EPT 怪星科技

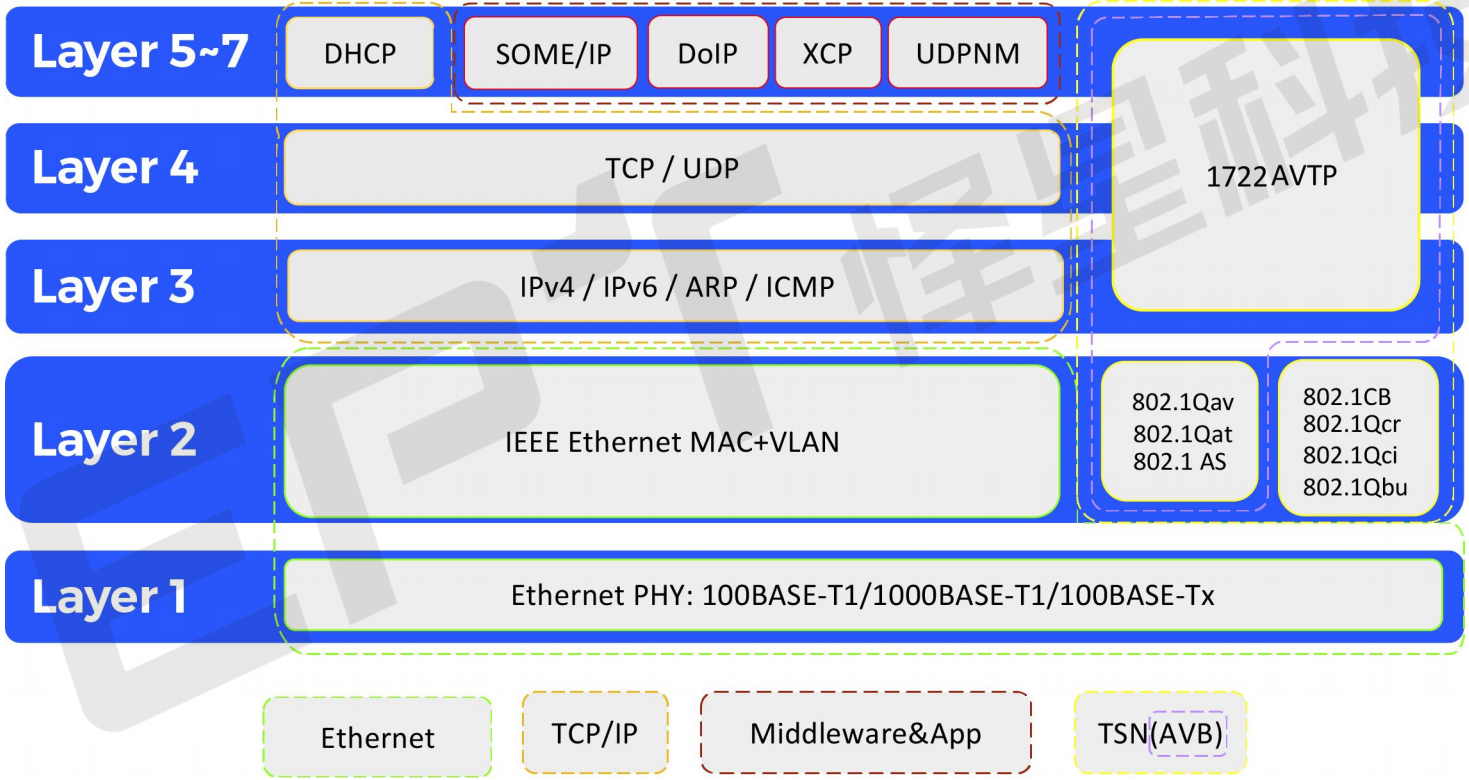
# 汽车以太网网络层/传输层技术

# CONTENTS

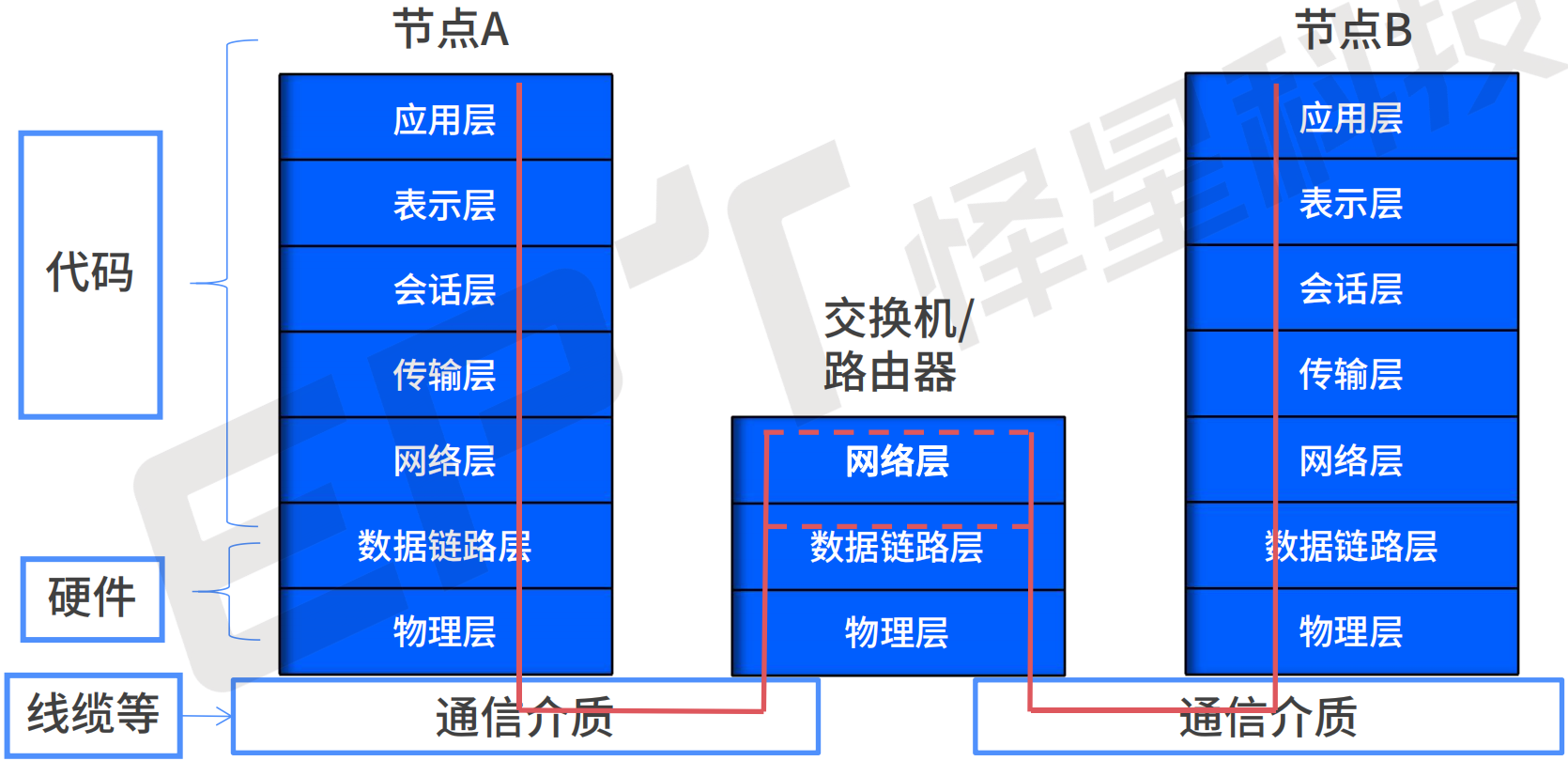
# 01

# 汽车以太网技术概述

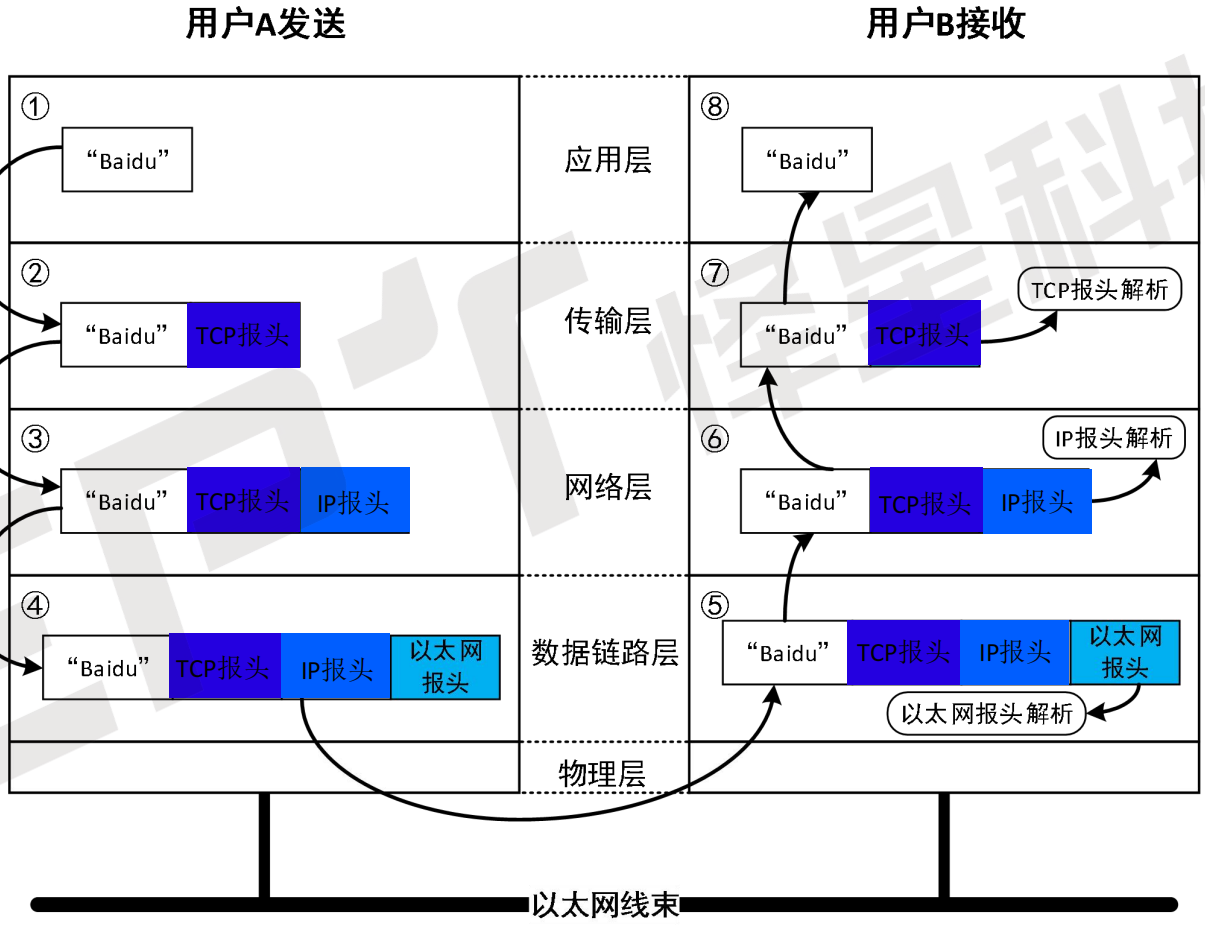
# 汽车以太网相关协议


Layer 5~7
DHCP
SOME/IP
DoIP
XCP
UDPNM
Layer 4
TCP / UDP
1722 AVTP
Layer 3
IPv4 / IPv6 / ARP / ICMP
Layer 2
IEEE Ethernet MAC+VLAN
802.1Qav
802.1Qat
802.1 AS
802.1CB
802.1Qcr
802.1Qci
802.1Qbu
Layer 1
Ethernet PHY: 100BASE-T1/1000BASE-T1/100BASE-Tx
Ethernet
TCP/IP
Middleware&App
TSN(AVB)

# 以太网传输机制


节点A
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
交换机/
路由器
网络层
数据链路层
物理层
节点B
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
代码
硬件
线缆等
通信介质
通信介质

# 以太网传输示例



02

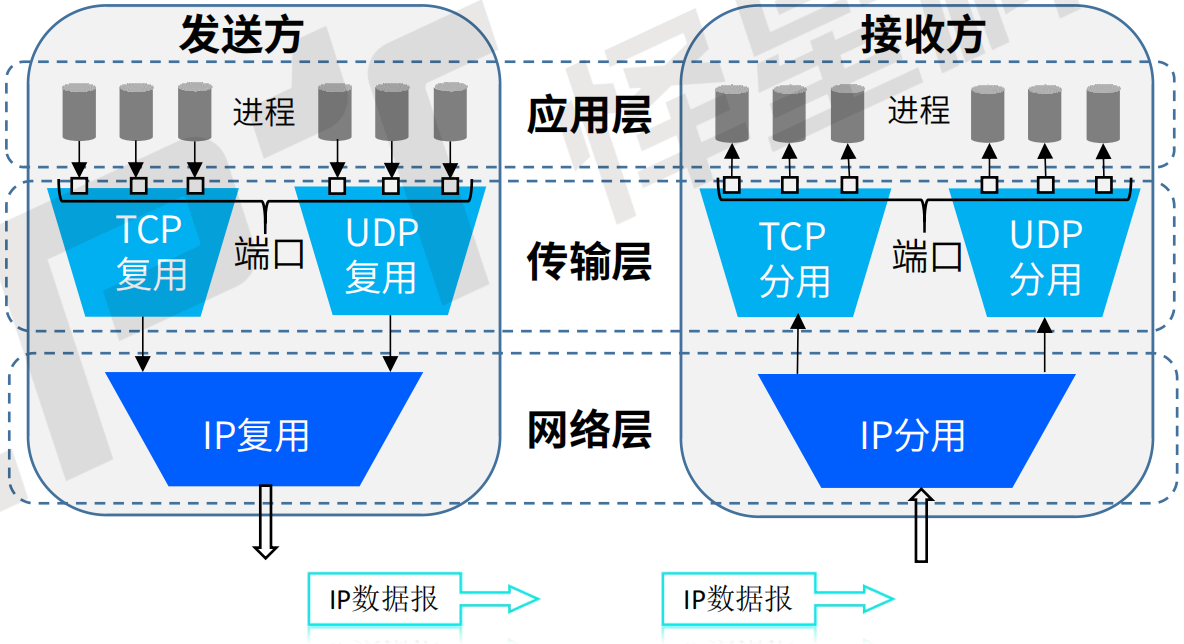
# TCP/IP主要协议介绍

# 传输层



传输层主要作用：

- 提供应用进程之间的逻辑通信
- 复用和分用
- 差错检测



# 端口号



IP设备中端口号和IP地址及传输层协议组成三元组用来识别一个特定的软件进程

端口号使用16bit表示，取值范围0~65535：

- 公认端口号：0~1023，ICANN把这些端口号指派给特定的一些协议
- 注册端口号：1024~49151，使用这些端口号必须在ICANN按照规定进行登记，以防止重复
- 动态和/或私有端口号：49152~65535，留给进程暂时使用，进程结束后可供其它进程使用

端口号只有本地意义，不同主机中端口号没有联系

| 协议 | 端口号 | 关键字 | 描述 |
| --- | --- | --- | --- |
| UDP | 68 | DHCP | 动态主机设置协议（客户端） |
| UDP | 67 | DHCP | 动态主机设置协议（服务器） |
| TCP | 22 | SSH | 安全外壳协议 |
| TCP | 23 | Telnet | 远程终端服务器 |
| TCP | 25 | SMTP | 简单邮件传输协议 |
| TCP | 80 | HTTP | 超文本传输协议 |
| TCP | 443 | HTTPS | 超文本传输安全协议 |

ICANN（The Internet Corporation for Assigned Names and Numbers）：互联网名称与数字地址分配机构，负责包括互联网协议（IP）地址的空间分配、协议标识符的指派、通用顶级域名（gTLD）以及国家和地区顶级域名（ccTLD）系统的管理、以及根服务器系统的管理

## 用户数据报协议 - User Datagram Protocol - RFC768

### 特点

- 面向报文
- 无连接
- 不保证传输数据的可靠性
- 报头简单


### 应用场景

- 视频，音频等多媒体通信(即时通信)
- 广播、多播

RFC（Request For Comments）：是一系列以编号排定的文件，文件收集了有关互联网相关信息，以及UNIX和互联网社区的软件文件，其中的Internet协议族文档部分由以太网工程师任务组定义发布。

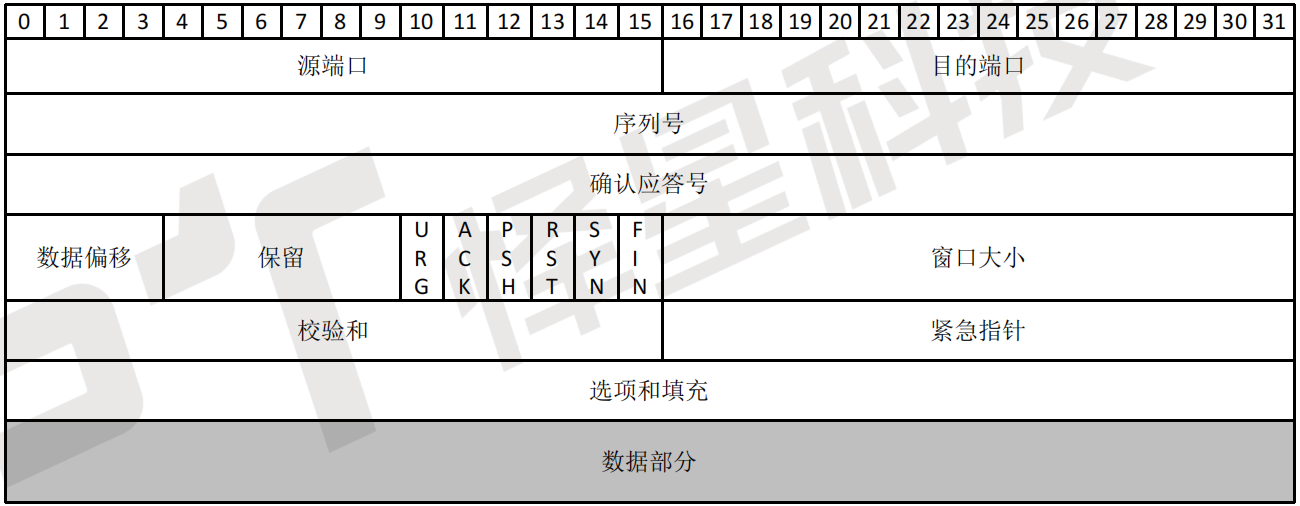
# UDP报文示例

```
User Datagram Protocol, Src Port: 1024, Dst Port: 5001
    Source Port: 1024
    Destination Port: 5001
    Length: 123
    Checksum: 0xf3f8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 18]
  [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
    UDP payload (115 bytes)
Data (115 bytes)
    Data: 01010e00e12b83c7249900650000000600095 44c2d57523838364e000b0003362e300007…
    [Length: 115]
```

# 传输控制协议 - Transmission Control - RFC793

## 特点

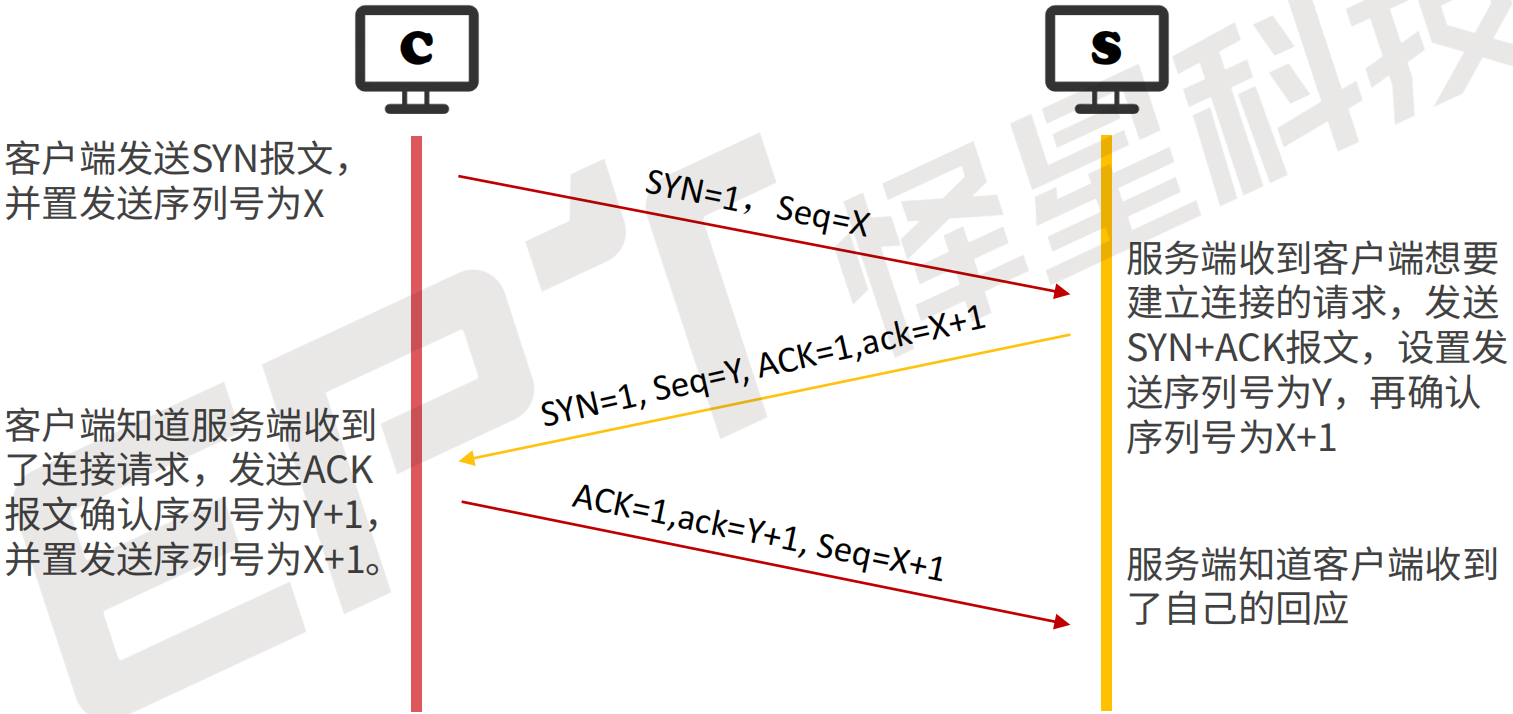
- 面向连接
  - ✓三次握手/四次挥手
- 可靠传输
  - ✓确认应答
  - ✓超时重传
- 基于字节流
  - ✓数据按字节拆分并编号 – 序列号
- 全双工通信




## 应用场景

- 文件传输
- 邮件

# TCP的连接建立 – 三次握手



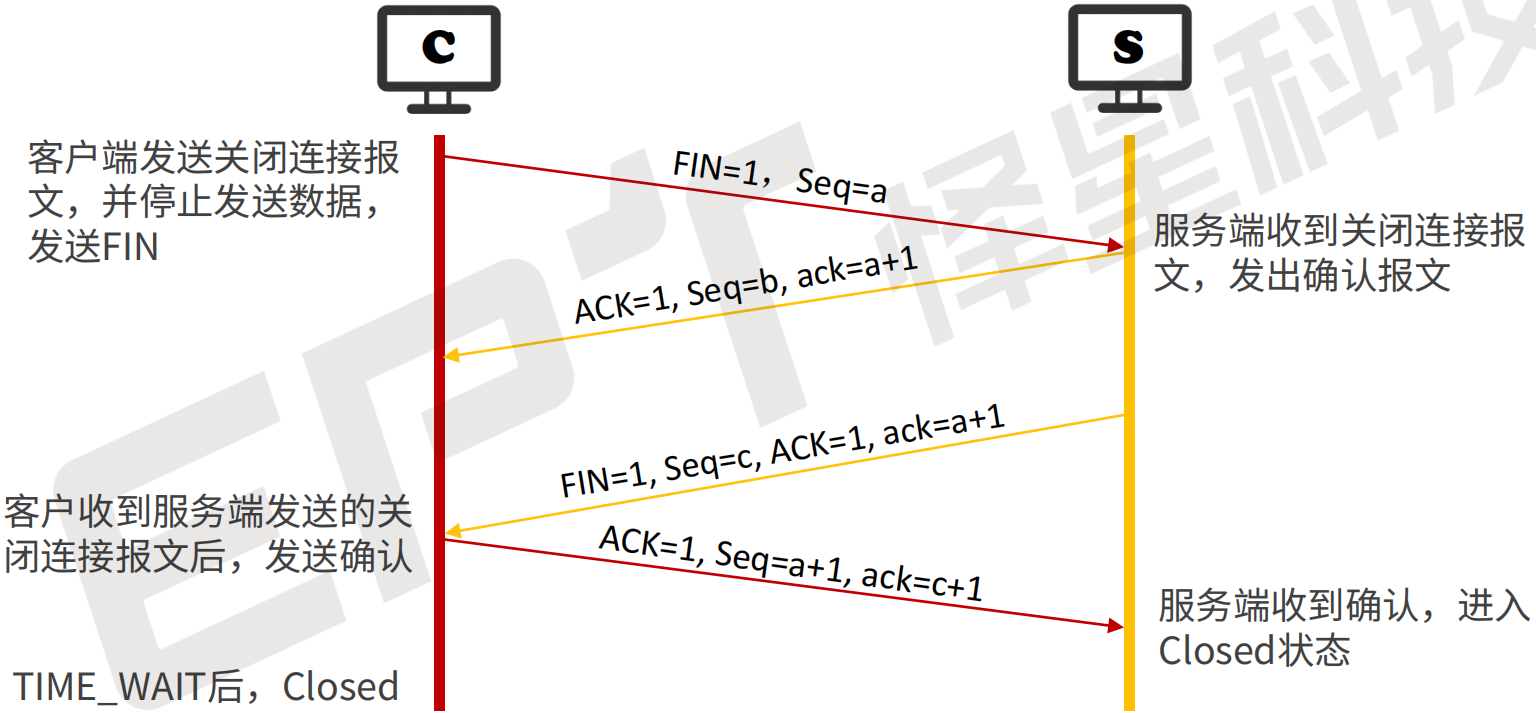
# 三次握手示例

| | | | | | |
|---|---|---|---|---|---|
| 7 | 0.205760 | 192.168.0.4 | 192.168.0.101 | TCP | 74 17132 → 17132 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=2403477319 TSecr=0 WS=256 |
| 8 | 0.206234 | 192.168.0.101 | 192.168.0.4 | TCP | 60 17132 → 17132 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 |
| 9 | 0.206931 | 192.168.0.4 | 192.168.0.101 | TCP | 60 17132 → 17132 [ACK] Seq=1 Ack=1 Win=29200 Len=0 |
| 10 | 0.207748 | 192.168.0.4 | 192.168.0.102 | UDP | 60 10000 → 14792 Len=16 |
| 11 | 0.208092 | 192.168.0.102 | 192.168.0.4 | UDP | 61 14792 → 10000 Len=19 |

```
> Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: 02:00:00:0b:00:03 (02:00:00:0b:00:03), Dst: 02:00:00:00:00:74 (02:00:00:00:00:74)
> Internet Protocol Version 4, Src: 192.168.0.4, Dst: 192.168.0.101
v Transmission Control Protocol, Src Port: 17132, Dst Port: 17132, Seq: 0, Len: 0
    Source Port: 17132
    Destination Port: 17132
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1316341987
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  > Flags: 0x002 (SYN)
    Window: 29200
    [Calculated window size: 29200]
    Checksum: 0x007a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  v Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
      > TCP Option - Maximum segment size: 1460 bytes
      > TCP Option - SACK permitted
      > TCP Option - Timestamps
      > TCP Option - No-Operation (NOP)
      > TCP Option - Window scale: 8 (multiply by 256)
  > [Timestamps]
```

```
0000  02 00 00 00 00 74 02 00  00 0b 00 03 08 00 45 00
0010  00 3c 35 b5 40 00 40 06  83 4d c0 a8 00 04 c0 a8
0020  00 65 42 ec 42 ec 4e 75  c8 e3 00 00 00 00 a0 02
0030  72 10 00 7a 00 00 02 04  05 b4 04 02 08 0a 8f 42
0040  27 47 00 00 00 00 01 03  03 08
```

# TCP的断开连接 – 四次挥手



# 四次挥手示例

| | | | | | |
|---|---|---|---|---|---|
| 12 | 0.208908 | 192.168.0.4 | 192.168.0.101 | TCP | 60 17132 → 17132 [FIN, ACK] Seq=1 Ack=1 Win=29200 Len=0 |
| 13 | 0.208908 | 192.168.0.4 | 192.168.0.102 | UDP | 60 10000 → 14792 Len=16 |
| 14 | 0.418354 | 192.168.0.4 | 192.168.0.101 | TCP | 60 [TCP Retransmission] 17132 → 17132 [FIN, ACK] Seq=1 Ack=1 Win=29200 Len=0 |
| 15 | 0.418935 | 192.168.0.101 | 192.168.0.4 | TCP | 60 17132 → 17132 [ACK] Seq=1 Ack=2 Win=65535 Len=0 |
| 16 | 0.419279 | 192.168.0.102 | 192.168.0.4 | UDP | 64 14792 → 10000 Len=22 |
| 17 | 0.420119 | 192.168.0.4 | 192.168.0.102 | UDP | 60 10000 → 14792 Len=18 |
| 18 | 0.420462 | 192.168.0.101 | 192.168.0.4 | TCP | 60 17132 → 17132 [PSH, ACK] Seq=1 Ack=2 Win=65535 Len=5 |
| 19 | 0.420921 | 192.168.0.4 | 192.168.0.101 | TCP | 60 17132 → 17132 [ACK] Seq=2 Ack=6 Win=29200 Len=0 |
| 20 | 0.422387 | 192.168.0.4 | 192.168.0.102 | DNS | 67 Standard query response 0x0105 No such name[Malformed Packet] |
| 21 | 0.422757 | 192.168.0.101 | 192.168.0.4 | TCP | 60 17132 → 17132 [FIN, ACK] Seq=6 Ack=2 Win=65535 Len=0 |
| 22 | 0.423489 | 192.168.0.4 | 192.168.0.101 | TCP | 60 17132 → 17132 [ACK] Seq=2 Ack=7 Win=29200 Len=0 |

```
> Frame 12: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: 02:00:00:0b:00:03 (02:00:00:0b:00:03), Dst: 02:00:00:00:00:74 (02:00:00:00:00:74)
> Internet Protocol Version 4, Src: 192.168.0.4, Dst: 192.168.0.101
v Transmission Control Protocol, Src Port: 17132, Dst Port: 17132, Seq: 1, Ack: 1, Len: 0
    Source Port: 17132
    Destination Port: 17132
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1316341988
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 310441686
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x011 (FIN, ACK)
    Window: 29200
    [Calculated window size: 29200]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x1580 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
```

```
0000  02 00 00 00 00 74 02 00  00 0b 00 03 08 00 45 00
0010  00 28 35 b7 40 00 40 06  83 5f c0 a8 00 04 c0 a8
0020  00 65 42 ec 42 ec 4e 75  c8 e4 12 80 f6 d6 50 11
0030  72 10 15 80 00 00 00 00  00 00 00 00
```

# TCP与UDP对比



共同点：

TCP与UDP都属于传输层协议。

差异点：

1）连接机制

TCP 是面向连接的传输层协议；

UDP 是不需要连接。

2）服务对象

TCP 是一对一的两点连接；

UDP 支持一对一、一对多。

3）可靠性

TCP 保证数据不丢失、不重复、按序到达；

UDP 是尽最大努力交付，不保证交付数据。

4）拥塞控制、流量控制

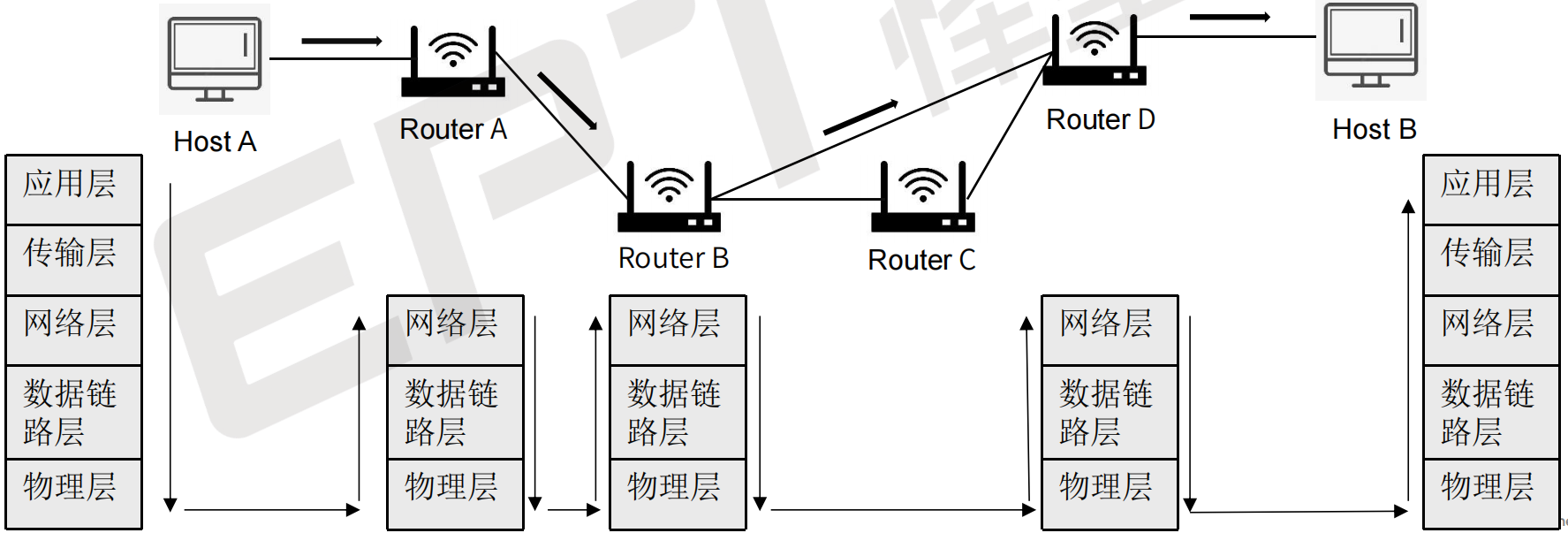
TCP 有拥塞控制和流量控制机制；

UDP 则没有拥塞控制和流量控制机制。

# 网络层

网络层主要功能：

- 为网络中的设备提供逻辑地址
- 数据包的寻径及转发
- 差错检测



# IPv4



IPv4 - InternetProtocolversion4，互联网通讯协议第四版本

协议标准

- RFC791 - Internet Protocol

基本特点

- 面向无连接、不可靠、尽最大努力交付数据报

作用

- 将数据报送到目的地

## 地址表示

点分十进制(192.168.1.1)，共32bit

| 计算机存储 | 1100 0000 | 1010 1000 | 0000 0001 | 0000 0001 |
| --- | --- | --- | --- | --- |
| 十进制 | 192 | 168 | 1 | 1 |

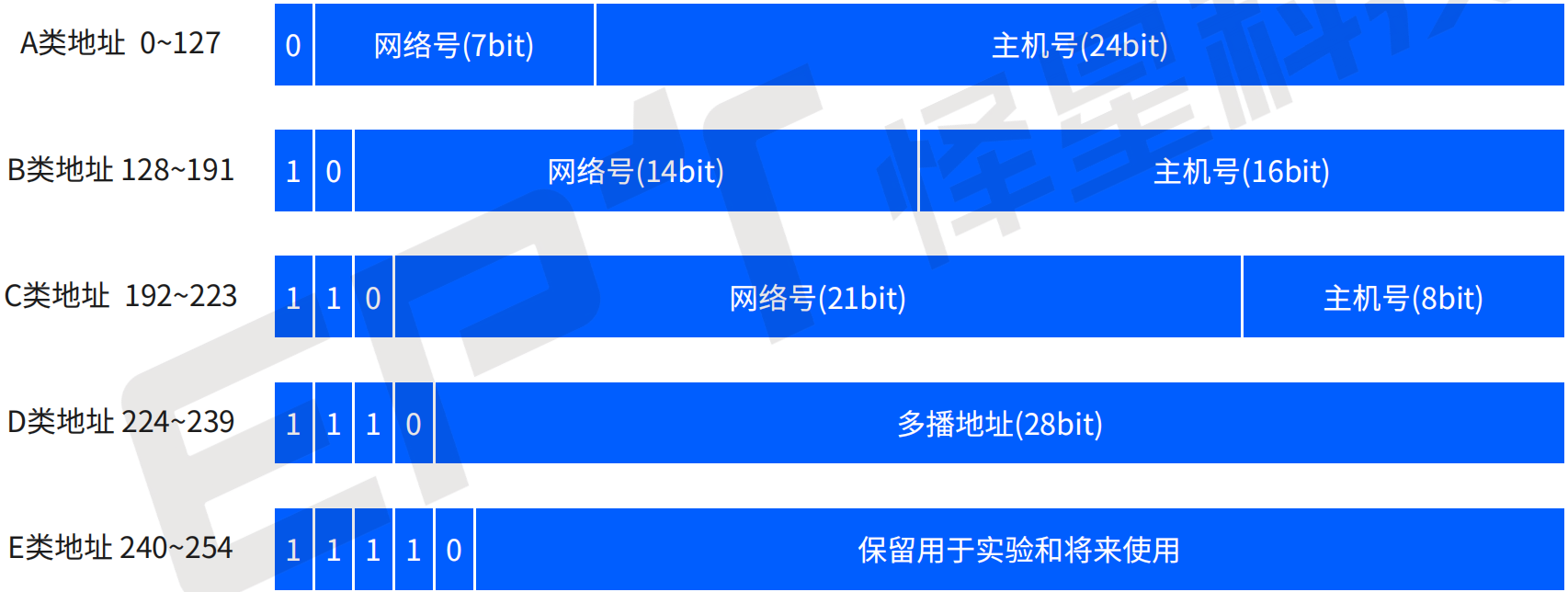
## 地址组成

网络号+主机号

网络号：用于识别主机所在的网络

主机号：用于识别该网络中的主机

## 地址分类


A类地址 0~127
0
网络号(7bit)
主机号(24bit)
B类地址 128~191
1
0
网络号(14bit)
主机号(16bit)
C类地址 192~223
1
1
0
网络号(21bit)
主机号(8bit)
D类地址 224~239
1
1
1
0
多播地址(28bit)
E类地址 240~254
1
1
1
1
0
保留用于实验和将来使用

## 特殊地址

| 地址/地址范围 | 用途 |
| --- | --- |
| 0.0.0.0 | 只能做源地址 |
| 127.0.0.1~127.255.255.254 | 环回地址(Localhost) |
| 255.255.255.255 | 广播地址 |
| 10.0.0.0 ~ 10.255.255.255 | 私有地址 |
| 172.16.0.0 ~ 172.31.255.255 | 私有地址 |
| 192.168.0.0 ~ 192.168.255.255 | 私有地址 |


https://www.icann.org/

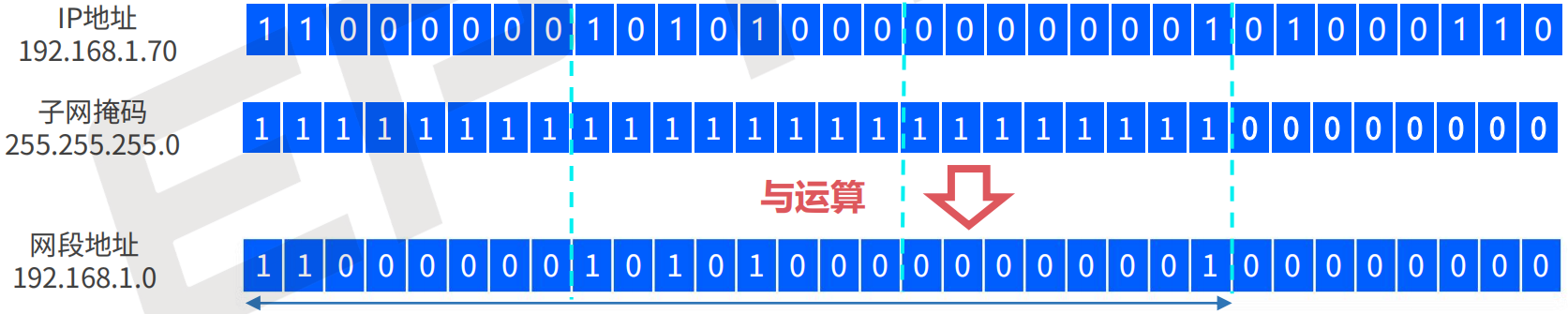
## 子网掩码

区分**网络ID**(*用1表示*) 和**主机ID**(*用0表示*)

C类地址默认的子网掩码为 255.255.255.0


判断通讯双方的IP是否在同一局域网

IP地址和子网掩码进行“与”运算.



ARP - Address Resolution Protocol，地址解析协议

ARP功能

询问目标IP对应的MAC地址

ARP缓存表

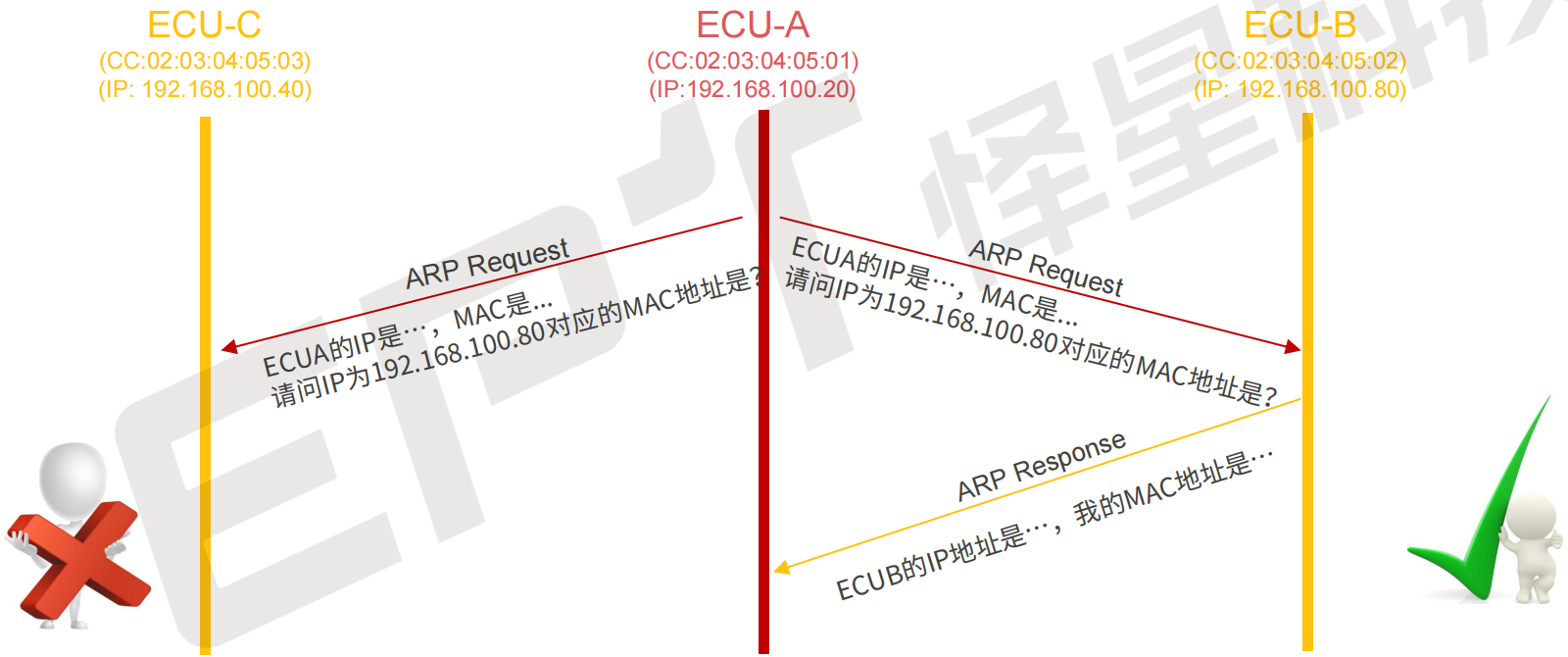
存储IP地址和MAC地址的映射表

- ✓动态保存：设置老化时间
- ✓静态存储：永久保存

协议标准

RFC826

# ARP通信过程


ECU-C
(CC:02:03:04:05:03)
(IP: 192.168.100.40)
ECU-A
(CC:02:03:04:05:01)
(IP:192.168.100.20)
ECU-B
(CC:02:03:04:05:02)
(IP: 192.168.100.80)
ARP Request
ECUA的IP是…，MAC是…
请问IP为192.168.100.80对应的MAC地址是?
ARP Request
ECUA的IP是…，MAC是…
请问IP为192.168.100.80对应的MAC地址是?
ARP Response
ECUB的IP地址是…，我的MAC地址是…

# ARP报文示例

```
Ethernet II, Src: Tp-LinkT_5c:4e:1b (94:d9:b3:5c:4e:1b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  Source: Tp-LinkT_5c:4e:1b (94:d9:b3:5c:4e:1b)
      Address: Tp-LinkT_5c:4e:1b (94:d9:b3:5c:4e:1b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Tp-LinkT_5c:4e:1b (94:d9:b3:5c:4e:1b)
    Sender IP address: 192.168.0.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.100
```

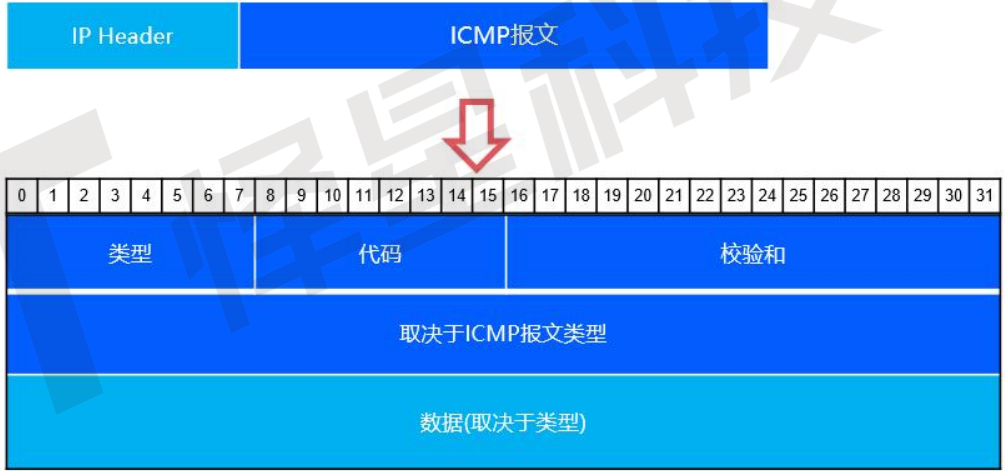
ICMP - Internet Control Message Protocol，以太网控制报文协议

在主机、路由器之间传递信息:

- 网络状况信息
- 主机状况信息
- 路由是否可用…

协议标准

RFC792




- 查询报文
  - 请求与回应报文
  - 路由查询或通告
  - 时间戳请求与应答
  - 地址掩码请求与应答
- 差错报文
  - 目的不可达
  - 超时问题
  - 参数问题
- 控制报文
  - 源站抑制
  - 路由重定向

## ICMP应用举例-ping（Packet InterNet Groper），分组网间探测

- 测试另一台主机是否可达
- 测试出两台主机间往返时间
- ICMP ping不使用TCP或UDP，应用层直接使用ICMP


```
C:\                    >ping 180.101.50.188

正在 Ping 180.101.50.188 具有 32 字节的数据:
来自 180.101.50.188 的回复: 字节=32 时间=12ms TTL=51
来自 180.101.50.188 的回复: 字节=32 时间=12ms TTL=51
来自 180.101.50.188 的回复: 字节=32 时间=11ms TTL=51
来自 180.101.50.188 的回复: 字节=32 时间=11ms TTL=51

180.101.50.188 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 11ms，最长 = 12ms，平均 = 11ms
```

# ICMP报文示例

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 15 | 3.399153 | 192.168.0.103 | 192.168.0.101 | ICMP | 74 | Echo (ping) request id=0x0001, seq=111/28416, ttl=64 (reply in 24) |
| 24 | 3.407643 | 192.168.0.101 | 192.168.0.103 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=111/28416, ttl=64 (request in 15) |
| 29 | 4.402600 | 192.168.0.103 | 192.168.0.101 | ICMP | 74 | Echo (ping) request id=0x0001, seq=112/28672, ttl=64 (reply in 32) |
| 32 | 4.475699 | 192.168.0.101 | 192.168.0.103 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=112/28672, ttl=64 (request in 29) |
| 34 | 5.415182 | 192.168.0.103 | 192.168.0.101 | ICMP | 74 | Echo (ping) request id=0x0001, seq=113/28928, ttl=64 (reply in 35) |
| 35 | 5.432336 | 192.168.0.101 | 192.168.0.103 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=113/28928, ttl=64 (request in 34) |
| 38 | 6.420093 | 192.168.0.103 | 192.168.0.101 | ICMP | 74 | Echo (ping) request id=0x0001, seq=114/29184, ttl=64 (reply in 39) |
| 39 | 6.429611 | 192.168.0.101 | 192.168.0.103 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=114/29184, ttl=64 (request in 38) |

```
> Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C295F7BF-CEDF-41BE-A72D-ABAAF6C0D596}, id 0
> Ethernet II, Src: IntelCor_79:04:28 (18:26:49:79:04:28), Dst: HuaweiTe_4f:56:5e (c8:14:51:4f:56:5e)
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.101
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4cec [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 111 (0x006f)
    Sequence Number (LE): 28416 (0x6f00)
    [Response frame: 24]
  > Data (32 bytes)
```

```
命令提示符

C:\[redacted]>ping 192.168.0.101

正在 Ping 192.168.0.101 具有 32 字节的数据:
来自 192.168.0.101 的回复: 字节=32 时间=8ms TTL=64
来自 192.168.0.101 的回复: 字节=32 时间=73ms TTL=64
来自 192.168.0.101 的回复: 字节=32 时间=17ms TTL=64
来自 192.168.0.101 的回复: 字节=32 时间=9ms TTL=64

192.168.0.101 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 8ms, 最长 = 73ms, 平均 = 26ms
```

```
> Frame 24: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C295F7BF-CEDF-41BE-A72D-ABAAF6C0D596}, id 0
> Ethernet II, Src: HuaweiTe_4f:56:5e (c8:14:51:4f:56:5e), Dst: IntelCor_79:04:28 (18:26:49:79:04:28)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.103
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x54ec [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 111 (0x006f)
    Sequence Number (LE): 28416 (0x6f00)
    [Request frame: 15]
    [Response time: 8.490 ms]
  > Data (32 bytes)
```

```
命令提示符

C:\[redacted]>ping 192.168.0.101

正在 Ping 192.168.0.101 具有 32 字节的数据:
来自 192.168.0.101 的回复: 字节=32 时间=8ms TTL=64
来自 192.168.0.101 的回复: 字节=32 时间=73ms TTL=64
来自 192.168.0.101 的回复: 字节=32 时间=17ms TTL=64
来自 192.168.0.101 的回复: 字节=32 时间=9ms TTL=64

192.168.0.101 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 8ms, 最长 = 73ms, 平均 = 26ms
```

# 03

# TC8中的TCP/IP协议测试简介

# TC8测试内容概览



## 物理层测试

- 物理层IOP测试
- 物理层PMA测试

## 数据链路层测试

- VLAN测试
- 通用测试
- 地址学习
- 帧过滤测试
- Qos测试
- 时钟同步测试

## TCP/IP一致性测试

- ARP测试
- ICMP测试
- IPv4测试
- IPv4动态配置测试
- UDP测试
- TCP测试
- DHCPv4-Client测试

## SOME/IP测试

- SOME/IP Server测试
- SOME/IP ETS测试

# UDP测试用例



## 报文字段测试

- 报文头测试
- 端口测试
- 长度测试
- 填充测试
- Checksum测试

## 接口测试

- 多连接测试

## IP相关测试

- 选项测试
- 组播广播测试
- 端口不可达测试

# TCP测试用例



## 状态机测试

- 握手机制检测 SYN(C/S) FIN
- 标志位检测
- 状态检测

## 报文字段测试

- Checksum检测
- 报文头检测
- 序列号测试
- ACK测试

## 行为测试

- 连接建立测试
- 连接关闭测试
- 重传超时测试
- 应答序列测试
- Nagle测试
- 无效数据包接收测试
- 应用层交互测试
- 窗口测试

# 网络层测试用例



## IP测试

### 报头字段测试

- 长度测试
- Checksum测试
- TTL测试
- 版本号测试

### 功能测试

- 分片测试
- 分片重组测试
- 广播和环回地址测试

## ARP测试

### IP/MAC对应关系

- 静态表项
- 动态学习

### 字段检测

- 硬件类型/源和目的地
- 协议类型/源和目的地

### ARP接收处理

- 正确学习
- 发送应答
- 错误忽略

## ICMP测试

### 错误测试

- 分片测试
- 广播地址测试
- 未知类型测试

### 消息类型测试

- 报文头错误测试
- Checksum测试
- Echo测试
- 时间戳响应测试
- 未知协议发送目的不可达测试

# 04

# SmartETH以太网测试套件简介

# 主流汽车以太网测试方案，在使用过程中的痛点或困难点



当前国内主流汽车以太网测试方案，通常为一套能够覆盖从L1到L7的全面测试方案

## 整套设备昂贵，占用大量资本

众所周知以太网机柜和台架的成本较高，目前市面上基本都是采用进口硬件方案进行测试。尤其是物理层测试设备，可能会占整套设备费用的40%以上

## 测试机柜使用不灵活

测试机柜通常会把L1~L7的测试设备安装到一起，进行特定线束连接设计，且通常放置在测试实验室里。会导致不同测试设备不方便进行移动，不方便单独使用，不方便在办公室进行快速调试

## 机柜拓展性低

因机柜通常为19寸标准机柜，而且每套机柜都是有特定的接线设计，以保证整体机柜的连通性和美观度，会导致设备扩展性较差

## 对测试人员能力要求较高

以太网协议和测试标准内容庞杂，涉及知识面较广，要测试好以太网必须了解相应协议内容，对测试人员要求较高

# SmartETH产品概述



## SmartETH

- TC8 3.0标准闭源测试软件
- TC8 3.0标准开源测试软件
- DoIP闭源/开源测试软件

## Option.Hardware

- 程控电源
- USB加密狗
- ETS4620（可选）

## Option.Service

- 物理层测试服务
- TC8 3.0标准测试服务
- DoIP测试服务

- 物理层-PMA测试服务
- 物理层-IOP测试服务
- L2层-Switch功能测试服务
- L2层-Switch性能测试服务
- L3~4层-TCP/IP测试服务
- L5~7层-SOMEIP测试服务
- L5~7层-DHCP测试服务
- UT集成服务（全栈系统）
- ETS集成服务（全栈系统）

## UT/ETS

### UT嵌入式插件

UT集成：
- UT binary for POSIX
- UT binary for AUTOSAR-CP

UT源码：
- UT Source for Linux
- UT Source for Android
- UT Source for QNX
- UT Source for Vector-CP
- UT Source for LwIP
- UT Source for OEM

### ETS嵌入式插件

ETS集成：
- ETS binary for POSIX
- ETS binary for AUTOSAR

ETS源码：
- ETS Source for vSOMEIP
- ETS Source for AUTOSAR
- ETS Source for OEM

非常灵活的配置，能够依据不同客户的需求进行组合：是否购买物理层测试设备、是否购买L2性能测试设备、是否具备UT/ETS的开发与集成能力等

# 测试应用场景



SmartETH产品因其配置灵活性，能够满足非常多的应用场景，以下列举常见使用场景：

**场景1：** 适用于不想做或不需要做L1/L2层测试的客户

## TC8 L3~L7协议一致性测试

需求内容：仅做TCP/IP协议及SOME/IP协议一致性测试,客户在被测样件中已经集成好自行开发的UT及ETS测试代码或者寻求EPT的UT/ETS。不进行物理层及数据链路层测试（通常此两层测试不会进行很多次迭代）

**场景2：** 适用于不想大量投资L1/L2层设备但仍需测试的客户

## TC8 L1~L7协议一致性测试

需求内容:物理层测试服务、数据链路层性能测试服务、TCP/IP协议、SOME/IP协议、DHCP协议一致性测试，且客户的样件没有UT及ETS。

**场景3：** 适用于DoIP协议从应用到底层的一致性测试

## TC8及DoIP协议一致性测试

需求内容：TC8 ETH测试(IPV4/UDP/TCP)及DoIP协议的一致性测试，不包括物理层及数据链路层测试，且客户的样件里没有UT及ETS。

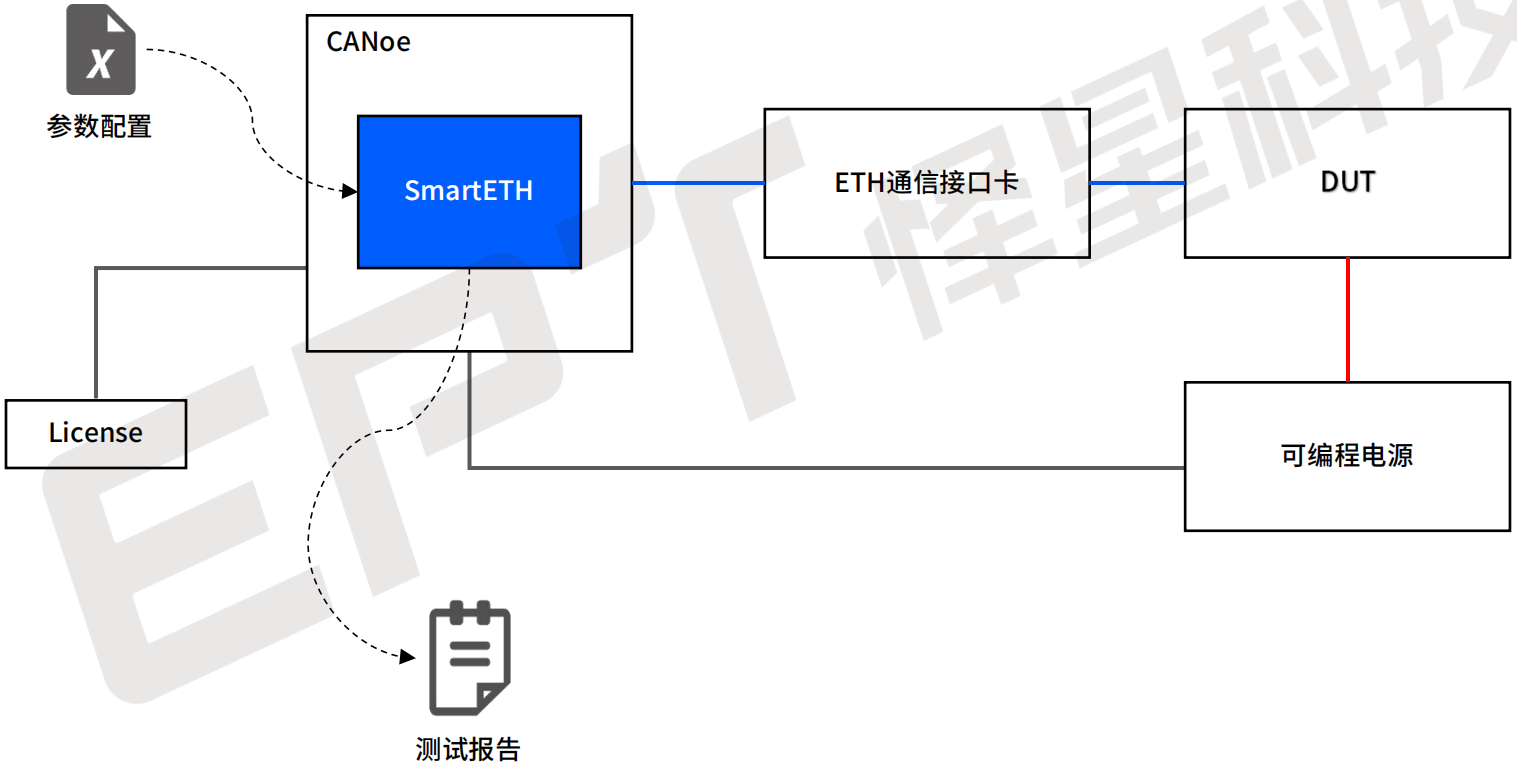
**场景4：** 适用于不想买任何设备，整个测试都外包出去的客户

## 汽车以太网测试服务

需求内容:根据客户样件提供全面的测试服务,输出测试报告。测试项包括:TC8 L3~L7协议一致性测试,L2Switch功能测试,RFC2554/RFC2889交换机性能测试,100BASE-T1/1000BASE-T1IOP和PMA测试。

*可根据客户实际使用场景随意搭配，以满足客户的测试需求。

# SmartETH测试拓扑



# SmartETH产品优势



- ✓ 测试软件严格遵照OPEN Alliance TC8 V3.0标准
- ✓ 不同测试模块使用统一的参数配置入口；对全部参数整理、归纳、分类，降低了软件使用难度和学习成本
- ✓ 灵活勾选测试用例，一键执行
- ✓ 提供与TC8 V3.0步骤一一对应的详细HTML测试报告
- ✓ 支持输出Excel测试报告，并支持定制风格样式
- ✓ 提供高度适配测试软件的UpperTester、SOME/IP-ETS可选产品，提高TC8测试效率
- ✓ 测试软件默认适配怿星推荐的硬件环境(eg.可编程电源、Neptune系列测试系统)，即装即用
- ✓ 软件框架设计巧妙，易于扩增其他通信协议测试，增量升级高效
- ✓ 专业测试工程师团队提供高效、可靠、准确的一站式测试服务

# 总结



- 汽车以太网技术概述
- TCP/IP主要协议介绍
- TC8中的TCP/IP协议测试简介
- SmartETH以太网测试套件简介

EPT 怪星科技

# 让每一台智能汽车都有我们的贡献

小怪助手

微信公众号

咨询邮箱 :mkt@eptcom.com

网 站 : www.e-planet.cn
电 话 : +86 21-53393860
总部地址 : 上海市徐汇区田林路487号宝石园20号楼25层