编程必备基础知识

@咚咚呛

微信搜一搜

了不起的咚咚呛

章节导学

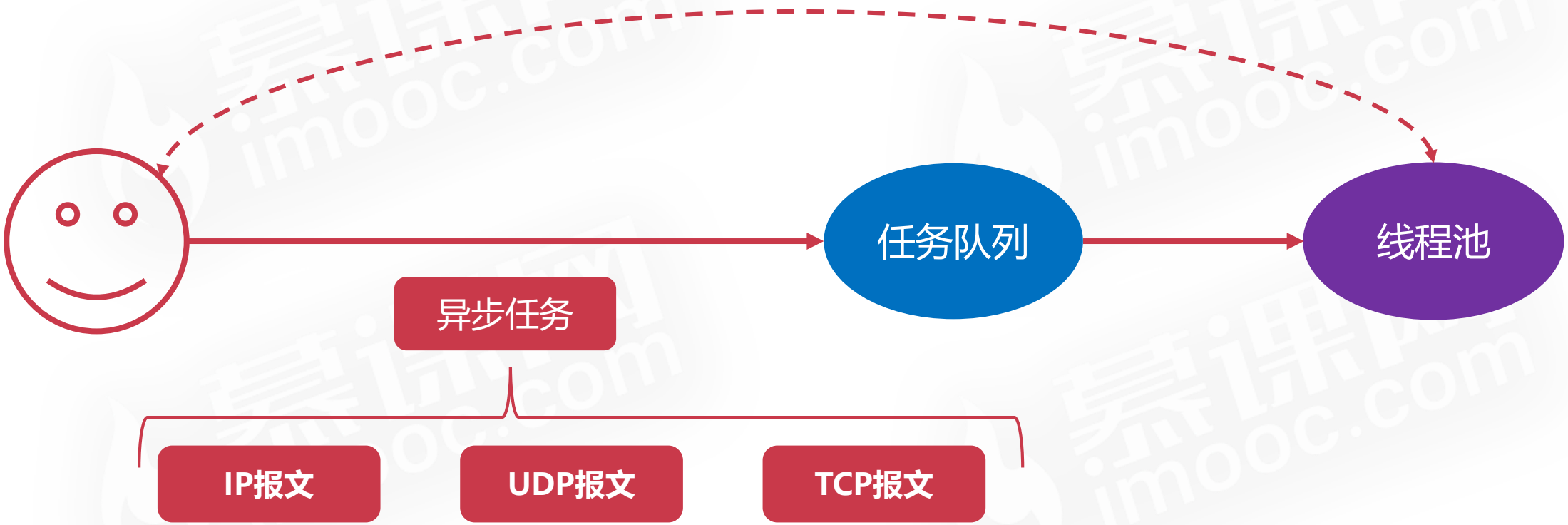
实现网络嗅探工具

章节导学

- IP协议报文
- TCP协议报文
- UDP协议报文

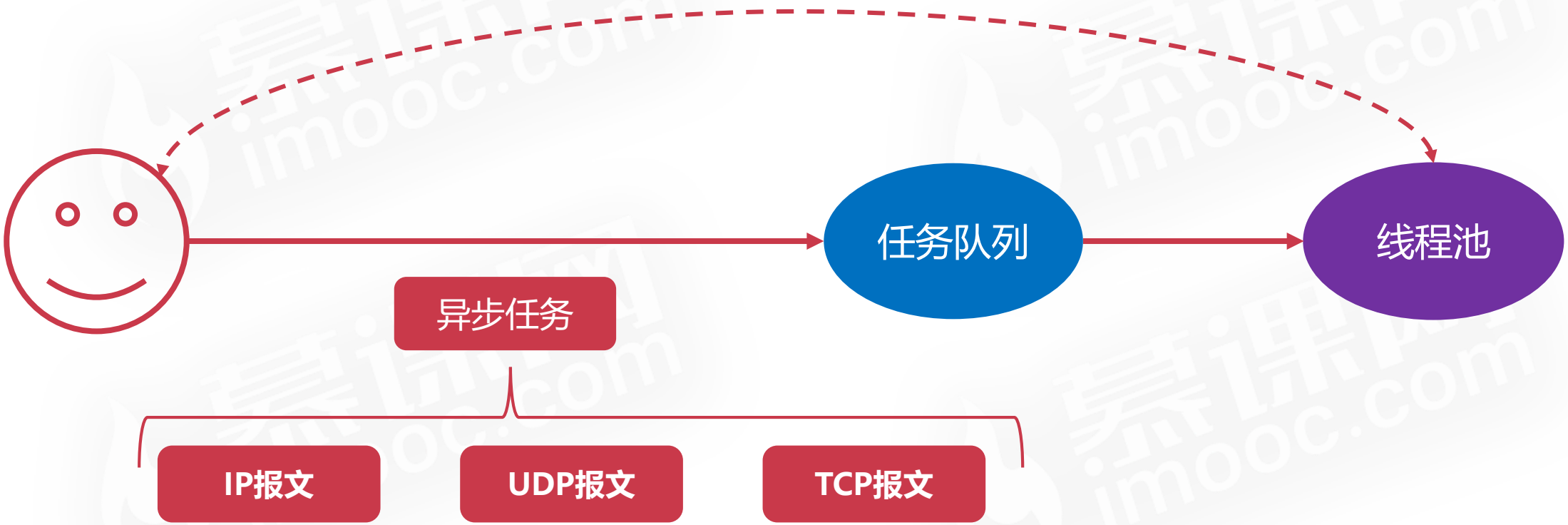
透彻理解网络协议

章节导学



章节导学

搭建服务基本框架



搭建服务基本框架

混杂模式	非混杂模式
接受所有经过网卡设备的数据	只接受目的地址指向自己的数据

Python操作字节序列

字节序

255 = 00000000,11111111

网络 — 大端字节序 — 00000000,11111111

主机 — 小端字节序 — 11111111, 00000000

Python操作字节序列

字节序

- 计算机电路先处理低位字节效率比较高
- 人类习惯读写大端字节序

Python操作字节序列

格式字符

格式字符	类型	例子
%s	字符串	
%d	整数	
%x	十六进制	
%f	浮点数	

Python操作字节序列

格式字符

格式字符	C++/Python类型	标准大小（字节）
B	unsigned char/整数	1
H	unsigned short/整数	2
L	unsigned long/整数	4
s	char[]/字节串	~

实现IP报文解析器

4位版本	4位首部长度	8位服务类型(TOS)	16位总长度(字节)	
16位标识			3位标志	13位片偏移
8位生存时间(TTL)		8位协议	16位首部校验和	
32位源IP地址				
32位目的IP地址				
选项options（若有）				
IP数据				

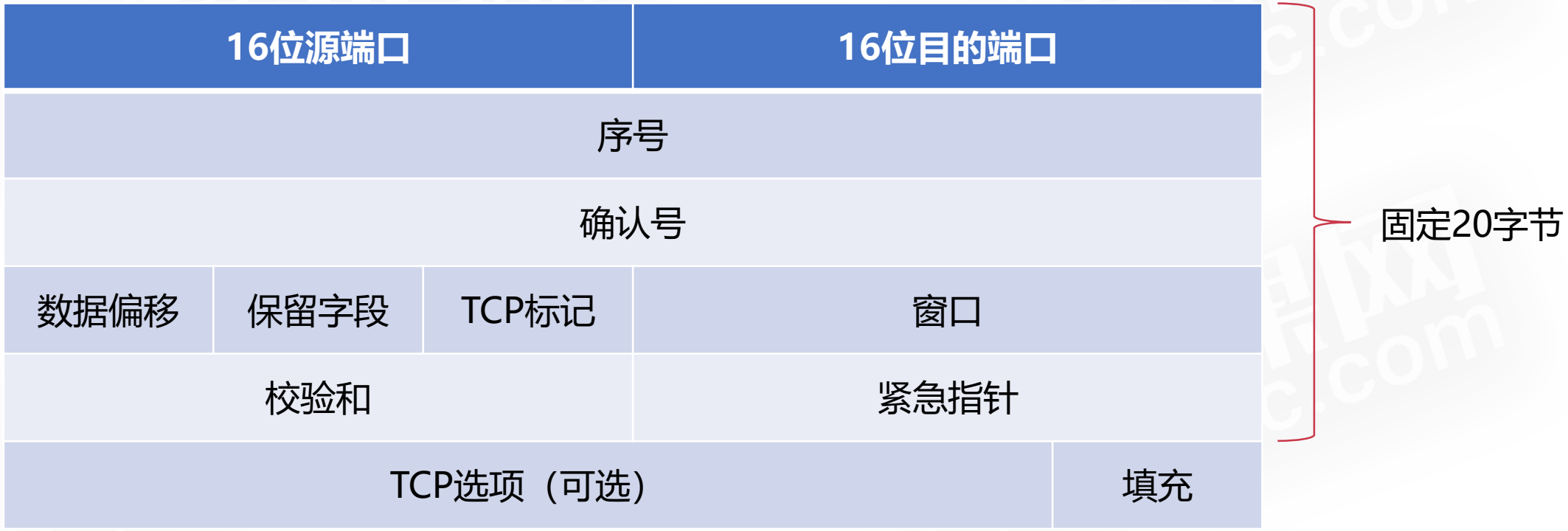
这是用在IPv4头部和IPv6头部的 *下一首部域*的**IP协议号列表**。

十进制	十六进制	关键字	协议
0	0x00	HOPOPT	IPv6逐跳选项
1	0x01	ICMP	互联网控制消息协议（ICMP）
2	0x02	IGMP	因特网组管理协议（IGMP）
3	0x03	GGP	网关对网关协议
4	0x04	IPv4	IPv4 (封装)
5	0x05	ST	因特网流协议
6	0x06	TCP	传输控制协议（TCP）
7	0x07	CBT	有核树组播路由协议
8	0x08	EGP	外部网关协议
9	0x09	IGP	内部网关协议（任意私有内部网关（用于思科的IGRP））
10	0x0A	BBN-RCC-MON	BBN RCC 监视
11	0x0B	NVP-II	网络语音协议
12	0x0C	PUP	Xerox PUP
13	0x0D	ARGUS	ARGUS
14	0x0E	EMCON	EMCON
15	0x0F	XNET	Cross Net Debugger
16	0x10	CHAOS	Chaos
17	0x11	UDP	用户数据报协议（UDP）

实现UDP报文解析器

16位源端口号	16位目的端口号
16位UDP长度	16位UDP校验和
UDP数据	

实现TCP报文解析器



章节回顾

- IP协议报文
- TCP协议报文
- UDP协议报文

透彻理解网络协议