Sniffer 软件的数据捕获与分析操作

1　软件功能

Sniffer 软件是一个功能强大的网络分析工具，主要功能如图 1 所示：

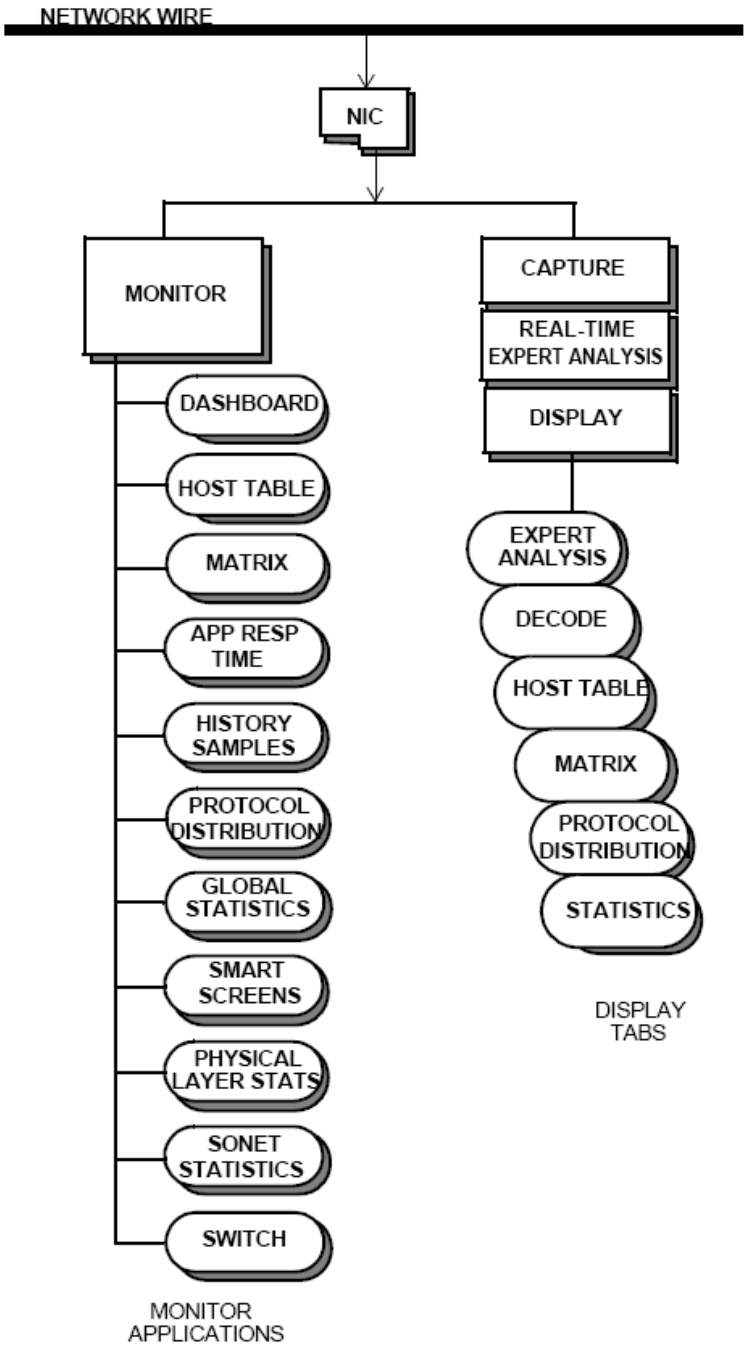


图 1　Sniffer 软件的功能示意图

Sniffer 主要的功能包括：

1) 监控功能（Monitor）：实时监控网络的数据流量。
2) 捕获功能（Capture）：捕获网络流量。
3) 实时专家分析功能（Real-time expert analysis）：详细分析所捕获的数据报文，对潜在的网络故障提供告警功能。
4) 显示功能（Display）：按照协议规定的格式显示所捕获的数据报文。

网络侦听实验主要使用 Sniffer 软件的捕获功能、实时专家分析功能和显示功能，验证 TCP/IP 各协议的原理和交互过程。下面以 Sniffer Pro 4.7 软件为例，介绍 Sniffer 软件捕获、专家分析和显示功能的具体操作过程。

2 软件操作

运行 Sniffer 软件时，首先需要选择捕获和监控计算机哪一个网卡上的网络数据流量，如图 2 所示。

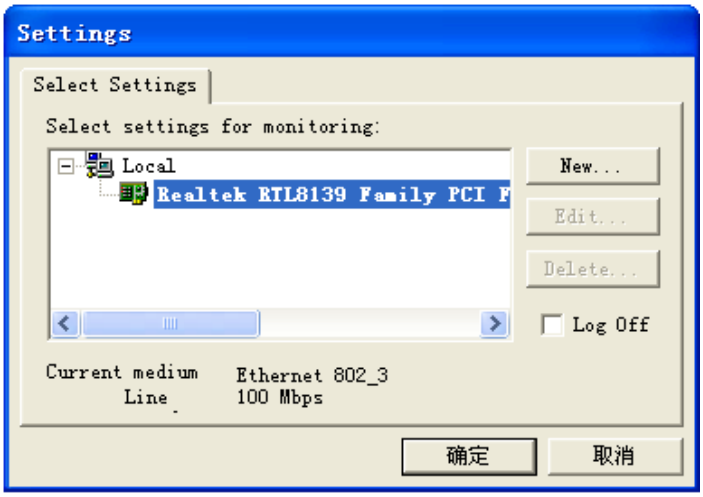


图 2　设置用于捕获数据的网卡

确定所选网卡后，进入 Sniffer 软件的主窗口界面（如图 3 所示），开始进行具体的功能操作。

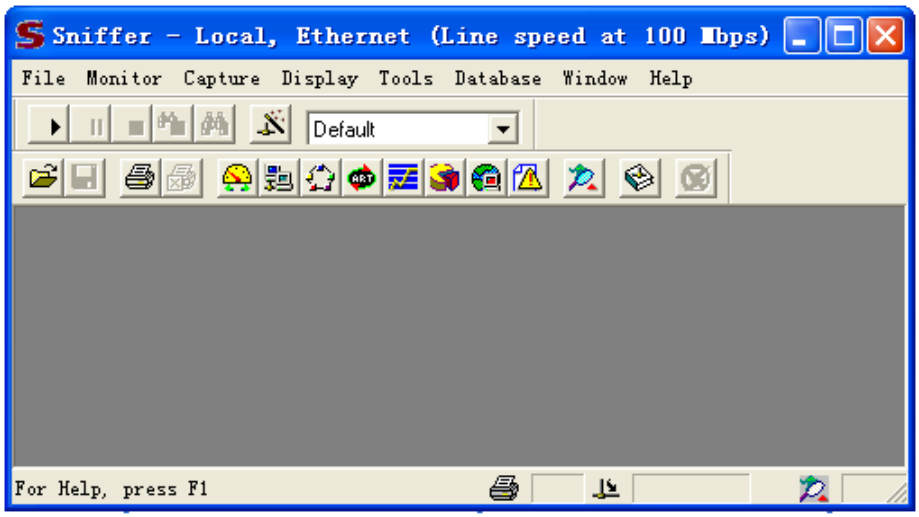
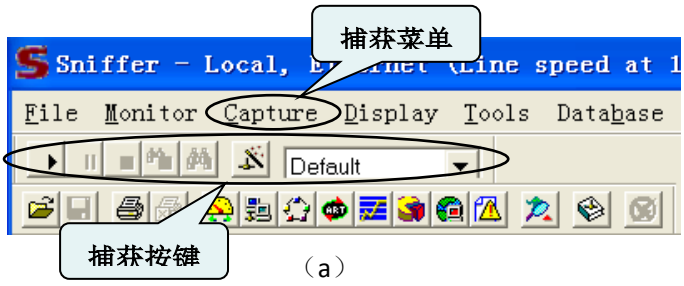


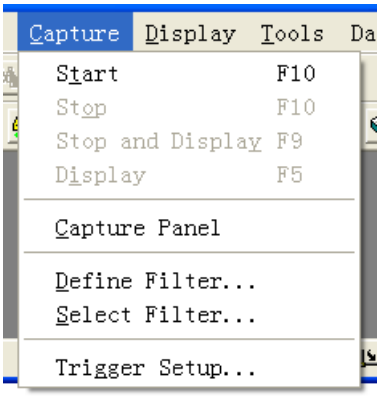
图 3　Sniffer 软件的主窗口界面

2.1数据报文捕获操作

Sniffer 软件捕获功能的操作可以通过其主窗口界面中的捕获菜单或一组捕获按键（如图 4 所示）进行。



（a）



（b）捕获菜单

（c）捕获按键

图 4　Sniffer 软件主窗口界面中的捕获功能实现

下面以捕获按键的操作为例，介绍 Sniffer 软件的数据报文捕获过程。

首先点击“定义捕获条件”按键，在随后弹出的捕获条件定义窗口（如图 5）中设置捕获条件。本课程实验仅使用基本捕获条件（Address）、高级捕获条件（Advanced）和缓冲区设置（Buffer）进行各实验中特定数据报文的捕获操作。

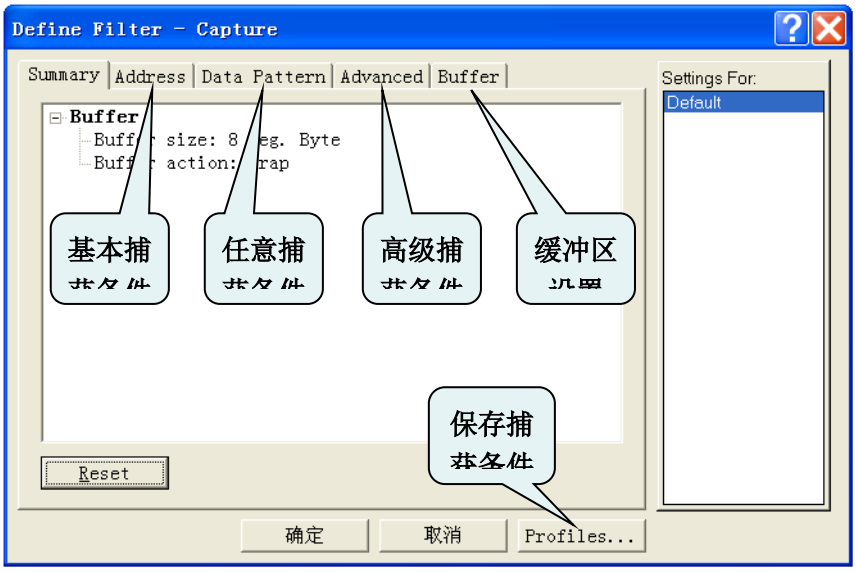


图 5　Sniffer 软件的捕获条件定义窗口

2.1.1 基本捕获条件设置

基本捕获条件用来设置被捕获数据报文的源和目的地址条件（如图 6 所示），主要有两种：

1）链路层捕获，按源和目的物理地址（如 MAC 地址）进行捕获。

2）网络层捕获，按源和目的协议地址（如 IP 地址、IPX 地址）进行捕获。如果选择网络层捕获条件，则 ARP 等报文将被过滤掉。

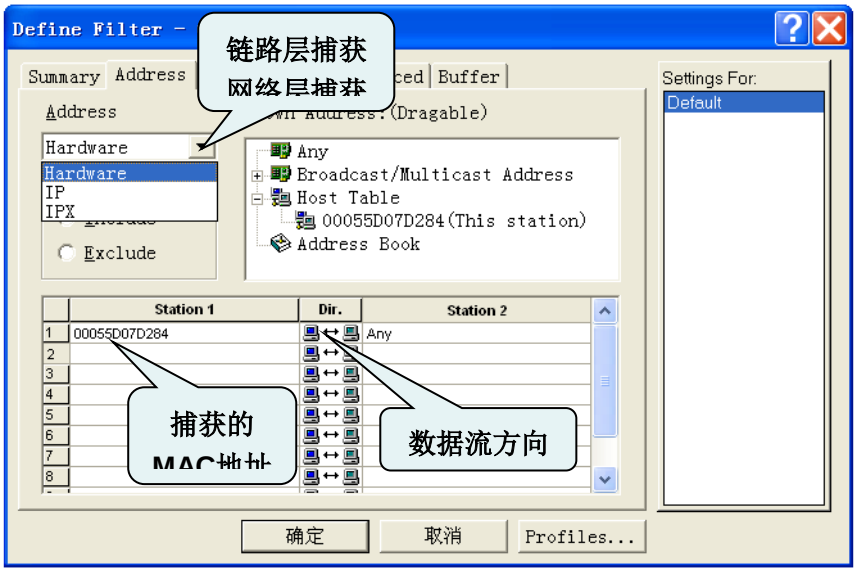


图 6　基本捕获条件设置

2.1.2 高级捕获条件设置

高级捕获条件用来设置被捕获数据报文的协议类型条件，如图 7 所示：

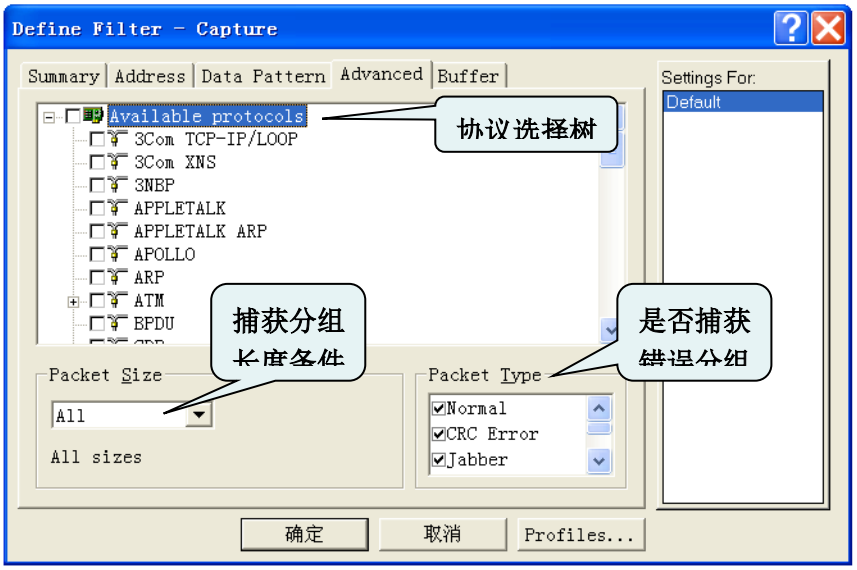


图 7　高级捕获条件设置

在协议选择树中如果不选任何协议，则表示捕获所有协议类型的数据报文。在捕获分组长度条件下，可以捕获等于、小于或大于某个值的分组。在是否捕获错误分组中可以选择当网络上有指定错误时是否进行捕获。

2.1.3 缓冲区设置

缓冲区设置指定用于数据捕获的内存大小、存放数据的文件名和目录等信息。

捕获条件设置完毕后即可使用捕获“开始”按键开始捕获网络数据报文。

捕获过程中可以通过主窗口界面下方状态栏中被捕获的数据报文数量（如图 8 所示），观察是否成功捕获到匹配条件的数据报文。

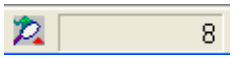


图 8　被捕获的数据报文数量

当观测到有捕获数据时，使用捕获“停止并显示”按键或者“停止”+“显示”按键结束捕获过程。

2.2数据报文分析操作

Sniffer 软件使用专家分析系统（Expert）对捕获的数据报文进行分析与统计，并显示分析统计的结果，如图 9。

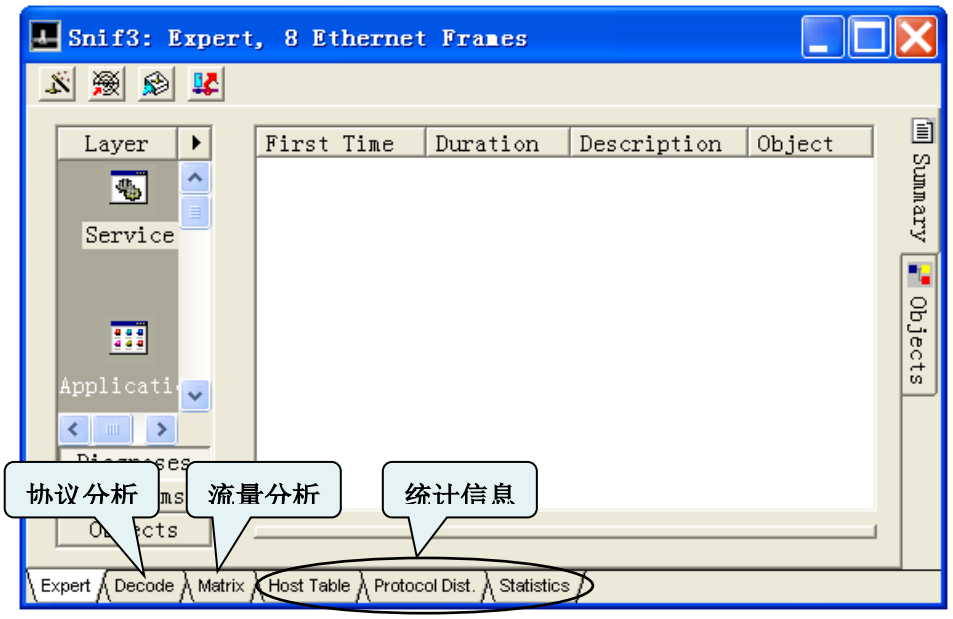


图 9　专家分析系统

本课程实验仅使用专家分析系统中的协议分析（Decode）功能查看各实验中捕获到的数据报文。

Sniffer 软件对捕获报文进行协议分析的结果通常显示为三部分：报文概要、报文解码和十六进制原始报文，如图 10 所示。目前大部分此类软件结构都采用这种结构显示。Sniffer 软件的协议分析内容只是为实验者提供一种辅助手段，实验者必须对协议比较熟悉，才能看懂解析出来的报文。

Snffier 软件对 MAC 地址进行了头部替换，将 MAC 地址中标识制造厂商的前 3 个字节替换成该厂商的名称，这样有利于了解网络上各种相关设备的制造厂商信息。例如将 MAC 地址 0x00055D07D284 替换为 DLink 07D284，表示该地址所标识的网卡由 DLink 制造。

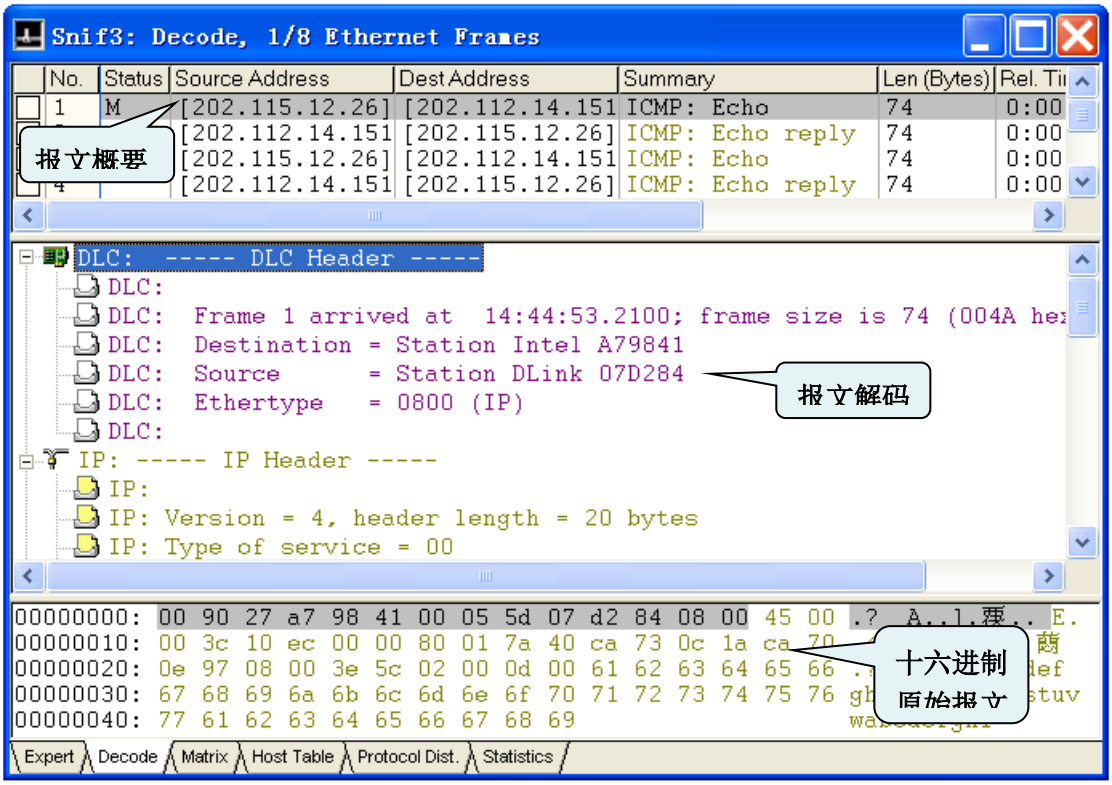


图 10　协议分析

3　协议数据报文格式

本课程实验所捕获的协议数据报文主要涉及：Ethernet 帧、IP 分组、ARP 分组、ICMP 报文、TCP 报文段、RIP 报文和 OSPF 报文。

3.1TCP/IP 协议层次

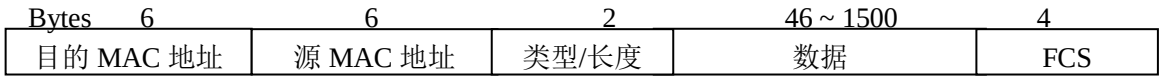
TCP/IP 协议分为四层结构，每一层完成特定的功能，包括多个协议。本课程实验中相关协议的层次分布如图 11 所示。

应用层	RIP、OSPF
运输层	TCP
网际层	IP、ARP、ICMP
网络接口层	底层协议（Ethernet）

图 11　TCP/IP 协议层次

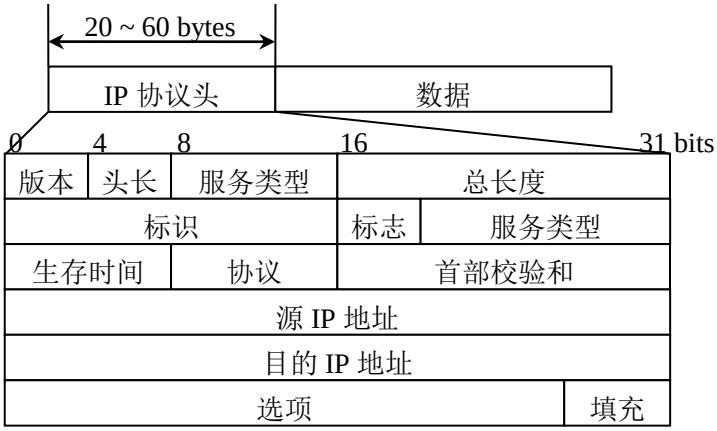
3.1.1 Ethernet 帧格式

最新的 IEEE 802.3 标准（2002 年）中定义 Ethernet 帧格式如下：



其中，类型/长度值小于 1536（0x0600）时表示数据字段的长度，大于等于 1536（0x0600）时表示数据字段的协议类型。类型/长度值 0x0800 表示帧中封装的数据为 IP 分组，类型值 0x0806 表示帧中封装的数据为 ARP 分组。

3.1.2 IP 分组格式（RFC 791）



协议值 1 表示 IP 分组中封装的数据为 ICMP 报文，协议值 6 表示 IP 分组中封装的数据为 TCP 报文段，协议值 17 表示 IP 分组中封装的数据为 UDP 报文。

3.1.3 ARP 分组格式（RFC 826）

注：每行 4 个字节（32bits）。

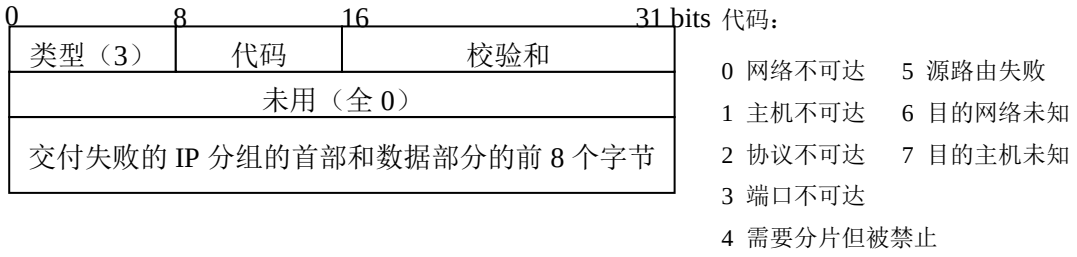
操作代码值 1 表示该分组是 ARP 请求分组，操作代码值 2 表示该分组是 ARP 响应分组。

硬件类型值 1 表示以太网，协议类型值 0x0800 表示 IP 协议。此时，硬件地址即为 6 字节长的 MAC 地址，协议地址即为 4 字节长的 IP 地址。

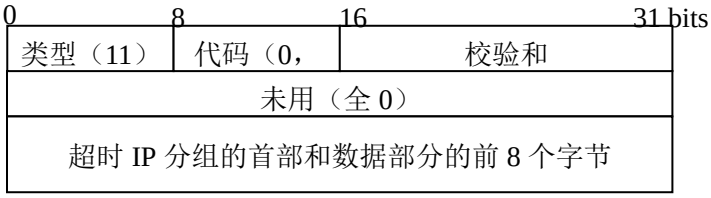
3.1.4 ICMP 报文格式（RFC 792）

ICMP 回送请求和回送应答报文：

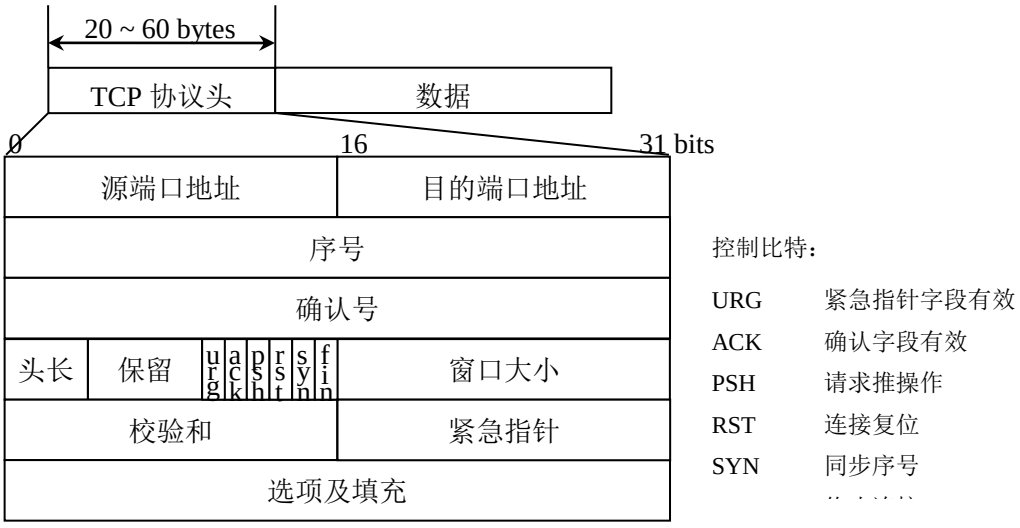
ICMP 目的不可达报文：



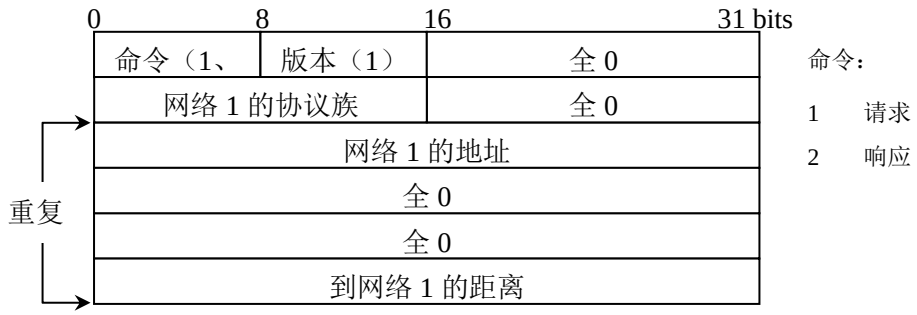
ICMP 超时报文：



3.1.5 TCP 报文段格式（RFC 793）



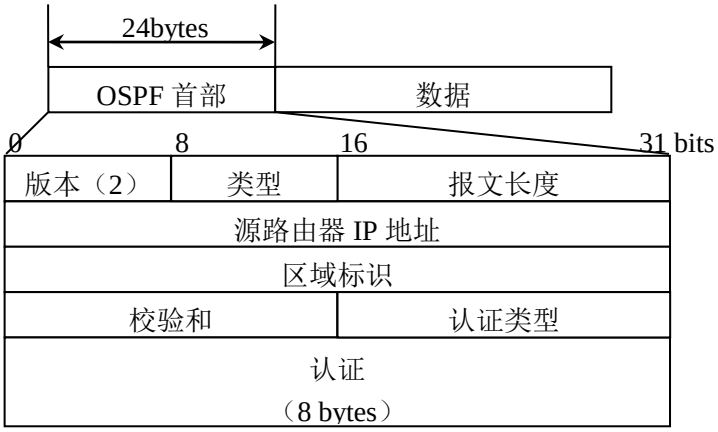
3.1.6 版本 1 的 RIP 报文格式（RFC 1058）



RIP 请求报文在某些 RIP 路由表项超时或路由器刚接入互联网时发送，请求报文可以询问特定路由或所有路由。

路由器在回应请求报文时发送携带被询问路由信息的 RIP 响应报文，也可以定期（30 秒）发送携带整个路由表信息的 RIP 响应报文。

3.1.7 OSPF 报文格式（RFC 2328）



类型：

1 HELLO 报文

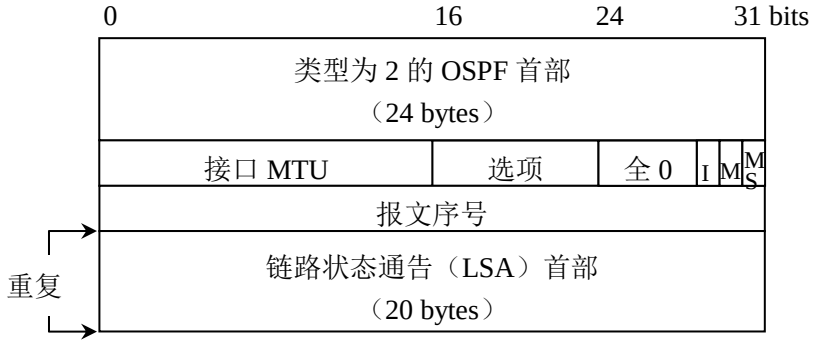
2 数据库描述报文（DBD）

3 链路状态请求报文（LSR）

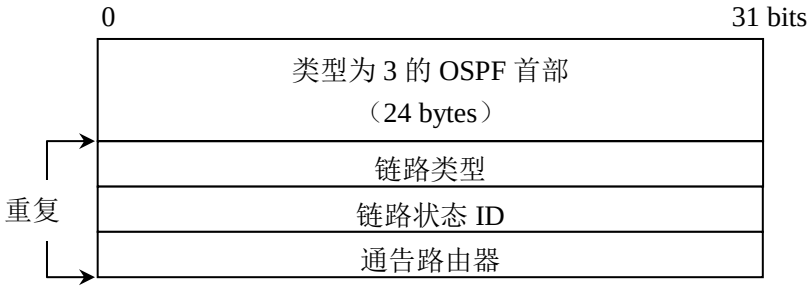
4 链路状态更新报文（LSU）

HELLO 报文：

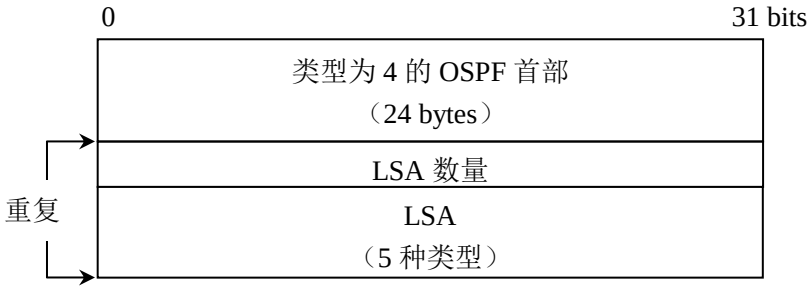
数据库描述（DBD）报文：



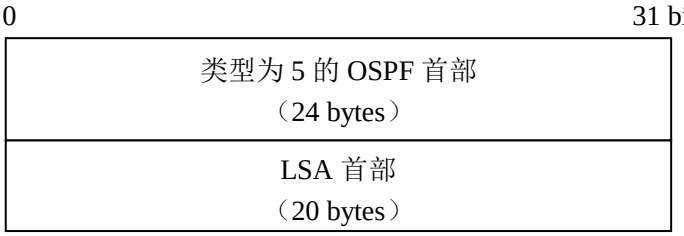
链路状态请求（LSR）报文：



链路状态更新（LSU）报文：



链路状态确认（LSAck）报文：



链路状态通告（LSA）首部：