ОНЛАЙН-ОБРАЗОВАНИЕ

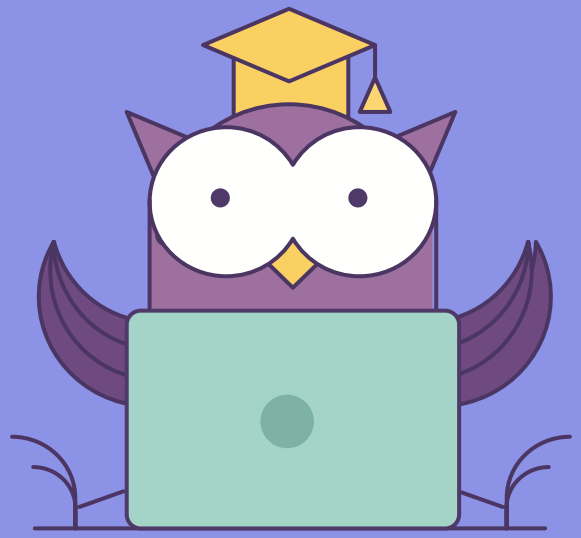
OTUS

Сетевая подсистема

Windows

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

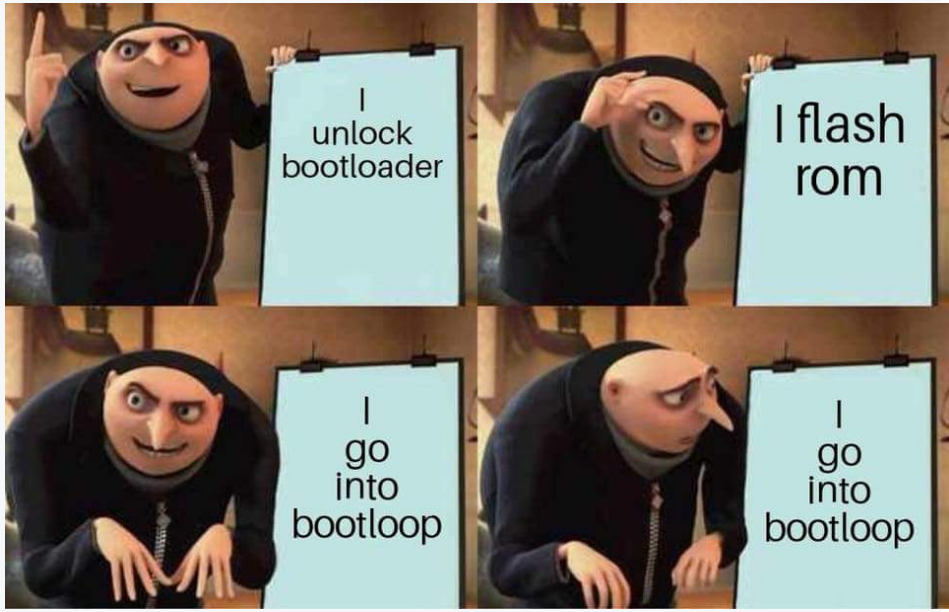
- **Основные элементы сетевой подсистемы**
  - Еще раз про модель OSI
  - Проекция подсистем на модель OSI
  - Состав сетевого API
- **Сетевые протоколы Windows**
  - LLMNR
  - Net-BIOS
  - SMB
- **Active Directory**
  - Структура и состав
  - Сервисы

Цель занятия

1. Рассмотреть архитектуру сетевой подсистемы

2. Научиться получать информацию о состоянии подсистемы

3. Закрепить полученные навыки на практике



Ответы на вопросы

00

DNS Spoofing

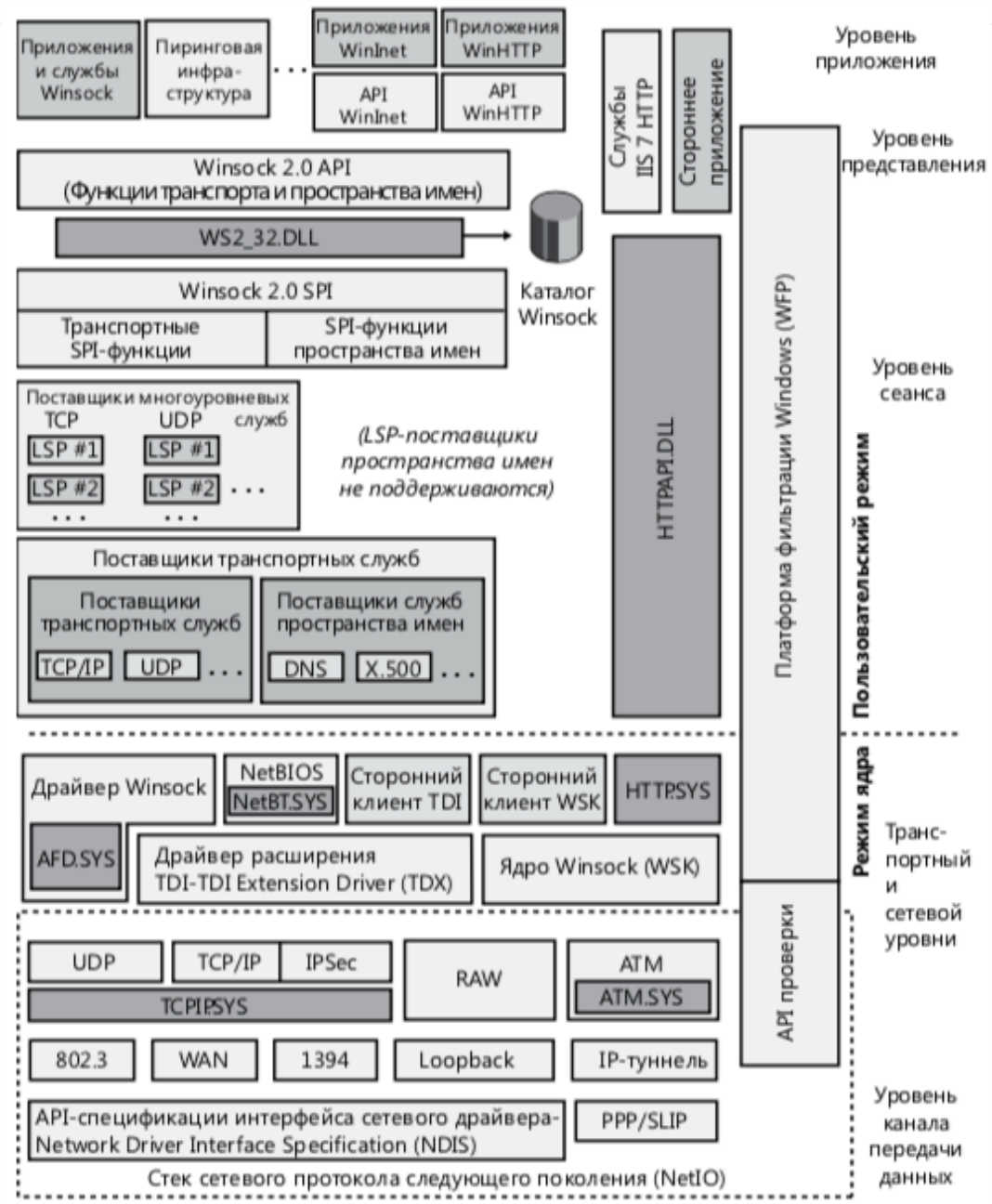
01

Элементы сетевой подсистемы

Модель OSI

Теоретическая модель

Проекция OSI на структуру Windows



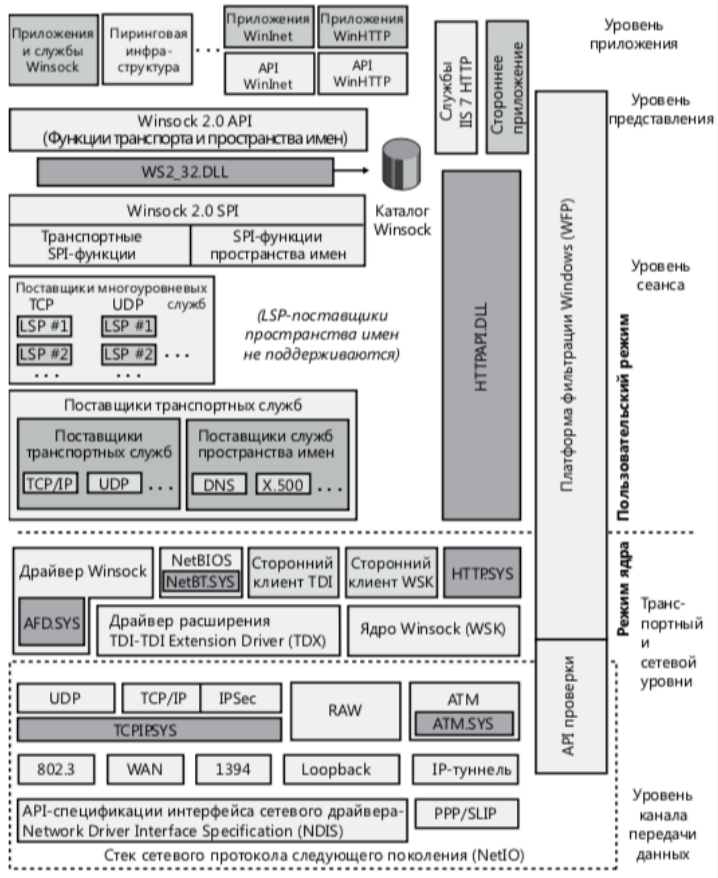
Особенность реализации

Основные:

1. Один уровень может быть растянут на несколько компонентов

2. Нет четкой границы где начинается один компонент и заканчивается другой

3. Все компоненты разнесены на пользовательскую часть и ядерную



Описание компонентов

Сетевые API интерфейсы - независимо от протокола предоставляют приложениям способ обмениваться по сети информацией.

Winsock Kernel(WSK) - часть API интерфейса, которая работает в режиме ядра.

Network Driver Interface Specification (NDIS) - драйверы протокола, при необходимости отправки информации по сети, добавляют в данные специфичные для протокола данные. Так же эта часть отвечает за фрагментацию, пересборку и повторную отправку.

Windows Filtering Platform (WFP) - плаформа фильтрации Windows. Предоставляет набор функций для написания фильтрующих программ.

Из чего состоит сетевое API

Windows Socket - объект, который состоит из адреса хоста и порта, на котором он будет получать/отправлять информацию по сети

> **Отличия от сокетов BSD/Linux:** есть функции которые за одну итерацию делают несколько действий. Например: коннект и прием первого пакета.

Ядро **Winsock** - интерфейс основанный на сокетах.

Удаленный вызов процедур **RPC** - стандарт сетевого программирования. Использует именованные каналы. Скрывает от программиста настройку и работу с сетью.

API интерфейсы доступа к Интернету - набор функций и механизмов, которые используются для взаимодействия с серверами, посредством выбранного протокола, например HTTP.

Именованные каналы и почтовые слоты - API интерфейсы, которые используются для обмена данными между процессами.

> **Особенности:**
>
> - Именованные каналы - надежная двунаправленная связь
> - Почтовые слоты используются для ненадежной связи

NetBIOS - интерфейс программирования основной системы сетевого ввода-вывода. Используется для поддержки старых приложений.

01

Просмотр службы Winsock, named pipes

Инструкции

Просмотр Winsock:

1. Открыть командную строку cmd.exe
2. Ввести команду netsh winsock show catalog

Просмотр списка именованных каналов:

1. Открыть командую строку cmd.exe
2. Ввести команду pipelist

Просмотр NetBIOS имен:

1. Открыть командую строку cmd.exe
2. Ввести команду nbtstat -n

02

Просмотр объектов устройтв TCP/IP

Инструкции

Просмотр объектов устройств:

1. !drvobj tdx
2. !devobj 0x00000

Просмотр списка мини-портов:

1. .load ndiskd
2. !miniports
3. !miniport 0x0000000

02

Сетевые протоколы Windows

Сетевые протоколы Windows

LLMNR (Link Local Multicast Network Resolution) - протокол основанный на DNS формате запроса. Позволяет производить поиск и резолв адресов хостов в сети.

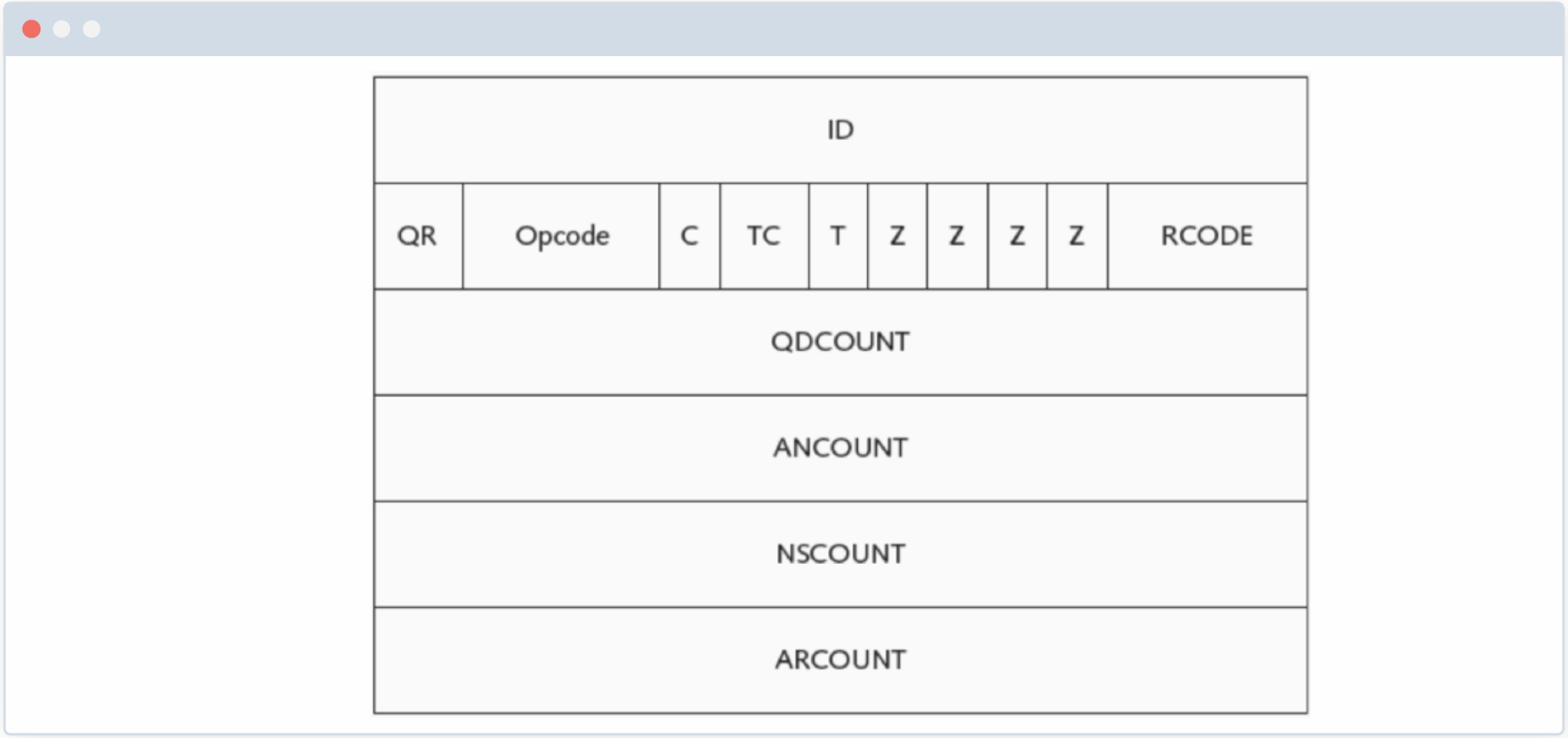
Net-BIOS - не протокол сетевого взаимодействия. Это API, который предоставляет возможность пересылки данными между хостами в локальной сети.

SMB (Server Message Block) - протокол который предоставляет общий доступ к файлам по сети

Заголовок LLMNR

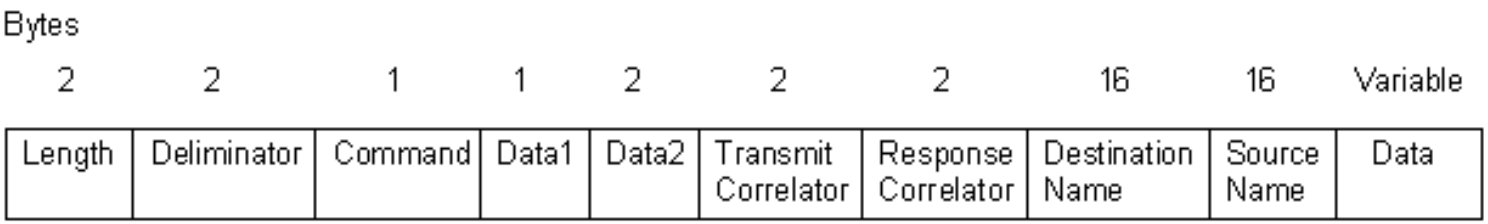
Работает на порту 5355 протоколы UDP/TCP

Описание параметров в заголовке.



Net-BIOS заголовок

NetBIOS frame in LLC



Заголовок SMB

8	16	24	32 bits
Command	**RCLS**	**Reserved**	**ERR**
ERR (cont)	**REB/FLG**	**Reserved**	
Reserved			
Reserved			
Reserved			
Tree ID		**Process ID**	
User ID		**Multiplex ID**	
WCT	**VWV**		
BCC		**BUF**	

SMB header structure

03

Создание и отправка пакетов протоколов Windows

03

Active Directory

Active Directory

OTUS

- Иерархическая структура, которая хранит в себе информацию об объектах, которые доступны в сети.

- Основная единица управления - объект:
  - Принтер
  - Директория с файлами
  - Сервер
  - Аккаунт пользователя
  - Доступ к сети
- Основные понятия **AD**:
  - **Scheme**
  - **Global Catalog**
  - **Query and index mechanism**
  - **Replication service**

- **Scheme(Схема)** - набор правил, который определяет характеристики объектов.

- **Global Catalog** - хранилище, которое хранит информацию по всем объектам, которые определены в AD.

- **Query and index mechanism** - предоставляет возможность производить поиск по параметрам и типам объектов.

- **Replication Service** - механизм, который распространяет информацию об объектах в рамках сети.

Структурные Объекты

- **Сервер** - хост в сети, который выполняет роли в домене
- **Контроллер домена** - сервер, который хранит каталог и, который обслуживает запросы пользователей к каталогу.
- **Домен** - иерархическая структурная единица AD
- **Дерево доменов** - иерархическая система доменов, которая имеет единый корень
- **Лес доменов** - множество деревьев доменов, находящихся в различных формах доверия

Административные Объекты

- **Сервер** - хост в сети, который выполняет роли в домене
- **Контроллер домена** - сервер, который хранит каталог и, который обслуживает запросы пользователей к каталогу.
- **Домен** - иерархическая структурная единица AD
- **Дерево доменов** - иерархическая система доменов, которая имеет единый корень
- **Лес доменов** - множество деревьев доменов, находящихся в различных формах доверия

04

Active Directory Lab

Александр Колесников

Спасибо
за внимание!