

# Конфигурирование компьютерных сетей

# Управление сетевыми параметрами (настройками)

Сетевые параметры:

- o IP-адреса
- o Маски интерфейсов
- o Маршруты по умолчанию
- o DNS-серверы
- o WINS-серверы
- o Proxu-серверы
- o И т.п.

# Управление сетевыми параметрами

Два подхода:

- o Ручная настройка
- o Автоматизированная настройка
  - o Протокол RARP
  - o Протокол BOOTP
  - o Протокол DHCP

# Автоматизированная настройка параметров. Протоколы RARP и BOOTP

## o **Протокол RARP**

- o RFC 903
- o Использует RARP-сервер
- o Используется только для получения IP-адреса

## o **Протокол BOOTP**

- o RFC 951, 1533, 1542
- o Использует BOOTP-сервер
- o Способен получать:
  - o IP-адрес
  - o Маску сети
  - o Маршрутизатор «по умолчанию»
- o Может использовать цепочку ретрансляторов
- o BOOTP-сервер содержит статическую таблицу соответствий MAC-адресов и параметров узла

# Автоматизированная настройка параметров. Протокол DHCP

- o Разработан Microsoft
- o RFC 2131, 2132
- o Является расширением BOOTP
  - o Информация размещается в поле опций BOOTP
- o Поддерживает 3 режима:
  - o Ручное распределение
  - o Автоматическое распределение
  - o Динамическое распределение

# Автоматизированная настройка параметров. Протокол DHCP

Типы опций:

- o Базовые параметры
  - o Маска сети
  - o Default gateway
  - o DNS
  - o HostName
  - o DomainName
- o Параметры узла
  - o IP forwarding
  - o Default TTL
  - o и т.п
- o Параметры интерфейсов
  - o MTU
  - o Broadcast
  - o Static routes



# Автоматизированная настройка параметров. Протокол DHCP

- o Параметры TCP
  - o TCP Default TTL
  - o KeepAlive time
  - o и т.п
- o Параметры приложений
  - o NIS, NIS+
  - o Wins
  - o POP3, SMTP, NNTP
  - o и т.п.
- o Параметры аренды
  - o Запрашиваемый IP
  - o Срок аренды
  - o Идентификатор сервера
  - o и т.п.

# Контроль сетевых параметров

- o Контроль сетевых интерфейсов
  - o ifconfig
  - o ipconfig
  - o netsh
- o Контроль маршрутизации
  - o route
  - o iproute2
- o Контроль сетевых соединений и сокетов
  - o netstat



# Контроль сетевых параметров

- o Контроль преобразования адресов
  - o arp
- o Контроль сетевой среды
  - o ping
  - o traceroute
- o Контроль и проверка DNS
  - o nslookup
  - o host
  - o dig

# Анализ компьютерных сетей

- o Сетевые анализаторы
  - o Аппаратные анализаторы
  - o Программные анализаторы (анализаторы протоколов)
    - o tcpdump
    - o MS Network Monitor
    - o WinDump
    - o Ethereal
    - o WireShark
    - o и т.п.

# Анализаторы протоколов

- o Два типа фильтрации:
  - o фильтры захвата (capture filters)
  - o фильтры отображения (view filters)
- o Фильтрация по
  - o типам кадров канального уровня
  - o протоколу сетевого уровня
  - o адресам канального уровня
  - o сетевому адресу источника
  - o сетевому адресу приемника
  - o по протоколу транспортного уровня
  - o по флагам протоколов
  - o по длине пакета

# Управление доставкой

- o Маршрутизация
- o Шлюзы уровня приложений (ALG)
  - o Серверы посредники
  - o Трансляторы протоколов
    - o Стандартные трансляторы (SOCKS)
    - o Специализированные трансляторы
- o Трансляция адресов (NAT)

# Серверы-посредники (прокси-серверы)

- o Основная идея – использовать посредников (проxy) для получения информации из Internet
- o Решаемые задачи:
  - o Кэширование информации
  - o Соккрытие внутренней части сети
  - o Сокращение времени доступа в сеть
- o Используют протоколы HTTP и FTP
- o Для доступа к серверу-посреднику обычно используется HTTP

# Серверы-посредники (проху-серверы)

- o Проху-серверы для протокола FTP
  - o HTTP-проху для FTP
    - o Используется протокол HTTP для доступа к проху-серверу
    - o Адрес FTP-сервера указывается в строке URL:  
<ftp://ftp.example.com>
    - o Требуется специального клиента
  - o FTP-проху – серверы
    - o Используется протокол FTP для доступа к проху-серверу
    - o Адрес FTP-сервера указывается в строке аутентификационных командах (USER или PASS)
    - o Не требует модификации клиента



# Серверы-посредники

- o Обычно используют протокол доступа HTTP
- o Используемые порты TCP:
  - o 3128
  - o 8080
  - o 80
  - o 8000
- o Программные пакеты
  - o squid
  - o Microsoft Forefront Threat Management Gateway
    - o Ранее – MS ISA Server, MS Proxy Server
  - o ...

# Серверы-посредники (проху-серверы)

- o Иерархии кэшей:
  - o Два типа отношений:
    - o Родительские/дочерние (parent)
    - o Родственные (sibling)
  - o Сокращение трафика
  - o Сокращение времени
  - o Ограничение на уровень иерархии

# Серверы-посредники. Синхронизация кэшей

- o Синхронизация кэшей
  - o Протокол ICP (Internet Cache Protocol)
    - o RFC 2186 и RFC2187 (ICPv2)
    - o Использует UDP, порт 3130

# Протокол SOCKS

- o Используются версии SOCKS 4 и SOCKS 5
- o Последняя действующая версия SOCKS 5
- o SOCK 5 описан в RFC 1928, RFC 1929
- o Основная цель – обеспечить локальным неанонсированным сетям доступ к Internet
- o Требуется специальных SOCKS-совместимых приложений (перекомпиляция)
- o Используется клиент-серверный механизм запросов услуг
- o Обеспечивается контроль доступа

# Протокол SOCKS

- o Предусмотрено два вида команд:
  - o Connect (TCP)
  - o Bind (TCP)
- o Используется транспорт TCP, порт 1080
- o Отличия SOCKS 5
  - o Наличие аутентификации
  - o Поддержка протокола UDP
    - o Associate (UDP)

# Трансляция адресов (NAT)

- o Описана в стандартах: RFC 1631, 2663
- o Основное отличие – «прозрачность» технологии для приложений
- o Основная идея – «вклиниться» между участниками соединения
- o Используется в неанонсированных сетях
- o Защищает клиентские станции от внешних сетей
- o Поддерживаемые протоколы
  - o TCP
  - o UDP
  - o ICMP



# Трансляция адресов (NAT)

- o Для транспортных протоколов выделяются ассоциированные порты, имитирующие участников соединения
- o Передача данных между ассоциированными портами происходит с помощью ПО
- o NAT могут использовать все протоколы, не требующие явной адресации клиента NAT
- o Не могут использовать NAT:
  - o FTP в активном режиме
  - o SNMP-trap
  - o И т.п.

# Transparent proxy

- o Идея – соединить достоинства NAT и Proxy:
  - o Кэширование
  - o Прозрачность для клиентского ПО
  - o Защищенность клиентского ПО
- o Реализуется на двух или одном сервере
- o Ограничения:
  - o Без модификации можно использовать только для HTTP-трафика
  - o Необходимо явно задавать все транслируемые порты
  - o Для других типов трафика (FTP) требуется ALG

# Туннелирование

- o Основные решаемые задачи:
  - o Доставка информации через альтернативную сетевую среду
  - o \* Маршрутизация
  - o Защита информации
- o Три протокола:
  - o Несущий протокол («подложка» туннеля)
  - o Туннельный протокол
  - o Переносимый протокол

# Туннелирование

- o Туннельные протоколы:
  - o GRE IP
  - o L2F
  - o PPTP
  - o L2TP
  - o Туннелирование «IP-IP»
  - o ...
- o Современное применение туннелирования:
  - o Объединение IP4-IP6
  - o Защита информации (VPN)