МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ЧЕРНИГОВСКИЙ НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ
КАФЕДРА ИНФОРМАЦИОННЫХ И КОМПЬЮТЕРНЫХ СИСТЕМ

АНАЛИЗ ФУНКЦИОНИРОВАНИЯ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Методические указания
к выполнению самостоятельных работ
по дисциплине „Компьютерные сети”
для студентов направления подготовки
6.050102 „Компьютерная инженерия”

Утверждено
на заседании кафедры
информационных и компьютерных систем

Протокол № 2 от «27» сентября 2013 г.

Чернигов ЧНТУ 2013

Аналіз функціонування локальних обчислюваних мереж. Методичні вказівки до виконання самостійних робіт з дисципліни „Комп'ютерні мережі" для студентів напряму підготовки 6.050102 "Комп'ютерна інженерія" / Укл. Є. В. Риндич. – Чернігів: ЧНТУ, 2013. – 22 с., рос. мовою.

Укладачі: Риндич Євген Володимирович, кандидат технічних наук, доцент кафедри інформаційних та комп'ютерних систем

Відповідальний за випуск: Казимир Володимир Вікторович, завідувач кафедри інформаційних та комп'ютерних систем, доктор технічних наук, професор

Рецензент: Нікітенко Євгеній Васильович, кандидат фізико-математичних наук, доцент кафедри інформаційних та комп'ютерних систем Чернігівського національного технологічного університету

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Межсетевой протокол IP на сегодняшний день доминируют как в локальных, так и в глобальных сетях. С развитием сети Интернет стек протоколов TCP/IP «оброс» огромным количеством сетевых сервисов, что и обусловило доминирование данного семейства протоколов во всех разновидностях сетей.

Данное руководство предназначено для начального знакомства со стеком протоколов TCP/IP, а так же взаимодействию межсетевого протокола с несущими сетями, в частности, с сетями, построенными по технологии Ethernet.

Цикл лабораторных работ, предлагаемый в данном пособии, поможет студентам усвоить базовые навыки по конфигурированию сетевых интерфейсов и устройств, диагностике сети, работе с сетевыми анализаторами.

1 Самостоятельная работа №1. Технические особенности сети Ethernet. Конфигурирование и настройка сетевых интерфейсов

1.1 Цель работы

Познакомиться с особенностями реализации сети Ethernet, изучить её характеристики. Познакомится и получить практические навыки конфигурирования сетевых интерфейсов в различных ОС.

1.2 Краткие теоретические сведения

Логическое устройство, осуществляющее передачу данных в сети на логическом уровне называется сетевым интерфейсом. Сетевой интерфейс может быть связан с определённым физическим устройством, - например, адаптер Ethternet или последовательный порт, а может быть просто логическим интерфейсом , например, интерфейс локальной обратной связи.

Сетевые интерфейсы делятся на 2 основных типа: интерфейс в широковещательную сеть, broadcast, например, Ethernet и интерфейс “точка-точка”, point-to-pint. Первые ассоциируются с одним сетевым адресом, вторые – с двумя, локальным и удаленным адресом. Сетевой интерфейс может использоваться для передачи данных по различным протоколам: IP v.4, IP v.6, IPX, AppleTalk и т.д. Наибольшее распространение получил на сегодня протокол IP v.4 (далее – IP), поскольку он используется в Интернете. В ОС Windows возможно использование протокола NetBIOS, однако, с точки зрения “прозрачности” сети рекомендуется использовать как основной протокол IP, с которым ассоциируются службы протокола NetBIOS. В ОС UNIX используются дополнительные программы для организации сервисов протокола NetBIOS (пакет Samba) поверх IP. Далее будем рассматривать только протокол IP.

Сетевые интерфейсы могут иметь псевдонимы, т.е. с интерфейсом могут ассоциироваться несколько сетевых адресов. Псевдонимы позволяют использовать различные схемы адресации на одном сегменте сети. Например, возможно одновременное использование приватных и публичных IP адресов.

Для конфигурирования сетевых интерфейсов в POSIX-совместимых ОС используется команда ifconfig. Команда ifconfig без параметров выдает текущую конфигурацию активных сетевых интерфейсов.

1.3 Ход работы

1. Изучить инструкцию по эксплуатации сетевого адаптера и определить:
   а) тип среды передачи, используемые соединители и скорость передачи информации;
   б) назначение переключателей на сетевом адаптере и их заводскую установку;

в) количество компьютеров, которые могут быть соединены вместе;
г) схемы подключения WS при использовании коаксиального кабеля и витой пары;
д) способы объединения отдельных сегментов в единую сеть.

2. Определить реальную пропускную способность сети Ethernet с использованием коммутатора:

а) при одновременном обращении 2, 4 и 6 WS к выделенному серверу;
б) при одновременном взаимодействии 2, 4 и 6 WS между собой.

Примечание: пропускную способность определять по скорости записи/чтения файлов большого размера (> 10МБ). Использовать команду ping. Провести эксперименты с различными вариантами запуска команды с использованием различных ключей.

3. Построить графические зависимости пропускной способности сети на витой паре от числа взаимодействующих рабочих станций. Повести анализ и описать структуру ЛВС ЧГТУ.

4. Проанализировать состояние сетевых интерфейсов с помощью команды ipconfig, ifconfig. Ознакомьтесь с документацией по командам. Выявить их различия.

1.4 Содержание отчета

1. Описание сетевого адаптера (технические характеристики и состояние переключателей).
2. Способы объединения сегментов.
3. Анализ полученных графических зависимостей пропускной способности сети от числа рабочих станций.
4. Графики и расчеты пропускной способности.
5. Схема и анализ ЛВС ЧГТУ.
6. Результаты и описание выполненных команд.

1.5 Контрольные вопросы

1. Какие параметры сетевого интерфейса свидетельствуют о проблемах в физической среде передачи данных?
2. Какие параметры интерфейса свидетельствуют о чрезмерной загрузке сети?
3. Какое среднее значение задержки в сети 100 Мбит/с?
4. Чем определяется время задержки в сети Ethernet?
5. Почему в стандарте 100baseT длина некоммутируемого сегмента не должна превышать 100 метров? Подкрепите ваше утверждение расчетами времени распространения 1 бита информации и одного кадра информации.
6. Перечислите основные параметры команды ifconfig при конфигурировании широковещательного сетевого интерфейса.
7. Перечислите основные параметры команды ifconfig при конфигурировании сетевого интерфейса точка-точка.

8. Опишите процесс конфигурирования сетевого интерфейса в ОС RedHat Linux при загрузке.
9. Как добавить сетевой интерфейс? Как добавить псевдоним для сетевого интерфейса?
10. Какое время занимает один пакет данных в сети Ethernet 100BaseT?
11. Почему в некоммутируемых сетях Ethernet максимальная длина соединительного кабеля не должна превышать 100м?
12. При каком уровне загрузки сети Ethernet процент потерь возрастает до критического?
13. Сколько времени нужно наблюдать сеть, что бы оценить уровень потерь пакетов?
14. В каком случае в канале допустимы значительные (>250ms) задержки?
15. Как снизить загрузку сети служебными данными?
16. Какой средний процент “полезных” данных в сетевом трафике Вы наблюдали при перекачке файла по протоколу FTP?
17. Объясните, зачем в ходе экспериментов использовалось 3 хоста.
18. Имеется коммутатор на 16 портов 100BaseT с общей пропускной способностью коммутирующей матрицы 1.2 Гбит/с. Оцените качество данного коммутатора.
19. Поясните, почему длина кабеля в коммутируемом сегменте Ethernet 100BaseT может превышать установленные стандартом 100 метров при сохранении удовлетворительной работы сети. На что влияет избыточная длина кабеля?

2 Самостоятельная работа №2. Изучение сетевых анализаторов tcpdump и Ethereal

2.1 Цель работы

Изучить сетевые анализаторы tcpdump и Ethereal. Провести исследования сетевого трафика и выявить его особенности.

2.2 Краткие теоретические сведения

Утилита tcpdump предназначена для анализа сетевого трафика и входит в поставку всех POSIX систем. Эта утилита выводит заголовки пакетов, которые соответствуют заданным критериям, на сетевом интерфейсе, переведенном предварительно в режим приема всех пакетов (promiscous mode). Критерии задаются в форме логического выражения.

Логические выражения для критериев необходимы для того, что бы из общего сетевого трафика выделить только интересующие нас пакеты. Синтаксис логических выражений включает следующие ключевые слова:

host - IP адрес или DNS имя хоста

net - адрес сети, например

net 192.168.7, net 192.168.7.0 mask 255.255.255.224

port – номер порта (имеет смысл для протоколов TCP и UDP)

proto – тип протокола. Возможные типы: ether, fddi, tr, ip, ip6, arp, rarp, decnet, lat, sca, moprc, mopdl, iso, esis, isis, icmp, icmp6, tcp and udp. Например, tcpdump tcp port 80

dir – направление, возможные значения – src или dst . Например, ***`tcpdump src host kid.stu`***.

Кроме того, можно использовать адреса несущей сети Ethernet: ***`tcpdump ether dst 00:02:44:5b:ee:9b`*** или IP сеть: ***`tcpdump net src 192.168.7.0/27`***

Более полную информацию о возможностях утилиты tcpdunp можно получить из стандартной страницы помощи, дав команду man tcpdump.

Сетевой анализатор Wireshar(Ethereal) построен на той же библиотеке (libpacap), что и утилита tcpdump, но имеет удобный графический пользовательский интерфейс.

2.3 Ход работы

1. Проведите захват пакетов утилитой **ethereal** без фильтра в течение нескольких минут и внимательно просмотрите результат. Отметьте, какие протоколы используются в сети.
2. Настройте фильтр на захват только широковещательных пакетов. Произведите захват в течение нескольких минут, рассмотрите результат.

3. Настройте фильтр на захват пактов ICMP. Проверьте результат, включив захват пакетов и запустив со своего хоста команду ping на соседний хост.
4. Не меняя настроек фильтра, запустите захват пакетов и запустите ping на другом хосте, направленый на третий хост в вашем сегменте. Удалось ли Вам захватить эти пакеты? Объясните результат.
5. Запустите утилиту tcpdump с пустым фильтром с перенаправлением пакетов в файл на несколько минут с ключами, обеспечивающими расшифровку пакетов. Поясните результат захвата пакетов.

2.4 Содержание отчета

Отчет должен содержать последовательность скриншотов по ходу выполнения работы и соответствующие комментарии.

2.5 Контрольные вопросы

1. Почему Вы не видите все пакеты, проходящие в данном сегменте Ethernet?
2. В каком случае хост может видеть все пакеты в данном сегменте Ethernet?
3. Какие пакеты будут видны наблюдающему хосту в коммутируемом сегменте Ethernet?
4. Как обеспечить захват всех пакетов, приходящих в данный сегмент сети и уходящих из него?
5. Что такое “зеркальный” порт коммутатора, и каково его назначение?
6. Какой параметр коммутатора отвечает за общую пропускную способность?

3 Самостоятельная работа №3. Изучение сетевого протокола TCP и протокола уровня приложений telnet

3.1 Цель работы

Изучить сетевой протокол TCP и протокол приложений telnet. Определить основные этапы и особенности использования протоколов.

3.2 Краткие теоретические сведения

Протокол TCP является транспортным протоколом с гарантированной доставкой данных, с установлением соединения и повторной передачей потерянных сегментов.

Установление соединения происходит при помощи механизма т.н. троекратного рукопожатия (three way handshake).

Хост А, инициатор соединения, посылает сегмент без данных с установленным флагом SYN. Инициирует соединения программа - клиент. Порт назначения определяется жёстко либо как хорошо известный сервис (Well Known Service), например web-сервис обычно имеет порт 80, либо задается пользователем. Порт источника обычно выделяется системой из пула свободных не привилегированных портов (>1023).

В ответ хост В посылает сегмент без данных с установленными флагами SYN,ACK. При этом, в зависимости от режима работы серверного сокета, возможна замена фиксированного порта на динамический в качестве исходящего.

Хост А, приняв описанный выше пакет, сигнализирует о готовности к обмену данными, посылая сегмент без данных с установленным флагом ACK. После этого сокеты готовы к двунаправленному обмену данными.

Разрыв соединения происходит аналогично с использованием флага FIN.

Протокол TELNET является протоколом уровня приложений, предназначенным для удалённого доступа по сети к текстовому терминалу. При инициализации соединения посылаются команды и клиентом, и сервером, обеспечивающие согласование возможностей пользовательского терминала и установку необходимых переменных окружения на сервере.

3.3 Ход работы

1. Установите сервис telnet на соседней рабочей станции (назовём ее host2). Для этого в директории /etc/xinetd.d в файле telnet строку "disabled = yes" замените строкой "disabled = no" и перезапустите сервис xinetd командой **/etc/rc.d/init.d/xinetd restart.**
2. Проверьте работоспособность сервиса: telnet host2. Вы должны получить терминальный доступ к машине host2.
3. Запустите на своей рабочей станции (далее -host1) программу захвата пакетов ethereal с фильтром, ограничивающим захват трафика между

host 1 и host2 по протоколу tcp, что бы в захваченные пакеты не попадал "мусор". Стартуйте захват пакетов.

4. В терминальном окошке запустите сессию telnet на host2. Войдите в систему, введя логин и пароль. Выйдите из системы командой logout. Поместите протокол сессии в файл для отчёта.
5. Остановите захват пактов и сохраните результат в формате tcpdump. Сохранённый результат захвата подайте на вход утилиты tcpdump и результат разбора перенаправьте файл для отчёта.
6. Изучая параллельно протокол сессии telnet, результаты захвата пакетов в окне ethereal и в файле с разобранными пакетами, найдите и прокомментируйте: установление и разрыв соединения по протоколу TCP с учётом флагов; пакеты, содержащие логин и пароль пользователя.
7. Покажите механизм инкапсуляции данных на примере пакета с данными от host2.

3.4 Содержание отчета

Отчет должен содержать протокол telnet сессии и распечатку дампа tcpdump. Пакеты, содержащие существенную информацию для данной лабораторной работы, должны быть тщательно прокомментированы. Кроме того, отчёт должен содержать выводы, описывающие процесс изучения протоколов TCP и telnet.

3.5 Контрольные вопросы

1. Из каких уровней состоит стек TCP/IP и для чего они предназначены?
2. Формат заголовка протокола TCP/IP?
3. Установление соединения, передачи данных и завершения соединения между клиентом и сервером с помощью протокола TCP/IP?
4. В чем состоят особенности протокола telnet?

4 Самостоятельная работа №4.Изучение сетевого протокола UDP и протокола уровня приложений DNS

4.1 Цель работы

Изучить сетевой протокол UDP и протокол уровня приложений DNS. Определить основные этапы и особенности использования протоколов.

4.2 Краткие теоретические сведения

Протокол UDP является простейшим транспортным протоколом без гарантии доставки данных и без установления соединения. Данный протокол обеспечивает мультиплексирование данных между приложениями при помощи поля port а так же контроль правильности данных при помощи поля checksum. Данный протокол используется для обмена короткими структурированными данными в режиме "запрос-ответ" а так же для посылки широковещательных сообщений. По сравнению с протоколом TCP этот протокол обеспечивает большее быстродействие, поскольку не имеет затрат на установку и разрыв соединения. Удобно так же применение протокола UDP для случаев специаль6ного транспорта, когда транспорт TCP по каким-либо соображениям не устраивает разработчика. Однако следует отметить, что механизмы подтверждения и сборки потока в этом случае должны обеспечиваться приложением.

Служба доменных имён DNS является основной системной службой в сетях TCP/IP, поскольку эта служба обеспечивает разрешение символьных имён в IP адреса и наоборот. Каждое приложение, использующее сетевые функции, обращается к базовой системной библиотеке libc, частью которой является так называемый резольвер (resolver). Резольвер имеет свой файл конфигурации /etc/resolv.conf, в котором описаны ближайшие сервера имён и порядок подстановки суффиксов.

order bind,hosts
search stu stu.cn.ua
nameserver 192.168.0.10
nameserver 192.168.0.14

В сети должно быть как минимум два сервера имён для обеспечения бесперебойного разрешения имён. Обращение резольвера происходит сначала к первому серверу, и если ответ не получен в течение короткого времени, ко второму. Если сервер не может самостоятельно отработать запрос, он обращается к серверам домена корневого домена "." и производит поиск сервера, способного обработать запрос. Полученный ответ перенаправляется клиенту и кешируется на сервере для ускорения последующих ответов.

4.3 Ход работы

1. Запустите анализатор ethereal с фильтром, настроенным на отслеживание трафика от вашего хоста до сервера DNS (далее - dns_host) и до сервера www (далее - www_host).
2. Проверьте работоспособность фильтра командами

ping www_host
ping dns_host

Анализатор должен показать захваченные пакеты.

3. Перестартуйте захват пакетов.
4. Запустите программу просмотра web на хост www_host.
5. Сохраните захваченные пакеты в формате libpcap.
6. Запустите анализатор tcpdump для разбора сохранённого файла со следующими ключами:

tcpdump -vvv -X -r файл_пакетов >файл_разбора

Данный файл будет содержать разобранные пакеты обращения браузера к веб-страничке и к серверу DNS.

7. Используя оба анализатора, отследите, как происходили обращения к серверам и прокомментируйте в файле все пакеты.
8. Запустите новую сессию захвата пакетов.
9. Выполните команды **host www.yahoo.com** и **host 193.193.193.100** и повторите описанную выше процедуру для захваченных пакетов.
10. Подробно разберите все запросы к серверу DNS.

4.4 Содержание отчёта

Отчет должен содержать прокомментированные файлы с разобранными результатами захвата пакетов. Пакеты, не представляющие особого интереса в ключе данной работы можно удалить из файла дампа.

4.5 Контрольные вопросы

1. Почему для службы DNS используется протокол UDP?
2. Какое поле заголовка UDP обеспечивает мультиплексирование пакетов между приложениями?
3. Как программы определяют, где находится ближайший сервер имён?
4. Какие дополнительные параметры передаются в ответе сервера имён?
5. Какого типа запросы отрабатывались при просмотре веб-странички?
6. Какой запрос использовался для определения имени хоста по его адресу?

5 Самостоятельная работа №5. Конфигурирование службы имён DNS в корпоративной сети

5.1 Цель работы

Научиться конфигурировать и тестировать службу имен для корпоративной сети на основе сервера DNS bind.

5.2 Краткие теоретические сведения

Служба доменных имён DNS является основной системной службой в сетях TCP/IP, поскольку эта служба обеспечивает разрешение символьных имён в IP адреса и наоборот. Каждое приложение, использующее сетевые функции, обращается к базовой системной библиотеке libc, частью которой является так называемый резольвер (resolver). Резольвер имеет свой файл конфигурации /etc/resolv.conf, в котором описаны ближайшие сервера имён и порядок подстановки суффиксов.

В сети должно быть как минимум два сервера имён для обеспечения бесперебойного разрешения имён. Обращение резольвера происходит сначала к первому серверу, и если ответ не получен в течение короткого времени, ко второму. Если сервер не может самостоятельно отработать запрос, он обращается к серверам домена корневого домена "." и производит поиск сервера, способного обработать запрос. Полученный ответ перенаправляется клиенту и кешируется на сервере для ускорения последующих ответов.

5.3 Ход работы

Выполнение данной лабораторной работы состоит из следующих шагов:

1. Создайте файлы зон для прямой и обратной приватной зоны. Возьмите блок адресов 172.16.X.0, где X – номер машины в классе. Сконфигурируйте первичный сервер DNS для этих зон на локальном компьютере и запустите его. Не забудьте, что все сообщения выводятся не на консоль, а в системный журнал. Сообщения удобнее всего просматривать в отдельном терминале командой:

tail -f /var/log/messages

2. Проведите тестирование созданных прямой и обратной зон при помощи команды ***dig***.
3. Проведите тестирование разрешения внешних имён вашим сервером. Запросите, например информацию о зоне slashdot.org.
4. Сконфигурируйте ваш сервер как вторичный для зон, которые создал ваш сосед по лаборатории. Произведите корректировку и проверку записей зон на предмет записей типа NS. Произведите проверку командой ***dig***, обращая особое внимание на секцию “AUTHORITY SECTION”.

5.4 Содержание отчета

Отчет должен содержать файлы зон, файл конфигурации сервера и результаты проверок. Наличие комментариев и выводов необходимо.

5.5 Контрольные вопросы

1. Почему для корпоративных зон удобнее использовать 3-х буквенные имена?
2. В каком случае сервер имён считается авторитетным?
3. Какие параметры отвечают за время обновления зоны вторичным сервером?
4. Как обеспечить защиту зоны от скачивания и от просмотра?
5. Какая запись RR применяется при создании виртуальных серверов?
6. Какая запись RR задаёт почтовый обменник для всей зоны?
7. Кокой файл содержит адреса корневых серверов имен, необходимых для инициализации кеша и рекурсивних запросив?
8. Что такое рекурсивный запрос?
9. Как производится установка ведомого сервера для конкретной зоны?

6 Самостоятельная работа №6. Сервисы для сетей Windows. Настройка сервиса Samba

6.1 Цель работы

Получить навыки в настройке сервиса на основе свободно распространяемого пакета Samba, обеспечивающего основные сервисы для рабочих станций под управлением ОС Windows.

6.2 Краткие теоретические сведения

Samba — пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных операционных системах попротоколу SMB/CIFS. Имеет клиентскую и серверную части. Является свободным программным обеспечением, выпущена под лицензиейGPL.

Samba первоначально назывался smbserver, но название было изменено в связи с извещением от компании «Syntax», которая является владельцем товарного знака на «SMBserver», о нарушении права на торговую марку.

6.3 Ход работы.

Лабораторная работа выполняется на 2-х компьютерах, один из которых работает под управлением ОС Windows, другой – под управлением ОС Linux.

Перед выполнением работы необходимо проверить, установлены ли необходимые пакеты, для этого выполните команду ***rpm –qa | grep samba*** .

На первом, ознакомительном этапе, необходимо запустить утилиту управления сервисами Samba Web Administration Tool – ***swat*** и сконфигурировать сервер в простейшем варианте – выделить домашние директории и один общий публичный ресурс.

На втором этапе необходимо изучить возможности сервера Samba и директивы конфигурации. Построение контроллера домена Active Directory не входит в данную работу.

Установка простого сервиса разделения ресурсов. Современные ОС для настольных ПК имеют в составе графических утилит управления системой имеют утилиту управления сервером Samba, однако наиболее полный интерфейс управления поставляется разработчиками Samba. Обычно, его нучно устанавливать отдельно командой:

yum install samba-swat

Программа swat запускается как сервис через сетевой супер-демон xinetd. Конфигурация отдельных сервисов находится в директории /etc/xinetd.d. Откройте файл /etc/xinetd.d/swat в редакторе и измените следующие опции:

disable = no

bind = 127.0.0.1

Первая опция разрешает сервис, вторая задает адреса, для которых сервис доступен. Если вы собираетесь запускать браузер на другом компьютере, то ее необходимо закоментировать. Дальше необходимо перезапустить сервис xinetd командой ***/etc/init.d/xinetd restart***.

Теперь нужно запустить браузер и указать следующий адрес: **http://localhost:901**. Браузер запросит параметры авторизации, необходимо ввести логин root и соответствующий пароль. Ниже на рисунке 6.1 приведен интерфейс программы.

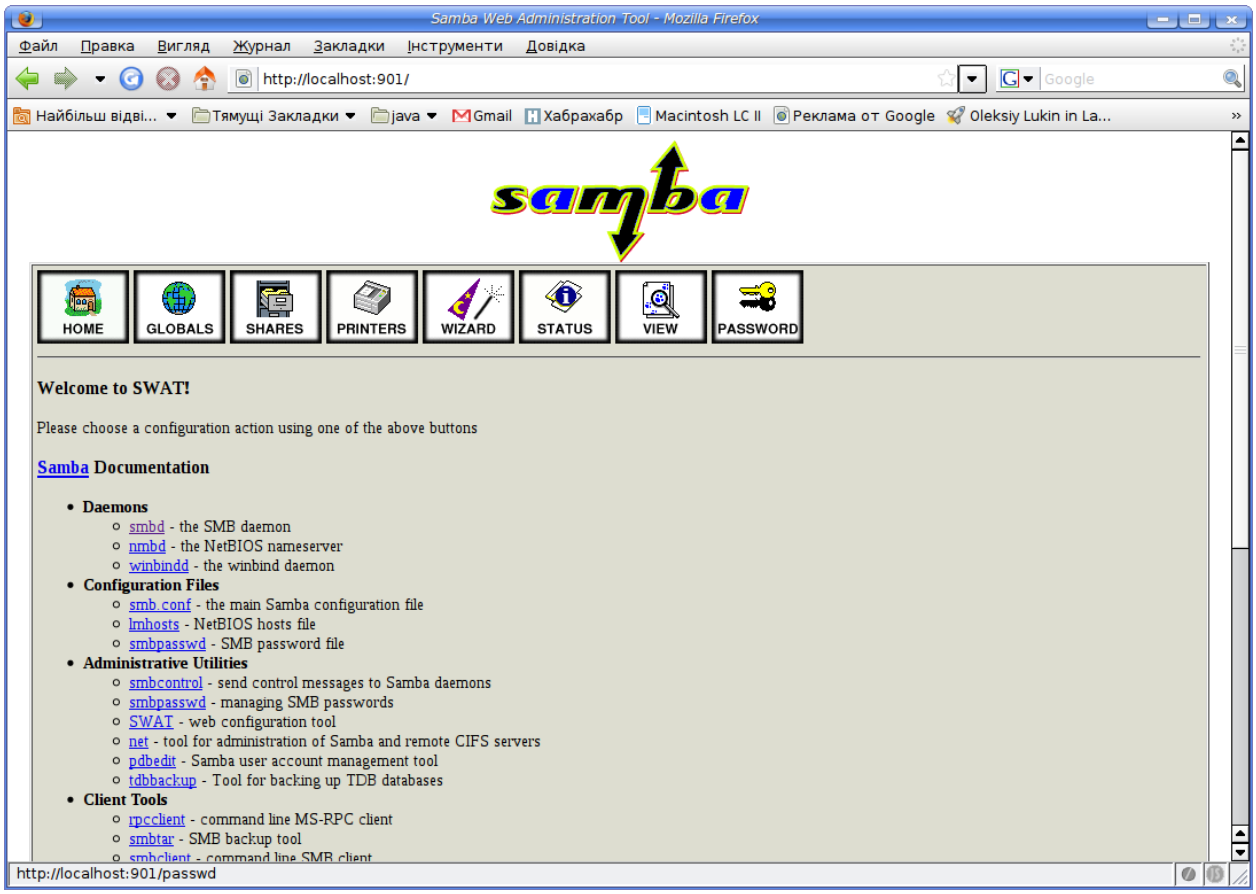

Рисунок 6.1 – Интерфейс управления программы swat

При удачном входе программа swat загружает страничку с документацией. Если установлен пакет с документацией samba, то все ссылки будут указывать на файлы на локальной файловой системе. Рекомендуется перед выполнением работы прочесть первую часть «Samba by Example».

Верхний набор пиктограмм используется для выбора режимов управления. Пиктокрамма «Globals» выбирает страницу управления секцией [globals] файла конфигурации smb.conf, т.е. настройками сервера. Пикторгамма «Shares» выбирает страницу выделения ресурсов, «Printers» - деления принетеров. Пиктограмма «Wizard» указывает на страницу быстрой настройки сервера, пиктограмма «Status» выбирает страницу просмотра и перезапуска сервисов, пиктограмма «View» позволяет просмотреть файл конфигурации smb.conf, и, наконец, пикторгамма «Password» уазывает на страницу управления пользователями.

Для начала выберите пиктограмму «Wizard» и настройте сервер в режим простой рабочей станции, не являющейся контроллером домена. Через пиктограмму «Shares» выделите домашние директории пользователей и один общий ресурс. Обратите внимание, что права UNIX являются определяющими, поэтому директория, в которую ползователи должны иметьправо на запись, должна иметь соответсвующих владельца, группу и права. Рекомендуется завести группу smbusers и включить в нее ваших пользователей средствами ОС.

Выделите в качестве доступных ресурсов домашние каталоги пользователей и какй-нибудь общий для всех катflог. Перезапустите сервер и проверьте выделенные ресурсы, как описано в разделе «Тестирование сервера».

Просмотрите файл конфигурации smb.conf и прочтите помощь по всем опциям, включенным в данной режиме.

Тестирование сервера. Для тестирования samba-сервера необходимо создать пользователя. Сначала создаем группу:

/usr/sbin/groupadd smbusers

Затем создаем пользователя:

useradd -c Test Samba -g smbusers -s /bin/false smbtester

Добавляем нашего тестового пользователя в список пользователей samba:

smbpasswd-a smbtester

Запуск сервера осуществляетс/ командой ***/sbin/service smb start***

Проверим корректность запуска сервера в системной журнале:

tail /var/log/messages

Проверяем доступность ресурсов samba-сервера сначала с локальной машины:

smbclient -L localhost smb_user

После проверки работоспособности сервера необходимо выполнить настройку рабочих станций Windows. Для этого необходимо на соседней машине загрузит операционную систему Windows, в режиме пользователя – администратора. Проверка сервера будет заключаться в подключении сетевого диска и установки системного времени, синхронизированного с samba-сервером. Желательно использовать не графическую оболочку, а оболочку cmd. Для работы с сетевыми ресурсами используется команда ***net.***

Присоединение сетевых дисков осуществляется командой net use, например:

net use h: \\ics-73-10\student

Команда ***net use*** без параметров показывает текущее использование сетевых ресурсов. Новые подключения будут запомнены.

```
Состояние  Локальный  Удаленный              Сеть
-------------------------------------------------------------
OK   Y:    \\ics-73-10\rt         Microsoft Windows Network
OK   Z:    \\ics-73-10\rt         Microsoft Windows Network
Отсоединен \\192.168.7.48\IPC$    Microsoft Windows Network
```

Команда выполнена успешно.

Команда ***net view*** показывает видмые в сети ресурсы:

```
Общие ресурсы на \\ics-73-10
73 samba server
Имя общего ресурса  Тип   Используется как  Комментарий
-------------------------------------------------------------
phenom              Диск                    Home directory of phenom
rt                  Диск  Z:                Mary's and Fred's stuff
Команда выполнена успешно.
```

Команда ***net time*** показывает, а с параметром ***/set*** устанавливает локальное время по серверу:

```
Текущее время на \\ics-73-10 равно 12/7/2005 12:44 PM
Команда выполнена успешно.
```

6.4 Содержание отчета

Отчет должен содержать файл конфигурации сервиса samba, а также отображать результаты всех выше указанных настроек сервиса. Наличие соответствующих комментариев и выводов необходимо.

6.5 Контрольные вопросы

1. Что такое сетевой сервис Samba?
2. Как установить пакет Samba? Какие демоны необходимы для работы Samba?
3. Какие настройки необходимо выполнить минимально для пакета Samba?
4. Как производится выделение домашних каталогов пользователей?
5. Как установить время на рабочей станции по серверу Samba?
6. Как настроить кириллицу в именах файлов и каталогов?

7 Самостоятельная работа №7. Конфигурирование службы DHCP в корпоративной сети

7.1 Цель работы

Ознакомиться с сервисом DHCP, а также получить навыки в его настройке.

7.2 Краткие теоретические сведения

DHCP (*Dynamic Host Configuration Protocol* — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому *серверу DHCP*, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP-адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP.

7.3 Ход работы

Выполнение лабораторной работы состоит из следующих шагов:

1. Проверка наличия установленных пакетов dhcp (команда rpm –qa | grep dhcp). Если пакеты установлены – приступаем к работе (шаг два), если нет – устанавливаем необходимые пакеты (dhcpd-XXX.rmp).
2. Создание конфигурационного файла сервера /etc/dhcpd.conf по приведенному выше примеру (подробности man dhcpd.conf).
3. Настройка одной из машин в аудитории на получение IP адреса автоматически. Зафиксируем результаты в отчете (ifconfig /all на клиенте и /var/lib/dhcp/dhcpd.leases на сервере).
4. Создание статической записи для каждого клиента сети на основе файла /var/lib/dhcp/dhcpd.leases. Зафиксируем результат в отчет.

7.4 Содержание отчета

Отчет должен содержать конфигурационный файл сервера /etc/dhcpd.conf, а также отображать результаты всех выше указанных действий. Наличие соответствующих комментариев и выводов необходимо.

7.5 Контрольные вопросы

1. Что представляет собой DHCP?

2. Как сконфигурировать DHCP-сервер под Unix?
3. Как сконфигурировать DHCP-клиент под Unix?
4. Какие основные параметры указываются в фале конфигурации dhcpd.conf?
5. Опишите механизм выделения IP-адресов с помощью сетевого сервиса DHCP.
6. В каком случае рекомендуется выделять фиксированные адреса хостов?
7. Какие параметры получает рабочая станция от сервера DHCP?

Рекомендованная литература

1. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы. СПб., Питер, 2001-672с.:ил, ШЫИТ 5-8046-0133-4
2. Э. Таненбаум. Компьютерные сети. / Пер. с англ. Под ред. д – К.: BHV, 2002 р.
3. Craig Hunt. TCP/IP network adminisration. O'Relly & Associates, Inc, 1994-1998. 472 pages.
4. http://www.freebsd.org/handbook– Проект документирования FreeBSD
5. http://www.isc.org Сайт проектов bind, dhcpd
6. http://www.kernel.org/LDP – Проект документирования Linux
7. http://www.rfc-editor.org RFC center
8. http://www.samba.org Сайт проекта Samba
9. UNIX. Пособие системного администратора. / Пер. с англ. Под ред. д – К.: BHV, 2002 р.