

Стек протоколов - иерархическая организованый набор протоколов достаточный для организации взаимодействия узлов сети.

Уровни стека протоколов:

TCP/IP	OSI
Прикладной (HTTP, Telnet, SNMP, SMTP, FTP)	Прикладной Представительский
Транспортный (TCP, UDP)	Сеансовый Транспортный
Межсетевого взаимодействия (IP, ICMP, ARP)	Сетевой
Сетевой интерфейс (Ethernet, x25, PPP)	Канальный Физический

TCP - передача данных пакетами.

UDP - передача данных дейтаграммами.

IP - протокол задающий маршрутизацию.

ARP - переводит IP адрес в MAC адрес.

Проблемы безопасности:

1. на **транспортном** уровне:
2. Ресурсоёмкость TCP - основа для DDOS атаки
3. Нет контроля целостности и конфиденциальности данных
4. на **сетевом** уровне (IP):
5. Не обеспечивает надёжную идентификацию отправителя и получателя
6. Не защищает данные от перехвата
7. Не контролирует целостность данных
8. Отправитель и получатель не контролируют маршрут

Логические и физические соединения между уровнями стека TCP/IP

Хост 1	Хост 2
Прикладной: сообщение	Прикладной
Транспортный	Транспортный
Межсетевого взаимодействия	Межсетевого взаимодействия
Сетевой интерфейс	Сетевой интерфейс

Классификация атак:

1. Нарушение конфиденциальности
2. Нарушение целостности
3. Отказ от обслуживания

Этапы сетевой атаки:

1. Сбор информации
 1. Изучение сетевой топологии
 2. Доступные сетевые сервисы
2. Выявление уязвимы мест атакуемой системы - анализ ПО, его настройки
3. Реализация выбранной атаки

Маска сети позволяет определить, где кончается локальная сеть и начинается глобальная сеть.