на обработку 100 и 200 vlan.

7.2. Интерфейс GigabitEthernet 0/0, подключенный к интерфейсу GigabitEthernet 0/2 маршрутизатора Router0, ip адрес 10.10.10.1/30.

7.3.Не забывать выводить интерфейсы маршрутизатора из состояния административного отключения командой no shutdown и сохранять конфигурацию.

8. Настроить маршрутизатор Router0 следующим образом:

8.1.Интерфейс GigabitEthernet 0/2, подключенный к интерфейсу GigabitEthernet 0/0 маршрутизатора Router3, ip адрес 10.10.10.2/30.

8.2.Интерфейс GigabitEthernet 0/0, подключенный к интерфейсу GigabitEthernet 0/1 маршрутизатора Router2, ip адрес 10.10.20.1/30.

8.3.Интерфейс GigabitEthernet 0/1, подключенный к интерфейсу GigabitEthernet 0/0 маршрутизатора Router1, ip адрес 10.10.20.10/30.

8.4.Не забывать выводить интерфейсы маршрутизатора из состояния административного отключения командой no shutdown и сохранять конфигурацию

9. Настроить маршрутизатор Router2 следующим образом:

9.1. Интерфейс GigabitEthernet 0/0, подключенный к интерфейсу GigabitEthernet 0/1 маршрутизатора Router1, ip адрес 10.10.20.5/30.

9.2. Интерфейс GigabitEthernet 0/1, подключенный к интерфейсу GigabitEthernet 0/0 маршрутизатора Router0, ip адрес 10.10.20.1/30.

9.3.Не забывать выводить интерфейсы маршрутизатора из состояния административного отключения командой no shutdown и сохранять конфигурацию

10. Настроить маршрутизатор Router2 следующим образом:

10.1. Интерфейс GigabitEthernet 0/2, подключенный к интерфейсу GigabitEthernet 0/0 маршрутизатора Router4, ip адрес 10.10.10.6/30.

10.2. Интерфейс GigabitEthernet 0/0, подключенный к интерфейсу GigabitEthernet 0/1 маршрутизатора Router0, ip адрес 10.10.20.9/30.

10.3. Интерфейс GigabitEthernet 0/1, подключенный к интерфейсу GigabitEthernet 0/0 маршрутизатора Router2, ip адрес 10.10.20.6/30.

10.4. Не забывать выводить интерфейсы маршрутизатора из состояния административного отключения командой no shutdown и сохранять конфигурацию

11. Настроить маршрутизатор Router4 следующим образом:

11.1. Интерфейс GigabitEthernet 0/1, подключенный к порту FastEthernet 0/24 коммутатора Switch 1, в режиме субинтерфейсов настроить на обработку 100 и 200 vlan.

11.2. Интерфейс GigabitEthernet 0/0, подключенный к интерфейсу GigabitEthernet 0/2 маршрутизатора Router0, ip адрес 10.10.10.5/30.

11.3. Не забывать выводить интерфейсы маршрутизатора из состояния административного отключения командой no shutdown и сохранять конфигурацию.

Часть 2.

1. Router4)

2. Проверить с помощью команды ping на одной из рабочих станций (PC0 или PC1) прохождение пакетов на участке от компьютера до шлюза, затем до внешнего интерфейса маршрутизатора (10.10.10.1), затем до интерфейса GigabitEthernet 0/2 маршрутизатора Router0. Попытаться объяснить наблюдаемый результат.

3. Настроить статическую маршрутизацию на маршрутизаторе Router0 в сторону клиентских сетей PC0 и PC1. Для этого необходимо выполнить следующие команды: ip route 192.168.0.0 255.255.255.0 10.10.10.1; ip route 192.168.1.0 255.255.255.0 10.10.10.1

4. Настроить статическую маршрутизацию на маршрутизаторе Router1 в сторону клиентских сетей PC2 и PC3. Для этого необходимо выполнить следующие команды: ip route 192.168.101.0 255.255.255.0 10.10.10.5; ip route 192.168.102.0 255.255.255.0 10.10.10.5.

5. Настроить статическую маршрутизацию на маршрутизаторе Router1 в сторону клиентских сетей PC0 и PC1. Так как у нас существует два маршрута к клиентским сетям PC0 и PC1, используем метрику маршрута. Для этого необходимо выполнить следующие команды: ip route 192.168.0.0 255.255.255.0 10.10.20.10 25; ip route 192.168.0.0 255.255.255.0 10.10.20.5 50, ip route 192.168.1.0 255.255.255.0 10.10.20.10 25; ip route 192.168.1.0 255.255.255.0 10.10.20.5 50.

6. Настроить статическую маршрутизацию на маршрутизаторе Router0 в сторону клиентских сетей PC2 и PC3. Так как у нас существует два маршрута к клиентским сетям PC2 и PC3, используем метрику маршрута. Для этого необходимо выполнить следующие команды: ip route 192.168.101.0 255.255.255.0 10.10.20.9 25; ip route 192.168.101.0 255.255.255.0 10.10.20.2 50, ip route 192.168.102.0 255.255.255.0 10.10.20.9 25; ip route 192.168.102.0 255.255.255.0 10.10.20.2 50.

7. Настроить статическую маршрутизацию на маршрутизаторе Router2 в сторону клиентских сетей PC0 и PC1. Существует единственный маршрут к клиентским сетям PC0 и PC1, поэтому метрику маршрута использовать не будем. Для этого необходимо выполнить следующие команды: ip route 192.168.0.0 255.255.255.0 10.10.20.1; ip route 192.168.1.0 255.255.255.0 10.10.20.1.

8. Настроить статическую маршрутизацию на маршрутизаторе Router2 в сторону клиентских сетей PC2 и PC3. Существует единственный маршрут к клиентским сетям PC2 и PC3, поэтому метрику маршрута использовать не будем. Для этого необходимо выполнить следующие команды: ip route 192.168.101.0 255.255.255.0 10.10.20.6; ip route 192.168.102.0 255.255.255.0 10.10.20.6.

Сохраните проект в целом и конфигурацию каждого маршрутизатора в отдельный файл.

Задание для самостоятельной работы

1. Построить в Packet Tracer топологию, представленную на рисунке 2.1 и выполнить индивидуальные задания согласно номеру варианта

Таблица 1 – Задание на самостоятельную работу

Вариант	VLAN100	VLAN200	Вариант	VLAN100	VLAN200
1	11.1.0.0/16	5.1.0.0/16	6	6.1.0.0/16	7.1.0.0/16
2	3.1.0.0/16	10.10.0.0/16	7	8.1.0.0/16	10.1.0.0/16
3	8.1.0.0/16	11.1.0.0/16	8	8.1.0.0/16	11.1.0.0/16
4	2.1.0.0/16	3.1.0.0/16	9	12.1.0.0/16	13.1.0.0/16

5	4.1.0.0/16	5.1.0.0/16	10	3.1.0.0/16	5.1.0.0/16

Контрольные вопросы

1. Чем статическая маршрутизация отличается от динамической?
2. Какие две формы задания статической маршрутизации вы знаете?
3. Как в команде маршрутизации определяется сеть назначения?
4. Почему для сетей типа Ethernet рекомендуется всегда использовать форму (2) команды маршрутизации?
5. Объясните значения полей в командах маршрутизации.
6. Почему в качестве поля Адрес рекомендуют использовать адрес следующего хопа по пути к сети назначения.
7. Когда используется маршрут по умолчанию?
8. Когда используют интерфейс петля?
9. Как работает команда трасировки?

Лабораторная работа №3.

Динамическая маршрутизация. Изучение протокола RIP.

Цель работы:

1. Изучение принципа работы и конфигурации RIP маршрутизации.

2. Получить навыки по конфигурированию протоколов динамической маршрутизации в локальных компьютерных сетях RIP.

1 Теоретическая часть

Для начала разберемся с понятием “динамическая маршрутизация”. До сего момента мы использовали так называемую статическую маршрутизацию, то есть прописывали руками таблицу маршрутизации на каждом роутере. Маршрутизаторы в сложных сетях должны быстро адаптироваться к изменениям топологии и выбирать лучший маршрут из многих кандидатов.

Динамическая маршрутизация – это вид маршрутизации, при котором таблица маршрутизации редактируется программно. Помимо удобства есть и другие аспекты. Например, отказоустойчивость. Имея сеть со статической маршрутизацией, вам крайне сложно будет организовать резервные каналы – некому отслеживать доступность того или иного сегмента.

Рисунок 1.1

Например, если в такой сети разорвать линк между R2 и R3, то пакеты с R1 будут уходить по-прежнему на R2, где будут уничтожены, потому что их некуда отправить. Протоколы динамической маршрутизации в течение нескольких секунд (а то и миллисекунд) узнают о проблемах на сети и перестраивают свои таблицы маршрутизации, и в вышеописанном случае пакеты будут отправляться уже по актуальному маршруту.

Рисунок 1.2

Ещё один важный момент – балансировка трафика. Протоколы динамической маршрутизации практически из коробки поддерживают эту фичу и вам не нужно добавлять избыточные маршруты вручную, высчитывая их.

Ну и внедрение динамической маршрутизации сильно будет облегчать масштабирование сети. Когда вы добавляете новый элемент в сеть или подсеть на существующем маршрутизаторе, вам нужно выполнить всего несколько действий, чтобы всё заработало, и вероятность ошибки, будет минимальна. При этом информация об изменениях мгновенно расходится по всем устройствам. Ровно то же самое можно сказать и о глобальных изменениях топологии.

2 Дистанционно-векторная маршрутизация

Эта маршрутизация базируется на алгоритме Белмана-Форда. Через определённые моменты времени маршрутизатор передаёт соседним маршрутизаторам всю свою таблицу маршрутизации. Такие простые протоколы как RIP и IGRP просто распространяют информацию о таблицах маршрутов через все интерфейсы маршрутизатора в широковещательном режиме без уточнения точного адреса конкретного соседнего маршрутизатора. Соседний маршрутизатор, получая широковещание, сравнивает информацию со своей текущей таблицей маршрутов. В неё добавляются маршруты к новым сетям или маршруты к известным сетям с лучшей метрикой. Происходит удаление несуществующих маршрутов.

Маршрутизатор добавляет свои собственные значения к метрикам полученных маршрутов. Новая таблица маршрутизации снова распространяется по соседним маршрутизаторам.

3 Классификация протоколов динамической маршрутизации

Все протоколы маршрутизации можно разделить на две большие группы: внешние (EGP – Exterior Gateway Protocol) и внутренние (IGP – Interior Gateway Protocol). Чтобы объяснить различия между ними, нам потребуется термин “автономная система”. В общем смысле, автономной системой (доменом маршрутизации) называется группа роутеров, находящихся под общим управлением.

Так вот, протоколы внутренней маршрутизации используются внутри автономной системы, а внешние – для соединения автономных систем между собой. В свою очередь, внутренние протоколы маршрутизации подразделяются на Distance-Vector (RIP, EIGRP) и Link State (OSPF, IS-IS).

В данной лабораторной работе мы будем затрагивать протоколы RIP и IGRP в силу их почтенного возраста.

3. Протокол RIP

Протокол RIP (Routing Information Protocol, протокол маршрутной информации) является наиболее простым протоколом динамической маршрутизации. Он относится к протоколам типа «вектор-расстояние». Под вектором протокол RIP определяет IP-адреса сетей, а расстояние измеряется в переходах («хопах», hope) – количестве маршрутизаторов, которое должен пройти пакет, чтобы достичь указанной сети. Следует отметить, что максимальное значение расстояния для протокола RIP равно 15, значение 16 трактуется особым образом «сеть недостижима». Это определило основной недостаток протокола – он оказывается неприменимым в больших сетях, где возможны маршруты, превышающие 15 переходов.

Протокол RIP версии 1 имеет ряд существенных для практического использования недостатков. К числу важных проблем относятся следующие:

1. Оценка расстояния только с учетом числа переходов. Протокол RIP не учитывает реальную производительность каналов связи, что может оказаться неэффективным в гетерогенных

сетях, т.е. сетях, объединяющих каналы связи различного устройства, производительности, в которых используются разные сетевые технологии.

2. Проблема медленной конвергенции. Маршрутизаторы, использующие протокол RIP, рассылают маршрутную информацию каждые 30 с, причем их работа не синхронизирована. В ситуации, когда некоторый маршрутизатор обнаружит, что какая-либо сеть стала недоступной, то в худшем случае (если проблема была выявлена сразу после очередной рассылки) он сообщит об это соседям через 30 с. Для соседних маршрутизаторов все будет происходить также. Это означает, что информация о недоступности какой-либо сети может распространятся маршрутизаторам в достаточно долго, очевидно, что сеть при этом будет находиться в нестабильном состоянии.

3. Широковещательная рассылка таблиц маршрутизации. Протокол RIP изначально предполагал, что маршрутизаторы рассылают информацию в широковещательном режиме. Это означает, что отправленный пакет вынуждены получить и проанализировать на канальном, сетевом и транспортном уровне все компьютеры сети, в которую он направлен. Для передачи сообщений RIPv1 в адресе получателя используется широковещательный адрес 255.255.255.255, а RIPv2 – мультикаст адрес 224.0.0.9.

Частично указанные проблемы решаются в версии 2 (RIP2).

4 Команды протокола RIP

Выбор протокола RIP к протоколу маршрутизации осуществляется командой:

Router(config)# router rip

Router(conf-router) # version 2

Router(conf-router) # network <классовая сеть>

RIPv2 бесклассовый протокол маршрутизации, но в команде network может быть указана только классовая сеть. Даже если указать сеть с маской, которая не соответствует классовой, RIP автоматически преобразует её в классовую сеть. Команда network указывает только на каких интерфейсах включить RIP, а фактическая сеть и маска будет взята из настроек интерфейса.

5 Маршрут по умолчанию

Команда default-information originate:

Router(config-router) # default- information originate [route-map <map-name>]

RIP будет анонсировать маршрут по умолчанию, даже если маршрута по умолчанию нет в таблице маршрутизации.

Команда redistribute static:

Если в таблице маршрутизации есть статический маршрут по умолчанию, то можно анонсировать его с помощью команды redistribute static.

Router(config-router) # redistribute static [metric <metric> [route-map <map-name>]. Команда debug ip rip выводит содержание пакетов актуализации маршрутной информации протокола RIP в том виде, в котором эти данные посылаются и принимаются.

6 Практическая часть.

Рисунок 6.1. Сеть для динамической маршрутизации

На рисунке 6.1 показана сеть, для которой будут применены протоколы маршрутизации. Очевидно, что к коммутаторам Switch0 и Switch1 можно добавить еще несколько компьютеров, не делая никаких дополнительных настроек в маршрутизаторах. PC0 имеет IP 192.168.1.2 (маска 255.255.255.0), шлюзом по умолчанию является интерфейс FastEthernet0/0 маршрутизатора Router0 с IP 192.168.1.1. Если подключить к Switch0 другие компьютеры, то им можно давать адреса 192.168.1.x, где x – число от 3 и до 254. Аналогично организована и подсеть Router1 – PC1 с IP, маршрутизатора – 192.168.2.1, компьютера – 192.168.2.2. Для интерфейсов FastEthernet0/1 маршрутизаторов Router0 и Router1 выделены IP адреса 172.16.1.2/24 и 172.16.2.2/24 соответственно. Маршрутизатор Router2 имеет адреса интерфейсов 172.16.1.1/24 и 172.16.2.1/24.

Таким образом, для того, если отправить пакет от PC0 до PC1, ему потребуется пройти несколько подсетей – 192.168.1.0, 172.16.1.0, 172.16.2.0 и 192.168.2.0. Если зайти с рабочего стола PC0 в командную строку (command promt) можно ввести команду tracert (trace route – трассировка маршрута), можно посмотреть, как будут идти пакеты. До настройки маршрутизации пакеты не могут уйти дальше шлюза, как показано на рисунке 6.2.

Рисунок 6.2. Трассировка маршрута до настройки маршрутизации

Протокол RIP довольно прост в конфигурировании. Для того чтобы сконфигурировать протокол, необходимо задать адреса подсетей, анонсируемых маршрутизатором.

Настройка маршрутизатора Router0:

```
Router(config-if)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.1.0
Router(config-router)#network 172.16.1.0
Router(config-router)#exit
Router(config)#exit
```

Настройка маршрутизатора Router1:

```
Router#enable
Router#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.2.0
Router(config-router)#network 172.16.2.0
Router(config-router)#exit
Router(config)#exit
```

Настройка маршрутизатора Router2:

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#router rip

Router(config-router)#version 2

Router(config-router)#network 172.16.1.0

Router(config-router)#network 172.16.2.0

Router(config-router)#exit

Router(config)#exit

Теперь протокол RIP на маршрутизаторе настроен, запустим снова команду tracert на PC0, ее результат показан на рисунке 6.3.

Рисунок 6.3. Трассировка маршрута после настройки маршрутизации

Варианты лабораторных работ

Задание.

- В задании дан рисунок – сеть, которую вы должны построить в Cisco Packet Tracer и ip-адреса компьютеров и других устройств, входящих в сеть.
- Адреса для маршрутизаторов предлагается придумать самостоятельно, для подсетей между маршрутизаторами можно использовать диапазон 10.0.0.0/8.
- Перед тем, как начать конфигурировать протоколы, постройте саму сеть, некоторые маршрутизаторы потребуют дополнительных портов – добавьте их.
- Настройте протокол RIP на всех маршрутизаторах. Вы должны уметь делать это и через графический интерфейс и (это более важно) с помощью команд CLI. Конечная цель – чтобы любой компьютер вашей сети мог отправить пакет с помощью команды ping или tracert на любой другой компьютер вашей сети.
- В отчете проиллюстрируйте как процесс работы (настройка компьютеров и маршрутизаторов, команды CLI) так и ее результат - (команды ping и трассировка). Не обязательно иллюстрировать отправку сообщений с каждого компьютера на каждый (для, например 5 компьютеров это довольно много).

Вариант 1.

На компьютерах настроить следующие IP-адреса:

ПК0: 192.168.1.2

ПК1: 192.168.2.2

ПК2: 192.168.3.2

Вариант 2.

На компьютерах настроить следующие IP-адреса:

ПК0: 172.16.5.7

ПК1: 172.16.38.3

ПК2: 172.16.24.17

ПК3: 172.16.82.5

Вариант 3.

На компьютерах настроить следующие IP-адреса:

ПК0: 192.168.135.5

ПК1: 192.168.122.4

ПК2: 192.168.115.3

ПК3: 192.168.109.2

Вариант 4.

На компьютерах настроить следующие IP-адреса:

ПК0: 172.16.11.2

ПК1: 172.16.12.4

ПК2: 172.16.13.5

ПК3: 172.16.14.6

Вариант 5.

На компьютерах настроить следующие IP-адреса:

ПК0: 192.168.70.2

ПК1: 192.168.71.2

ПК2: 192.168.72.2

ПК3: 192.168.73.2

Вариант 6.

На компьютерах настроить следующие IP-адреса:

ПК0: 192.168.1.1

ПК1: 172.16.1.1

Вариант 7.

На компьютерах настроить следующие IP-адреса:

ПК0: 192.168.2.2 ПК1: 192.168.2.3 ПК2: 192.168.2.4

ПК3: 192.168.3.2 ПК4: 192.168.4.2 На принтере: 192.168.2.5

Вариант 8.

На компьютерах настроить следующие IP-адреса:

ПК0: 172.16.3.2

ПК1: 172.16.4.2

ПК2: 172.16.5.2

ПК3: 172.16.6.2

ПК4: 172.16.7.2

Вариант 9.

Сервер: 192.168.1.1

Принтер: 192.168.100.17

ПК0: 192.168.100.16

ПК1: 172.16.2.2

ПК2: 172.16.3.2

ПК3: 172.16.105.7

Вариант 10.

На компьютерах настроить следующие IP-адреса:

ПК0: 192.168.1.2 ПК1: 192.168.2.2 ПК2: 192.168.3.2

ПК3: 192.168.4.2 ПК4: 192.168.5.2 ПК5: 192.168.6.2

Контрольные вопросы

1.Чем динамическая маршрутизация отличается от статической?

2.Плюсы и минусы динамической маршрутизации?

3.Что такое метрика?

4.Что такое хоп?

5.Какие существуют два класса протоколов динамической маршрутизации?

6.Как на маршрутизаторе запустить и настроить протокол маршрутизации RIP?

7.Когда сеть-получатель считается недостижимой?

8.Чем отличается RIPv1от RIPv2?

9.Что такое маршрут по умолчанию?

Лабораторная работа №4.

Динамическая маршрутизация. Протокол EIGRP.

Цель работы:

1. Изучение принципа работы и конфигурации EIGRP маршрутизации.

2. Получить навыки по конфигурированию протоколов динамической маршрутизации в локальных компьютерных сетях EIGRP.

1 Теоретическая часть

Маршрутизаторы используют метрики для оценки или измерения маршрутов. Когда от маршрутизатора к сети назначения существует много маршрутов, и все они используют один протокол маршрутизации, то маршрут с наименьшей метрикой рассматривается как лучший. Если используются разные протоколы маршрутизации, то для выбора маршрута используется административные расстояния, которые назначаются маршрутам операционной системой маршрутизатора. RIP использует в качестве

метрики количество переходов (хопов). EIGRP использует сложную комбинацию факторов, включающую полосу пропускания канала и его надёжность.

Для того чтобы динамические протоколы маршрутизации обменивались информацией о статических маршрутах, следует осуществлять дополнительное конфигурирование.

Метрика, применяемая протоколом EIGRP составная потому, что выбор лучшего маршрута осуществляется на базе более одного значения. Факторы, на основе которых EIGRP вычисляет метрику, – это пропускная способность, нагрузка, задержка и надежность.

2 Конфигурирование динамической маршрутизации

Для конфигурирования динамической маршрутизации используются две основные команды: router и network. Команда router запускает процесс маршрутизации и имеет форму:

Router(config)# router protocol [keyword], где Protocol - любой из протоколов маршрутизации: RIP, IGRP, OSPF и т.п., keyword – дополнительные параметры.

Затем необходимы команды network:

Router (config-router)# network network-number [keyword], где network-number - идентифицирует непосредственно подключенную сеть, добавляемую в процесс маршрутизации, keyword –дополнительные параметры. Networknumber позволяет процессу маршрутизации определить интерфейсы, которые будут брать участие в отсылке и приёме пакетов актуализации маршрутной информации. Для просмотра информации о протоколах маршрутизации используется команда show ip protocol, которая выводит значения таймеров процессов маршрутизации и сетевую информацию, имеющую отношение к маршрутизации. Эта информация может использоваться для идентификации маршрутизатора, подозреваемого в поставке плохой маршрутной информации Содержимое таблицы IP маршрутизации выводится командой show ip route. Она содержит записи про все известные маршрутизатору сети и подсети и указывает на способ получения этой информации.

3 Протокол EIGRP

Протокол EIGRP (Enhanced Interior Getaway Routing Protocol) – расширенный протокол маршрутизации внутреннего шлюза является расширенной версией протокола IGRP. Он является фирменным протоколом корпорации Cisco представленным в 1994 году, однако в настоящее время ряд сторонних производителей лицензировал EIGRP для реализации в своем телекоммуникационном оборудовании.

По способу представления маршрутной информации протокол EIGRP все же является дистанционно-векторным протоколом. Сети получатели в маршрутных обновлениях сопровождаются метриками и адресами «следующих» маршрутизаторов. Подобно другим дистанционно-векторным протоколам, протокол EIGRP не обладает полными знаниями о топологии сети передачи данных.

Однако в основе протокола EIGRP лежит не алгоритм Беллмана-Форда, а алгоритм DUAL (Diffusing Update Algorithm), алгоритм диффузионного обновления.

1.3 Алгоритм диффузионного обновления

Алгоритм DUAL лежит в основе протокола EIGRP. Поэтому рассмотрим его первым. Начнем с классического алгоритма DUAL. А затем рассмотрим необходимые изменения для адаптации алгоритма для протокола маршрутизации EIGRP.

Протоколы маршрутизации на основе дистанционно-векторного алгоритма Беллмана-Форда, имеют две фундаментальные проблемы:

–Маршрутные петли;

–Счет до бесконечности.

Обе эти проблемы обусловлены тем, что маршрутизаторы ничего не знают о действительной топологии сети передачи данных. Все что они знают, это какие сети получатели доступны через каждого из соседей. Когда в сети происходят изменения, маршрутизаторы пытаются переключать маршруты на основании новых метрик, которые им становятся известны.

До достижения сходимости сети, метрики могут неточно отражать действительную стоимость маршрутов, что может привести к маршрутным петлям.

Основным методом борьбы с возникновением маршрутных петель является введение метрики равной бесконечности, при достижении которой маршрут считается недоступным. Обычно маршрутизаторам необходимо выполнить некоторое число итераций, перед тем как установить метрику в бесконечность, следовательно, время сходимости сети с использованием дистанционно-векторных алгоритмов значительно увеличивается. Чтобы ускорить схождение сети, приходиться применять дополнительные методы: правило расщепления горизонта, метод обратного обновления, мгновенные обновления и таймеры удержания информации.

Вспомним, какую информацию маршрутизаторы получают друг от друга и как они ее используют. Маршрутизаторы в случае использования алгоритма Беллмана-Форда, обмениваются маршрутными обновлениями, содержащими известные им сети получатели. Каждая сеть получатель, сопровождается метрикой, отражающей, насколько далеко маршрутизатор, отправляющий это маршрутное обновление, по его мнению, находиться от данной сети.

Отслеживание метрик соседей маршрутизатора - это то, что составляет ядро подхода DUAL. По сравнению с подходом DUAL дистанционно-векторный алгоритм Беллмана-Форда кажется несколько близоруким. Подход алгоритма DUAL заключающийся в более глубоком рассмотрении окружения, позволяет получить знания о топологии, которых часто оказывается достаточно для принятия быстрых решений о маршрутизации, что очень важно для достижения более быстрого схождения.

2 Преимущества протокола EIGRP

Как и все бесклассовые протоколы маршрутизации, протокол EIGRP рассылает обновления маршрутной информации с масками подсетей. Это позволяет поддерживать работу с изолированными подсетями и масками подсетей переменной длины.

Протокол EIGRP представляет собой комбинированный протокол маршрутизации, включающий многие свойства дистанционно-векторных протоколов и, кроме того, некоторые характеристики протоколов маршрутизации по состоянию канала. Такой гибридный протокол обеспечивает следующие возможности:

– Быстрота процесса сходимости. Маршрутизатор, с запущенным протоколом EIGRP, сохраняет резервные маршруты, что повышает скорость сходимости сети. Если в локальной таблице маршрутизации нет соответствующего резервного маршрута, протокол EIGRP опрашивает соседние маршрутизаторы. Эти запросы рассылаются до тех пор, пока альтернативный маршрут не будет найден.

– Снижение служебного трафика. Протокол EIGRP не рассылает периодические обновления. Вместо этого здесь используются частичные обновления при изменении маршрутов или метрик маршрутов

к получателям. При изменении маршрутизирующей информации алгоритм DUAL рассылает обновление только о конкретном канале передачи данных, не затрагивая при этом всю таблицу маршрутизации.

– Поддержка на различных сетевых уровнях. Протокол EIGRP поддерживает сети IP, IPX, и Apple Talk благодаря применению модулей PDM (protocol dependent modules).

– Совместимость между всеми протоколами и топологиями. EIGRP не требует специальной конфигурации для работы с любыми протоколами второго уровня. Другие протоколы маршрутизации, например OSPF, используют различные конфигурации для различных протоколов второго уровня, таких как Ethernet или Frame Relay. EIGRP также поддерживает настройки позволяющие снижать служебный трафик по низкоскоростным каналам связи.

3 Конфигурация EIGRP

Создание процесса EIGRP:

Router(config)# router eigrp <AS>

Номер автономной системы должен быть одинаковым на всех маршрутизаторах, которые должны обмениваться информацией по протоколу EIGRP. Для того чтобы маршрутизаторы начали обмениваться информацией, необходимо включить EIGRP на интерфейсах.

Включение EIGRP на интерфейсах:

Router(config)# router eigrp 100

Router(config-router)# network <network> [wildcard mask]

<network> – непосредственно присоединенная сеть к маршрутизатору. [wildcard mask] – маска, которая указывает с помощью нулей, какая часть из указанной сети должна совпадать, а с помощью 1 какая часть сети может быть произвольной. Этот параметр опциональный. Если его не задать, то будет использоваться классовая маска для указанной сети.

Маршрут по умолчанию

Маршрут по умолчанию EIGRP может быть настроен с помощью команды:

Router(config-router)# ip default-network <network-number>

Очистка отношений соседства

Для того чтобы удалить соседа, маршруты полученные от него и заново начать процесс установки отношений соседства, необходимо выполнить команду:

Router# clear ip eigrp neighbors [ip-address]

Очистить все отношения соседства, соответственно очищается вся таблица топологии:

Router# clear ip eigrp neighbors

Очистить все отношения соседства для указанного интерфейса:

Router# clear ip eigrp neighbors [interface]

Аутентификация EIGRP

Создание цепочки ключей:

Router(config)# key chain passw

Router(config-keychain)# key 1

Router(config-keychain-key)# key-string password1

Настройка аутентификации:

Router(config-if)# ip authentication mode eigrp 1 md5

Router(config-if)# ip authentication key-chain eigrp 1 passw

4 Практическая часть

Зайдите в CLI маршрутизатора. В режиме глобальной конфигурации введите команду router eigrp 1. Как и в OSPF, «1» - это идентификатор процесса. Команды конфигурации EIGRP очень похожи на команды конфигурации OSPF, однако в EIGRP нет поддержки логического разбиения на зоны, поэтому команда network принимает следующий вид: network <адрес_сети> <инвертированная_маска>. С помощью этой команды перечислите все сети, на интерфейсах которых должен быть задействован протокол EIGRP. Отключите автосуммирование маршрутов командой no auto-summary. Повторите данные действия на оставшихся маршрутизаторах, а также на многоуровневом коммутаторе.

Стоит отметить, что после завершения всех настроек оптимальный путь от сети первого филиала до сети второго будет проходить через следующий маршрутизатор, т.е EIGRP автоматически просчитывает правильные метрики даже для маршрутов с высокоскоростными интерфейсами GigabitEthernet. С помощью команды key chain <название_цепочки>в режиме глобальной конфигурации устройства создайте цепочку ключей (эта команда переводит CLI в режим конфигурирования цепочки). Укажите идентификатор ключа с помощью команды key <идентификатор>, эта команда также переводит CLI в режим конфигурирования ключа. Задайте ключ (т.е. пароль) для аутентификации командой key-string<значение> в режиме конфигурирования ключа.

Включите MD5-аутентификацию для протокола EIGRP на интерфейсе для определенного номера автономной системы (ASN) с помощью команды ip authentication mode eigrp <номер-АС> md5 в режиме конфигурирования интерфейса. Привяжите правильную цепочку ключей к интерфейсу. Для этого перейдите в режим конфигурирования интерфейса и введите команду ipauthentication key-chain eigrp <номер-АС> <название_цепочки>. Повторите эти действия на всех интерфейсах маршрутизаторов, которые учавствуют в динамической маршрутизации (коммутаторы третьего уровня не поддерживают аутентификацию). Обратите внимание, что идентификатор ключа и сам ключ должны совпадать на обоих концах линии связи.

Включение протокола EIGRP

Рисунок 4.1

1) Соберите схему как показано на рисунке 4.1.

2) Задайте каждому компьютеру IP-адрес и шлюз (возьмите индивидуальный IP-адрес и шлюз).

Пример.

Таблица 4.1

Компьютер	IP-адрес/маска	Шлюз по-умолчанию

PC0	172.16.1.2/24	172.16.1.1
PC1	172.17.1.2/24	172.17.1.1
PC2	172.18.1.2/24	172.18.1.1

3) Выполните настройку маршрутизаторов по примеру:

Router0

Router(config)#int fa0/0

Router(config-if)#ip ad 172.16.1.1 255.255.255.0

Router(config-if)#no shut

Router(config)#int s0/3/0

Router(config-if)#ip ad 192.168.1.1 255.255.255.0

Router(config-router)#network 172.16.0.0

Router(config-router)#network 192.168.1.0

Router(config-router)#network 192.168.3.0

Router1

Router(config)#int fa0/0

Router(config-if)#ip ad 172.17.1.1 255.255.255.0

Router(config-if)#no shut

Router(config)#int s0/3/0

Router(config-if)#ip ad 192.168.2.1 255.255.255.0

Router(config-if)#no shut

Router(config)#int s0/3/1

Router(config-if)#no shut

Router(config)#router eigrp 100

Router(config-router)#network 172.17.0.0

Router(config-router)#network 192.168.1.0

Router(config-router)#network 192.168.2.0

Router2

Router(config)#int fa0/0

Router(config-if)#ip ad 172.18.1.1 255.255.255.0

Router(config-if)#no shut

Router(config)#int s0/3/0

Router(config-if)#ip ad 192.168.3.2 255.255.255.0

Router(config-if)#no shut

Router(config)#int s0/3/1

Router(config-if)#ip ad 192.168.2.2 255.255.255.0

Router(config-if)#no shut

Router(config)#router eigrp 100

Router(config-router)#network 172.18.0.0

Router(config-router)#network 192.168.2.0

Router(config-router)#network 192.168.3.0

4) Выполните на маршрутизаторе 1 эхо-запросы на маршрутизаторы 2 и 3 ping 172.17.1.1 и ping 172.18.1.1.

5) Выполните на маршрутизаторе 1 следующую команду и просмотрите таблицу маршрутизации.

Router#sh ip route

D 172.16.0.0/16 [90/20994560] via 192.168.1.1, 00:33:14, Serial0/3/0

172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks

D 172.17.0.0/16 is a summary, 00:33:14, Null0

C 172.17.1.0/24 is directly connected, FastEthernet0/0

D 172.18.0.0/16 [90/20994560] via 192.168.2.2, 00:32:14, Serial0/3/1

C 192.168.1.0/24 is directly connected, Serial0/3/0

C 192.168.2.0/24 is directly connected, Serial0/3/1

D 192.168.3.0/24 [90/21504000] via 192.168.1.1, 00:33:14, Serial0/3/0

[90/21504000] via 192.168.2.2, 00:32:07, Serial0/3/1

Обратите внимание на маршрут, выделенный жирным шрифтом. Null0 – это нулевой интерфейс (null interface). Весь трафик, отправляемый на нулевой интерфейс, удаляется. Это полезно для фильтрации нежелательного трафика. Протокол EIGRP создал этот маршрут по умолчанию для того, чтобы предотвратить возможные “черные дыры” при использовании одновременно маршрута по умолчанию и объединенного маршрута.

Контрольные задания

Модифицировать свой вариант из Лабораторной работы №4. Заменить динамическую маршрутизацию по протоколу EIGRP, а также включить аутентификацию с помощью хэшаMD5.

Контрольные вопросы

1.В чем заключается главный недостаток протокола EIGRP?

2.Какие положительные особенности EIGRP вы знаете?

3.При помощи каких составляющих рассчитывается метрика EIGRP?

4.Как на маршрутизаторе запустить и настроить протокол маршрутизации EIGRP?

5.Что такое автономная система?

Лабораторная работа № 5. Списки управления доступом ACL

Цель: изучение механизма фильтрации трафика с использованием списков управления доступом ACL.

1 Теоретическая часть

В результате применения списков управления доступом (access list, или сокращенно ACL) маршрутизатор или коммутатор третьего уровня (а также многие другие устройства) отбрасывает некоторые пакеты, учитывая критерии, которые определены сетевым инженером в списках. Назначение этих фильтров состоит в блокировании нежелательного трафика в сети, что позволяет не только создавать препятствия перед злоумышленниками, пытающимися проникнуть в сеть, но и не позволить служащим самой компании обращаться к тем системам, которые для них должны быть закрыты.

Ниже перечислены некоторые важные особенности списков управления доступом Cisco:

- фильтрация пакетов может осуществляться по мере их поступления в интерфейс, еще до принятия решений о маршрутизации (список на входящий трафик);
- фильтрация пакетов может производиться перед выходом из интерфейса, после принятия решений о маршрутизации (список на исходящий трафик);
- в программном обеспечении Cisco IOS для указания на то, что пакет должен быть отфильтрован, используется термин deny (запретить), а для пропуска пакета далее – термин permit (разрешить);

- если в списке управления доступом определено несколько инструкций, то пакет сравнивается с каждой инструкцией последовательно до тех пор, пока не будет найдена та инструкция, которой соответствует пакет;
- в конце каждого списка управления доступом находится неявная инструкция, запрещающая весь трафик (deny all). Поэтому, если пакет не соответствует ни одной из инструкций в списке управления доступом, он отбрасывается.

Списки управления доступом делятся на 5 видов:

Стандартные (standard) – позволяют фильтровать трафик по одному единственному критерию – IP-адрес отправителя.

Расширенные (extended) – позволяют фильтровать трафик по пяти различным критериям: IP-адрес отправителя, IP-адрес получателя, порт отправителя, порт получателя, а также протокол, инкапсулированный в пакет.

Рефлексивные (reflexive) – предоставляют возможность предотвращать атаки определенного класса, направленные на бреши в системе безопасности, поскольку позволяют отдельно пропускать через устройство каждый разрешенный TCP- или UDP-сеанс. Для этого предусмотрено, чтобы устройство реагировало определенным образом, обнаруживая первый пакет в новом сеансе обмена данными между двумя узлами. Реагируя на появление пакета, устройство добавляет в список управления доступом инструкцию permit, в результате чего разрешается прохождение в сеансе трафика, характеризующегося применением определенных IP-адресов отправителя и получателя, а также конкретного порта.

Динамические (dynamic) – связывают применение списка управления доступом с процессом аутентификации пользователя. Если аутентификация прошла успешно, то устройство динамически добавляет запись в начало списка, разрешая прохождение трафика, отправителем которого является узел, прошедший проверку подлинности.

Временные (time-based) – позволяют добавлять ограничения по времени в команды конфигурации. В некоторых случаях может потребоваться проверка пакетов с учетом критериев в списке управления доступом, но только в определенное время дня или даже в определенные дни недели.

В данной лабораторной работе будут подробно рассматриваться только стандартные и расширенные списки управления доступом, так как они имеют наиболее широкий спектр применения в корпоративных сетях. Поэтому далее будут приведены сведения, которые характеризуют только эти два вида списков управления доступом.

Существует два разных синтаксиса для обозначения списков управления доступом:

«Старый» синтаксис – для идентификации используются номера. За стандартными ACL закреплены номера 1-99 и 1300-1999, за расширенными – 100-199 и 2000-2699;

«Новый» синтаксис – для идентификации используется имя, выбранное администратором.

Независимо от того, используются ли стандартные или расширенные списки управления доступом, можно дать устройству указание, должна ли проверка проводиться с учетом всего IP-адреса или только части IP-адреса. Для этого используются инвертированные (обратные) маски подсети. Маски с инвертированными битами описывают 32-битовый номер, как и маски подсети. В отличие от последних, нулевые биты (0) в инвертированной маске служат для устройства указанием, что при выполнении операции сопоставления необходимо сравнивать соответствующие им биты в адресе с инструкцией списка управления доступом. Двоичные единицы (1) в инвертированной маске указывают устройству, что

обозначенные ими биты не должны сравниваться. Например, инвертированная маска 0.0.0.0 указывает на то, что должен быть сопоставлен весь IP-адрес, а маска 255.255.255.255 рассматривается как сопоставляемая с любыми адресами. Инвертированная маска 0.0.0.0 в Cisco IOS может быть заменена на ключевое слово host, а маска 255.255.255.255 – на ключевое слово any.

Общий синтаксис команды настройки конструкции стандартного списка управления доступом выглядит следующим образом: access-list <номер_списка> <deny | permit> <отправитель> <инвертированная_маска_отправителя>.

Примеры стандартных списков управления доступом:

access-list 1 deny host 192.168.0.1 – инструкция фильтрует все пакеты, в которых IP-адрес отправителя равен 192.168.0.1;

access-list 1 permit ip any – инструкция разрешает все пакеты с любыми IP-адресами;

access-list 1 deny ip 192.168.1.0 0.0.0.255 – инструкция фильтрует пакеты, в которых IP-адрес отправителя принадлежит подсети 192.168.1.0.

Расширенные списки управления доступом позволяют проводить проверку по многим критериям, поэтому синтаксис соответствующей команды невозможно записать в виде одной универсальной команды. В такие списки также можно вводить наименования протоколов и номера портов. Ниже приведены таблицы, в которых указана необходимая информация о приложениях и соответствующих им стандартных номеров портов, а также операторы, которые используются при проверке номеров портов:

Таблица 1.1 – Приложения и соответствующие им номера портов

Номер порта	**Протокол**	**Приложение**	**Ключевое слово с обозначением названия приложения в синтаксисе команды *access-list***
20	TCP	FTP	*data ftp-data*
21	TCP	FTP	*ftp*
22	TCP	SSH	-
23	TCP	Telnet	*telnet*
25	TCP	SMTP	*smtp*
53	TCP, UDP	DNS	*domain*
67,68	UDP	DHCP	*nameserver*
69	UDP	TFTP	*tftp*
80	TCP	HTTP(WWW)	*www*
110	TCP	POP3	*pop3*
161	UDP	SNMP	*snmp*
443	TCP	SSL	-
16384-32767	UDP	Передача голоса (VoIP)	-

Таблица 1.2 – Операторы, использующиеся при проверке номеров портов

Оператор в команде access-list	**Значение**
Eq	Равно
Neq	Не равно
Lt	Меньше
Gt	Больше
Range	Диапазон номеров портов

Примеры расширенных списков управления доступом:

access-list 101 deny ip any host 192.168.1.1 – инструкция фильтрует IP-пакеты с любым адресом отправителя и адресом получателя 192.168.1.1;

access-list 101 deny tcp any host 192.168.1.1 eq telnet – инструкция фильтрует TCP-пакеты с любым адресом отправителя, адресом получателя 192.168.1.1 и номером порта получателя 23 (используется ключевое слово telnet);

access-list 101 permit tcp host 192.168.2.1 any eq smtp – инструкция разрешает TCP-пакеты с адресом отправителя 192.168.2.1, номером порта отправителя 25 (smtp), и любым IP-адресом получателя.

Компания Cisco также разработала рекомендации для применения списков управления доступом, ниже приведены некоторые из них:

размещайте стандартные ACL как можно ближе к получателю, т.к они часто уничтожают важные пакеты, нужные другим сетям;

размещайте расширенные ACL как можно ближе к отправителю пакета, чтобы сразу же отбросить определенные типы пакетов;

размещайте более специфичные (т.е. узкие) правила проверки ближе к началу списка управления доступом;

прежде чем вносить изменения в ACL, удалите его в интерфейсе, в котором он был задан (с помощью команды no ip access-group);

создавайте списки управления доступом с помощью текстового редактора, а затем вносите готовые команды конфигурации на устройство с использованием копирования и вставки.

2 Практическая часть

В качестве исходной будет использоваться сеть филиала предприятия, состоящая из четырех отделов. Для начала проверьте связь различных устройств с помощью команды ping. Echo-запросы должны успешно выполняться между всеми устройствами в сети. Это важно, потому что далее с помощью списков управления доступом связь между некоторыми устройствами будет ограничиваться. Будем использовать схему приведенную на рисунке (2.1).

Рисунок 2.1 – Исходная сеть предприятия

Для создания простейшего стандартного списка управления доступом последовательно выполните следующие действия:

1. Предположим, что нужно ограничить доступ ПК1 к Сервер1. Необходимо принять решение о том, на каком интерфейсе оптимальнее всего расположить список управления доступом, а также в каком направлении будет осуществляться фильтрация трафика. Следуя рекомендациям Cisco, стандартные ACL лучше всего располагать как можно ближе к получателю, то есть на сегменте от коммутатора третьего уровня до Коммутатор2. Списки доступа можно располагать как на физических интерфейсах, так и на логических, в данном случае будет использоваться логический интерфейс VLAN4. Оптимальнее всего будет фильтровать исходящий трафик на этом интерфейсе, чтобы снизить нагрузку на Сервер1. Зайдите в CLI Многоуровневого коммутатора0, а затем в режим конфигурации интерфейса Vlan 4 (conf t int vlan 4). Здесь необходимо указать список управления доступа и направление фильтрации. Введите команду ip access-group 1 out. Номер 1 указывает на будущий список доступа, а ключевое слово out определяет, что фильтроваться будет исходящий трафик.

Теперь нужно создать сам список управления доступа. Создание всех ACL происходит из режима глобальной конфигурации. Введите команду access-list 1 deny host 192.168.0.2 (возможно у вас будет другой IP-адрес на ПК1, тогда введите его). Теперь все пакеты, исходящие из интерфейса VLAN4 будут отбрасываться, если IP-адрес отправителя будет равен 192.168.0.2. Однако на этом настройка не окончена, потому что все остальные пакеты также будут отбрасываться из-за неявной инструкции deny ip any any которая расположена в конце каждого списка управления доступом.

Введите команду access-list 1 permit any. Это позволит пропускать весь остальной трафик, не удовлетворяющий первой инструкции созданного ACL. Обратите внимание, что инструкции для списка доступа должны быть введены именно в таком порядке, иначе трафик от ПК1 все равно будет проходить до Сервер1, т.к он удовлетворяет инструкции access-list 1 permit any.

Проверьте работу списка управления доступом. Попробуйте создать echo-запрос от ПК1 до Сервер1. Он должен заканчиваться неудачей.

Созданный стандартный список доступа обладает явным недостатком – он фильтрует трафик только от одного узла-отправителя. А что если необходимо заблокировать трафик от нескольких узлов? Очевидно, что писать множество инструкций не самый лучший вариант. Вместо этого можно написать одну инструкцию, которая будет фильтровать трафик от множества узлов, например, от всей подсети, в которой состоит ПК1. Для этого в списке управления доступом необходимо указать IP-адрес подсети и инвертированную маску. Рассмотрим пример создания такого списка:

2. Удалите ранее созданный ACL с помощью команды no access-list 1, также в режиме конфигурации интерфейса VLAN4 удалите указание на этот список командой no ip access-group 1 out.

Не выходя из конфигурации интерфейса VLAN4, введите указание на новый список командой ip access-group Test-access out. В этой команде «Test-access» является именем списка управления доступом. Использование именованных списков вместо нумерованных – это «новый» синтаксис для обозначения ACL.

В режиме конфигурации введите команду ip access-list standard Test-access. Коммутатор должен перейти в режим конфигурации списка управления доступом с именем «Test-access». На это указывает надпись «(config-std-nacl)» после имени устройства в CLI.

Теперь необходимо последовательно ввести инструкции для созданного ACL. Чтобы выполнялась фильтрация трафика от всей подсети, в которой состоит ПК1, необходимо указать IP-адрес этой подсети

(192.168.0.0), а также инвертированную маску, которую необходимо вычислить с помощью вычитания стандартной маски подсети из маски 255.255.255.255. Каждый октет маски вычитается отдельно, поэтому если стандартная маска подсети равна 255.255.255.224, то инвертированная маска будет равна 0.0.0.31. Итоговая инструкция будет выглядеть следующим образом: deny ip 192.168.0.0 0.0.0.31.

Вторая инструкция будет разрешать весь трафик, который не удовлетворяет условию первой инструкции – permit any.

Проверьте работу созданного списка управления доступом – узел ПК3, который находится с ПК1 в одной подсети теперь не должен иметь доступа к Сервер1.

Побочным эффектом от списка доступа с такой конфигурацией является невозможность связи узлов ПК1 и ПК3 с Сервером0, поскольку он находится в той же подсети, что и Сервер1, а значит трафик у обоих серверов обрабатывается логическим интерфейсом VLAN4.

Для того, чтобы ограничить связь ПК1 и ПК3 только с Сервер1 необходимо использовать расширенные списки управления доступом. Однако, чтобы продемонстрировать полный функционал таких списков, задание следует усложнить. Предположим, что требуется ограничить доступ двум подсетям (с которыми ассоциированы VLAN2 и VLAN3) к Сервер1 по любому другому протоколу, кроме FTP (чтобы оставить возможность пользоваться файловым сервером). Исходя из рекомендаций Cisco по использованию списков управления доступом, расширенные ACL следует размещать как можно ближе к отправителю, это означает, что список следует установить на интерфейсах VLAN2 и VLAN3 с фильтрацией на входящий трафик. Следует просчитать инвертированную маску подсети таким образом, чтобы она покрывала диапазоны IP-адресов сразу двух подсетей. Для этого сначала возьмем обычную маску подсети 255.255.255.192, с помощью которой покрывается диапазон из 64 IP-адресов (192.168.0.0 – 192.168.0.64), а затем вычтем ее из маски 255.255.255.255. Итоговая инвертированная маска будет равна 0.0.0.63. Далее следует составить инструкции для будущего списка управления доступом, помещая самые узкие правила проверок в начало, а самые широкие – в конец. Ниже приведены эти инструкции в том порядке, в котором они должны быть в итоговом ACL:

permit tcp 192.168.0.0 0.0.0.63 host 192.168.0.82 eq ftp - лишнее

deny ip 192.168.0.0 0.0.0.63 host 192.168.0.82

Первая инструкция разрешает проходить TCP-пакетам с IP-адресом отправителя из подсети 192.168.0.0 и маской 255.255.255.192, IP-адресом получателя 192.168.0.82, и портом получателя 21. Вторая инструкция блокирует весь остальной трафик из этой подсети, если он направлен к узлу с IP-адресом 192.168.0.82. Предварительный список управления доступом создан, теперь необходимо реализовать его на Многоуровневый коммутатор0:

3. Удалите предыдущий ACL (no ip access-list standard Test-access) и указание на него (no ip access-group Test-access out).

Зайдите в режим конфигурации и создайте расширенный ACL с помощью команды ip access-list extended ftp. Здесь ftp – имя списка, а ключевое слово extended указывает на то, что созданный список управления доступом – расширенный.

Последовательно введите все инструкции, описанные ранее:

Рисунок- 2.2 – Создание расширенного списка управления доступом

Перейдите в режим конфигурации логического интерфейса VLAN2, затем введите команду ip access-group ftp in. Повторите эту же команду для логического интерфейса VLAN 3.

Проверьте работу созданного списка управления доступом. С любых узлов, входящих в рассматриваемые подсети, отправьте echo-запросы до Сервер1, они должны заканчиваться неудачей. Также проверьте можно ли обратиться к Сервер1 по протоколу ftp, для этого воспользуйтесь кнопкой «Добавить сложный PDU», а затем укажите применение (FTP) и адрес назначения (192.168.0.82), а также порт источника (21). Такой PDU должен успешно доходить.

До сих пор, настройка всех устройств в Cisco Packet Tracer происходила через встроенную вкладку CLI, однако реальные устройства Cisco настраиваются напрямую через консольный порт, который есть на каждом коммутаторе или маршрутизаторе, или виртуально через удаленный доступ. Если для того, чтобы настроить устройство через консольный порт, необходимо находиться рядом с устройством, то для удаленного доступа настройка устройства может осуществляться с любого узла в сети, поэтому важно предотвратить нежелательные подключения с помощью списков управления доступом, тем самым обеспечив дополнительную безопасность сети. Далее будет рассмотрен процесс создания удаленного подключения к Многоуровневый коммутатор0 с помощью протокола Telnet:

4. Сначала необходимо создать учетную запись пользователя с паролем и уровнем привилегий. Зайдите в режим конфигурации и введите команду username admin privilege 15 password cisco. Будет создана учетная запись с именем пользователя admin, уровнем привилегий 15 (максимальные), и паролем cisco.

Введите команду line vty 0 4. Устройство перейдет в режим конфигурации виртуальной терминальной линии (сокращ. vty) под номером 0 4 (это значение по умолчанию).

Введите команду transport input telnet. Теперь устройство будет готово к использованию протокола Telnet для входящих подключений.

Необходимо включить аутентификацию через имя пользователя и пароль с помощью команды login local. Теперь все удаленные подключения будут защищены паролем.

Проверьте удаленное подключение. Зайдите в консоль на узле ПК5 и введите команду telnet 192.168.0.65. Должен появиться запрос на имя пользователя и пароль. Пройдите аутентификацию с помощью имени пользователя admin и пароля cisco.

Рисунок 2.3 – Удаленное подключение по протоколу Telnet

С помощью списков управления доступом возможно ограничить количество узлов, с которых будет возможно удаленное подключение. Для этого необходимо создать расширенный ACL с несколькими инструкциями. Предположим, что подсеть, в которой состоят ПК5 и ПК6 – это подсеть администраторов, для них будет доступно удаленное подключение по Telnet, для всех остальных это подключение будет запрещено.

Инвертированная маска для этой подсети будет равна 0.0.0.15 (обычная маска – 255.255.255.240), список управления доступом будет включен на всех логических интерфейсах Многоуровневого коммутатора0, фильтрация будет осуществляться на входящий трафик. Список инструкций будет выглядеть следующим образом:

permit tcp 192.168.0.64 0.0.0.15 host 192.168.0.65 eq telnet

deny tcp 192.168.0.0 0.0.0.255 any eq telnet

permit ip any any

Далее будет описан процесс создания расширенного списка управления доступа с заданной конфигурацией:

5. Зайдите в режим конфигурации и наберите команду ip access-list extended Telnet.

Последовательно введите все инструкции, описанные ранее:

Рисунок 2.4 – Создание расширенного списка управления доступом

Перейдите в режим конфигурации диапазона интерфейсов VLAN 2 – 6 с помощью команды interface range vlan 2-6.

Введите команду ip access-group Telnet in, указывая всем логическим интерфейсам на ACL с именем «Telnet».

Проверьте удаленное подключение по протоколу Telnet. Узлы ПК5 и ПК6 должны успешно подключаться и проходить аутентификацию, любые другие узлы должны выдавать ошибку:

Рисунок 2.5 – Ошибка «хост не отвечает»

Заключение

Навыки работы со стандартными и расширенными списками управления доступом позволяют сетевым инженерами обеспечить первоначальную защиту сети от злоумышленников, а также обеспечивают фильтрацию трафика, оптимизируя тем самым загрузку сети. Также списки управления доступом могут применяться для:

- фильтрации обновлений маршрутизации и установки приоритета пакетов (QoS);
- построения тоннелей виртуальной частной сети (VPN). ACL определяют, какой трафик следует шифровать и пропускать через VPN-туннель;
- разграничения доступа к оборудованию (Установка паролей и ограничений);
- настройки конфигурации службы трансляции сетевых адресов (NAT);
- для использования Policy-based Routing (PBR) – маршрутизации на основе некоторых политик, установленных администратором.

Владение рефлексивными, динамическими и временными списками управления доступом еще сильнее расширяет область применения ACL, позволяя решать сложные узконаправленные задачи на предприятиях, такие как адаптация к внешним угрозам, автоматическое изменение уровня доступа для устройств и пользователей в зависимости от топологии сети, а также смена привилегий в зависимости от времени суток.

Задания

1. Запретить доступ к серверу всем узлам в сети, кроме тех, которые находятся в отделе администраторов, сохранив возможность обращаться только по протоколу HTTP.

2. Настроить на коммутаторе третьего уровня удаленные подключения по Telnet, ограничить такие подключения всем, кроме администраторов.

3. Запретить доступ узлам из отдела 1 в отдел 3 и 4 и наоборот.

4. Запретить доступ узлам из отдела 2 в отдел 4 по всем портам, чей номер больше 21.

5. Выделить один узел из отдела 1, которому будет дана возможность обращаться к узлам из отдела 2, всем остальным запретить доступ.

6. Запретить доступ к серверу всем узлам из отдела производства, остальным отделам разрешить обращаться к серверу только по портам 1541 и 1560-1591 (диапазон).

7. Разрешить общаться узлам из двух отделов только по следующим протоколам – TFPT, FTP, HTTP.

8. Настроить на коммутаторе третьего уровня удаленные подключения по Telnet, ограничить такие подключения всем, кроме двух выбранных администраторов, каждый из которых должен находиться в разных зданиях.

Контрольные вопросы

1. Что такое ACL?
2. Какой адрес является критерием для разрешения/запрещения пакета?
3. Где применяются ACL?
4. Как задать элемент ACL и что такое инверсная маска?
5. Как роутер обрабатывает элементы ACL?
6. Какой элемент всегда неявно присутствует в ACL?
7. Как ACL применить к интерфейсу и затем его отменить?
8. Чем отличается входной ACL от выходного?
9. Где в сети рекомендуется размещать ACL?

Лабораторная работа №6-7. Преобразование сетевых адресов NAT.

Цель работы:

1. Изучение принципа работы и конфигурации NAT.

2. Получить навыки по конфигурированию NAT и PAT.

1 Теоретическая часть

Network address translation (NAT - перенос сетевых адресов) создан для упрощения и сокрытия IP адресации. Трансляция порт-адрес (англ. Port address translation, PAT) – технология трансляции сетевого адреса в зависимости от TCP/UDP-порта получателя. Является частным случаем NAT. NAT эффективно скрывает внутреннюю сеть от внешнего мира. Поэтому он обеспечивает дополнительную безопасность. Одна из основных функций NAT это статическая трансляция портов (Port Address Translation, PAT), которая называется ”overload” в конфигурациях Cisco.. NAT позволяет представить внешнему миру внутреннюю структуру IP адресации предприятия иначе, чем она на самом деле выглядит. Это разрешает организации соединяться с Интернетом, не имея внутри себя глобальной уникальной IP адресации. Это даёт возможность выхода в Интернет для корпоративных внутренних IP сетей с внутренними IP адресами (intranet), которые глобально неуникальны и поэтому не могут маршрутизироваться в Интернете. NAT

применяется также для связи территориально распределённых подразделений организации через Интернет. Мировым сообществом для Интранет адресации выделены следующие диапазоны адресов.

Class A: 10.0.0.0-10.255.255.255

Class B: 172.16.0.0-172.16.255.255

Class C: 192.168.1-192.168.255.255

NAT переводит внутренний IP адрес из внутреннего адресного пространства в IP адрес во внешнем адресном пространстве. Когда NAT получает пакет из intranet, он изменяет в нём адрес источника, пересчитывает контрольную сумму и отправляет его в Интернет. NAT преобразует и отображает адреса из одной области в другую. Это обеспечивает прозрачную маршрутизацию от узла к узлу. В NAT существует несколько способов трансляции адресов, используемых в различных частных случаях. Cisco использует для NAT специфическую терминологию для узлов в intranet и интернет как до, так и после преобразования адресов:

- Внутренний (inside) адрес- адрес, используемый в организации. Разные организации могут иметь одинаковые внутренние адреса.
- Внешний адрес (outside)- адрес, определённый где-либо вне данной организации. Внешний адрес иной организации может совпадать с внутренним адресом данной организации.
- Глобальный адрес- зарегистрированный и законный адрес IP, который может проходить через Интернет.
- Локальный адрес- адрес IP, используемый внутренне в Intranet. Эти адреса не пересекают Интернет адреса и поэтому рассматриваются как локальные.
- Внутренний локальный адрес (inside local)- адрес, используемый в организации, не пересекающие Интернет адреса.
- Внутренний глобальный адрес (inside global). Адрес, используемый в организации, являющийся Интернет адресом.
- Внешний локальный адрес (outside local)- адрес, определённый где-либо вне данной организации, не являющийся Интернет адресом.
- Внешний глобальный адрес (outside global)- адрес, определённый где-либо вне данной организации, являющийся Интернет адресом.

Симулятор всегда показывает, что Внешний локальный адрес (Outside Local) всегда равен внешнему глобальному адресу (outside global).

При отправке пакетов от интерфейса внутреннего хоста NAT заменяет в нём адрес источника на некоторый глобальный адрес. При приёме ответного пакета NAT заменяет в нём глобальный адрес приёмника (адрес внешнего интерфейса локального маршрутизатора) на адрес интерфейса внутреннего хоста. Для такой замены маршрутизатор поддерживает специальные таблицы преобразований адресов, которые постоянно обновляются. Различают три способа преобразования адресов: статический, динамический и перегрузка (overload). При статическом NAT в явном виде с помощью команд IOS задаются пары внутренний_адрес - глобальный _адрес.

При динамическом преобразовании глобальные адреса берутся из определённого пула внешних адресов. При перегрузке все внутренние адреса, подлежащие преобразованию, заменяются на единственный глобальный адрес внешнего интерфейса маршрутизатора.

Для конфигурирования NAT следует определить на маршрутизаторе внутренние и внешние сети с помощью команд ip nat inside | outside. Эти команда определяется на уровне интерфейсов, то есть в контексте команды interface. Дополнительные команды зависят от используемого типа NAT. Это либо задание статического NAT, либо определение пула внешних адресов либо задание команды для перегрузки. Как правило, следует также задать список управления доступом ACL для определения внутреннего трафика, который будет преобразовываться. Сам по себе ACL не осуществляет никакого NAT преобразования.

Остановимся дополнительно на перегрузке, которую, как правило называют PAT (Port Address Translation - преобразование адресов с помощью портов). PAT разрешает нескольким внутренним хостам использовать один глобальный адрес. Один из вариантов реализации PAT базируется на использовании последовательности свободных TCP и UDP портов и состоит в следующем.

Служба NAT находится на маршрутизаторе M с внутренним глобальным адресом X. Пусть имеется пакет П от внутреннего локального адреса Yi и порта Pi к внешнему адресу G и порту p. Пакет проходит через маршрутизаторM. NAT заменяет в нём адрес Yi источника и порт источника Pi внутреннего хоста на уникальную пару X:Pinew, где Pinew– очередной свободный номер порта. Строка (Yi:Pi , X: Pinew, G:p) заносится в таблицу NAT маршрутизатора M. Ответный пакет в поле адрес приёмника будет содержать X, а в поле порт приёмника – Pinew. В поле адрес:порт источника будет G:p . Маршрутизатор M по значениям X, Pinew, G, p находит в своей NAT таблице строку (Yi:Pi , X: Pinew, G:p) и заменяет в пакете адрес приёмника X на Yi, а порт назначения Pinew на Pi. Ответный пакет придёт по нужному адресу Yi с нужным номером порта назначения Pi. Порт Pinew возвращается в список свободных портов.

Процесс NAT прозрачен для внутренних адресов. Так хост с внутренним адресом Yi, отправивший пакет во внешний мир и получивший ответ «не догадывается», что пакет прошел NAT преобразование на маршрутизаторе как при отправке так и при приёме. Внутреннему хосту представляется, что он имеет непосредственный выход во внешний мир.

Рисунок 1.1 – Сеть NAT

Вот так конфигурируется классический NAT на маршрутизаторе Cisco.

1.1 Типы NAT

1.1.1 Статический

В этом случае один внутренний адрес преобразуется в один внешний. И при этом все запросы, приходящие на внешний адрес будут транслироваться на внутренний. Словно бы этот хост и является обладателем этого белого IP-адреса.

Настраивается следующей командой:

Router (config)# ip nat inside source static 172.16.6.5 198.51.100.2

Такой подход бывает полезным, когда у вас есть сервер внутри вашей сети, к которому необходим полный доступ извне. Разумеется, этот вариант вы не можете использовать, если хотите триста хостов выпустить в Интернет через один адрес. Такой вариант NAT’а никак не поможет сохранить белые IP-адреса, но тем не менее он бывает полезен.

Рисунок 1.2 – Сеть статистической NAT

1.1.2 Динамический

У вас есть пул белых адресов, например, провайдер выделил вам сеть 198.51.100.0/28 с 16-ю адресами. Два из них (первый и последний) – адрес сети и широковещательный, ещё два адреса назначаются на оборудование для обеспечения маршрутизации. 12 оставшихся адресов вы можете использовать для NAT'а и выпускать через них своих пользователей.

Ситуация похожа на статический NAT – один приватный адрес транслируется на один внешний, – но теперь внешний не чётко зафиксирован, а будет выбираться динамически из заданного диапазона.

Настраивается он так:

Router(config)#ip nat pool lol_pool 198.51.100.3 198.51.103.14

Задали пул (диапазон) публичных адресов, из которого будет выбираться адрес для натирования

Router(config)#access-list 100 permit ip 172.16.6.0 0.0.0.255 any

Задаём список доступа, который пропускает все пакеты с адресом источника 172.16.6.x, где x варьируется 0-255.

Router(config)#ip nat inside source list 100 pool lol_pool

Этой командой мы стыкуем созданный ACL и пул. Этот вариант тоже не универсальный, своих 300 пользователей вы так же не сможете выпустить всех в Интернет, если у вас нет 300 внешних адресов. Как только белые адреса исчерпаются, никто новый уже не сможет получить доступ в Интернет. При этом те пользователи, что уже успели отхватить себе внешний адрес, будут работать. Скинуть все текущие трансляции и освободить внешний адреса вам поможет команда clear ip nat translation * Помимо динамического выделения внешних адресов, этот динамически NAT отличается от статического тем, что без отдельной настройки проброса портов уже невозможно внешнее соединение на один из адресов пула.

1.2 Port Address Translation (PAT)

Следующий тип имеет несколько названий: NAT Overload, Port Address Translation (PAT), IP Masquerading, Many-to-One NAT. Вся внутренняя сеть построена на протоколе IPv6. Тем не менее провайдер, к которому подключена данная компания даже не слышал про существование IPv6, поэтому придется использовать на пограничном маршрутизаторе NAT-PT (Protocol Translation). Данная технология, как это понятно из названия, позволяет осуществлять трансляцию из одного сетевого протокола в другой, и, соответственно, общаться хостам, поддерживающим только IPv6 или только IPv4, друг с другом.

Рисунок 1.3 – Сеть PAT

PAT-значит, через один внешний адрес выходит в мир много приватных. Это позволяет решить проблему с нехваткой внешних адресов и выпустить в мир всех желающих. Тут надо бы дать пояснение, как это работает. Как два приватных адреса транслируются в один можно представить, но как маршрутизатор понимает кому нужно переслать пакет, вернувшийся из Интернета на этот адрес? Предположим, что от двух хостов из внутренней сети приходят пакеты на натирующее устройство. Оба с запросом к WEB-серверу 192.0.2.2.

Данные от хостов выглядят так:

Таблица 1.1 – Данные от хостов

Адрес отправителя	Порт отправителя	Адрес получателя	Порт получателя
172.16.6.5	23761	192.0.2.2	80

172.16.4.5	39800	192.0.2.2	80

Маршрутизатор расчехляет IP-пакет от первого хоста, извлекает из него TCP-сегмент, распечатывает его и узнаёт, с какого порта устанавливается соединение. У него есть внешний адрес 198.51.100.2, на который будет меняться адрес из внутренней сети.

Далее он выбирает свободный порт, например, 11874. И что он делает дальше? Все данные уровня приложений он упаковывает в новый TCP сегмент, где в качестве порта назначения по-прежнему остаётся 80 (именно на него ждёт коннектов WEB-сервер), а порт отправителя меняется с 23761 на 11874. Этот TCP-сегмент инкапсулируется в новый IP-пакет, где меняется IP-адрес отправителя с 172.16.6.5 на 198.51.100.2.

То же самое происходит для пакета от второго хоста, только выбирается следующий свободный порт, например 11875. “Свободный” означает, что он ещё не занят другими такими соединениями.

Данные, которые отправляются в интернет, теперь буду выглядеть так.

Таблица 1.2 – Данные, отправленные в интернет

Адрес отправителя	Порт отправителя	Адрес получателя	Порт получателя
198.51.100.2	11874	192.0.2.2	80
198.51.100.2	11875	192.0.2.2	80

В свою NAT-таблицу он заносит данные отправителей и получателей

Таблица 1.3 – Адреса отправителей и получателей

Лок. адрес отправителя	Лок.порт отправителя	Глоб. адрес отправителя	Глоб. порт отправителя	Адрес получателя	Порт получателя
172.16.6.5	23761	198.51.100.2	11874	192.0.2.2	80
172.16.4.5	39800	198.51.100.2	11875	192.0.2.2	80

Для WEB-сервера – это два совершенно разных запроса, которые он должен обработать каждый индивидуально. После этого он отсылает ответ, который выглядит так:

Таблица 1.4 – Адреса отправителя и получателя

Адрес отправителя	Порт отправителя	Адрес получателя	Порт получателя
192.0.2.2	80	198.51.100.2	11874
192.0.2.2	80	198.51.100.2	11875

Когда один из этих пакетов доходит до нашего маршрутизатора, тот сопоставляет данные в этом пакете со своими записями в NAT-таблице. Если совпадение найдено, происходит обратная процедура – пакету и TCP сегменту возвращаются его изначальные параметры только в качестве назначения:

Таблица 1.5 – Адреса получателя и отправителя

Адрес отправителя	Порт отправителя	Адрес получателя	Порт получателя
192.0.2.2	80	172.16.6.5	23761

192.0.2.2	80	172.16.4.5	39800

И теперь пакеты доставляется по внутренней сети компьютерам-инициаторам, которым и невдомёк даже, что где-то с их данными так жёстко обошлись на границе

Каждое ваше обращение – это отдельное соединение. То есть попытались вы открыть WEB-страницу – это протокол HTTP, использующий порт 80. Для этого ваш компьютер должен установить TCP-сессию с удалённым сервером. Такая сессия (TCP или UDP) определяется двумя сокетами: локальный IP-адрес: локальный порт и удалённый IP-адрес: удалённый порт. В обычной ситуации у вас устанавливается одно соединение компьютер-сервер, в случае же NATа соединения будет как бы два:, маршрутизатор-сервер и компьютер думает, что у него есть сессия компьютер-сервер. Настройка отличается совершенно незначительно:

добавочным словом overload:

Router (config) # access-list 101 permit 172.16.4.0 0.0.0.255

Router (config) # ip nat inside source list 101 interface fa0/1 overload

При этом, разумеется, сохраняется возможность настроить пул адресов:

Router (config) # ip nat pool lol_pool 198.51.100.2 198.51.103.14

Router (config) # access-list 100 permit 172.16.6.0 0.0.0.255

Router (config) # ip nat inside source list 100 pool lol_pool overload

1.3 Перенаправление портов

Иначе говорят ещё проброс портов или mapping.

Когда мы только начали говорить про NAT, трансляция у нас была один-в-один и все запросы, приходящие извне автоматически перенаправлялись на внутренний хост. Таким образом можно было бы выставить сервер наружу в Интернет. Но если у вас нет такой возможности – вы ограничены в белых адресах, или не хотите выставлять всем пучком портов его наружу, что делать?

Вы можете указать, что все запросы, приходящие на конкретный белый адрес и конкретный порт маршрутизатора, должны быть перенаправлены на нужный порт нужного внутреннего адреса.

Router (config) # ip nat inside source static tcp 172.16.0.2 80 198.51.100.2 80extendable

Применение данной команды означает, что TCP-запрос, пришедший из интернета на адрес 198.51.100.2 по порту 80, будет перенаправлен на внутренний адрес 172.16.0.2 на тот же 80-й порт. Разумеется, вы можете пробрасывать и UDP и делать перенаправление с одного порта на другой. Это, например, может оказаться полезным, если у вас есть два компьютера, к которым нужен доступ по RDP извне. RDP использует порт 3389. Один и тот же порт вы не можете пробросить на разные хосты (при использовании одного внешнего адреса). Поэтому вы можете сделать так:

Router (config) # ip nat inside source static tcp 172.16.6.61 3389 198.51.100.23389

Router (config) # ip nat inside source static tcp 172.16.6.66 3389 198.51.100.2 3398

Тогда, чтобы попасть на компьютер 172.16.6.61 вы запускаете RDP-сессию на порт 198.51.100.2:3389, а на 172.16.6.66 – 198.51.100.2:3398. Маршрутизатор сам раскидает всё, куда надо.

Эта команда – частный случай самой первой: ip nat inside source static 172.16.6.66 198.51.100.2. Только в этом случае речь идёт о пробросе всего трафика, а в наших примерах – конкретных портов протокола TCP.

1.4 Плюсы и минусы NAT

1.4.1 Положительные стороны NAT

1. NAT позволяет сэкономить публичные IP-адреса. Собственно для этого он и был создан. Через один адрес, теоретически можно выпустить больше 65000 серых адресов (по количеству портов).

2. PAT и динамический NAT является в какой-то степени файрволом, препятствуя внешним соединениям доходить до конечных компьютеров, на которых может не оказаться своего файрвола и антивируса. Дело в том, что если извне на натирующее устройство приходит пакет, который тут не ожидается или не разрешён, он просто отбрасывается. Чтобы пакет был пропущен и обработан, должны выполниться условия:

2.1. В NAT-таблице должна быть запись для этого внешнего адреса, указанного как адрес отправителя в пакете.

2.2. Порт отправителя в пакете должен совпадать с портом для этого белого адреса в записи.

2.3. Порт назначения в пакете, совпадает с портом в записи.

2.4. Настроен проброс портов.

3. NAT скрывает от посторонних глаз внутреннюю структуру вашей сети – при трассировке маршрута извне вы не увидите ничего далее натирующего устройства.

1.4.2 Есть у NAT'а и минусы.

1. Некоторые протоколы не могут работать через NAT.

2. С одного адреса идёт много запросов на один сервер.

3. Нагрузка на процессор и оперативную память. Поскольку объём работы довольно велик по сравнению с простой маршрутизацией.

Одно из возможных решений – вынести функцию NAT на отдельный ПК либо на специализированное устройство, например Cisco ASA.

2 Практическая часть

Подключение к Интернету будет организовано через существующий линк, который предоставляет провайдер. Он уходит в сеть провайдера. Напоминаем, что всё в этом облаке – это абстрактная сеть, которая на деле может состоять из десятков маршрутизаторов и сотен коммутаторов. Но нам нужно нечто управляемое и предсказуемое, поэтому водружаем сюда ещё маршрутизатор. С одной стороны в него линк из коммутатора, с другой сервера в Интернете.

Задание:

1)Сеть управления не имеет доступа в интернет вообще

2) Хосты из сети ПТО имеют доступ только к профильным сайтам, например, Linkmeup.ru

3)Из бухгалтерии нужно вырубить окно в мир клиент-банков.

4) ФЭО не выпускать никуда, за исключением финансового директора

5) В сети Other наш компьютер и компьютер админа – им дадим полный доступ в интернет. Всем остальным можно открывать по письменному запросу.

6) Не забудем про филиалы в Питере и в Кемерово. Для простоты настроим полный доступ для эникиев из этих подсетей.

7) С серверами отдельная песня. Для них мы настроим перенаправление портов. Всё, что нам нужно:

а)WEB-сервер должен быть доступен по 80-му порту

б)Почтовый сервер по 25-му и 110-му

в)Файловый сервер доступен из мира по FTP.

8) Компьютеры админа и наш должны быть доступны из Интернета по RDP. Вообще-то это неправильный путь – для удалённого подключения нужно использовать VPN-подключение и уже будучи в локальной сети использовать RDP, но это тема отдельной совсем другой статьи.

Рисунок 2.1 – Сеть управления

Для такого подключения мы поднимем ещё один Vlan на msk-arbat-gw1. Его номер, разумеется, согласуется с провайдером. Пусть это будет VLAN 6. Предположим, провайдер предоставляет нам подсеть 198.51.100.0/28. Первые два адреса используются для организации линка (198.51.100.1 и 198.51.100.2), а оставшиеся мы используем, как пул для NAT'а. Впрочем, никто совершенно нам не мешает использовать и адрес 198.51.100.2 для пула. Так и сделаем: пул: 198.51.100.2-198.51.100.14Для простоты предположим, что публичные сервера у нас находятся в одной подсети:192.0.2.0/24.

Поскольку у нас только один маршрутизатор в сети провайдера, и все сети подключены непосредственно к нему, то необходимости настраивать маршрутизацию.

А вот наш msk-arbat-gw1 должен знать куда отправлять пакеты в Интернет, поэтому нам нужен маршрут по умолчанию:

msk-arbat-gw1(config)# ip route 0.0.0.0 0.0.0.0 198.51.100.1

Теперь по порядку

1. Настроим пул адресов

msk-arbat-gw1(config)# ip nat pool main_pool 198.51.100.2 198.51.100.14 netmask255.255.255.240

2. Собираем ACL:

msk-arbat-gw1(config)# ip access-list extended nat-inet

2.1. Сеть управления не имеет доступа в интернет вообще

Готово

2.2. Хосты из сети ПТО

Имеют доступ только к профильным сайтам, например, Linkmeup.ru

msk-arbat-gw1(config-ext-nacl)# permit tcp 172.16.3.0 0.0.0.255 host 192.0.2.2 eq 80

2.3.Бухгалтерия

Даём доступ всем хостам на оба сервера

msk-arbat-gw1(config-ext-nacl)# permit ip 172.16.5.0 0.0.0.255 host 192.0.2.3

msk-arbat-gw1(config-ext-nacl)# permit ip 172.16.5.0 0.0.0.255 host 192.0.2.4

2.4. ФЭО

Даём разрешение только финансовому директору – это только один хост. msk-arbat-gw1(config-ext-nacl)# permit ip host 172.16.4.123 any

2.5. Other

Наши компьютеры с полным доступом

msk-arbat-gw1(config-ext-nacl)# permit ip host 172.16.6.61 any msk-arbat-gw1(config-ext-nacl)# permit ip host 172.16.6.66 any

2.6. Филиалы в Санкт-Петербурге и Кемерово

Пусть адреса эникиев будут одинаковыми: 172.16.x.222

msk-arbat-gw1(config-ext-nacl)# permit ip host 172.16.16.222 any msk-arbat-gw1(config-ext-nacl)# permit ip host 172.16.17.222 any msk-arbat-gw1(config-ext-nacl)# permit ip host 172.16.24.222 any

Вот так выглядит сейчас ACL полностью:

ip access-list extended nat-inet

remark PTO

permit tcp 172.16.3.0 0.0.0.255 host 192.0.2.2 eq www

remark ACCOUNTING

permit ip 172.16.5.0 0.0.0.255 host 192.0.2.3

permit ip 172.16.5.0 0.0.0.255 host 192.0.2.4

remark FEO

permit ip host 172.16.4.123 any

remark IAM

permit ip host 172.16.6.61 any

remark ADMIN

permit ip host 172.16.6.66 any

remark SPB_VSL_ISLAND

permit ip host 172.16.16.222 any

remark SPB_OZERKI

permit ip host 172.16.17.222 any

remark KMR

permit ip host 172.16.24.222 any

Запускаем:

msk-arbat-gw1(config)# ip nat inside source list nat-inet pool main_pool overload

Полная настройка интерфейсов:

На внешнем интерфейсе нужно дать команду ip nat outside На внутреннем: ip nat inside msk-arbat-gw1(config)# int fa0/0.101

msk-arbat-gw1(config-subif)# ip nat inside

msk-arbat-gw1(config)# int fa0/0.102

msk-arbat-gw1(config-subif)# ip nat inside

msk-arbat-gw1(config)# int fa0/0.103

msk-arbat-gw1(config-subif)# ip nat inside

msk-arbat-gw1(config)# int fa0/0.104

msk-arbat-gw1(config-subif)# ip nat inside

msk-arbat-gw1(config)# int fa0/1.6

msk-arbat-gw1(config-subif)# ip nat outside

Это позволит маршрутизатору понять откуда ждать пакеты, которые нужно будет обработать и куда их потом слать.

Чтобы сервера в интернете были доступны по доменному имени, нам бы неплохо было обзавестись DNS-сервером в нашей сети:

Рисунок 2.2 – DNS-сервер

Рисунок 2.3 – DNS-сервер

Естественно, его нужно прописать на тех устройствах, с которых будем проверять доступ:

Рисунок 2.4 – Конфигурация

Show must go on!

С компьютера админа доступно всё:

Рисунок 2.5 – Командная строка

Рисунок 2.6 – Командная строка

Рисунок 2.7 – Рабочий стол

В сети ФЭО в мир выходит только 4.123 (финдиректор)

Рисунок 2.8 – Командная строка

Рисунок 2.9 – Командная строка

В бухгалтерии работают только сайты клиент-банков. Но, поскольку разрешение дано полностью на протокол IP, то их можно и пинговать:

Рисунок 2.10 – Командная строка

Рисунок 2.11 – Рабочий стол

7) Сервера

Тут нам нужно настроить проброс портов, чтобы к ним можно было обращаться из Интернета:

Рисунок 2.12 – Сервер

а) Веб-сервер

msk-arbat-gw1(config)# ip nat inside source static tcp 172.16.0.2 80 198.51.100.2 80

Сразу проверяем, например, мы можем это делать с тестового ПК с аресом 192.0.2.7. Сейчас ничего не заработает, потому что для сети серверов у нас не настроен интерфейс на msk-arbat-gw1:

msk-arbat-gw1(config)# int fa0/0.3

msk-arbat-gw1(config-subif)# ip nat inside А теперь:

Рисунок 2.13 – Веб-сервер

б) Файловый сервер msk-arbat-gw1(config)# ip nat inside source static tcp 172.16.0.3 20 198.51.100.3 20 msk-arbat-gw1(config)# ip nat inside source static tcp 172.16.0.3 21 198.51.100.3 21

Вот для этого в ACL Servers-out мы открывали также и 20-21-й порты для всех

Рисунок 2.14 – Командная строка

в) Почтовый сервер msk-arbat-gw1(config)# ip nat inside source static tcp 172.16.0.4 25 198.51.100.4 25 msk-arbat-gw1(config)# ip nat inside source static tcp 172.16.0.4 110 198.51.100.4 110

Проверить также не сложно. Следуйте инструкциям:

Сначала настраиваем почтовый сервер. Указываем домен и создаём двух пользователей.

Рисунок 2.15 – Настройка почтового сервера

Далее вносим домен в DNS. Этот шаг необязательный – можно к серверу обращаться и по IP, но почему бы и нет?

Рисунок 2.16 – Внесение домена в DNS

Настраиваем компьютер из нашей сети:

Рисунок 2.17 – Настройка компьютера из нашей сети

Из внешней:

Рисунок 2.18 – Настройка компьютера из внешней сети

Готовим письмо:

Рисунок 2.19 – Готовим письмо

На локальном хосте нажимаем Receive:

Рисунок 2.20 – Почтовый сервер

8) Доступ по RDP к компьютерам админа и нашему

msk-arbat-gw1(config)# ip nat inside source static tcp 172.16.6.61 3389 198.51.100.10 3389

msk-arbat-gw1(config)# ip nat inside source static tcp 172.16.6.66 3389 198.51.100.10 3398

3 Задания по вариантам:

1)Соберите схему как показано на рисунке 3.1.

2)Задайте каждому компьютеру IP-адрес и шлюз (возьмите индивидуальный IP-адрес и шлюз).

3)Настроить NAT на Router 1 и Router 2, чтобы компьютеры сети 1 пинговались с компьютерами сети 2.

ЛВС 1 - 192.168.10.0/24 ЛВС 2 - 172.16.0.0/28

В Интернете использовать любые белые IP адреса

4)Каждый вариант берет свои пулы адресов

Таблица 3.1 – Задание по вариантам

1 вариант	192.168.43.128/25 и 10.10.10.0/28
2 вариант	172.16.0.0/24 и 192.168.0.0/20
3 вариант	10.10.0.0/28 и 10.0.0.0/26
4 вариант	172.16.43.64/26 и 10.27.84.128/25

5 вариант	192.168.13.16/28 и 192.168.64.0/24
6 вариант	172.16.123.16/28 и 192.168.0.0/25
7 вариант	10.11.12.0/26 и 10.13.14.0/26
8 вариант	172.16.73.128/ и 25 10.1.2.4/30
9 вариант	10.20.30.64/26 и 10.20.40.0/28
10 вариант	192.168.0.0/28 и 172.16.8.16/28

Рисунок 3.1 – Сеть для задания

Контрольные вопросы

1. Какие задачи решает NAT?
2. Как связана проблема нехватки IP адресов и NAT?
3. Какие вы знаете диапазоны для Интранет адресации?
4. Что такое внутренний адрес?
5. Что такое внешний адрес?
6. Что такое глобальный адрес?
7. Что такое локальный адрес?
8. Что такое внутренний локальный адрес?
9. Что такое внутренний глобальный адрес?
10. Что такое внешний глобальный адрес?
11. Что такое внешний локальный адрес?
12. Назовите три способа преобразования адресов.

Лабораторная работа № 8

Изучение протокола динамической конфигурации узла DHCP

Цель: настроить и изучить протокол динамической конфигурации узла DHCP.

1 Теоретическая часть

DHCP (Dynamic Host Configuration Protocol/протокол динамической конфигурации узла) – это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. DCHP позволяет автоматически настраивать на клиенте следующие основные параметры:

1. IP адрес.
2. Основной шлюз.
3. Маска подсети.

4. DNS сервера.
5. Имя домена.

Это наиболее частое использование DHCP, но можно передавать и огромное количество других параметров. Например, можно передавать дополнительные маршруты, чтобы в разные сети компьютер ходил через разные шлюзы. Или, с помощью DHCP можно организовывать загрузку устройств по сети. В этом случае клиент получает помимо основных параметров, адрес TFTP сервера и имя файла на нём (я имею в виду имя файла – загрузчика ОС, которую необходимо загрузить по сети).

Когда клиент, например, обычный компьютер, запускается, ОС видит, что для некой сетевой карты стоит «Получить параметры по DHCP». Такой компьютер не имеет пока IP адреса и происходит следующая процедура получения:

1. Компьютер отправляет широковещательный запрос. При этом на втором уровне в фрейме стоит мак адрес отправителя – адрес компьютера, мак адрес получателя – ffff.ffff.ffff, а на третьем уровне – в пакете адрес отправителя отсутствует, адрес получателя стоит 255.255.255.255. Такое DHCP сообщение называется «DHCP discover».
2. Далее все устройства в сети получают это широковещательное сообщение. DHCP сервера (а их теоретически может быть несколько) отвечают клиенту. Сервер резервирует в своём пуле адресов какой-то адрес (если не было резервации до этого для данного mac-адреса клиента) и выделяет этот ip клиенту на какое-то время (lease time). Берутся другие настройки и всё вместе высылается. При этом в качестве адресов получателя используется уже новый выделенный клиентский ip и клиентский mac. Это называется «DHCP offer».
3. Клиент выбирает первый ближайший сервер (обычно он всего один) либо выбирается тот кто ответил первым. И отправляет со своего mac и нового ip-адреса на mac-адреса и ip-адреса уже конкретного сервера «DHCP request» – согласие с полученными параметрами.
4. Сервер резервирует за клиентом выделенный адрес на какое-то время (lease time). До этого момента адрес был выделен, но не зарезервирован. Теперь же он окончательно закреплён за клиентом. Сервер вносит так же строчку в свою ARP таблицу и высылает клиенту, сообщение, что он успешно зарегистрирован – «DCHP Acknowledge».
5. Клиент начинает работать.

Включение DHCP-сервера на маршрутизаторе Cisco

По умолчанию на маршрутизаторах Cisco включена функциональная возможность DHCP-сервера.

Если же она не активирована, то это возможно сделать командой:

```
Router(config)# service dhcp
```

Отключить данную функциональную возможность:

```
Router(config)# no service dhcp
```

Исключение IP-адресов

Исключить из пула адрес интерфейса маршрутизатора и DNS-сервера:

```
uter(config)# ip dhcp excluded-address 192.168.20.1
Router(config)# ip dhcp excluded-address 192.168.20.101
```

Ручное резервирование IP-адресов

Есть возможность вручную сопоставить определенный MAC-адрес с необходимым IP-адресом.

```
Router(config)# ip dhcp pool Test
Router(config-pool)#host 192.168.2.4 255.255.255.0
Router(config-pool)#client-identifier 0100.0476.106c.bc
Router(config-pool)#client-name Test
```

В данной конструкции необходимо указать:

1. адрес, который будет сопоставлен с физическим адресом: host address [mask | prefix-length]
2. физический адрес (идентификатор) сетевой карты: client-identifier unique-identifier
3. имя клиента: client-name name

То есть, для компьютера с MAC-адресом 00.04.76.10.6c.bc, который работает в среде Windows строчка client-identifier будет выглядеть как:

```
Router(config-pool)#client-identifier 0100.0476.106c.bc
```

Для компьютера с MAC-адресом 00.04.76.10.6c.bc который работает в среде UNIX строчка client-identifier будет выглядеть как:

```
Router(config-pool)#client-identifier 0000.0476.106c.bc
```

Пример:

```
Router(config)#ip dhcp pool glh-pc-5443
Router(config-pool)#host 10.84.130.10 255.255.255.0
Router(config-pool)#client-identifier 0100.2264.15c4.96
Router(config-pool)#client-name glh-pc-5443
Router(config-pool)#domain-name glh.sm.aval


Router(config)#ip dhcp pool glh-pc-5436
Router(config-pool)#host 10.84.130.15 255.255.255.0
Router(config-pool)#client-identifier 0100.2264.15c3.64
```

```
Router(config-pool)#client-name glh-pc-5436
Router(config-pool)#domain-name glh.sm.aval

Router(config)#ip dhcp pool glh-pc-2342
Router(config-pool)#host 10.84.130.42 255.255.255.0
Router(config-pool)#client-identifier 0100.0cf1.7ffd.03
Router(config-pool)#client-name glh-pc-2342
Router(config-pool)#domain-name glh.sm.aval

Router(config)#ip dhcp pool glh-pc-2325
Router(config-pool)#host 10.84.130.101 255.255.255.0
Router(config-pool)#client-identifier 0100.07e9.594f.bf
Router(config-pool)#client-name glh-pc-2325
Router(config-pool)#domain-name glh.sm.aval
```

2 Практическая часть

На рисунке (2.1) приведена следующая топология сети. Выполнить следующие шаги:

Рисунок 2.1 – Расположение подсетей на логическом рабочем пространстве

6. Заполните начальный IP-адрес (192.168.0.0) и маску подсети (255.255.255.224).

7. В поле «Максимальное кол-во пользователей» введите 30 (количество доступных для назначения IP-адресов).

8. Нажмите кнопку «Добавить», а затем «Сохранить».

9. Аналогичным образом создайте пулы для VLAN3 и VLAN5 (для VLAN4 не нужно создавать пул, потому что в этой виртуальной локальной сети находятся только серверы, а для них рекомендуется настраивать статический IP-адрес). Обратите внимание, что поля «Имя пула», «Основной шлюз», «Начальный IP-адрес», «Маска подсети», а также «Максимальное кол-во пользователей» будут отличаться для разных VLAN. Поле «DNS-сервер» может совпадать.

10. Включите службу DHCP, отметив «Вкл» рядом с именем интерфейса.

После создания трех пулов должны получиться следующие настройки:

Рисунок 2.2 – Настройка DHCP-сервера

Теперь необходимо настроить агента DHCP-Relay на коммутаторе третьего уровня. Суть DHCP-Relay заключается в пересылке широковещательного пакета от клиента одноадресатным пакетом DHCP-

серверу, поэтому для каждого VLAN, на который будет приходить сообщение DHCPDISCOVER необходимо указать IP-адрес DHCP-сервера:

11. На коммутаторе третьего уровня войдите в режим конфигурации интерфейса VLAN2 командой interface vlan2.

12. Укажите адрес DHCP-сервера с помощью команды ip helper-address 192.168.0.82.

Аналогичные действия проведите для VLAN3 и VLAN5.

Проверьте работу DHCP-сервера. Зайдите в настройки IP-адреса любого ПК и отметьте пункт «DHCP». Через некоторое время автоматически заполнятся все поля и появится надпись: «Успешный DHCP запрос».

Рисунок – 2.3. Автоматическое получение IP-адреса с помощью протокола DHCP

В качестве DHCP-сервера может также выступать коммутатор третьего уровня. Это может быть полезно, если в сети не присутствует сервер, но присутствует множество узлов. Выключите существующий DHCP-сервер:

13. В настройках сервера выключите службу DHCP, отметив «Откл» во вкладке «Службы».

14. На коммутаторе третьего уровня в режиме конфигурации VLAN-интерфейса введите команду no ip helper-address 192.168.0.83, тем самым удаляя перенаправление клиентских широковещательных сообщений DHCPDISCOVER к DHCP-серверу.

15. Теперь можно перейти к настройке DHCP-сервера на коммутаторе третьего уровня. Введите команды так, как показано на рисунках ниже:

Рисунок 2.4 – Настройка DHCP для VLAN2

Рисунок 2.5 – Настройка DHCP для VLAN3

Рисунок 2.6 – Настройка DHCP для VLAN5

Команда Switch (config) #ip dhcp pool – задание poola подсети .

Команда Switch (dhcp-config) #network – pool, выдаваемых ip адресов.

Команда Switch (dhcp-config) #default-router- назначение шлюза по умолчанию.

Команда Switch (dhcp-config) #dns-server – прописать существующие dns-сервера сети.

После выполнения всех настроек обязательно проверьте работу протокола DHCP с помощью способа, описанного выше. Также на коммутаторе третьего уровня можно посмотреть список всех выданных IP-адресов. Это можно сделать из привилегированного режима командой show ip dhcp binding.

Рисунок 2.7 – Вывод команды show ip dhcp binding

Задание для самостоятельной работы

1. Добавить в сеть коммутатор третьего уровня, подключить к нему коммутаторы второго уровня, расположенные в разных подсетях. Организовать отказоустойчивость по технологии динамического агрегирования LACP. Добавить сервер, настроить автоматическую выдачу IP-адресов с помощью DHCP. Разбить сеть на подсети:

16. отдел программистов: 4 узла;

17. отдел тестеров: 3 узла;

18. отдел администраторов. 2 узла;

19. серверная: 1 узел.

В качестве начального IP-адреса сети взять 192.168.10.0 с маской 255.255.255.0.

Заменить центральный коммутатор второго уровня на коммутатор третьего уровня. Организовать отказоустойчивость по технологии статического агрегирования каналов. Настроить DHCP на коммутаторе третьего уровня. Разбить сеть на подсети:

20. отдел 1: 111 узлов;

21. отдел 2: 55 узлов;

22. отдел 3: 10 узлов;

23. отдел 4: 20 узлов.

В качестве начального IP-адреса сети взять 192.168.20.0 с маской 255.255.255.0.

Добавить в сеть коммутатор третьего уровня, подключить к нему коммутаторы второго уровня. Добавить сервер, настроить автоматическую выдачу IP-адресов с помощью DHCP. Разбить сеть на подсети:

24. отдел производства: 5 узла;

25. отдел кадров: 3 узла;

26. отдел бухгалтерии: 2 узла;

27. отдел продаж: 2;

28. серверная: 1 узел.

В качестве начального IP-адреса сети взять 192.168.30.0 с маской 255.255.255.0.

Добавить коммутатор третьего уровня, подключить к нему коммутаторы второго уровня. Настроить DHCP на коммутаторе третьего уровня. Разбить сеть на подсети:

29. отдел производства: 62 узла;

30. отдел разработки: 30 узла.

В качестве начального IP-адреса сети взять 192.168.40.0 с маской 255.255.255.0.

Добавить в сеть коммутатор третьего уровня, подключить к нему коммутаторы второго уровня, расположенные в разных подсетях. Добавить сервер, настроить автоматическую выдачу IP-адресов с помощью DHCP. Разбить сеть на подсети:

31. отдел диспетчеров: 5 узла;

32. отдел бухгалтеров: 7 узла;

33. отдел кадров: 4 узла;

34. серверная: 1 узел.

В качестве начального IP-адреса сети взять 192.168.50.0 с маской 255.255.255.0.

Заменить центральный коммутатор второго уровня на коммутатор третьего уровня. Настроить DHCP на коммутаторе третьего уровня. Разбить сеть на подсети:

35. отдел 1: 79 узлов;

36. отдел 2: 34 узлов;

37. отдел 3: 5 узлов;

38. отдел 4: 45 узлов.

В качестве начального IP-адреса сети взять 192.168.60.0 с маской 255.255.255.0.

Добавить в сеть коммутатор третьего уровня, подключить к нему коммутаторы второго уровня. Добавить сервер, настроить автоматическую выдачу IP-адресов с помощью DHCP. Разбить сеть на подсети:

39. отдел производства: 8 узлов;

40. отдел кадров: 2 узла;

41. отдел бухгалтерии: 4 узла;

42. отдел продаж: 3 узла;

43. серверная: 1 узел.

В качестве начального IP-адреса сети взять 192.168.70.0 с маской 255.255.255.0.

Добавить коммутатор третьего уровня, подключить к нему коммутаторы второго уровня. Настроить DHCP на коммутаторе третьего уровня. Разбить сеть на подсети:

44. отдел производства: 82 узла;

45. отдел разработки: 33 узла.

В качестве начального IP-адреса сети взять 192.168.80.0 с маской 255.255.255.0.

Контрольные вопросы

1. Что такое DHCP? Необходим ли подобные сервис в локальных сетях?

2. Опишите назначение пакетов: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, DHCPNACK, DHCPINFORM.

3. Зачем нужен dhcpclient?

4. Что такое класс клиента? Как можно задать класс клиента при использовании пакета dhcpclient?

5. Что такое диапазон адресов (range)?

6. Как используется резервирование и зачем?

7. Как указать в настройках сетевой конфигурации узла host3 какой из интерфейсов использовать для передачи данных "по умолчанию"?

8. Зачем используется агент ретрансляции?

Лабораторная работа №9

Цель лабораторной работы: Изучение и настройка протокола GRE

1 Теоретическая часть

GRE (Generic Routing Encapsulation) – протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Широко применяется как сам по себе, так и в совокупности с IPSec для создания туннелей. GRE может быть использован для переноса многих других протоколов пассажиров. Туннели являются point-to-point соединениями, определяющимися tunnel source и tunnel destination адресами на обоих концах. Его основное назначение – инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP пакеты.

GRE не обеспечивает безопасности передаваемых данных – это site-to-site VPN туннель. Обычно такой туннель используется, когда есть специфичные задачи, связанные с маршрутизацией и нет требований к безопасности. Не стоит забывать, что чистый GRE туннель – не нагружает оборудование, а нагрузка при шифровании большого объёма данных весьма существенна.

Протокол GRE инкапсулируется напрямую в IP, минуя TCP или UDP, в IP пакете есть специальное поле «Protocol type», в котором содержится число, обозначающее протокол, инкапсулированный в данный IP пакет, для GRE protocol type равен 47. В связи с этим, если в сети есть GRE туннели, то стоит внимательно относиться к написанию расширенных списков контроля доступа.

Поскольку GRE это инкапсулируемый протокол, необходимо настроить maximum transfer unit (mtu) на 1400 и maximum segment size (mss) на 1360 байт. Поскольку в большинстве случае используется MTU 1500, а у нас есть еще поле GRE, необходимо уменьшить MTU. Значение 1400 - это самое распространенное решение, при котором фрагментация пакетов сведена к минимуму.

Схема IP пакета:

Проходя через GRE-туннель, к пакету добавляется заголовок GRE:

А сверху добавляется новый заголовок IP, где будет значится адрес tunnel source в качестве отправителя, и tunnel destination в качестве получателя:

2 Практическая часть

Настройка GRE-туннеля на оборудовании Cisco.
Соберем топологию сети, которая представлена на рисунке:

Рисунок 1 – Схема топологии сети

L1:

Рисунок 2 – Физический уровень

L2:

Рисунок 3 – Канальный уровень.

L3:

Рисунок 4 – Сетевой уровень.

Ход работы:

1. Настраиваем ip адреса как показано на рисунке и настраиваем на данной топологии статическую маршрутизацию.

2. Из PC0 выполняем трассировку до компьютера PC1 с помощью команды tracert:

Tracing route to 192.168.1.2 over a maximum of 30 hops:

1 0 ms 0 ms 0 ms 192.168.0.1

2 0 ms 0 ms 0 ms 7.7.7.2

3 0 ms 1 ms 0 ms 8.8.8.1

4 10 ms 11 ms 11 ms 192.168.1.2

Как мы видим пакет проходит через все маршрутизаторы последовательно вплоть до компьютера адресата.

3. Теперь создадим GRE туннель между маршрутизаторами R1 и R3 со внутренней адресацией 10.10.10.0/24. Для этого заходим в режим конфигурации и пишем команды маршрутизаторе R1:

R1(config)#interface tunnel 0

%LINK-5-CHANGED: Interface Tunnel0, changed state to up

R1(config-if)# tunnel mode gre ip

R1(config-if)# ip address 10.10.10.1 255.255.255.0

Далее пишем на каком интерфейсе мы хотим настроить GRE:

R1(config-if)# tunnel sourse gigabitEthernet 0/1

Теперь пишем ip адрес назначения (вторая сторона туннеля):

R1(config-if)# tunnel destination 8.8.8.1

%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up.

4. Таким же образом настраиваем GRE туннель на маршрутизаторе R3 в сторону R2.

5. Теперь выполним трассировку с маршрутизатора R1 противоположного конца туннеля – на R3:

Router#traceroute 10.10.10.2

Tracing the route to 10.10.10.2

1 10.10.10.2 33 msec 0 msec 3 msec

Как видно, трассировка проходит внутри туннеля и мы не видим лишнего хопа в виде R2.

Посмотрим таблицу маршрутизации на R1:

Router#show ip route

Gateway of last resort is 7.7.7.2 to network 0.0.0.0

7.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 7.7.7.0/24 is directly connected, GigabitEthernet0/1

L 7.7.7.1/32 is directly connected, GigabitEthernet0/1

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.10.10.0/24 is directly connected, Tunnel0

L 10.10.10.1/32 is directly connected, Tunnel0

192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.0.0/24 is directly connected, GigabitEthernet0/0

L 192.168.0.1/32 is directly connected, GigabitEthernet0/0

S* 0.0.0.0/0 [1/0] via 7.7.7.2

Видно, что новая сеть отображается, как непосредственно подключенная к интерфейсу Tunnel0. Если сейчас попробовать сделать трассировку с компьютера 1 до компьютера 2, то она не пойдёт по туннелю. Это связано с тем, что на маршрутизаторе R1 нет соответствующего маршрута. Просматривая свою таблицу маршрутизации, R1 отправит пакеты на PC2 по маршруту «L 192.168.0.1/32 is directly connected, GigabitEthernet0/0

S* 0.0.0.0/0 [1/0] via 7.7.7.2», то есть как и раньше – в обход туннеля.

6. Чтобы исправить ситуацию пропишем с двух сторон на R1 и R3 статические маршруты, в которых явно укажем, что в сети 192.168.0.0 и 192.168.1.0 надо доставлять трафик через туннель.

На R1:

Router(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.2

На R3:

Router(config)#ip route 192.168.0.0 255.255.255.0 10.10.10.1

Посмотрим таблицу маршрутизации снова:

Router#show ip route

Gateway of last resort is 8.8.8.2 to network 0.0.0.0

8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 8.8.8.0/24 is directly connected, GigabitEthernet0/2

L 8.8.8.1/32 is directly connected, GigabitEthernet0/2

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.10.10.0/24 is directly connected, Tunnel0

L 10.10.10.2/32 is directly connected, Tunnel0

S 192.168.0.0/24 [1/0] via 10.10.10.1

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0

L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

S* 0.0.0.0/0 [1/0] via 8.8.8.2

Теперь, как видно из таблицы маршрутизации, трафик пойдёт через GRE туннель.

7. Проверим это, выполнив трассировку с PC0 до PC1.

C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

1 0 ms 1 ms 0 ms 192.168.0.1

2 11 ms 11 ms 1 ms 10.10.10.2

3 12 ms 15 ms 22 ms 192.168.1.2

Trace complete.

Как видно, из результатов трассировки, теперь на пути всего два хопа: 192.168.0.1 – R1, шлюз PC1, который заворачивает трафик в туннель. Далее, транспортный (внешний) IP пакет с GRE внутри проходит на R2, затем на R3 и только тут из пакета декапсулируется внутренний IP – это и есть наш второй хоп – 10.10.10.2, затем пакет по локальной сети идёт адресату – на 192.168.1.2, если добавить в интернете ещё несколько маршрутизаторов, то трассировка не изменится, в ней по-прежнему будет два хопа до адресата.

Примеры конфигурации маршрутизаторов:

R1:

```
Building configuration...


Current configuration : 922 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX15247LP5
spanning-tree mode pvst
!
interface Tunnel0
ip address 10.10.10.1 255.255.255.0
mtu 1476
tunnel source GigabitEthernet0/1
tunnel destination 8.8.8.1
!
!
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 7.7.7.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
```

```
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 7.7.7.2
ip route 192.168.1.0 255.255.255.0 10.10.10.2
!
ip flow-export version 9
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
R2:
Building configuration...
Current configuration : 794 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX152409PR
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
no ip address
duplex auto
```

```
speed auto
shutdown
!
interface GigabitEthernet0/1
ip address 7.7.7.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 8.8.8.2 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.0.0 255.255.255.0 7.7.7.1
ip route 192.168.1.0 255.255.255.0 8.8.8.1
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
End
```

R3:

```
Building configuration...
Current configuration : 922 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
```

```
hostname Router
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1524S5MM
!
spanning-tree mode pvst
!
interface Tunnel0
ip address 10.10.10.2 255.255.255.0
mtu 1476
tunnel source GigabitEthernet0/2
tunnel destination 7.7.7.1
!
!
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
ip address 8.8.8.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 8.8.8.2
ip route 192.168.0.0 255.255.255.0 10.10.10.1
```

```
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
end
```

Задание для самостоятельной работы:

Используя представленную в практической части топологию сети, настроить ip-адреса по следующей схеме, где X – ваш номер в подгруппе:

Для сети 192.168.0.0/24 ---- 192.168.X.0/24
Для сети 192.168.1.0/24 ---- 192.168.X+5.0/24
Для сети 10.10.10.0/24 ---- 10.10.X.0/24
Для сети 7.7.7.0/24 ---- 7.7.X.0/24
Для сети 8.8.8.0/24 ---- 8.8.X.0/24

Контрольные вопросы

1. Что такое GRE?
2. Что он позволяет делать?
3. В каких случаях используется данный протокол?
4. Какой протокол используется GRE для инкапсуляции в IP?

Лабораторная работа №10

Изучение протокола SSH

1 Теоретическая часть

SSH (Secure Shell) – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

SSH позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол. Таким образом, можно не только удалённо работать на компьютере через командную оболочку, но и передавать по шифрованному каналу звуковой поток или видео. Также SSH может использовать сжатие передаваемых данных для последующего их шифрования.

Техническая информация о протоколе:

Для аутентификации сервера в SSH используется протокол аутентификации сторон на основе алгоритмов электронно-цифровой подписи RSA или DSA, но допускается также аутентификация при помощи пароля.

SSH-сервер обычно прослушивает соединения на TCP-порту 22.

1. Аутентификация по паролю наиболее распространена. При каждом подключении подобно https вырабатывается общий секретный ключ для шифрования трафика.

2. При аутентификации по ключевой паре предварительно генерируется пара открытого и закрытого ключей для определённого пользователя. На машине, с которой требуется произвести подключение, хранится закрытый ключ, а на удалённой машине - открытый. Эти файлы не передаются при аутентификации, система лишь проверяет, что владелец открытого ключа также владеет и закрытым. При данном подходе, как правило, настраивается автоматический вход от имени конкретного пользователя в ОС.

3. Аутентификация по ip-адресу небезопасна, эту возможность чаще всего отключают.

Для создания общего секрета (сеансового ключа) используется алгоритм Диффи – Хеллмана (DH). Для шифрования передаваемых данных используется симметричное шифрование.

Для сжатия шифруемых данных может использоваться алгоритм LempelZiv, который обеспечивает такой же уровень сжатия, что и архиватор ZIP. Сжатие SSH включается лишь по запросу клиента, и на практике используется редко.

Протокол SSH-1, в отличие от протокола telnet, устойчив к атакам прослушивания трафика («снифинг»), но неустойчив к атакам «человек посередине». Протокол SSH-2 также устойчив к атакам путём присоединения посередине, так как невозможно включиться в уже установленную сессию или перехватить её.

Для предотвращения атак «человек посередине» при подключении к хосту, ключ которого ещё не известен клиенту, клиентское ПО показывает пользователю «слепок ключа». Рекомендуется тщательно сверять показываемый клиентским ПО «слепок ключа» со слепком ключа сервера, желательно полученным по надёжным каналам связи или лично.

Для работы по SSH нужен SSH-сервер и SSH-клиент. Сервер прослушивает соединения от клиентских машин и при установлении связи производит аутентификацию, после чего начинает обслуживание клиента. Клиент используется для входа на удалённую машину и выполнения команд.

Для соединения сервер и клиент должны создать пары ключей – открытых и закрытых – и обменяться открытыми ключами. Обычно используется также и пароль.

SSH-туннелирование:

SSH-туннель – это туннель, создаваемый посредством SSH-соединения и используемый для шифрования туннелированных данных. Используется для того, чтобы обезопасить передачу данных в Интернете При пересылке через SSH-туннель незашифрованный трафик любого протокола шифруется на одном конце SSH-соединения и расшифровывается на другом.

Практическая реализация может выполняться несколькими способами:

- Созданием Socks-прокси для приложений, которые не умеют работать через SSH-туннель, но могут работать через Socks-прокси
- Использованием приложений, умеющих работать через SSH-туннель.
- Созданием VPN-туннеля, подходит практически для любых приложений.
- Если приложение работает с одним определённым сервером, можно настроить SSH-клиент таким образом, чтобы он пропускал через SSH-туннель TCP-соединения, приходящие на определённый TCP-порт машины, на которой запущен SSH-клиент.

2 Практическая часть

Рисунок 2.1 – Топология сети

Настройка SSH на маршрутизаторе:

1. Заходим в привилегированный режим.

Router>enable

2. Настроим параметры, необходимые для генерации ключа, используемого ssh.

Для этого установим точную текущую дату и время.

Router#clock set 11:25:00 23 September 2018

3. Заходим в режим конфигурирования.

Router#configure terminal

4. Задаем домен.

Router(config)# ip domain name newdomain.ru

5. Задаем имя роутера.

Router(config)#hostname myRouter

6. Задаем версию протокола SSH.

myRouter(config)#ip ssh version 2

7. Задаем количество попыток подключения по SSH.

myRouter(config)#ip ssh authentication-retries 5

8. Задаем хранение паролей в зашифрованном виде.

myRouter(config)#service password-encryption

9. Включаем протокол AAA (Authentication, Authorization, Accounting).

myRouter(config)#aaa new-model

10. Создаем пользователя admin с паролем 1234 и максимальным уровнем привилегий (15)

myRouter(config)#username admin privilege 15 secret 1234

11. Задаем пароль для привилегированного режима

myRouter(config)#enable secret 1234

12. Генерируем RSA ключ для SSH (для большей надежности длиной не менее 1024).

myRouter(config)#crypto key generate rsa

The name for the keys will be: myRouter.newdomain.ru

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

13. Разрешаем доступ по SSH только из определенной сети (172.16.0.0/24).

myRouter(config)#access-list 30 permit 172.16.0.0 0.0.0.255

14. Входим в режим конфигурирования терминальных линий.

myRouter(config)#line vty 0 4

15. Разрешаем доступ только по SSH.

myRouter(config-line)#transport input ssh

16. По умолчанию журнальные сообщения могут выводиться в независимости от того набирает пользователь какие-либо команды или нет, прерывая исполнение текущих команд. Включая logging synchronous маршрутизатор начинает дожидаться завершения текущей команды и вывода ее отчета.

myRouter(config-line)#logging synchronous

17. Позволяем входить сразу в привилегированный режим.

myRouter(config-line)#privilege level 15

18. Включаем автоматическое закрытие SSH сессии через 15 минут.

myRouter(config-line)#exec-timeout 15 0

19. Теперь привязываем группу доступа к терминальной линии.

myRouter(config-line)#access-class 30 in

Настройка SSH на коммутаторе:

Сначала повторяем пункты 1-7 из настройки маршрутизатора:

1. Заходим в режим конфигурации и вводим:

MySwitch(config)# line vty 0 4 (виртуальный терминал).

2. Включаем SSH Для входящего трафика:

MySwitch (config-line)# transport input ssh

3. Говорим что авторизация будет через локальное хранилище учетных записей, и сохраняем настройки:

MySwitch (config-line)# login local

MySwitch (config-line)# end

MySwitch # write memory

4. Генерируем RSA ключ для SSH (для большей надежности длиной не менее 1024).

mySwitch(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

5. Задаем количество попыток подключения по SSH.

mySwitch(config)#ip ssh authentication-retries 5

Включение SSH на оборудовании закончено.

3 Задание для самостоятельной работы:

1) Настроить SSH-1 если у вас нечетный номер в подгруппе, SSH-2 если четный.
2) В качестве имени маршрутизатора используйте свою фамилию, имя коммутатора – ваше имя.

4 Контрольные вопросы

1. Что такое SSH?
2. Что он позволяет делать?
3. На основе чего производится аутентификация в SSH?
4. Что генерируется при аутентификации для пользователя?
5. Какой алгоритм используется при создании общего секрета?
6. Чем отличаются протоколы SSH-1 и SSH-2?
7. Что такое SSH-туннелирование?
8. Какими способами реализуется SSH-туннелирование?
9. Какой порт использует протокол SSH?

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕ- ЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для организации и проведения самостоятельной работы
студентов по дисциплине «Вычислительные системы и компьютерные сети»
направления подготовки 09.03.01 Информатика и вычислительная техника,
направленность (профиль) «Программное обеспечение средств вычислительной техники и автоматизированных систем»

Ставрополь, 2026

Методические указания по организации самостоятельной работы студентов составлено в соответствии с требованиями программы дисциплины «Вычислительные системы и компьютерные сети» для бакалавров направления подготовки 09.03.01 Информатика и вычислительная техника. Учебно-методическое пособие посвящено планируемой учебной работе студентов, выполняемой во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия, при частичном, непосредственном участии преподавателя.

СОДЕРЖАНИЕ

1. Самостоятельная работа как важнейшая форма учебного процесса

Самостоятельная работа – это планируемая учебная, учебно- исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Изначально необходимо ознакомиться с технологической картой самостоятельной работы обучающегося.

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	очная форма				Формы текущего контроля успеваемости
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов	
			Лекции	Практические занятия	Лабораторные работы		
6 семестр							
	Многомашинные и многопроцессорные вычислительные системы, супер-ЭВМ Архитектурные особенности вычислительных систем различных классов. SMP, MPP, NUMA, PVP - архитектуры. Способы организации высокопроизводительных процессоров. Основные сферы применения многопроцессорных ВС. Обработка транзакций в режиме реального времени (OLTP, On line transaction processing). Лабораторная работа 1. Исследование технологий создания виртуальных процессоров ЦОД.	ПК-7 ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ПК-8 ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$	4		4/4	6	Защита лабораторной работы

	Технологии локальных вычислительных сетей Определение информационно-компьютерной сети. Технология Gigabit Ethernet. Технология Fast Ethernet. Технология Ethernet. Принципы коммутации информации. Типы линий связи локальных сетей Лабораторная работа 2. Статическая маршрутизация Лабораторная работа 3. Динамическая маршрутизация. Изучение протокола RIP Лабораторная работа 4. Динамическая маршрутизация. Протокол EIGRP	ПК-7 ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ПК-8 ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$	12		28/28	18	Защита лабораторной работы
	ИТОГО за 6 семестр		16		32/32	24	
7 семестр							
	Современные сетевые технологии Виртуальные частные сети. Протоколы IGMP и UPnP. Качество обслуживания и технология SharePort. Технология преобразования сетевых адресов. Списки управления доступом Лабораторная работа 5. Списки управления доступом ACL Лабораторная работа 6-7. Преобразование сетевых адресов NAT	ПК-7 ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ПК-8 ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$	8		8	15	Защита лабораторной работы
	Объединенные локальные сети Принципы объединения сетей на основе протоколов сетевого уровня. Виртуальные локальные сети. Планирование сетей Лабораторная работа 8 Изучение протокола динамической конфигурации узла DHCP Лабораторная работа 9. GRE Лабораторная работа 10. Изучение протокола SSH	ПК-7 ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ПК-8 ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$	10		10	21	Защита лабораторной работы
	ИТОГО за 7 семестр		18		18	36	
	ИТОГО		34		50	60	

Самостоятельная работа студентов в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения. Обучение в ВУЗе включает в себя две, практически одинаковые по объему и взаимовлиянию части – процесса обучения и процесса самообучения.

Поэтому СРС должна стать эффективной и целенаправленной работой студента.

Концепцией модернизации российского образования определены основные задачи профессионального образования - "подготовка квалифицированного работника соответствующего уровня и профиля, конкурентоспособного на рынке труда, компетентного, ответственного, свободно владеющего своей профессией и ориентированного в смежных областях деятельности, способного к эффективной работе по специальности на уровне мировых стандартов, готового к постоянному профессиональному росту, социальной и профессиональной мобильности".

Решение этих задач невозможно без повышения роли самостоятельной работы студентов над учебным материалом, усиления ответственности преподавателей за развитие навыков самостоятельной работы, за стимулирование профессионального роста студентов, воспитание творческой активности и инициативы.

К современному специалисту общество предъявляет достаточно широкий перечень требований, среди которых немаловажное значение имеет наличие у выпускников определенных способностей и умения самостоятельно добывать знания из различных источников, систематизировать полученную информацию, давать оценку конкретной финансовой ситуации. Формирование такого умения происходит в течение всего периода обучения через участие студентов в лабораторных или практических занятиях, в выполнении контрольных заданий и тестов, написание курсовых и выпускных квалификационных работ. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Формы самостоятельной работы студентов разнообразны. По данной дисциплине «Вычислительные системы и компьютерные сети» предусмотрены следующие:

Использование материала учебно-методического комплекса дисциплины

На первом этапе необходимо ознакомиться с обязательным минимумом содержания основной образовательной программы по изучаемой дисциплине. Далее необходимо изучить рабочую программу дисциплины, в которой рассмотрено содержание тем дисциплины лекционного курса, взаимосвязь тем лекций лабораторных/практических занятий, темы и виды самостоятельной работы. По каждому виду самостоятельной работы предусмотрены определённые формы отчетности, представленные в учебной программе по дисциплине «Вычислительные системы и компьютерные сети».

Работа с литературой

Для успешного освоения дисциплины, необходимо самостоятельно детально изучить представленные темы по рекомендуемым источникам информации, которые представлены в учебной программе.

Самостоятельная работа приобщает студентов к научному творчеству, поиску и решению актуальных современных проблем.

2. Цели и основные задачи СРС

Ведущая цель организации и осуществления СРС должна совпадать с целью обучения студента – подготовкой бакалавра с высшим образованием. При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности.

Целью самостоятельной работы студентов является овладение фундаментальными

знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

– систематизация и закрепление полученных теоретических знаний и практических умений студентов;

– углубление и расширение теоретических знаний;

– формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;

– развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

– формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

– развитие исследовательских умений;

– использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Виды самостоятельной работы

В образовательном процессе высшего профессионального образовательного учреждения выделяется два вида самостоятельной работы – аудиторная, под руководством преподавателя, и внеаудиторная. Тесная взаимосвязь этих видов работ предусматривает дифференциацию и эффективность результатов ее выполнения и зависит от организации, содержания, логики учебного процесса (межпредметных связей, перспективных знаний и др.):

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Основными видами самостоятельной работы студентов без участия пре- подавателя по данной дисциплине являются:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– подготовка к лабораторным или практическим работам, их оформление.

Основными видами самостоятельной работы студентов с участием пре- подавателей являются:

– текущие консультации;

– прием и защита лабораторных работ (во время проведения л/р, если они предусмотрены учебным планом);

– выполнение заданий на практических занятиях (если таковые предусмотрены учебным планом дисциплины);

– выполнение курсовой работы или проекта, если они предусмотрены учебным планом.

4. Организация СРС

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей дисциплины «Вычислительные системы и компьютерные сети», объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

– подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);

– основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);

– заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Деятельность студентов по формированию и развитию навыков учебной самостоятельной работы

В процессе самостоятельной работы студент приобретает навыки самоорганизации, самоконтроля, самоуправления, саморефлексии и становится активным самостоятельным субъектом учебной деятельности.

Выполняя самостоятельную работу под контролем преподавателя студент должен:

– освоить минимум содержания, выносимый на самостоятельную работу студентов и предложенный преподавателем в соответствии с Федеральными государственными образовательными стандартами высшего образования;

– планировать самостоятельную работу в соответствии с графиком самостоятельной работы, предложенным преподавателем;

– самостоятельную работу студент должен осуществлять в организационных формах, предусмотренных учебным планом и рабочей программой преподавателя;

– выполнять самостоятельную работу и отчитываться по ее результатам в соответствии с графиком представления результатов, видами и сроками отчетности по самостоятельной работе студентов.

студент может:

сверх предложенного преподавателем (при обосновании и согласовании с ним) минимума обязательного содержания, определяемого программой по данной дисциплине:

– самостоятельно определять уровень (глубину) проработки содержания материала;

– предлагать темы и вопросы для самостоятельной проработки;

– в рамках общего графика выполнения самостоятельной работы предлагать обоснованный индивидуальный график выполнения и отчетности по результатам самостоятельной работы;

– предлагать свои варианты организационных форм самостоятельной работы;

– использовать для самостоятельной работы методические пособия, учебные

пособия, разработки сверх предложенного преподавателем перечня;

– использовать не только контроль, но и самоконтроль результатов самостоятельной работы в соответствии с методами самоконтроля, предложенными преподавателем или выбранными самостоятельно.

Самостоятельная работа студентов должна оказывать важное влияние на формирование личности будущего профессионала, она планируется студентом самостоятельно. Каждый студент самостоятельно определяет режим своей работы и меру труда, затрачиваемого на овладение учебным содержанием по каждой дисциплине. Он выполняет внеаудиторную работу по личному индивидуальному плану, в зависимости от его подготовки, времени и других условий.

5. Общие рекомендации по организации самостоятельной работы

Основной формой самостоятельной работы студента является изучение конспекта лекций, их дополнение, рекомендованной литературы, активное участие на лабораторных или практических занятиях (в зависимости от учебного плана). Но для успешной учебной деятельности, ее интенсификации, необходимо учитывать следующие субъективные факторы:

1. Знание школьного программного материала, наличие прочной системы зияний, необходимой для усвоения основных вузовских курсов. Это особенно важно для математических и инженерных дисциплин. Необходимо отличать пробелы в знаниях, затрудняющие усвоение нового материала, от малых способностей. Затратив силы на преодоление этих пробелов, студент обеспечит себе нормальную успеваемость и поверит в свои способности.

2. Наличие умений, навыков умственного труда:

а) умение конспектировать на лекции и при работе с книгой;

б) владение логическими операциями: сравнение, анализ, синтез, обобщение, определение понятий, правила систематизации и классификации.

3. Специфика познавательных психических процессов: внимание, память, речь, наблюдательность, интеллект и мышление. Слабое развитие каждого из них становится серьезным препятствием в учебе.

4. Хорошая работоспособность, которая обеспечивается нормальным физическим состоянием. Ведь серьезное учение - это большой многосторонний и разнообразный труд. Результат обучения оценивается не количеством сообщаемой информации, а качеством ее усвоения, умением ее использовать и развитием у себя способности к дальнейшему самостоятельному образованию.

5. Соответствие избранной деятельности, профессии индивидуальным способностям. Необходимо выработать у себя умение регулировать свое эмоциональное состояние и устранять обстоятельства, нарушающие деловой настрой, мешающие намеченной работе.

6. Овладение оптимальным стилем работы, обеспечивающим успех в деятельности. Чередование труда и пауз в работе, периоды отдыха, индивидуально обоснованная норма продолжительности сна, предпочтение вечерних или утренних занятий, стрессоустойчивость на экзаменах и особенности подготовки к ним,

7. Уровень требований к себе, определяемый сложившейся самооценкой. Адекватная оценка знаний, достоинств, недостатков - важная составляющая самоорганизации человека, без нее невозможна успешная работа по управлению своим поведением, деятельностью.

Одна из основных особенностей обучения в высшей школе заключается в том, что постоянный внешний контроль заменяется самоконтролем, активная роль в обучении принадлежит уже не столько преподавателю, сколько студенту.

Зная основные методы научной организации умственного труда, можно при наименьших затратах времени, средств и трудовых усилий достичь наилучших результатов.

Эффективность усвоения поступающей информации зависит от работоспособности человека в тот или иной момент его деятельности.

Работоспособность - способность человека к труду с высокой степенью напряженности в течение определенного времени. Различают внутренние и внешние факторы работоспособности.

К внутренним факторам работоспособности относятся интеллектуальные особенности, воля, состояние здоровья.

К внешним:

- организация рабочего места, режим труда и отдыха;
- уровень организации труда - умение получить справку и пользоваться информацией;
- величина умственной нагрузки.

Выдающийся русский физиолог Н. Е. Введенский выделил следующие условия продуктивности умственной деятельности:

- во всякий труд нужно входить постепенно;
- мерность и ритм работы. Разным людям присущ более или менее разный темп работы;
- привычная последовательность и систематичность деятельности;
- правильное чередование труда и отдыха.

Отдых не предполагает обязательного полного бездействия со стороны человека, он может быть достигнут простой переменой дела. В течение дня работоспособность изменяется. Наиболее плодотворным является *утреннее время (с 8 до 14 часов),* причем максимальная работоспособность приходится на период с 10 до 13 часов, затем *послеобеденное* - (с 16 до 19 часов) и *вечернее* (с 20 до 24 часов). Очень трудный для понимания материал лучше изучать в начале каждого отрезка времени (лучше всего утреннего) после хорошего отдыха. Через 1-1,5 часа нужны перерывы по 10 - 15 мин, через 3 - 4 часа работы отдых должен быть продолжительным - около часа.

Составной частью научной организации умственного труда является овладение техникой умственного труда.

Время, которым располагает студент для выполнения учебного плана, складывается из двух составляющих: одна из них – это аудиторная работа в вузе по расписанию занятий, другая - внеаудиторная самостоятельная работа. Задания и материалы для самостоятельной работы выдаются во время учебных занятий по расписанию, на этих же занятиях преподаватель осуществляет контроль за самостоятельной работой, а также оказывает помощь студентам по правильной организации работы.

Самостоятельные занятия потребуют интенсивного умственного труда, который необходимо не только правильно организовать, но и стимулировать. При этом очень важно уметь поддерживать устойчивое внимание к изучаемому материалу. Выработка внимания требует значительных волевых усилий. Именно поэтому, если студент замечает, что он часто отвлекается во время самостоятельных занятий, ему надо заставить себя сосредоточиться.

Подобную процедуру необходимо проделывать постоянно, так как это является тренировкой внимания. Устойчивое внимание появляется тогда, когда человек относится к делу с интересом.

Следует правильно организовать свои занятия по времени: 50 минут - работа, 5-10 минут - перерыв; после 3 часов работы перерыв - 20-25 минут. Иначе нарастающее утомление повлечет неустойчивость внимания. Очень существенным фактором, влияющим на повышение умственной работоспособности, являются систематические занятия физической культурой. Организация активного отдыха предусматривает чередование умственной и физической деятельности, что полностью восстанавливает работоспособность человека.

6. Самостоятельная работа студента - необходимое звено становления исследователя

Прогресс науки и техники, информационных технологий приводит к значительному увеличению научной информации, что предъявляет более высокие требования не только к моральным, нравственным свойствам человека, но и в особенности, постоянно возрастающие требования в области образования – обновление, модернизация общих и профессиональных знаний, умений специалиста.

Всякое образование должно выступать как динамический процесс, присущий человеку и продолжающийся всю его жизнь. Овладение научной мыслью и языком науки является необходимой составляющей в самоорганизации будущего специалиста исследователя. Под этим понимается не столько накопление знаний, сколько овладение научно обоснованными способами их приобретения. В этом, вообще говоря, состоит основная задача вуза.

Специфика вузовского учебного процесса, в организации которого самостоятельной работе студента отводятся все больше места, состоит в том, что он является как будто бы последним и самым адекватным звеном для реализации этой задачи. Поскольку во время учебы в вузе происходит выработка стиля, навыков учебной (познавательной) деятельности, рациональный характер которых будет способствовать постоянному обновлению знаний высококвалифицированного выпускника вуза.

Однако до этом пути существуют определенные трудности, в частности, переход студента от синтетического процесса обучения в средней школе, к аналитическому в высшей. Это связано как с новым содержанием обучения (расширение общего образования и углубление профессиональной подготовки), так и с новыми, неизвестными до сих пор формами: обучения (лекции, семинары, лабораторные занятия и т.д.). Студент получает не только знания, предусмотренные программой и учебными пособиями, но он также должен познакомиться со способами приобретения знаний так, чтобы суметь оценить, что мы знаем, откуда мы это знаем и как этого знания мы достигли. Ко всему этому приходят через собственную самостоятельную работу.

Это и потому, что самостоятельно приобретенные знания являются более оперативными, они становятся личной собственностью, а также мотивом поведения, развивают интеллектуальные черты, внимание, наблюдательность, критичность, умение оценивать. Роль преподавателя в основном заключается в руководстве накопления знаний (по отношению к первокурсникам), а в последующие годы учебы, на старших курсах, в совместном установлении проблем и заботе о самостоятельных поисках студента, а также

контролирования за их деятельностью. Отметим, что нельзя ограничиваться только приобретением знаний, предусмотренных программой изучаемой дисциплины, надо постоянно углублять полученные знания, сосредотачивая их на какой-нибудь узкой определенной области, соответствующей интересам студента. Углубленное изучение всех предметов, предусмотренных программой, на практике является возможным, и хорошая организация работы позволяет экономить время, что создает условия для глубокого, систематического, заинтересованного изучения самостоятельно выбранной студентом темы.

Конечно, все советы, примеры, рекомендации в этой области, даваемые преподавателем, или определенными публикациями, или другими источниками, не гарантируют никакого успеха без проявления собственной активности в этом деле, т. е. они не дают готовых рецептов, а должны способствовать анализу собственной работы, ее целей, организации в соответствии с индивидуальными особенностями. Учитывая личные возможности, существующие условия жизни и работы, навыки, на основе этих рекомендаций, возможно, выработать индивидуально обоснованную совокупность методов, способов, найти свой стиль или усовершенствовать его, чтобы изучив определенный материал, иметь время оценить его значимость, пригодность и возможности его применения, чтобы, в конечном счете, обеспечить успешность своей учебе с будущей профессиональной деятельности

7. Методические рекомендации для студентов по отдельным формам самостоятельной работы

Система вузовского обучения подразумевает значительно большую самостоятельность студентов в планировании и организации своей деятельности.

Работа с литературой

При работе с литературой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой – это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять,

чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента. Различают два вида чтения; первичное и вторичное. *Первичное* - эти внимательное, неторопливое чтение, при котором можно остановиться на трудных местах. После него не должно остаться ни одного непонятного олова. Содержание не всегда может быть понятно после первичного чтения.

Задача *вторичного* чтения полное усвоение смысла целого (по счету это чтение может быть и не вторым, а третьим или четвертым).

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют четыре основные установки в чтении научного текста:

1. информационно-поисковый (задача – найти, выделить искомую информацию);

2. усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения, излагаемые автором, так и всю логику его рассуждений);

3. аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему);

4. творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

С наличием различных установок обращения к научному тексту связано существование и нескольких ***видов чтения***:

1. библиографическое – просматривание карточек каталога, рекомендательных списков, сводных списков журналов и статей за год и т.п.;

2. просмотровое – используется для поиска материалов, содержащих нужную информацию, обычно к нему прибегают сразу после работы со списками литературы и каталогами, в результате такого просмотра читатель устанавливает, какие из источников будут использованы в дальнейшей работе;

3. ознакомительное – подразумевает сплошное, достаточно подробное прочтение отобранных статей, глав, отдельных страниц, цель – познакомиться с характером информации, узнать, какие вопросы вынесены автором на рассмотрение, провести сортировку материала;

4. изучающее – предполагает доскональное освоение материала; в ходе такого чтения проявляется доверие читателя к автору, готовность принять изложенную информацию, реализуется установка на предельно полное понимание материала;

5. аналитико-критическое и творческое чтение – два вида чтения близкие между собой тем, что участвуют в решении исследовательских задач. Первый из них предполагает направленный критический анализ, как самой информации, так и способов ее получения и подачи автором; второе – поиск тех суждений, фактов, по которым или в связи с которыми,

читатель считает нужным высказать собственные мысли.

Из всех рассмотренных видов чтения основным для студентов является изучающее – именно оно позволяет в работе с учебной литературой накапливать знания в различных областях. Вот почему именно этот вид чтения в рамках учебной деятельности должен быть освоен в первую очередь. Кроме того, при овладении данным видом чтения формируются основные приемы, повышающие эффективность работы с научным текстом.

Основные виды систематизированной записи прочитанного:

1. Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

2. Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

3. Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

4. Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

5. Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта.

2. Выделите главное, составьте план.

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора.

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

Лабораторные/Практические занятия (в зависимости от учебного плана)

Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на лабораторных или практических занятиях как в результате обсуждения и

анализа лекционного материала, так и с помощью выполнения заданий лабораторной или практической работы, поставленных задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном выполнении заданий нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение задач или примеров следует излагать по дробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что выполнение каждого учебного задания должно до водиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Выполнение заданий данного типа нужно продолжать до приобретения твердых навыков в их решении.

Самопроверка

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих заданий на лабораторных занятиях и самостоятельно студенту рекомендуется, используя лист опорных материалов, воспроизвести по памяти определения, выводы формул, формулировки основных положений и доказательств.

В случае необходимости нужно еще раз внимательно разобраться в мате риале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

Консультации

Если в процессе самостоятельной работы над изучением теоретического материала или при выполнении заданий у студента возникают вопросы, разрешить которые самостоятельно не удается, необходимо обратиться к преподавателю для получения у него разъяснений или указаний. В своих вопросах студент должен четко выразить, в чем он испытывает затруднения, характер этого затруднения. За консультацией следует обращаться и в случае, если возникнут сомнения в правильности ответов на вопросы самопроверки.

Подготовка к экзамену по дисциплине «Вычислительные системы и компьютерные сети»

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом в 4 и 5 семестре. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к нему, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания.

Для успешной сдачи экзамена студенту важно в течение семестра полностью выполнить задания лабораторных или практических работ, подготовить отчет по каждой

работе и отчет по результатам самостоятельного изучения тем, согласно учебной программе.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Текущая аттестация студентов проводится преподавателями, ведущими лабораторные или практические занятия по дисциплине в следующих формах: собеседование при защите лабораторной работы или заданий практической работы с предоставлением письменного (или в электронной форме) отчета, в зависимости от предъявляемых требований.

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература	1. Олифер, В. Г. Компьютерные сети : принципы, технологии, протоколы : учеб. пособие для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. [и др.] : Питер, 2014. - 944 с. : ил. - (Учебник для вузов). - Гриф: Рек. МО. - Библиогр.: с. 917. - Алф. указ.: с. 918-943. - ISBN 978-5-469-00004-8 2.Мелехин, В. Ф. Вычислительные системы и сети : учебник для вузов / В.Ф. Мелехин, Е.Г. Павловский. - Москва : Академия, 2013. - 207, [1] с. : ил. ; 22. - (Высшее профессиональное образование. Автоматика и управление. Бакалавриат) (Бакалавриат). - Библиогр.: с. 205-206. - ISBN 978-5-7695-9663-6. 3.Шишова, Н. А. Основы построения инфокоммуникационных систем и сетей [Электронный ресурс] : учебное пособие / Н. А. Шишова. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 43 c. — 2227-8397.
Дополнительная литература	1. Деарт, В. Ю. Мультисервисные сети связи. Транспортные сети и сети доступа [Электронный ресурс] : учебное пособие / В. Ю. Деарт. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2014. — 101 c. — 948-5-905376-13-9. — Режим доступа: 2. Пуговкин, А. В. Телекоммуникационные системы [Электронный ресурс] : учебное пособие / А. В. Пуговкин. — Электрон. текстовые данные. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2007. — 202 c. — 5-86889-337-9.
Программное обеспечение	Альт Рабочая станция 10 Альт Рабочая станция K Альт «Сервер» Пакет офисных программ - Р7-Офис