ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Кафедра «Вычислительные системы и информационная безопасность»

СБОРНИК УПРАЖНЕНЕЙ

по дисциплинам

«Инфокоммуникационные системы и сети», «Сети и передачи информации»

Автор
Чуйкова Е.Н.
Галушка В.В.

Ростов-на-Дону, 2014

Аннотация

Методические указания предназначены для студентов специальностей 230201, 220201, направлений 230400, 090900 очной, заочной форм обучения.

Автор

к.т.н., доцент

Чуйкова Е.Н.

к.т.н., доцент

Галушка В.В.

Оглавление

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: АДМИНИСТРИРОВАНИЕ ЛОКАЛЬНЫХ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ

Цель работы: изучение технологии создания локальных учетных записей пользователей, групп и настройка их свойств с помощью утилиты ***Локальные пользователи и группы***.

Теоретические сведения

Одной из основных задач управления сетью является создание учетных записей пользователей и групп. Создание учетных записей и групп занимает важное место в обеспечении безопасности Windows 2000, поскольку, назначая им права доступа, администратор получает возможность ограничить пользователей в доступе к конфиденциальной информации компьютерной сети, разрешить или запретить им выполнение в сети определенного действия, например архивацию данных или завершение работы компьютера. Обычно право доступа ассоциируется с объектом — файлом или папкой. Оно определяет возможность данного пользователя получить доступ к объекту.

Учетной записью называется совокупность прав и дополнительных параметров, ассоциированных с определенным пользователем.

Учетные записи пользователей и компьютеров представляют физический объект, такой как компьютер или пользователь. Учетные записи пользователей и компьютеров (а также группы) называются участниками безопасности. Участники безопасности являются объектами каталога, которым автоматически присваиваются коды безопасности. Объекты с кодами безопасности могут входить в сеть и получать доступ к ресурсам домена. Учетная запись пользователя или компьютера используется для следующих целей.

- Проверка подлинности пользователя или компьютера.
- Разрешение или запрещение доступа к ресурсам домена.
- Администрирование других участников безопасности.
- Аудит действий, выполняемых с использованием учетной записи пользователя или компьютера.

Любой пользователь характеризуется наличием определенной *учетной записи*, которая позволяет пользователю производить вход на компьютеры и домены, если она может быть проверена и допущена к ресурсам домена. Каждый входящий в сеть

пользователь должен иметь собственную учетную запись и пароль. Учетные записи пользователей также могут использоваться для некоторых приложений как учетные записи службы.

Каждый компьютер, работающий под управлением Windows 2000 или Windows NT, который присоединяется к домену, имеет собственную уникальную учетную запись. Так же, как и учетные записи пользователей, учетные записи компьютеров предоставляют возможность проверки подлинности и аудита доступа компьютеров к сети, а также доступ к ресурсам домена.

Windows 2000 Server поддерживает локальных пользователей и группы, а также пользователей и группы Active Directory, поэтому работать с пользователями можно локально и посредством Active Directory.

В Windows 2000 с пользователями и группами на локальном уровне можно работать на рядовых серверах Windows 2000 и на компьютерах Windows 2000 Professional. На контроллерах доменов Windows 2000 для этого служит Active Directory.

В Windows 2000 поддерживаются пользователи двух видов: локальные и пользователи Active Directory (доменов). Компьютер, на котором функционирует Windows 2000 Professional или Windows 2000 Server (установленный как рядовой сервер), имеет возможность хранить свою собственную базу данных учетных записей пользователей. Пользователи, сведения о которых хранятся на локальном компьютере, называются локальными пользователями.

Active Directory – это служба каталога, доступная на платформе Windows 2000 Server и хранящая информацию в центральной базе данных, которая дает пользователям возможность иметь одну учетную запись в сети. Пользователи и группы, сведения о которых содержатся в центральной базе данных Active Directory, называются пользователями Active Directory или пользователями доменов.

Active Directory (активный каталог) разработан как масштабируемая сетевая структура. Он логически состоит из контейнеров, доменов и подразделений.

Контейнер – это объект Active Directory, в котором хранятся другие объекты Active Directory. Примерами объектов – контейнеров являются домены и подразделения.

Домен - основная логическая единица организации Active Directory. Объекты домена используют общую систему безопасности и информацию об учетных записях. У каждого домена должен быть как минимум один контроллер. Контроллер домена – это

компьютер Windows 2000 Server, содержащий всю базу данных домена (компьютер, на котором установлен Active Directory).

Локальные учетные записи пользователя должны присутствовать на каждом компьютере сети, к которому пользователю необходимо иметь доступ. Именно поэтому в больших сетях чаще применяются учетные записи пользователей доменов.

На компьютерах с Windows 2000 Professional и на рядовых серверах Windows 2000 Server локальные пользователи создаются и обслуживаются с помощью утилиты *Локальные пользователи и группы*, а на контроллерах доменов Windows 2000 пользователи обслуживаются посредством утилиты *Пользователи и компьютеры Active Directory*.

При установке Windows 2000 Server несколько встроенных учетных записей пользователей создаются по умолчанию. В таблице 1 описаны эти учетные записи и указана среда (локально или домен) для каждой из них.

ТАБЛИЦА 1. ВСТРОЕННЫЕ УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ

Встроенный пользователь	**ОПИСАНИЕ**	**Среда**
Администратор	Это специальная учетная запись, обладающая полным контролем над компьютером. Пароль для нее указывается при установке Windows 2000. Эта учетная запись может выполнять все задачи, например, создавать пользователей и группы, управлять файловой системой и настраивать печать.	Локально и домен

Гость	Эта учетная запись позволяет пользователям обращаться к компьютеру, даже если они не имеют уникального пользовательского имени и пароля. Работа такого пользователя всегда связана с определенным риском для безопасности системы, поэтому данная учетная запись по умолчанию запрещена. При разрешении ей, как правило, предоставляется крайне незначительное число привилегий.	Локально и домен
ILS_Anonymous_User	Это специальная учетная запись, используемая службой IIS. ILS поддерживает приложения телефонии, в которых применяются такие средства, как идентификатор вызывающего, видеоконференции, вызов конференции и работа с факсами. Для использования ILS необходимо установить службу IIS.	Домен
IUSR_имя компьютера	Это специальная учетная запись, применяемая в IIS для анонимного обращения (на компьютере, где служба IIS установлена).	Локально и домен

На рядовом сервере Windows 2000 можно использовать только локальные группы, которые размещаются в локальной базе данных рядового сервера Windows 2000.

В Active Directory на контроллере домена Windows 2000 можно создать группы безопасности и группы распространения. Группа безопасности – это логическая группа пользователей, которым необходимо обращаться к определенным ресурсам. Группы безопасности применяются для назначения полномочий на ресурсы. Группа распространения – это логическая группа пользовате-

лей с общими характеристиками. Группы распространения применяются приложениями и программами электронной почты.

На контроллерах доменов Windows 2000 также разрешается создавать группы, которые могут быть локальными, глобальными и универсальными:

– *Локальные группы доменов* применяются для назначения полномочий на ресурсы и могут содержать учетные записи пользователей, универсальные группы и глобальные группы из любого домена дерева или леса. В локальной группе домена могут содержаться также другие локальные группы домена из своего локального домена.

– *Глобальные группы* применяются для организации пользователей со схожими потребностями доступа к сети и могут содержать пользователей и глобальные группы из локального домена.

– *Универсальные группы* применяются для логической организации пользователей и отображаются в глобальном каталоге (в специальном списке, содержащем сведения о каждом объекте Active Directory). Универсальные группы могут содержать пользователей из любой области дерева или леса доменов, другие универсальные группы и глобальные группы.

При установке Windows 2000 Server несколько встроенных учетных записей групп создаются по умолчанию. В таблице 2 описаны эти учетные записи и указана среда (локально или домен) для каждой из них.

Таблица 2. Встроенные учетные записи групп

ВСТРОЕННАЯ ГРУППА	**Описание**	**Среда**
Операторы учетных записей	Члены группы могут создавать пользовательские и групповые учетные записи доменов, но управлять могут только теми учетными записями, которые создали.	Домен

Администраторы	Эта группа обладает всеми правами и привилегиями. Ее члены могут предоставить себе любые полномочия, которыми не обладают по умолчанию, чтобы управлять всеми объектами компьютера (файловой системой, принтерами и средствами управления учетными записями).	Локально и домен
Операторы архива	Члены группы имеют право архивировать и восстанавливать файловую систему, даже если у них нет полномочий на файловую систему. Но для прямого доступа к файловой системе им должны быть предоставлены явные полномочия. По умолчанию членом группы никто не становится.	Локально и домен
Гости	Группа имеет ограниченный доступ к компьютеру и предназначена для того, чтобы к некоторым ресурсам сети могли обращаться люди, делающие это нерегулярно. Обычно администраторы не разрешают гостевой доступ из-за угрозы безопасности системы. По умолчанию членом локальной группы Гости становится учетная запись пользователя Гость.	Локально и домен

Опытные пользователи	Группа имеет меньше прав, чем группа Администраторы, но больше, чем группа Пользователи. Члены группы могут создавать пользователей и группы, но управлять могут только теми пользователями и группами, которые создали сами. Им также разрешается создавать общие ресурсы и принтеры сети.	Локально
Операторы печати	Члены группы могут управлять принтерами доменов.	Домен
Репликатор	Группа предназначена для репликации каталога, что используется серверами доменов. В эту группу следует включать только тех пользователей доменов, которые запускают службу репликации. По умолчанию членом группы никто не становится.	Локально и домен
Операторы серверов	Могут управлять серверами доменов.	Домен
Пользователи	Группа применяется конечными пользователями, которые должны иметь очень ограниченный доступ к ресурсам системы. По умолчанию членами локальной группы Пользователи становятся все пользователи, созданные на компьютере, кроме Гость.	Локально и домен
Издатели сертификатов	Члены группы могут управлять сертификацией предприятий и агентами возобновления.	Глобально
Администраторы домена	Имеют полные административные права на домен.	Глобально
Компьютеры домена	Группа содержит все рабочие станции и серверы домена.	Глобально

Контроллеры домена	Группа содержит все контроллеры домена.	Глобально
Гости домена	Группа имеет ограниченный доступ к домену и предназначена для того, чтобы к некоторым ресурсам сети могли обращаться люди, делающие это не регулярно.	Глобально
Пользователи домена	Группа содержит всех пользователей домена, и ее члены должны иметь ограниченный доступ к системе.	Глобально
Администраторы предприятия	Группа имеет полные административные права на предприятие. Эта группа должна иметь высший уровень полномочий по сравнению со всеми другими группами.	Глобально
Владельцы создателей групповой политики	Группа обладает полномочиями на модификацию групповой политики домена.	Глобально
Администраторы схемы	Группа обладает специальными полномочиями на модификацию схемы Active Directory.	Глобально

На контроллере домена группы размещаются в папках Users (Пользователи) и Builtin (Встроенные).

Руководство к выполнению.

Работа с локальными учетными записями пользователей

Для работы с локальными учетными записями пользователей в Windows 2000 следует обратиться к утилите *Локальные пользователи и группы* через утилиту *Управление компьютером*. Для этого щелкните правой кнопкой мыши на *Мой компьютер* и выберите *Управление* во всплывающем меню. Откроется окно *Управление компьютером*. Раскройте папку *Локальные пользователи и группы*, чтобы можно было обратиться к папкам *Пользователи* и *Группы*.

Создание новых пользователей

Для создания пользователей на компьютере с Windows 2000

Server нужно войти в систему как пользователь с полномочиями на создание новых пользователей и быть членом группы Администраторы или Опытные пользователи.

Единственным обязательным требованием при создании новых пользователей является указание достоверного имени. Достоверное означает, что оно должно соответствовать правилам для имен пользователей, принятым в Windows 2000.

Правила Windows 2000 для имен пользователей таковы:

- Имя должно содержать от 1 до 20 символов.
- Оно должно отличаться от всех других имен пользователей и групп, хранящихся на данном компьютере.
- Имя пользователя не может содержать следующих символов:

  * / \ [ ] : ; | = , + ? < > “
- Оно не может состоять только из точек или пробелов.

Для создания нового пользователя откройте утилиту *Локальные пользователи и группы*, выделите папку *Пользователи* и выберите *Действие* → *Новый пользователь*. Откроется диалоговое окно *Новый пользователь*.

В этом окне заполните поле *Имя пользователя*. Все другие установки окна необязательны. Текстовые поля и переключатели окна *Новый пользователь* описаны в таблице 3.

Таблица 3. Параметры диалогового окна *Новый пользователь*

ПАРАМЕТР	ОПИСАНИЕ
Пользователь	Определяет имя пользователя для новой учетной записи. Это единственное обязательное поле. В именах регистр символов не учитывается.
Полное имя	Позволяет ввести более подробные сведения о пользователе. Это обычно имя и фамилия пользователя. По умолчанию здесь указывается то же, что и в поле Пользователь.
Описание	Позволяет ввести дополнительную информацию. Это обычно используется для указания звания и/или местонахождения.

Пароль	Назначает начальный пароль для пользователя. Пароли могут иметь длину до 14 символов и учитывают регистр символов.
Подтверждение	Служит для подтверждения введенного пароля.
Требовать смену пароля при следующем входе в систему	Обязывает пользователя изменить пароль при первом вхождении в систему, что делается для повышения безопасности. По умолчанию этот флажок установлен.
Запретить смену пароля пользователем	Это полезно для таких учетных записей, как Гость, и тех, что применяются несколькими пользователями. По умолчанию флажок сброшен.
Срок действия пароля не ограничен	Этот вариант можно выбрать для учетной записи службы, когда изменение пароля излишне. По умолчанию флажок сброшен.
Отключить учетную запись	Показывает, что данную учетную запись нельзя использовать для входа в систему. Этот вариант может быть выбран для учетной записи, не используемой в тот момент. Он обеспечивает защиту неактивных учетных записей. По умолчанию флажок сброшен.

Пользователей можно создавать и утилитой командной строки NET USER. Для получения сведений об этой команде введите NET USER /? в командной строке.

Отключение учетных записей пользователей

Если учетная запись пользователя больше не нужна, ее нужно отключить или удалить. Отключенную учетную запись впоследствии можно включить, восстановив свойства пользователя. Удаленную учетную запись восстановить нельзя.

Учетная запись отключается, если пользователь не работает с ней в течение некоторого времени, например, если служащий уходит в отпуск. Другой причиной отключения является замена одного пользователя другим.

Учетная запись пользователя отключается установкой флажка *Отключить учетную запись* в диалоговом окне свойств пользователя. Чтобы обратить- ся к этому диалоговому окну,

дважды щелкните мышью на учетной записи в папке *Пользователи* утилиты *Локальные пользователи и группы*.

Удаление учетных записей пользователей

Удалять учетную запись следует только тогда, когда точно известно, что она больше не понадобится.

Для удаления пользователя откройте утилиту *Локальные пользователи и группы*, выделите удаляемую учетную запись и щелкните мышью на кнопке *Действие*. В открывшемся меню выберите *Удалить*.

Удаление – операция необратимая, поэтому появится диалоговое окно, предлагающее подтвердить желание удалить учетную запись.

Учетные записи Администратор и Гость удалить нельзя, а учетную запись начального пользователя – можно.

Переименование пользователей

Учетную запись можно переименовать в любой момент. Переименование позволяет сохранить все свойства пользователя.

Для переименования откройте утилиту *Локальные пользователи и группы*, выделите переименовываемую учетную запись и выберите *Действие* → *Переименовать*. Измените имя пользователя и нажмите *Enter*, завершив операцию.

Изменение пароля пользователя

Если какой-то пользователь забыл свой пароль и не может войти в систему, нельзя посмотреть его старый пароль, но администратор может изменить пароль, которым тот и будет пользоваться.

Для изменения пароля откройте утилиту *Локальные пользователи и группы*, выделите учетную запись и выберите *Действие* → *Задать пароль*. Введите новый пароль и подтвердите его. Щелкните ОК.

Работа со свойствами локальных пользователей

Для лучшего управления учетными записями пользователей следует настроить их свойства. В диалоговом окне свойств пользователя можно изменить исходные параметры пароля, добавить пользователей в существующие группы и указать сведения о профиле пользователя.

Чтобы открыть диалоговое окно свойств пользователя, обратитесь к утилите *Локальные пользователи и группы*, откройте папку *Пользователи* и дважды щелкните мышью на учетной записи пользователя. Диалоговое окно свойств пользователя состоит из четырех вкладок, соответствующих классам свойств: *Общие*, *Членство в группах*, *Профиль*, *Удаленный доступ*.

Общие содержит сведения, предоставляемые при создании новой учетной записи пользователя, а также сведения об отключении или включении учетной записи. Для изменения любого из этих параметров существующего пользователя откройте диалоговое окно свойств и внесите изменения на вкладке *Общие*.

Членство в группах используется для организации членства пользователя в группах.

Профиль позволяет настроить среду для пользователя. Профиль пользователя содержит сведения о среде Windows 2000 для конкретного пользователя. К параметрам профиля относятся, например, расположение ярлыков на рабочем столе, цвет экрана, который видит пользователь при входе в систему. По умолчанию при входе пользователя в систему открывается его профиль. При первом входе пользователи получают профиль по умолчанию. В папке Documents and Settings для пользователя создается папка с именем, соответствующим имени входа пользователя. При выходе пользователя из системы все изменения, сделанные им на рабочем столе, сохраняются на локальном компьютере.

Удаленный доступ используется для описания свойств удаленного доступа и ответного вызова. Эти параметры применяются при работе с серверами удаленного доступа и серверами виртуальной частной сети.

Организация членства пользователей в группах

На вкладке *Членство в группах* показаны все группы, к которым принадлежит пользователь. Здесь можно включить пользователя в существующую группу или удалить его из группы. Для включения пользователя в группу щелкните мышью на кнопке *Добавить,* выберите нужную группу, щелкните *Добавить*, а затем ОК. Щелкните мышью на кнопке ОК, закрыв диалоговое окно *Свойства* пользователя.

Для удаления пользователя из группы выделите группу и щелкните мышью на кнопке *Удалить*.

Работа с локальными учетными записями групп

Группы – это важный элемент управления сетью. Грамотные администраторы большую часть своих задач управления выполняют с помощью групп и крайне редко предоставляют полномочия отдельным пользователям.

На рядовых серверах Windows 2000 могут находиться локальные группы, а на контроллерах доменов Windows 2000 в Active Directory – группы безопасности и распространения. По области действия они могут делиться на локальные, глобальные и универсальные.

Для создания локальных групп применяется утилита *Локальные пользователи и группы*, с помощью которой можно создавать, переименовывать и удалять группы, а также менять их состав.

Создание новых локальных групп

Для создания группы необходимо войти в систему как член группы *Администраторы* или *Опытные пользователи*. Группа *Администраторы* обладает всеми полномочиями для работы с пользователями и группами. Члены группы *Опытные пользователи* могут работать только с теми группами, которые они сами создают.

По возможности следует не создавать новых групп, а включать пользователей в состав встроенных локальных групп. Это упрощает работу администратора, так как встроенные группы уже обладают соответствующими полномочиями. Все, что нужно при этом выполнить, - сделать пользователей членами группы.

При создании локальной группы рекомендуется соблюдать следующие правила:

- Имя группы должно быть уникальным для компьютера, т.е. отличаться от имен всех других групп и пользователей компьютера.
- Длина имени группы может составлять 256 символов. Символ обратной косой черты (\) использовать нельзя.

Создание групп похоже на создание пользователей. Откройте утилиту *Локальные пользователи и группы*, щелкните правой кнопкой мыши на папке *Группы* и выберите *Новая группа* во всплывающем меню. На экране появится диалоговое окно *Новая группа*. Единственным обязательным элементом окна является имя группы. При желании можно привести описание группы и добавить (или удалить) членов группы. Введя сведения о новой группе, щелкните мышью на кнопке *Создать*.

Настройка свойств локальных групп

После создания группы можно добавить в нее членов. Пользователь может принадлежать нескольким группам. Добавляются и удаляются пользователи с помощью диалогового окна свойств группы. Откройте его, дважды щелкнув мышью в папке *Группы* утилиты *Локальные пользователи и группы* на нужной группе.

В диалоговом окне свойств группы можно добавить или удалить ее членов. Щелчком мыши на кнопке *Добавить* открывается диалоговое окно *Выбор пользователей и групп*. Здесь выбираются учетные записи пользователей, которых нужно включить

в группу. После этого нужно щелкнуть мышью на кнопке *Добавить*, а затем на кнопке ОК.

Чтобы удалить члена группы, выберите его в списке *Члены* диалогового окна свойств группы и щелкните мышью на кнопке *Удалить*.

Для выбора нескольких расположенных по порядку пользователей для добавления или удаления, щелкните мышью на первом и последнем из них при нажатой клавише Shift. Для выбора нескольких пользователей не по порядку щелкните мышью на каждом из них при нажатой клавише Ctrl.

Переименование групп

Группа, как и учетная запись пользователя, при переименовании сохраняет все свои свойства, в том числе членов и полномочия.

Чтобы переименовать группу, щелкните на ней правой кнопкой мыши и выберите *Переименовать* во всплывающем меню. Переименуйте группу и нажмите Enter.

Удаление групп

Для удаления группы щелкните правой кнопкой мыши и выберите *Удалить* во всплывающем меню. Появится диалоговое окно с предупреждением о том, что после удаления восстановить группу нельзя. Щелкните мышью на кнопке *Да*.

Задание к лабораторной работе.

• Создайте четырех новых пользователей (например, Дима, Саша, Таня, Ира). Для каждого из них снимите флажок «Требовать смену пароля при следующем входе в систему». Для первых двух пользователей пароль не задавайте, для последних установите пароли. После создания всех пользователей выйдите из диалогового окна, щелкнув мышью на кнопке *Закрыть*.

• Отключите учетную запись одного из пользователей. Выйдите из системы и попытайтесь войти с именем отключенного пользователя. Попытка будет неудачна. Войдите в систему как Администратор.

• Удалите одного из созданных ранее пользователей.

• Переименуйте одного из созданных ранее пользователей.

• Измените пароль одного из созданных ранее пользователей.

• Выполните настройку профилей пользователей.

Выберите *Пуск → Программы → Стандартные→ Проводник*, раскройте *Мой компьютер*, затем Диск C: и Documents and Settings. В этой папке будут находиться подпапки только тех

пользователей, которые вошли в систему. Убедитесь, что профили для некоторых пользователей (например, Таня, Ира) не существуют (так как они еще не вошли в систему).

Выйдите как Администратор и войдите как Таня. Щелкните правой кнопкой мыши на незанятой области рабочего стола и выберите *Свойства*. В окне *Свойства экрана* выберите вкладку *Оформление*. Выберите цветовую схему красно-бело-синяя (VGA).

Щелкните правой кнопкой мыши на незанятой области рабочего стола и выберите *Создать* → *Ярлык*. Создайте ярлык с именем CALC.

Выйдите как Таня и войдите как Ира. Обратите внимание: пользователь Ира видит конфигурацию рабочего стола, хранящуюся в профиле по умолчанию.

Выйдите как Ира и войдите как Таня. Обратите внимание: Таня видит конфигурацию рабочего стола такой, какой она была установлена в последний раз.

Выйдите как Таня и войдите как Администратор. Раскройте Documents and Settings. Убедитесь, что теперь для Тани и Иры существуют папки с профилями пользователей.

- Создайте две локальные группы с именами *Пользователи данных* и *Пользователи приложений*.
- Добавьте созданных Вами пользователей в группу *Пользователи данных*.
- Переименуйте группу *Пользователи приложений*.
- Удалите группу *Пользователи приложений*.
- Удалите все созданные группы и пользователей.

Содержание отчета

1. Наименование и цель выполняемой работы.
2. Формулировка задания на лабораторную работу.
3. Описание хода выполнения работы по каждому пункту задания.
4. Выводы по проделанной работе.

Контрольные вопросы

1. Дайте краткое определение учетной записи.
2. Для каких целей используется учетная запись пользователя или компьютера.
3. Назовите встроенные учетные записи и дайте их характеристики.
4. На каких компьютерах могут храниться сведения о локальных пользователях Windows 2000 в их локальной базе данных

учетных записей? Выберите все подходящие варианты.

A. Windows NT 4 Workstation
B. Windows 2000 Professional
C. На рядовых серверах Windows 2000
D. На контроллерах доменов Windows 2000

5. Какая утилита применяется для создания учетных записей пользователей, хранящихся на рядовых серверах Windows 2000?

6. Назовите встроенные группы.

7. Опишите последовательность действий для создания учетной записи пользователя.

8. Опишите последовательность действий для создания группы.

9. Опишите последовательность действий для добавления пользователя в группу.

10. Какая папка применяется по умолчанию для хранения профилей пользователей?

11. Если пользователь должен архивировать и восстанавливать файловую систему, но не должен иметь к ней доступ, в какую группу его следует включить?

12. Какое из следующих прав не предоставляется членам группы Опытные пользователи на рядовых серверах Windows 2000?

A. Создание любых пользователей и групп
B. Удаление любых пользователей и групп
C. Создание сетевых ресурсов
D. Создание сетевых принтеров

13. Какая группа создается на контроллерах доменов Windows 2000 по умолчанию и разрешает членам управлять контроллерами доменов, но не разрешает управлять учетными записями пользователей и групп?

14. Какую утилиту может применить администратор на рядовом сервере Windows 2000 для изменения пароля пользователя?

15. Какая из следующих групп имеет наивысший уровень полномочий в Active Directory?

A. Администраторы
B. Администраторы домена
C. Администраторы предприятия
D. Администраторы Active Directory

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: ДОСТУП К ФАЙЛАМ И ПАПКАМ

Цель работы: изучение технологии управления доступом к локальным и сетевым ресурсам, в том числе конфигурации полномочий NTFS и полномочий на доступ к сетевым папкам.

Теоретические сведения

Локальный доступ определяет возможности пользователя по работе с локальными ресурсами. Для ограничения локального доступа к файлам и папкам NTFS служат полномочия NTFS.

Мощной связанной с работой в сети возможностью является предоставление доступа по сети к локальным папкам. В системе Windows 2000 Server сделать папки совместно используемыми (их также называют разделяемыми или общими) несложно. К совместно используемым папкам разрешается применять политику безопасности так же, как полномочия NTFS. Если Вы обобществили папку, пользователь с соответствующим правом доступа может работать с ней различными способами.

Процедуры управления доступом к файлам и папкам одинаковы для обычных серверов Windows 2000, контроллеров доменов и компьютеров под управлением Windows 2000 Professional.

Управление локальным доступом

В локальных разделах используются обычно файловые системы двух типов: FAT и NTFS. Разделы FAT, в отличие от разделов NTFS, не поддерживают локальной безопасности. Разделы NTFS позволяют определить доступ пользователя к конкретным файлам или папкам в зависимости от его имени и группы.

Полномочия NTFS управляют доступом к папкам и файлам NTFS. Это управление осуществляется путем предоставления или отказа в определенных полномочиях NTFS пользователям и группам. Если полномочия связаны с разрешением доступа, то они кумулятивны и основаны на принадлежности пользователя к группе. Однако если пользователю запрещен доступ (непосредственно или через группу), этот запрет перекрывает разрешения.

ОС Windows 2000 Server предусматривает пять уровней полномочий NTFS:

- Полномочие **Полный контроль** связано со следующими правами:
  - Перемещение по папкам и выполнение содержащихся в них файлов (программ)
  - Чтение содержимого папки и данных в файлах папки

- Просмотр атрибутов файла или папки
- Изменение атрибутов файла или папки
- Создание новых файлов и запись в них данных
- Создание новых папок и добавление данных к файлам
- Удаление вложенных папок и файлов
- Удаление файлов
- Изменение разрешений на доступ к файлам или папкам.
- Принятие файлов или папок в собственность.

• Полномочие **Модификация** предполагает следующие права:

- Перемещение по папкам и выполнение содержащихся в них файлов (программ)
- Чтение содержимого папки и данных в файлах папки
- Просмотр атрибутов файла или папки
- Изменение атрибутов файла или папки
- Создание новых файлов и запись в них данных
- Создание новых папок и добавление данных к файлам
- Удаление файлов

• Полномочия **Чтение и запись, Просмотр содержимого папки** предполагают следующие права:

- Перемещение по папкам и выполнение содержащихся в них файлов (программ)
- Чтение содержимого папки и данных в файлах папки
- Просмотр атрибутов файла или папки

• Полномочие **Чтение** предполагает следующие права:

- Чтение содержимого папки и данных в файлах папки
- Просмотр атрибутов файла или папки

• Полномочие **Запись** предполагает следующие права:

- Изменение атрибутов файла или папки
- Создание новых файлов и запись в них данных
- Создание новых папок и добавление данных к файлам

Любой пользователь с правом полного контроля может управлять безопасностью папки. По умолчанию это право для целого раздела NTFS имеет группа Everyone (Каждый). Кроме того, чтобы обратиться к файлу, пользователь должен иметь физический доступ к компьютеру, а также допустимые входное имя и пароль. По умолчанию обычные пользователи не могут обращаться к папкам по сети, если эти папки не являются совместно используемыми.

Назначение полномочий NTFS

Для назначения полномочий NTFS сделайте следующее:

1. В **Проводнике** щелкните правой кнопкой мыши на файле

или папке, для которой нужно задать полномочия доступа, в открывшемся меню выберите пункт **Свойства** и перейдите на вкладку **Безопасность** диалогового окна свойств.

2. Нажмите на кнопку **Добавить**. Откроется диалоговое окно выбора пользователей, компьютеров и групп. Пользователей локальной базы данных вашего компьютера, вашего домена или доверенных доменов можно выбрать в списке в верхней части окна. Список в нижней части окна содержит всех указанных в верхнем списке пользователей и группы.

3. Щелкните мышью на пользователе, компьютере или группе, которую Вы хотите добавить, и нажмите на кнопку **Добавить**. Соответствующий объект появится в нижнем списке. Для одновременного выбора нескольких пользователей, компьютеров или групп нужно щелкать на них мышью при нажатой клавише Ctrl; если эти объекты идут подряд, можно использовать клавишу Shift.

4. Вернитесь на вкладку безопасности диалогового окна свойств папки. Индивидуально выделите каждого пользователя, компьютер или группу в верхнем списке и укажите применяемые к ним полномочия NTFS. Завершив работу, нажмите на кнопку ОК.

Для удаления полномочия NTFS выделите пользователя, компьютер или группу на вкладке безопасности и нажмите на кнопку **Удалить**. Если полномочия наследуются, необходимо сначала снять флажок **Разрешить распространение на этот объект полномочий, наследуемых от его предка**.

Управление наследованием полномочий

По умолчанию в системе Windows 2000 Server полномочия родительской папки применяются ко всем ее файлам и вложенным папкам. Такие полномочия называются *наследуемыми*. Вкладка безопасности диалогового окна свойств папки позволяет отменить наследование полномочий вложенными папками и файлами путем снятия флажка **Разрешить распространение на этот объект полномочий, наследуемых от его предка**.

Если флажок **Разрешить** или **Запретить** в списке полномочий вкладки безопасности помечен и окрашен серым цветом, это означает, что полномочия наследуются от папки верхнего уровня. Если он только помечен, но не окрашен, то полномочие впервые было применено к данной папке, т.е. назначено явным образом.

Определение эффективных полномочий

Для определения *эффективных прав*, т.е. прав на доступ к папке или файлу, которые пользователь имеет фактически, сложите вместе все полномочия, полученные пользователем непо-

средственно и через группы, в которые он входит. После этого вычтете все полномочия, которые были запрещены пользователю непосредственно и через группы.

Допустим, что пользователь **Ира** входит в состав групп **Учет** и **Приложения**. Эти группы имеют следующие полномочия:

Полномочия группы Учет

Полномочие	**Разрешить**	**Запретить**
Полный контроль		
Модификация	∨	
Чтение и выполнение	∨	
Просмотр содержимого папки		
Чтение		
Запись		

Полномочия группы Приложения

Полномочие	**Разрешить**	**Запретить**
Полный контроль		
Модификация		
Чтение и выполнение		
Просмотр содержимого папки		
Чтение	∨	
Запись		

Для определения эффективных прав Иры нужно объединить назначенные полномочия. В результате оказывается, что данный пользователь имеет права Модификация, Чтение и выполнение и Чтение.

Пусть пользователь **Таня** входит в состав групп **Продажи** и **Временные**. Эти группы имеют следующие полномочия:

Полномочия группы Продажи

Полномочие	**Разрешить**	**Запретить**
Полный контроль		
Модификация		∨
Чтение и выполнение		
Просмотр содержимого папки		
Чтение		
Запись		∨

Полномочия группы Временные

Полномочие	**Разрешить**	**Запретить**
Полный контроль		
Модификация	∨	

Чтение и выполнение ∨
Просмотр содержимого папки ∨
Чтение ∨
Запись ∨

Для определения эффективных прав этого пользователя необходимо выяснить, что ему разрешается делать. Это полномочия Модификация, Чтение и выполнение, Просмотр содержимого папки, Чтение и Запись. Затем следует вычесть то, что запрещено: Модификация и Запись. Таким образом, эффективными правами этого пользователя являются Чтение и выполнение, Просмотр содержимого папки и Чтение.

Управление сетевым доступом

Совместным использованием называется процесс предоставления сетевым пользователям доступа к папке, расположенной на компьютере, который работает под управлением операционной системы Windows 2000 Server. Эта папка называется *совместно используемой* (общая, разделяемая). Сетевой доступ позволяет хранить в одном месте данные, совместно используемые различными людьми. Кроме того, совместное использование позволяет администратору установить приложение только один раз, а не делать это локально на каждом компьютере, и управлять им из одного центра.

Создание совместно используемых папок

Чтобы обобществить папку на сервере или участнике домена Windows 2000, зарегистрируйтесь как член группы Администраторы или Опытные пользователи. Чтобы обобществить папку на контроллере домена Windows 2000, необходимо зарегистрироваться в системе в качестве члена группы Администраторы или Операторы сервера. Совместное использование активизируется и конфигурируется на вкладке Доступ диалогового окна свойств папки. При этом нужно задать параметры, представленные в таблице 1.

Таблица 1. Параметры совместного использования папок

Параметр	**Описание**
Отменить общий доступ	Разрешен только локальный доступ к данной папке
Открыть общий доступ	Разрешен локальный и сетевой доступ к данной папке
Сетевое имя	Описательное имя, по которому пользователи смогут обращаться к папке

Комментарий	Дополнительная описательная информация о совместно используемой папке (заполнять необязательно)
Предельное число пользователей	Максимальное количество одновременных соединений с совместно используемой папкой
Полномочия	Позволяет определить, каким образом пользователи смогут обращаться к папке по сети
Кэширование	Определяет метод кэширования папок при работе в автономном режиме

Если вы совместно использовали папку в течение некоторого времени и затем решили запретить ее обобществление, пометьте переключатель **Закрыть общий доступ к папке** на вкладке **Доступ** диалогового окна свойств папки.

В Проводнике около совместно используемой папки располагается знак руки.

Конфигурирование полномочий совместно используемой папки

Доступ пользователей к разделяемой папке контролируется путем назначения полномочий на нее. *Полномочия на доступ* к совместно используемой папке не столь сложны, как полномочия NTFS, и могут быть применены только к папкам (в отличие от полномочий NTFS, применяемых к папкам и файлам).

Для назначения прав доступа к совместно используемой папке щелкните мышью на кнопке **Полномочия** вкладки **Доступ** диалогового окна свойств папки. Появится диалоговое окно **Полномочия совместно используемой папки**. Полномочия на доступ к совместно используемой папке могут быть трех типов:

- Полный контроль – полный доступ к совместно используемой папке.
- Изменение – пользователи могут изменять данные в файле или удалять файлы.
- Чтение – пользователи могут просматривать и выполнять файлы в совместно используемой папке.

По умолчанию полномочие **Полный контроль** для совместно используемой папки предоставляется группе **Everyone**. Если оно назначено, остальные два полномочия помечаются автоматически.

В совместно используемых папках реализована концепция наследования, отличная от применяемой в папках NTFS. Обобществляя папку, Вы не сможете заблокировать доступ к ресурсам

нижнего уровня с помощью ее полномочий.

Работа с совместно используемыми папками

Создавать и обслуживать совместно используемые папки на компьютере позволяет утилита **Общие папки**, которая входит в состав группы **Управление компьютером**. Окно этой утилиты показывает все созданные на данном компьютере совместно используемые папки, все открытые для каждой папки сеансы пользователей, а также открытые в настоящий момент файлы (последние сгруппированы по пользователям).

Для того чтобы открыть утилиту **Общие папки**, щелкните правой кнопкой мыши на значке **Мой компьютер** на рабочем столе и в появившемся меню выберите пункт **Управление**. В окне **Управление компьютером** разверните пункт **Системные инструменты** и **Общие папки**.

Просмотр совместно используемых папок

Утилита **Общие папки** позволяет просмотреть совместно используемые папки, сконфигурированные на данном компьютере. Для этого выберите пункт **Общие ресурсы**. Помимо созданных Вами папок, Вы увидите также специальные совместно используемые папки Windows 2000, автоматически создаваемые системой для целей администрирования. Если за названием папки следует знак $, это означает, что данная папка скрыта от пользователей, когда они с помощью таких средств, как **Сетевое окружение**, ищут сетевые ресурсы. В зависимости от конфигурации компьютера, можно видеть следующие специальные папки:

• *Буква_диска*$ - совместно используемая папка для корня диска. По умолчанию совместно используется корень любого диска. Так, диск C: представляется совместно используемой папкой C$.

На серверах – участниках домена Windows 2000 и на компьютерах под управлением Windows 2000 Professional доступ к папке *буква_диска*$ имеют только члены групп Администраторы и Операторы архива. На контроллерах доменов Windows 2000, помимо вышеназванных, доступ имеют еще члены группы Операторы сервера.

• Совместно используемая папка ADMIN$ указывает на корневой каталог системы Windows 2000.

• Совместно используемая папка IPC$ позволяет администрировать компьютер удаленно и содержит список его совместно используемых ресурсов. (IPC означает interprocess communication – взаимодействие между процессами).

• Папка PRINT$ позволяет удаленно администрировать

принтеры.

Создание новых совместно используемых папок

Создание новых совместно используемых папок с помощью утилиты **Общие папки** осуществляется следующим образом:

1. Щелкните правой кнопкой мыши на папке **Общие ресурсы** и в открывшемся меню выберите пункт **Новая совместно используемая папка с файлами**.

2. Будет запущен мастер создания совместно используемой папки. Укажите обобществляемую папку (для ее выбора можно использовать кнопку **Обзор**), введите ее имя и описание. Щелкните мышью на кнопке **Далее**.

3. Появится диалоговое окно мастера, в котором можно назначить полномочия на доступ к этой папке. Можно выбрать одно из предлагаемых полномочий или настроить свое собственное. Указав назначаемое полномочие, нажмите на кнопку **Готово**.

4. Откроется диалоговое окно **Создание совместно используемой папки**. Оно подтверждает создание папки. Нажав **Да**, перейдете к созданию следующей папки. Кнопка **Нет** завершит работу мастера.

Чтобы папка перестала быть совместно используемой, достаточно щелкнуть на ней правой кнопкой мыши и в открывшемся меню выбрать пункт **Прекратить совместное использование**.

Просмотр сеансов связи с совместно используемыми папками

Выбрав в утилите **Общие папки** пункт **Сеансы**, можно увидеть список всех пользователей, в настоящий момент работающих с совместно используемыми папками компьютера. Список содержит следующую информацию:

- Имя пользователя, установившего связь с совместно используемым ресурсом
- Название компьютера, с которого установлено соединение
- Операционная система клиента, используемая на его компьютере
- Число открытых им файлов
- Время, в течение которого пользователь работает с ресурсом
- Время простоя для этого соединения
- Установил ли пользователь связь посредством гостевого доступа

Просмотр открытых файлов в утилите Общие папки

Если в утилите **Общие папки** выбрать пункт **Открытые файлы**, то появится список всех файлов, открытых в совместно

используемых папках. Этот список содержит следующую информацию:

- Открытые файлы и пути к ним
- Имена пользователей, работающих с файлами
- Операционные системы, используемые теми, кто работает с этими файлами
- Применяются ли блокировки файлов (блокировки не дают двум пользователям одновременно открыть один файл)
- Используемый режим открытия файла (например, чтение или запись)

Получение доступа к разделяемым ресурсам

Пользователь может обратиться к совместно используемому ресурсу тремя способами:

- С помощью **Сетевого окружения**
- Подключением сетевого диска в **Проводнике**
- Применением утилиты командной строки **NET USE**

Доступ к совместно используемым ресурсам с помощью Сетевого окружения

Чтобы обратиться к совместно используемому ресурсу с помощью **Сетевого окружения**, сделайте следующее:

1. Дважды щелкните мышью на значке **Сетевое окружение** на рабочем столе.
2. Дважды щелкните мышью на пунке **Добавить место в сети**.
3. Будет запущен мастер. Введите местоположение сетевого ресурса. Это может быть путь к совместно используемой сетевой папке, путь HTTP к папке Web или путь FTP к сайту FTP. Для поиска пути можно использовать кнопку **Просмотр**. Указав путь, щелкните мышью на кнопке **Далее**.
4. Введите имя сетевого ресурса. Оно появится в списке сетевых мест.

Подключение сетевого диска с помощью Проводника

Проводник позволяет отобразить сетевой диск на букву диска, так что пользователь сможет работать с ним как с локальным. После создания подключенного диска, доступ к нему можно получить по букве с помощью **Мой компьютер**.

Для подключения сетевого диска сделайте следующее:

1. Откройте Проводник.
2. Выполните команду Сервис → Подключить сетевой диск.
3. Появится диалоговое окно подключения сетевого диска. Укажите букву, которая будет связана с сетевым диском.

4. В раскрывшемся списке Папка выберите сетевую совместно используемую папку, которая будет связана с этой буквой.

5. Чтобы сделать это соединение постоянным (сохранить его и использовать при каждом следующем сеансе работы за компьютером), пометьте флажок **Автоматически подключать при входе в систему**.

6. Если нужно соединиться с папкой с помощью другого имени пользователя, щелкните мышью на подчеркнутой части фразы **Соединиться с помощью другого имени пользователя**. Появится диалоговое окно **Соединиться как**. Введите имя пользователя и пароль, затем щелкните мышью на кнопке ОК.

Использование утилиты командной строки NET USE

Утилита **NET USE** позволяет подключить сетевой диск. Синтаксис этой команды:

net use x: \\имя компьютера\имя совместно используемой папки

Например, следующая команда подключает диск G: к папке AppData на компьютере AppServer:

net use G: \\AppServer\AppData

Доступ к локальным и сетевым ресурсам

Системы локальной и сетевой безопасности работают совместно. То, что разрешается делать пользователю, определяет наиболее ограничивающий доступ. Например, если полномочия по умолчанию для локальной папки раздела NTFS не были изменены, то группа **Everyone** имеет право полного контроля. С другой стороны, если эта локальная папка используется совместно и соответствующие полномочия определяют, что право Чтение имеется только у группы **Sales**, то обратиться к совместно используемой папке смогут только участники группы **Sales**.

Напротив, если локальные полномочия NTFS разрешают чтение этой папки только группе **Managers** и эта папка совместно используется с полномочием по умолчанию, предоставляющим полный доступ группе **Everyone**, работать с ней смогут только члены группы **Managers** и только с правом Чтение, поскольку оно является более ограничивающим.

Предположим, что для папки DATA установлены полномочия NTFS и полномочия доступа к совместно используемой папке, как показано на рис. 1.

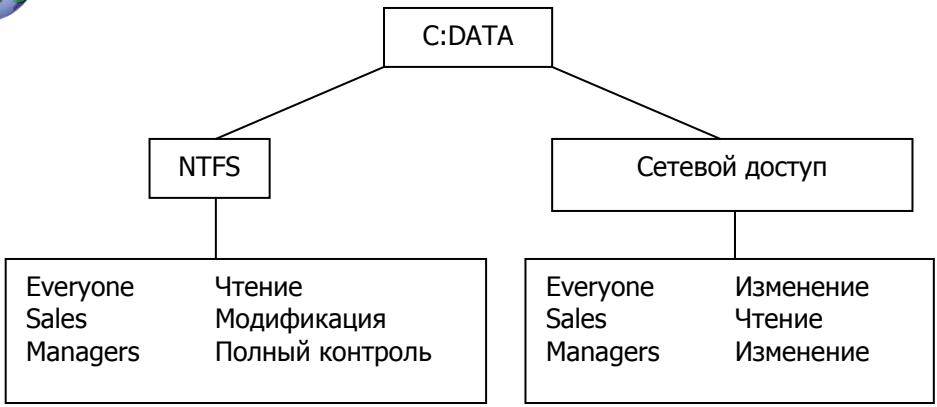


Рисунок 1. Управление доступом в системах локальной и сетевой безопасности.

Допустим также, что пользователь **Ира** входит в группу **Sales** и хочет открыть папку DATA. Обратившись к ней локально, она получит только полномочия NTFS, так что будет иметь право Модификация. Однако, обратившись к папке по сети, она получит более ограничивающее разрешение сетевого доступа Чтение.

Допустим теперь, что пользователь **Миша** входит в группу **Everyone**. Он хочет открыть папку DATA. Делая это локально, он получит право Чтение. Попытавшись сделать это удаленно через сеть, он получит то же самое право. Сетевая папка предоставляет группе **Everyone** право Изменение, но применяется более ограничивающее разрешение (в данном случае это полномочие NTFS Чтение).

Задание к лабораторной работе:

1. Создайте структуру файлов и каталогов. Для этого на диске **C:** создайте новую папку **DATA**. Откройте ее. Создайте в ней две новые папки **WP DOCS** и **SS DOCS** и новый файл **DOC1.TXT**. В папке **WP DOCS** создайте файл **DOC2.TXT**, а в папке **SS DOCS** – файл **DOC3.TXT**.

2. Выполните настройку полномочий NTFS. С помощью утилиты **Локальные пользователи и группы** создайте двух пользователей **Машу** и **Диму**. Снимите пометку с пункта **Пользователь должен сменить пароль при следующей регистрации**.

С помощью утилиты **Локальные пользователи и группы** создайте четыре группы: **Accounting**, **Execs**, **Sales** и **Temps**. Добавьте **Машу** к первым двум группам, а **Диму** – к двум по-

следним.

Чтобы проверить взаимодействие полномочий различных групп, нужно удалить полномочия группы **Everyone**. Для этого откройте свойства папки **C:\DATA** в Проводнике, перейдите на вкладку **Безопасность**. Попробуйте удалить группу **Everyone**. Появится диалоговое окно, информирующее о том, что вы не можете удалить эту группу, так как она наследует полномочия более высокого уровня. Щелкните ОК.

На вкладке **Безопасность** сбросьте флажок разрешения наследования полномочий. В появившемся диалоговом окне нажмите на кнопку **Удалить**.

Для устранения возможных проблем, связанных с полномочиями, добавьте группе Администратор право Полный контроль.

Теперь сконфигурируйте полномочия **NTFS** следующим образом:

- группе **Accounting** разрешите Чтение и выполнение, Запись;
- группе **Execs** разрешите Чтение;
- группе **Sales** разрешите Модификацию;
- группе **Temps** запретите Запись.

Нажав на ОК, закройте окно свойств папки. Появится окно безопасности, предупреждающее о том, что вы запрещаете одно из полномочий. Щелкните мышью на кнопке **Да**.

Выйдите из системы и зарегистрируйтесь как **Маша**. Откройте файл **C:\DATA\DOC1**, внесите изменения и сохраните их. Полномочия этого пользователя позволяют выполнить указанные действия.

Выйдите из системы и зарегистрируйтесь как **Дима**. Откройте файл **C:\DATA\DOC1**, внесите изменения и сохраните их. Полномочия этого пользователя позволят вам открыть файл, но не разрешат сохранить сделанные изменения.

Снова выйдите из системы и зарегистрируйтесь как администратор.

3. Создайте совместно используемую папку. Для этого откройте **Проводник** и создайте на диске **C:** новую папку с именем **Test**. Сделайте ее общей. В качестве сетевого имени папки задайте **Тестовая общая папка**. Укажите предельное число пользователей 5. Нажав на ОК, закройте диалоговое окно.

4. Установите права доступа к совместно используемой папке. Для этого в **Проводнике** откройте диск **C:**.

Щелкните правой кнопкой мыши на папке **Test**, в открывшемся меню выберите пункт **Доступ** и нажмите на кнопку **Пол-**

номочия.

В диалоговом окне полномочий доступа выделите группу **Everyone** и нажмите на кнопку **Удалить**. Затем щелкните мышью на кнопке **Добавить**.

В диалоговом окне **Выбор пользователей, компьютеров и групп** добавьте **Машу** и **Диму**.

Для **Маши** установите полномочие Полный контроль. Для **Димы** – полномочие Чтение. Щелкнув на ОК, закройте диалоговое окно.

5. Получите доступ к сетевым ресурсам с помощью **Сетевого окружения**. Для этого зарегистрируйтесь как пользователь **Маша**. Дважды щелкните мышью на значке **Сетевое окружение** на рабочем столе.

Дважды щелкните мышью на значке **Добавить место в сети**. В мастере нажмите на кнопке **Далее**.

Выберите домен, в котором установлен ваш компьютер. Щелкните мышью на имени своего компьютера. Укажите совместно используемую папку **Test** и нажмите на ОК. Щелкните **Далее**.

Введите имя сетевого ресурса. Оно появится в списке сетевых мест.

Примите предлагаемое по умолчанию имя для сетевого места и нажмите на кнопку **Готово**.

Папка откроется автоматически. Закройте ее. Она появится в списке **Сетевое окружение**.

6. Подключите сетевой диск в **Проводнике**. Для этого выйдите из системы и зарегистрируйтесь как **Дима**.

Дважды щелкните мышью на значке **Сетевое окружение**. Вы не увидите нового сетевого места, которое создали, будучи Машей.

Откройте **Проводник** и выберите команду Сервис → Подключить сетевой диск.

В диалоговом окне подключения сетевого диска примите предлагаемую по умолчанию букву и нажмите на кнопку **Обзор**, чтобы выбрать папку. Укажите домен, в котором установлен ваш компьютер. Щелкните мышью на имени вашего компьютера. Укажите совместно используемую папку **Test** и нажмите на кнопку **Готово**.

7. Выйдите из системы и войдите как Администратор. Удалите все созданные вами папки, файлы, группы, пользователей.

Содержание отчета

1. Наименование и цель выполняемой работы.
2. Формулировка задания на лабораторную работу.
3. Описание хода выполнения работы по каждому пункту задания.
4. Выводы по проделанной работе.

Контрольные вопросы

1. Какая из перечисленных файловых систем поддерживает локальную безопасность в Windows 2000?

A. NTFS
B. FAT16
C. FAT32
D. HPFS

2. Какое из перечисленных прав не связано с полномочием Модификация системы NTFS?

A. Изменение атрибутов папки или файла
B. Просмотр папок и выполнение содержащихся в них файлов
C. Принятие файлов или папок в собственность
D. Удаление файлов

3. К каким двум из перечисленных объектов можно применить полномочия NTFS?

A. Принтеры
B. Совместно используемые папки
C. Файлы
D. Папки

4. Какой наименьший уровень пользователя или группы может по умолчанию изменять полномочия папки NTFS?

A. Администратор
B. Администратор домена
C. Опытный пользователь
D. Everyone

5. Какое полномочие применяется по умолчанию к вложенным папкам, когда вы назначаете полномочие NTFS родительской папке?

A. Полный контроль
B. Чтение
C. То же полномочие, которое применено к родительской папке
D. Вам предлагается указать, какое полномочие нужно при-

менить

6. Какие две группы могут создавать совместно используемые папки в контроллерах доменов Windows 2000?

A. Опытные пользователи
B. Опытные операторы
C. Операторы сервера
D. Администраторы

7. Какое из перечисленных полномочий не относится к доступу к совместно используемой папке?

A. Чтение
B. Запись
C. Изменение
D. Полный контроль

8. С помощью какой утилиты можно просмотреть все папки, совместно используемые на компьютере под управлением Windows 2000?

A. Общие папки
B. Управление файлами
C. Проводник
D. Управление доступом

9. Какая специальная папка позволяет осуществлять удаленное администрирование компьютера и используется для просмотра его разделяемых ресурсов?

A. ADMIN$
B. WINNT$
C. IPC$
D. NET$

10. Какие две группы имеют полномочия создавать совместно используемые папки на серверах – участниках Windows 2000?

A. Опытные пользователи
B. Опытные операторы
C. Операторы сервера
D. Администраторы

11. Пользователь Олег назначил участникам группы Managers полномочие NTFS Чтение на доступ к папке D:\DATA. Какое право будет дано по умолчанию участникам этой группы на доступ к папке D:\DATA\1999?

A. Полный контроль
B. Модификация
C. Чтение
D. Запись

12. Какая утилита командной строки может применяться для

доступа к совместно используемой сетевой папке?

A. net share
B. net use
C. net access
D. net manage

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: КОМАНДНЫЙ РЕЖИМ УПРАВЛЕНИЯ СЕТЬЮ

Цель работы: изучение команд net и освоение методов управления сетью с помощью этих команд, знакомство с тестовыми утилитами стека протоколов TCP/IP.

Руководство к выполнению

Команда

net help

выводит список всех возможных команд net.

Команда

net help имя команды

выводит справку о назначении и параметрах данной команды.

Утилиты для тестирования IP-соединения

Протокол TCP/IP снабжен несколькими утилитами для тестирования адресов сети. С помощью этих утилит можно определить время реакции на запрос и путь к серверу.

Утилита **ping** позволяет проверить наличие связи с запрашиваемым узлом и определить время отклика сервера. Чтобы использовать эту утилиту необходимо в командной оболочке набрать команду **ping** и IP – адрес узла сети.

Утилита **tracert** помогает определить путь, по которому Ваш пакет добирается до другого узла. Команда **tracert** перечисляет все промежуточные узлы, через которые пакет двигался к указанному узлу, а также сообщает время, затраченное на прохождение каждого промежуточного узла.

Утилита **Ipconfig** позволяет определить IP – адрес Вашего компьютера и параметры конфигурации хоста.

Задание к лабораторной работе

Изучите команды net.

В командном режиме выполните следующие действия:

1. Посмотрите список глобальных групп на сервере. Добавьте глобальную группу. Добавьте пользователя в группу. Убедитесь, что изменения действуют. Удалите пользователя. Удалите группу. Убедитесь, что удаление выполнено.

2. Выведите список учетных записей пользователей локального компьютера. Добавьте пользователя с паролем. С помощью утилиты **Мой компьютер** посмотрите свойства введенного пользователя. Отключите учетную запись пользователя и про-

верьте, как изменились свойства пользователя. Удалите пользователя, убедитесь, что изменения действуют.

3. Посмотрите список локальных групп. Добавьте новую группу. Добавьте пользователей в группу. Посмотрите членов группы. Удалите пользователей из группы. Удалите группу.

4. Посмотрите параметры входа в сеть, измените длину пароля (установите 0), добавьте нового пользователя без пароля, установите исходную длину пароля (7), убедитесь, что изменения действуют (попытайтесь добавить нового пользователя без пароля).

5. Пошлите сообщение всем узлам сети. Пошлите сообщение конкретному компьютеру, задав на этом компьютере имя для получения сообщений.

6. Посмотрите список общих ресурсов компьютера. Создайте папку, сделайте ее общей. Посмотрите список общих ресурсов. Прекратите совместное использование папки, удалите ее с помощью утилиты **Мой компьютер**.

7. Посмотрите список запущенных служб.

8. Подключите компьютер к совместно используемой папке Info на сервере. Отключите от папки Info.

9. Наберите команду **ping** и нажмите Enter. Прочитайте текст справки. С помощью команды **ping** проверьте IP - адрес Вашего сервера. Запомните время отклика, сообщенное командой **ping**. Повторите команду **ping** несколько раз, чтобы выяснить, изменяется ли время, сообщаемое командой.

10. Наберите команду **tracert**, затем нажмите клавишу Enter. Прочитайте текст справки. Наберите IP – адрес сервера сети или его имя. Запишите промежуточные узлы, через которые пакет двигался к указанному серверу, и время, затраченное на прохождение каждого промежуточного узла.

11. Наберите команду **Ipconfig/?**, затем нажмите ENTER. На экране появится список параметров команды **Ipconfig**. Наберите команду **Ipconfig/All** и нажмите ENTER. На экране появится список атрибутов IP – адреса.

Содержание отчета

1. Наименование и цель выполняемой работы.
2. Формулировка задания на лабораторную работу.
3. Описание хода выполнения работы по каждому пункту задания.
4. Выводы по проделанной работе.

Контрольные вопросы

1. Какая сетевая команда используется для создания учетной записи пользователя?
2. Какая сетевая команда используется для создания локальной группы (глобальной группы)?
3. Какой командой можно добавить пользователя в группу?
4. Какая команда позволяет просмотреть настройки входа в сеть?
5. Какой командой можно изменить длину пароля?
6. Какая команда позволяет объявить ресурс общим? Каков синтаксис этой команды?
7. Какая команда позволяет получить доступ к общему ресурсу?
8. Для чего используется команда ping?
9. Что можно получить в результате выполнения команды tracert ?

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: ИЗУЧЕНИЕ РАБОТЫ КОНЦЕНТРАТОРА И КОММУТАТОРА В СРЕДЕ CISCO PACKET TRACER

Цель: Изучить программное средство для моделирования сетей — Cisco Packet Tracer, получить базовые навыки проектирования структуры локальной сети, изучить работу концентратора и коммутатора.

Руководство к выполнению

1. Ознакомление с интерфейсом программы Cisco Packet Tracer

Packet Tracer — эмулятор сети передачи данных, выпускаемый фирмой Cisco Systems — одним из крупнейших производителей сетевого оборудования.

Интерфейс Cisco Packer Tracer может быть переключён между физическим и логическим представлениями сети (рис. 1).

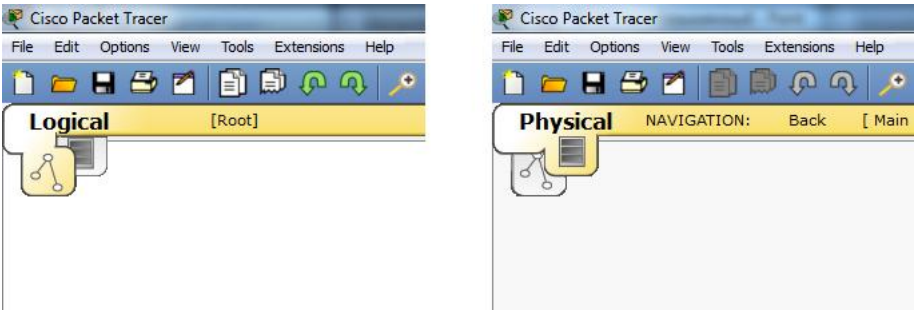


Рис. 1. Вид интерфейса программы Cisco Packer Tracer

В нижней части экрана имеется возможность переключения режимов работы сети:

— Realtime — режим реального времени. В данном режиме моделируется обычный режим работы сети, аналогичный по временным характеристикам работе реального оборудования.

— Simulation — режим симуляции позволяет вручную управлять наступлением очередного события, связанного с передачей данных по сети.

В нижней части экрана имеется меню, в котором представлено оборудование, эмуляция которого возможна в Packet Tracer.

— Routers — маршрутизаторы;
— Switches — свитчи (сетевые коммутаторы);
— Hubs — хабы (концентраторы);
— Wireless Devices — беспроводные устройства;
— Connections — линии связи;
— End Devices — конечные устройства (компьютеры, ноутбуки, телефоны, планшетные ПК);
— Wan Emulation — средства эмуляции глобальных сетей;
— Custom Made Devices — устройства, созданные пользователем;
— Multiuser Connections — средства эмуляции многопользовательских соединений.

2. Построение простейшей сети

Построим сеть, объединяющую 4 компьютера.

Для этого запустим программу Cisco Packet Tracer и в меню выбора устройств нажмем "End Devices", в появившемся списке оконечных устройств выберем значок компьютера. Расположим на схеме сети 4 таких компьютера (см. рис. 2).

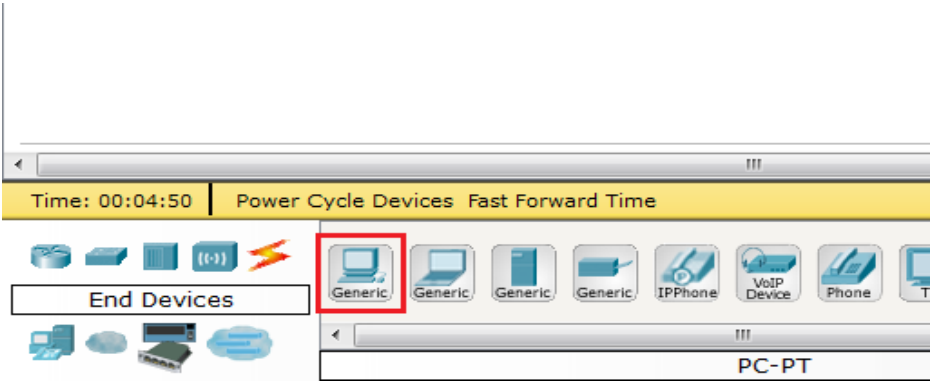


Рис. 2. Выбор конечного оборудования в меню программы Cisco Packet Tracer

Далее в списке "Hubs" выберем первое из доступных устройств — хаб и расположим его на схеме (см. рис. 3).

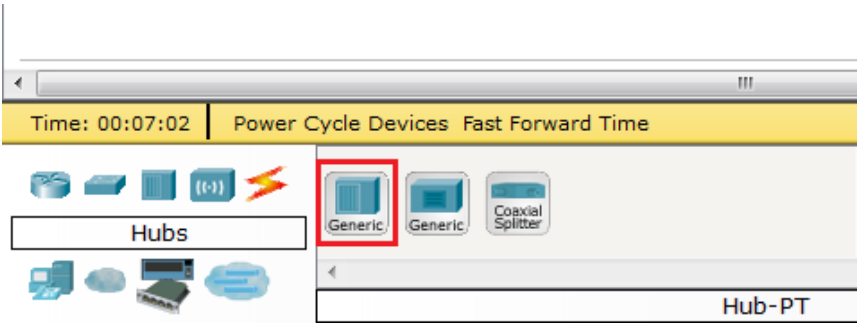


Рис. 3. Выбор хаба в меню программы Cisco Packet Tracer

Теперь необходимо соединить все компьютеры с хабом. Для этого нажмем на пункт “Connections” в списке доступных устройств и выберем “Copper Straight-Through”, что соответствует медному кабелю витой пары (см. рис. 4).

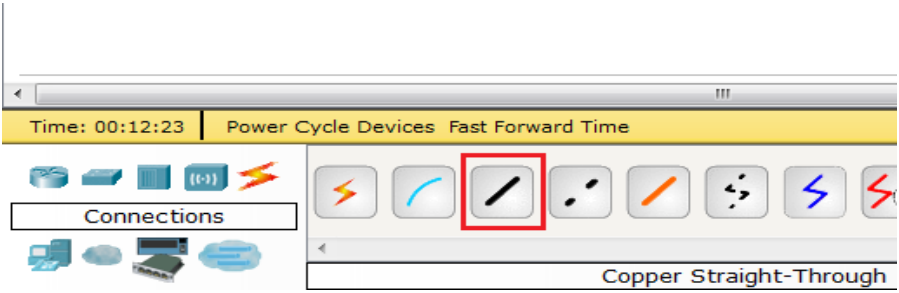


Рис. 4. Выбор кабеля для соединения устройств сети

Щелкнем на компьютере и в появившемся меню выберем соответствующий порт, к которому необходимо подключить кабель, — FastEthernet. Затем нажмем на хаб и аналогичным образом выберем один из его портов (см. рис. 5).

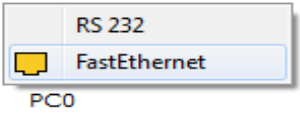


Рис. 5. Выбор порта компьютера

В результате необходимо получить сеть, представленную на рисунке 6.

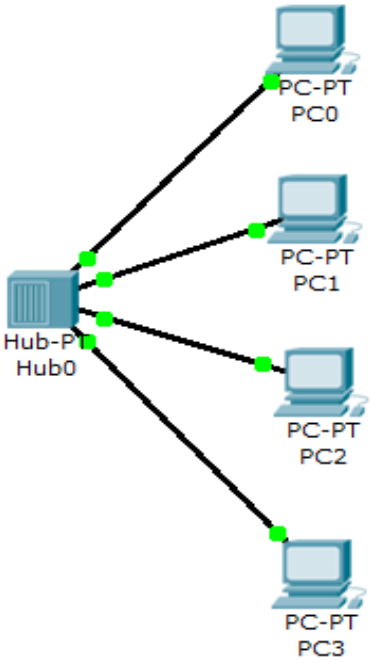


Рис. 6. Вид построенной сети

После физического соединения компьютеров необходимо присвоить каждому из них IP-адрес. Для этого нажмем один раз на компьютер — в результате откроется окно свойств данного компьютера (см. рис. 7).

Рис. 7. Вид окна свойств компьютера

Выберем “IP Configuration” и введем IP-адрес и маску сети в соответствии с вариантом задания.

Для проверки связи между компьютерами используем команду

ping адрес

где адрес — IP адрес одного из компьютеров в сети.

Выполнять данную команду необходимо в командной строке. Для этого в окне компьютера выберем Command Promt (см. рис. 8).

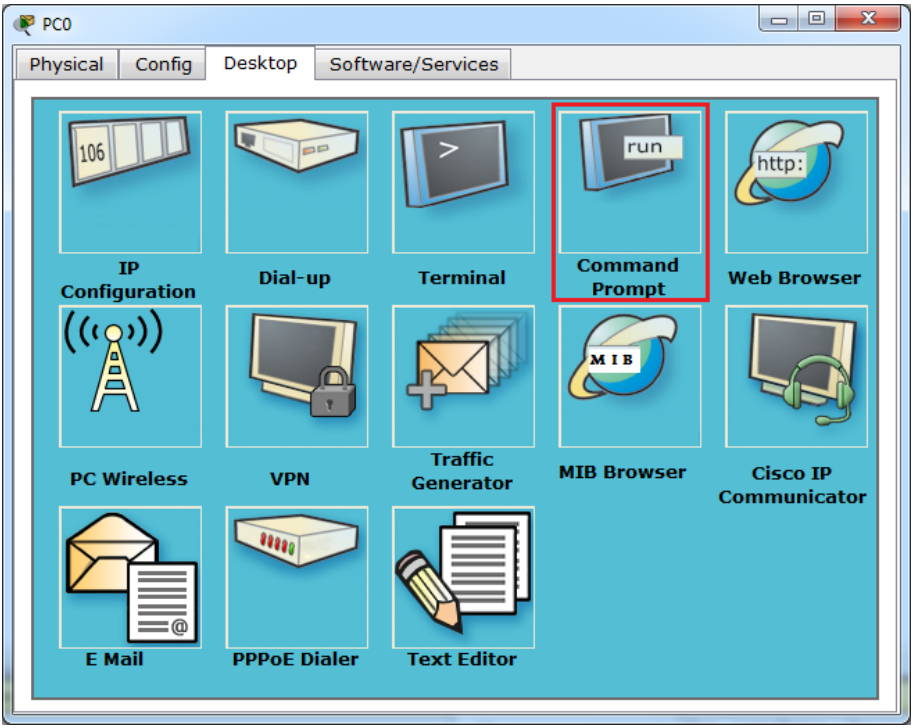


Рис. 8. Выбор режима «Командная строка»

3. Изучение работы концентратора 1-го уровня (хаба)

Для просмотра пакетов, передаваемых по сети перейдем в режим симуляции (Simulation) (см. рис. 9).

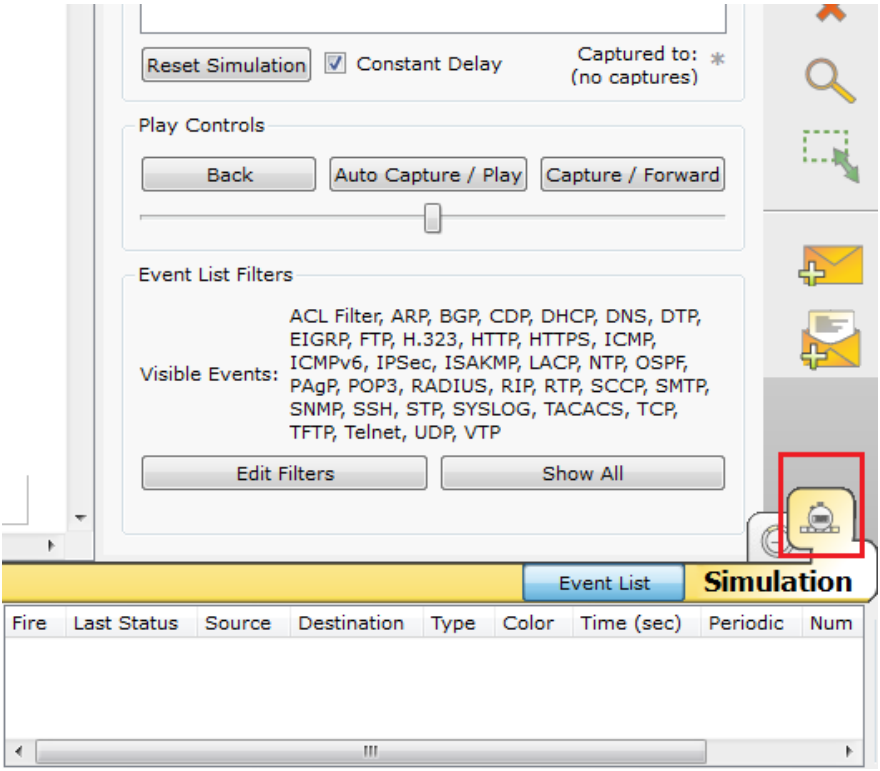


Рис. 9. Выбор режима симуляции

Выполним команду ping на компьютере, на котором не выполняли её ранее. При этом на схеме сети возле данного компьютера должны появиться значки двух пакетов — ARP-пакета и ICMP-пакета.

Команда ping использует протокол ICMP (Internet Control Message Protocol — протокол межсетевых управляющих сообщений), выполняющий сервисные функции, в том числе проверку доступности узла сети. Узел при этом задаётся своим IP-адресом, однако для доставки ему Ethernet-кадра необходимо знать MAC-адрес. Для получения MAC-адреса узла по его IP-адресу используется протокол ARP (Address Resolution Protocol — протокол определения адреса) (см. рис. 10).

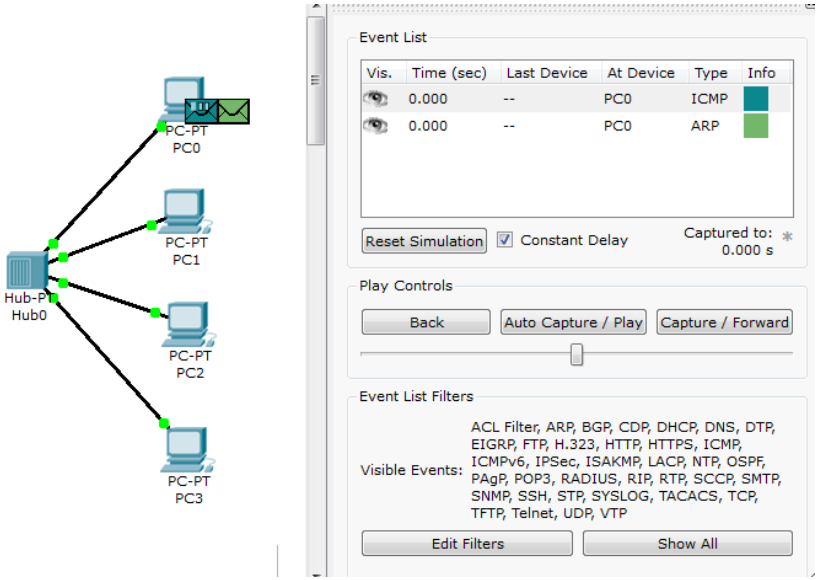


Рис. 10. Визуализация выполнения команды ping

Если нажать на изображение пакета или на поле Info в окне “Event List”, откроется окно с подробной информацией о пакете (см. рис. 11).

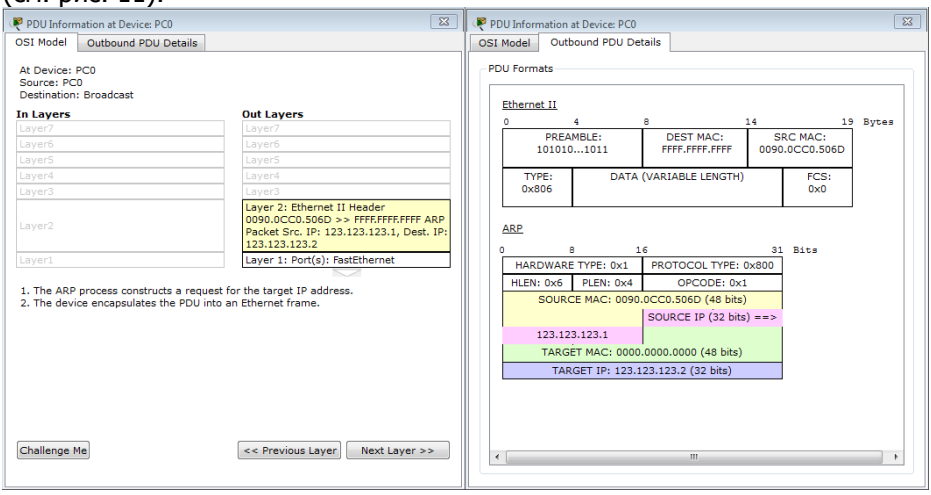


Рис. 11. Информация о пакете

Нажмем кнопку “Capture / Forward” и понаблюдаем за передачей пакетов по сети.

После окончания симуляции проверим ARP-таблицу компьютера, на котором выполнялась команда ping. Для этого откро-

ем на нём командную строку и введем

arp -a

4. Построение сети на основе коммутатора 2-го уровня (свитча)

В построенной схеме сети заменим хаб на свитч. Для этого в списке оборудования нажмем "Switches" и выберем первый в списке свитч (см. рис. 12).

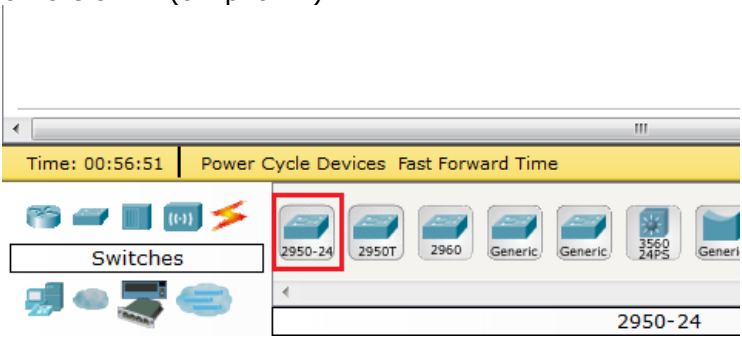


Рис. 12. Выбор свитча

Выполним действия, аналогичные описанным выше.

Задание на лабораторную работу

1. Постройте сеть на базе концентратора, как описано выше. Изучите работу концентратора и опишите пути передачи пакетов и содержимое их заголовков.

2. Постройте сеть на основе коммутатора 2-го уровня (свитча). Изучите работу коммутатора. Опишите различия в передаче пакетов хабом и свитчем.

Варианты задания

Вариант	IP-адрес сети
1,2	200.200.200.152/29
3,4	200.200.200.208/28
5,6	200.200.200.128/27
7,8	200.200.200.192/26
9,10	200.200.200.128/25
11,12	150.100.96.0/23
13,14	150.100.136.0/22
15,16	150.100.160.0/21
17,18	150.100.192.0/20
19,20	150.100.128.0/19
21,22	150.100.64.0/18

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: КОНФИГУРИРОВАНИЕ МАРШРУТИЗАТОРА

Цель работы: получение навыков конфигурирования маршрутизатора (роутера) от компании Cisco с помощью программного пакета **Cisco Packet Tracer**, ознакомление с различными уровнями доступа к маршрутизатору, командами, используемыми в разных режимах.

Руководство к выполнению

Сетевым оборудованием, выполняющим функции маршрутизации, является маршрутизатор (router).

Все маршрутизаторы, представленные в Cisco Packet Tracer, построены по модульному принципу и позволяют использовать модули для подключения к сетям различных типов (см. рис. 1).

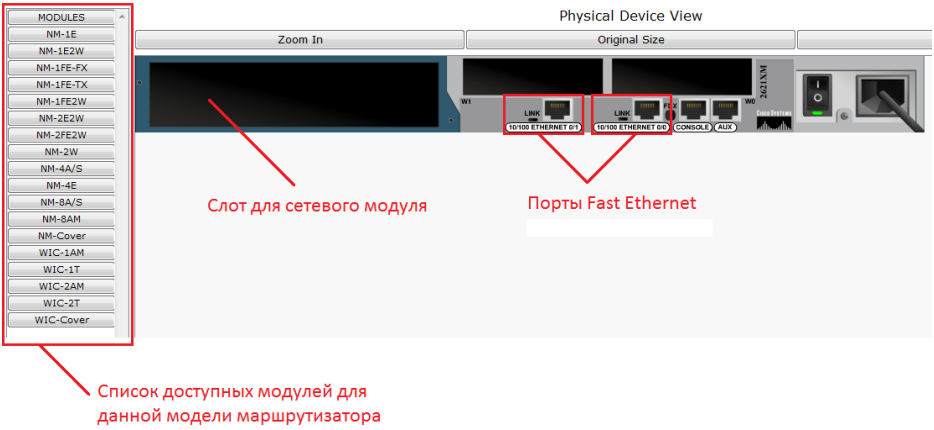


Рис. 1. Вид физического устройства маршрутизатора

Чтобы добавить модуль к маршрутизатору:

1. Выключите питание маршрутизатора.
2. Выберите необходимый сетевой модуль. Для сетей стандарта Fast Ethernet можно выбрать один из следующих модулей:
   — NM-1FE2W — включает 1 Fast Ethernet порт;
   — NM-2FE2W — включает 2 Fast Ethernet порта.
3. Перетяните мышкой изображение модуля из нижнего правого угла в подходящий слот маршрутизаора.
4. Включите питание.

После построения инфраструктуры сети необходимо настроить маршрутизаторы:

1. Для работы в сетях, к которым непосредственно подключён маршрутизатор;
2. Для осуществления маршрутизации между сетями.

Настройка маршрутизатора осуществляется в режиме командной строки (см. рис.2).

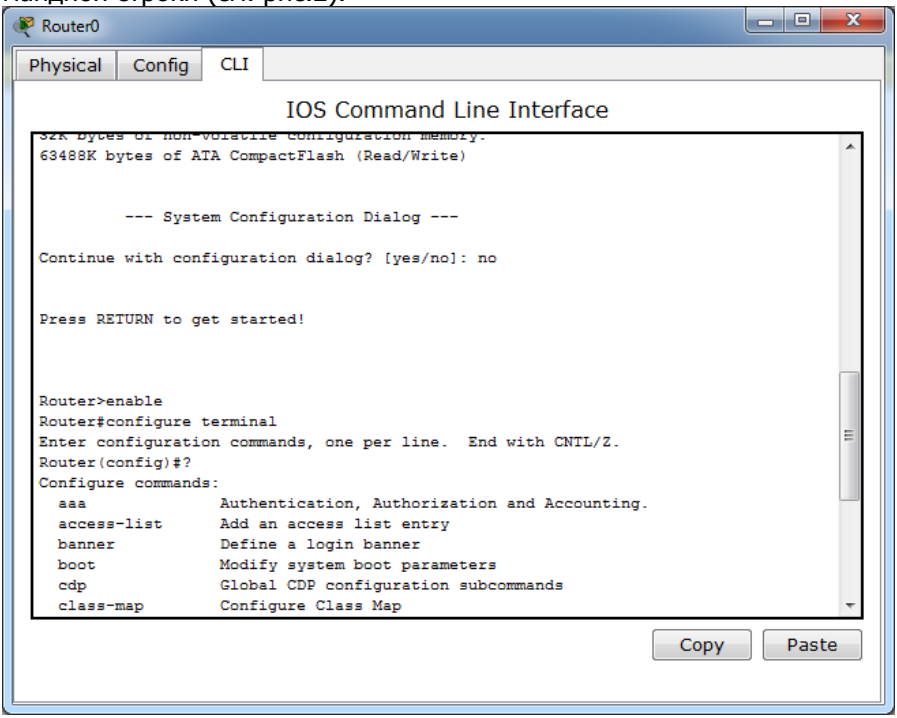


Рис. 2. Вид командного интерфейса маршрутизатора

Существуют 2 режима доступа к маршрутизатору – пользовательский и привилегированный.

Пользовательский режим идентифицируется знаком '**>**' после имени роутера. В этом режиме можно просмотреть настройки роутера, но нельзя внести в них изменения.

В привилегированном режиме (режим определяется знаком '**#**') вы получаете полное управление маршрутизатором и можете изменять его настройки.

Для просмотра всех команд, доступных в данном режиме, следует набрать '**?**' и нажать клавишу <**enter**>. На экране появится список всех доступных команд для роутера в текущем режиме. Можно также использовать знак вопроса после того, как вы начали набирать команду. Например, если хотите использовать команду **show**, но не помните как ее применить, наберите **show**

? и получите все разновидности команды **show**.

В последней строке после выведенной информации может появиться слово

--More--

--More-- означает, что есть еще информация, относящаяся к последней команде. Чтобы просмотреть ее построчно, нажмите enter, для постраничного просмотра нажмите space bar. Чтобы завершить вывод и вернуться в консоль маршрутизатора, нажмите e, что соответствует команде exit.

Команда **'show version'** позволяет получить более полную информацию о маршрутизаторе, такую как тип платформы маршрутизатора, время последней загрузки операционной системы и размещение файла образа ОС, объем памяти, число интерфейсов маршрутизатора, содержимое регистра конфигурации.

В буферной памяти роутера сохраняются 10 последних команд, которые можно просмотреть с помощью команды **'show history'**:

Это облегчает восстановление или исправление вводимых команд. Можно восстановить команду, нажав 'стрелку вверх' (для получения предыдущей команды) или 'стрелку вниз' (для получения следующей команды).

Маршрутизатор имеет свои собственные часы, которые можно использовать для синхронизации устройств. Для просмотра времени применяется команда '**show clock**':

Маршрутизатор может иметь различные типы интерфейсов, такие как token ring, FDDI, ethernet, serial, ISDN и другие. Часто нас интересует состояние и настройки интерфейсов маршрутизатора. Команда '**show interfaces**' выведет детальную информацию обо всех сконфигурированных интерфейсах роутера:

Router1#show interfaces

FastEthernet1/0 is administratively down, line protocol is down (disabled)

Hardware is Lance, address is 00e0.f986.b301 (bia 00e0.f986.b301)

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00,

Здесь вы видите, что интерфейс Ethernet 0 административно отключен (administratively down). Это значит, что он выключен с помощью команды '**shutdown**'. Возможные состояния интерфейса представлены в таблице 1.

Таблица 1. Возможные состояния интерфейса

Ethernet 0 is	Line protocol is	Значение
administratively down	down	Интерфейс выключен командой '**shutdown**'
up	down	Кабель подсоединен, но передача данных не поддерживается.
down	down	Проблема с кабелем или нет синхронизации. Или другой интерфейс роутера выключен.
up	up	Подсоединен и поддерживается передача. Это то, что нам требуется!!!

Команда **'show protocols'** позволяет просмотреть состояние протоколов маршрутизации и других протоколов, сконфигурированных в настоящее время на маршрутизаторе:

Router>show protocols
Global values:
Internet Protocol routing is enabled

BRI0 is administratively down, line protocol is Down
Ethernet0 is administratively down, line protocol is Down

Serial0 is administratively down, line protocol is Down

Здесь указывается, что на маршрутизаторе доступен протокол IP, интерфейсы BRI0, Ethernet0, Serial0 отключены администратором и соответствующие протоколы отключены.

Из привилегированного режима можно войти в режим конфигурирования командой '**conf t**'. Выйти из режима конфигурирования можно, набрав команду '**end**' или **<ctl>+Z**.

В режиме конфигурирования можно сконфигурировать интерфейсы маршрутизатора: назначить им ip - адреса и включить их.

Основные команды конфигурирования маршрутизатора Cisco IOS:

enable или en — переход в привилегированный режим.

configure terminal или conf t — переход в режим конфигурирования.

interface название номер — переход в режим настройки оп-

ределённого интерфейса.

пример: interface FastEthernet0/0

ip address адрес маска — задаёт IP-адрес текущего интерфейса

пример: ip address 192.168.1.1 255.255.255.0

no shutdown — включает интерфейс

exit — выход из текущего режима

write mem — запись текущей конфигурации в память

Задание к лабораторной работе

1) В программе **Cisco Packet Tracer** добавить маршрутизатор в рабочей области.

2) Скомпоновать маршрутизатор так, чтобы у него было 3 интерфейса FastEthernet.

3) Войти в командный режим работы с маршрутизатором.

4) Посмотреть список доступных команд.

5) Войти в привилегированный режим и посмотреть список доступных команд.

6) Посмотреть все разновидности команды **show** в привилегированном режиме.

7) Посмотреть текущее состояние интерфейсов маршрутизатора с помощью команды.

Ответить на следующие вопросы:

- какие интерфейсы имеет маршрутизатор,
- какова их конфигурация.

8) Вывести информацию о текущих протоколах маршрутизатора. Ответить на следующие вопросы:

- какие протоколы доступны на маршрутизаторе;
- сколько интерфейсов включено и сколько отключено администратором.

9) Просмотреть список всех сохраненных в памяти роутера команд. Сколько команд было вами введено?

Вывести время и дату маршрутизатора.

10) Сконфигурировать один из интерфейсов маршрутизатора, назначив ему ip - адрес 10.1.1.1 и маску . 255.255.255.0.

11) Выйти из режима конфигурирования интерфейсов и просмотреть текущую конфигурацию интерфейсов.

12) Набрать команду, которая вернет вас в пользовательский режим.

Содержание отчета

1. Наименование и цель выполняемой работы.

2. Формулировка задания на лабораторную работу.
3. Описание хода выполнения каждого пункта задания и ответов на вопросы.
4. Выводы по проделанной работе.

Контрольные вопросы

1. Какие существуют режимы работы с маршрутизатором? Как просмотреть все доступные команды в данном режиме?
2. Какая команда используется для входа в привилегированный режим?
3. Что нужно набрать, чтобы получить список всех доступных команд Show?
4. Какая команда позволяет просмотреть текущую конфигурацию интерфейсов маршрутизатора?
5. С помощью какой команды можно вернуться в пользовательский режим?
6. Как просмотреть список всех сохраненных в памяти роутера команд?
7. В чем состоит процедура конфигурирования интерфейсов маршрутизатора?

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: ПОСТРОЕНИЕ ТОПОЛОГИИ СЕТИ

***Цель работы**:* изучение основ проектирования составной сети, объединяющей несколько подсетей, с помощью программного пакета Cisco Packet Tracer.

Руководство к выполнению:

Необходимо спроектировать большую сеть. В качестве маршрутизаторов, использующихся в этой сети, применяются роутеры от компании Cisco. Также известна подсеть, которую выделил провайдер.

Сначала необходимо построить топологию сети. Запустите программу **Cisco Packet Tracer** и постройте сеть, показанную на рис. 1. Сеть включает 2 подсети, организованные с помощью коммутаторов, и объединенные маршрутизаторами.

Будем считать, что связь между маршрутизаторами и конечными подсетями происходит с помощью технологии Fast Ethernet. Подразумеваются резервные связи между маршрутизаторами.

Сохраните созданную топологию в файл topology и закройте программу.

Теперь нужно разбить сеть, выданную провайдером, на мелкие подсети. Причем разбить рационально, чтобы гарантированно хватило IP-адресов для каждого компьютера в конечной сети. Построенная сеть включает 5 подсетей, для которых необходимо выделить IP-адреса.

Предположим, что провайдер продал нам сеть 195.48.0.0/16. Число 16 задает длину маски сети (число единичных разрядов в маске). Пусть для конечных подсетей (их две) будет использована маска 255.255.192.0, а для соединений маршрутизаторов хватит маски 255.255.255.252 (реально потребуется занять всего два IP-адреса из подсети). В итоге первого разбиения на 4 подсети получились следующие сегменты:

195.48.0.0/18
195.48.64.0/18
195.48.128.0/18
195.48.192.0/18

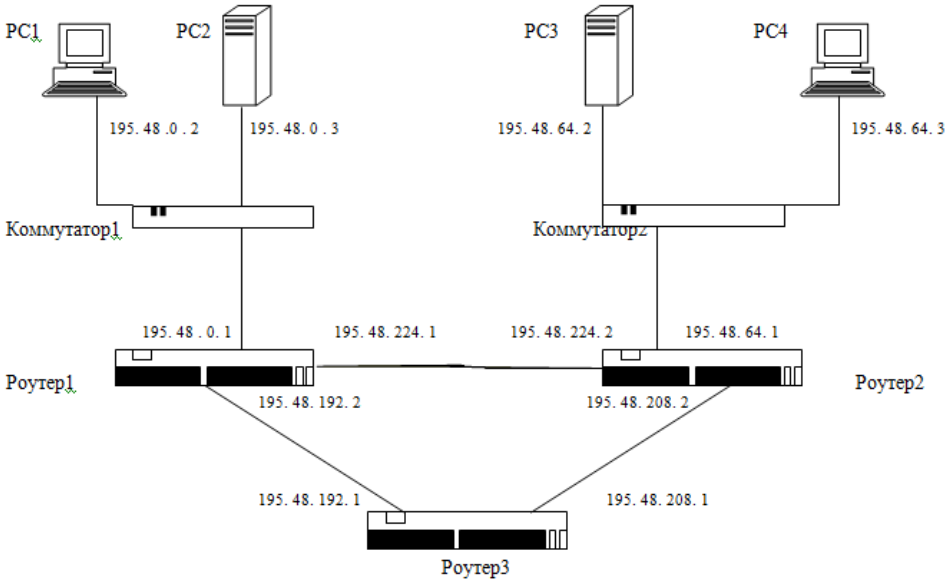


Рисунок 1. Схема сетевой топологии.

Теперь возьмем одну из подсетей и раздробим ее на 3 более мелкие. Пусть это будет сеть 195.48.192.0/18. После разбиения получим еще четыре сегмента:

195.48.192.0/30
195.48.208.0/30
195.48.224.0/30
195.48.240.0/30

Теперь решим, какие сегменты мы применим к нашей топологии. Пусть для конечных сетей будут использованы подсети 195.48.0.0/18 (ROUTER1, PC1, PC2), 195.48.64.0/18 (ROUTER2, PC3, PC4), 195.48.192.0/30 (ROUTER1, ROUTER3), 195.48.208.0/30 (ROUTER2, ROUTER3) и 195.48.224.0/30 (резервный канал между ROUTER1 и ROUTER2). Для удобства все данные занесем в таблицу:

№ подсети	Адрес подсети	Устройства в подсети
1	195.48.0.0/18	ROUTER1, PC1, PC2

2	195.48.64.0/18	ROUTER2, PC3, PC4
3	195.48.192.0/30	ROUTER1, ROUTER3
4	195.48.208.0/30	ROUTER2, ROUTER3
5	195.48.224.0/30	ROUTER1, ROUTER2

Задание к лабораторной работе:

Изучите данные методические указания.

Выполните построение топологии составной сети, как описано выше.

Содержание отчета

1. Наименование и цель выполняемой работы.
2. Формулировка задания на лабораторную работу.
3. Топология сети с указанием на схеме ip – адресов и номеров портов всех интерфейсов, ip – адресов и масок подсетей.
4. Выводы по проделанной работе.

Контрольные вопросы

1. Каким образом исходная сеть разбивается на несколько подсетей.
2. Сколько подсетей определено в построенной составной сети.
3. Какие устройства и какие ip – адреса включает каждая подсеть.
4. Сколько узлов может содержать сеть, имеющая маску длины 30. Сколько бит ip – адреса выделяется под номера узлов в сети.

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: КОНФИГУРИРОВАНИЕ ИНФОРМАЦИОННОЙ СЕТИ

***Цель работы**:* изучение основ конфигурирования составной сети, объединяющей несколько подсетей, с помощью программного пакета **Cisco Packet Tracer**.

Руководство к выполнению:

Выполним практическое конфигурирование составной сети, топология которой была построена на предыдущем занятии. При этом на всех интерфейсах маршрутизаторов и конечных узлов надо прописать соответствующие ip-адреса, которые указаны на схеме сети (смотри рис. 1 в лабораторной работе «Построение топологии сети»).

Начнем с центрального маршрутизатора. На двух его портах необходимо прописать ip-адреса 195.48.192.1/30 и 195.48.208.1/30.

Запустите программу **Cisco Packet Tracer** и загрузите сохраненную схему сети.

Выполните конфигурирование портов маршрутизатора Router3, назначив всем его интерфейсам соответствующие ip-адреса. После задания ip-адреса не забудьте включить интерфейс, который по умолчанию находится в выключенном состоянии. Проверьте правильность своих действий с помощью команды '**show interfaces**'. Проанализируйте настройки интерфейсов. Обязательно проверьте соответствие портов на схеме и в конфигурации, а также правильность адресов и масок.

По аналогии настройте все остальные маршрутизаторы.

После настройки маршрутизаторов выполните настройку конечных узлов, назначив интерфейсу каждого компьютера соответствующий ip-адрес.

Свитчи (коммутаторы) в эмуляторе также являются управляемыми, но по умолчанию пропускают пакеты куда надо без каких-либо ограничений. Поэтому коммутаторы можно не настраивать.

Теперь проверьте работоспособность всех устройств. Для проверки запустите стандартную команду **ping ip_address**. Сначала запустите эту команду из конечных станций. Например, проверяем связь между PC3 и ROUTER2. Для этого наберите команду **ping 195.48.64.1**. Если связь есть, получите стандартный ответ (смотри экран на рисунке 1), в противном случае придет сообщение о превышении времени (таймаут). Аналогично проверь-

те связь маршрутизатора ROUTER1 (195.48.192.2) с тором ROUTER3. Если маршрутизатор вернет пять восклицательных знаков, значит, связь есть. В случае возврата пяти точек – команда не прошла.

Также проверьте связь других маршрутизаторов между собой.

Если Вы попробуете проверить связь между центральным маршрутизатором и PC1, получите отрицательный ответ. Это объясняется тем, что шлюз (роутер) не знает об этой сети, так как не может найти маршрут к ней. Чтобы пакеты передавались во все стороны, необходимо на маршрутизаторе прописать все маршруты ко всем сетям.

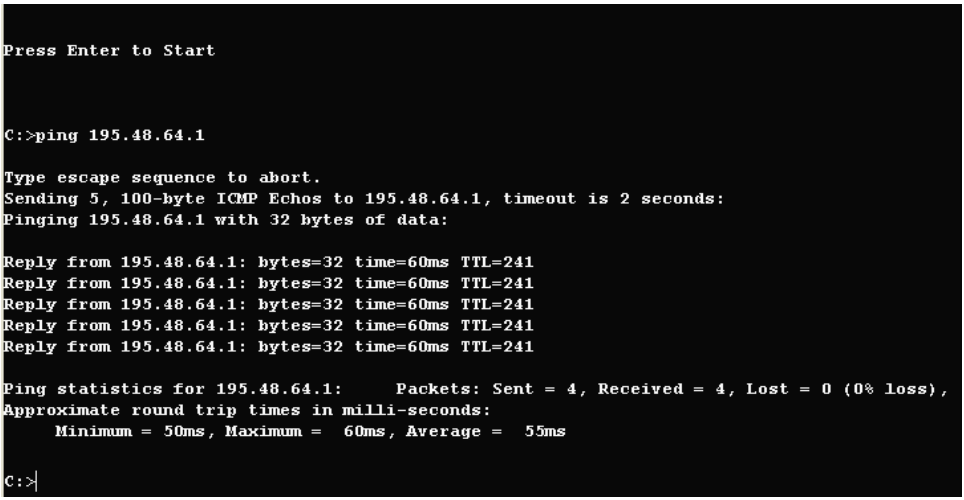


Рисунок 1. Успешное выполнение команды ping.

Задание к лабораторной работе:

Выполните конфигурирование интерфейсов устройств и проверьте их связь, как описано выше.

Содержание отчета

1. Наименование и цель выполняемой работы.
2. Формулировка задания на лабораторную работу.
3. Топология сети с указанием на схеме ip – адресов всех интерфейсов, ip – адресов и масок подсетей.
4. Протоколы конфигурирования интерфейсов устройств.
5. Выполненные команды проверки связности сети и их ре-

зультаты.

6. Выводы по проделанной работе.

Контрольные вопросы

1. В чем состоит конфигурирование информационной сети.
2. В каком режиме выполняется конфигурирование интерфейсов маршрутизаторов.
3. Каков синтаксис команды назначения ip – адреса интерфейсу.
4. Какая команда позволяет просмотреть текущую конфигурацию маршрутизатора.
5. Какая команда позволяет проверить наличие связи между устройствами.
6. Какой результат выдается этой командой в случае успешного выполнения.
7. Какой результат выдается при отсутствии связи с запрашиваемым устройством.

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Цель: Изучить способы настройки статической маршрутизации.

Теоретические сведения

При статической маршрутизации все маршруты прописываются и изменяются администратором системы вручную. Это самый простой способ организации маршрутизации. Однако он подходит только для небольших сетей, изменения в структуре которых происходят достаточно редко. Кроме того, данный способ маршрутизации не годится в случае, когда важно обеспечить высокую надежность межсетевого взаимодействия. Если один из маршрутов окажется по каким-либо причинам недоступен, администратору необходимо будет вручную изменить таблицу маршрутизации на всех маршрутизаторах в сети. До этого момента межсетевое взаимодействие на отдельных участках сети будет невозможно.

Перечень выполняемых действий

1) Построить топологию составной сети согласно варианту задания

2) Сконфигурировать интерфейсы маршрутизаторов

3) Проверить связность непосредственно соединенных интерфейсов с помощью команды ping

4) Установить статические маршруты между сетями, представленными на схеме, в соответствии с вариантом задания

5) Просмотреть таблицу маршрутизации

6) Проверить связность всех интерфейсов с помощью команды ping

Руководство к выполнению:

Установка статических маршрутов на каждом маршрутизаторе выполняется в режиме конфигурации маршрутизатора с помощью следующей команды:

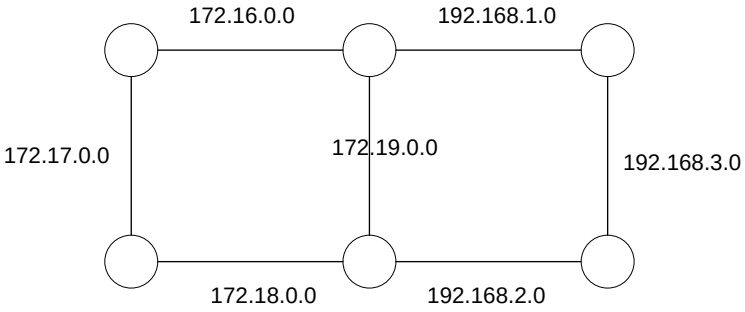
ip route сеть маска следующий_маршрутизатор

пример: ip route 172.18.0.0 255.255.0.0 192.168.1.2

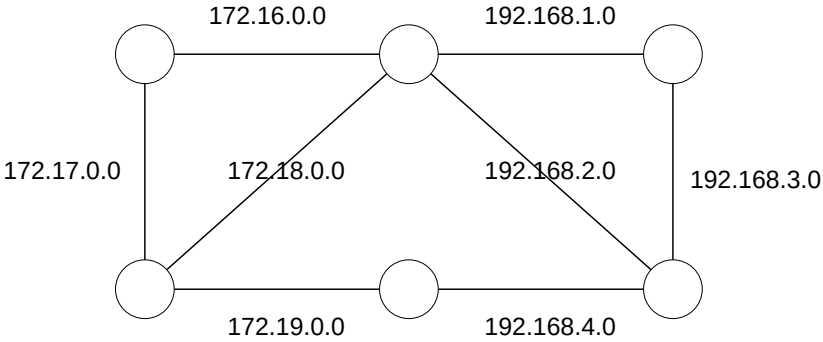
С помощью команды **show ip route** осуществляется просмотр таблицы маршрутизации.

Варианты заданий

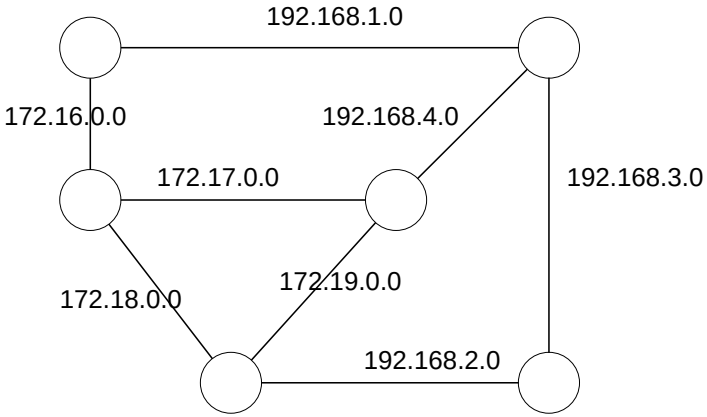
Вариант 1



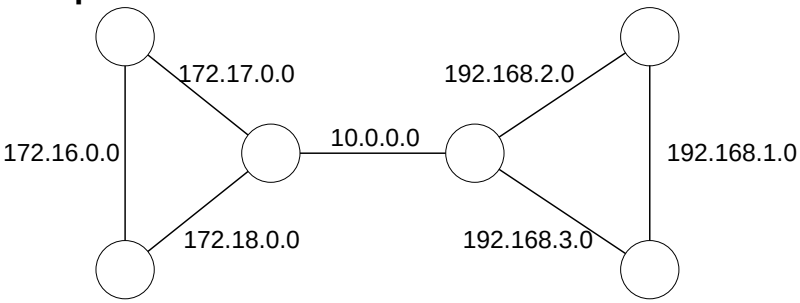
Вариант 2



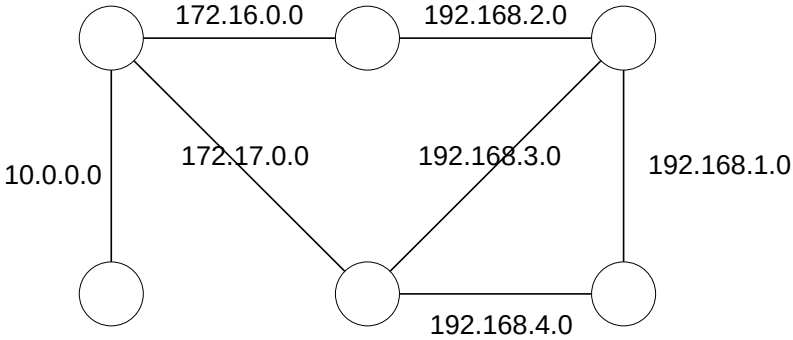
Вариант 3



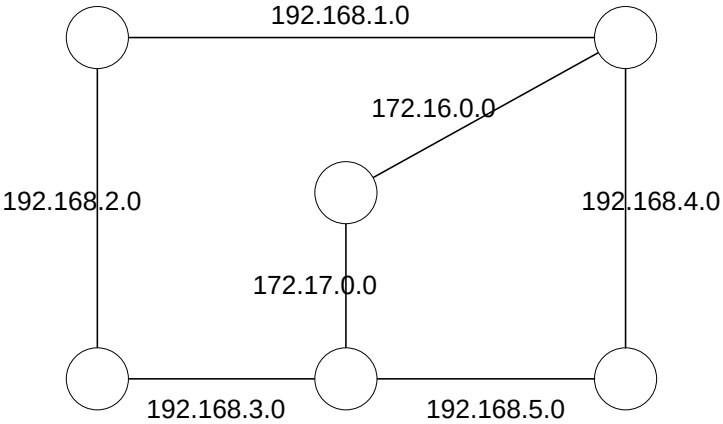
Вариант 4



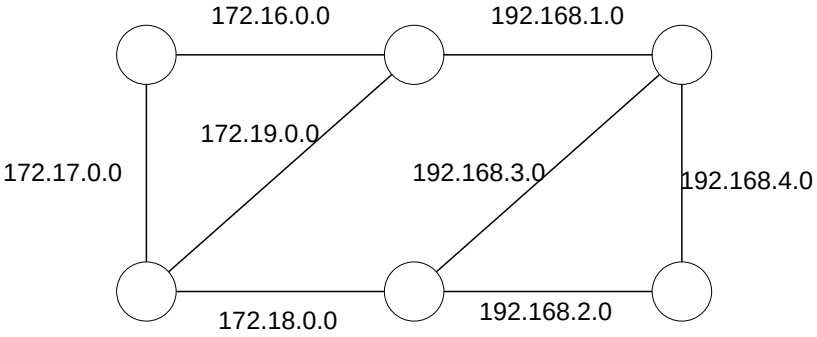
Вариант 5



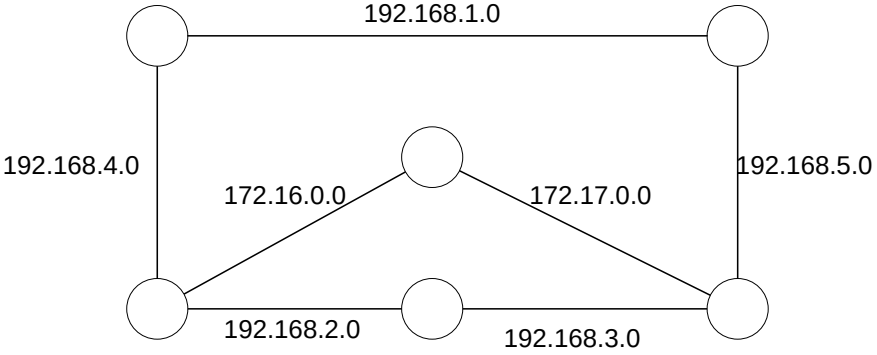
Вариант 6



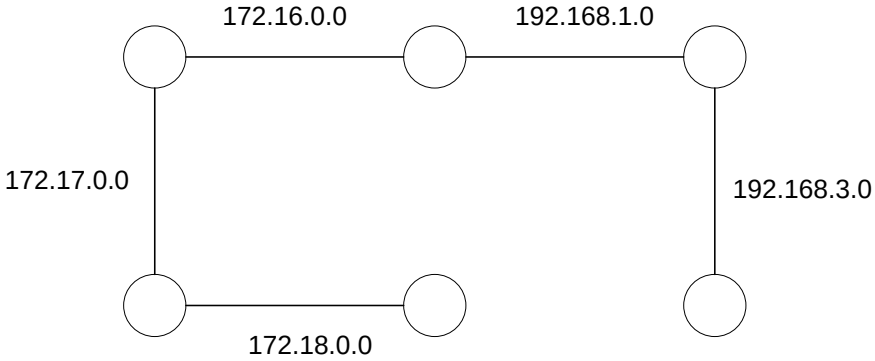
Вариант 7



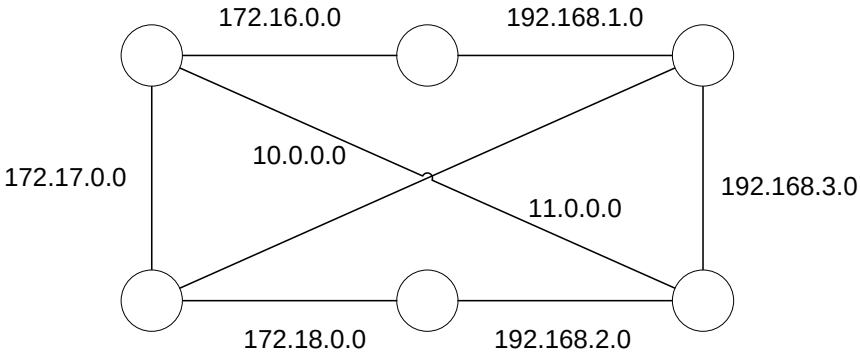
Вариант 8



Вариант 9



Вариант 10



Отчёт по лабораторной работе должен содержать:

1. Титульный лист
2. Цель, задание
3. Схему сети из Packet Tracer с указанными IP-адресами всех портов всех маршрутизаторов
4. Последовательность команд для настройки интерфейсов хотя бы одного маршрутизатора
5. Последовательность команд для настройки статической маршрутизации на каждом маршрутизаторе
6. Таблицы маршрутизации каждого маршрутизатора
7. Несколько результатов команды trace до несоседнего маршрутизатора
8. Выводы по проделанной работе

Контрольные вопросы

1. Какой маршрут является статическим?
2. Какая информация определяется для маршрута?
3. В чем состоит статическая маршрутизация?
4. Как обозначается статический маршрут в таблице маршрутизации?

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Цель: Изучить способы настройки динамической маршрутизации по протоколам RIP и OSPF.

Теоретические сведения

В зависимости от способа формирования содержимого таблицы маршрутизации различают два вида маршрутизации.

При статической маршрутизации все маршруты прописываются и изменяются администратором системы вручную.

При динамической маршрутизации построение таблицы маршрутизации осуществляется посредством специальных протоколов маршрутизации. Участие администратора в этом процессе минимально и сводится к изначальной конфигурации маршрутизаторов. Два наиболее распространенных протокола IP-маршрутизации, используемых в интрасетях, — протоколы RIP (Routing Information Protocol) и OSPF (Open Shortest Path First). Посредством указанных протоколов маршрутизаторы способны информировать друг друга об изменениях в структуре сети. В случае недоступности одного из маршрутов, маршрутизаторы автоматически перестроят свои таблицы маршрутизации и, при возможности, выберут другой маршрут доставки сообщений.

Протокол RIP относится к классу дистанционно-векторных протоколов. После конфигурирования RIP – системы происходит рассылка так называемых векторов расстояний по всем интерфейсам обо всех известных сетях. В вектор расстояния входит адрес сети и метрика (изначально 1). После приема данного вектора, соседний маршрутизатор просмотрит свою таблицу и при отсутствии данных о сети внесет запись в память. Затем он увеличит метрику на единицу и разошлет пакет по всем своим каналам. Если запись присутствует в таблице маршрутизации, роутер сравнивает метрики и вносит строку в таблицу только в случае более выгодной метрики. Несмотря на простоту и удобство, протокол RIP не пригоден в больших сетях. Он не может оптимально применяться в сетях с разными каналами, так как в любом случае пакет пойдет по кратчайшему пути независимо от пропускной способности линии связи. В этом протоколе также случаются такие явления, как зацикливание и образование петель. К недостаткам протокола RIP относится и засорение сети широковещательным трафиком.

Указанные проблемы ре- шаются в протоколе OSPF. Он

относится к классу протоколов состояния связей. OSPF не рассылает данные обо всех сегментах. Он шлет только сведения о соседних сетях в коротких HELLO – сообщениях. После отправки и получения информации, протокол OSPF строит так называемую базу, на основе которой составляет наиболее оптимальный маршрут до каждой подсети, учитывая стоимость прохождения пакета по каналу и его пропускную способность.

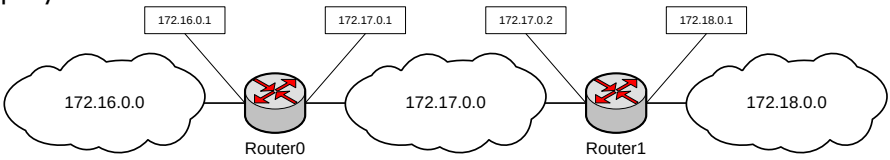
Для настройки динамической маршрутизации по протоколу RIP используются следующие команды:

В режиме конфигурации маршрутизатора:

router rip — переход в режим настройки протокола RIP.

network адрес — задаёт адрес сети, к которой подключен маршрутизатор и информация о которой должна передаваться соседним маршрутизаторам.

Рассмотрим пример соединения сетей, представленный на рисунке:



Для настройки маршрутизации по протоколу RIP следует выполнить следующие команды:

на маршрутизаторе Router0:

```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 172.16.0.0
Router(config-router)#network 172.17.0.0
```

на маршрутизаторе Router1:

```
Router>enable
Router#configure terminal
Router(config)#router rip
Router(config-router)#network 172.17.0.0
Router(config-router)#network 172.18.0.0
```

Настройка динамической маршрутизации по протоколу OSPF выполняется аналогичным образом — для каждого маршрутизатора необходимо указать сети, информацию о которых он будет рассылать другим маршрутизаторам. Для этого используются

следующие команды:

route ospf 1 — переход в режим настройки протокола OSPF.

network адрес маска area зона

Например: network 172.16.0.0 area 0

network 172.17.0.0 area 0

Для проверки настроек можно использовать следующие команды:

show ip route — показывает таблицу маршрутизации,

trace адрес — выводит путь до указанного узла.

Задание

Для схем сетей, приведённых в предыдущей лабораторной работе, настроить динамическую маршрутизацию отдельно по протоколу RIP и отдельно по протоколу OSPF.

Удалить или отключить соединение между двумя маршрутизаторами, не нарушая связности сети (то есть так, чтобы осталась возможность из любого узла сети попасть на любой другой узел). Определить, как данные изменения отразятся в таблицах маршрутизации.

Отчёт по лабораторной работе должен содержать:

1. Титульный лист.
2. Цель, задание.
3. Схему сети из Packet Tracer с указанными IP-адресами всех портов всех маршрутизаторов.
4. Последовательность команд для настройки динамической маршрутизации на каждом маршрутизаторе.
5. Таблицы маршрутизации каждого маршрутизатора.
6. Несколько результатов команды trace до несоседнего маршрутизатора.

Контрольные вопросы

1. Какой маршрут является динамическим?
2. Какие протоколы динамической маршрутизации изучены в ходе работы?
3. Чем отличается настройка этих протоколов?
4. Каковы преимущества, недостатки, области применения данных протоколов?
5. Что содержит таблица маршрутизации?
6. Какая информация задается для каждого маршрута в таблице маршрутизации?

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: ПРОТОКОЛ DHCP

Цель: Изучить способы настройки протокола динамической конфигурации хоста.

Теоретические сведения

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической настройки узла) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие настройки, необходимые для работы в сети, такие как маска подсети, шлюз по умолчанию, адрес DNS-сервера.

Централизованное распределение IP-адресов позволяет не только избежать ручного ввода настроек сети на каждом компьютере, но и гарантирует отсутствие повторяющихся адресов внутри сети.

Для настройки DHCP используются следующие команды, вводить которые необходимо в режиме конфигурации маршрутизатора:

ip dhcp excluded-address адрес — позволяет исключить адрес из выдачи по протоколу DHCP.

ip dhcp pool название — создаёт пул (множество) IP-адресов для выдачи узлам сети и переходит в режим его конфигурирования.

В режиме конфигурации пула адресов:

default-router адрес — задаёт адрес, который будет назначен узлам сети в качестве шлюза по умолчанию.

network адрес маска — указывает сеть, из которой должны браться адреса для выдачи узлам сети.

Например, следующие настройки позволяют маршрутизатору, подключённому к сети 192.168.0.0 и имеющему в ней адрес 192.168.0.1, выдавать IP-адреса компьютерам, находящимся в этой сети, исключая уже занятый им адрес:

```
Router>enable
Router#configure terminal
Router(config)#ip dhcp excluded-address 192.168.0.1
Router(config)#ip dhcp pool my_net
Router(dhcp-config)#default-router 192.168.0.1
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
```

Задание

Для схем сетей, постро- енных в предыдущей

торной работе, настроить автоматическую выдачу IP-адресов, масок и шлюзов по умолчанию в каждой сети.

Отчёт по лабораторной работе должен содержать:

1. Титульный лист.
2. Цель, задание.
3. Схему сети из Packet Tracer с указанными IP-адресами всех портов всех маршрутизаторов.
4. Последовательность команд для настройки протокола DHCP на тех маршрутизаторах, на которых она выполнялась.
5. Скриншоты окна конфигурации с полученными по протоколу DHCP настройками для хотя бы одного компьютера в каждой сети.

Контрольные вопросы

1. Для чего используется протокол DHCP ?
2. На каком сетевом устройстве надо выполнять настройку протокола DHCP?
3. Какие команды используются для настройки протокола DHCP?

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: ТРАНСЛЯЦИЯ СЕТЕВЫХ АДРЕСОВ

Цель: Изучить способы настройки динамической трансляции сетевых адресов.

Теоретические сведения

NAT (от англ. Network Address Translation — трансляция сетевых адресов) — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса в заголовках пакетов, проходящих через какое-либо устройство.

Узлам сети, находящимся с внутренней стороны устройства NAT, назначаются частные IP-адреса; обычно это делается через службу DHCP или путем статической настройки, выполняемой администратором.

Когда приложение, запущенное на компьютере во внутренней сети, инициирует отправку данных, частный IP-адрес клиента (IP-адрес источника) и клиентский порт (порт источника) вставляются в пакет в поля параметров источника. Поля параметров пункта назначения будут содержать IP-адрес сервера (IP-адрес назначения — удаленный узел) и порт сервера. Поскольку пункт назначения пакета находится вне частной сети, клиент направляет его в основной шлюз, на котором должна быть настроена трансляция адресов и портов.

Устройство NAT перехватывает исходящий пакет и производит сопоставление порта, используя IP-адрес назначения (адрес сервера), порт назначения, внешний IP-адрес устройства NAT, внешний порт, сетевой протокол, а также внутренние IP-адрес и порт клиента.

Устройство NAT ведет таблицу сопоставлений портов и сохраняет созданное сопоставление в этой таблице. Внешние IP-адрес и порт — это общие IP-адрес и порт, которые будут использоваться в текущем сеансе передачи данных вместо внутренних IP-адреса и порта клиента.

Затем устройство NAT «транслирует» пакет, преобразуя в пакете поля источника: частные, внутренние IP-адрес и порт клиента заменяются внешними IP-адресом и портом устройства NAT.

Преобразованный пакет пересылается по внешней сети и в итоге попадает на заданный сервер.

Получив пакет, сервер полагает, что имеет дело с каким-то одним компьютером, IP-адрес которого допускает глобальную маршрутизацию. Сервер будет направлять ответные пакеты

на внешние IP-адрес и порт устройства NAT, указывая в полях источника свои собственные IP-адрес и порт.

NAT принимает эти пакеты от сервера и анализирует их содержимое на основе своей таблицы сопоставления портов. Если в таблице будет найдено сопоставление порта, для которого IP-адрес источника, порт источника, порт назначения и сетевой протокол из входящего пакета совпадают с IP-адресом удаленного узла, удаленным портом и сетевым протоколом, указанным в сопоставлении портов, NAT выполнит обратное преобразование. NAT заменяет внешний IP-адрес и внешний порт в полях назначения пакета на частный IP-адрес и внутренний порт клиента.

Затем NAT отправляет пакет клиенту по внутренней сети. Однако если NAT не находит подходящего сопоставления портов, входящий пакет отвергается и соединение разрывается.

Благодаря устройству NAT клиент получает возможность передавать данные в глобальной среде Интернета, используя лишь частный IP-адрес; ни от приложения, ни от клиента не требуется никаких дополнительных усилий.

Задание

1. Добавить на схему из предыдущей лабораторной работы еще 2 сети с адресами 192.168.0.0/24.

2. На каждом маршрутизаторе, соединяющем новые сети с созданными ранее, настроить трансляцию сетевых адресов.

Настройка трансляции сетевых адресов осуществляется с помощью следующих команд:

В режиме настройки интерфейса:

ip nat inside — указывает, что данный интерфейс находится во внутренней сети.

ip nat outside — указывает, что данный интерфейс находится во внешней сети.

В режиме конфигурации маршрутизатора:

ip access-list extended имя — создаёт список контроля доступа с заданным именем и переходит в режим его настройки.

В режиме настройки списка контроля доступа:

permit ip any any — разрешает всем узлам доступ к любым адресам по любому протоколу.

В режиме конфигурации маршрутизатора:

ip nat inside source list имя interface название_интерфейса overload — включает трансляцию адресов внутренней сети в адрес указанного интерфейса.

3. Создать внутри каждой добавленной сети web-сервер и

настроить доступ к нему из внешних сетей.

Для этого в режиме конфигурации маршрутизатора используется команда:

ip nat inside source static протокол(TCP|UDP) внутренний_адрес внутренний_порт внешний_адрес внешний_порт

По мере осуществление трансляции в NAT-таблицах маршрутизаторов накапливается информация, посмотреть которую можно в привилегированном режиме маршрутизатора командой

show ip nat translations

Отчёт по лабораторной работе должен содержать:

1. Титульный лист
2. Цель, задание
3. Команды, использованные для настройки NAT
4. Скриншот заголовков пакета при его прохождении через устройство с NAT
5. NAT-таблицы маршрутизаторов

Контрольные вопросы

1. Каково назначение протокола NAT ?
2. К какому стеку протоколов относится протокол NAT?
3. Каким образом работает протокол NAT?

ЛАБОРАТОРНАЯ РАБОТА НА ТЕМУ: ПОСТРОЕНИЕ ВИРТУАЛЬНЫХ ТУННЕЛЕЙ

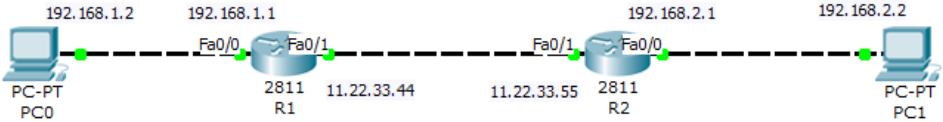
Цель: Изучить возможности построения виртуальных туннелей поверх существующих сетей.

Краткие теоретические сведения

Туннелирование (от англ. tunnelling — «прокладка туннеля) — процесс, в ходе которого создается логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов.

Generic Routing Encapsulation (GRE) — протокол туннелирования сетевых пакетов, разработанный фирмой Cisco. Этот протокол используется для передачи пакетов одной сети через другую сеть. GRE туннель представляет собой соединение точка-точка, его можно считать одной из разновидностей VPN туннеля без шифрования. Основное достоинство GRE - это возможность передавать широковещательный трафик, что позволяет пропускать через такой туннель использующие его протоколы маршрутизации. При использовании публичных сетей необходимо совместно с GRE применять IPSec для реализации защищенных VPN соединений.

Ниже приведен пример создания простого туннеля между двумя сетями.



R1	R2
R1(config)# interface Tunnel0 R1(config-if)# ip address 172.16.0.1 255.255.0.0 R1(config-if)# tunnel source FastEthernet0/1 R1(config-if)# tunnel destination 11.22.33.55	R2(config)# interface Tunnel0 R2(config-if)# ip address 172.16.0.2 255.255.0.0 R2(config-if)# tunnel source FastEthernet0/1 R2(config-if)# tunnel destination 11.22.33.44

В первой строке создаётся виртуальный интерфейс для организации туннеля. Во второй строке данному интерфейсу присваивается адрес. Адреса туннельных интерфейсов должны при-

надлежать одной сети (в данном случае 172.16.0.0). В следующих двух строках указываются адреса начала и конца туннеля.

После настройки интерфейсов необходимо задать маршруты в удалённые сети через адреса виртуальных интерфейсов:

R1(config)# ip route 192.168.2.0 255.255.0.0 172.16.0.2

R2(config)# ip route 192.168.1.0 255.255.0.0 172.16.0.1

Результат команды tracert, выполненной на компьютере PC0:

```
PC>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1    78 ms      31 ms      31 ms      192.168.1.1
  2    *          63 ms      49 ms      172.16.0.2
  3    *          93 ms      94 ms      192.168.2.2

Trace complete.
```

На рисунке видно, что сначала пакет отправляется на шлюз по умолчанию, затем на адрес виртуального туннельного интерфейса и в конце - на компьютер назначения.

Задание

1. Добавить 3 сети к схеме, разработанной в предыдущей лабораторной работе. Перед добавлением необходимо убедиться, что между всеми маршрутизаторами сети настроена маршрутизация и каждый узел доступен с любого другого узла сети. Для адресации внутри сетей можно использовать любые частные адреса из тех, которые еще не присутствуют на схеме. При подключении данных сетей необходимо использовать маршрутизатор серии 2811.

2. Настроить тунеллирование между данными сетями.

Отчёт по лабораторной работе должен содержать:

1. Титульный лист
2. Цель, задание
3. Схему сети
4. Команды, использованные для создания туннелей
5. Команды, использованные для настройки маршрутизации между виртуальными сетями
6. Скриншот содержимого пакета при его прохождении по виртуальному туннелю
7. Скриншоты результатов команды tracert, выполненной на

компьютерах внутри добавленных локальных сетей

Контрольные вопросы

1. Что означает туннелирование ?
2. Какой протокол туннелирования разработан фирмой Cisco?
3. Каким преимуществом обладает этот протокол?
4. Каким образом выполняется создание туннеля в данном протоколе?