Федеральное агентство по образованию

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ГОУВПО “АмГУ”

УТВЕРЖДАЮ

Зав.кафедрой ИУС

_____А. В. Бушманов

“_____”_____2007г.

АДМИНИСТРИРОВАНИЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО ДИСЦИПЛИНЕ

Для специальности: 230201 – “Информационные системы и технологии”

Составитель: С.С. Охотников

Благовещенск

2007 г.

Печатается по решению
редакционно-издательского совета
факультета математики и информатики
Амурского государственного
университета

С.С. Охотников
Учебно-методический комплекс по дисциплине "Администрирование в информационных системах" для студентов очной формы обучения специальности 230201 – “Информационные системы и технологии”
– Благовещенск: Амурский гос. ун-т, 2007. – 50 с.

Учебно-методический комплекс предназначен для оказания помощи преподавателям и студентам очной формы обучения по дисциплине "Администрирование в информационных системах" для студентов очной формы обучения специальности 230201 – “Информационные системы и технологии” и может использоваться для подготовки и проведения занятий, а также для самостоятельного изучения дисциплины.

СОДЕРЖАНИЕ

Федеральное агентство по образованию РФ

Амурский государственный университет

УТВЕРЖДАЮ

Проректор по УНР

_____ Е. С. Астапова

“_____”_____ 200___ г.

РАБОЧАЯ ПРОГРАММА

По дисциплине “Администрирование в информационных системах”

Для специальности: 230201 – “Информационные системы и технологии”

Курс – 4 семестр – 7

Лекции– 30 час. Экзамен – 7 семестр

Курсовая работа – 7 семестр

Практические (семинарские) занятия –нет Зачет – нет

Лабораторные занятия – 30 час.

Самостоятельная работа – 50 час.

Всего часов – 110 час.

Составитель: Охотников С. С., ст. преподаватель

Факультет: Математики и информатики

Кафедра : Информационных и управляющих систем

2006 г.

Рабочая программа дисциплины составлена на основании Государственного образовательного стандарта высшего профессионального образования для специальности 230201 - “Информационные системы и технологии” и примерной программы дисциплины, рекомендуемой МО РФ.

Рабочая программа обсуждена на заседании кафедры

"__" _____200___ г., протокол № _____

Заведующий кафедрой _____

Рабочая программа одобрена на заседании

УМС_____"__" _____200___ г., протокол № _____

(наименование специальности)

Председатель _____

(подпись, И.О.Ф.)

Рабочая программа переутверждена на заседании кафедры от _____

протокол № _____ .

Зав.кафедрой _____

Подпись Ф.И.О.

СОГЛАСОВАНО

Начальник УМУ

_____

(подпись, И.О.Ф.)

“__” _____200___ г.

СОГЛАСОВАНО

Председатель УМС факультета

_____

(подпись, И.О.Ф.)

“__” _____200___ г.

СОГЛАСОВАНО

Заведующий выпускающей кафедрой

_____

(подпись, И.О.Ф.)

“__” _____200___ г.

Госстандарт:

Функции, процедуры и службы администрирования; объекты администрирования; программная структура; методы администрирования. Службы управления конфигурацией, контролем характеристик, ошибочными ситуациями, учетам и безопасностью; службы управления общего пользования; информационные службы; интеллектуальные службы; службы регистрации, сбора и обработки информации; службы планирования и развития; эксплуатация и сопровождение информационных систем; инсталляция ИС. Оперативное управление и регламентные работы; управление и обслуживание технических средств; аппаратно-программные платформы администрирования; информационные системы администрирования; организация баз данных администрирования; программирование в системах администрирования; примеры систем администрирования.

1. Цели и задачи дисциплины.

1.1. Целями преподавания данной дисциплины являются ознакомление с принципами работы систем администрирования и управления в информационных системах, изучение их программно-аппаратной структуры, функций, специальных и общей процедур административного управления.

1.2. Задачи дисциплины состоят в определении места изучаемых процессов и аппаратуры среди других технических систем, построении изучаемых систем в различных предметных областях, оценке их характеристик.

1.3. Перечень дисциплин с указанием разделов (тем), усвоение которых студентами необходимо при изучении данной дисциплины: Все темы дисциплны “Операционные системы”

2. Содержание дисциплины

2.1. федеральный компонент – все содержание дисциплины.

2.2. наименование тем, их содержание, объем в лекционных часах (1 лекция-2часа)

ЛЕК.1. Введение. Основы администрирования и управления в информационных системах. Эксплуатация и сопровождение информационных систем ИС. Жизненный цикл ИС. Объекты и субъекты управления и администрирования. Типы рабочих мест и серверов. Понятия операционной и информационной сред сети. Схемы администрирования и управления.

ЛЕК.2. Администрирование операционной сетевой среды. Состав и структура операционной сетевой среды. Операционные среды рабочей станции, сервера и пользователя. Процедуры и файлы конфигурации операционной среды рабочей станции и сервера. Сетевое окружение рабочей станции и сервера, настройка и загрузка.

ЛЕК.3. Установка и настройка приложений. Сценарии подключения пользователей. Назначение сетевых дисков и путей доступа к программам и данным. Диалоговый интерфейс пользователя. Организация и настройка сетевой печати.

ЛЕК.4. Администрирование информационной сетевой среды. Состав и структура информационной сетевой среды. Ведение и обработка системной информации. Организация системных баз данных. Сетевые информационные службы.

ЛЕК.5. Сопровождение сетевых файловых систем. Распределение дискового пространства. Наблюдение за использованием томов и каталогов. Резервное копирование и восстановление сетевых данных. Информационная сетевая среда пользователя. Доступные сетевые ресурсы.

ЛЕК.6. Программная структура систем административного управления. Управление взаимодействием открытых систем ВОС.Управление прикладными процессами и ресурсами ВОС. Функции управления

прикладными процессами. Функции и иерархия управления ресурсами ВОС. Управление системами, уровнем и операциями уровня. Управление системами.Компоненты системы административного управления. Информационная база данных управления. Протокол "Администрация-Агент".

ЛЕК.7. Аттрибуты, события и действия. Протоколы и интерфейсы управления объектами. Протоколы сетевого управления SNMP, CMIP, RMON. Интерфейсы управления настольными системами DMI. Использование Web-технологии.

ЛЕК.8. Функции и функциональные области административного управления. Стандарты ISO. SMF-функции административного управления. Управление объектами, состояниями, соотношениями, оповещением об ошибках, услугами, проверками и тестированием, регистрацией. SFMA-функциональные области административного управления. Связь SFMA и SMF.

ЛЕК.9. Процедура управления системами общего пользования. Общая характеристика структуры системы административного управления. Функции регистрации, сбора и обработки информации. Служба справочника. Информационно-справочные системы.

ЛЕК.10. Управление конфигурацией. Конфигурация ресурсов и ее модель. Внешние параметры. Наблюдаемые характеристики : вероятностные, вероятностно-временные и стоимостные. Управляемые ресурсы. База данных конфигурации. Реконфигурация. Реконфигурация физической среды и топологии. Трассировка физической среды. Загрузка программного обеспечения. Протоколы загрузки. Примеры управления конфигурацией.

ЛЕК.11. Управление контролем характеристик. Поддержка SMF и подсистемой регистрации, сбора и обработки информации. Измерения параметров и характеристик. Анализ ВВХ и управление. Результаты измерений и их обработка. Формализация обозначений измеряемых характеристик и параметров. Форматы и поля сообщений об измеряемых параметрах и характеристиках. Контроль характеристик и прогнозирование.

ЛЕК.12. Управление учетом. Службы управления ошибочными ситуациями. Отчеты. Модели отказов. Вероятностно-временные характеристики. Тарификация. Управление тарификацией. Стоимостные характеристики . Управление услугами и тарификацией. Структура систем расчета с пользователями за услуги.

ЛЕК.13. Управление ошибочными ситуациями и безопасностью. Процедуры управления ошибочными ситуациями. Структура систем управления ошибочными ситуациями. Тестеры протоколов. Способы диагностики. Службы и отчеты управления учетом.Службы безопасности. Механизмы обеспечения безопасности. Поддержка служб механизмами. Реализация служб на уровнях ЭМВОС.
Криптография и управление ключами безопасности. Стандарт DES. Идентификация объекта и механизмы поддержания подлинности. Пароли. Цифровая подпись. Шифрование информации при передаче по каналам связи. Безопасность баз данных административного управления. Протоколы и процедуры безопасности передачи файлов.

ЛЕК.14. Оперативное управление и регламентные работы. Основные команды и процедуры оперативного управления. Содержание регламентных работ. Средства автоматизации регламентных работ. Обслуживание, поддержка и управление кабельного и сетевого оборудования, серверов. Управление и обслуживание технических средств. Аппаратно-программные платформы администрирования. Информационные системы администрирования. Программирование в системах администрирования.

ЛЕК.15. Примеры систем управления. Управление сетями TCP/IP over Ethernet. Системы CISCO NetFlow, IDS. Администрирование сети и сервисов INTERNET. Подключение локальной сети к INTERNET. Регистрация Доменных Имен. Конфигурирование интерфейсов. Драйверы сетевых интерфейсов. Сервисы INTERNET. Организация FTP- сервера. Администрирование серверов WWW. Протокол HTTP.
Заключение. Перспективы развития систем административного управления.

2.3. практические и семинарские занятия, их содержание и объем в часах (нет);

2.3. лабораторные занятия, их наименование и объем в часах (1лаб. – 2часа)

Лаб.1. Приемы работы CLI и утилиты командной строки Win2k
Лаб.2. Сетевые утилиты Win2k
Лаб.3. Утилита Net.exe Win2k
Лаб.4. Приемы работы CLI Linux
Лаб.5. Изучение программной структуры административного управления в сетях Ethernet
Лаб.6. Процедура управления конфигурацией в сетях Ethernet
Лаб.7. Настройки стека протоколов TCP/IP Win2k
Лаб.8. Инсталляция рабочей станции ОС Linux
Лаб.9. Настройки стека протоколов TCP/IP Linux
Лаб.10. Инсталляция серверных компонент ОС Linux (ч.1)
Лаб.11. Инсталляция серверных компонент ОС Linux (ч.2)
Лаб.12. Инсталляция серверных компонент ОС Linux (ч.3)
Лаб.13. Настройка системы учета трафика NetFlow/FlowTools (ч.1)
Лаб.14. Настройка системы учета трафика NetFlow/FlowTools (ч.2)
Лаб.15. Настройки системы IDS snort

2.5. курсовой проект (работа), его характеристика;

Курсовая работа, предусмотренная планом, выполняется студентом в течение семестра. Темы курсовых работ формируются путем слияния термов трех групп, определенных ниже:

A1. Реализация протокола <название>
A2. Настройка службы <название>
A3. Новые программные средства

B1. обеспечения информационной безопасности Linux
B2. обеспечения информационной безопасности Windows
B3. учета пользователей Linux
B4. учета пользователей Windows
B5. сетевых файловых систем Linux
B6. сетевых файловых систем Windows
B7. учета трафика
B8 регулирования трафика
B9. аутентификации пользователей

C1 в локальной сети
C2 в сети Internet

Например: A2+B5+C1 = Настройка службы GFS сетевых файловых систем Linux в локальной сети
Критерий оценки: студент должен знать принципы построения, настройки и функционирования конкретных систем администрирования и управления.

2.6. самостоятельная работа студентов

Проводится в соответствии с технологической картой дисциплины, темы

для самостоятельного изучения соответствуют темам лекционных и лабораторных занятий.

2.7. перечень и темы промежуточных форм контроля знаний;

Формы промежуточного контроля знаний - открытые и закрытые тесты по следующим темам:

1. CLI Win2k
2. CLI Linux
3. Утилиты сетевого администратора
4. Распределение дискового пространства.
5. Наблюдение за использованием томов и каталогов.
6. Резервное копирование и восстановление сетевых данных.
7. Информационная сетевая среда пользователя.
8. Доступные сетевые ресурсы.
9. Конфигурация ресурсов и ее модель.
10. Внешние параметры.
11. Наблюдаемые характеристики
12. Управляемые ресурсы.
13. База данных конфигурации.
14. Реконфигурация физической среды и топологии.
15. Трассировка физической среды.
16. Загрузка программного обеспечения.
17. Протоколы загрузки.
18. Управление сетями TCP/IP over Ethernet.
19. Системы CISCO NetFlow
20. IDS
21. Администрирование сети и сервисов INTERNET.
22. Подключение локальной сети к INTERNET.
23. Конфигурирование интерфейсов.Драйверы сетевых интерфейсов.
24. Сервисы INTERNET.
25. Организация FTP- сервера.
26. Администрирование серверов WWW.
27. Протокол HTTP.

Критерий оценки - соответствие знаний рассмотренному вопросу

2.8. вопросы к экзамену

1. функции администрирования
2. процедуры администрирования
3. службы администрирования

4. объекты администрирования
5. методы администрирования
6. службы управления конфигурацией
7. службы управления контролем характеристик
8. службы управления ошибочными ситуациями
9. службы управления учетом и безопасностью
10. службы управления общего пользования
11. информационные службы
12. интеллектуальные службы
13. службы регистрации
14. службы обработки информации
15. службы планирования и развития
16. эксплуатация и сопровождение информационных систем
17. инсталляция ИС
18. оперативное управление и регламентные работы
19. управление и обслуживание технических средств
20. аппаратно-программные платформы администрирования
21. информационные системы администрирования
22. организация баз данных администрирования
23. программирование в системах администрирования
24. примеры систем администрирования

Критерий оценки - соответствие знаний рассмотренному вопросу

3. Учебно-методические материалы по дисциплине

3.1. перечень обязательной (основной) литературы

1. Протоколы информационно-вычислительных сетей:Справочник/ Под ред. Мизина И.А., Кулешова А.П. М: Радио и связь, 1990.- 504с.

2. Суздалев А.В., Чугреев О.С. Передача данных в локальных сетях связи.М: Радио и связь, 1987.- 168с.

3. Зелигер Н.Б., Чугреев О.С., Яновский Г.Г. Проектирование сетей и систем передачи дискретных сообщений. М.:Радио и связь, 1984.- 176с

4. Богуславский Л.Б., Дрожжинов В.И. Основы построения вычислительных сетей для автоматизированных систем.

М:Энергоатомиздат, 1990.- 256с.

5. Шатт С. Мир компьютерных сетей. Киев: BHV, 1996.- 288с.

6. Компьютерные сети. Принципы, технологии, протоколы/ В.Г.Олифер, Н.А. Олифер.- СПб.: Изд-во "Питер", 1999.- 672с.

7. Барабаш П.А., Воробьев С.П., Махровский О.В., Шибанов В.С. Мультисервисные сети кабельного телевидения.-СПб.: Наука, 2000.- 336с.

8. Федотов М. Системы сетевого/системного управления: принципы создания http://books.kulichki.net/data/lan/lan7/

3.2. перечень дополнительной литературы

1. Щербо В.К., Киреичев В.М., Самойленко С.И. Стандарты по локальным вычислительным сетям. М:Радио и связь, 1990.- 304с.

2. Мафтик С. Механизмы защиты в сетях ЭВМ.- М.: Мир, 1993.- 216с.

3. Шибанов В.С., Лычагин Н.И., Серегин А.В. Средства автоматизации управления в

системах связи.- М.:Радио и связь,1990.-232с.

3.3. перечень пособий и технических средств.

3.3.1 On-line документация ОС Win2k,

3.3.2 On-line документация ОС Linux

3.3.3 CISCO UniverCD.

Компьютерный класс, оборудованный Pentium III - 600 или выше,

подключенный к ЛВС университета. ОС - Win2k, Debian Linux Based (Mandrake)

4. Учебно-методическая (технологическая) карта дисциплины “Администрирование в информационных системах”.

Номер Недели	Но-мер Темы	Вопросы, Изучаемые на лекции	Занятия (номера)		Используемые нагляд. и метод. пособия	Самостоятельная работа студентов		Формы Контроля
			практич. (семин.)	лаборат.		содерж.	часы	
1	2	3	4	5	6	7	8	9
1.	1	1		1	3.3.1			
2.	2	2		2	3.3.1	2	2	
3.	3	3		3	3.3.1	3	4	
4	4	4		4	3.3.2	4	4	Консультац.
5.	5	5		5	3.3.2	5	4	Аттестация
6.	6	6		6	3.3.2	6	4	
7.	7	7		7	3.3.1	7	4	
8.	8	8		8	3.3.2	8	4	
9.	9	9		9	3.3.2	9	4	Консультац.
10.	10	10		10	3.3.2	10	4	Аттестация
11.	11	11		11	3.3.2	11	4	
12.	12	12		12	3.3.2	12	4	
13.	13	13		13	3.3.3	13	4	
14.	14	14		14	3.3.3	14	4	Консультац.
15.	15	15		15	3.3.2			Аттестация

СОДЕРЖАНИЕ ЛЕКЦИОННОГО КУРСА

ЛЕК.1. Введение. Основы администрирования и управления в информационных системах. Эксплуатация и сопровождение информационных систем ИС. Жизненный цикл ИС. Объекты и субъекты управления и администрирования. Типы рабочих мест и серверов. Понятия операционной и информационной сред сети. Схемы администрирования и управления.

Администратор системы включает задачи, обычно выполняемые в вычислительной системе: создание резервных копий и восстановление файлов, добавление и удаление пользователей, управление сетью, добавление и удаление аппаратных средств и т.д.

Для выполнения этих задач в системе имеется два интерфейса: команды shell, являющиеся непосредственным пользовательским интерфейсом с административными функциями среды системы UNIX, и меню sysadm, обеспечивающие интерфейс меню с теми же задачами с помощью команды sysadm. Опытные администраторы системы должны быть знакомы с обоими интерфейсами.

Если вы инсталировали пакет прикладных программ "Operations, Administration and Maintenance" (OA&M), sysadm обращается к меню в формате окон, используя интерфейс форм, меню и языка (FMLI). Примечание. Рекомендуется инсталировать пакет OA&M до инсталяции Экранной командной оболочки Framed Acces Command Environment (FACE) ("Файловый доступ к командной среде"). Если вы инсталируете пакет FACE первым, вы получите сообщения об ошибках при загрузке первого гибкого диска. Инсталяция завершится частичным сбоем установки.

При инсталяции пакета OA&M вам предлагается выбор между основным пакетом или пакетом расширений OA&M. Пакет расширений OA&M - выбор по умолчанию - дает более широкий диапазон услуг по

созданию резервных копий и восстановлению файлов, плюс другие услуги - создание группы пользователей, сопровождение программ, сопровождение файлов и т.д.

При первоначальной инсталяции можно установить основной пакет OA&M или вместе и основной пакет и пакеты расширений OA&M. Если вы инсталировали оба пакета OA&M - и основной, и пакет расширений - и хотите удалить расширение для сохранения пространства, следует удалить и основной и пакеты расширений и заново инсталировать основной пакет OA&M. Расширение меню помечается #oam# на поврежденных строках меню в файлах меню OA&M.

Примечание. Файлы ".menu" object_gen позволяют добавить исходные тексты FML (Form., Menu., или Text. файлы) с помощью пакетов расширений в структуре каталога расширений. Эти добавления можно удалять (в соответствии с правилами в Руководстве разработчиков пакетов расширений), когда удаляется пакет расширений (модульность). Меню усовершенствуются автоматически; прототип пакета расширений содержит файлы ".mi", определенные как OAMmif. Документы о действиях OAMmif, представленные в OA&M, корректируют главные меню, объявленные в пакете расширений как именующие специфическое расширение. Это вызывает переадресацию на местоположение специфических каталогов расширений, где должны постоянно находиться файлы FML.

Например, расширение Small Computer Systems Interfase (SCSI) (Интерфейса систем малых ЭВМ) добавляет выбор типов меню "buses" и "devices". Специфический выбор SCSI (строки) в меню "buses" и в меню "devices" определен в поле 4 с помощью метки #scsi#. #scsi# интерпретируется с помощью object_gen и преобразуется в /usr/sadm/sysadm/add-ons/scsi (в противоположность /usr/sadm/sysadm/menu/*) - местоположение специфического расширения SCSI. В дальнейшем другие пакеты расширений могут привносить

расширения в те же элементы главного меню (они будут содержать соответствующее перемещение #add-on_name#).

ЛЕК.2. Администрирование операционной сетевой среды. Состав и структура операционной сетевой среды. Операционные среды рабочей станции, сервера и пользователя. Процедуры и файлы конфигурации операционной среды рабочей станции и сервера. Сетевое окружение рабочей станции и сервера, настройка и загрузка.
Выбор сети и средств доступа к сервису (SAF) возникли из-за необходимости устанавливать связь систем UNIX с другими системами UNIX, а также с другими операционными системами.

Задания, связанные с администрированием сетевой системы можно выполнять, используя или систему меню, или команды shell. Нижеприводимый экран представляет верхний уровень меню System Administration системы UNIX System V Release 4.0 Version 1.0, который показывает администрирование сетевой системы как одну из опций.

application - Administration for Available Application
backup_service - Backup Scheduling, Setup and Control
file_system - File System Creation, Checking and Mouting
network_services - Network Services Advinistration
preSVR4 - Peripherals setup
ports - Port Access Services and Monitors
restore_services - Restore from Backup Data
schedule_task - Schedule Automatic Task
software - Software Installation And Removal
storage_devices - Storage Devices Operations and Definitions
system_setup - System Name, Date/Time And Initial Password Setup
users - User Login and Group Administration

Вышеприведенное меню можно вывести на экран командой sysadm.

Когда вы выбираете одну из опций, подменю и команды проведут вас по требуемым процедурам. Вы также можете обойти систему меню, выдавая команды shell. Если вы редактируете системные файлы, обязательно сохраните запасную копию файла. После окончания редактирования файла, используйте diff в отредактированном файле и запасную копию, чтобы проверить, что только нужные изменения были внесены.

Чтобы прикладные программы сетей являлись переносимыми в различные среды, в процессе их применения должен быть стандартный интерфейс с разнообразными сетями, имеющимися в любой текущей среде. Выбор сетей обеспечивает простой и последовательный интерфейс, который позволяет пользователю прикладных программ выбирать сети (на уровне транспортировки), дающие возможность прикладным программам быть независимыми от протоколов и носителей данных.

Прикладные программы сетевого сервиса (Networking Services), которые позволяют пользователю влиять на выбор сетей, используют стандартный интерфейс, который здесь описан.

Выполняйте эти меню для вывода на экран конфигурации Network Selection:

1. Выберите display из меню Network Selection Management. Система выведет на экран текущую конфигурацию сетевого выбора (Network Selection).
2. Нажмите CANCEL, чтобы возвратиться в меню 3 - Network Selection Management. Повторное нажатие CANCEL возвращает вас в меню 2 - Network Selection Management.

Команда shell, выводящая на экран текущую сетевую конфигурацию, такая:

vi/etc/netconfig

Выполняйте эти меню, чтобы модифицировать конфигурацию сетевого выбора.

1. Выберите modify из меню Network Selection Management.

2. Переместите курсор к тому элементу, который собираетесь модифицировать в меню Existing Network Identifiers (Идентификаторы существующих сетей) и нажмите Enter.

Система отображает экран Modify Network Selection Configyration:

```
5 Modify Network Selection Configuration
----------------------------------------
 Networking Identifier:
 Default Network?
 Networking Device:      /dev/ticlts
 Semantics:              tpi_clts
 Protocol Family:        loopback
 Protocol:               none
 Directory Lookup Libraries:
                         /usr/lib/straddr.so
     Modify the fields and press [SAVE]
```

3. Нажмите CONT, чтобы модифицировать еще один элемент, или нажмите QUIT, чтобы закончить модификацию.

Команда shell, модифицирующая конфигурацию сетевого выбора, следующая:

vi/etc/netconfig

Средство преобразования имени в адрес позволяет прикладной программе получать адрес сервиса указанной машины способом, не зависимым от транспортного уровня. Задания, связанные с управлением преобразования базового имени в адрес, могут выполняться с помощью системы меню или команды shell.

Пакет утилит построения базовых сетей позволяет компьютерам, использующим операционную систему UNIX, соединиться друг с другом и с удаленными терминалами. Эти утилиты включают и те, что используются для копирования файлов между компьютерами (uucp и uuto), и те, что используются для дистанционной регистрации и выполнения

команд (cu, ct, и uux). Нижеприводимый экран представляет меню верхнего уровня для выбора BNU (утилиты построения базовых сетей).

```
3 Basic Networking Utilites Management
--------------------------------------
devices - Adding, Listing, and Removing Networking Devices
polling - Adding, Listing, and Removing Systems to be Polled
Setup   - Initial Basic Networking Setup
Systems - Adding, Listing, and Removing Remote Systems
```

Меню устройств позволяет вам управлять параметрами устройств, используемых базовыми утилитами сети. Устройство указывается заданием своего типа, конкретного порта, а также скоростью и процедурой набора номера, используемой в порте. Устройство выбирается для использования при построении базовых сетей на основании требуемого типа устройства и скорости. Так несколько устройств могут иметь одни и те же скорость и тип, и утилита постоения базовых сетей может попытаться подсоединиться к удаленной станции, используя для этого в свою очередь несколько устройств. Нижеприводимый экран представляет верхний уровень меню для выбора устройств:

```
4 Adding, Listing, and Removing Networking Devices
--------------------------------------------------
add    - Adds Devices for use by Basic Networking
list   - Lists Devices available for Basic Networking
remove - Remove devices from use by Basic Networking
```

Задание по добавлению позволяет сообщить вашей системе о тех устройствах, через которые она может инициировать установление связи с другими системамами. Такие устройства следует подсоединить к тем портам, которые поддерживают только выходящий поток информационного обмена или как входящий, так и выходящий потоки (т.е. двунаправленный поток). Порт, который поддерживает только входящий поток обмена может использоваться утилитами построения сетей для

приема сообщений; такое использование не требует управления.Выполняйте следующее меню, чтобы добавить новое устройство:

1. Выберите devices из меню Basic Networking Utilities.
2. Выберите add из меню Adding, Listing and Removing Network Devices.

Система отобразит следующий экран:

5 Adds a Device for Use by Basic Networks

Device Category:

3. Нажмите CHOICES, чтобы выбрать category, затем нажмите SAVE.

Система отобразит один из нижеприводимых экранов в зависимости от выбранной категории.

6 Adds a Direct Device for Use by Basic Networking

System: Direct

Port:

Speed:

6 Adds a Modem Device for Use by Basic Networking

Device Type: ACU

Modem Type:

6 Add a TLI Device for Use by Basic Networking

Network Name:

Port:

Dialer Type: TLIS

6 Add a Generic Device for Use by Basic Networking

Device Type:

Port:

Dialer Port:

Speed:

First Dialer: First Token:

Second Dialer Second Dialer:

Third Dialer Third Token:

4. Внесите требуемую информацию в отображенную на экране форму.

5. Нажмите SAVE, чтобы сохранить информацию.

Система отображает элементы, внесенные в /etc/uucp/Devices из информации, предложенной на этапе 4.

6. Нажмите CONT, чтобы добавить еще одно устройство, или нажмите CANCEL и вернитесь в меню 4.

Команда shell, добавляющая устройство построения сети, следующая:

vi/etc/uucp/devices

ЛЕК.3. Установка и настройка приложений. Сценарии подключения пользователей. Назначение сетевых дисков и путей доступа к программам и данным. Диалоговый интерфейс пользователя. Организация и настройка сетевой печати.

Чтобы добавить пользователя в систему, вам нужно создать группу пользователей и присвоить пользователю регистрационное имя. Если группа, к которой принадлежит пользователь уже существует, вам не нужно создавать новую. (Используйте опцию list в меню User Login и Group Administration, чтобы просмотреть текущие определенные группы пользователей). Обратиться к меню можно через опцию users в главном меню System Administration.

Создание группы пользователей

Группы следует создавать в системе до того, как им могут быть присвоены пользователи.

Для каждой создаваемой группы требуется следующая информация:

* имя группы - максимум 8 символов;

* идентификационный номер группы - максимум 5 цифр;

* первичные члены - регистрационные имена членов, которые принадлежат группе во время регистрации;

* дополнительные члены - регистрационные имена членов, которые могут обратиться к файлам, принадлежащим группе, через newgrp(1M).

Для создания группы требуются следующие действия:

1. Выберите add из меню User Login and Group Administration. Система выводит на экран меню Add Users (Добавление пользователей) или меню Groups:

```
3     Add Users or Groups
User or group:
```

2. Введите имя группы или нажмите CHOICES, чтобы выбрать группу, затем нажмите SAVE. Система выводит на экран меню Add a Group с присвоенным Group IDD по умолчанию:

```
4     Add a group
-----------------------------------
Group name:
Group ID:
Primary member(s):
Supplementary member(s):
```

3. Заполните информацию о группе, затем нажмите SAVE.

4. Нажмите CONT, чтобы добавить еще одну группу, нажмите CANCEL, чтобы возвратиться в предыдущее меню.

Для создания группы используется команда:

```
groupadd -g group_ID group_name
```

где group_ID - идентификатор группы;

group_name - имя группы.

Пользователей можно добавить к этой группе, выполняя указания из следующего пункта "Присваивание регистрационных имен".

После определения группы пользователей, ей можно присвоить имена регистрации пользователей. Каталог /etc/skel содержит стандартный файл .profile, который автоматически копируется в домашний каталог нового пользователя. Если вы хотите, чтобы новому имени регистрации автоматически включалось содержимое любого другого файла или каталога, такого как каталог rje, вам нужно создать файл или каталог в /etc/skel.

Вам нужна следующая информация для каждого имени регистрации пользователя, добавляемого вами:

* имя пользователя и/или другие комментарии - максимум 64 символа;
* идентификатор регистрации - максимум 8 цифр;
* идентификатор пользователя - максимум 5 цифр;
* имя первичной группы, к которой будет принадлежать пользователь - максимум 8 символов;
* дополнительные группы, если есть;
* домашний каталог пользователя;
* привилегии администратора системы (yes или no); командный файл регистрации пользователей.

1. Чтобы добавить новое регистрационное имя, введите следующие команды:

```
useradd -u user_number -g primary_group_ID -G
supplementary_group_ID -c comment -d home_directory
-s program -m login_ID
```

Примечание. Команда вводится одной строкой. Все аргументы - необязательные, за исключением login_ID.

После ключа -G вы можете указать несколько идентификаторов дополнительных членов группы, отделив их друг от друга запятыми без пробелов:

supplementary_group_ID1,supplementary_group_ID2 или заключив идентификаторы в двойные кавычки с пробелами, например:

"supplementary_group_ID1 supplementary_group_ID2"

Если в тексте комментария, который следует за ключом -c, слова разделены пробелами, текст должен быть заключен в двойные кавычки. Кавычки не нужны, когда между словами пробелы не используются, например:

-c Art_and_Graphics

Ключ -d используется для указания домашнего каталога пользователя. Указывается полное имя каталога, например: as/home3/login_ID.

Параметр -s используется, чтобы указать программу не по умолчанию. Для этого указывается полное имя программы, например: as/sbin/sh.

Параметр -m не имеет аргумента; login_ID - это аргумент команды useradd. Этот параметр задает копирование соджержимого каталога /etc/skel в каталог нового пользователя. Каталог /etc/skel должен содержать стандартные файлы, такие как стандартный профиль пользователя (.profile) и стандартные каталоги (такой как rje), используемые в вашей системе.

2. Чтобы присвоить пароль, введите:

passwd options login_ID

где options - это один из следующих параметров:

-n days - указывает минимальное количество дней (при необходимости), в течение которых новому пользователю будет разрешено изменять свой пароль;

-x days - указывает максимальное количество дней (при необходимости), в течение которых новому пользователю будет разрешено сохранять свой существующий пароль;

-f - заставляет нового пользователя изменить пароль в следующем сеансе регистрации.

В системе UNIX есть два файла паролей - /etc/passwd и /etc/shadow. Файл /etc/passwd идентифицирует каждого пользователя системе. Этот файл содержит информацию для каждого ID регистрации пользователя, номера ID пользователя, номер группового ID, номер ID дополнительной

группы, комментария о пользователе, программы по умолчанию, выполняемой после регистрации пользователя (обычно /sbin/sh), и начального каталога пользователя.

Каждый раз, когда создается какое-то имя регистрации, к файлу добавляется новый элемент. Каждый элемент - это строка, которая имеет семь полей, отделенных друг от друга двоеточием. Файл /etc/default/passwd можно создавать со следующими пременными:

PASSLENGTH -

эта переменная представляет минимальную длину пароля. Любой пароль меньшей длины будет запрещен. Длина по умолчанию - 6 символов;

MINWEEKS -

эта переменная представляет количество недель после смены пароля, в течение которых пароль можно не менять;

MAXWEEKS -

эта переменная представляет количество недель, по истечении которых вам поступит запрос изменить пароль во время вашей следующей регистрации;

WARNWEEKS -

эта переменная представляет количество недель существования пароля, до того как пользователю поступит предупреждение о его предстоящем исчезновении.

Переменные MINWEEKS и MAXWEEKS может проигнорировать пользователь root, если явно установит возраст пароля для конкретного пользователя.

Файл /etc/shadow содержит зашифрованный пароль каждого пользователя и информацию о возрасте пароля. Этот файл может считываться только суперпользователем. Пароль и информация о его возрасте добавляется в /etc/shadow с помощью новой программы pwconv(1M). Эта программа может выполняться только суперпользователем.

Если у вас есть программа, которая пишет пароль и/или информацию о возрасте пароля в /etc/passwd, эту программу следует модифицировать, чтобы pwconv(1M) могла быть выполнена после добавления информации в /etc/passwd. До возможности выполнения модификации администратор с привилегией суперпользователя должен прогнать программу, прежде чем добавленный пользователь или тот, чья информация о пароле модифицирована, сможет зарегистрироваться.

ЛЕК.4. Администрирование информационной сетевой среды. Состав и структура информационной сетевой среды. Ведение и обработка системной информации. Организация системных баз данных. Сетевые информационные службы.

Система UNIX V Release 4.0 Version 1.0 позволяет поддерживать автоматическое функционирование программ в указанное время. Это можно сделать с помощью программы cron. Программа cron и команда crontab позволяют вам прогонять программы в нерабочие часы. Это удобно при работе с затратными по времени программами или с управляющими процедурами, или процедурами подчистки, которые требуют наличия машины, находящейся в спокойном состоянии.

Любое задание, которое требует повторных выполнений в указанное время, является потенциальным заданием файла cron, помещенного в каталог /var/spool/cron/crontabs. Вы можете использовать команду crontab, чтобы организовать нужные вам элементы.

Команда crontab используется следующим образом:

crontab file

crontab -r

crontab -l

Команда crontab копирует указанный file (или стандартный ввод, если файл не указан) в каталог, который содержит все crontab пользователя. Параметр -r удаляет crontab пользователя из каталога crontab. Параметр -l

выполнит просмотр файла crontab, чтобы вызвать пользователя.

Каждая строка файла crontab определяет одну процедуру. Формат строкового элемента выглядит следующим образом:

minute hour day month day-of-week command

Каждое поле определяется следующим образом

minute (0-59),

hour (0-23),

day (1-31),

month (1-12),

day-of-week (0-6, 0=Sunday)

command (команда, которая должна выполняться в указанное время).

Нижеприводимые правила относятся к первым пяти полям.

Два числа, отделенные друг от друга дефисом, указывают диапазон чисел.

Список чисел, отделенных друг от друга запятыми, указывает, что использоваться будут только перечисленные числа.

Звездочка указывает все разрешенные значения.

Например, 0 0 1,14 * 2

указывает, что команда будет функционировать первого и четырнадцатого числа каждого месяца, а также каждый вторник. Если в командном поле (шестое поле) размещен знак %, система UNIX переведет его как символ новой строки. Только первая строка командного поля (символьная строка до знака %) выполняется командным файлом. Все другие строки бывают доступными для команды в виде стандартного ввода.

Например, пусть файл, вызванный anyfile, содержит следующий элемент cron:

0 0 1 * * mailx $LOGNAME % Subject: Call Mom! % now

Когда выполняется командная строка crontab anyfile, пользователь, чье имя регистрации $LOGNAME, будет получать напоминание с Call Mom! первого числа каждого месяца.

Время от времени систему UNIX необходимо подчищать. Вы можете избежать этого занятия благодаря команде crontab и файлу crontab. Вы можете указать задание подчистки (например, удаление устаравших файлов) и время, когда вы хотите выполнить файл crontab.

Ваш компьютер уже имеет несколько определенных процедур подчистки. Эти процедуры выполняются с помощью имени регистрации root под управлением crontab каждое воскресное утро в 5:17. Файл /etc/cleanup определяет какие именно процедуры подчистки выполняются.Некоторые из файлов, которые подчищаются каждое воскресенье утром, перечислены ниже:

Файл /var/adm/wtmp: этот файл содержит архив имен регистрации в системе. Каждый раз когда пользователь регистрируется в системе, в этом файле делается запись. Чтобы не удалять этот файл вручную, когда он станет слишком большим, можно использовать cron.

Файл /var/adm/sulog: этот файл содержит архив пользователей, которые используют команду su для подключения имен регистрации. В качестве меры защиты этот файл не должен считываться другими пользователями.

Файл /var/cron/log: этот файл содержит архив всех действий, предпринятых cron.

Зарегистрировавшись как root и выполнив crontab -l, вы сможете увидеть элемент crontab, который выполняет /etc/cleanup, а также другие рутины подчистки для базовой сети (UUCP). Вы можете редактировать /etc/cleanup и модифицировать root crontab, тем самым по своему желанию выполнив подчистку заданий другим способом.

Программа системы UNIX boot загружает и выполняет автономные программы системы UNIX. Так как boot используется для первоначальной загрузки и выполнения ядра системы UNIX, она может загружать и выполнять любые другие программы, которые связаны с автономным выполнением. Система вызывает программу boot при каждом запуске компьютера. Она сначала пытается поместить программу boot в

устройство для гибкого диска; если устройство для гибкого диска пусто, система вызывает процедуру загрузки жесткого диска.

При первом вызове, boot выведет на экран следующее сообщение о состоянии:

Bootung the UNIX System...

Следующий этап зависит от того, хотите ли вы загрузить программу по умолчанию или другую автономную программу.

Чтобы дать boot команду на использование программы по умолчанию (ядро системы) и значений, указанных в файле загрузки по умолчанию - etc/default/boot, нажмите ENTER. Если вы только что загрузили программу boot с дистрибутивного диска, нажмите ENTER, boot сделает паузу и даст подсказку на использование информации о настройке.

Чтобы загрузить программу, отличную от программы по умолчанию, нажмите любую клавишу (за исключением ENTER) по подсказке "Загрузка системы UNIX", чтобы прервать boot. Программа boot делает паузу и дает подсказку с помощью следующего сообщения для ввода имени программы, которую вы хотите загрузить:

Enter the name of a kernel:

Система ждет, когда вы наберете имя нужной программы и нажмете ENTER.

Чтобы загрузить на дистрибутивный диск программу, отличную от boot, вы должны указать местонахождение программы, предоставив имя файла (если нужная вам программа находится в устройстве загрузки по умолчанию), или предоставить имя устройства и имя файла (если программы, которую вы хотите загрузить нет в устройстве по умолчанию). Имя файла нужно включить в полное имя файла, содержащего автономную программу. Указание местонахождения программы, которую вы хотите загрузить, должно стоять первым в командной строке и должно присутствовать, если другие параметры boot указываются или на командной строке или в /etc/default/boot. Чтобы указать программу,

отличную от boot, на дистрибутивном диске, используйте один из нижеследующих форматов:

filename

или

xx(m,o)filename

где filename - это полное имя файла системы UNIX;

xx - это имя устройства (hd - для жесткого диска или fd - для гибких дисков);

m - это вторичный номер устройства (1 для системы файлов root на жестком диске);

o - это смещение в сегменте (обычно 0).

Аргумент filename должен начинаться с косой черты, если программа не находится в каталоге root. Если filename является единственным аргументом, набранным по подсказке загрузки, boot ищет filename в устройстве загрузки по умолчанию и пытается оттуда его загрузить. Обратите внимание, что все числа являются десятичными.

Планирование автоматических заданий

Средство планирования автоматических заданий (Shedule Automatic Tasks) дает возможность планировать задания, выполняющиеся автоматически в более позднее время или в регулярно установленное время. Вы можете добавлять, изменять, удалять или выводить на экран свои собственные запланированные задания.

Примечание. Если вы выбираете средство планирования автоматических заданий и не имеете доступ к cron, вы получите предупреждение. Пользователь, зарегистрировавшийся как "root", редактирует файл /etc/cron.d/cron.allow и добавляет ваше имя регистрации, прежде чем вы сможете обратиться к средству cron.

Кроме того, если вы выбираете средство планирования автоматических заданий, а демон (следящий процесс) не функционирует, вы получите

предупреждение. Вы можете запланировать свое задание, но оно не будет выполняться пока не будет запущен планировщик заданий.
Обращайтесь к меню этих заданий с помощью параметра schedule_task из главного меню System Administration.
Примером задания может служить

mail dlt < mailfile

которое отсылает почту в dlt пользователя.
Выполняйте следующие меню, чтобы добавить автоматически планируемое задание:

1. Выберите Add из меню Schedule Automatic Task.

Система выводит на экран следующую информацию:

```
_____________________________________________
|  3                Schedule a Task        |
---------------------------------------------
Month(s) of thr Year:
Day(s) of the Month:
Day(s) of the Week:
Hour(s) of the Day:
Minute(s) past the Hour:
Task:
```

2. Нажмите CHOICES. Система выводит на экран числовой список месяцев.
3. Используйте клавиши со стрелками, чтобы переместить курсор, и нажмите MARK, отметив каждый из планируемых месяцев. Звездочка (*) будет отображаться рядом с каждым выбранным месяцем.
4. Нажмите Enter.
5. Используйте клавиши со стрелками, чтобы переместиться к следующему полю.
6. Повторите вышеуказанные этапы 2-5 в следующих четырех полях.
7. Для поля Task: введите команду для планируемого задания, а затем

нажмите SAVE.

Система выводит экран, подтверждающий информацию о задании.

8. Нажмите CONT, чтобы подтвердить запланированное задание или
9. нажмите CANCEL, чтобы выйти из задания.

ЛЕК.5. Сопровождение сетевых файловых систем. Распределение дискового пространства. Наблюдение за использованием томов и каталогов. Резервное копирование и восстановление сетевых данных. информационная сетевая среда пользователя. Доступные сетевые ресурсы.

Создание рабочей файловой системы проводится в несколько этапов:

1. Форматирование гибких дисков.
2. Создание файловой системы с использованием меню OA&M или команды mkfs.
3. Установка файловой системы.
4. Демонтирование файловой системы при отсутствии обращения к ней.

В данном подразделе сначала обсуждается общий формат команды mkfs, а затем ее специфическое применение для создания файловой системы s5 или ufs. Формат команды mkfs:

mkfs [-F filetype] [-V] [-m] [current_options]
[-o specific_options] special operands

где filetype - тип файловой системы - либо s5, либо ufs; -V - отображает полностью командную строку, включая информацию файла ufstab; -m - возвращает командную строку, используемую для создания существующей файловой системы. Этот параметр позволяет пользователю видеть атрибуты, из которых состоит файловая система; current_options - параметры, поддерживаемые s5; specific_options - атрибуты файловой системы должны быть введены в файл /etc/vfstab. special - имя элемента vfstab, содержащее атрибуты особой файловой системы; special_operands - операнды, специфичные для типа создаваемой файловой системы.
При построении файловой системы ufs команда mkfs создает файловую

систему с корневым каталогом и с каталогом lost+found. Число индексных дескрипторов файла высчитывается как функция размера файловой системы.

Введите следующие команды, чтобы создать новую файловую систему ufs или преобразовать старую в новый логический размер блока:

1. Если новая файловая система будет создаваться на части диска, где находится старая файловая система, создайте резервную копию старой системы.
2. Если новая файловая система будет создаваться из старой, выполните команду labelit, которая сообщает и имя смонтированной файловой системы и физическое имя тома старой файловой системы. Эти метки уничтожаются, когда создается новая файловая система. Необходимо определить тип файловой системы при использовании labelit. Например, если у вас устройство f0q15d, файловой системой будет memo, а именем тома memo 2.0. Введите:

   labelit -F ufs/dev/dsk/f0q15d memo memo 2.0

3. Используйте одну из следующих команд:

   mkfs -F ufs [-o] [arguments special size

   или

   mkfs -F ufs [-o] [arguments special prototype

   где special - вход в файле vfstab, содержащий атрибуты файловой системы; size - количество секторов в файловой системе; arguments - необязательные параметры - это список параметров, отделяемых запятыми и позволяющих настраивать файловую систему. Ниже приводится список наиболее важных параметров:

   * nsect - число секторов на одну дорожку на диске. Значение по умолчанию 18. Если вы выдаете команду prtvtoc -p для дискового запоминающего устройства, число секторов выводится как "# sectors";

   ntrack - число дорожек на один цилиндр на диске. Значение по умолчанию 0. Команда prtvtoc -p выводится как "# heads";

bsize - первоначальный размер блоков для файлов файловой системы, выбираемый из 4096 (по умолчанию) или 8192;

fragsize - наименьшее пространство на диске, которое выделяется для файла. Значение должно быть степенью числа 2, выбранное из диапазона от 512 до 8192. Значение по умолчанию 1024;

cgsize - количество дисковых цилиндров на одну группу цилиндров. Это число должно быть в диапазоне от 1 до 32. Значение по умолчанию 16;

free - минимальный процент допустимого свободного дискового пространства. Если объем файловой системы достигает этого порога, вы должны быть привилегированным пользователем, чтобы выделить дисковые блоки. Значение по умолчанию 10.

Если списку параметров предшествует -o, тогда необходимо специфицировать только желаемые параметры, но каждый параметр должен быть явно маркирован. Иначе, параметры исследуются слева направо, где первым параметром считается nsect, вторым - ntrack и т.д. Следующие две команды схожи по функциям:

```
mkfs -F ufs -o bsize=4096,nsect=18,
        ntrack=9 /dev/rdsk/1s2 35340
mkfs -F ufs /dev/rdsk/1s2 35340 32 16 4096
```

prototype - имя файла, которое может включать: количество блоков, необходимое для файловой системы, каталог и файловая структура, а также команды считывания содержания соответствующих файлов в файловую систему.

4. Прогоните команду labelit, чтобы восстановить файловую систему и имена томов.

5. Заполните новую файловую систему - например, восстановите из резервной копии файловой системы или, если в вашей системе два жестких диска, выполните команду cpio (1M) из смонтированной файловой системы. (Команды volcopy (1M) и dd (1M) копируют образ файловой системы; они не могут преобразовывать логический размер блока).

ЛЕК.6. Программная структура систем административного управления. Управление взаимодействием открытых систем ВОС.Управление прикладными процессами и ресурсами ВОС. Функции управления прикладными процессами. Функции и иерархия управления ресурсами ВОС. Управление системами, уровнем и операциями уровня. Управление системами.Компоненты системы административного управления. Информационная база данных управления. Протокол "Администрация-Агент".

Система UNIX использует схему Устанавливаемых управляющих программ/Настраиваемых параметров (ID/TP). Настройка этих параметров может оказывать значительное влияние на работу системы (как положительное, так и отрицательное). Перед настройкой ядра основательно продумайте использование своего компьютера, проанализируйте его текущую работу и рассмотрите другие факторы работы, например, организацию файловой системы, вторые промежуточные биты округления, эффективность $PATH и размеры блоков файловой системы.

После добавления сетевого сервиса к UNIX System V появились нестандартные методы доступа к сервису системы, давшие непоследовательные интерфейсы и среду выполнения, затрудняющие работу пользователей. SAF (средство доступа к сервису) обеспечивает механизм унифицированного доступа к сервису. Управляющие компоненты этого средства - это команды инсталяции, создания конфигурации и поддержки мониторов порта и сервиса, а также файлов, в которых хранится сервисная информация и информация монитора порта.

Способ управления и организации монитором порта доступа к порту зависит от конкретного монитора порта, а не отдельного компонента SAF. Следовательно, пользователи могут расширять свои системы, разрабатывая и устанавливая свои собственные мониторы порта.

Пользователям, которые хотят написать собственные мониторы порта, следует обратиться к книге "Руководство программиста: Сетевые интерфейсы". В этом разделе описание конкретных мониторов порта ограничено теми программами, которые поставляются вместе с системой UNIX, ttymon и "приемником".

С точки зрения SAF сервис - это процесс, который запускается. Ограничений функций, которые предоставляет сервис, не существует. SAF состоит из управления процессом - контроллера доступа к сервису (SAC), а также двух управляющих уровней, соответствующих двум уровням в поддерживаемой структуре каталогов. Верхний управляющий уровень соотносится с управлением монитором порта, нижний уровень - с управлением сервисом.

SAF состоит из следующих компонентов:

* контроллер доступа к сервису;
* командный файл конфигурации системы;
* управляющий файл SAC;
* команда администратора SAC sacadm;
* мониторы портов;
* необязательные файлы конфигурации мониторов портов;
* управляющий файл для каждого монитора порта;
* команда администратора pmadm;
* необязательные файлы конфигурации сервиса.

В этом разделе описываются SAC, управляющие файлы, а также файлы конфигурации системы, мониторов порта и сервиса.

Контроллер доступа к сервису (SAC) управляет механизмом обслуживания. Это процесс управления средством доступа к сервису (SAF). SAC запускается с помощью команды init (1M) посредством входа в /sbin/inittab. Его функция - поддерживать мониторы порта системы в состоянии, которое вы указываете. Эти состояния включают: STARTING, ENABLED, DISABLED, STOPPING, NOTRUNNING и FAILED (Монитор

порта вводит состояние FAILED, когда SAC не может запустить его после указанного числа попыток).

Команда администратора sacadm используется для того, чтобы сообщить SAC о необходимости изменить состояние монитора порта, sacadm также можно использовать для добавления или удаления монитора порта из области управления SAC и просмотра информации о мониторах портов, известных SAC.

Управляющий файл SAC содержит уникальный тег для каждого монитора порта, известного SAC, и полное имя команды, используемой для запуска каждого монитора порта.

SAC:

* настраивает свою собственную среду;
* запускает требуемые мониторы портов;
* опрашивает свои мониторы порта и инициирует процедуры восстановления при необходимости.

При инициации SAC настраивает свою собственную среду запуска командного файла конфигурации системы. Затем он считывает свой управляющий файл, чтобы определить те мониторы портов, которые следует запустить. Для каждого монитора порта, который он запускает, он интерпретирует файл конфигурации этого монитора порта, если таковой существует. Наконец мониторы портов, указанные в управляющем файле (например, ttymon) запускаются.

После запуска мониторов портов SAC периодически опрашивает их для получения информации о состоянии. Параметр командной строки sac (1M), -t, позволяет администратору системы управлять частотой опроса. Когда монитор порта получает запрос о состоянии из SAC, он должен ответить сообщением, содержащим его текущее состояние (например, ENABLED). Если SAC не получит ответа, он предполагает, что монитор порта не запущен. Если монитор порта, который должен прогоняться, остановился, SAC предполагает, что он допустил сбой и предпринимает

требуемое действие восстановления.

SAC повторно запустит монитор порта с отказом, если для этого монитора порта был указан ненулевой счетчик повторного запуска, когда он создавался. SAC представляет собой административную точку управления для всех мониторов портов, (а, следовательно, для всех портов системы). Команды администратора sacadm (1M) и pmadm (1M) передают запросы в SAC, который в свою очередь устанавливает связь с мониторами портов. Эти запросы включают разрешение запрещенного монитора порта, и тот начинает прием запросов сервиса в свои порты, запуск мониторов портов, которые до этого были остановлены, а также просмотр текущего состояния всех мониторов порта системы.
Файл конфигурации системы - /etc/saf/_sysconfig - поставляется пустым. Его может использовать администратор системы, чтобы настроить среду для всего сервиса системы, написав командный файл на интерпретированном языке. Командный файл конфигурации системы интерпретируется контроллером доступа к сервису после запуска SAC. SAC запускается, когда система переходит в многопользовательский режим.

Файлы конфигурации сервиса позволяют вам настраивать среду для конкретного сервиса. Например, сервис может потребовать каких-то специальных привилегий, которые не доступны обычному пользователю. Используя язык, описанный на странице руководства doconfig (3N), вы можете написать командный файл, который предоставит или ограничит такие специальные привилегии конкретного сервиса, предложенные через конкретный монитор порта.

Файл конфигурации сервиса может игнорировать безусловные значения, поддерживаемые файлами конфигурации более высокого уровня. Например, файл конфигурации сервиса может указать множество модулей STREAMS, отличное от безусловного множества.

Управляющий файл SAC содержит информацию о всех мониторах

порта, за которые несет ответственность SAC. Этот файл существует в поставляемой системе. Изначально он является пустым, за исключением одной строки комментария, которая содержит номер версии контроллера доступа к сервису. Администратор системы добавляет мониторы портов к системе, осуществляя вводы в управляющий файл SAC. Эти вводы осуществляются с помощью команды sacadm с параметром -a. Команда sacadm также используется для удаления вводов из управляющего файла SAC.

ЛЕК.7. Аттрибуты, события и действия. Протоколы и интерфейсы управления объектами. Протоколы сетевого управления SNMP, CMIP, RMON. Интерфейсы управления настольными системами DMI. Использование Web-технологии.

Некоторые программные пакеты добавляют свои собстввенные вводы мониторов портов в ходе инсталяции, в других - вам придется добавлять их вручную. Каждый ввод в управляющий файл SAC содержит следующую информацию:

PMTAG -

уникальный тег, который идентифицирует конкретный монитор порта. Этот тег затем используется контроллером доступа к сервису (SAC) для идентификации монитора порта при всех целях администрирования. PMTAG может включать до 14 буквенных символов;

PMTYPE -

тип монитора порта. В добавок к своему уникальному тегу, каждый монитор порта имеет указатель типа. Указатель типа идентифицирует группу мониторов портов, которые являются различными вызовами одного и того же объекта. ttymon и listen являются примерами действительных типов мониторов портов. Указатель типа используется, чтобы облегчить администрирование групп соответственных мониторов портов. Без указателя типа у вас нет возможности узнать какие теги мониторов портов

соответствуют мониторам портов того же типа. PMTYPE может включать до 14 буквенных символов;

FLGS -

флаги, которые определяются в текущий момент, это: d - если запускается, не разрешайте монитор порта; x - не запускайте монитор порта. Если флаг не указывается, предпринимается безусловное действие. Монитор порта запускается и разрешается по умолчанию;

RCNT -

число раз, которое монитор порта может допустить сбой, прежде чем будет помещен в состояние отказа. После того как монитор порта ввел состояние отказа, SAC не будет пытаться повторно его запустить. Если счет не указан при создании ввода, это поле устанавливается на 0. Счет повторного запуска 0 указывает, что монитор порта не следует повторно запускать, если он дает отказ;

COMMAND -

символьная строка, представляющая команду, которая будет запускать монитор порта. Первый компонент символьной строки, сама команда, должен представлять собой полное имя пути.

Каждый монитор порта имеет свой собственный управляющий файл. Команда pmadm используется для добавления, удаления или модификации элементов в этом файле. При внесении каждого изменения соответствующему монитору порта сообщается о необходимости повторного считывания его управляющего файла.

Каждый элемент, вводимый в управляющий файл монитора порта определяет способ обработки монитором конкретного порта и сервис, который следует выполнять для этого порта. Некоторые поля должны присутствовать во всех типах мониторов портов. Каждый ввод должен включать тег сервиса для идентификации сервиса как уникального и значение, которое следует присвоить сервису, когда он будет запускаться.

Примечание. Комбинация тега сервиса и тега монитора порта уникально определяют случай использования сервиса. Тот же самый тег сервиса может использоваться для идентификации какого-то сервиса при другом мониторе порта.

Запись также должна содержать конкретные данные монитора порта, такие как строку подсказки, которая является значимой для ttymon. В целом, каждый тип монитора порта обеспечивает какую-то команду, которая воспринимает конкретные данные нужного монитора как аргументы и выводит эти данные в форме, соответствующей хранению в файле. Команда ttyadm (1M) делает это вместо ttymon, а nlsadmin (1M) - вместо listen.

Примечание. Если ПО при инсталяции добавляет требуемые вводы сервиса в управляющий файл монитора порта, вам не нужно добавлять ввод в ручную pmadm с параметром -a. Например, при инсталяции совместного использования дистанционных файлов (RFS), пакет ПО устанавливает требуемый сервис при каждом мониторе listen-типа.

Каждый ввод в управляющий файл монитора порта содержит следующую информацию:

SVCTAG -

уникальный тег, который идентифицирует сервис. Этот тег является уникальным только для монитора порта, через который этот сервис становится доступным. Другие мониторы порта могут предложить тот же или другой сервис с тем же самым тегом. Сервис требует наличия и тега монитора порта, и тега сервиса для идентификации его как уникального. SVCTAG может включать до 14 буквенных символов;

FLGS -

флаги с нижеследующими значениями могут быть включены как текущие в это поле:

x - Не разрешайте этот порт. Порт разрешается по умолчанию

u - Создавайте ввод utmp для этого сервиса. Обратите внимание, что

мониторы портов могут игнорировать флаг u, если создание ввода utmp для сервиса не соответствует способу, в котором следует вызывать этот сервис. Некоторые программы сервиса не могут запускаться нужным образом, если для них не созданы вводы utmp (например, login);

ID -

значение под которым следует запускать сервис. Значение имеет ту форму имени протокола, в которой оно появляется в /etc/passwd;

PMSPECIFIC -

примерами конкретной информации мониторов порта являются адреса, имя процесса, который должен выполняться или имя программного канала STREAMS, через который устанавливается связь между процессами;

COMMENT -

комментарий, относящийся к элементу сервиса.

Примечание. Каждый управляющий файл монитора порта должен содержать один специальный комментарий следующей формы:

#VERSION = value

где value - это целое число, которое представляет номер версии монитора порта.

Номер версии определяет формат управляющего файла монитора порта. Эта строка комментария создается автоматически, когда монитор порта добавляется к системе. Он появляется на строке сам собой до появления элементов сервиса. Обратите внимание, что вся информация в колонке PMSPECIFIC является конкретной информацией для монитора порта ttymon. К примеру, перечень управляющего файла listen будет содержать другое множество элементов в этой колонке. Конкретная информация монитора порта форматируется с помощью команды администратора монитора, в данном примере - командой ttyadm. Команда ttyadm включена как часть команды pmadm, когда она используется с параметром -a.

ЛЕК.8. Функции и функциональные области административного

управления. Стандарты ISO. SMF-функции административного управления. Управление объектами, состояниями, соотношениями, оповещением об ошибках, услугами, проверками и тестированием, регистрацией. SFMA-функциональные области административного управления. Связь SFMA и SMF.

Любое действие по администрированию системы Unix заключается в проведении целого "пакета" действий - запуска различных утилит с хитрыми параметрами и внесении изменений в большое количество конфигурационных файлов. Естественно, что все это можно, а иногда и нужно, проделывать вручную. Иногда это единственный способ что-либо сделать. В помощь начинающему администратору в операционных системах Unix V (например в SVR4/88, ISC Unix V, UnixWare) предназначена "интегрированная диалоговая утилита для системных работ" sysadm.

Для запуска sysadm ОБЯЗАТЕЛЬНО нужно быть Суперпользователем.

Способ употребления:

```
#  sysadm
   Type of your terminal> vt220
```

Или

```
   Login:  sysadm
   Password:
```

Появляется меню, двигаясь по которому стрелочками, Enter'ом, функциональными клавишами, можно добиться того, чего (надеюсь вы знаете чего) хотите.

Внизу, в строке будет иногда появляться посказка примерно такого содержания:

Fill the form and press Continue

В самой нижней строке экрана находится подсказка: Какая именно функциональная клавиша соответствует клавише "CONTINUE". Будьте внимательны. Значение функциональных клавиш может меняться в

зависимости от того, где именно вы находитесь.
Чтобы увидеть возможные варианты выбора, нажимайте F2 (Choices)
Чтобы завершить работу в sysadm, нажмите F7 (CMD-MENU) и выберите "exit".
Примечание. Часто бывает, нужно нажать функциональную клавишу номер такой-то, а она ничего не делает. ВНИМАНИЕ: тогда вместо функциональной клавиши надо нажимать: Ctrl-F Цифра , где Цифра равна номеру требуемой функциональной клавиши. Например, вместо F4 можно нажать Ctrl-F 4
Перемещаться по меню можно не только стрелочками, но также и Ctrl-клавишами: Ctrl-h,j,k,l, ПРОБЕЛОМ, Tab, и первыми буквами команд меню.

ЛЕК.9. Процедура управления системами общего пользования. Общая характеристика структуры системы административного управления. Функции регистрации, сбора и обработки информации. Служба справочника. Информационно-справочные системы.
Утилита системного администратора ADMINTOOL
На рабочих станциях Sun, IBM RS/6000 утилиты для администрирования работают в графическом режиме, под X Windows, с использованием мышки.
Конфигурирование NIS на SunOS 4
Мастер-NIS-сервер.
domainname foms.msk.su
echo foms.msk.su > /etc/defaultdomain
mkdir /var/yp
В файле /etc/rc.local раскомментировать или добавить:

ypserv
ypbind
rpc.yppasswdd /etc/passwd -m passwd

ypxfrd

Скопировать NIS-Makefile в /var/yp : cp /usr/lib/NIS.Makefile /var/yp/Makefile или вставить CD-ROM с системой и

```
cd /tmp
/usr/etc/extract_files sr0 root -f ./var/yp/Makefile
mv ./var/yp/Makefile /var/yp/Makefile
```

Проинициализировать сервера в Мастер-режиме

```
cd /usr/etc/yp
ypinit -m
```

В ответ на запросы перечислить всех предполагаемых slave-серверов, и нажать CTRL-D

Перезагрузиться

После любого изменений информационных файлов, лежащих в NIS на мастер-сервере

```
cd /var/yp
make
```

NIS клиент.

```
domainname foms.msk.su
echo foms.msk.su > /etc/defaultdomain
mkdir /var/yp
```

В файле /etc/rc.local раскомментировать или добавить: ypbind

Slave-NIS-сервер.

```
domainname foms.msk.su
echo foms.msk.su > /etc/defaultdomain
mkdir /var/yp
```

В файле /etc/rc.local раскомментировать или добавить:

ypserv

ypbind

Сделать копию текущих NIS-карт с мастер-NIS сервера

cd /usr/etc/yp

ypinit -s master_nis_server.your.nis.domain

"Ознакомить" Мастер-сервера с новым клиентом

НА МАСТЕР-СЕРВЕРЕ

cd /usr/etc/yp

ypcat -k ypservers > /tmp/tmp-file

echo nowyj_slave_server >> /tmp/tmp-file

ypinit -m < /tmp/tmp-file

Чтобы карты на slave-сервере всегда были свежими

На slave-сервере должна периодически запускаться команда yprfr, которая опрашивает мастер-сервера на предмет изменения NIS-карт.

Частота опроса и внесения изменений задается скриптами

/usr/etc/yp/ypfxr_1perday

/usr/etc/yp/ypfxr_2perday

которые необходимо запускать из root-crontab. Добавьте их туда, если их еще нет. Для справки наберите команду

crontab -l

Информационные команды NIS.

ypwich

ypwich -m

ypwich clientname

yppush map

ypcat map

ypcat -k map

ypmatch key1 key2 map

ЛЕК.10. Управление конфигурацией. Конфигурация ресурсов и ее модель. Внешние параметры. Наблюдаемые характеристики : вероятностные, вероятностно-временные и стоимостные. Управляемые ресурсы. База данных конфигурации. Реконфигурация. Реконфигурация

физической среды и топологии. Трассировка физической среды. Загрузка программного обеспечения. Протоколы загрузки. Примеры управления конфигурацией.

В настоящее время в связи с интеграцией корпоративных сетей передачи данных все более остро встает проблема управления распределенными гетерогенными сетями, состоящими из множества локальных сетей, функционирующих на основе различных стандартов и протоколов. Поставленная в заголовке статьи цель — создание системы интегрированного сетевого управления — требует решения целого ряда задач. В их число входят:

* традиционные задачи сетевого управления (управление конфигурацией, управление производительностью, управление сбоями, управление безопасностью, учет использования ресурсов);

* управление распределенными приложениями в гетерогенных сетях;

* мониторинг текущего состояния системно-технического обеспечения организации (ведение визуализированной базы данных, содержащей полную информацию как о технических, так и об учетных параметрах всего технического и программного обеспечения, имеющегося в той или иной организации);

* поддержка принятия решений по модернизации технического и программного обеспечения с учетом текущего состояния технического прогресса, информации о производителях и поставщиках технических и программных средств и о сравнительных характеристиках этих продуктов;

* управление модернизацией (контроль и управление установкой нового технического и программного обеспечения, включая оптимизацию этого процесса);

* моделирование работы существующих сетей (включая анализ нагрузок на отдельные их участки и поддержку принятия решений по перепланированию).

Следует заметить, что ни один из имеющихся на сегодняшний день

на рынке программного обеспечения продуктов не решает целиком ни одной из перечисленных задач. Поэтому наиболее целесообразным решением в данном случае является либо разработка такой интегрированной системы самостоятельно, либо заказ на ее разработку фирме — системному интегратору.

Напомним, что в настоящее время под собственно сетевым управлением обычно подразумевают совокупность пяти взаимосвязанных задач, в число которых входят:

Управление конфигурацией (Configuration Management), включающее:

* регистрацию устройств сети, их сетевых адресов и идентификаторов;
* определение конфигурации элементов сети;
* определение параметров сетевой операционной системы;
* описание протоколов сетевых взаимодействий;
* построение топологической карты физических соединений сети.

Управление безопасностью (Security Management) подразумевает поддержку служб и отчетов обеспечения защиты информации, что предполагает:

* управление доступом и полномочиями пользователей;
* контроль и управление межсетевыми взаимодействиями;
* защиту от несанкционированного доступа извне;
* обнаружение и устранение вирусов.

Управление сбоями (Fault & Problem Management), в которое входит:

* наблюдение за трафиком;
* обнаружение чрезмерного числа конфликтов и повторных передач данных;
* предупреждение и профилактика ошибок путем анализа работы сети;
* наблюдение за кабельной системой и состоянием сетевых устройств;
* мониторинг удаленных сегментов и межсетевых связей.

Учет использования ресурсов (Accounting Management) предполагает слежение за использованием и оплатой сетевых услуг, в том числе:

* регистрацию и учет использования сетевых ресурсов;
* регистрацию лицензий и учет использования программных средств;
* управление приоритетами пользователей и приложений.

Управление производительностью (Performance Management) — это оценка состояния ресурсов и эффективности их использования, что предполагает:

* сбор и анализ статистических данных о функционировании сети;
* анализ трафика;
* планирование и оценку эффективности использования ресурсов сети;
* выявление узких мест сети;
* анализ сетевых протоколов;
* планирование развития сети.

К продуктам, в той или иной степени реализующим все пять задач сетевого управления, на сегодняшний день относятся:

* OpenView от Hewlett-Packard;
* NetView (Tivoli) от IBM;
* Spectrum от Cabletron;
* Solstice от SunSoft (Sun планирует уход с этого рынка);
* CA Unicenter от Computer Associates.

Следует заметить, что, во-первых, все эти системы по своим функциональным возможностям примерно одинаковы, и, во-вторых, ни один из перечисленных продуктов не реализует все пять задач в полной мере. Стоимость подобных систем составляет от 5 до 100 тысяч долларов, в зависимости от комплектации.

Кроме перечисленных пяти интегрированных продуктов, существует множество решений от сравнительно небольших фирм, в которых реализованы отдельные функции, причем обычно далеко не в полном объеме. При этом продукты третьих фирм не обладают средствами интеграции друг с другом и обычно не поддерживают разработку дополнительных модулей (add-on’s) сторонними разработчиками, не имеют средств работы с внешними базами данных (Oracle, Informix, Ingres)

и поддерживают ограниченный спектр сетевых устройств.

ЛЕК.11. Управление контролем характеристик. Поддержка SMF и подсистемой регистрации, сбора и обработки информации. Измерения параметров и характеристик. Анализ ВВХ и управление. Результаты измерений и их обработка. Формализация обозначений измеряемых характеристик и параметров. Форматы и поля сообщений об измеряемых параметрах и характеристиках. Контроль характеристик и прогнозирование.

Под управлением распределенными приложениями мы будем понимать мониторинг использования приложениями сетевых и локальных ресурсов и возможность изменения управляемых параметров работы этих приложений для достижения наиболее эффективной эксплуатации имеющихся ресурсов.

ЛЕК.12. Управление учетом. Службы управления ошибочными ситуациями. Отчеты. Модели отказов. Вероятностно-временные характеристики. Тарификация. Управление тарификацией. Стоимостные характеристики . Управление услугами и тарификацией. Структура систем расчета с пользователями за услуги.

Следует заметить, что при подобной постановке задачи подходящих готовых средств на современном рынке программного обеспечения просто не существует. Основная причина этого в том, что в настоящее время не существует общего стандарта на протокол обмена информацией с распределенными приложениями. Если для технических устройств есть SNMP, CMIP и RMON, то соответствующий стандарт для ПО еще не принят. Вследствие этого существующие решения не охватывают всего спектра ПО.

Основным подходом к решению проблемы в настоящее время является разработка MIB (Management Information Base) для приложений, что позволяет при наличии соответствующих программ-агентов работать с этими приложениями так же, как с физическими сетевыми устройствами. При этом приложения становятся SNMP-управляемыми. Подобный подход применяет, в частности, фирма Microsoft для своих DHCP- и WINS-серверов, входящих в состав операционной системы Windows NT. Недостатком данного метода является то, что фактически в этом случае возможно управление только серверной частью распределенного приложения, а учет использования сетевых ресурсов для всех компонентов системы невозможен.

Другим подходом к данной задаче является концепция Web-управления, при котором те же функции, что и в случае с SNMP, выполняются через стандартные браузеры (например, Netscape Navigator или Microsoft Internet Explorer). В таком случае, однако, приходится интегрировать в приложение, которым предполагается управлять, Web-сервер, что является достаточно нетривиальной задачей. Кроме того, отмеченные выше недостатки при этом сохраняются.

В любом из перечисленных случаев управление существующими приложениями, особенно если они создавались несколько лет назад, становится практически нереализуемой задачей.

Мониторинг технического и программного обеспечения

Может показаться, что данная задача является повторением задачи номер 1, однако это не совсем так. Сетевое управление хоть и подразумевает ведение базы устройств, однако во всех перечисленных продуктах чисто сетевого управления поддерживаются только технические параметры, причем далеко не все и не для всех устройств. Кроме того, средств добавления интересующих пользователя параметров в базу устройств просто нет.

Некоторые функции мониторинга обеспечивают такие платформы системного управления, как Microsoft System Management Server, который позволяет создавать и поддерживать в актуальном состоянии визуализированную базу данных, содержащую информацию как о техническом, так и о программном обеспечении, имеющемся в организации, однако возможности представления и анализа имеющейся информации в подобных системах довольно ограничены.

В качестве другого подхода к решению данной задачи можно предложить применение СУБД, таких как Informix или Oracle, в которых существуют мощные возможности хранения и выборки интересующей пользователя информации о тех или иных устройствах и программном обеспечении. Недостатком такого подхода, однако, является, во-первых, необходимость поддержания информации в актуальном состоянии, и, во-вторых, отсутствие развитых средств визуализации топологии сети. Поддержка принятия решений по модернизации комплекса технических и программных средств

ЛЕК.13. Управление ошибочными ситуациями и безопасностью. Процедуры управления ошибочными ситуациями. Структура систем управления ошибочными ситуациями. Тестеры протоколов. Способы диагностики. Службы и отчеты управления учетом.Службы безопасности. Механизмы обеспечения безопасности. Поддержка служб механизмами. Реализация служб на уровнях ЭМВОС.

Криптография и управление ключами безопасности. Стандарт DES. Идентификация объекта и механизмы поддержания подлинности. Пароли. Цифровая подпись. Шифрование информации при передаче по каналам связи. Безопасность баз данных административного управления. Протоколы и процедуры безопасности передачи файлов.

Как известно, темпы развития современных технических и программных средств настолько высоки, что время морального устаревания той или иной технологии измеряется не десятилетиями, как в большинстве областей человеческой деятельности, а месяцами. С другой стороны, в любой достаточно крупной организации существует проблема, связанная с постоянным увеличением числа решаемых задач и объемов обрабатываемой информации.

Данные факторы приводят к необходимости создания системы, которая обеспечивала бы поддержку принятия решений по модернизации существующего технического и программного обеспечения для эффективного осуществления предприятием своей основной деятельности. Данная система должна учитывать:

* состав технических и программных средств, имеющихся в организации;

* текущее состояние рынка технических и программных средств;

* информацию о производителях ПО и средств вычислительной техники и их номенклатуре;

* сравнительные характеристики однотипных технических и программных средств;

* сведения о поставщиках технических средств и ПО (номенклатура, уровень цен, надежность, уровень сервиса и т.п.).

Для решения поставленной задачи с учетом всей необходимой информации в настоящий момент пригодны только экспертные системы, к ведущим производителям которых относятся фирмы Gensym (продукт G2), Talarian (RTWorks), COGSYS. Данные фирмы предлагают не готовые экспертные системы для решения данной задачи, а развитые инструментарии их создания, поддерживающие как традиционные парадигмы (графический интерфейс пользователя, объектная ориентированность, управление по событиям), так и парадигмы искусственного интеллекта (продукционные правила, механизмы прямого и обратного вывода и т.п.).

Управление модернизацией

Данная задача очень тесно смыкается с предыдущей, так как после принятия решения по модернизации и осуществления закупки технического и/или программного средства требуется внедрить его в существующую инфраструктуру предприятия, не прерывая технологического процесса.

Некоторые функции управления модернизацией выполняют платформы системного/сетевого управления (например, уже упоминавшийся Microsoft System Management Server или CA Unicenter), поддерживающие некоторые функции централизованной установки программного обеспечения, или специализированные пакеты распространения программных средств (Seagate SoftwareInstall и ему подобные). Недостатком всех этих продуктов является то, что они работают только с ПО, не решая при этом никаких оптимизационных задач.

Для адекватного подхода к управлению модернизацией требуется наличие модели, представляющей текущее состояние технических и программных средств и позволяющей анализировать последствия того или иного изменения этого состояния. Практически единственным подходом в этом случае остается, опять-таки, использование экспертных систем.

Моделирование сетей

Моделирование сетей обычно используется для обоснования принимаемых решений по их модернизации, но иногда может являться вполне самостоятельной задачей.

Модель сети должна обеспечивать:

* визуализацию топологии сети и распределения нагрузок по отдельным сегментам;

* возможность варьирования нагрузок в соответствии с требованиями пользователя, которые определяются спектром решаемых задач;

* отображение работы сети с заданными нагрузками и получение количественных характеристик (длины очередей в буферах, задержки при передаче данных, использование полосы пропускания линий связи и т.п.);

* формирование вариантов модификации как топологии сети, так и устройств, ее составляющих.

Как видно, для анализа работы сети требуется информация, которую можно получать из систем сетевого управления. Результаты моделирования, в свою очередь, используются при принятии решений по модернизации сетей.

В настоящее время на рынке, насколько нам известно, не существует ни одного универсального продукта, пригодного для полномасштабного моделирования работы сети. Это связано с тем, что точное количественное моделирование сколько-нибудь сложной сети (более 100 узлов) требует огромных вычислительных затрат и при современном состоянии вычислительной техники чрезвычайно трудоемко.

Альтернативой точному количественному моделированию сетей может служить имитационное моделирование, позволяющее отслеживать тенденции и выявлять проблемы, связанные с пропускной способностью сегментов сети. Для решения данной задачи средствами имитационного моделирования можно применять и такие средства, как GPSS, но целесообразнее это делать с помощью экспертных систем реального времени, которые зачастую имеют свой собственный планировщик событий и подсистему моделирования.

Использование экспертных систем для решения задачи моделирования позволяет получать обобщенные оценки параметров сети и вариантов ее модернизации; детальное же описание в экспертных системах общего назначения сетевых устройств и протоколов, которые они используют, требует очень больших трудозатрат. Далее можно применить один из специализированных продуктов сетевого моделирования, обеспечивающий поддержку множества реальных сетевых устройств, каналов связи и протоколов взаимодействия. К таким продуктам относятся:

* семейство продуктов Comnet фирмы CACI Products Company;
* OPNET от MIL3;
* SimuNet от Telenix и другие.

Используя эти продукты, можно выработать точный план модернизации сетевого комплекса с учетом текущих нагрузок на сеть и перспектив ее развития.

ЛЕК.14. Оперативное управление и регламентные работы. Основные команды и процедуры оперативного управления. Содержание регламентных работ. Средства автоматизации регламентных работ. Обслуживание, поддержка и управление кабельного и сетевого оборудования, серверов. Управление и обслуживание технических средств. Аппаратно-программные платформы администрирования. Информационные системы администрирования. Программирование в системах администрирования.

Итак, рассмотрев основные задачи сетевого/системного управления, можно сделать вывод, что универсального решения всего комплекса указанных задач не существует. Однако приемлемое решение создать можно. В качестве такого решения предлагается система, состоящая из следующих компонентов:

* ядро системы — экспертная система реального времени;
* платформа сетевого управления — HP OpenView или IBM NetView;
* подсистема моделирования — Comnet III;
* СУБД — Oracle или Informix.

При этом экспертная система (ЭС) является центральным звеном интегрированной среды управления. Она использует информацию из платформы сетевого управления и, в свою очередь, хранит свои данные и результаты работы во внешних СУБД типа Informix или Oracle. Кроме того, ЭС обеспечивает двухсторонний интерфейс с подсистемой точного моделирования сети. В такой конфигурации ЭС выполняет функции мониторинга текущего состояния технического и программного обеспечения, принятия решений по их модернизации и управления процессом модернизации. И, наконец, ЭС объединяет все эти функции в единой распределенной среде с общим интерфейсом.

Одним из возможных кандидатов на создание такой экспертной системы на сегодняшний день является система G2 фирмы Gensym — оболочка, ориентированная на создание экспертных систем реального

времени. Эта система обеспечивает:

* средства работы в реальном времени, внутреннее планирование, параллельные рассуждения;

* структурированный управляемый посредством меню естественно-языковый интерфейс с автоматической проверкой синтаксиса;

* общие правила, уравнения и динамические модели, применимые к классам объектов;

* обратный и прямой вывод, сканирование, фокусирование, использование метазнаний;

* средства управления доступом с помощью механизма авторизации пользователя и обеспечение желаемого “взгляда” на приложение;

* интерфейс оператора, включающий графики, диаграммы, шкалы, кнопки, редактор многослойных пиктограмм;

* взаимодействие с приложениями по сетевым протоколам TCP/IP и DECnet;

* интерфейсы с источниками данных, обеспечивающие эффективную связь с внешними системами, в том числе с СУБД;

* многоплатформность и переносимость создаваемых приложений.

ЛЕК.15. Примеры систем управления. Управление сетями TCP/IP over Ethernet. Системы CISCO NetFlow, IDS. Администрирование сети и сервисов INTERNET. Подключение локальной сети к INTERNET. Регистрация Доменных Имен. Конфигурирование интерфейсов. Драйверы сетевых интерфейсов. Сервисы INTERNET. Организация FTP- сервера. Администрирование серверов WWW. Протокол HTTP. Заключение. Перспективы развития систем административного управления.

В настоящее время существует несколько проблемно-ориентированных средств — надстроек над G2, предназначенных для выполнения специфических операций. К ним относятся:

* Fault Expert — средство для разработки интеллектуального ПО сетевого управления, интегрируемого с традиционными платформами, значительно расширяющее их функциональность;

* ReThink — средство имитационного моделирования сложных систем;

* Neuro-On-Line — средство создания и расчета нейронных сетей, применимых для решения задач, которые практически невозможно решить другими средствами. В частности, нейронные сети можно применять к задаче управления безопасностью, обучив сеть на типичных моделях поведения пользователей различных категорий. После обучения нейронная сеть сможет эффективно распознавать отклонения в поведении и автоматически сигнализировать об этом.

СПРАВОЧНЫЙ МАТЕРИАЛ К ЛАБОРАТОРНЫМ РАБОТАМ

Лаб.1. Приемы работы CLI и утилиты командной строки Win2k

```
ASSOC    Вывод либо изменение сопоставлений по расширениям имен файлов.
AT       Выполнение команд и запуск программ по расписанию.
ATTRIB   Отображение и изменение атрибутов файлов.
BREAK    Включение/выключение режима обработки комбинации клавиш CTRL+C.
CACLS    Отображение/редактирование списков управления доступом (ACL) к файлам.
CALL     Вызов одного пакетного файла из другого.
CD       Вывод имени либо смена текущей папки.
CHCP     Вывод либо установка активной кодовой страницы.
CHDIR    Вывод имени либо смена текущей папки.
CHKDSK   Проверка диска и вывод статистики.
CHKNTFS  Отображение или изменение выполнения проверки диска во время загрузки.
CLS      Очистка экрана.
CMD      Запуск еще одного интерпретатора командных строк Windows 2000.
COLOR    Установка цвета текста и фона, используемых по умолчанию.
COMP     Сравнение содержимого двух файлов или двух наборов файлов.
COMPACT  Отображение/изменение сжатия файлов в разделах NTFS.
CONVERT  Преобразование дисковых томов FAT в NTFS. Нельзя выполнить
         преобразование текущего активного диска.
COPY     Копирование одного или нескольких файлов в другое место.
DATE     Вывод либо установка текущей даты.
DEL      Удаление одного или нескольких файлов.
DIR      Вывод списка файлов и подпапко из указанной папки.
DISKCOMP Сравнение содержимого двух гибких дисков.
DISKCOPY Копирование содержимого одного гибкого диска на другой.
DOSKEY   Редактирование и повторный вызов командных строк; создание макросов.
ECHO     Вывод сообщений и переключение режима отображения команд на экране.
ENDLOCAL Конец локальных изменений среды для пакетного файла.
ERASE    Удаление одного или нескольких файлов.
EXIT     Завершение работы программы CMD.EXE (интерпретатора командных строк).
FC       Сравнение двух файлов или двух наборов файлов
         и вывод различий между ними.
FIND     Поиск текстовой строки в одном или нескольких файлах.
FINDSTR  Поиск строк в файлах.
FOR      Запуск указанной команды для каждого из файлов в наборе.
FORMAT   Форматирование диска для работы с Windows 2000.
FTYPE    Вывод либо изменение типов файлов, используемых при сопоставлении по
         расширениям имен файлов.
GOTO     Передача управления в отмеченную строку пакетного файла.
GRAFTABL Позволяет Windows 2000 отображать расширенный набор символов
         в графическом режиме.
```

```
HELP     Выводит справочную информацию о командах Windows 2000.
IF       Оператор условного выполнения команд в пакетном файле.
LABEL    Создание, изменение и удаление меток тома для дисков.
MD       Создание папки.
MKDIR    Создание папки.
MODE     Конфигурирование системных устройств.
MORE     Последовательный вывод данных по частям размером в один экран.
MOVE     Перемещение одного или нескольких файлов из одной папки в другую.
PATH     Вывод либо установка пути поиска исполняемых файлов.
PAUSE    Приостановка выполнения пакетного файла и вывод сообщения.
POPD     Восстановление предыдущего значения текущей активной папки,
         сохраненного с помощью команды PUSHD.
PRINT    Вывод на печать содержимого текстовых файлов.
PROMPT   Изменение приглашения в командной строке Windows 2000.
PUSHD    Сохранение значения текущей активной папки и переход
         к другой папке.
RD       Удаление папки.
RECOVER  Восстановление читаемой информации с плохого или поврежденного диска.
REM      Помещение комментариев в пакетные файлы и файл CONFIG.SYS.
REN      Переименование файлов и папок.
RENAME   Переименование файлов и папок.
REPLACE  Замещение файлов.
RMDIR    Удаление папки.
SET      Вывод, установка и удаление переменных среды Windows 2000.
SETLOCAL Начало локальных изменений среды для пакетного файла.
SHIFT    Изменение содержимого (сдвиг) подставляемых параметров
         для пакетного файла.
SORT     Сортировка ввода.
START    Запуск программы или команды в отдельном окне.
SUBST    Сопоставляет заданному пути имя диска.
TIME     Вывод и установка системного времени.
TITLE    Назначение заголовка окна для текущего сеанса
         интерпретатора командных строк CMD.EXE.
TREE     Графическое отображение структуры папок заданного диска
         или заданной папки.
TYPE     Вывод на экран содержимого текстовых файлов.
VER      Вывод сведений о версии Windows 2000.
VERIFY   Установка режима проверки правильности записи файлов на диск.
VOL      Вывод метки и серийного номера тома для диска.
XCOPY    Копирование файлов и дерева папок.
```

Лаб.2. Сетевые утилиты Win2k

```
Отображение и изменение таблиц преобразования IP-адресов в физические, используемые
протоколом разрешения адресов (ARP).
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
```

```
ARP -a [inet_addr] [-N if_addr]

  -a            Отображает текущие ARP-записи, опрашивая текущие данные
                протокола. Если задан inet_addr, то будут отображены IP и
                и физический адреса только для заданного компьютера.
                Если более одного сетевого интерфейса используют ARP,
                то будут отображаться записи для каждой таблицы.
  -g            То же, что и ключ -a.
  inet_addr     Определяет IP-адрес.
  -N if_addr    Отображает ARP-записи для заданного в if_addr сетевого
                интерфейса.
  -d            Удаляет узел, задаваемый inet_addr. inet_addr может содержать
                символ шаблона * для удаления всех узлов.
  -s            Добавляет узел и связывает internet адрес inet_addr
                с физическим адресом eth_addr. Физический адрес задается
                6 байтами (в шестнадцатеричном виде), разделенных дефисом.
                Эта связь является постоянной.
  eth_addr      Определяет физический адрес.
  if_addr       Если параметр задан, - он определяет интернет адрес интерфейса,
                чья таблица преобразования адресов должна измениться.
                Если не задан, - будет использован первый доступный интерфейс.
Пример:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  ... Добавляет статическую запись.
  > arp -a                                    ... Выводит ARP-таблицу.

Использование: ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS]
               [-r число] [-s число] [[-j списокУзлов] | [-k списокУзлов]]
               [-w таймаут] списокРассылки

Параметры:
    -t              Отправка пакетов на указанный узел до команды прерывания.
                    Для вывода статистики и продолжения нажмите
                    <Ctrl>+<Break>, для прекращения - <Ctrl>+<C>.
    -a              Определение адресов по именам узлов.
    -n число        Число отправляемых запросов.
    -l размер       Размер буфера отправки.
    -f              Установка флага, запрещающего фрагментацию пакета.
    -i TTL          Задание срока жизни пакета (поле "Time To Live").
    -v TOS          Задание типа службы (поле "Type Of Service").
    -r число        Запись маршрута для указанного числа переходов.
    -s число        Штамп времени для указанного числа переходов.
    -j списокУзлов  Свободный выбор маршрута по списку узлов.
    -k списокУзлов  Жесткий выбор маршрута по списку узлов.
    -w таймаут      Таймаут каждого ответа в миллисекундах.
Отображение статистики протокола и текущих сетевых подключений TCP/IP.

NETSTAT [-a] [-e] [-n] [-s] [-p имя] [-r] [интервал]
```

```
  -a            Отображение всех подключений и ожидающих портов.
                (Подключения со стороны сервера обычно не отображаются).
  -e            Отображение статистики Ethernet. Этот ключ может
                применяться вместе с ключом -s.
  -n            Отображение адресов и номеров портов в числовом формате.
  -p имя        Отображение подключений для протокола "имя": tcp или udp.
                Используется вместе с ключом -s для отображения статистики
                по протоколам. Допустимые значения "имя": tcp, udp или ip.
  -r            Отображение содержимого таблицы маршрутов.
  -s            Отображение статистики по протоколам. По умолчанию выводятся
                данные для TCP, UDP и IP. Ключ -p позволяет указать
                подмножество выводящихся данных.
  интервал      Повторный вывод статистических данных через указанный
                интервал в секундах. Для прекращения вывода данных
                нажмите клавиши CTRL+C. Если параметр не задан, сведения
                о текущей конфигурации выводятся один раз.
Использование: tracert [-d] [-h максЧисло] [-j списокУзлов] [-w интервал] имя

Параметры:
    -d                Без разрешения в имена узлов.
    -h максЧисло      Максимальное число прыжков при поиске узла.
    -j списокУзлов    Свободный выбор маршрута по списку узлов.
    -w интервал       Интервал ожидания каждого ответа в миллисекундах.
```

Лаб.3. Утилита Net.exe Win2k

```
Синтаксис данной команды:
NET HELP имя_команды
      -или-
NET имя_команды /HELP

   Можно использовать следующие имена команд:

   NET ACCOUNTS             NET HELP             NET SHARE
   NET COMPUTER             NET HELPMSG          NET START
   NET CONFIG               NET LOCALGROUP       NET STATISTICS
   NET CONFIG SERVER        NET NAME             NET STOP
   NET CONFIG WORKSTATION   NET PAUSE            NET TIME
   NET CONTINUE             NET PRINT            NET USE
   NET FILE                 NET SEND             NET USER
   NET GROUP                NET SESSION          NET VIEW

   NET HELP SERVICES - эта команда выводит список всех служб, которые
                       можно запустить.
   NET HELP SYNTAX   - эта команда выводит объяснения синтаксических
                       правил, используемых при описании команд в Справке.
```

```
   NET HELP имя_команды | MORE - просмотр справки по одному экрану за раз.

NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
      SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]

NET COMPUTER \\имя_компьютера {/ADD | /DEL}

NET SEND {имя | * | /DOMAIN[:имя] | /USERS} сообщение

NET USE [имя_устройства | *] [\\имя_компьютера\имя_ресурса[\том] [пароль | *]]
        [/USER:[имя_домена\]имя_пользователя]
        [/USER:[имя_домена_с_точками\]имя_пользователя]
        [/USER:[имя_пользователя@имя_домена_с_точками]
        [[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE {имя_устройства | *} [пароль | *] /HOME

NET USE [/PERSISTENT:{YES | NO}]

NET VIEW [\\имя_компьютера [/CACHE] | /DOMAIN[:имя_домена]]
NET VIEW /NETWORK:NW [\\имя_компьютера]
```

Лаб.4. Приемы работы CLI Linux

```
# help
GNU bash, version 2.03.19(1)-release (i586-mandrake-linux-gnu)
These shell commands are defined internally.  Type `help' to see this list.
Type `help name' to find out more about the function `name'.
Use `info bash' to find out more about the shell in general.

A star (*) next to a name means that the command is disabled.

 %[DIGITS | WORD] [&]               . filename
 :                                  [ arg... ]
 alias [-p] [name[=value] ... ]     bg [job_spec]
 bind [-lpvsPVS] [-m keymap] [-f fi break [n]
 builtin [shell-builtin [arg ...]]  case WORD in [PATTERN [| PATTERN].
 cd [-PL] [dir]                     command [-pVv] command [arg ...]
 continue [n]                       declare [-afFrxi] [-p] name[=value
 dirs [-clpv] [+N] [-N]             disown [-h] [-ar] [jobspec ...]
 echo [-neE] [arg ...]              enable [-pnds] [-a] [-f filename]
 eval [arg ...]                     exec [-cl] [-a name] file [redirec
 exit [n]                           export [-nf] [name ...] or export
 false                              fc [-e ename] [-nlr] [first] [last
 fg [job_spec]                      for NAME [in WORDS ... ;] do COMMA
 function NAME { COMMANDS ; } or NA getopts optstring name [arg]
 hash [-r] [-p pathname] [name ...] help [pattern ...]
```

```
history [-c] [n] or history -awrn  if COMMANDS; then COMMANDS; [ elif
jobs [-lnprs] [jobspec ...] or job kill [-s sigspec | -n signum | -si
let arg [arg ...]                  local name[=value] ...
logout                             popd [+N | -N] [-n]
printf format [arguments]          pushd [dir | +N | -N] [-n]
pwd [-PL]                          read [-r] [-p prompt] [-a array] [
readonly [-anf] [name ...] or read return [n]
select NAME [in WORDS ... ;] do CO set [--abefhkmnptuvxBCHP] [-o opti
shift [n]                          shopt [-pqsu] [-o long-option] opt
source filename                    suspend [-f]
test [expr]                        time [-p] PIPELINE
times                              trap [arg] [signal_spec ...] or tr
true                               type [-apt] name [name ...]
typeset [-afFrxi] [-p] name[=value ulimit [-SHacdflmnpstuv] [limit]
umask [-p] [-S] [mode]             unalias [-a] [name ...]
unset [-f] [-v] [name ...]         until COMMANDS; do COMMANDS; done
variables - Some variable names an wait [n]
while COMMANDS; do COMMANDS; done  { COMMANDS ; }
```

man(1) Команда Русский ман man(1)

НАЗВАНИЕ

man - форматирует и отображает страницы руководства (man pages)

manpath - определяет пользовательские пути поиска руководства

СИНТАКСИС

<code>man [-adfhkKtwW] [-m система] [-p строка] [-C файл_конфигурации] [-M путь] [-P программа_просмотра]

[-S список_секций] [секция] имя ...</code>

ОПИСАНИЕ

Команда man форматирует страницы руководства. Текущая версия знает о переменных среды MANPATH и (MAN)PAGER, поэтому Вы можете установить свой собственный набор страниц руководства и свою собственную программу их просмотра. Если указана секция, то man ищет указанную страницу только в этой секции руководства. Вы также можете указать порядок поиска страниц по секциям, а также набор препроцессоров для обработки страниц, с помощью аргументов командной строки либо в переменных среды. Если имя содержит знак `/', то оно считается сначала именем файла, и Вы можете задавать командную строку в виде man ./foo.5 или даже man /cd/foo/bar.1.gz.

ОПЦИИ

-C файл_конфигурации

Указывает, какой из файлов конфигурации man.config использовать; по умолчанию /usr/lib/man.config. (См. man.config(5).)

-M путь

Указывает список директориев для поиска страниц руководства. Если эта опция не указана, то используется переменная среды MANPATH. Если такая переменная не определена, то список директориев поиска по умолчанию берется из /usr/lib/man.config. Пустая строка в переменной MANPATH также означает список

по умолчанию.

-P программа_просмотра

Указывает используемую программу просмотра. Эта опция переопределяет переменную среды MANPAGER, которая, в свою очередь, переопределяет переменную PAGER. По умолчанию man использует /usr/bin/less -is.

-S список_секций

Список секций руководства, в которых производится поиск указанного имени, разделенных двоеточиями. Эта опция переопределяет переменную среды MANSECT.

-a По умолчанию man завершает работу после показа первой найденной страницы руководства с указанным именем. При использовании этой опции man отображает все страницы, имеющие указанное имя, а не только первую.

-c Переформатировать исходную страницу, даже если существует обновленная страница просмотра. Это может быть полезно в тех случаях, когда страница просмотра была отформатирована для экрана с отличным от текущего количеством столбцов.

-d Не отображать страницу, а просто вывести отладочную информацию.

-D Вывести и страницу, и отладочную информацию.

-f Эквивалент whatis.

-h Печатает одну строку помощи и завершается.

-k Эквивалент apropos.

-K Искать указанную строку во *всех* страницах руководства. Предупреждение: эта операция может длиться очень долго! Указание секции может ускорить ее.

-m система

Указать другой набор страниц, в которых следует произвести поиск, основанный на имени заданной системы.

-p строка

Указать последовательность препроцессоров, запускаемых до nroff или troff. Не во всех операциоонных системах устанавливается полный набор препроцессоров. Вот список некоторых препроцессоров и первые их буквы, используемые для задания опции -p: eqn (e), grap (g), pic (p), tbl (t), vgrind (v), refer (r). Эта опция переопределяет переменную среды MANROFFSEQ.

-t Использовать для форматирования страниц команду /usr/bin/groff -Tps -mandoc и вывести результат на стандартный выход (stdout). Результат команды форматирования /usr/bin/groff -Tps -mandoc перед печатью может быть пропущен через те или иные специальные фильтры.

-w или --path

</tag> Не отображать страницы, а вывести полные имена файлов, которые будут форматированы или отображены. Если не дано имя искомой страницы: вывести (на стандартный вывод) список директориев, в которых проводит поиск man. Если команда manpath является ссылкой на man, то `manpath' эквивалентно`man --path'.

-W То же, что и -w, но печатает по одному имени файла на строку, без дополнительной информации. Это бывает полезно в командах шелла вроде man -aW man | xargs ls -l Страницы для просмотра (cat pages) Man пытается сохранить отформатированные страницы для того, чтобы избежать повторного форматирования в

следующий раз при вызове страницы. По традиции отформатированные страницы в DIR/manX сохраняются в DIR/catX, но в файле конфигурации /usr/lib/man.config можно задать иной способ. Если требуемый директорий для страниц просмотра не существует, то они и не сохраняются. Возможно также установить для команды man бит suid с владельцем man. Тогда, если директорий для страниц просмотра имеет владельца man и права 0755 (записывать может только пользователь man), а страницы просмотра имеют права 0644 или 0444 (записывать может только пользователь man, либо вообще никто не может изменять страницы просмотра), никакой другой (обычный) пользователь не сможет изменить страницы просмотра либо положить какие-либо файлы в соответствующий директорий. Если man не является suid-программой, то для обеспечения возможности создания любым пользователем страниц просмотра соответствующие директории должны иметь права 0777.

С опцией -c man переформатирует исходную страницу, даже если существует свежая страница просмотра.

ОКРУЖЕНИЕ

MANPATH Если переменная MANPATH установлена, то ее значение используется как список путей поиска страниц руководства.

MANROFFSEQ Если переменная MANROFFSEQ установлена, то ее значение используется как последовательность вызова препроцессоров перед запуском nroff или troff. По умолчанию исходные страницы пропускаются через табличный препроцессор перед nroff.

MANSECT Если переменная MANSECT установлена, то ее значение используется как список секций руководства, в которых следует производить поиск.

MANWIDTH Если переменная MANWIDTH установлена, то ее значение используется как ширина отображения страниц руководства. В противном случае страницы отображаются на всю ширину экрана.

MANPAGER Если переменная MANPAGER установлена, то ее значение используется как имя программы просмотра

отформатированных страниц руководства. В противном случае используется переменная PAGER. Если ни та, ни другая переменная не установлены, то используется команда /usr/bin/less -is.

LANG Если переменная LANG установлена, то ее значение используется как имя поддиректория, в котором man производит поиск страниц руководства. Так, команда `LANG=dk man 1 foo' приведет к тому, что man будет искать страницу foo сначала в .../dk/man1/foo.1; если же страница не будет найдена, то man продолжит поиск в .../man1/foo.1 (здесь `...' - один из путей поиска, указанных в переменной MANPATH, либо опцией -M).

NLSPATH, LC_MESSAGES, LANG

Переменные NLSPATH и LC_MESSAGES (или LANG, когда последняя не определена) используются для определения директория с файлом сообщений. (Однако сообщения на английском языке влинкованы в команду man, и в этом случае подобный директорий не требуется.) Заметьте, что команды вроде col(1), вызываемые man'ом, также используют, например, LC_CTYPE.

PATH Переменная PATH также используется в определении путей поиска страниц руководства по умолчанию.

SYSTEM Переменная SYSTEM используется для определения имени системы по

умолчанию (совместно с опцией -m).

СМ. ТАКЖЕ

apropos(1) , whatis(1) , less(1) , groff(1) .

Перевод Игоря В. Спиридонова (C) 1998

Лаб.5. Изучение программной структуры административного управления в сетях Ethernet

ARP(8) Linux Programmer's Manual ARP(8)

NAME

arp - manipulate the system ARP cache

SYNOPSIS

arp [-vn] [-H type] [-i if] -a [hostname]

arp [-v] [-i if] -d hostname [pub]

arp [-v] [-H type] [-i if] -s hostname hw_addr [temp]

arp [-v] [-H type] [-i if] -s hostname hw_addr [netmask nm] pub

arp [-v] [-H type] [-i if] -Ds hostname ifa [netmask nm] pub

arp [-vnD] [-H type] [-i if] -f filename

DESCRIPTION

Arp manipulates the kernel's ARP cache in various ways. The primary options are clearing an address mapping entry and manually setting up one. For debugging purposes, the arp program also allows a complete dump of the ARP cache.

OPTIONS

-v, --verbose

Tell the user what is going on by being verbose.

-n, --umeric

shows numerical addresses instead of trying to determine symbolic host, port or user names.

-H type, --hw-type type

When setting or reading the ARP cache, this optional parameter tells arp which class of entries it should check for. The default value of this parameter is ether (i.e. hardware code 0x01 for IEEE 802.3 10Mbps Ethernet). Other values might include network technologies such as ARCnet (arcnet) , PROnet (pronet) , AX.25 (ax25) and NET/ROM (netrom).

-a [hostname], --display [hostname]

Shows the entries of the specified hosts. If the hostname parameter is not used, all entries will be displayed.

-d hostname, --delete hostname

Remove any entry for the specified host. This can be used if the

indicated host is brought down, for example.

-D, --use-device

Use the interface ifa's hardware address.

-i If, --device If

Select an interface. When dumping the ARP cache only entries matching the specified interface will be printed. When setting a perma-

nent or temp ARP entry this interface will be associated with the entry; if this option is not used, the kernel will guess based on the routing table. For pub entries the specified interface is the interface on which ARP requests will be answered.

NOTE: This has to be different from the interface to which the IP datagrams will be routed.

-s hostname hw_addr, --set hostname

Manually create an ARP address mapping entry for host hostname with hardware address set to hw_addr class, but for most classes one can assume that the usual presentation can be used. For the Ethernet class, this is 6 bytes in hexadecimal, separated by colons. When adding proxy arp entries (that is those with the publish flag set a netmask may be specified to proxy arp for entire subnets. This is not good practice, but is supported by older kernels because it can

be useful. If the temp flag is not supplied entries will be permanent stored into the ARP cache.

NOTE: As of kernel 2.2.0 it is no longer possible to set an ARP entry for an entire subnet.

-f filename, --file filename

Similar to the -s option, only this time the address info is taken from file filename set up. The name of the data file is very often /etc/ethers, but this is not official.

The format of the file is simple; it only contains ASCII text lines with a hostname, and a hardware address separated by whitespace. Additionally the pub, temp and netmask flags can be used.

In all places where a hostname is expected, one can also enter an IP address in dotted-decimal notation.

Each complete entry in the ARP cache will be marked with the C flag. Permanent entries are marked with M and published entries have the P flag.

FILES

/proc/net/arp,
/etc/networks

/etc/hosts

/etc/ethers

SEE ALSO

rarp(8), route(8), ifconfig(8), netstat(8)

AUTHORS

Fred N. van Kempen, <waltje@uwalt.nl.mugnet.org> with a lot of improvements from net-tools Maintainer Bernd Eckenfels <net-tools@lina.inka.de>.

NAME

ping - send ICMP ECHO_REQUEST packets to network hosts

SYNOPSIS

ping [-dfnqrvR] [-c count] [-i wait] [-l preload] [-p pattern] [-s packetsize]

DESCRIPTION

Ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams (``pings'') have an IP and ICMP header, followed by a ``struct timeval'' and then an arbitrary number of ``pad'' bytes used to fill out the packet. The options are as follows: Other options are:

-c count

Stop after sending (and receiving) count ECHO_RESPONSE packets.

-d Set the SO_DEBUG option on the socket being used.

-f Flood ping. Outputs packets as fast as they come back or one hundred times per second, whichever is more. For every ECHO_REQUEST sent a period ``.'' is printed, while for ever ECHO_REPLY received a backspace is printed. This provides a rapid display of how many packets are being dropped. Only the super-user may use this option. This can be very hard on a network and should be used with caution.

-i wait

Wait wait seconds between sending each packet. The default is to wait for one second between each packet. This option is incompatible with the -f option.

-l preload

If preload is specified, ping sends that many packets as fast as possible before falling into its normal mode of behavior. Only the super-user may use this option.

-n Numeric output only. No attempt will be made to lookup symbolic names for host addresses.

-p pattern

You may specify up to 16 ``pad'' bytes to fill out the packet you send. This is useful for diagnosing data-dependent problems in a network. For example, ``-p ff'' will cause the sent packet to be filled with all ones.

-q Quiet output. Nothing is displayed except the summary lines at startup time and when finished.

-R Record route. Includes the RECORD_ROUTE option in the ECHO_REQUEST packet and displays the route buffer on returned packets. Note that the IP header is only large enough for nine such routes. Many hosts ignore or discard this option.

-r Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached

network, an error is returned. This option can be used to ping a local host through an interface that has no route through it (e.g., after the interface was dropped by routed(8)).

-s packetsize

Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.

-v Verbose output. ICMP packets other than ECHO_RESPONSE that are received are listed.

When using ping for fault isolation, it should first be run on the local host, to verify that the local network interface is up and running. Then, hosts and gateways further and further away should be ``pinged''. Round-trip times and packet loss statistics are computed. If duplicate packets are received, they are not included in the packet loss calculation, although the round trip time of these packets is used in calculating the minimum/average/maximum round-trip time numbers. When the specified number of packets have been sent (and received) or if the program is terminated with a SIGINT, a brief summary is displayed.

If ping does not receive any reply packets at all it will exit with code 1. On error it exits with code 2. Otherwise it exits with code 0. This makes it possible to use the exit code to see if a host is alive or not.

This program is intended for use in network testing, measurement and management. Because of the load it can impose on the network, it is unwise to use ping during normal operations or from automated scripts.

ICMP PACKET DETAILS

An IP header without options is 20 bytes. An ICMP ECHO_REQUEST packet contains an additional 8 bytes worth of ICMP header followed by an arbitrary amount of data. When a packetsize is given, this indicated the size of this extra piece of data (the default is 56). Thus the amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space (the ICMP header).

If the data space is at least eight bytes large, ping uses the first eight bytes of this space to include a timestamp which it uses in the computation of round trip times. If less than eight bytes of pad are specified, no round trip times are given.

DUPLICATE AND DAMAGED PACKETS

Ping will report duplicate and damaged packets. Duplicate packets should never occur, and seem to be caused by inappropriate link-level retransmissions. Duplicates may occur in many situations and are rarely (if ever) a good sign, although the presence of low levels of duplicates may not always be cause for alarm.

Damaged packets are obviously serious cause for alarm and often indicate broken hardware somewhere in the ping packet's path (in the network or in the hosts).

TRYING DIFFERENT DATA PATTERNS

The (inter)network layer should never treat packets differently depending on the data contained in the data portion. Unfortunately, data-dependent

problems have been known to sneak into networks and remain undetected for long periods of time. In many cases the particular pattern that will have problems is something that doesn't have sufficient ``transitions'', such as all ones or all zeros, or a pattern right at the edge, such as almost all zeros. It isn't necessarily enough to specify a data pattern of all zeros (for example) on the command line because the pattern that is of interest is at the data link level, and the relationship between what you type and what the controllers transmit can be complicated.

This means that if you have a data-dependent problem you will probably have to do a lot of testing to find it. If you are lucky, you may manage to find a file that either can't be sent across your network or that takes much longer to transfer than other similar length files. You can then examine this file for repeated patterns that you can test using the -p option of ping.

TTL DETAILS

The TTL value of an IP packet represents the maximum number of IP routers that the packet can go through before being thrown away. In current practice you can expect each router in the Internet to decrement the TTL field by exactly one.

The TCP/IP specification states that the TTL field for TCP packets should be set to 60, but many systems use smaller values (4.3 BSD uses 30, 4.2 used 15).

The maximum possible value of this field is 255, and most Unix systems set the TTL field of ICMP ECHO_REQUEST packets to 255. This is why you will find you can ``ping'' some hosts, but not reach them with telnet(1) or ftp(1).

In normal operation ping prints the ttl value from the packet it receives. When a remote system receives a ping packet, it can do one of three things with the TTL field in its response:

- Not change it; this is what Berkeley Unix systems did before the 4.3BSD-Tahoe release. In this case the TTL value in the received packet will be 255 minus the number of routers in the round-trip path.
- Set it to 255; this is what current Berkeley Unix systems do. In this case the TTL value in the received packet will be 255 minus the number of routers in the path from the remote system to the pinging host.
- Set it to some other value. Some machines use the same value for ICMP packets that they use for TCP packets, for example either 30 or 60. Others may use completely wild values.

BUGS

Many Hosts and Gateways ignore the RECORD_ROUTE option.

The maximum IP header length is too small for options like RECORD_ROUTE to be completely useful. There's not much that that can be done about this, however.

Flood pinging is not recommended in general, and flood pinging the broadcast address should only be done under very controlled conditions.

SEE ALSO

netstat(1), ifconfig(8), routed(8)

HISTORY

The ping command appeared in 4.3BSD.

Linux NetKit 0.09 August 30, 1996 1

Лаб.6. Процедура управления конфигурацией в сетях Ethernet

IFCONFIG(8) Linux Programmer's Manual IFCONFIG(8)

NAME

ifconfig - configure a network interface

SYNOPSIS

ifconfig [interface]

ifconfig interface [aftype] options | address ...

DESCRIPTION

Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed.

If no arguments are given, ifconfig displays the status of the currently active interfaces. If a single interface argument is given, it displays the status of the given interface only; if a single -a argument is given, it displays the status of all interfaces, even those that are down. Otherwise, it configures an interface.

Address Families

If the first argument after the interface name is recognized as the name of a supported address family, that address family is used for decoding and displaying all protocol addresses. Currently supported address families include inet (TCP/IP, default), inet6 (IPv6), ax25 (AMPR Packet Radio), ddp (Appletalk Phase 2), ipx (Novell IPX) and netrom (AMPR Packet radio).

OPTIONS

interface

The name of the interface. This is usually a driver name followed by a unit number, for example eth0 for the first Ethernet interface.

up This flag causes the interface to be activated. It is implicitly specified if an address is assigned to the interface.

down This flag causes the driver for this interface to be shut down.

[-]arp Enable or disable the use of the ARP protocol on this interface.

[-]promisc

Enable or disable the promiscuous mode of the interface. If selected, all packets on the network will be received by the interface.

[-]allmulti

Enable or disable all-multicast mode. If selected, all multicast packets on the network will be received by the interface.

metric N

This parameter sets the interface metric.

mtu N This parameter sets the Maximum Transfer Unit (MTU) of an interface.

dstaddr addr

Set the remote IP address for a point-to-point link (such as PPP). This keyword is now obsolete; use the pointopoint keyword instead.

netmask addr

Set the IP network mask for this interface. This value defaults to the usual class A, B or C network mask (as derived from the interface IP address), but it can be set to any value.

add addr/prefixlen

Add an IPv6 address to an interface.

del addr/prefixlen

Remove an IPv6 address from an interface.

tunnel aa.bb.cc.dd

Create a new SIT (IPv6-in-IPv4) device, tunnelling to the given destination.

irq addr

Set the interrupt line used by this device. Not all devices can dynamically change their IRQ setting.

io_addr addr

Set the start address in I/O space for this device.

mem_start addr

Set the start address for shared memory used by this device. Only a few devices need this.

media type

Set the physical port or medium type to be used by the device. Not all devices can change this setting, and those that can vary in what values they support. Typical values for type are 10base2 (thin Ethernet), 10baseT (twisted-pair 10Mbps Ethernet), AUI (external transceiver) and so on. The special medium type of auto can be used to tell the driver to auto-sense the media. Again, not all drivers can do this.

[-]broadcast [addr]

If the address argument is given, set the protocol broadcast address for this interface. Otherwise, set (or clear) the IFF_BROADCAST flag for the interface.

[-]pointopoint [addr]

This keyword enables the point-to-point mode of an interface, meaning that it is a direct link between two machines with nobody else listening on it.

If the address argument is also given, set the protocol address of

the other side of the link, just like the obsolete dstaddr keyword does. Otherwise, set or clear the IFF_POINTOPOINT flag for the interface.

hw class address

Set the hardware address of this interface, if the device driver supports this operation. The keyword must be followed by the name of the hardware class and the printable ASCII equivalent of the hardware address. Hardware classes currently supported include ether (Ethernet), ax25 (AMPR AX.25), ARCnet and netrom (AMPR NET/ROM).

multicast

Set the multicast flag on the interface. This should not normally be needed as the drivers set the flag correctly themselves.

address

The IP address to be assigned to this interface.

txqueuelen length

Set the length of the transmit queue of the device. It is useful to set this to small values for slower devices with a high latency (modem links, ISDN) to prevent fast bulk transfers from disturbing interactive traffic like telnet too much.

NOTES

Since kernel release 2.2 there are no explicit interface statistics for alias interfaces anymore. The statistics printed for the original address are shared with all alias addresses on the same device. If you want per-address statistics you should add explicit accounting rules for the address using the ipchains(8) command.

FILES

/proc/net/socket

/proc/net/dev

/proc/net/if_inet6

BUGS

While appletalk DDP and IPX addresses will be displayed they cannot be altered by this command.

SEE ALSO

route(8), netstat(8), arp(8), rarp(8), ipchains(8)

AUTHORS

Fred N. van Kempen, <waltje@uwalt.nl.mugnet.org>

Alan Cox, <Alan.Cox@linux.org>

Phil Blundell, <Philip.Blundell@pobox.com>

Andi Kleen, <ak@muc.de>

net-tools 4 August 1997 1

Лаб.7. Настройки стека протоколов TCP/IP Win2k

Настройка протокола IP для Windows 2000

ИСПОЛЬЗОВАНИЕ:

```
   ipconfig [/? | /all | /release [адаптер] | /renew [адаптер]
            | /flushdns | /registerdns | /showclassid адаптер
            | /setclassid адаптер [устанавливаемый_код_класса_dhcp] ]
   адаптер    Полное имя или имя, содержащие подстановочные знаки "*" и "?" из
              допустимого множества:
              * - любое количество символов, ? - один любой символ.
```

```
   ключи:
       /?           Отобразить это справочное сообщение.
       /all         Отобразить полную информацию о настройке параметров.
       /release     Освободить IP-адрес для указанного адаптера.
       /renew       Обновить IP-адрес для указанного адаптера.
       /flushdns    Очистить кэш разрешений DNS.
       /registerdns Обновить все DHCP-аренды и перерегистрировать DNS-имена
       /displaydns  Отобразить содержимое кэша разрешений DNS.
       /showclassid Отобразить все допустимые для этого адаптера коды (IDs)
                    классов DHCP.
       /setclassid  Изменить код класса DHCP (ID).
По умолчанию отображается только IP-адрес, маска подсети и стандартный шлюз
для каждого подключенного адаптера, для которого выполнена привязка с
TCP/IP.
Для ключей /Release и /Renew, если не указано имя адаптера, то будет
освобожден или обновлен IP-адрес, выданный для всех адаптеров,
для которых существуют привязки с TCP/IP.
Для ключа SetClassID, если не указан код класса (ID),
то существующий код класса будет удален.
Примеры:
    > ipconfig                      - Отображает краткую информацию.
    > ipconfig /all                 - Отображает полную информацию.
    > ipconfig /renew               - Обновляет сведения для всех адаптеров.
    > ipconfig /renew EL*           - Обновляет сведения для адаптеров,
                                      начинающихся с EL....
    > ipconfig /release *ELINK?21*  - Освобождает IP-адреса для всех адаптеров,
    удовлетворяющих запросу, например, ELINK-21, myELELINKi21adapter.
```

Лаб.8-9 Инсталляция рабочей станции ОС Linux. Настройки стека протоколов TCP/IP Linux

```
ROUTE(8)            Linux Programmer's Manual            ROUTE(8)
NAME
       route - show / manipulate the IP routing table
SYNOPSIS
       route [-CFvnee]
       route  [-v] [-A family] add [-net|-host] target [netmask Nm] [gw Gw] [met-
              ric N] [mss M] [window W] [irtt I] [reject] [mod] [dyn] [reinstate]
              [[dev] If]
       route  [-v] [-A family] del [-net|-host] target [gw Gw] [netmask Nm] [met-
              ric N] [[dev] If]
       route  [-V] [--version] [-h] [--help]
DESCRIPTION
       Route manipulates the kernel's IP routing table.  Its primary  use  is  to
       set  up static routes to specific hosts or networks via an interface after
       it has been configured with the ifconfig(8) program.
```

OPTIONS

-v select verbose operation.

-A family

Use the specified address family (eg `inet', `inet6').

-n show numerical addresses instead of trying to determine symbolic host names. This is useful if you are trying to determine why the route to your nameserver has vanished.

-e use netstat(8)-format for displaying the routing table. -ee will generate a very long line with all parameters from the routing table.

-net the target is a network.

-host the target is a host.

-F displays the kernel FIB routing table. The layout can be changed with -e and -ee

-C displays the kernel's route cache.

del deletes a route.

add adds a route.

target The destination network or host. You can provide IP addresses in dotted decimal or host/network names.

netmask Nm

modifier specifies the netmask of the route to be added.

gw Gw Any IP packets for the target network/host will be routed through the specified gateway. NOTE: The specified gateway must be reachable first. This usually means that you have to set up a static route to the gateway beforehand. If you specify the address of one of your local interfaces, it will be used to decide about the interface to which the packets should be routed to. This is a BSDism compatibility hack.

metric M

Set the metric field in the routing table (used by routing daemons) to M.

mss M Set the TCP Maximum Segment Size (MSS) for connections over this route to M bytes. This is normally used only for fine optimisation of routing setups. The default is 536.

window W

Set the TCP window size for connections over this route to W bytes. This is typically only used on AX.25 networks and with drivers unable to handle back to back frames.

irtt I Set the initial round trip time (irtt) for TCP connections over this route to I milliseconds (1-12000). This is typically only used on AX.25 networks. If omitted the RFC 1122 default of 300ms is used.

reject Install a blocking route, which will force a route lookup to fail. This is for example used to mask out networks before using the default route. This is NOT for firewalling.

mod, dyn, reinstate

Install a dynamic or modified route. Both flags are generally only

set by a routing daemon. This is only for diagnostic purpose.

dev If Forces the route to be associated with the specified device, as the kernel will otherwise try to determine the device on its own (by checking already existing routes and device specifications, and where the route is added to). In most normal networks you won't need this.

If dev If is the last option on the command line, the word dev may be omitted, as it's the default. Otherwise the order of the route modifiers (metric - netmask - gw - dev) doesn't matter.

EXAMPLES

route add -net 127.0.0.0

adds the normal loopback entry, using netmask 255.0.0.0 (class A net, determined from the destination address) and associated with the "lo" device (assuming this device was prviously set up correctly with ifconfig(8)).

route add -net 192.56.76.0 netmask 255.255.255.0 dev eth0

adds a route to the network 192.56.76.x via "eth0". The Class C netmask modifier is not really necessary here because 192.* is a Class C IP address. The word "dev" can be omitted here.

route add default gw mango-gw

adds a default route (which will be used if no other route matches). All packets using this route will be gatewayed through "mango-gw". The device which will actually be used for that route depends on how we can reach "mango-gw" - the static route to "mango-gw" will have to be set up before.

route add ipx4 sl0

Adds the route to the "ipx4" host via the SLIP interface (assuming that "ipx4" is the SLIP host).

route add -net 192.57.66.0 netmask 255.255.255.0 gw ipx4

This command adds the net "192.57.66.x" to be gatewayed through the former route to the SLIP interface.

route add 224.0.0.0 netmask 240.0.0.0 dev eth0

This is an obscure one documented so people know how to do it. This sets all of the class D (multicast) IP routes to go via "eth0". This is the correct normal configuration line with a multicasting kernel.

route add 10.0.0.0 netmask 255.0.0.0 reject

This installs a rejecting route for the private network "10.x.x.x."

OUTPUT

The output of the kernel routing table is organized in the following columns

Destination

The destination network or destination host.

Gateway

The gateway address or '*' if none set.

Genmask

The netmask for the destination net; '255.255.255.255' for a host

destination and '0.0.0.0' for the default route.

Flags Possible flags are

U (route is up)

H (target is a host)

G (use gateway)

R (reinstate route for dynamic routing)

D (dynamically installed by daemon or redirect)

M (modified from routing daemon or rederict)

! (reject route)

Metric The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.

Ref Number of references to this route. (Not used in the Linux kernel.)

Use Count of lookups for the route. Depending on the use of -F and -C this will be either route cache misses (-F) or hits (-C).

Iface Interface to which packets for this route will be sent.

MSS Default maximum segement size for TCP connections over this route.

Window Default window size for TCP connections over this route.

irtt Initial RTT (Round Trip Time). The kernel uses this to guess about the best TCP protocol parameters without waiting on (possible slow) answers.

HH (cached only)

The number of ARP entries and cached routes that refer to the hardware header cache for the cached route. This will be -1 if a hardware address is not needed for the interface of the cached route (e.g. lo).

Arp (cached only)

Whether or not the hardware address for the cached route is up to date.

FILES

/proc/net/ipv6_route

/proc/net/route

/proc/net/rt_cache

SEE ALSO

ifconfig(8), netstat(8), arp(8), rarp(8)

HISTORY

Route for Linux was originally written by Fred N. van Kempen, <waltje@uwalt.nl.mugnet.org> and then modified by Johannes Stille and Linus Torvalds for pl15. Alan Cox added the mss and window options for Linux 1.1.22. irtt support and merged with netstat from Bernd Eckenfels.

AUTHOR

Currently maintained by Phil Blundell <Philip.Blundell@pobox.com>.

Лаб.10-12 Инсталляция серверных компонент ОС Linux

```
HTTPD(8)                          httpd                          HTTPD(8)
NAME
       httpd - Apache Hypertext Transfer Protocol Server
SYNOPSIS
       httpd [ -d serverroot ] [ -f config ] [ -C directive ] [ -c directive ]
       [ -D parameter ] [ -e level ] [ -E file  ]  [  -k  start|restart|grace-
       ful|stop|graceful-stop ] [ -R directory ] [ -h ] [ -l ] [ -L ] [ -S ] [
       -t ] [ -v ] [ -V ] [ -X ] [ -M ]
       On Windows systems, the following additional arguments are available:
       httpd [ -k install|config|uninstall ] [ -n name ] [ -w ]
SUMMARY
httpd is the Apache HyperText Transfer Protocol (HTTP) server  program.
       It is designed to be run as a standalone daemon process. When used like
       this it will create a pool of child  processes  or  threads  to  handle
       requests.
       In  general, httpd should not be invoked directly, but rather should be
       invoked via apachectl on Unix-based systems or as a service on  Windows
       NT, 2000 and XP and as a console application on Windows 9x and ME.
oPTIONS
       -d serverroot
              Set  the  initial  value for the ServerRoot directive to server-
              root. This can be overridden by the ServerRoot directive in  the
              configuration file. The default is /usr/local/apache2.
       -f config
              Uses  the  directives  in  the file config on startup. If config
              does not begin with a /, then it is taken to be a path  relative
              to the ServerRoot. The default is conf/httpd.conf.
       -k start|restart|graceful|stop|graceful-stop
              Signals  httpd  to  start, restart, or stop. See Stopping Apache
              for more information.
       -C directive
              Process the configuration directive before reading config files.
       -c directive
              Process  the configuration directive after reading config files.
       -D parameter
              Sets a configuration parameter which can be used with <IfDefine>
              sections  in  the  configuration  files to conditionally skip or
              process commands at server startup and restart.
       -e level
              Sets the LogLevel to level during server startup. This is useful
              for  temporarily  increasing the verbosity of the error messages
              to find problems during startup.
       -E file
```

Send error messages during server startup to file.

-R directory

When the server is compiled using the SHARED_CORE rule, this specifies the directory for the shared object files.

-h Output a short summary of available command line options.

-l Output a list of modules compiled into the server. This will not list dynamically loaded modules included using the LoadModule directive.

-L Output a list of directives together with expected arguments and places where the directive is valid.

-M Dump a list of loaded Static and Shared Modules.

-S Show the settings as parsed from the config file (currently only shows the virtualhost settings).

-t Run syntax tests for configuration files only. The program immediately exits after these syntax parsing tests with either a return code of 0 (Syntax OK) or return code not equal to 0 (Syntax Error). If -D DUMP_VHOSTS is also set, details of the virtual host configuration will be printed. If -D DUMP_MODULES is set, all loaded modules will be printed.

-v Print the version of httpd, and then exit.

-V Print the version and build parameters of httpd, and then exit.

-X Run httpd in debug mode. Only one worker will be started and the server will not detach from the console.

The following arguments are available only on the Windows platform:

-k install|config|uninstall

Install Apache as a Windows NT service; change startup options for the Apache service; and uninstall the Apache service.

-n name

The name of the Apache service to signal.

-w Keep the console window open on error so that the error message can be read.

Apache HTTP Server 2005-09-20 HTTPD(8)

Лаб.13-14 Настройка системы учета трафика NetFlow/FlowTools (ч.1)

flow-capture(1) flow-capture(1)

NAME

flow-capture -- Manage storage of flow file archives by expiring old data.

SYNOPSIS

flow-capture [-hu] [-b big|little] [-C comment] [-c flow_clients] [-d debug_level] [-D daemonize] [-e expire_count] [-f filter_fname] [-F filter_definition] [-E expire_size] [-n rotations] [-N nesting_level] [-p pidfile] [-R rotate_program] [-S stat_interval] [-t tag_fname] [-T active_def|active_def,active_def ...] [-V pdu_version] [-z z_level] -w workdir [-x xlate_fname] [-X xlate_definition]

localip/remoteip/port

DESCRIPTION

The flow-capture utility will receive and store NetFlow exports to disk. The flow files are rotated rotationstimes per day and expiration of old flow files can be configured by number of files or total space utilization. Files are stored in workdir and can optionally be stored in additional levels of directories. Active files created by flow-capture begin with 'tmp'. Files that are complete begin with 'ft'.

When the remoteip is configured only flows from that exporter will be processed, this is the most secure and recommended configuration. When the localip is configured flow-capture will only process flows sent to the localip IP address. If remoteip is 0 (not configured) flows from any source IP address are accepted. Multiple non aggregated PDU versions may be accepted at once to support Cisco's Catalyst 6500 NetFlow implementation which exports from both the supervisor and MSFC with the same IP address and same port but different export versions. In this case the exports will be stored in the format specified by pdu_version or whichever export type is received first.

NetFlow exports are UDP and do not employ congestion control or a retransmission mechanism. If the server flow-capture is configured on is too busy, or the network is congested or lossy NetFlow exports will be lost. An estimate of lost flows is recorded in the flow files, and logged via syslog. Most servers will provide a count of dropped packets due to full socket buffers via the netstat utility. For example netstat -s | grep full will provide a count of UDP packets dropped due to full socket buffers. If this is a persistent occurrence either flow-capture will need a larger server or the compression level should be decreased with -z.

A SIGHUP signal will cause flow-capture to close the current file and create a new one.

A SIGQUIT or SIGTERM signal will cause flow-capture to close the current file and exit.

OPTIONS

-b big|little

Byte order of output.

-c flow_clients

Enable flow_clients TCP clients. When libwrap is available the client must be in a permit list for the service flow-capture-client.

-C Comment

Add a comment.

-d debug_level

Enable debugging.

-e expire_count

Retain the maximum number of files so that the total file count is less than expire_count. Defaults to 0 (do not expire).

-E expire_size

Retain the maximum number of files so that the total storage is less than expire_size. The letters b,K,M,G can be used as multipliers, ie 16 Megabytes is 16M. Default to 0 (do not expire).

-f filter_fname

Filter list filename. Defaults to /usr/local/etc/flow-tools/filter.

-F filter_definition

Select the active definition. Defaults to default.

-h Display help.

-n rotations

Configure the number of times flow-capture will create a new file per day. The default is 95, or every 15 minutes.

-N nesting_level

Configure the nesting level for storing flow files. The default is 0.

-3	YYYY/YYYY-MM/YYYY-MM-DD/flow-file
-2	YYYY-MM/YYYY-MM-DD/flow-file
-1	YYYY-MM-DD/flow-file
0	flow-file
1	YYYY/flow-file
2	YYYY/YYYY-MM/flow-file
3	YYYY/YYYY-MM/YYYY-MM-DD/flow-file

-p pidfile

Configure the process ID file. Use - to disable pid file creation.

-R rotate_program

Execute rotate_program with the first argument as the flow file name after rotating it.

-S stat_interval

When configured flow-capture will log a timestamped message every stat_interval minutes indicating counters such as the number of flows received, packets processed, and lost flows.

-t tag_fname

Load tags from tag_name

-T active_def|active_def,active_def...

Use active_def as the active tag definition(s).

-u Preserve inherited umask. By default the umask will be set to 0022.

-V pdu_version

Use pdu_version format output.

1	NetFlow version 1 (No sequence numbers, AS, or mask)
5	NetFlow version 5
6	NetFlow version 6 (5+ Encapsulation size)
7	NetFlow version 7 (Catalyst switches)
8.1	NetFlow AS Aggregation

8.2 NetFlow Proto Port Aggregation
8.3 NetFlow Source Prefix Aggregation
8.4 NetFlow Destination Prefix Aggregation
8.5 NetFlow Prefix Aggregation
8.6 NetFlow Destination (Catalyst switches)
8.7 NetFlow Source Destination (Catalyst switches)
8.8 NetFlow Full Flow (Catalyst switches)
8.9 NetFlow ToS AS Aggregation
8.10 NetFlow ToS Proto Port Aggregation
8.11 NetFlow ToS Source Prefix Aggregation
8.12 NetFlow ToS Destination Prefix Aggregation
8.13 NetFlow ToS Prefix Aggregation
8.14 NetFlow ToS Prefix Port Aggregation
1005 Flow-Tools tagged version 5

-w workdir
Work in workdir.

-x xlate_fname
Translation config file name. Defaults to /usr/local/etc/flow-tools/xlate.c fg

-X xlate_definition
Translation definition. Defaults to default.

-z z_level
Configure compression level to z_level. 0 is disabled (no compression), 9 is highest compression.

EXAMPLES

Receive flows from the exporter at 10.0.0.1 port 9800. Maintain 5 Gigabytes of flow files in /flows/krc4. Mask the source and destination IP addresses contained in the flow exports with 255.255.248.0.

```
flow-capture -w /flows/krc4 -m 255.255.248.0 -E5G 0/10.0.0.1/9800
```

Receive flows from any exporter on port 9800. Do not perform any flow file space management. Store the exports in /flows/krc4. Emit a stat log message every 5 minutes.

```
flow-capture -w /flows/krc4 0/0/9800 -S5
```

BUGS

Empty directories are not removed.

FILES

Configuration files:
Tag - /usr/local/etc/flow-tools/tag.cfg.
Filter - /usr/local/etc/flow-tools/filter.cfg.
Xlate - /usr/local/etc/flow-tools/xlate.cfg.

AUTHOR

Mark Fullmer maf@splintered.net

SEE ALSO

flow-tools(1)

Лаб.15. Настройки системы IDS snort

How to use Snort by Martin Roesch

1.0 GETTING STARTED

Snort really isn't very hard to use, but there are a lot of command line options to play with, and it's not always obvious which ones go together well. This file aims to make using Snort easier for new users.

Before we proceed, there are a few basic concepts you should understand about Snort. There are three main modes in which Snort can be configured: sniffer, packet logger, and network intrusion detection system. Sniffer mode simply reads the packets off of the network and displays them for you in a continuous stream on the console. Packet logger mode logs the packets to the disk. Network intrusion detection mode is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user defined rule set and perform several actions based upon what it sees.

2.0 SNIFFER MODE

First, let's start with the basics. If you just want to print out the TCP/IP packet headers to the screen (i.e. sniffer mode), try this:

./snort -v

This command will run Snort and just show the IP and TCP/UDP/ICMP headers, nothing else. If you want to see the payload data in transit, try the following:

./snort -vd

This instructs Snort to display the packet data as well as the headers. If you want an even more descriptive display, showing the data link layer headers do this:

./snort -vde

(As an aside, these switches may be divided up or smashed together in any combination. The last command could also be typed out as:

./snort -d -v -e

and it would do the same thing.)

3.0 PACKET LOGGER MODE

Ok, all of these commands are pretty cool, but if you want to record the packets to the disk, you need to specify a logging directory and Snort will automatically know to go into packet logger mode:

```
./snort -dev -l ./log
```

Of course, this assumes you have a directory named "log" in the current directory. If you don't, Snort will exit with an error message. When Snort runs in this mode, it collects every packet it sees and places it in a directory hierarchy based upon the IP address of one of the hosts in the datagram.

If you just specify a plain "-l" switch, you may notice that Snort sometimes uses the address of the remote computer as the directory in which it places packets, and sometimes it uses the local host address. In order to log relative to the home network, you need to tell Snort which network is the home network:

```
./snort -dev -l ./log -h 192.168.1.0/24
```

This rule tells Snort that you want to print out the data link and TCP/IP headers as well as application data into the directory ./log, and you want to log the packets relative to the 192.168.1.0 class C network. All incoming packets will be recorded into subdirectories of the log directory, with the directory names being based on the address of the remote (non-192.168.1) host. Note that if both hosts are on the home network, then they are recorded based upon the higher of the two's port numbers, or in the case of a tie, the source address.
If you're on a high speed network or you want to log the packets into a more compact form for later analysis you should consider logging in "binary mode". Binary mode logs the packets in "tcpdump format" to a single binary file in the logging directory:

```
./snort -l ./log -b
```

Note the command line changes here. We don't need to specify a home network any longer because binary mode logs everything into a single file, which eliminates the need to tell it how to format the output directory structure. Additionally, you don't need to run in verbose mode or specify the -d or -e switches becuase in binary mode the entire packet is logged, not just sections of it. All that is really required to place Snort into logger mode is the specification of a logging directory at the command line with the -l switch, the -b binary logging switch merely provides a modifier to tell it to log the packets in something other than the default output format of plain ASCII text.

Once the packets have been logged to the binary file, you can read the packets

back out of the file with any sniffer that supports the tcpdump binary format such as tcpdump or Ethereal. Snort can also read the packets back by using the -r switch, which puts it into playback mode. Packets from any tcpdump formatted file can be processed through Snort in any of its run modes. For example, if you wanted to run a binary log file through Snort in sniffer mode to dump the packets to the screen, you can try something like this:

```
./snort -dv -r packet.log
```

You can manipulate the data in the file in a number of ways through Snort's packet logging and intrusion detection modes, as well as with the BPF interface that's available from the command line. For example, if you only wanted to see the ICMP packets from the log file, simply specify a BPF filter at the command line and Snort will only "see" the ICMP packets in the file:

```
./snort -dvr packet.log icmp
```

For more info on how to use the BPF interface, read the man page.

4.0 NETWORK INTRUSION DETECTION MODE

To enable network intrusion detection (NIDS) mode (so that you don't record every single packet sent down the wire), try this:

```
./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf
```

Where snort.conf is the name of your rules file. This will apply the rules set in the snort.conf file to each packet to decide if an action based upon the rule type in the file should be taken. If you don't specify an output directory for the program, it will default to /var/log/snort.

One thing to note about the last command line is that if Snort is going to be used in a long term way as an IDS, the "-v" switch should be left off the command line for the sake of speed. The screen is a slow place to write data to, and packets can be dropped while writing to the display.

It's also not necessary to record the data link headers for most applications, so the so it's not necessary to specify the -e switch either.

```
./snort -d -h 192.168.1.0/24 -l ./log -c snort.conf
```

This will configure Snort to run in it's most basic NIDS form, logging packets that the rules tell it to in plain ASCII to a hierarchical directory structure (just like packet logger mode).

4.1 NIDS MODE OUTPUT OPTIONS

There are a number of ways to configure the output of Snort in NIDS mode. The

default logging and alerting mechanisms are to log in decoded ASCII format and use "full" alerts. The full alert mechanism prints out the alert message in addition to the full packet headers. There are several other alert output modes available at the command line, as well as two logging facilities. Packets can be logged to their default decoded ASCII format or to a binary log file via the -b command line switch. If you wish to disable packet logging all together, use the -N command line switch.

Alert modes are somewhat more complex. There are seven alert modes available at the command line: full, fast, socket, syslog, console, cmg, and none. Six of these modes are accessed with the -A command line switch. These are:

```
    -A fast    -  fast alert mode, write the alert in a simple format with a
                  timestamp, alert message, source and destination IPs/ports

    -A full    -  this is also the default alert mode, so if you specify
                  nothing this will automatically be used

    -A unsock  -  send alerts to a UNIX socket that another program can
                  listen on

    -A none    -  turn off alerting

    -A console -  send "fast-style" alerts to the console (screen)

    -A cmg     -  generate "cmg style" alerts
```

To send alerts to syslog, use the -s switch. The default facilities for the syslog alerting mechanism are LOG_AUTHPRIV and LOG_ALERT. If you want to configure other facilities for syslog output, use the output plugin directives in the rules files (see the snort.conf file for more information).

Here are some output configuration examples:

1) Log to default (decoded ASCII) facility and send alerts to syslog
```
snort -c snort.conf -l ./log -s -h 192.168.1.0/24
```

2) Log to the default facility in /var/log/snort and send alerts to a fast alert file:
```
snort -c snort.conf -s -h 192.168.1.0/24
```

3) Log to a binary file and use fast alerting mode, logging to /var/snort:
```
snort -c snort.conf -b -A fast -l /var/snort
```

4.2 PERFORMANCE CONFIGURATION

If you want Snort to go *fast* (like keep up with a 100 Mbps net fast) use the

"-b" and "-A fast" or "-s" (syslog) options. This will log packets in tcpdump format and produce minimal alerts. For example:
./snort -b -A fast -c snort-lib

In this configuration, Snort has been able to log multiple simultaneuos probes and attacks on a 100 Mbps LAN running at a saturation level of approximately 80 Mbps. In this configuration the logs are written in binary format to the snort.log tcpdump-formatted file. To read this file back and break out the data in the familiar Snort format, just rerun Snort on the data file with the "-r" option and the other options you would normally use. For example:

./snort -d -c snort-lib -l ./log -h 192.168.1.0/24 -r snort.log

Once this is done running, all of the data will be sitting in the log directory in its normal decoded format. Cool, eh?

4.3 OTHER STUFF

Some people don't like the default way in which Snort applies it's rules to packets, with the Alert rules applied first, then the Pass rules, and finally the Log rules. This sequence is somewhat counterintuitive, but it's a more foolproof method than allowing the user to write a hundred alert rules and then disable them all with an errant pass rule. For people who know what they're doing, the "-o" switch has been provided to change the default rule applicaition behavior to Pass rules, then Alert, then Log:

./snort -d -h 192.168.1.0/24 -l ./log -c snort.conf -o

5.0 MISCELLANEOUS STUFF

If you are willing to run snort in "daemon" mode, you can add -D switch to any combination above. PLEASE NOTE that if you want to be able to restart snort by sending SIGHUP signal to the daemon, you will need to use full path to snort binary, when you start it, i.g.:

/usr/local/bin/snort -d -h 192.168.1.0/24 -l /var/log/snortlogs -c /usr/local/etc
/snort-lib -s -D

Relative pathes are not supported due to security concerns.

If you're going to be posting packet logs to public mailing lists you might want to try out the -O switch. This switch "obfuscates" your the IP addresses in the packet printouts. This is handy if you don't want the people on the mailing list to know the IP addresses involved. You can also combine the -O switch with the -h switch to only obfuscate the IP addresses of hosts on the home network. This is useful if you don't care who sees the address of the attacking host. For example:

```
./snort -d -v -r snort.log -O -h 192.168.1.0/24
```

This will read the packets from a log file and dump the packets to the screen, obfuscating only the addresses from the 192.168.1.0/24 class C network.

If you want to see Snort's packet statistics without stopping the process, send a SIGUSR1 to the Snort process ID and it will dump stats to the screen or syslog if it's running in daemon mode. This will allow you to see which protocols Snort has been seeing, get counts of alerts and logged packets and counts of total packets seen and dropped. It's a very handy capability if you're tweaking Snort for performance.

Well, that's about it for now. If you have any further questions about using Snort, drop me an e-mail at roesch@sourcefire.com.

ПРИМЕРЫ ТЕСТОВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ЗНАНИЙ

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Дисциплина: "Администрирование информационных систем"

Тест по контролю остаточных знаний
Факультет МиИ Специальность: 0719 Курс IV

Утверждено на заседании кафедры _____ 2003г. **"Утверждаю":_____ зав. кафедрой ИУС**

Группа: _____ ФИО Студента:_____

1 Виртуальные адреса заменяются на физические во время:

	1	2	3	4	5
	загрузки программы в ОП	обращения к виртуальному адресу	компиляции программы	обращения к физическому адресу	выделения сегмента кода для программы

2 Где хранятся каталоги и таблицы станиц:

	1	2	3	4	5
	в регистрах процессора	в стеке ядра ОС	в RAM	в ROM	в области своппинга

3 Выделите термины, являющиеся синонимами, применительно к сетевым ОС:

	1	2	3	4	5
	оболочка	сервер	клиент	сервис	услуга

4 Драйвер устройства выполняет функции:

	1	2	3	4	5
	управления файловой системой	обработки прерывания от устройства	организации прямого доступа к памяти	управления выводом информации	низкого уровня по управлению устройством

5 Выделите термины, являющиеся синонимами, применительно к многозадачной ОС:

	1	2	3	4	5
	программа	процесс	задача	поток	нить

6 За приоритетное обслуживание запросов устройств ввода-вывода к процессору отвечает:

	1	2	3	4	5
	Контроллер ПДП	Сопроцессор	Микропроцессор	Контроллер прерываний	Контроллер ввода/вывода

7 Выделите термины, являющиеся синонимами, применительно к режимам работы задачи:

	1	2	3	4	5
	реальный	супервизора	защищенный	ядра	пользовательский

8 Роль арбитра шины, помимо процессора, выполняет:

	1	2	3	4	5
	Сопроцессор	Контроллер ПДП	Контроллер прерываний	Видео-контроллер	Системный таймер

9 За трансляцию виртуальных адресов в физические отвечает:

	1	2	3	4	5

	Буфер TLB	Кэш-память данных/команд	Регистр CR2	Дескриптор сегмента	Контроллер НЖМД

10 Дескриптор сегмента x86 НЕ содержит поля:

	1	2	3	4	5
	Base	Type	Length	RPL	Limit

11 Процесс, при прочих равных условиях, будет выполняться быстрее:

	1	2	3	4	5
	в мультизадачной ОС	в ОС реального времени	в невытесняющей ОС	в однозадачной ОС	в ОС с вытеснением

12 За текущий уровень привилегии задачи отвечает:

	1	2	3	4	5
	Поле RPL селектора сегмента	Поле CPL	Поле DPL	Регистр CR0	Регистр GDTR

13 ОС выделяет файлам пространство на диске

	1	2	3	4	5
	секторами	дорожками	кластерами	цилиндрами	байтами

14 Для файла TEST в NTFS утановлены права: Группе -NoAccess, пользователю группы -Change какие действия разрешены данному пользователю над файлом TEST:

	1	2	3	4	5
	Change	Read	Write	FullControl	NoAccess

15 Какой смысл имеет разрешение "выполнить" для каталога TEST в UFS

	1	2	3	4	5
	просмотр содержимого каталога TEST	сменить текущий каталог на каталог TEST	выполнять программы, содержащиеся в каталоге TEST	открыть любой файл, содержащиеся в каталоге TEST	уничтожить каталог TEST

16 Увеличение доступного дискового пространства в UFS позволяет выполнить операция

	1	2	3	4	5
	монтирования	реплицирования	кэширования	резервирования	инкременти-рования

17 Приведите сетевые ОС с выделенным сервером

	1	2	3	4	5
	NT	UNIX	QNX	NetWare	Windows 2003

18 Распределенные приложения, по сравнению с локальными, обеспечивают:

	1	2	3	4	5
	масштабируемость	отказоустойчи-вость	безопасность	скорость реакции	простоту программирования

19 После логического входа пользователя в систему неоднократно выполяется операция

	1	2	3	4	5
	авторизации	аутентификации	регистрации	учета	квотирования

20 Совокупность защищенных каналов в публичной сети называется:

	1	2	3	4	5
	VPN	WLAN	VLAN	Intranet	WAN

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Дисциплина: "Администрирование в информационных системах"

Промежуточный тест

Факультет МиИ Специальность: 0719 Курс IV

Утверждено на заседании кафедры _____ 2006г. **"Утверждаю":_____ зав. кафедрой ИУС**

Группа: _____ ФИО Студента:_____

1 Приведите иерархию ПО ВС

2 Перечислите компоненты ядра ОС

3 Укажите ключевое слово, определяющее обслуживающее запросы ПО

оболочка	сервер	клиент	сервис	услуга

4 Драйвер устройства выполняет функции:

управления файловой системой	обработки прерывания от устройства	организации прямого доступа к памяти	управления выводом информации	низкого уровня по управлению устройством

5 Синоним хранимого в файле кода:

программа	процесс	задача	поток	нить

6 Преречислите ресурсы, за которые "борятся" приложения в многозадачной ОС

7 Ядро многозадачной ОС работает в режиме:

реальном	супервизора	защищенном	прикладном	пользовательском

8 Опишите алгоритм установления сессии TCP

9 Интерфейс системных вызовов предназначен для обращения к:

процессору	устройству	пользовательскому процессу	функциям ядра ОС	BIOS

10 Опишите кратко функционирование механизма подкачки страниц по требованию

11 Уражите ключевое слово, относящееся к NTFS

Распределенная	журнализируемая	кластерная	монтируемая	зеркалируемая

12 Процесс, при прочих равных условиях, будет выполняться быстрее:

в мультизадачной ОС	в ОС реального времени	в невытесняющей ОС	в однозадачной ОС	в ОС с вытеснением

13 Расставьте номера уровня модели OSI для приведенных протоколов:

ARP	SSH	SSL	IEEE 802.3	IPv6

14 Файловая подсистема ОС выделяет для файла пространство на диске

секторами	дорожками	кластерами	цилиндрами	байтами

15 Для файла TEST в NTFS утановлены права: Группе -NoAccess, пользователю группы -Change какие действия разрешены данному пользователю над файлом TEST по умолчанию:

Change	Read	Write	FullControl	NoAccess

16 Какой смысл имеет разрешение "выполнить" для каталога TEST в UFS

просмотр содержимого каталога TEST	сменить текущий каталог на каталог TEST	выполнять программы, содержащиеся в каталоге TEST	открыть любой файл, содержащиеся в каталоге TEST	уничтожить каталог TEST

17 Увеличение доступного дискового пространства в UFS позволяет выполнить операция

монтирования	реплицирования	кэширования	резервирования	инкрементирования

18 Сформулируйте гипотезу локальности данных

19 Приведите сетевые ОС с выделенным сервером

NT	UNIX	QNX	NetWare	Windows 2003

20 Распределенные приложения, по сравнению с локальными, обеспечивают:

масштабируемость	отказоустойчи-вость	безопасность	скорость реакции	простоту программирования

21 Укажите операцию, безусловно выполняемую перед входом в систему

авторизации	аутентификации	аккаунтинга	учета	квотирования

22 Совокупность защищенных каналов в публичной сети называется:

VPN	WLAN	VLAN	Intranet	WAN

23 Укажите правильный MAC-адрес

12.45.34.56	ab-89-03-67-g6-04	03:78:EC:21:07:FA	45:90:A3:67	CD.45.AF.12

24 Укажите примерно время, затрачиваемое на передачу содержимого полного CD по сети 100BaseT

1мин.	5 мин.	10 мин	30 мин.	60 мин.

25 Перечислите утилиты UNIX для диагностики сети

26 Перечислите известные Вам службы каталогов

27 Перечислите известные Вам технологии обеспечения сохранности и доступности данных

28 Опишите кратко функционирование механизма прерываний

29 Опишите кратко состав ядра ОС

30 Распишите известные Вам протоколы по уровням модели OSI

L1	L2	L3	L4	L5
L6	L7			

ПРИМЕРЫ ЭКЗАМЕНАЦИОННЫХ ТЕСТОВ

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Дисциплина: "Администрирование информационных систем"

Экзаменационный тест

Факультет МиИ Специальность: 0719 Курс IV

Утверждено на заседании кафедры _____ 2005г. **"Утверждаю":_____ зав. кафедрой ИУС**

Группа: _____ ФИО Студента:_____

1 Укажите место системных утилит в иерархии ПС ВС (после … и перед ...)

2 Перечислите компоненты ядра ОС

3 Укажите ключевое слово, определяющее обслуживающее запросы ПО

1	2	3	4	5
оболочка	сервер	клиент	сервис	услуга

4 Драйвер устройства выполняет функции:

1	2	3	4	5
управления файловой системой	обработки прерывания от устройства	организации прямого доступа к памяти	управления выводом информации	низкого уровня по управлению устройством

5 Синоним хранимого в файле кода:

1	2	3	4	5
программа	процесс	задача	поток	нить

6 Пречислите ресурсы, за которые "борятся" приложения в многозадачной ОС

7 Ядро многозадачной ОС работает в режиме:

1	2	3	4	5
реальном	супервизора	защищенном	прикладном	пользовательском

8 Интерфейс системных вызовов предназначен для обращения к:

1	2	3	4	5
процессору	устройству	пользовательскому процессу	функциям ядра ОС	BIOS

9 Укажите ключевое слово, относящееся к механизму виртуальной памяти:

1	2	3	4	5
Буфер TLB	Кэш-память данных/команд	Регистр CR2	Дескриптор сегмента	Контроллер НЖМД

10	Уражите ключевое слово, относящееся к NTFS				
	1	2	3	4	5
	Распределенная	журнализируемая	кластерная	монтируемая	зеркалируемая

11	Процесс, при прочих равных условиях, будет выполняться быстрее:				
	1	2	3	4	5
	в мультизадачной ОС	в ОС реального времени	в невытесняющей ОС	в однозадачной ОС	в ОС с вытеснением

12	Расставьте номера уровня модели OSI для приведенных протоколов:				
	ARP	SSH	SSL	IEEE 802.3	IPv6

13	Файловая подсистема ОС выделяет для файла пространство на диске				
	1	2	3	4	5
	секторами	дорожками	кластерами	цилиндрами	байтами

14	Для файла TEST в NTFS утановлены права: Группе -NoAccess, пользователю группы -Change какие действия разрешены данному пользователю над файлом TEST по умолчанию:				
	1	2	3	4	5
	Change	Read	Write	FullControl	NoAccess

15	Какой смысл имеет разрешение "выполнить" для каталога TEST в UFS				
	1	2	3	4	5
	просмотр содержимого каталога TEST	сменить текущий каталог на каталог TEST	выполнять программы, содержащиеся в каталоге TEST	открыть любой файл, содержащиеся в каталоге TEST	уничтожить каталог TEST

16	Увеличение доступного дискового пространства в UFS позволяет выполнить операция				
	1	2	3	4	5
	монтирования	реплицирования	кэширования	резервирования	инкременти-рования

17	Приведите сетевые ОС с выделенным сервером				
	1	2	3	4	5
	NT	UNIX	QNX	NetWare	Windows 2003

18	Распределенные приложения, по сравнению с локальными, обеспечивают:				
	1	2	3	4	5
	масштабируемость	отказоустойчи-вость	безопасность	скорость реакции	простоту программирования

19	Укажите операцию, безусловно выполняемую перед входом в систему				
	1	2	3	4	5
	авторизации	аутентификации	аккаунтинга	учета	квотирования

20	Совокупность защищенных каналов в публичной сети называется:				
	1	2	3	4	5
	VPN	WLAN	VLAN	Intranet	WAN

21	Укажите правильный MAC-адрес				
	1	2	3	4	5

	12.45.34.56	ab-89-03-67-g6-04	03:78:EC:21:07:FA	45:90:A3:67	CD.45.AF.12

22 Укажите примерно время, затрачиваемое на передачу содержимого полного CD по сети 100BaseT

	1	2	3	4	5
	1мин.	5 мин.	10 мин	30 мин.	60 мин.

23 Перечислите утилиты UNIX для диагностики сети

24 Перечислите известные Вам службы каталогов

25 Перечислите известные Вам технологии обеспечения сохранности и доступности данных

ПРИМЕРЫ ЭКЗАМЕНАЦИОННЫХ БИЛЕТОВ

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Экзаменационный тест по дисциплине: "Администрирование информационных систем"
Факультет МиИ Специальность 0719
Курс IV
Утверждено на заседании кафедры _____ 2003г. УТВЕРЖДАЮ _____
Зав.кафедрой ИУС

БИЛЕТ N 1

Группа_____ ФИО
Студента_____

| 1) Приведите пример CLI
|

| 2) В чем заключаются преимущества компиляторов перед интерпретаторами
|
|
|

| 3) Расшифруйте понятие механизма защиты:
|
|
|

| 4) Выберете блочное устройство:
| 1.FDD 2.HDD 3.USB 4.AUX 5.LPT

| 5) В командной строке надо вывести число UDP портов, ожидающих подключения
|
|

| 6) Перечислите стадии жизненного цикла процесса
|

| 7) Дайте краткое описание мэйнфрейма:
|
|
|

| 8) В командной строке надо вывести число видимых в сети windows доменов и рабочих групп.
|
|

| 9) Выберете утилиту ОС windows, позволяющую изменить размер кластера NTFS.
| 1.format 2.compact 3.chkdsk 4.convert 5.fdisk

| 10) Какой механизм часто использует windows для выбора драйвера устройства.
| 1.USB 2.Flash 3.PnP 4.DLL 5.DRV

| 11) Приведите пример CUI
|

| 12) Кэш-память процессоров i486 и старше по умолчанию включена в:
| 1.Реальном режиме 2.Защищенном режиме 3.Режиме ввода-вывода
4.В режиме ПДП 5.В режиме отладки

| 13) Драйверы символьных устройств активно используют механизм:
| 1.Страничного преобразования 2.Прямого доступа к памяти 3.Защиты
| 4.Буфферизации 5.Сегментного преобразования

| 14) Выберете название, относящееся к интерфейсам жестких дисков:
| 1.SATA 2.DFS 3.NFS 4.USB 5.CSMA

| 15) Выберете программу, не хранящуюся на жестком диске:
| 1.cmd 2.POST 3.BIOS 4.BASH 5.flash

| 16) Как обычно называется исполняемый файл, содержащий ядро ОС
| 1.core 2.windows 3.linux 4.kernel 5.system

| 17) Механизм прерываний использует:
| 1.Кэширование команд 2.Сегментное преобразвание адреса 3.Прямой доступ к памяти

| 4.Отображение ввода/вывода на память 5.Стек

| 18) Назовите параметр сессии TCP, позволяющий адаптироваться к эффективной полосе пропускания.
|

| 19) Дайте определение архитектуры ВС
|
|
|

| 20) Скомпилированная программа Java содержит последовательность команд в виде
| 1.Объектного кода 2.Ассемблера 3.Байт-кода 4.Кода NRZ 5.Команд языка Си

| 21) Укажите ключевое слово, не относяшееся к многопроцессорным ВС.
| 1.BUS 2.SMP 3.ACPI 4.I/O 5.MMU

| 22) Что такое маршрутизатор
|
|
|

| 23) Что такое сегмент Ethernet
|
|

| 24) Выберете событие, вызывающее прерывание нормальной работы задачи:
| 1.Ловушка 2.Передача управления 3.Инструкция умножения 4.Операция ввода-вывода 5.Включение питания

| 25) Перечислите известные Вам протоколы 2 уровня
|

| 26) Определите состав ИС:
|
|

| 27) Что такое маршрут по умолчанию
|

| 28) В командной строке надо найти в файле TEST.TXT строки с цифрами , но без пробелов
|

| 29) Перечислите известные Вам протоколы аутентификации
|
|

| 30) Что такое реестр windows
|
|
|

| 31) Максимальная емкость ОЗУ = 48Мбайт. Разрядность шины данных=24. Назовите разрядность шины адреса:
|

| 32) Перечислите кратко основные составляющие ядра ОС
|

|
|

| 33) ОЗУ в архитектуре "Общая шина" выполняет роль:
| 1.ROM 2.Арбитра 3.Процессора 4.RAM 5.Коммутатора

| 34) Перечислите известные Вам утилиты работы с файлами windows
|

| 35) В командной строке надо вывести число физических интерфейсов.
|
|

| 36) Удаленный терминал реализует служба:
| 1.ftpd 2.sshd 3.COM 4.TTY 5.PuTTY

| 37) Какую утилиту обычно используют для тьюнинга NTFS
| 1.format 2.cacls 3.regedit 4.chkdsk 5.cmd

| 38) Оптимизация работы устройств ввода/вывода обычно реализуется с помощью:
| 1.Страничного преобразования 2.Сегментного преобразования
3.Случайной выборки 4.Кэширования 5.Хэширования

| 39) Каким расширением обычно снабжаются исполняемые программы windows
|

| 40) В командной строке надо вывести число файлов текущего каталога с расширением
.TXT
|
|