Что такое OSI model?

OSI model — это **7-уровневая модель**, описывающая, как данные передаются по сети шаг за шагом.

Её определила **ISO** в 1984 году. Она даёт каждому устройству и инженеру **общий «язык».**



ПОЧЕМУ ЭТО ВАЖНО

Общий язык



Вендоры, инструменты и инженеры описывают сети **одинаково**.

Карта для troubleshooting



Когда что-то ломается, вы **точно знаете**, на каком уровне проблема.

Лестница для обучения



Изучайте **по одному уровню**, а не всю сеть сразу.

Модульность



Каждый уровень работает **независимо**: меняй один — остальные не ломаются.



Коротко:

OSI model — это модель для **понимания**.
Интернет работает на более простой,
но реальной **TCP/IP** модели,
о которой мы поговорим на слайде **12**.

Physical



Преобразует данные в **electrical**, **light** или **radio signals** и передаёт их по **physical medium**.

PROTOCOL DATA UNIT	ITS JOB
Bits	**Raw 1s and 0s**

ЧТО ОН ДЕЛАЕТ

Определяет **cables**, **connectors**, **voltages** и распиновку (**pin layouts**).

Устанавливает **data rate**, сигнализацию (**signaling**) и расстояние передачи (**transmission distance**).

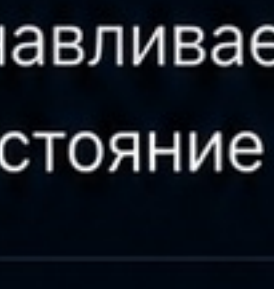
101
010

Передаёт **bits**, не заботясь о их **значении**.

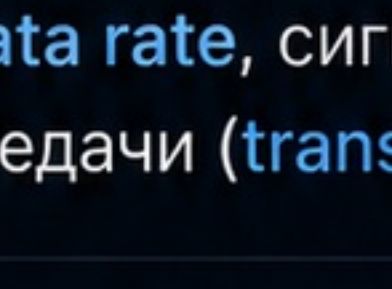
ГДЕ ЭТО ВСТРЕЧАЕТСЯ



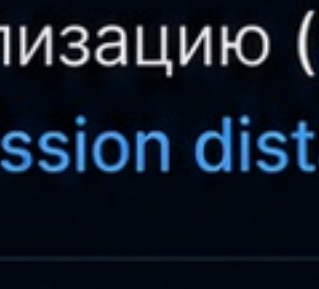
Copper & fiber



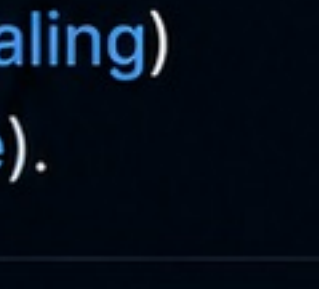
Wi-Fi radio



Hubs



Repeaters



NIC hardware

WATCH FOR

Physical доступ сам по себе позволяет кому-то **tap**, **jam** или **cut the line**.



> Представьте это как **road itself** — по дороге ваше сообщение физически перемещается.



Data Link



Упаковывает биты в frames и передаёт их между устройствами в одной local сети.

PROTOCOL DATA UNIT	ITS JOB
Frames	Local delivery

ЧТО ОН ДЕЛАЕТ

MAC

Использует MAC addresses для идентификации каждого устройства.

Добавляет error detection, чтобы повреждённые frames были пойманы.

Делит на LLC и MAC sublayers под капотом.

ГДЕ ЭТО ВСТРЕЧАЕТСЯ



MAC address



Ethernet



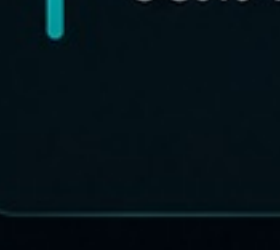
Switches



Wi-Fi 802.11

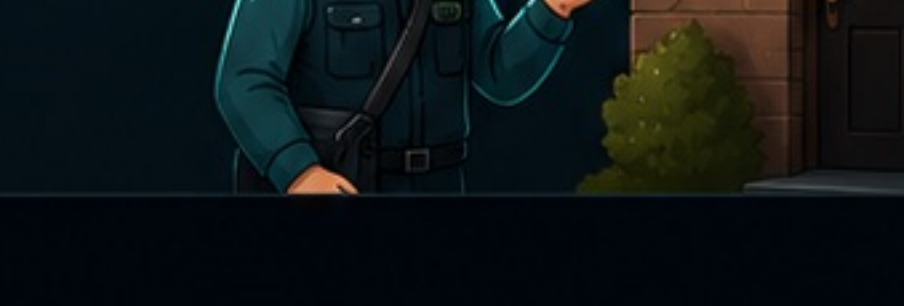
ARP

ARP



WATCH FOR

Поддельные MAC addresses и ARP tricks могут перенаправлять трафик в local сети.



> *Как local mail carrier, который знает каждый дом на своей улице по номеру.*

Network



Передаёт packets
между разными networks
и выбирает лучший путь
до destination.

PROTOCOL DATA UNIT	ITS JOB
Packets	Routing

ЧТО ОНА ДЕЛАЕТ

IP

Назначает логические IP addresses
(IPv4 и IPv6).



Маршрутизирует traffic
от hop к hop к цели.



Обрабатывает fragmentation,
когда packets слишком большие.



ГДЕ ЭТО ВСТРЕЧАЕТСЯ

IP
IP

Routers

ICMP
ICMP

OSPF & BGP

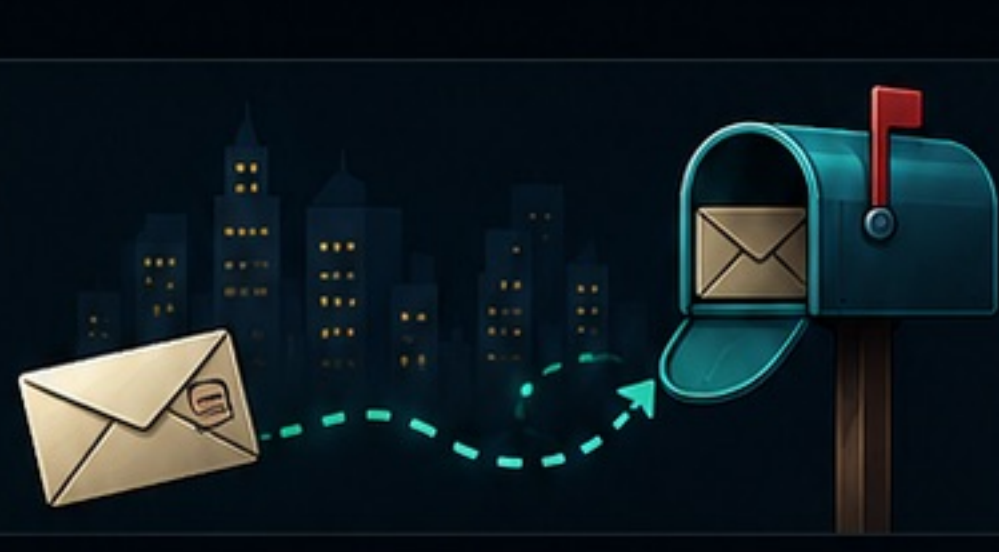
Subnets

WATCH FOR

Поддельные source IPs можно подделать,
а routes — отравить, чтобы перенаправить
packets в другое место.



Как postal system: почта пересылает
письма между городами, используя
адрес на конверте.



Transport



Доставляет данные end to end
между программами и решает,
насколько how reliable будет эта доставка.

PROTOCOL DATA UNIT	ITS JOB
Segments	End to end

ЧТО ОНА ДЕЛАЕТ

:8080

Использует port numbers,
чтобы доставить данные
в нужное приложение.



TCP гарантирует порядок и доставку
с помощью handshake.



UDP обеспечивает скорость,
а не надёжность.



ГДЕ ЭТО ВСТРЕЧАЕТСЯ

TCP

TCP

UDP

UDP



Ports



Sequencing



Flow control

WATCH FOR

Открытые порты и потоки half-open connections
могут вызвать злоупотребления.



> Представьте это как registered mail
> с подписью или открытку,
> которую кладут в почтовый ящик.



Session

Открывает, управляет и закрывает **conversations** между двумя **applications**.



PROTOCOL DATA UNIT	ITS JOB
Data	**Conversations**

ЧТО ОНА ДЕЛАЕТ

- Устанавливает и завершает **sessions** чисто и корректно.
- Поддерживает диалог в правильном порядке с помощью **checkpoints**.
- Позволяет передать управление с помощью **resume** вместо restart.

ГДЕ ЭТО ВСТРЕЧАЕТСЯ

Sessions · RPC · NetBIOS · Tokens · Checkpoints

WATCH FOR

Скомпрометированный **session token** позволяет атакующему **hijackнуть** активное соединение.



*Оператор **switchboard**, который подключает ваш звонок, держит линию открытой, а затем кладёт трубку.*



Presentation



Преобразует **data** в формат, понятный обеим сторонам, затем **шифрует** и **сжимает** его.

PROTOCOL DATA UNIT	ITS JOB
Data	**Translation**

ЧТО ОНА ДЕЛАЕТ

Выполняет **encryption** и **decryption** данных (payload).



Сжимает **data** для экономии **bandwidth**.



Преобразует **encoding** и **character sets**.



ГДЕ ЭТО ВСТРЕЧАЕТСЯ

TLS / SSL · Encryption · JPEG & MP4 · Aあ Unicode · Compression

WATCH FOR

Слабые шифры или **stripped encryption** могут легко раскрыть **payload**.



Хороший translator переписывает ваше сообщение на общем языке, а затем надёжно защищает его.



Application

Это слой, с которым вы работаете напрямую. Он предоставляет приложениям сетевые сервисы, которые они запрашивают.



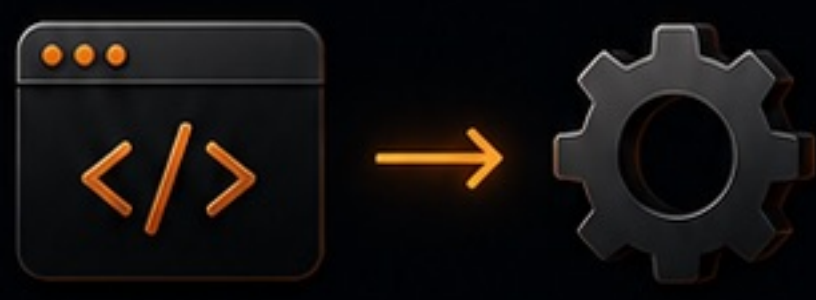
PROTOCOL DATA UNIT	ITS JOB
Data	User services

ЧТО ОНА ДЕЛАЕТ

Опирается на протоколы приложений, такие как HTTP и DNS.



Это не само приложение, а набор правил, по которым оно работает.



Определяет, где начинаются requests и заканчиваются responses.



ГДЕ ЭТО ВСТРЕЧАЕТСЯ

HTTP HTTPS				
HTTP / HTTPS	DNS	SSH	SMTP	DHCP

WATCH FOR

Большинство реальных атак происходит здесь: injection, phishing, и floods.



Как front desk в отеле: вы приходите и делаете запрос, а он связывает вас с нужным сервисом.



Как протекают data flows



Data не передаётся напрямую по проводу. При движении **вниз** по **stack** каждый **layer** добавляет свой **header**. При движении **вверх** каждый **layer** снимает свой **header**.

ENCAPSULATION ↓ send

receive ↑ DECAPSULATION

L2 · FRAME + header & trailer

L3 · PACKET + IP header

L4 · SEGMENT + TCP / UDP header

DATA

L5 to L7 payload

PDU НА КАЖДОМ ШАГЕ

Data
Ваши данные (приложения)

Segment
TCP / UDP добавляет header

Packet
IP добавляет header

Frame
L2 добавляет header & trailer

Bits
Преобразуется в биты и передаётся

ИТОГ: Data → Segment → Packet → Frame → Bits

OSI vs TCP/IP

Модель OSI состоит из 7 layers для понимания.
Интернет работает на 4 layer TCP/IP модели.
Вот как они соответствуют друг другу.



OSI · 7 LAYERS

- **L7** Application — Приложение
- **L6** Presentation — Представление
- **L5** Session — Сеансовый уровень
- **L4** Transport — Транспортный уровень
- **L3** Network — Сетевой уровень
- **L2** Data Link — Канальный уровень
- **L1** Physical — Физический уровень

TCP/IP · 4 LAYERS

- **Application** — Приложение — OSI 5 · 6 · 7
- **Transport** — Транспорт — OSI 4
- **Internet** — Интернет — OSI 3
- **Network Access** — Доступ к сети — OSI 1 · 2

OSI для понимания и устранения проблем,
TCP/IP для реальной работы.

Понимание **OSI** → Диагностика (Troubleshoot) → Разработка (Build) → Работа (Рабочая сеть)

Атаки на каждом layer



Каждый **layer** — потенциальная **цель**. Вот классические атаки на каждом уровне **stack**.

L7 **Application**
Прикладной уровень

Атаки: Injection, XSS, app DDoS



L6 **Presentation**
Уровень представления

Атаки: SSL stripping



L5 **Session**
Сеансовый уровень

Атаки: Session hijacking



L4 **Transport**
Транспортный уровень

Атаки: SYN flood



L3 **Network**
Сетевой уровень

Атаки: IP spoofing



L2 **Data Link**
Канальный уровень

Атаки: ARP poisoning



L1 **Physical**
Физический уровень

Атаки: Wiretapping & jamming



Глубокая защита: каждый **layer** требует своего **контроля**.

Шпаргалка: 7 layer в одной таблице



Вся модель на одном экране. Сделайте screenshot и держите под рукой.

LAYER			PDU	KEY EXAMPLES
7		**Application** Прикладной уровень	Data 	HTTP, DNS  
6		**Presentation** Уровень представления	Data 	TLS, JPEG  
5		**Session** Сеансовый уровень	Data 	RPC, Sockets 
4		**Transport** Транспортный уровень	Segments 	TCP, UDP TCP UDP
3		**Network** Сетевой уровень	Packets 	IP, Routers IP 
2		**Data Link** Канальный уровень	Frames 	MAC, Switch MAC 00:1A:2B:3C:4D:5E 
1		**Physical** Физический уровень	Bits 10110 01011	Cables, Wi-Fi  

Запомните: каждый **layer** имеет свою задачу и потенциальные атаки. Защищайте каждый **layer!**