Конфигурирование компьютерных сетей

КСПТ
КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ПРОГРАММНЫЕ ТЕХНОЛОГИИ

ФТК

Управление сетевыми параметрами (настройками)

Сетевые параметры:

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

Управление сетевыми параметрами

Два подхода:

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

Автоматизированная настройка параметров. Протоколы RARP и BOOTP

- **Протокол RARP**
  - RFC 903
  - Использует RARP-сервер
  - Используется только для получения IP-адреса
- **Протокол BOOTP**
  - RFC 951, 1533, 1542
  - Использует BOOTP-сервер
  - Способен получать:
    - IP-адрес
    - Маску сети
    - Маршрутизатор «по умолчанию»
  - Может использовать цепочку ретрансляторов
  - BOOTP-сервер содержит статическую таблицу соответствий MAC-адресов и параметров узла

Автоматизированная настройка параметров. Протокол DHCP

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

Автоматизированная настройка параметров. Протокол DHCP

Типы опций:

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

Автоматизированная настройка параметров. Протокол DHCP

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

Контроль сетевых параметров

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

Контроль сетевых параметров

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

Анализ компьютерных сетей

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

Анализаторы протоколов

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

Управление доставкой

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

Серверы-посредники (proxy-серверы)

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

Серверы-посредники (proxy-серверы)

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

Серверы-посредники

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

Серверы-посредники (proxy-серверы)

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

Серверы-посредники. Синхронизация кэшей

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

Протокол SOCKS

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

Протокол SOCKS

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

Трансляция адресов (NAT)

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

Трансляция адресов (NAT)

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

Transparent proxy

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

Туннелирование

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

Туннелирование

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