

网络层协议

✚ TCP/IP 四层模型

TCP/IP 模型是互联网使用的核心网络模型，它大致分为四层（从上到下）：

1. 应用层 (Application Layer)

- 直接面向用户，提供各种应用服务。
- 协议举例：HTTP、FTP、SMTP、DNS ...

2. 传输层 (Transport Layer)

- 负责端到端的通信，保证数据从一个应用进程传到另一个应用进程。
- 协议举例：
 - TCP（可靠、面向连接，适合文件传输、网页加载）
 - UDP（不可靠、无连接，适合实时音视频、DNS）

3. 网络层 (Internet Layer)

- 负责主机到主机的通信，即数据从源设备发送到目标设备。
- 主要任务：寻址、路由选择。
- 协议举例：IP（IPv4/IPv6）、ICMP、ARP ...

4. 网络接口层 (Network Access Layer / Link Layer)

- 负责具体的物理传输（以太网、Wi-Fi、光纤等）。
- 协议举例：以太网协议、PPP、MAC ...

主要过程

✚ 数据在网络层的传输过程

举个例子：你访问一个网页时，数据传输流程如下：

1. 应用层 (HTTP)：浏览器发出请求 → 请求报文。
2. 传输层 (TCP)：加上 TCP 头 → TCP 报文段。
3. 网络层 (IP)：加上 IP 头 → IP 数据报。
4. 链路层 (以太网)：加上 MAC 头尾 → 以太网帧。
5. 物理层：转化为电信号/光信号，无线电波，传输出去。

数据到达对方主机后，反向解封装（剥掉各层头部），最终交给应用层。

主要的协议

📌 网络层的传输

重点来说网络层 (Internet Layer)。

- **核心协议：IP (Internet Protocol)**
 - 作用：把数据从源主机传到目标主机。
 - **数据单位：IP 数据报 (IP Datagram)。**
 - 功能：
 1. **寻址**：通过 IP 地址标识源和目的主机。
 2. **路由**：决定数据报经过哪些路径才能到达目标。
 3. **分片与重组**：当链路层帧的最大长度不足时，IP 报文会被分片。
- **辅助协议：**
 1. **ICMP** (Internet Control Message Protocol)
 - 用来反馈网络错误和诊断 (比如 `ping` 命令就是 ICMP) 。
 2. **ARP** (Address Resolution Protocol)
 - 解决 **IP 地址** ↔ **MAC 地址** 的映射问题。
 3. **RARP** (已被淘汰)
 - 反向解析地址 (MAC → IP) 。

✅ 总结一句话：

- **网络层 (Internet Layer)** = 负责“主机到主机”的传输 (IP寻址+路由) 。
- **传输层 (Transport Layer)** = 负责“进程到进程”的传输 (TCP/UDP) 。

IP 协议

(Internet Protocol)

它是 TCP/IP 网络体系里 **网络层** 的核心协议。

什么是 IP 协议?

- IP (Internet Protocol, 网际协议) 是 TCP/IP 协议族中的核心协议。
- 它主要负责 把数据从源主机传输到目标主机, 但它只提供 **尽力而为 (Best-Effort)** 的传输:
 - **不可靠**: 不保证数据一定到达。
 - **无连接**: 发送数据之前不需要建立连接。
 - **逐包独立**: 每个 IP 数据报独立路由, 可能走不同的路径。

IP 协议的主要功能

1. 寻址 (Addressing)

- 每个主机都有一个 **IP 地址**, 用来标识网络中的设备。
- IPv4: 32 位地址 (如 192.168.1.1)。
- IPv6: 128 位地址 (如 2001:db8::1)。

2. 路由 (Routing)

- IP 协议负责把数据报送到目标主机, 即使中间有多个路由器。
- 每个路由器根据 **目标 IP 地址** 决定下一跳。

3. 分片与重组 (Fragmentation & Reassembly)

- 不同网络的数据链路层最大传输单元 (MTU) 可能不同。
- 如果 IP 数据报太大, 就会被分片, 目标主机再重组。

4. 封装与解封装 (Encapsulation)

- IP 把传输层数据 (TCP 段/UDP 数据报) 封装成 **IP 数据报**。
- 收到后再解封装, 交给上层。

📌 IP 数据报格式 (IPv4 为例)

一个 IPv4 数据报头部最小 20 字节，最大 60 字节，结构如下：

字段	长度	说明
版本号	4 位	IPv4 = 4, IPv6 = 6
首部长度	4 位	表示 IP 头的长度
区分服务 (DSCP)	8 位	QoS 服务质量标识
总长度	16 位	整个数据报的长度
标识	16 位	分片时用来区分数据报
标志	3 位	是否分片的控制位
片偏移	13 位	分片在原数据报中的位置
生存时间 (TTL)	8 位	防止数据包无限循环
协议	8 位	表示上层协议 (TCP=6, UDP=17, ICMP=1)
首部校验和	16 位	检测头部是否出错
源 IP 地址	32 位	发送方的 IP
目的 IP 地址	32 位	接收方的 IP
可选字段	0-40 字节	不常用

👉 IP 数据报 = IP 头部 + 数据部分 (数据部分通常是 TCP 或 UDP 报文段) 。

IPv4 与 IPv6 的区别

特点	IPv4	IPv6	
地址长度	32 位, 约 42 亿个地址	128 位, 几乎无限	
地址表示	点分十进制 (192.168.0.1)	十六进制 (2001:db8::1)	
地址耗尽	已耗尽	解决了地址枯竭问题	
首部复杂度	可变长度 (20–60 字节)	固定长度 (40 字节), 效率更高	
NAT 依赖	常用 NAT 节省地址	不需要 NAT	

总结

- **IP 协议 = 网络层的灵魂**
- 它负责 **寻址、路由、分片**, 但 **不保证可靠性**。
- 可靠性、顺序控制等工作交给 **传输层 (TCP)** 。