**Практическая работа №1**

**Утилиты настройки сетевых компонентов в MS Windows 2000/XP/2003**

**Цель:** получить практические навыки по конфигурированию сети Microsoft, ознакомится с утилитами командной строки, предназначенными для диагностики и настройки сетевых компонентов ОС Windows, разработать скрипт, конфигурирующий IP по заданным параметрам, ознакомиться с форматом записи пути до сетевого ресурса UNС.

**Необходимо**:

1. компьютер под управлением MS Windows 2000/XP/2003/7
2. пользователь с администраторскими правами
3. справка Windows

**Порядок выполнения работы:**

1. Установить Microsoft Loopback Adapter (адаптер Microsoft замыкания на себя) (Панель управления\Установка оборудования … Установить вручную).
2. С помощью графического интерфейса убедится, что к Microsoft Loopback Adapter подключены Клиент для сетей Microsoft, Служба доступа к файлам и принтерам Microsoft, TCP/IP. Разобраться с назначением этих компонентов.

В свойствах протокола TCP/IP задать параметры IP 10.10.10.1 mask 255.255.255.0 gateway 10.10.10.10 DNS 10.10.10.11

3) Сделать так, чтобы внешний пользователь не смог по сети через Microsoft
Loopback Adapter получить доступ к ресурсам вашего компьютера.

Проверить можно так: Пуск\Выполнить -> набрать адрес компьютера \\10.10.10.1 до отключения доступа будут «видна» как минимум папка с Принтерами, после отключения система выдаст сообщения о недостижимости ресурса. Этот формат записи пути до сетевого ресурса называется UNC (Universal Name Conversion)

\\имя\_или\_адрес\_компьютера\путь\путь\ресурс\_или\_файл (может использоваться сокращенная нотация как в этом примере).

4) используя встроенную справку Windows и справку командной строки разобраться в назначении и ключах следующих утилит:

* Ping
* Ipconfig
* net с директивами use и view

Справку по утилитам командной строки можно получить так:

command\_name /?

А по команде net так: net help имя\_директивы

5) используя встроенную справку Windows и справку командной строки разобраться в назначении и принципах работы утилиты netsh

**В отчет:**

в заголовке письма: №группы ФИО №работы (например: 3155 Фёдор Сумкин 1) Ответы на вопросы:

1) Как с помощью графического интерфейса Windows запретить доступ через определенный сетевой интерфейс к ресурсам компьютера?

1. Как с помощью ipconfig узнать адрес DNS на который настроен ваш компьютер?
2. Зачем нужна команда net use? Как с помощью этой утилиты подключить на локальный диск R: папку TEST на компьютере SRV (приведите командную строку)?

4) В чем назначение утилиты ping?

Кроме вопросов еще:

5) текст командного файла(ов) (для командного интерпретатора CMD.exe), с помощью
которого(ых) можно было бы настраивать IP на выбранном сетевом интерфейсе двумя
способами или:

1. получение все настроек автоматически (IP, mask, gate, DNS)
2. или статически (IP 10.10.10.1 mask 255.255.255.0 gateway 10.10.10.10 DNS 10.10.10.11).

При выполнении этого задания учтите что:

1. в netsh есть директива exec, выполняющая текстовый файл настройки
2. в netsh в любом контексте есть директива dump, которая выводит на экран все команды необходимые для настройки контекста до текущего состояния (в том числе и контекста interface ip).
3. директивы netsh можно выполнять и из командной строки, например C:\>netsh interface ip dump
4. командные интерпретаторы умеют перенаправлять консольный вывод в текстовый файл.

**Практическая работа №2**

**Анализ трафика в сетях Ethernet**

**Цель:** получить практические навыки по работе с анализаторами сетевого трафика, по сбору данных и анализу статистики трафика. На практике ознакомится с отличиями работы активного оборудования. Уяснить особенности взаимодействия сетевого и канального уровня на примере стека TCP\IP. Выяснить форматы кадров Ethernet.

**Необходимо**:

1. компьютер под управлением MS Windows 2000/XP/2003
2. пользователь с администраторскими правами
3. сетевое подключение по протоколу IP поверх Ethernet.
4. доступ к Web.

**Порядок выполнения работы:**

1. Установить на компьютер программу WinPcap и оболочку к ней Wireshark либо iris, либо esa. Запустить сеанс перехвата пакетов. Запустить для интенсивной генерации кадров браузер и откройте в нем любой сайт по выбору.
2. Установить какой тип кадров Ethernet в данной сети.
3. На основании собранной статистики определить к коммутационному оборудованию какого типа подключен ваш компьютер.

Разберитесь, какие типы оборудования могут в принципе использоваться в вашей сети.

Сортируйте пакеты по адресам отправителя и получателя. Определите, какие группы кадров по адресам присутствуют в собранной статистике. Это поможет сделать выводы.

Поможет также знание собственного IP адреса.

5) найдите широковещательные кадры и пакеты. Изучите их заголовки.

**В отчет:**

в заголовке письма: №группы ФИО №работы (например: 3155 Фёдор Сумкин 2)

Ответы на вопросы:

1. Какие типы кадров Ethernet бывают, в чем их отличие?
2. Какой тип кадров Ethernet кадров используется? Почему именно он?
3. Какой тип коммутационного оборудования используется? Обоснуйте ваше мнение.
4. На какой канальный адрес осуществляются широковещательные рассылки?
5. Для чего применяются перехваченные вами широковещательные рассылки?

**Практическая работа №3**

**Выбор коммутационного оборудования**

**Цель:** получить практические навыки по подбору коммутационного оборудования для решения формализованных задач, а так же опыта работы с описаниями оборудования и техническими спецификациями.

**Необходимо**:

1) Доступ к справочной информации в WWW

**Порядок выполнения работы:**

1. В работе приведены описания нескольких систем, для которых необходимо подобрать активное оборудование.
2. В описаниях указаны транспортные задачи, которые должно решить оборудование, а также дополнительные требования к разворачиваемой системе.
3. При подборе оборудования необходимо соблюдать принцип минимизации финансовых затрат.
4. Ограничения по производителям оборудования нет, однако рекомендуется обратить внимание на оборудование 3Com, CISCO и D-LINK.

*Задание 1* – подобрать коммутационное оборудование для сети небольшого офиса. В состав сети входят 15 компьютеров с равным уровнем доступа. Максимальная нагрузка на сеть возможна при одновременном доступе к файловой базе данных объемом 96 Мб.

*Задание 2* – подобрать коммутационное оборудование для проведения чемпионата России по киберспорту. Планируется обеспечить совместную работу 80 компьютеров. Следует избежать ситуации задержек в игре из-за недостаточной производительности коммутационного оборудования. Считайте, что пиковый трафик, генерируемый средней современной сетевой игрой составляет 10 Мб\с. Возможна компактная установка коммутационного оборудования в одной стойке.

*Задание 3* – подобрать коммутационное оборудование для сети крупного предприятия. Требуется организовать изолированные потоки данных для разных отделов предприятия и высокоскоростной back-bone для связи отделов и доступа к сервисам предприятия. Примем количество отделов 5, по 30 компьютеров в каждом отделе.

*Задание 4* – подобрать коммутационное оборудование для сети студии киномонтажа. В студии создан вычислительный кластер для обсчета цифрового видео из 4 компьютеров. Оборудование должно быть гарантированно неблокирующем, то есть обладать внутренней шиной такой производительности, чтобы гарантированно обработать максимально возможные потоки между всеми нагруженными портами коммутатора.

*Задание 5* – подобрать коммутационное оборудование для ядра крупной корпоративной сети. Обеспечить коммутацию 18 стомегабитных каналов от подразделений. Необходимо реализовать фильтрацию на основе IP адресов и поддержку протоколов маршрутизации RIP2.

*Задание 6* – подобрать коммутационное оборудование для использования в качестве узловых точек растущей сети провайдера кабельного домашнего Internet. Необходимо обеспечить удаленное управление устройством.

*Задание 7* – подобрать коммутационное оборудование для оператора сети. Через сеть в среднем передается 4 Терабайта в день. Необходимо обеспечить соединение сетей с разными канальными протоколами (FastEthernet, GigabitEthernet и FDD).

**В отчет:**

в заголовке письма: №группы ФИО №работы (например: 3155 Фёдор Сумкин 3)

В теле письма:

Модели подобранного оборудования, с характеристиками обеспечивающими решение

поставленных задач. Стоимость устройства. И комментарии, за счет чего именно

достигается решение поставленных задач.

**Практическая работа №4**

**Работа с адресами IP сетей**

**Цель:** получить практические навыки по работе с пространством IP-адресов, масками и управления адресацией в IP сетях.

**Необходимо**:

1) Навыки по переводу чисел из десятичной в двоичную систему и наоборот, в ручном режиме или с помощью компьютера.

**Краткие теоретические сведения**

1. Все пространство IP адресов делится на логические группы – IP-сети. Они нужны для организации иерархической адресации в составной IP-сети, например Интернете. Каждой локальной сети присваивается своя IP-сеть, маршрут до IP-узлов, находящихся в этой локальной сети строится на маршрутизаторах как маршрут до их IP-сети. И только после того, как пакет попал в конкретную IP-сеть, решается задача его доставки на отдельный узел.
2. В IP-адресе выделяются две части – адрес сети и адрес узла. Деление происходит с помощью маски – 4-x байтного числа, которое поставлено в соответствие IP-адресу. Макса содержит двоичные 1 в тех разрядах IP-адреса, которые определяют адрес сети и двоичные 0 в тех разрядах IP адреса, которые определяют адрес узла.
3. Адресом IP-сети считается IP-адрес из этой сети, в котором в поле адреса узла содержатся двоичные 0. Этот адрес обозначает сеть целиком в таблицах маршрутизации.

Есть еще служебный IP-адрес – адрес ограниченного широковещания – в поле
адреса узла он содержит двоичные 1. Оба эти адреса не используются для адресации реальных узлов сети, однако входят в диапазон адресов IP-сети.

1. Рассмотрим пример: есть адрес 192.168.170.15 с маской 255.255.252.0. Определим
адрес сети, адрес широковещания и допустимый для данной IP-сети диапазон
адресов.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DEC IP | 192 | 168 | 170 | 15 |
| DEC MASK | 255 | 255 | 252 | 0 |
| BIN IP | 11000000 | 10101000 | 10101010 | 00001111 |
| BIN MASK Зеленый – адрес сети Серый – адрес узла | 11111111 | 11111111 | 11111100 | 00000000 |
| BIN IP сети(скопируем сетевую часть IP изаполним узловую часть 0) | 11000000 | 10101000 | 10101000 | 00000000 |
| DEC IP сети | 192 | 168 | 168 | 0 |
| BIN IP широковещания (скопируем сетевую часть IP и заполним узловую часть 1) | 11000000 | 10101000 | 10101011 | 11111111 |
| DEC IP широковещания | 192 | 168 | 171 | 255 |
| Начало диапазона IP-адресов для узлов (значение поля узла +1 к IP адресу сети) | 192 | 168 | 168 | 1 |
| Окончание диапазона IP-адресов для узлов (значение поля узла -1 от IP-адреса широковещания) | 192 | 168 | 171 | 254 |

5) если имеется сеть, составленная из нескольких локальных сетей, соединенных между собой маршрутизаторами, то нужно каждой из этих локальных сетей назначить отдельную IP-сеть. В случае, если вам для такой сети выдается большая IP-сеть в управление (например, такую сеть может назначить провайдер Интернет), то эту сеть необходимо разделить с помощью масок на части. (необходимо отметить, что подобная ситуация может иметь место, если вам необходимо назначить узлам вашей сети реальные IP адреса, для того чтобы ваши компьютеры были «видны» из Интернета каждый под своим адресом).

**Порядок выполнения работы:**

В работе даны 4 варианта задания (Табл. 2). Необходимо сделать все варианты. На приведенной схеме представлена составная локальная сеть. Отдельные локальные сети соединены маршрутизаторами. Для каждой локальной сети указано количество компьютеров. Провайдер, для вас выдал IP-cеть (данные о сети представлены в табл. 2). Ваша задача установить IP-адрес сети и допустимый диапазон адресов. Разделить вашу сеть на части, используя маски. Маску надо выбирать так, чтобы в отделяемой IP подсети было достаточно адресов. Помните, что и порт маршрутизатора, подключенный к локальной сети, имеет IP адрес! Некоторые маски представлены в табл.3.

Таблица1

|  |  |
| --- | --- |
| Вариант | IP- адрес из сети |
| 1 | 192.169.168.70 |
| 2 | 172.21.25.202 |
| 3 | 83.14.53.9 |
| 4 | 190.23.23.23 |

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| маска | Сеть 1 | Сеть 2 | Сеть 3 |
| 255.255.248.0 | 500 комп. | 16 комп. | 19 комп. |
| 255.255.255.224 | 1 комп. | 4 комп. | 2 комп. |
| 255.255.255.128 | 10 комп. | 12 комп. | 8 комп. |
| 255.255.255.192 | 5 комп | 3 комп. | 3 комп. |



Рис 1.

|  |  |  |
| --- | --- | --- |
| Маска | Количество двоичных 0 | Количество всех адресов в IP сети с такой маской |
| 255.255.255.252 | 00 | 4 |
| 255.255.255.248 | 000 | 8 |
| 255.255.255.240 | 0000 | 16 |
| 255.255.255.224 | 00000 | 32 |
| 255.255.255.192 | 000000 | 64 |
| 255.255.255.128 | 0000000 | 128 |
| 255.255.255.0 | 00000000 | 256 |
| 255.255.254.0 | 0.00000000 | 512 |

Таблица 3

**В отчет:**

в заголовке письма: №группы ФИО №работы (например: 3155 Фёдор Сумкин 4)

В теле письма таблицу:

|  |  |  |  |
| --- | --- | --- | --- |
| **Вариант:** | 1 |  |  |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 |
| IP-сети, маска |  |  |  |
| Количество IP адресов в IP-сети |  |  |  |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров. |  |  |  |
| **Вариант:** | 2 |  |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 |
| IP-сети, маска |  |  |  |
| Количество IP адресов в IP-сети |  |  |  |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров. |  |  |  |
| **Вариант:** | 3 |  |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 |
| IP-сети, маска |  |  |  |
| Количество IP адресов в IP-сети |  |  |  |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров. |  |  |  |
| **Вариант:** | 4 |  |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 |
| IP-сети, маска |  |  |  |
| Количество IP адресов в IP-сети |  |  |  |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров. |  |  |  |

**Практическая работа №5**

**Конфигурирование межсетевого экрана**

**Цель:** получить представление о работе классического межсетевого экрана. Закрепить понимание адресации на сетевом и транспортном уровне стека TCP\IP.

**Необходимо**:

1. Система Win32 (win9x/2000/XP/2003)
2. Доступ к Web
3. Пакет установки KerioWinRoute 4 (или любой другой файерволл)

**Краткие теоретические сведения:**

1. Под межсетевым экраном или firewall или брандмауэром понимают фильтр IP пакетов предназначенный для формального ограничения соединений клиентов и серверов работающих «поверх» TCP\IP.
2. В основу работы классического firewall положен контроль формальных признаков. В общем случае фильтрация осуществляется по:
3. IP адресам отправителя и получателя в заголовке IP пакета,
4. номерам портов приложения-получателя и приложения-отправителя,
5. инкапсулированным в IP протоколам транспортного (TCP, UDP) и сетевого уровней (ICMP).
6. Контролировать контент проходящих пакетов классический firewall не может.
7. В работе используется KerioWinRoute 4 поскольку из распространенных firewall под платформу Windows он обладает наименьшими средствами автоматизации (мастерами) и, как следствие, дает полное представление о сути настроек.

**Порядок выполнения работы:**

1. Зарегистрируйтесь на компьютере с администраторскими полномочиями и установите на вашем компьютере WinRoute
2. Настройте firewall таким образом, чтобы выполнялись следующие условия:
3. с вашей системы должны быть доступны: DNS сервер с адресом шлюза по умолчанию, DNS сервер c адресом 194.85.32.18, все наружные Web сервера и HTTP прокси с адресом вашего шлюза по умолчанию, FTP сервер ftp.ifmo.ru, все наружные POP3 сервера, и SMTP сервер mail.ifmo.ru.
4. с наружи, в вашей системе должен быть доступен SSH сервер на всех узлах с подсети 83.0.0.4 \ 255.255.0.0
5. отдельно блокируется доступ к вашей системе с хоста 10.10.11.173.
6. ваша система не должна отвечать на запросы команды PING.
7. работа с остальными сервисами должна быть блокирована.

Кроме правил разрешения, должно быть правило, ограничивающее передачу всего

неразрешенного трафика. А раз правила выполняются последовательно, то это правило

должно быть последним в списке.

Определить какой номер порта соответствует какому серверу можно

воспользовавшись Web.

Ограничивайте также диапазоны портов программ-клиентов.

Для каждого правила на исходящий трафик создается зеркальное правило на входящий

и наоборот. При написании этих правил обратите внимание что является в конкретном

случае источником (Source) а что получателем (Destination)

3) после завершения работы удалите WinRoute (Панель управления \ установка удаления программ)!

**В отчет:**

в заголовке письма: №группы ФИО №работы (например: 3155 Фёдор Сумкин 5)

В теле письма:

1. Правила фильтрации в виде скриншотов WinRoute или в любой другой понятной мнемонической записи. Ответы на вопросы:
2. от чего не способен защитить классический firewall?
3. можно ли организовать доступ к Web серверу если у клиентов закрыт доступ к 80 порту?
4. в чем разница между правилами Deny и Drop?

**Практическая работа №6**

**Маршрутизация в IP сетях**

**Цель:** получить представление о работе IP маршрутизатора, попрактиковаться в

составлении таблиц маршрутизации и работе протоколов внутренней маршуртизации.

Дополнительной целью работы является приобретение опыта работы в средах

виртуализации.

**Необходимо**:

1. Семь компьютеров, объединенных локальной сетью.
2. Установление на них программа VMWare Workstation и сташе.
3. Виртуальные машины Windows 2003 Server и Windows XP.
4. Понимание структуры IP адресов и принципов маршрутизации.

Использование виртуальных машин в этой работе обусловлено исключительно соображениями удобства развертывания нескольких операционных систем на одном компьютере и не связано напрямую с главной целью работы.

В работе операционные системы Microsoft © могут заменяться на любые другие при условии, что последние поддерживают программную маршрутизацию IP. Так же в работе сделано еще одно допущение: реально, маршрутизатор объединяет несколько локальных сетей, имея по интерфейсу (порту) в каждой локальной сети. В случае программного маршрутизатора, работающего в составе ОС, в качестве портов выступают сетевые карты на компьютере. В работе программный маршрутизатор использует единственный интерфейс с двумя IP адресами для доступа к единой локальной сети, маршрутизируя фактически изолированные IP потоки.

**Краткие теоретические сведения**

1. Маршрутизаторы (аппаратные или программные) выполняют задачу выбора оптимального маршрута следования IP пакета и его отправки по этому маршруту. Для принятия решения анализируется адрес получателя и устанавливается маршрут следования на основе неких формализованных записей о структуре составной сети. Эти записи называются таблицами маршрутизации.
2. В таблице маршутизации присутствуют как минимум следующие поля: адрес назначения (адрес IP-сети или IP адрес хоста), идентификатор порта, через который пакет идет до сети назначения (порт обозначается IP-адресом или внутренним номером), шлюз (IP адрес на который необходимо пойти после того как пакет покинет порт), метрика (показатель качества маршрута).
3. На каждом маршрутизаторе сети присутствует таблица полностью описывающая структуру всей сети и, иногда, содержащая записи о маршрутах по умолчанию.
4. Таблицы маршрутизации составляются вручную или с помощью протоколов маршрутизации, автоматизирующих этот процесс. Одним из таких протоколов является протокол RIP2.
5. В работе используется пакет виртуализации VMWare. Принцип его работы заключается в программной эмуляции в рамках основной операционной системы аппаратной среды выполнения для гостевой операционной системы. Такой подход позволяет запускать операционные системы в выделенной виртуальной машине, программные интерфейсы которой перехватывают обращение гостевой ОС к аппаратуре и передающей их реальным устройствам от имени основной ОС. В работе такой подход позволяет безболезненно развернуть серверную ОС на компьютере без угрозы штатной операционной системе.



Рис 1.

В нашей сети 7 компьютеров. Три рабочих станции и четыре маршуртизатора. В качестве этих компьютеров будут выступать гостевые операционные системы. Рабочие станции будут работать под windows XP, а программные маршрутизаторы под управлением Windows 2003 (XP не поддерживает программную маршрутизацию). Как было сказано в разделе «Необходимо» работа выполняется с некой условностью. Все компьютеры будут подключены к одной локальной сети, а в ней организуются изолированные по адресам IP сети. Одновременная работа одного сетевого интерфейса в разных IP сетях достигается назначением двух и более IP адресов одному сетевому интерфейсу (Свойства сетевого соединения Свойства TCP\IP \ Дополнительно).

1. На первом этапе вам необходимо составить план сети (заранее выбрать IP-адреса для сетей, рабочих станций и портов маршрутизаторов). Определить на каком компьютере будет запущен какой виртуальный компьютер. Выбрать уникальное имя для каждого виртуального компьютера.
2. Установить при необходимости программу VMWare. В ней запустить необходимую виртуальную машину из папки C:\VM
3. В виртуальной операционной системе:
4. поменять MAC адрес сетевой платы на новый уникальный (Свойства сетевого соединения \ Настройка сетевого адаптера \ Сетевой адрес). Делать это необходимо из-за того что виртуальные машины созданы из одной копии, и, следовательно, обладают идентичными MAC адресами, что приводит к неправильной работе коммутатора локальной сети.
5. Изменить имя компьютера (панель управления \ свойства системы \ имя)
6. Установить все необходимые IP адреса.

На рабочих станциях необходимо указывать шлюз по умолчанию – IP адрес порта маршрутизатора из IP сети.

На маршрутизаторах делать этого не следует – маршрута по умолчанию нет. Адреса DNS остаются пустыми.

1. обязательно с помощью команды PING проверить видимость ближайших соседей по локальной сети.
2. На маршрутизаторах запустите службу Routing and Remote Access (Панель управления \ Администрирование \ Routing and Remote Access). С помощью мастера сконфигурируйте службу как LAN Router.
3. С помощью консольной команды ROUTE изучите таблицу маршрутизации по умолчанию.
4. С помощью консольной команды ROUTE (рекомендуемый способ) или с помощью графической консоли службы Routing and Remote Access дополните таблицу необходимыми записями.
5. С помощью команды ping проверьте достижимость рабочих станций друг с друга, а с использованием команд tracert и pathping проверьте путь следования IP пакетов.
6. Сохраните таблицы маршрутизации в текстовом файле.
7. Удалите созданные в ручную записи в таблицах маршрутизации. Убедитесь, что рабочие станции перестали «видеть друг-друга».
8. Добавьте в консоли службы Routing and Remote Access добавьте на маршрутизаторах протокол RIP2 (General \ Add new routing protocol). В нем добавьте интерфейс, через который будет происходить обмен векторами маршрутизации. Установите интервал обмена 60 секунд.
9. обновляя консоль убедитесь что пошли рассылки таблицы. После получения чужих таблиц выведите таблицу динамической маршрутизации (IP-routing \ Routing tables)
10. после того, как будут получены все необходимые записи с помощью команды ping проверьте достижимость рабочих станций друг с друга, а с использованием команд tracert и pathping проверьте путь следования IP пакетов.

15) отключите службу Routing and Remote Access, установите автоматическое
получение IP адресов на витальных системах.

**В отчет:**

в заголовке письма: №группы ФИО №работы (например: 3155 Фёдор Сумкин 6)

В теле письма:

1. Схему сети с адресами узлов,
2. таблицы маршрутизации всех маршрутизаторов Ответы на вопросы:
3. как в таблице маршрутизации MS отличить маршрут на хост от маршрута на сеть?
4. как в таблице маршрутизации MS отличить маршрут по умолчанию?
5. как с помощью команды route вывести таблицу маршрутизации, добавить и удалить маршрут?
6. какие методы предотвращающие возникновение ложных маршрутов в RIP2 включены на маршрутизаторе MS по умолчанию?

Для тех, кто решит выполнить работу в иной ОС (например Linux) следует готовить этот отчет в терминах и применительно к другой ОС.

**Практическая работа №7**

**DNS.**

**Цель:** получить представление о работе DNS сервера. Получить практические навыки использования утилит работы с серверами системы DNS и конфигурирования системы.

**Необходимо**:

1. Установление на них программа VMWare Workstation и сташе.
2. Виртуальные машины Windows 2003 Server.
3. Представление о работе системы DNS.
4. Доступ в Web.

**Краткие теоретические сведения**

1. Система DNS – распределенная база данных хранящая соответствие между IP адресом и доменным именем компьютера.
2. Система DNS – клиент - серверная. DNS-клиент получает в качестве конфигурационного параметра IP адрес обслуживающего DNS-сервера и получает к нему доступ напрямую.

3) На сервере DNS могут присутствовать множество записей разных типов и назначения.

4) Диагностику работы DNS с клиента можно выполнять с помощью команд ping
(формальная проверка разрешения имени) и с помощью консольной утилиты nslookup (работа с DNS сервером в режиме запрос-ответ)

**Порядок выполнения работы:**

Первая часть работы – работа с консольной утилиты nslookup. Она посвящена получению практических навыков диагностики DNS-серверв.

1. С помощью консольной утилит nslookup определите адреса хостов обслуживающих почтовый домен yandex.ru (запрос необходимо выполнить к NS северу сети RunNet (домен runnet.ru)).
2. С помощью консольной утилит nslookup определите каноническое имя (CNAME) для хоста proxy.ifmo.ru.
3. С помощью консольной утилит nslookup определите e-mail администратора DNS сервера зоны.ifmo.ru (запрос можно следует к DNS серверу зоны ifmo.ru).

Разберитесь, какие типы DNS записей вам понадобятся в каждом случае. Определить адрес DNS сервера, обслуживающего конкретную зону можно также с помощью утилиты nslookup. Используйте встроенную справку утилиты (в утилите знак ?).

Во второй части идет работа с DNS-севером. В этой части работы необходимо установить DNS-сервер, настроить на нем зону второго уровня и настроить ваш Windows XP на работу через этот DNS-сервер. Принципиальная схема представлена на рис.1

4) Запустите на одном компьютере в программе VMWare виртуальную систему Windows 2003 из каталога c:\vm.



Рис. 1

5) В виртуальной операционной системе Windows 2003:выставите автоматическое получение IP-адресов. Определите какой IP адрес получит ваш виртуальный сервер с DHCP сервера компьютерного класса и запишите его.

1. В конфигурации TCP/IP установите адрес DNS равный IP адресу вашего Windows 2003 сервера.
2. Установите DNS-сервер для обслуживания зоны с именем «Моя\_фамимлия.loc», где loc – виртуальный домен первого уровня. Например sumkin.loc.Сервер естественно должен быть primary.

Установить сервер можно так: Панель управления\ Добавить удалить

программу \ Установка компонентов windows \ Сетевые службы ->

Дополнительно -> DNS

Зоны добавляются в консоли DNS (на папке Зоны прямого просмотра –

контекстное меню -> добавить зону).

Указывайте имя зоны с доменом первого уровня .loc!

1. Настройте ваш DNS-сервер так, чтобы он запрашивал внешний сервер с адресом 194.85.32.18 в случаях когда сам не способен разрешить имена. (Свойства сервера)
2. В основной операционной системе, в которой запущена VMWare, установите в свойствах TCP\IP адрес DNS сервера, равный IP вашего виртуального сервера.
3. В вашем DNS-сервере создайте:
4. А запись на сервер Mirror (192.168.3.1), и алиасы на него (WWW, MAIL).
5. Основную зону обратного просмотра (Reverse Zone) на ваш домен с автоматическим импортом данных.
6. Из вашей родительской системы (windows XP) с помощью команды ping проверьте
доступность хоста WWW в вашем домене ([www.sumkin.loc](http://www.sumkin.loc)). Обратите внимание с какого
доменного имени идет ответ

10) Выполните ping запрос к хосту [www.novell.com](http://www.novell.com) для проверки работы вашего DNS в рекурсивном режиме.

**В отчет:**

в теме письма: №группы ФИО №работы (например: 3155 Фёдор Сумкин 7)

В теле письма:

1. консольный вывод команды nslookup по первым трем заданиям.
2. консольный вывод команды ping из задания №9

Ответы на вопросы:

1. в каком режиме работает ваш DNS-сервер (рекурсивном или нет)?
2. Приведите несколько адресов корневых DNS серверов «известных» вашему DNS-серверу по умолчанию.
3. Если в свойствах вашего DNS удалить перенаправление запроса на DNS север класса то разрешение имени внешних хостов (как в 10 задании) будет работать, но значительно медленнее. Почему?
4. В чем назначение зоны обратного просмотра?
5. Опишите значения полей записи SOA.

Для тех, кто решит выполнить работу в иной ОС (например Linux) следует готовить этот отчет в терминах и применительно к другой ОС.