

Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Московский авиационный институт»
(национальный исследовательский университет)»

Факультет прикладной математики и физики

Курсовая работа по информатике на тему:

«Схема лабораторной сети»

Работу выполнил
студент I курса
очного отделения
группы М80-107Б
Лихарев С.С.

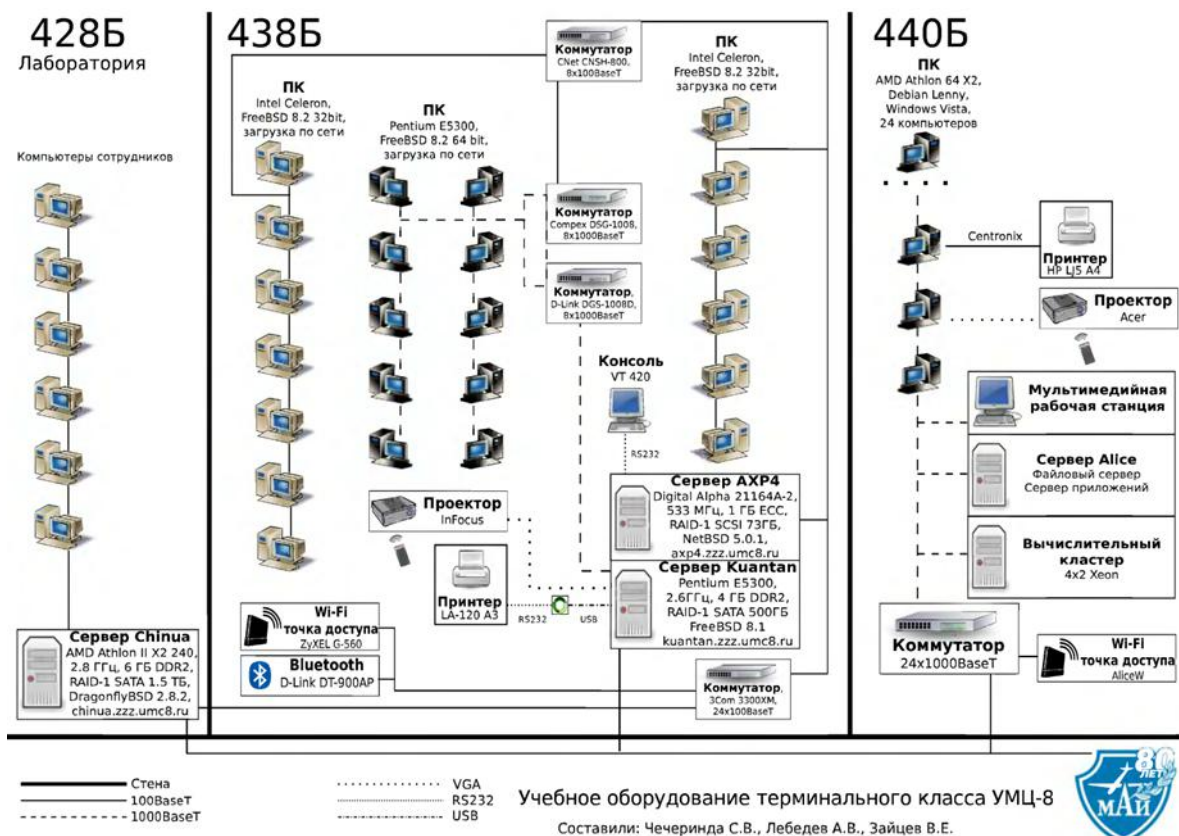
Преподаватель:
Ридли М.К.

Дата сдачи:

«___»_____200__г.

Москва 2016

1. Схема лабораторной сети.



В аудитории находятся:

1. 25 ЭВМ (13 компьютеров на базе Intel Celeron, 10 компьютеров на Intel Pentium E5300 и 2 серверные машины — АХР4 и Kuantan)
2. 4 коммутатора (CNet, Comrex, D-Link и 3com), соединяющие все компьютеры аудитории в единую сеть.
3. Принтер LA-120 A3, с помощью которого студенты распечатывают протоколы своих лабораторных работ. Для этого используется утилита proto, которую необходимо запускать с серверной машины (axp4 или kuantan), предварительно подключившись к ним по ssh.
4. Проектор InFocus.
5. WiFi- и bluetooth- точки доступа (ZyXel и D-Link).
6. Консоль VT420.

2. Основные устройства

Сервера AXP4 и Kuantan.

Сервером называется компьютер, выделенный из группы персональных (или рабочих станций) для выполнения какой-либо сервисной задачи без непосредственного участия человека. Сервер и рабочая станция могут иметь одинаковую аппаратную конфигурацию, так как различаются лишь по участию в своей работе человека за консоль.

1. Сервер AXP4

Процессор: Digital Alpha 21164A-2, 533 МГц
Память: 1Гб ECC
RAID-1 SCSI 73Гб
Адрес: axp4.zzz.umc8.ru

DEC Alpha (также известный как Alpha AXP) — 64-разрядный RISC (компьютер с сокращённым набором команд) микропроцессор, первоначально разработанный и произведённый компанией DEC, которая использовала его в собственной линейке рабочих станций и серверов.

Микропроцессор был создан для компьютеров, которые планировались на смену серии VAX и изначально поддерживался операционными системами VMS и DEC OSF/ 1. AXP (в 1995 переименована в Digital UNIX, после покупки DEC компанией Compaq переименована в Tru64 UNIX). Позднее на него были перенесены свободные операционные системы GNU/Linux и BSD UNIX. Компания Microsoft производила Windows NT с поддержкой Alpha до версии Windows NT 4.0 SP6, однако поддержка была свёрнута после выпуска Windows 2000 Release Candidate 2.

Digital Alpha 21164A-2:

Процессор Alpha 21164 (EV5) стал доступен в 1995 году и работал на частотах до 333 МГц. В июле 1996 частота была доведена до 500 МГц, а в марте 1998 — до 666 МГц. Кроме того, в 1998 году был выпущен 21264 (EV6), первоначальная тактовая частота которого составляла 450 МГц; со временем она возросла до 1,25 ГГц (это было сделано в моделях 2001 года 21264C/EV68CB).

Alpha 21164 - это процессор с суперскалярной архитектурой, способный обрабатывать до четырех инструкций за цикл. Он объединяет в себе кэш данных и кэш команд первого уровня, а также высокопроизводительную и объемную кэш-память второго уровня. Микропроцессор 21164 использует скоростной 128-битовый интерфейс для доступа к памяти, а также имеет возможность подключения кэша третьего уровня.

Alpha 21164 состоит из пяти независимых функциональных блоков:

1. блок выборки, декодирования инструкций и предсказания ветвлений;
2. блок обработки целочисленных данных;
3. блок управления памятью;
4. блок шинного интерфейса и управления кэш-памятью;
5. блок обработки данных с плавающей запятой.

2.Сервер Kuantan

Процессор: Pentium E5300

Память: 4Гб DDR2

RAID-1 SATA 500Гб

Адрес: kuantan.zzz.umc8.ru

Технические характеристики процессора:

Производитель: Intel

Модель: Pentium Dual-Core Processor E5300

Частота работы процессора: 2.6 ГГц

Поддерживаются дополнительные наборы инструкций: SSE, SSE2, SSE3, поддерживается технология EVP (Enhanced Virus Protection или Execute Disable Bit)

Корпус: FC-LGA6

Частота шины CPU: 800 МГц

Ядро: Wolfdale

Рассеиваемая мощность: 65 Вт

Критическая температура: 74.1 °C

Технология: 0.045 мкм

Кэш L1: 64 Кб x2

Кэш L2: 2048 Кб

Количество ядер: 2

Умножение: 13

Гнездо процессора: Socket LGA775

Технологии уменьшения шума охлаждающей системы: Enhanced Halt State (C1E),

Enhanced Intel Speedstep

Напряжение питания: 0.85 ~ 1.3625В

Сетевые коммуникаторы.

Сетевой коммутатор или свитч (от англ. switch - переключатель) - устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента. Коммутатор передаёт данные только непосредственно получателю. Это повышает

производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Благодаря тому, что коммутаторы могут управлять трафиком на основе протокола канального уровня (Уровня 2) модели OSI, он в состоянии контролировать MAC адреса подключенных к нему устройств и даже обеспечивать трансляцию пакетов из стандарта в стандарт (например Ethernet в FDDI и обратно). Особенно удачно результаты этой возможности представлены в коммутаторах Уровня 3, т.е. устройствах, возможности которых приближаются к возможностям маршрутизаторов.

В лабораторном классе (ауд.438Б) находятся четыре коммутатора:

Зcom 3300XM



Характеристики:

Есть возможность установки в стойку.

24 порта коммутатора Ethernet 10/100 Мбит/сек.

Есть поддержка работы в стеке, Web-интерфейс.

Поддержка стандартов: Auto MDI/MDIX, IEEE 802.1p (Priority tags), IEEE 802.1q (VLAN)

Буфер 128 Кб

Индикаторы Power, Link/Act, 1000Mbps, 100Mbps

Внешний блок питания

Метод доступа CSMA/CD

MAC Address Table 4K адресов

Потребление энергии 10,5 ватт

Размеры (Ш x В x Г) 190 x 38 x 120 мм

Рабочая температура 0 ~ 40°C

CNet CNSH-800



Характеристики:

8 портов 10/100 Мбит/сек. RJ-45

Полнодуплексный или полудуплексный режим обмена данными

Размер буфера 128 КБ

Количество MAC адресов 1К

Сетевые стандарты: IEEE 802.3, IEEE 802.3u

Индикаторы: Power и для каждого порта: Link/Act

Внешний блок питания

Размеры (ШхГхВ) 145 x 85 x 27 мм

Comrex DSG-1008



Характеристики:

8-портовый коммутатор.

Скорость передачи данных 10/100/1000 Мбит/сек.

Буфер 128 КБ

Индикаторы Power, Link/Act, 1000Mbps, 100Mbps

Внешний блок питания

Метод доступа CSMA/CD

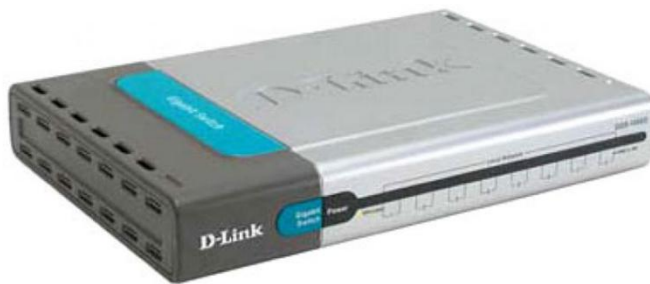
MAC Address Table 4K адресов

Потребление энергии 10,5 ватт

Размеры (Ш x В x Г) 190 x 38 x 120 мм

Рабочая температура 0 ~ 40° C

D-link DGS-1008D



Характеристики:

8-и портовый коммутатор

Скорость передачи данных 10/100/1000 Мбит/сек

Буфер 144 Кб на устройство

Индикаторы Link/ACT, Power

Внешний блок питания

Поддержка стандартов Auto MDI/MDIX

Пропускная способность 16 Гбит/с

Метод коммутации Store-and-forward

Метод доступа CSMA/CD

MAC Address Table 8000 адресов

Максимальное потребление энергии 11 Вт

Размеры (Ш x В x Г) 235 x 36 x 162 мм

Рабочая температура 0 ~ 40°C

3. Программное обеспечение.

На ЭВМ кабинета 438Б установлены операционные системы семейства UNIX, основанные на Berkeley Software Distribution (BSD).

BSD — система распространения программного обеспечения в исходных кодах, созданная для обмена опытом между учебными заведениями. Особенностью пакетов ПО BSD была специальная лицензия BSD, которую кратко можно охарактеризовать так: весь исходный код — собственность BSD, все правки — собственность их авторов.

В данный момент термин BSD чаще всего употребляется как синоним BSD-UNIX общего названия вариантов UNIX, восходящих к дистрибутивам университета Беркли.

К семейству BSD относятся: NetBSD, FreeBSD, OpenBSD, ClosedBSD, MirBSD, DragonFly BSD, PC-BSD, DesktopBSD, SunOS, TrueBSD, Frenzy, Ultrix.

Отличия от «классической» системы UNIX состоят в отсутствии переключения уровней выполнения, системе печати, файловой системе и командного процессора.

Пользовательские команды практически идентичны.

В нашем случае, в аудитории используются два дистрибутива:

1. FreeBSD — свободная Unix -подобная операционная система. Потомок AT&T Unix по линии BSD. FreeBSD работает на PC-

совместимых системах семейства x86, включая Microsoft Xbox, а также на DEC Alpha, Sun UltraSPARC, IA-64, AMD64, PowerPC, NEC PC-98, ARM. Готовится поддержка архитектуры MIPS.

FreeBSD разрабатывается как целостная операционная система. Исходный код ядра, драйверов устройств и базовых пользовательских программ (т. н. userland), таких как командные оболочки и т. п., содержится в одном дереве системы управления версиями. Это отличает FreeBSD от GNU/Linux — другой свободной UNIX-подобной операционной системы, — в которой ядро разрабатывается одной группой разработчиков, а набор пользовательских программ — другими (например, проект GNU), а многочисленные группы собирают это всё в единое целое и выпускают в виде различных дистрибутивов Linux.

FreeBSD хорошо зарекомендовала себя как система для построения интранет- и интернет-серверов. Она предоставляет достаточно надёжные сетевые службы и эффективное управление памятью.

Помимо своей стабильности, FreeBSD популярна и благодаря своей лицензии, которая существенно отличается от широко известной лицензии GNU. В отличие от GNU LGPL, которая тоже позволяет использовать свободный код в закрытой программе, лицензия BSD более простая и короткая.

2. NetBSD — свободно распространяемая, защищенная, кросс-платформенная операционная система. Похожа на UNIX, но таковой не является. Первая официальная версия NetBSD — 0.8 — была выпущена в апреле 1993 года. NetBSD происходит из систем 4.3BSD и 386BSD. В конце 1995 года от NetBSD отделился проект OpenBSD. Текущая версия — NetBSD 5.1 — выпущена 19 ноября 2010 года. NetBSD портирована на огромное количество компьютерных архитектур.

Поддерживаются 53 аппаратные платформы (существуют 57 портов, включая последний официальный выпуск и мгновенные копии). Компиляция пакетов происходит из одного дерева исходных кодов, поэтому новые функции в машинно-независимых частях появляются сразу для всех платформ без необходимости адаптации. Разработка драйверов также машинно-независима, поэтому один драйвер для карты, работающей на шине PCI, будет работать на платформах i386, Alpha, PowerPC, SPARC и других, поддерживающих шину PCI. Такая платформенезависимость позволяет разрабатывать встраиваемые системы с помощью целого набора инструментов: компиляторов, отладчиков и других инструментов, поддерживающих кросс-компиляцию.

4. Термины

DNS (Domain Name System — система доменных имён) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись). Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу. Основой DNS является представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Начиная с 2010 года в систему DNS внедряются средства проверки целостности передаваемых данных, называемые DNS Security Extensions (DNSSEC). Передаваемые данные не шифруются, но их достоверность проверяется криптографическими способами. Внедряемый стандарт DANE обеспечивает передачу средствами DNS достоверной криптографической информации (сертификатов), используемых для установления безопасных и защищённых соединений транспортного и прикладного уровней.

DNS обладает следующими характеристиками:

Распределённость администрирования. Ответственность за разные части иерархической структуры несут разные люди или организации.

Распределённость хранения информации. Каждый узел сети в обязательном порядке должен хранить только те данные, которые входят в его зону ответственности, и (возможно) адреса корневых DNS-серверов.

Кеширование информации. Узел может хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.

Иерархическая структура, в которой все узлы объединены в дерево, и каждый узел может или самостоятельно определять работу нижестоящих узлов, или делегировать (передавать) их другим узлам.

Резервирование. За хранение и обслуживание своих узлов (зон) отвечают (обычно) несколько серверов, разделённые как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

DNS важна для работы Интернета, так как для соединения с узлом необходима информация о его IP-адресе, а для людей проще запоминать буквенные (обычно осмысленные) адреса, чем последовательность цифр IP-адреса. В некоторых случаях это позволяет использовать виртуальные серверы, например, HTTP-серверы, различая их по имени запроса. Первоначально

преобразование между доменными и IP-адресами производилось с использованием специального текстового файла `hosts`, который составлялся централизованно и автоматически рассылался на каждую из машин в своей локальной сети. С ростом Сети возникла необходимость в эффективном, автоматизированном механизме, которым и стала DNS.

NAT (Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

Существует 3 базовых концепции трансляции адресов:

Статический NAT — Отображение незарегистрированного IP-адреса на зарегистрированный IP-адрес на основании один к одному. Особенно полезно, когда устройство должно быть доступным снаружи сети.

Динамический NAT — Отображает незарегистрированный IP-адрес на зарегистрированный адрес от группы зарегистрированных IP-адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированным и зарегистрированным адресом, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.

Перегруженный NAT — форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты. Известен также как PAT (Port Address Translation). При перегрузке каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта.

NAT выполняет три важных функции.

1. Позволяет сэкономить IP-адреса (только в случае использования NAT в режиме PAT), транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 публичный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с приватными (внутренними) IP-адресами.

2. Позволяет предотвратить или ограничить обращение снаружи к внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует, они не пропускаются.

3. Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов. По сути, выполняется та же указанная выше трансляция на определённый порт, но возможно подменить внутренний порт официально зарегистрированной службы (например, 80-й порт TCP (HTTP-сервер) на внешний 54055-й). Тем самым, снаружи, на внешнем IP-адресе после трансляции адресов на сайт (или форум) для осведомлённых посетителей можно будет попасть по адресу `http://example.org:54055`, но на внутреннем сервере, находящемся за NAT, он будет работать на обычном 80-м порту. Повышение безопасности и скрытие «непубличных» ресурсов.

NIS (Network Information Service, Информационная служба сети) — это клиент-серверный протокол, созданный Sun Microsystems, который позволяет обеспечивать доступ к системной конфигурации по всей сети. Первоначально назывался Yellow Pages (Жёлтые страницы) по аналогии с бумажным справочником, в котором перечисляются телефонные номера, но, из-за судебных преследований владельцами торговой марки, был переименован в NIS.

В NIS первых версий присутствовала существенная уязвимость — все данные, включая пароли пользователей, передавались открытым текстом, из-за чего злоумышленник мог получить учетные записи практически ко всей локальной сети из интернета.

Kerberos - сетевой протокол аутентификации, позволяющий передавать данные через незащищённые сети для безопасной идентификации. Он ориентирован в первую очередь на клиент-серверную модель и обеспечивает взаимную аутентификацию — оба пользователя через сервер подтверждают личности друг друга.

Распространение реализации Kerberos происходит в рамках авторского права аналогичного правам для BSD.

В настоящее время множество ОС поддерживают данный протокол, в число которых входят:

Windows 2000 и более поздние версии, которые используют Kerberos как метод аутентификации в домене между участниками. Некоторые дополнения к этому протоколу отражены в RFC 3244 "Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols". Документ RFC 4757 описывает использование RC4 Kerberos в Windows

Различные UNIX и UNIX подобные ОС (Apple Mac OS X, Red Hat Enterprise Linux 4, FreeBSD, Solaris, AIX, OpenVMS).

5. Заключение

В лабораторном классе 438Б находятся два сервера, четыре коммутатора, десять компьютеров Pentium E5300 и тринадцать Intel Celeron, проектор inFocus, Wi-Fi и Bluetooth точки доступа, принтер,

поддерживающий печать формата А3, текстовый терминал VT420. Хотя оборудование класса достаточно старое, оно полностью пригодно для выполнения лабораторных и курсовых работ. Также на всех ЭВМ, кроме сервера АХР4, используется операционная система FreeBSD.