项目 2 网络安全常用命令及协议分析工具 Sniffer 的应用

- 了解计算机网络协议的基础知识。
- 了解 OSI 模型及安全体系结构。
- 了解 TCP/IP 模型及安全体系结构。
- 掌握常用的网络协议和常用命令。
- 掌握协议分析工具 Sniffer 的使用方法。

某公司拥有数百台计算机组成的企业网，并且公司网络接入了互联网。某日发现公司网络流量增大，有些计算机之间无法通信，公司需要你对公司网络的状态进行分析并排除故障。你作为网络管理人员可以使用网络常用命令和 Sniffer 分析工具对网络故障诊断、协议分析、应用性能分析和网络安全保障等方面进行评估和分析。

第一部分　项目学习引导

2.1　网络安全协议

2.1.1　网络协议

无论是面对面还是通过网络进行的所有通信都要遵守预先确定的规则，即协议。这些协议由会话的特性决定。在日常的个人通信中，通过一种介质（如电话线）通信时采用的规则不一定与使用另一种介质（如邮寄信件）时的协议相同。

规范世界上现存的所有通信方法需要很多种不同的规则或协议。

网络中不同主机之间的成功通信需要在许多不同协议之间进行交互。执行某种通信功能所需的一组内在相关协议称为协议簇。这些协议通过加载到各台主机和网络设备中的软件和硬件执行。

网络协议簇说明了以下过程：

（1）消息的格式或结构。

（2）网络设备共享通往其他网络的通道信息的方法。

（3）设备之间传送错误消息和系统消息的方式与时间。

（4）数据传输会话的建立和终止。

协议簇中单独的协议可能是特定厂商的私有协议。这里所说的私有指的是由一家公司或厂商控制协议的定义及其运作方式。经过拥有者许可，其他组织也可使用某些私有协议。其他私有协议则只能在私有厂商制造的设备上执行。

2.1.2　协议簇及行业标准

组成协议簇的许多协议通常都要参考其他广泛采用的协议或行业标准。标准是指已经受到网络行业认可并经过电气电子工程师协会（IEEE）或 Internet 工程任务组（IETF）之类标准化组织批准的流程或协议。

在协议的开发和实现过程中使用标准可以确保来自不同制造商的产品协同工作，从而获得有效的通信。如果某家制造商没有严格遵守协议，其设备或软件可能就无法与其他制造商生产的产品成功通信。

例如，在数据通信中，如果会话的一端使用控制单向通信的协议，而另一端却采取描述双向通信的协议，那么几乎可以肯定它们之间将无法交换信息。

2.1.3　协议的交互

Web 服务器和 Web 浏览器之间的交互是协议簇在网络通信中的典型应用示例。这种交互在二者之间的信息交换过程中使用了多种协议和标准。各种不同协议共同确保双方都能接收和理解交换的报文。这些协议包括：

1. 应用程序协议

超文本传输协议（HTTP）是一种公共协议，控制 Web 服务器和 Web 客户端进行交互的方式。HTTP 定义了客户端和服务器之间交换的请求和响应的内容与格式。客户端软件和 Web 服务器软件都将 HTTP 作为应用程序的一部分来实现。HTTP 依靠其他协议来控制客户端和服务器之间传输报文的方式。

2. 传输协议

传输控制协议（TCP）是用于管理 Web 服务器与 Web 客户端之间单个会话的传输协议。TCP 将 HTTP 报文划分为要发送到目的客户端的较小片段，称为数据段。它还负责控制服务器和客户端之间交换的报文的大小和传输速率。

3. 网间协议

最常用的网间协议是 Internet 协议（IP）。IP 负责从 TCP 获取格式化数据段，将其封装成数据包、分配相应的地址并选择通往目的主机的最佳路径。

4. 网络访问协议

网络访问协议描述数据链路管理和介质上数据的物理传输两项主要功能。数据链路管理协议接收来自 IP 的数据包并将其封装为适合通过介质传输的格式。物理介质的标准和协议规定了通过介质发送信号的方式以及接收方客户端解释信号的方式。网卡上的收发器负责实施介质所使用的标准。

2.1.4 技术无关协议

网络协议描述的是网络通信期间实现的功能。在面对面交谈的示例中，通信的一项协议可能会规定，为了发出交谈结束的信号，发言者必须保持沉默两秒钟。但是，这项协议并没有规定发言者在这两秒钟内应该如何保持沉默。

协议通常都不会说明如何实现特定的功能。通过仅仅说明特定通信规则所需要的功能是什么，而并不规定这些规则应该如何实现，特定协议的实现就可以与技术无关。

以 Web 服务器为例，HTTP 并没有指定创建浏览器使用什么编程语言、提供网页应该使用什么 Web 服务器软件、软件运行在什么操作系统之上或者显示该浏览器需要满足什么硬件要求。而且，尽管 HTTP 说明了发生错误时服务器应该如何操作，但却并未规定服务器应该如何检测错误。

这就意味着，无论 Web 服务器是哪种类型，使用的是哪种形式的操作系统，计算机和其他设备（如移动电话或 PDA）都可以从 Internet 上的任何位置访问存储于服务器中的网页。

2.2 OSI 参考模型的安全体系

2.2.1 计算机网络体系结构

要形象地显示各种协议之间的交互，通常会使用分层模型。分层模型形象地说明了各层内协议的工作方式及其与上下层之间的交互。每一层实现相对独立的功能，每一层向上一层提供服务，同时接受下一层的服务。每一层不必知道下一层是如何实现的，只要知道下层通过层间的接口提供的服务是什么，以及本层向上层提供什么样的服务，就能独立地设计，这就是常说的网络层次结构。如图 2-1 所示，系统经过分层后，每一层次的功能相对简单且易于实现和维护。此外，某一层需要做改动或被替代时，只要不改变它和上、下层的接口服务关系，则其他层次不会受其影响，因此具有很大的灵活性。使用分层结构，既提供了描述网络功能和能力的通用语言，也有利于同时使用不同厂商的产品，促进竞争。

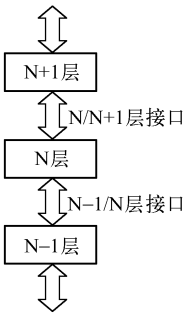

图 2-1 网络的层次结构

参考模型为各类网络协议和服务之间保持一致性提供了通用的参考。参考模型的目的并不是作为一种实现规范，也不是为了提供充分的详细信息来精确定义网络体系结构的服务。学习参考模型的主要用途是帮助读者更清晰地理解网络的功能和过程。

2.2.2 OSI 参考模型简介

开放系统互连参考模型（Open System Interconnection Reference Model，OSI-RM）最初由国际标准化组织（ISO）设计，旨在提供一套开放式系统协议的构建框架。早期网络刚刚出现的时候，很多大型的公司都拥有了网络技术，公司内部计算机可以相互连接，可是却不能与其他公司的计算

机连接。因为没有一个统一的规范，计算机之间相互传输的信息对方不能理解，所以不能互连。而“开放”这个词表示能使任何两个遵守参考模型和有关标准的系统进行互连。

在 OSI 参考模型中，采用了三级抽象，包括体系结构、服务定义和协议规范。OSI 参考模型的体系结构定义了一个 7 层模型，用以进行进程间的通信，并作为一个框架来协调各层标准的制定。OSI 参考模型的服务定义描述了各层所提供的服务，以及层与层之间的抽象接口和用于交互的服务原语；OSI 参考模型各层的协议规范，定义了应当发送何种控制信息及用何种过程来解释该控制信息。

1. OSI 参考模型的层次结构

OSI 参考模型将整个通信网络划分为 7 层，OSI 参考模型如图 2-2 所示，主机 A 和主机 B 可以看成资源子网中的主机，可以参照这个 7 层模型理解整个通信过程。在 OSI 参考模型中，从下到上依次为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。从图 2-2 可以理解数据在网络中传输的详细过程，主机 A 和主机 B 涉及了整个 OSI 参考模型中的 7 层，即资源子网；但在连接部分，一般只需要最低的 3 层（路由）甚至两层（交换）的功能就可以了，即通信子网。OSI 参考模型 7 层的定义和功能如下：

（1）物理层（Physical Layer）：物理层是 OSI 参考模型的最底层，它定义了通信介质的机械特性、电气特性、功能特性和过程特性，是激活、维护和拆除网络设备之间的数据传输而使用的物理连接。

（2）数据链路层（Data Link Layer）：描述了设备之间通过公共介质交换数据帧的方法。数据链路层检测和校正物理层可能发生的错误。数据链路层将从其上层接收的数据包封装成特定格式的数据单元，这种数据单元称为“帧”，在帧中除了数据部分外还附加了一些控制信息，如帧类型、流量控制和差错控制信息等，可以实现数据流控制、差错控制及发送顺序控制等功能。

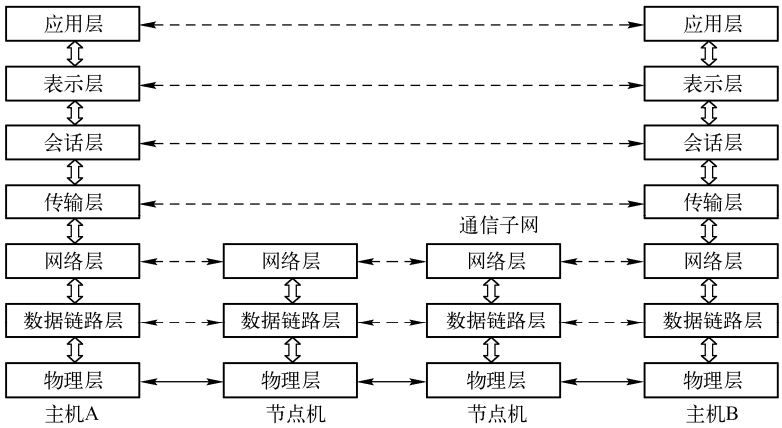

图 2-2　网络通信的 OSI 参考模型

（3）网络层（Network Layer）：网络层主要实现线路交换、路由选择和网络拥塞控制等功能，保证信息包在接收端以准确的顺序接收。

（4）传输层（Transport Layer）：传输层定义了数据分段、重组和传输服务。传输层提供了两端点之间可靠的、透明的数据传输，执行端到端的差错控制、流量控制及管理多路复用。

（5）会话层（Session Layer）：会话层为表示层提供组织对话和管理数据交换的服务。它建立、维护和同步通信设备之间的交互操作，保证每次会话都正常关闭。会话层建立和验证用户之间的连

接，控制数据交换，决定以何种顺序将对话单元传送到传输层，决定传输过程中哪一点需要接收端的确认。

（6）表示层（Presentation Layer）：表示层对应用层服务之间传输的数据规定了通用的表示方式。不同的计算机系统中数据的表示不同，通过表示层的处理可以消除不同实体之间的差异。还可以代表应用进程协商数据表示，完成数据转换、格式化和文本压缩等功能。

（7）应用层（Application Layer）：应用层为不同用户提供实现使用网络服务连接的接口，它直接为网络用户或应用程序提供各种网络服务。应用层提供的网络服务包括文件服务、事物管理服务、网络管理服务、数据库服务等。

2.2.3 ISO/OSI 安全体系

ISO/OSI 安全体系包含 4 部分内容：安全服务、安全机制、安全管理和安全层次，其中安全机制是其核心内容之一。

1. 安全服务

ISO/OSI 安全服务是指计算机网络提供的安全防护措施。国际标准化组织（ISO）定义了以下几种基本的安全服务：认证服务、访问控制、数据机密性服务、数据完整性服务、抗否认服务。

（1）认证服务。

认证可分为对等实体认证和数据源发认证。对等实体认证是指参与通信连接或会话的一方向另一方提供身份证明，接收方通过一定的方式来鉴别实体所提供的身份证明的真实性。数据源发认证是指某个数据的发送者在发送数据时向接收方提交身份证明，这个身份证明同具体的某些数据关联，用于确认接收到的数据的来源的真实性。

（2）访问控制。

访问控制是指只有经过授权的实体才能访问受保护的资源，防止未经授权的实体查看、修改、销毁资源等。访问控制对于保障系统的机密性、完整性、可用性及合法使用具有重要作用。

（3）数据机密性服务。

这种服务就是保护信息不泄露给那些没有授权的实体。包含连接保密、无连接保密、选择字段保密、分组流保密。

（4）数据完整性服务。

这种服务对付主动威胁，保证数据在从起点到终点的传输过程中，如果因为机器故障或人为的原因而造成数据的丢失、被篡改等问题，接收端能够知道或恢复这些改变，从而保证接收到的数据的真实性。数据完整性服务包含可恢复连接完整性、无恢复连接完整性、选择字段连接完整性、无连接完整性、选择字段无连接完整性。

（5）抗否认服务。

“否认”是指参与通信的一方事后不承认曾发生过本次信息交换，常见于电子商务中。数字签名就是针对这种威胁的。

2. 安全机制

ISO 7408-2 中制定了支持安全服务的 8 种安全机制，分别如下：

（1）加密机制（Enciphermant Mechanisms）。

加密就是对数据进行密码变换以产生密文。利用加密机制可以提供数据的安全保密，也可以提

供通信的保密。

（2）数字签名机制（Digital Signature Mechanisms）。

数字签名是对附加在数据单元上的一些数据，或是对数据单元所做的密码变换，这种变换可以使数据单元的接收者确认数据单元的来源和完整性，并使发送者能有效地保护数据，防止被人伪造。

（3）访问控制（Access Control Mechanisms）。

访问控制是依据实体所具有的权限，对实体提出的资源访问请求加以控制。访问控制机制依据该实体已鉴别的身份，或使用有关该实体的信息及该实体的权利进行。

（4）数据完整性（Data Intergrity Mechanisms）。

数据完整性机制保证接收者能够鉴别收到的消息是否为发送者发送的原始数据。

（5）鉴别交换机制（Authentication Mechanisms）。

这种机制可提供对等实体鉴别，在鉴别实体时得到否定的结果，就会导致连接被拒绝或终止，或在安全审计跟踪中增加一个记录，或向安全管理中心报警。

（6）通信流量填充机制（Traffic Padding Mechanisms）。

通信流量填充机制用来防止攻击者通过对通信双方的数据流量分析，根据流量的变化来推出一些有用的信息或线索。

（7）路由选择控制机制（Routing Control Mechanisms）。

路由选择控制机制是发送者对数据通过网络的路径加以控制，选择相对安全的网络节点，以提高信息的安全性。

（8）公证机制（Notarization Mechanisms）。

公证机制是指由通信各方都信任的第三方来确保数据的完整性，以及数据源、时间及目的地的正确性。

安全服务基本机制直接保护计算机网络安全，但真正实现这些机制必须有下面一些机制的配合，使安全服务满足用户需求。这些机制的实现与网络层次没有必然的联系，它们侧重于安全管理方面，主要包括：安全机制可信度评估、安全标识、安全审计、安全响应与恢复。安全服务与安全机制的关系见表 2-1。

表 2-1　安全机制与安全服务关系表（“√”代表该机制提供此安全服务）

安全机制 / 安全服务	加密	数字签名	访问控制	数据完整性	鉴别交换	通信流量填充	路由选择控制	公证机制
对等协议实体鉴别	√	√			√			
数据源鉴别	√	√						
访问控制服务			√					
连接保密	√						√	
无连接保密	√						√	
选择字段保密	√							
分组流保密					√	√		
可恢复连接完整性	√			√				
无恢复连接完整性	√			√				

续表

安全服务 \ 安全机制	加密	数字签名	访问控制	数据完整性	鉴别交换	通信流量填充	路由选择控制	公证机制
选择字段连接完整性	√			√				
无连接完整性	√	√		√				
选择字段无连接完整性		√		√				
数字签名		√		√				

3. 安全管理

ISO/OSI 安全管理分为系统安全管理、安全服务管理和安全机制管理 3 个部分。

系统安全管理包括安全策略管理、事件处理管理、安全审计管理、安全恢复管理等。安全服务管理包括为服务决定与指派目标安全保护、指定与维护选择规则、为选择的安全服务而特定的安全机制、对那些需要事先取得管理同意的可用安全机制进行协商、通过适当的按机制管理功能调用特定的安全机制。安全机制管理包括密钥管理、加密管理、数字签名管理、访问控制管理、数据完整性管理、鉴别管理、通信业务填充管理、路由选择控制管理和公证管理等。

4. 安全层次

ISO/OSI 安全体系是通过在不同的网络层上分布不同的安全机制来实现的，这些安全机制是为了满足相应的安全服务所必须选择的，其在不同网络层上的分布见表 2-2。

表 2-2 安全服务与 OSI 层次关系表

安全服务 \ OSI 层次	1	2	3	4	5	6	7
对等协议实体鉴别			√	√		√	
数据源鉴别			√	√			√
访问控制服务			√	√		√	√
连接保密	√	√	√	√		√	
无连接保密		√	√	√		√	
选择字段保密							√
分组流保密	√		√				√
可恢复连接完整性				√			
无恢复连接完整性			√	√		√	
选择字段连接完整性						√	
无连接完整性			√	√		√	
选择字段无连接完整性						√	
数字签名						√	

OSI 的安全体系主要是针对网络协议的有关部分，相对于保证网络安全来说，可能是不完整的。当前主要使用的网络系统是 Internet 或基于 TCP/IP 参考模型的 Intranet 等，因此，基于 TCP/IP 参考模型的网络安全显得更为重要。

2.3　TCP/IP 参考模型的安全体系

2.3.1　TCP/IP 参考模型

根据 OSI 参考模型可以说明构成 TCP/IP 协议簇的协议。TCP/IP 参考模型与 OSI 参考模型的对应关系如图 2-3 所示。在 OSI 参考模型中，TCP/IP 参考模型中的网络接入层和应用层被进一步划分，用于说明这些协议层需要实现的详细功能。

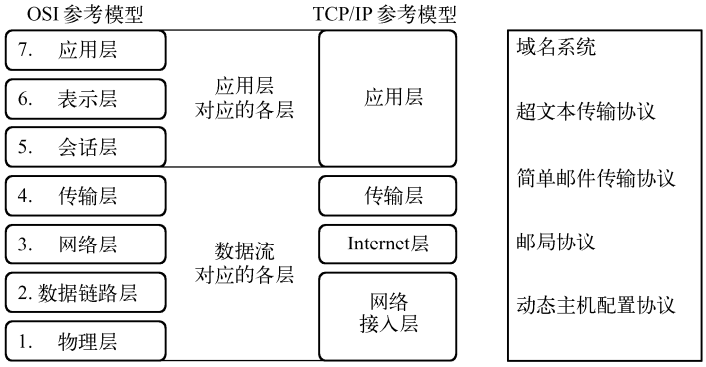

图 2-3　TCP/IP 参考模型与 OSI 参考模型的对应关系

TCP/IP 协议簇在网络接入层并没有指定通过物理介质传输时使用的协议，而只是描述了从 Internet 层到物理网络协议的传递。而 OSI 参考模型第 1 层和第 2 层则论述了接入介质所需的步骤以及通过网络发送数据的物理手段。

这两个网络模型之间主要的相似之处在于它们的第 3 层和第 4 层。OSI 参考模型第 3 层是网络层，几乎全部用于论述和记录发生在所有数据网络中的用于编址并在网际网络中路由消息的过程。Internet 协议（IP）是 TCP/IP 协议簇中包含第 3 层所述功能的协议。

OSI 参考模型的第 4 层是传输层，通常用于描述管理源主机和目的主机之间各个会话的一般服务或功能。这些功能包括确认、错误恢复和定序。传输控制协议（TCP）和用户数据报协议（UDP）这两个 TCP/IP 提供了这一层需要的功能。

TCP/IP 参考模型的应用层包括许多协议，为各种最终用户应用程序提供特定功能。OSI 参考模型第 5 层、第 6 层和第 7 层供应用程序软件开发人员和厂商参考，用于生产需要访问网络进行通信的产品。

TCP/IP 参考模型中各层功能如下：

（1）应用层：是用户访问网络的界面。包括一些向用户提供的常用应用程序，如电子邮件、Web 浏览器、文件传输、远程登录等，也包括用户在传输层之上建立的自己的应用程序。

（2）传输层：负责实现源主机和目的主机上的实体之间的通信。它提供了两种服务：一种是可靠的、面向连接的服务（TCP）；一种是无连接的数据报服务（UDP）。为了实现可靠传输，要在会话时建立连接，对数据包进行校验和收发确认，通信完成后再拆除连接。

（3）Internet 层：负责数据包的路由选择，保证数据包能顺利到达指定的目的地。一个报文的不同分组可能通过不同的路径到达目的地，因此要对报文分组加一个顺序标识符，以使目标主机接收到所有分组后，可以按序号将分组装配起来，恢复原报文。

（4）网络接入层：负责接收 IP 数据包并通过网络传输介质发送数据包。

2.3.2 TCP/IP 参考模型的安全体系

1. 网络接入层安全

对于 OSI 参考模型的物理层，可以在通信线路上采用某些防窃听技术使得搭线窃听变得不可能或者不容易被窃听者监测到；数据链路层上，点对点的链路可以采用硬件实现方案，使用通信加密设备进行加密和解密。网络接入层安全主要是针对数据链路层安全的。

基于数据链路层在网络通信中所处的位置，它不可能提供真正的终端用户级认证，也不能在合理成本下提供网络内用户间的保密性，仅提供网络接入层安全机制对终端用户来说还是不安全的。例如，限制设备的信息流等防火墙之类的功能，应在数据链路层加密机制之前设置。

数据链路层保护有一定的局限性，但有些保护机制和高层相比更容易在此层实现。第一种是通信安全机制，如防范 MAC 地址泛洪攻击、针对 STP 的攻击等，就必须采用这种安全机制；第二种是高层不拥有的安全机制，如针对隐通道方面的安全机制，隐通道是指系统的一个用户以违反系统安全策略的方式传送信息给另外一个用户的机制。任何利用非正常的通信手段在网络中传递信息，从而突破网络安全机制的通道都可以称做隐通道。在 TCP/IP 协议簇中，在设计上有些安全方面的缺陷，由于这些缺陷的存在，网络隐通道才能够建立成功。在协议中，有很多设计得不严密的地方，可以用来秘密地隐藏信息，这就给建立隐通道秘密传输信息提供了场所。隐通道的存在会对网络的安全构成威胁，数据包中任何字节的改变或传输参数的任何变化都是潜在的隐通道。数据链路层保护可以有效地取出诸如传输信息长度、时间以及地址的隐通道。

除此之外，数据链路层系统设计较为简单，与其他层相比更容易达到预期目标。

2. Internet 层安全

Internet 层安全主要是为了保证 IP 数据包能够正确地发往目的地，攻击者可能通过修改网络的操作以达到他们的攻击目的，数据包有可能被路由器发往错误的地方。

网络中的路由器对路由表的维护一般采用的是动态路由机制，它依赖路由器的两个最基本的功能：一是路由表的维护；另一个是路由器之间适时的路由信息交换。因此，路由表和路由信息的准确性和完整性对 IP 网络来说是相当关键的，路由表的完整正确与否直接关系到能否连接到目的设备并有效使用网络资源。

保证路由器间更新信息的完整性也很重要。路由器更新信息是由路由协议来实现的，常见的路由协议有 RIPv2、OSPF、EIGRP 等。无论采取何种协议，都要确保路由更新信息在网络上传送时不会被修改。同时，路由器的内部也需要完整性机制。路由器可以采用设置不同级别的访问并授予相应的权限等方式以防止非授权用户的非法修改，确保路由表信息的准确性。另外，还需要认证机制，以确保非授权的路由更新信息插入网络。

在新一代的互联网协议 IPv6 包头设计中，对原 IPv4 包头所做的一项重要改进就是将所有可选字段移出 IPv6 包头，置于扩展头中。由于除 Hop-by-Hop 选项扩展头外，其他扩展头不受中转路由器检查或处理，这样就能提高路由器处理包含选项的 IPv6 分组的性能。通常，一个典型的 IPv6 包

没有扩展头。仅当需要路由器或目的节点做某些特殊处理时，才由发送方添加一个或多个扩展头。

目前，RFC2460 中定义了 6 个 IPv6 扩展头，其中认证包头提供数据源认证、数据完整性检查和反重播保护。ESP（Encapsulating Security Payload）协议包头提供加密服务。当认证和加密两者都需要时，可以将它们结合起来使用。

Internet 层安全性的主要特点是它的透明性，对同一目的地址的数据包，按照同样的加密密钥和访问控制策略来处理。也就是说，对属于不同进程的包不做区别。Internet 层非常适合提供基于主机的安全服务。

3. *传输层安全*

传输层提供 TCP 和 UDP 两种服务，TCP 提供可靠的面向连接的服务，UDP 提供无连接的服务。传输层的安全主要针对端对端的数据传输。确保传输层安全的相应协议有 SSL、TLS、SOCKS、WTLS 等。

由于在 TCP/IP 中没有加密、安全认证等安全机制，所以 Netscape 研发了 SSL（Secure Socket Layer）协议，用以保障在 Internet 上数据传输的安全。SSL 协议位于 TCP 与应用层协议之间，为数据通信提供安全支持。SSL 协议可分为两层：SSL 记录协议（SSL Record Protocol），它建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持；SSL 握手协议（SSL Handshake Protocol），它建立在 SSL 记录协议之上，用于在实际的数据传输开始前，对通信双方进行身份认证、协商加密算法、交换加密密钥等。

TLS（Transport Layer Security）协议包括两个协议组——TLS 记录协议和 TLS 握手协议。TLS 记录协议是一种分层协议，每一层中的信息可能包含长度、描述和内容等字段。TLS 记录协议支持信息传输、将数据分段到可处理块、压缩数据、应用 MAC、加密以及传输结果等；对接收到的数据进行解密、校验、解压缩、重组等，然后将它们传送到高层客户机。TLS 握手协议由 3 个子协议组构成，允许对等双方在记录层的安全参数上达成一致、自我认证、协商安全参数、互相报告出错条件。

相对于网络层的安全机制，传输层安全机制是基于进程和进程之间的安全服务和加密传输信道，它不具备透明性。只要应用到传输层安全协议（如 SSL），就必定要对其他层次进行若干修改，以增加相应的功能，并使用稍微不同的进程间通信界面。它的实现涉及公钥体系，安全强度高，支持用户选择的加密算法。缺点是它所涉及的公钥和私钥用户很难记忆，需要通过其他方式加以保存。

4. *应用层安全*

应用层是直接面向用户的，TCP/IP 的应用层协议很多，常见的运行在网络层的安全协议有 Telnet、FTP、SMTP 和 HTTP 等。正是这些应用层协议将 TCP/IP 的优势发挥出来，使 Internet 的内容丰富多彩。而网络接入层与网络层是无法对所传送的不同内容的安全要求予以区别对待的。如果确实想区分具体文件的不同安全性要求，就必须在应用层采用安全机制。例如，Internet 蠕虫和 Melissa 病毒利用了邮件服务器不检查传送邮件信息内容，若发送大量的请求容易导致正常请求不能响应的弱点。面对这些威胁，低层的协议安全功能一般达不到对安全的要求，只有应用层是唯一能够提供这种安全服务的层次，以下是有关应用层安全的相关实例：

（1）利用其他软件实现对已有应用层协议安全功能的扩展。

如 PEM（Privacy Enhanced Mail，增强保密的邮件），用户使用本地 PEM 软件以及 PSE 环境信息生成 PEM 邮件，然后通过基于 SMTP 的报文传递代理（MTA）发给对方。接收方在自身的 PSE 中将报文解密，并通过目录检索其证件，查阅证件注销表以核实证件的有效性。

（2）提供文件级别的安全机制。

S-HTTP（Secure Hypertext Transfer Protocol）是 Web 上使用的超文本传输协议（HTTP）的安全增强版本，它与 HTTP 相兼容，但是要实现 S-HTTP 的安全特性，必须是服务器与客户机同时使用 S-HTTP。S-HTTP 提供了完整且灵活的加密算法、模态及相关参数。使用 S-HTTP，敏感的数据信息不会以明文形式在网络上发送。

（3）提供多种安全服务的安全协议。

SET 协议（Secure Electronic Transaction），被称为安全电子交易协议，是由 Master Card 和 Visa 联合 Netscape、Microsoft 等公司，推出的一种新的电子支付模型。SET 协议是 B2C 上基于信用卡支付模式而设计的，它保证了开放网络上使用信用卡进行在线购物的安全。SET 协议主要是为了解决消费者、商家、银行之间通过信用卡的交易而设计的，由于 SET 协议提供了消费者、商家和银行之间的认证，确保了交易数据的安全性、完整可靠性和交易的不可否认性，特别是保证不将消费者银行卡号暴露给商家等优点，因此它成为了目前公认的信用卡/借记卡的网上交易的国际安全标准。

2.4 常用网络协议和服务

2.4.1 常用网络协议

1. IP

IP（Internet Protocol）是为计算机网络相互进行通信而设计的协议。在 Internet 中，它是能使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在 Internet 上进行通信时应当遵守的规则。IP 数据报的结构为：IP 头加数据，IP 头包括一个 20 字节的固定长度部分和一个可选的任意长度部分，其结构如图 2-4 所示（图中数字代表长度大小，单位为位），其中包含的各个字段含义如下：

- 版本：IP 的版本。通信双方使用的 IP 版本必须一致。目前广泛使用的 IP 版本号为 4（即 IPv4）。关于 IPv6，目前还处于草案阶段（4 位）。
- 报头长度：指定数据报报头的大小（4 位）。

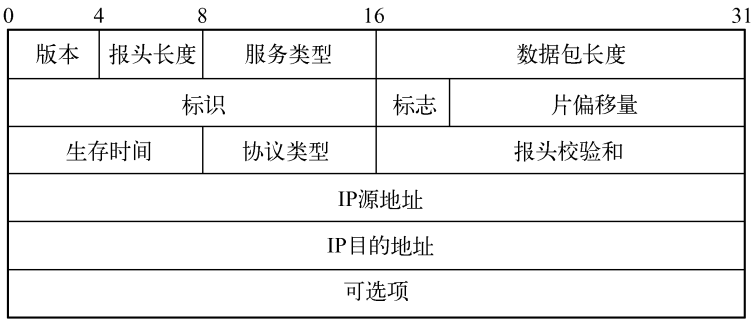

图 2-4 IP 数据报头结构

- 服务类型：服务类型字段包含一个 8 位二进制值，用于确定每个数据包的优先级别（8 位）。
- 数据包长度：此字段以字节为单位，提供了包括报头和数据在内的整个数据包的大小（16 位）。
- 标识：此字段主要用于唯一标识原始 IP 数据包的数据片（16 位）。
- 标志：占 3 位，第 1 个未用，第 2 个为 DF，第 3 个为 MF（3 位）。

不分片（DF）标志：不分片（DF） 标志是标志字段中的一个位，表示不允许对数据包分片。如果设置了不分片标志位，则表示不允许对此数据包分片。如果路由器必须对数据包分片后才能将其向下传送到数据链路层，但此时 DF 位却设置为 1，则该路由器将丢弃此数据包。

更多片（MF）标志：更多片（MF） 标志是标志字段中的一个位，与片偏移量共同用于数据包的分片和重建。如果设置了更多片标志位，则表示这并非数据包的最后一个数据片。当接收方主机收到 MF = 1 的数据包时，会检查片偏移量以便了解此数据片在重建的数据包中应放置的位置。当接收方主机收到 MF = 0 且片偏移量中的值非零的帧时，会将该数据片作为重建的数据包的最后一部分放置。未分片数据包的分片信息全部为零（MF = 0，片偏移量= 0）。

- 片偏移量：片偏移量字段用于标识数据包的数据片在重建时的放置顺序。当路由器从一种介质向具有较小 MTU 的另一种介质转发数据包时必须将数据包分片。如果出现分片的情况，IPv4 数据包会在到达目的主机时使用 IP 报头中的片偏移量字段和 MF 标志来重建数据包（13 位）。
- 生存时间：生存时间（TTL）是一个 8 位二进制值，表示数据报的剩余“寿命”。数据报每经过一个路由器（即每一跳）处理，TTL 值便至少减 1。当该值变为零时，路由器会丢弃数据报并从网络数据流量中将其删除。此机制可以防止无法到达其目的地的数据在路由环路中的路由器之间无限期转发。如果允许路由环路继续，网络将会因永远也无法到达目的地的数据报而出现堵塞。在每一跳处减少 TTL 值可以确保该值最终变为 0 并且丢弃 TTL 字段过期的数据报（8 位）。
- 协议类型：表示数据报传送的数据负载类型。网络层参照协议字段将数据传送到相应的上层协议（8 位）。

典型的值如下：

01：ICMP　　06：TCP　　17：UDP

- 报头校验和：报头校验和字段用于对数据包报头执行差错校验（16 位）。
- IP 源地址：IP 源地址字段包含一个 32 位二进制值，代表数据包源主机的网络层地址（32 位）。
- IP 目的地址：IP 目的地址字段包含一个 32 位二进制值，代表数据包目的主机的网络层地址（32 位）。
- 可选项：IPv4 报头中为提供其他服务另行准备了一些字段，但这些字段极少使用（可变长度）。

2. TCP

TCP（Transmission Control Protocol）是一种面向连接的、可靠的、基于字节流的传输层（Transport Layer）通信协议。

发送和接收方 TCP 实体以数据段（Segment）的形式交换数据。一个数据段包含一个固定的

20 字节的头和任意长度的可选部分。TCP 的头的结构如图 2-5 所示，各个字段的含义如下：

- 源端口：长度为 16 位的源端口字段的值为初始化通信的端口号。
- 目的端口：长度为 16 位的目的端口字段的值为传输的端口号。
- 顺序号：发送方向接收方发送的封包的顺序号，长度为 32 位。TCP 连接上的每个字节均有它自己的 32 位的顺序号，顺序号经过一段时间（如一个小时或更长）后会出现重复。
- 确认号：发送方希望接收的下一个封包的顺序号，长度为 32 位。

<table>
<tr><td colspan="8">源端口</td><td colspan="2">目的端口</td></tr>
<tr><td colspan="10">顺序号</td></tr>
<tr><td colspan="10">确认号</td></tr>
<tr><td>TCP
头
长</td><td></td><td>U
R
G</td><td>A
C
K</td><td>P
S
H</td><td>R
S
T</td><td>S
Y
N</td><td>F
I
N</td><td colspan="2">窗口大小</td></tr>
<tr><td colspan="8">校验和</td><td colspan="2">紧急指针</td></tr>
<tr><td colspan="10">可选项（0或更多的32位字）</td></tr>
</table>

图 2-5　TCP 头结构图

- TCP 头长：表明 TCP 头包含多少个 32 位字，长度为 4 位。

接下来的 6 位未用，再接下来的 6 个标识位长度各为 1 位。

- URG：是否使用紧急指针。

  1：使用；

  0：不使用。
- ACK：是请求状态还是应答状态。

  1：应答，则确认号有效；

  0：请求，则确认号被忽略。
- PSH：PSH=1，表示接收方请求的数据收到后立刻送往应用程序而不必等到缓冲区满。
- RST：用于复位由于主机崩溃或其他原因而出现的错误连接。常用于拒绝非法的数据或非法的连接请求。
- SYN：用于建立连接。在连接请求中，SYN=1，ACK=0，表示连接请求；SYN=1，ACK=1，表示连接被接受。
- FIN：用于释放连接。它表明发送方已没有数据发送了。
- 窗口大小：实现流量控制的字段，表示接收方想收到的每个 TCP 数据段的大小。若该字段值为 0 则表示希望发送方暂停发送数据。长度为 16 位。
- 校验和：对整个数据包的校验和。长度为 16 位。
- 紧急指针：当 URG 为 1 时才有效，是发送紧急数据的一种方式。长度为 16 位。
- 可选项：用于提供一种增加额外设置的方法，这种设置在常规的 TCP 包中是不包括的。

3. UDP

UDP 向应用程序提供了一种无连接的服务，通常用于每次传输量较小或有实时需要的程序，在这种情况下，使用 UDP 开销较小，避免频繁建立和释放连接的麻烦。

一个 UDP 数据段包括一个 8 字节的头和数据部分，如图 2-6 所示。

UDP 头只包括 4 个字段，每个字段的长度为 16 位。

图 2-6　UDP 头结构

- 源端口、目的端口的作用与 TCP 中的相同。
- 封包长度：UDP 头和数据的总长度。
- 校验和：与 TCP 头中的校验和一样，不仅对头数据进行检验，还对包的内容进行校验。

2.4.2　常用网络服务

1. 活动目录

活动目录（Active Directory，AD）是面向 Windows Standard Server、Windows Enterprise Server 以及 Windows Datacenter Server 的目录服务。活动目录不能运行在 Windows Web Server 上，但是可以通过它对运行 Windows Web Server 的计算机进行管理。活动目录存储了有关网络对象的信息，并且让管理员和用户能够轻松地查找和使用这些信息。活动目录使用了一种结构化的数据存储方式，并以此作为基础对目录信息进行合乎逻辑的分层组织。

活动目录服务是 Windows 平台的核心组件，它为用户管理网络环境各个组成要素的标识和关系提供了一种有力的手段。

2. WWW 服务

WWW 服务是目前最常用的服务，使用 HTTP，默认端口为 80。使用 Apache 可以在 Linux/UNIX/Windows 2003 上架设 Web 服务器，在 Windows 下，一般使用 IIS 作为 Web 服务器。

用户通过浏览器可以方便地访问处于世界上任何地方的 Web 服务器上的网页，网页包含了文本、图片、语音、动画等各种文件。

3. 电子邮件

电子邮件（E-mail）是目前较流行和最基本的网络服务之一。

电子邮件地址的格式由 3 部分组成。第 1 部分“用户名”代表用户信箱的账号，对于同一个邮件接收服务器来说，这个账号必须是唯一的；第 2 部分“@”是分隔符；第 3 部分是用户信箱的邮件接收服务器域名，用以标识其所在的位置。

电子邮件系统由客户端软件和邮件服务端软件组成。电子邮件系统的工作方式遵循客户机/服务器（C/S）模式。使用电子邮件服务的每个用户必须在一个邮件服务器上申请一个电子邮箱。邮件服务器管理着众多的客户电子邮箱。

目前，电子邮件服务使用的两个最主要的协议是简单邮件传输协议（SMTP）和邮局协议（POP3）。SMTP 默认使用 25 号端口，用于发送邮件；POP3 使用 110 号端口，用来接收邮件。

SMTP 是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。它是以明文方式进行传输的，存在着较大的安全隐患。

POP3 允许用户从服务器上把邮件存储到本地主机（即用户自己的计算机）上，同时根据客户端的操作，删除或保存邮件服务器上的邮件。

4. Telnet

Telnet 是一种 Internet 远程终端访问服务，使用 23 号端口。它能够以字符方式模仿远程终端登录远程服务器，访问服务器上的资源。Telnet 是以明文方式发送信息的，也存在较大的安全隐患。

要建立一个到远程主机的对话，只需在命令提示符下输入命令：Telnet　远程主机　IP 地址（远

程主机名）。用户也可以用具有图形界面的 Telnet 客户端程序与远程主机建立 Telnet 连接。

5. FTP

FTP（File Transfer Protocol，文件传输协议）的主要作用是让用户连接到一个远程计算机（运行着 FTP 服务器程序），查看远程计算机上文件，把文件从远程计算机上下载到本地计算机或把本地计算机文件上传到远程计算机中。FTP 服务的端口为 21（20）。

与大多数 Internet 服务一样，FTP 的工作方式也遵循 C/S 模式。FTP 从远程计算机复制文件时实际上启动了两个程序：一个是本地计算机上的 FTP 客户程序，它向 FTP 服务器提出复制文件的请求；另一个是启动在远程计算机上的 FTP 服务器程序，它响应复制请求并把指定的文件传送到本地计算机中。FTP 客户程序有字符界面和图形界面两种。字符界面的 FTP 的命令复杂、繁多。图形界面的 FTP 客户程序，操作简洁方便。

使用 FTP 时必须先登录，在远程计算机上获得相应的权限以后，方可上传或下载文件。也就是说，要想向哪一台计算机传送文件，就必须具有哪一台计算机的适当授权。换言之，除非拥有用户 ID 和密码，否则便无法传送文件。Internet 上的 FTP 主机有很多，不可能要求每个用户在每一台主机上都拥有账号，匿名 FTP 就是为了解决这个问题而产生的。用户可以使用 anonymous 作为用户 ID，E-mail 地址作为密码连接到提供了匿名 FTP 服务的远程主机上，并下载文件，而无须成为其注册用户。

为了安全起见，不要往匿名 FTP 服务器上存放机密文件。

6. DNS

DNS 是域名系统（Domain Name System）的缩写，它是由解析器和域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应 IP 地址，并具有将域名转换为 IP 地址功能的服务器。其中域名必须对应一个 IP 地址，而 IP 地址不一定有域名。域名系统采用类似目录树的等级结构。域名服务器为客户机/服务器模式中的服务器方，它主要有两种形式：主服务器和转发服务器。将域名映射为 IP 地址的过程就称为“域名解析”。在 Internet 上，域名与 IP 地址之间是一对一（或者多对一）的，域名虽然便于人们记忆，但机器之间只是互相认识 IP 地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。

2.5 Windows 常用的网络命令

Windows 操作系统自带有许多网络命令，它们虽然简单，但是却可以实现强大的功能。下面介绍一些常用的网络命令。

2.5.1 ping 命令

这个命令用来检测当前主机与目的主机之间的连通情况，它是 ICMP 使用的一个实例。使用 ping 进行测试，如果 ping 运行正确，大体上就可以排除网络访问层、网卡的输入输出线路、电缆和路由器等存在的故障，从而减小了问题的范围。但由于可以自定义所发数据报的大小及无休止的高速发送，ping 也被某些别有用心的人作为 DDoS（分布式拒绝服务攻击）的工具。

ping 命令的格式如图 2-7 所示（在命令行状态下输入 ping 即可显示其格式及参数的说明）。

其中的常用参数说明如下：

-t：使当前主机不断地向目的主机发送数据，直到使用 Ctrl+C 组合键中断。

-n：执行特定次数的 ping 命令，其中 count 为正整数值。

-l size：指定发送的数据包的大小，而不是默认的 32 字节。

ping 命令格式为：ping 主机名-t。如图 2-8 所示，如果 ping 某一网站，如 www.yahoo.com，出现“Reply from 72.30.2.43:bytes=32 time=182ms TTL=53”则表示本地主机与该网站的 IP 级连接是畅通的。其中“72.30.2.43”是对方的 IP 地址，“bytes=32”表示数据包大小为 32 个字节，“time=182ms”表示完成命令所花时间为 182ms。“TTL=53”表示生存时间。

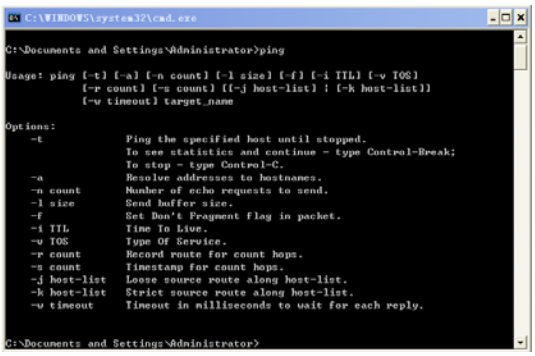

图 2-7　ping 命令参数

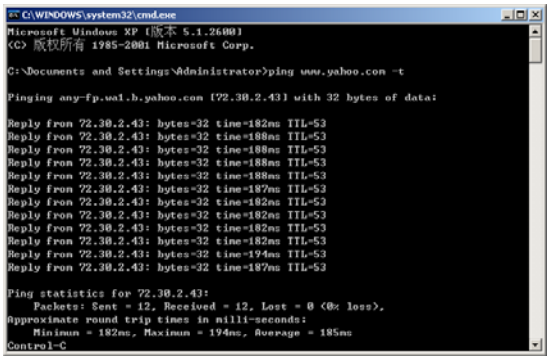

图 2-8　带参数-t 的 ping 命令

TTL 是 IP 包中的一个值，它告诉网络中的设备包在网络中的时间是否太长而应被丢弃。有很多原因使包在一定时间内不能被传递到目的地。例如，不正确的路由表可能导致包的无限循环。一个解决方法就是在一段时间后丢弃这个包，然后给发送者一个报文，由发送者决定是否重发。TTL 的初值通常是系统默认值，是包头中的 8 位的域。TTL 的最初设想是确定一个时间范围，超过此时间就把包丢弃。由于每个路由器都至少要把 TTL 域减 1，TTL 通常表示包在被丢弃前最多能经过的路由器个数。当计数到 0 时，路由器决定丢弃该包，并发送一个 ICMP 报文给最初的发送者。

如果出现如图 2-9 所示的提示，则说明本地 DNS 配置有问题或 DNS 服务器无此域名信息。

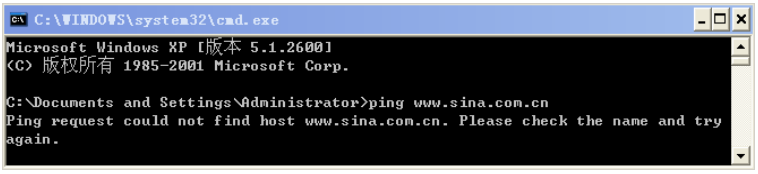

图 2-9　DNS 查找不到目标

如果出现“Request timed out”，如图 2-10 所示，则表示此时发送的数据包不能到达目的地，可能有以下两种情况：一种是网络不通；另一种是此时网络连通状况不佳。

默认情况下，在出现“Request timed out”之前，ping 会等待 1000ms（1s）的时间让每个响应返回。如果通过 ping 探测的目标系统经由时间延迟较长的链路，如卫星链路，则响应可能会花更长的时间才能返回。此时可以使用-w（等待）参数选项指定更长时间的超时。

如果执行 ping 命令不成功，则可以预测故障出现在以下几个方面：网线是否连通、网络适配

器是否安装正确、IP 地址是否可用等；如果执行 ping 命令成功而网络仍无法使用，那么问题很可能出在网络系统的软件配置方面，执行 ping 命令成功只能保证当前主机与目的主机间存在一条连通的物理路径。

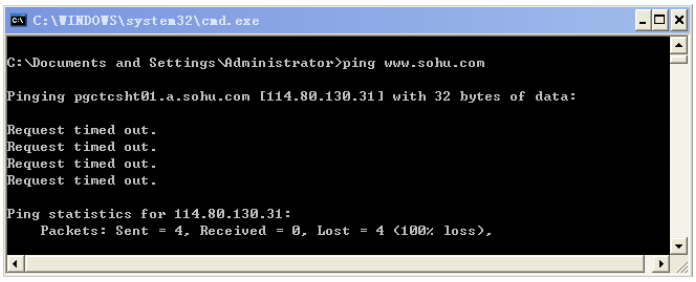

图 2-10　ping 不通目标

另外，由于 ping 命令可以被攻击者用来收集主机信息和作为攻击的手段，因此，出于安全的考虑，许多主机的防火墙配置了“拒绝外部的 ICMP 信息包”这样的规则，这样的主机也是无法 ping 到的。例如，使用“ping www.sohu.com”，返回信息可能为“Request timed out”，看起来好像该主机不可达，而实际上可以通过浏览器访问该网站。

2.5.2　at 命令

这个命令的作用是安排在特定的日期或时间执行某个特定的命令或程序。当知道要运行命令主机的当前时间，就可以使用此命令让其在以后的某个时间去执行某个程序或命令。具体用法和参数，如图 2-11 所示。

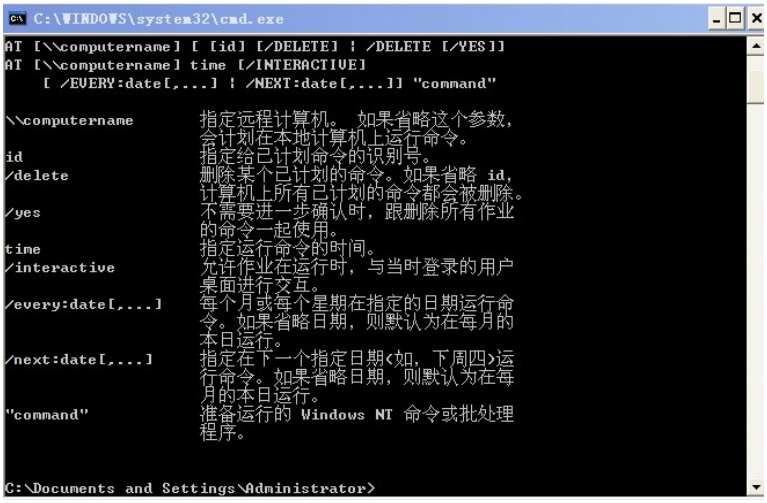

图 2-11　at 命令参数

图 2-12 就是利用 at 命令实现计算机定时关机，如设定关机时间为 17:00。at 命令的执行与用户权限以及相关的服务有关。如果在执行过程中提示“服务尚未启动”，则需开启服务中的“Task Scheduler”选项。

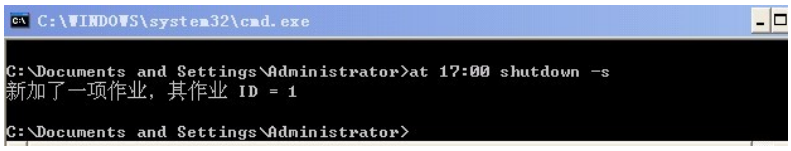

图 2-12　at 命令使用示例

2.5.3　netstat 命令

netstat 命令可以用来显示当前的 TCP/IP 连接、Ethernet 统计信息、路由表等。netstat 命令的格式如下：

```
netstat[-a][-e][-n][-o][-s][-p proto][-r][interval]
```

-s：按照各个协议分别显示其统计数据。如果用户的应用程序（如 Web 浏览器）运行速度比较慢，或者不能显示 Web 页之类的数据，那么就可以用本选项来查看一下所显示的信息。

需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。图 2-13 显示了当前计算机协议的统计信息（图中统计信息未显示完）。

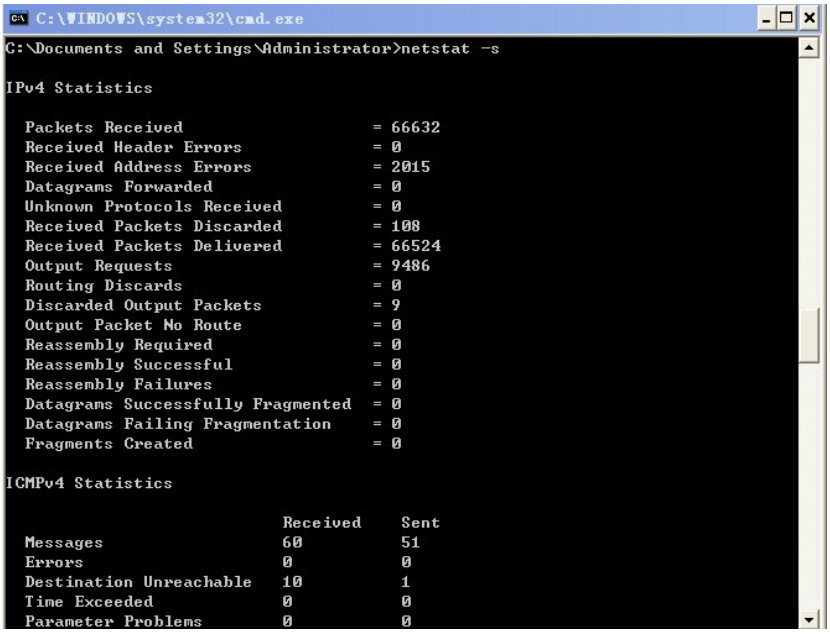

图 2-13　netstat 命令查看协议统计信息

-e：显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数，以及数据报的数量和广播的数量。

-r：显示关于路由表的信息，类似于使用 route print 命令时显示的信息。除了显示有效路由外，还显示当前有效的连接。

-a：显示一个所有的有效连接信息列表，包括已建立的连接（ESTABLISHED），也包括监听连接请求（LISTENING）的那些连接。

-n：显示所有已建立的有效连接。

从图 2-14 中可以看到，计算机打开许多端口，其中有些端口的状态为“LISTENING”，表示该端口处于监听状态，没有和其他计算机建立连接；而有的端口状态为“ESTABLISHED”，表明该端口正与某计算机进行通信。

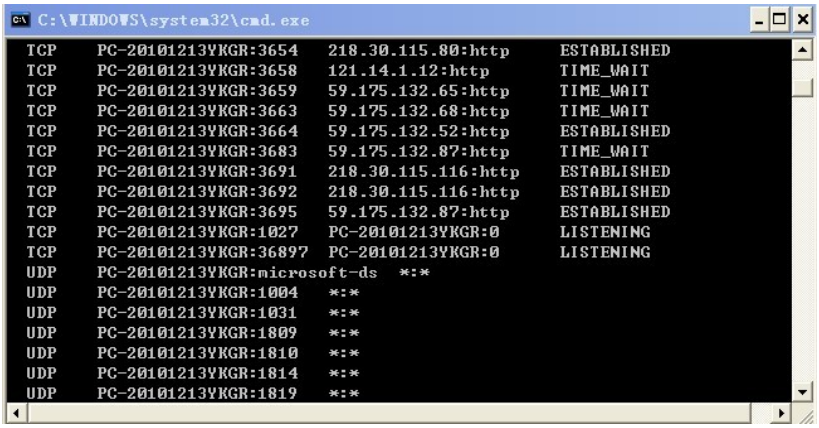

图 2-14　netstat-a 命令输出示例

2.5.4　tracert 命令

当数据报从本地经过多个网关传送到目的地时，tracert 命令可以用来跟踪数据报使用的路由（路径）。该程序跟踪的路径是源计算机到目的地的一条路径，tracert 命令诊断程序确定到目标所采取的路由。

tracert 命令的使用是在后面加上一个 IP 地址或 url，tracert 命令会进行相应的域名解析。tracert 命令一般用来检测故障的位置，可以用 tracert 命令测试在哪个环节上出了问题。

tracert 命令的用法示例如图 2-15 所示。从图 2-15 中可以看出，经过了 59.172.218.219 这个网络节点后显示请求超时，而这个时候本机又是能够访问该网站的，说明 tracert 命令相关的协议服务被该网络节点拒绝了。

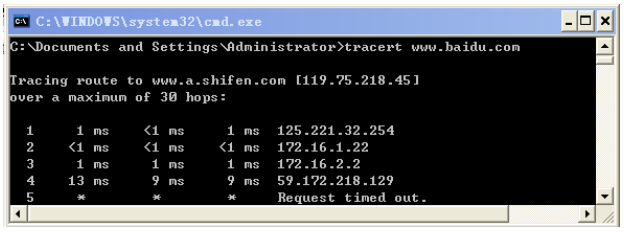

图 2-15　tracert 命令示例

2.5.5　net 命令

net 命令中有很多函数用于配置部分本地操作系统的常用选项和核查计算机之间的 NetBIOS 连接，输入 net /?，然后按 Enter 键，显示该命令的用法：

```
net[accounts | computer | config | continue | file | group | help | helpmsg | localgroup | name | pause | print | send | session | share | start | statistics | stop | time | use | user | view]
```

1. net start　<service name>

启动本地主机或远程主机上的服务。输入“net start telnet”，就可以启动本机上的 telnet 服务，如图 2-16 所示。

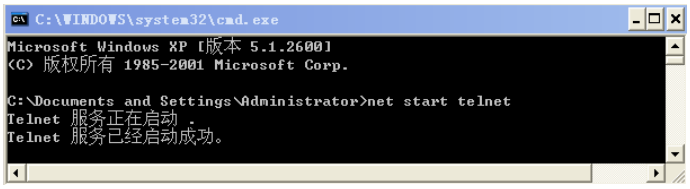

图 2-16　启动 telnet 服务

2. net stop　<service name>

停止本地或远程主机上已开启的服务。输入“net stop server”，就可以停止 server 及与之关联的服务，如图 2-17 所示。

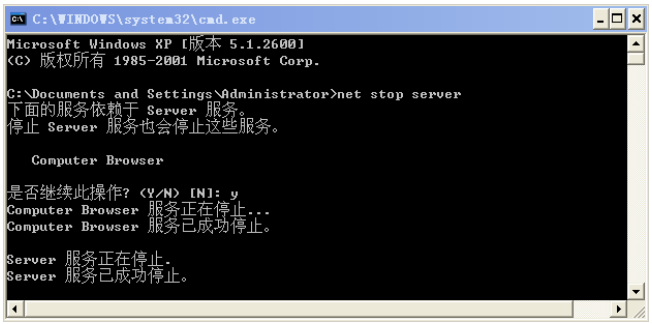

图 2-17　停止某个服务

3. net user

执行和账户相关的一些操作，包括新建账户、删除账户、查看特定账户、激活账户、禁用账户等。输入不带参数的“net user”命令，可以查看所有账户，如图 2-18 所示。

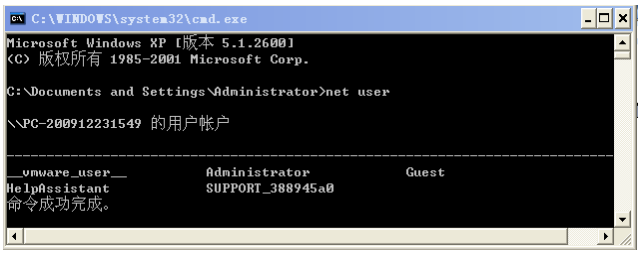

图 2-18　显示所有账户

（1）创建新账户。“net user peter 123456 /add”命令：表示新建一个账户名为 peter，密码为 123456，默认为 user 组成员，如图 2-19 所示。

（2）删除账户。“net user peter /del”命令：表示将账户名为 peter 的账户删除，如图 2-19 所示。

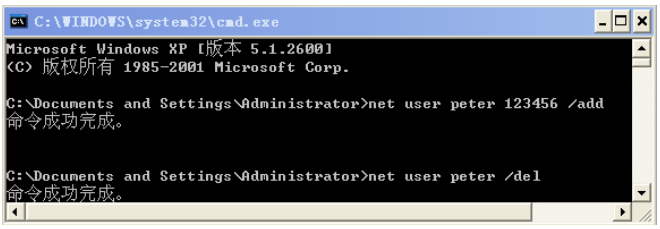

图 2-19　添加、删除账户

（3）禁用某个账户。假设 john 为一个已存在的账户，使用命令：net user john /active:no，可将账户名为 john 的账户禁用，如图 2-20 所示。

（4）激活某个账户。“net user john /active:yes”命令：表示激活账户名为 john 的账户，如图 2-20 所示。

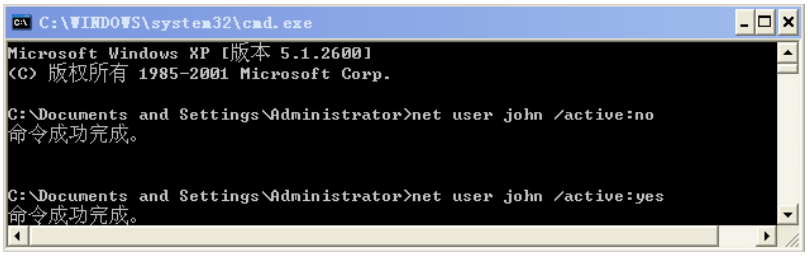

图 2-20　禁用、激活账户

（5）查看账户信息。“net user john”命令，表示查看账户名为 john 的用户的情况，包括账户的状态、密码有效期、所属组和上次登录时间等。

4. net localgroup

查看所有和用户组有关的信息以及进行的相关操作。不带参数的“net localgroup”命令可列出当前所有的用户组。可以把某个账户提升为 administrators 组成员，用法为：net localgroup groupname username/add。例如，把账户 john 添加到管理员组中去，可使用命令：net loaclgroup administrators john /add，john 就成为管理员组的成员，获得了管理员的权限。使用命令：net localgroup administrators john /del，就可以把 john 这个账户从管理员组中删除。使用“net localgroup groupname”命令，本例中的 groupname 为 administrators，可查看组信息，以及该组包含的成员。以上命令如图 2-21 所示。

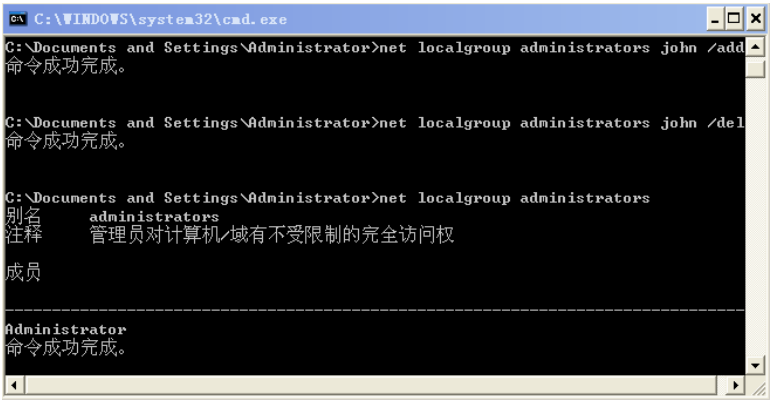

图 2-21　net localgroup 命令示例

2.5.6　ftp 命令

基本的 ftp 命令使用方法为：首先在命令行中输入 ftp，然后按 Enter 键（也可直接添加对方 IP 地址或完全域名登录），也可以输入“help”来查看帮助（任何 DOS 命令都可以用此方法查看命令帮助）。

接下来是登录过程，直接在 ftp 的提示符下输入“open 主机 IP 地址 ftp 端口”命令格式，然后按 Enter 键即可，默认端口都是 21，可以不写。提示输入合法的用户名和密码进行登录，若以匿名 ftp 登录，可在 User 提示符后面输入 anonymous，并在 password 提示符后面输入一个邮件地址为密码。ftp 命令示例如图 2-22 所示。

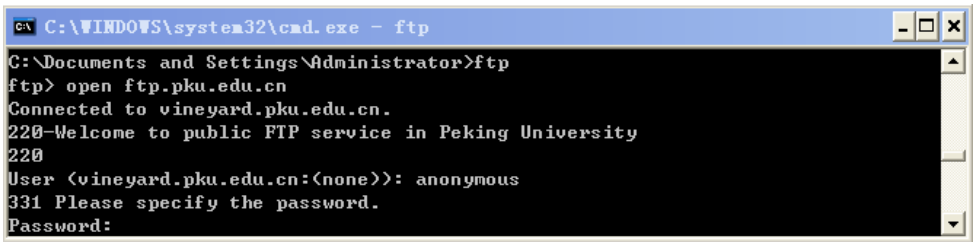

图 2-22　使用 ftp 命令

使用 ftp 命令登录后，可使用如下命令进行操作：

dir：和 DOS 命令一样，用于查看服务器的文件，直接输入 dir，然后按 Enter 键，就可以看到此 ftp 服务器上的文件，如图 2-23 所示。

cd：进入某个文件夹。

get：下载文件到本地计算机。

put：上传文件到文件服务器（需要远程服务器配置相应权限）。

delete：删除远程 ftp 服务器上的文件（需要远程服务器配置相应权限）。

disconnect：断开当前连接。

bye：退出 ftp 服务。

quit：退出 ftp 服务。

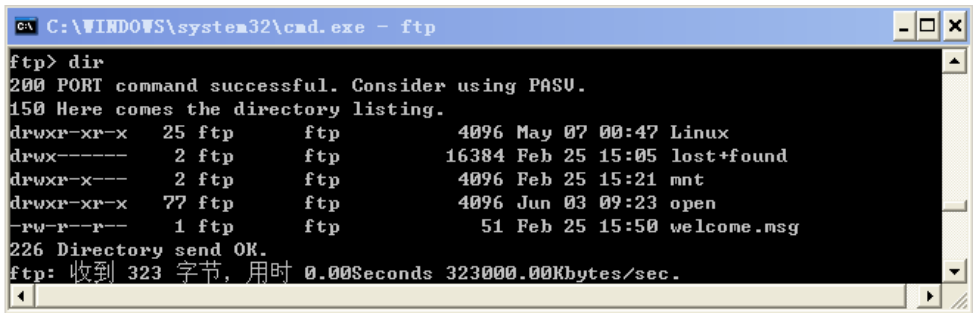

图 2-23　ftp 服务器上的文件列表

2.5.7 nbtstat 命令

nbtstat 命令用于提供关于 NetBIOS 的统计数据。使用 nbtstat 命令，可以查看本地计算机或远程计算机上的 NetBIOS 名字列表。图 2-24 就是 nbtstat 命令查看远程计算机 NetBIOS 的示例。

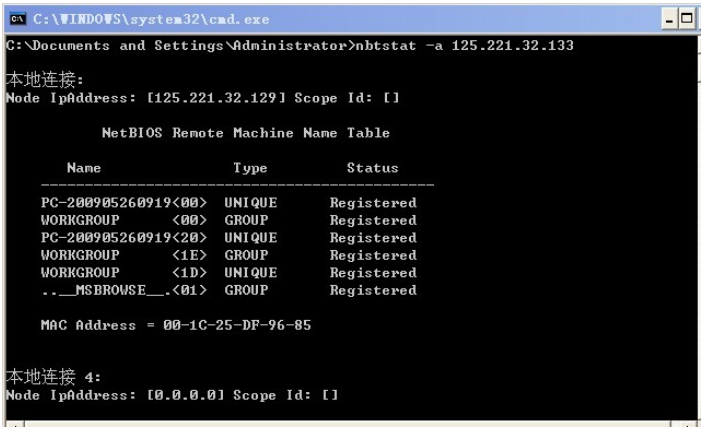

图 2-24 nbtstat 命令示例

nbtstat 常用参数选项如下：

-n：显示寄存在本地的名字和服务程序。

-r：清除 NetBIOS 中的高速缓存。

-a IP 地址：通过 IP 地址显示另一台计算机的物理地址和名字列表，所显示的内容就像另一台计算机自己运行 nbtstat -n 命令一样。

-s IP 地址：显示使用其 IP 地址的另一台计算机的 NetBIOS 连接表。

-c：显示 NetBIOS 名字高速缓存的内容。NetBIOS 名字高速缓存用于存放与本计算机最近进行通信的其他计算机的 NetBIOS 名字和 IP 地址对。

2.5.8 telnet 命令

telnet 命令为远程登录命令。使用时，先输入 telnet，然后按 Enter 键，在提示符下输入“open 主机名（IP 地址）”命令格式，示例如图 2-25 所示，这时就出现了登录窗口，用户可输入合法的用户名和密码，这里输入的密码都是不显示的。

当输入的用户名和密码都正确后，就成功建立了 telnet 连接，这时用户就在远程主机上具有了相应的权限。

当然，以上命令能成功运行需要 telnet 的目标设备支持并开启了 telnet 访问。

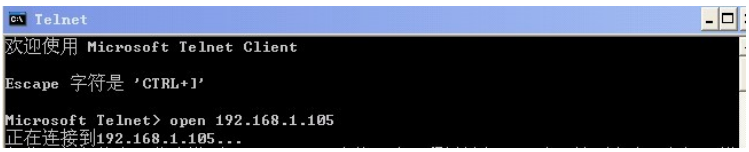

图 2-25 建立 telnet 连接

2.6　协议分析工具——Sniffer 的应用

Sniffer 软件是 NAI 公司推出的功能强大的协议分析软件。Sniffer 技术被广泛地应用于网络故障诊断、协议分析、应用性能分析和网络安全保障等各个方面。

Sniffer 软件是一种利用以太网的特性把网络适配卡（NIC，一般为以太网卡）置为杂乱模式状态的工具，一旦网卡设置为这种模式，它就能接收在网络上传输的每一个信息包。在某些操作系统中，由于普通用户缺少相应的权限，所以必须以管理员身份进行安装，如 Linux 下就必须以 root 身份进行安装。

2.6.1　Sniffer 的启动和设置

1. *启动* Sniffer

Sniffer 安装好后，启动 Sniffer 执行程序。进入 Sniffer 主界面后，要对 Sniffer 启动的网络适配器进行选择，选择后就可以在该网络适配器上捕捉流量。单击“File”菜单下的“Select Settings”，弹出“Settings”对话框，如图 2-26 所示，选择想要进行流量捕捉的适配器，选中“Log On”复选框，单击“确定”按钮，Sniffer 变成“Log On”状态，如图 2-27 所示，此时 Sniffer 在选定的网络适配器下就处于工作状态了。

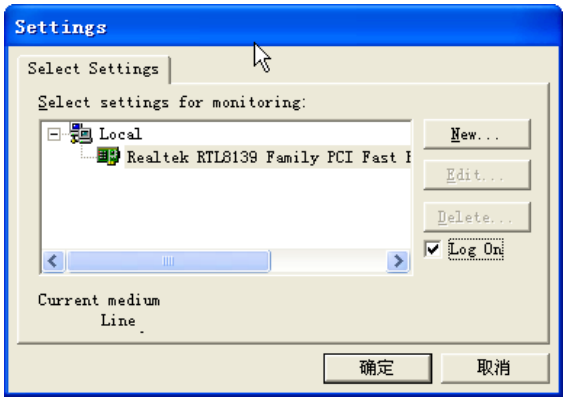

图 2-26　“Settings”对话框

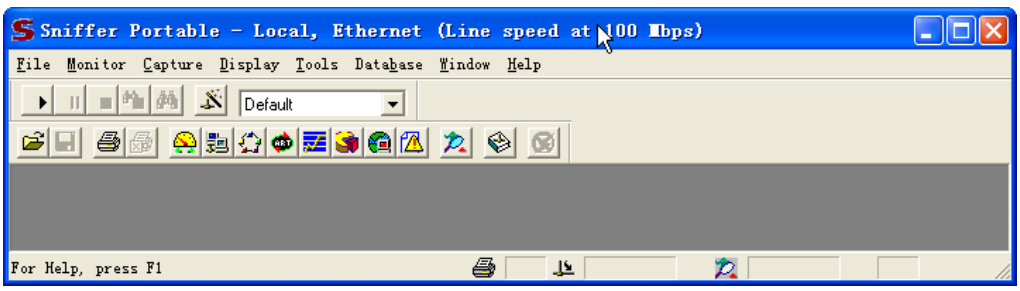

图 2-27　Sniffer 主界面（Log On 状态）

2. 设置

设置过滤器：从 Capture 菜单启动 Define filter，弹出如图 2-28 所示的 Define Filter-Capture 对话框，其中包括 Summary、Address、Data Pattern、Advanced、Buffer 五个选项卡，即摘要、地址、数据模式、高级、缓冲五个选项卡。

（1）Summary 选项卡。显示摘要信息，显示过滤器的一些信息，如地址、选定的协议类型、缓冲器信息等。

（2）Address 选项卡。可以选择地址类型并按相应的类型添加地址。若在“Address”下拉列表框中选择“Hardware”，即在下面的“Station 1”和“Station 2”设备中填写 MAC 地址；若选择“IP”，即填写 IP 地址。如图 2-28 所示，“Station1”处的源 MAC 地址为 0019213d7d44，“Station2”不填写，默认为任意 MAC 地址。也可以选择 IP 层捕获，即按源 IP 和目的 IP 进行捕获。还可以对“Include”、“Exclude”进行设定，即捕获是否包含选择条件的流量。

（3）Data Pattern 选项卡。自定义要过滤的数据模式。

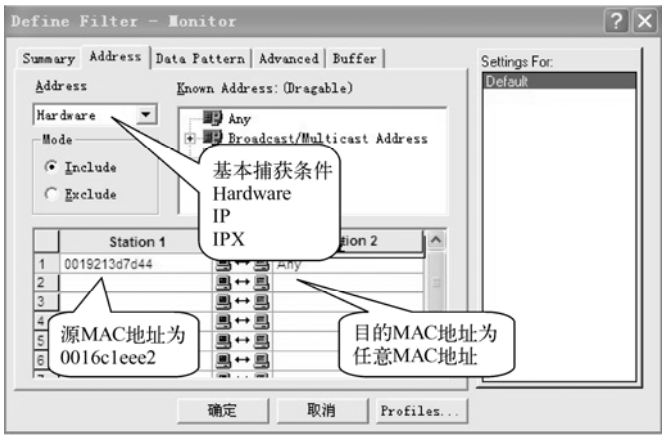

图 2-28 “Define Filter-Capture”对话框

（4）Advanced 选项卡。如图 2-29 所示，可以在此选项卡中编辑数据包的大小、协议类型、数据包的类型，并可以通过单击 Profiles 按钮将设置进行保存。

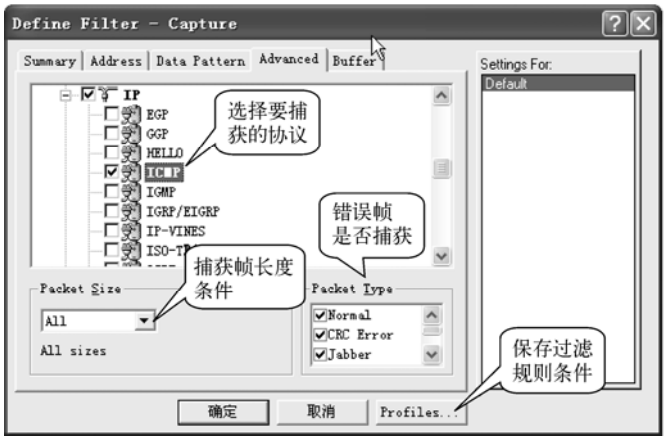

图 2-29 选择捕获协议、类型和长度

（5）Buffer 选项卡。对 Sniffer 的缓冲进行设置，即可以对缓冲大小、缓冲满后的处理方式、数据包大小、保存文件位置等进行设置，如图 2-30 所示。

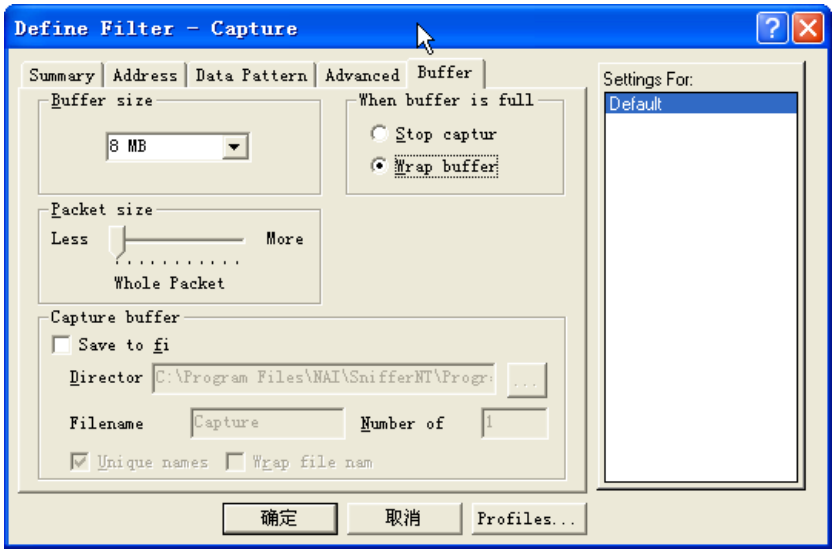

图 2-30　缓冲设置

过滤器编辑好后保存，以后可以随时通过在 Capture 菜单栏中选择过滤器来调用该设置从而启用 Sniffer。

还可以设置触发器来设置捕获，选择 Capture 中的触发设置命令来进行触发器设置。可以定义触发器的时间、警报类型来启用触发，也可以按捕获量或自定义条件定义停止触发器的条件。

3. 报文捕获解析

（1）捕获面板。可以按已定义的捕获条件单击“开始捕获”图标按钮进行捕获；也可以在开始捕获前重新定义捕获条件，进行捕获操作；在“选择捕获条件”下拉菜单中可以选择已保存的过滤器设置对捕获条件进行编辑，如图 2-31 所示是处于开始状态的捕获面板。

图 2-31　捕获面板

（2）捕获过程报文统计。如图 2-32 所示的面板可以查看捕获报文数和捕获报文的数据缓冲大小。

（3）捕获报文查看。提供专家分析系统、解码分析、矩阵分析和其他统计信息，如图 2-33 所示。

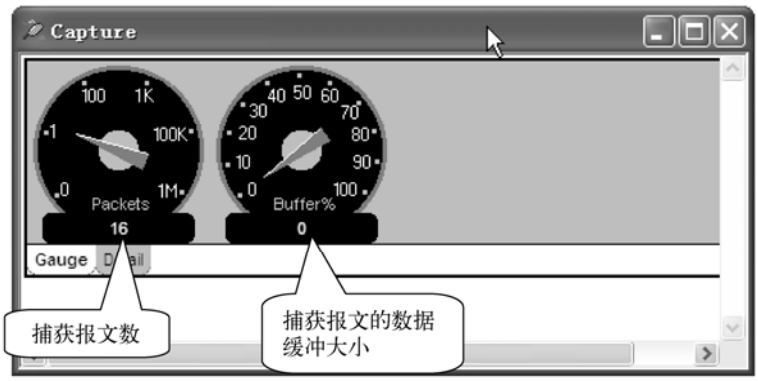

图 2-32　捕获报文统计

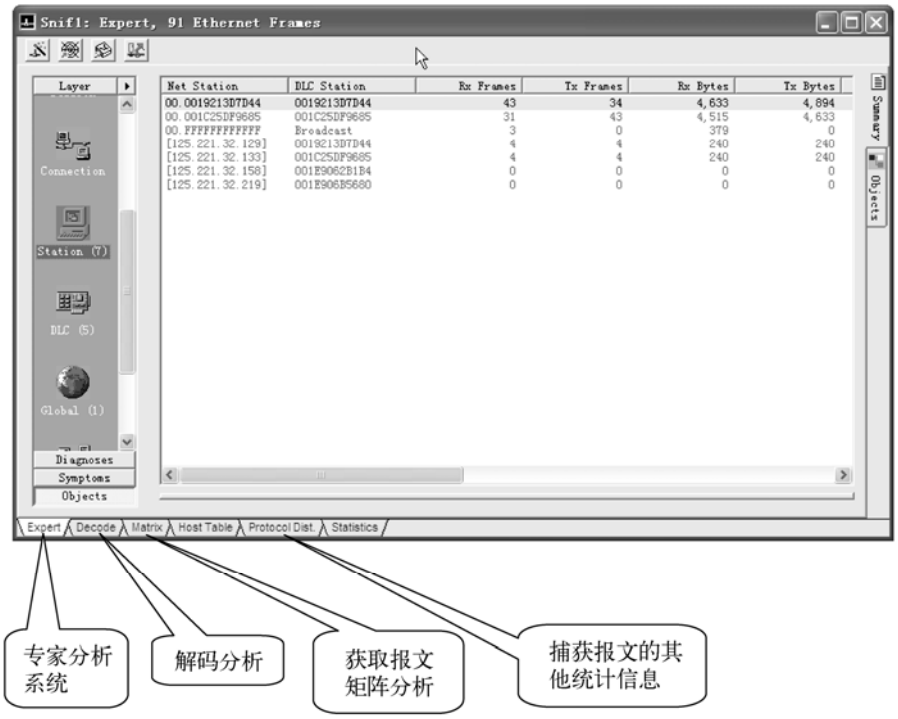

图 2-33　专家分析界面

2.6.2　解码分析

如图 2-34 所示是对捕获的报文进行解码分析的显示，此工具的使用要求对协议比较熟悉。如图 2-35 和图 2-36 所示分别为 Sniffer 对 ARP 报文和 IP 协议首部的解码分析结构。

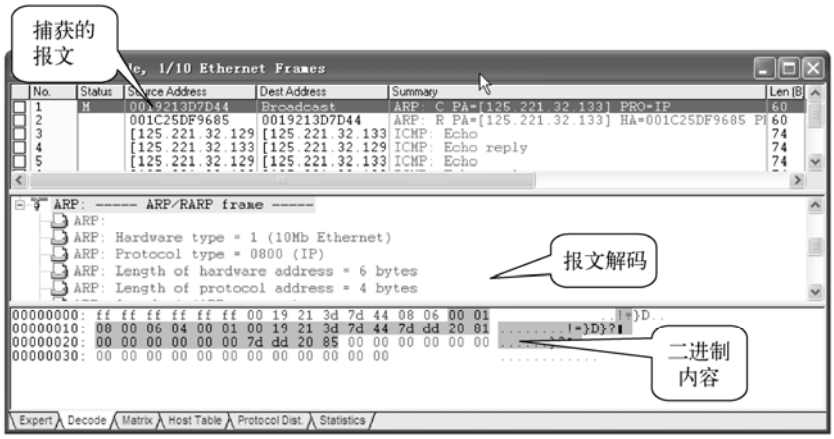

图 2-34　解码分析界面

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 6 arrived at  10:53:47.6617; frame size is 60 (003C hex) bytes.
DLC:  Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC:  Source      = Station 0019213D7D44
DLC:  Ethertype   = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 1 (ARP request)
ARP: Sender's hardware address = 0019213D7D44
ARP: Sender's protocol address = [125.221.32.129]
ARP: Target hardware address   = 000000000000
ARP: Target protocol address   = [125.221.32.133]
ARP:
ARP: 18 bytes frame padding
ARP:
```

图 2-35　通过 Sniffer 解码的 ARP 报文结构

```
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:       000. ....   = routine
IP:       ...0 ....   = normal delay
IP:       .... 0...   = normal throughput
IP:       .... .0..   = normal reliability
IP:       .... ..0.   = ECT bit - transport protocol will ignore the CE bit
IP:       .... ...0   = CE bit - no congestion
IP: Total length    = 1465 bytes
IP: Identification  = 13998
IP: Flags           = 0X
IP:       .0.. .... = may fragment
IP:       ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live    = 64 seconds/hops
IP: Protocol        = 17 (UDP)
IP: Header checksum = B7DE (correct)
IP: Source address      = [125.221.32.129]
IP: Destination address = [59.175.172.154]
IP: No options
IP:
```

图 2-36　Sniffer 对 IP 协议首部的解码分析结构

第二部分　典型项目实训任务

2.7　典型任务

2.7.1　典型任务一　常用网络命令实训

【任务目的】

（1）使用 net 命令添加账户 ntuser1，密码为 123456，并将 ntuser1 添加到管理员组。

（2）显示计算机当前共享，关闭其中一个共享，并重新开启。

（3）使用命令以匿名账户登录一台 ftp 服务器，并下载文件到本地计算机。

【任务实施步骤】

1. 使用 net 命令建立账户，并将账户加入到管理员工作组

（1）选择“开始”→“运行”，然后在打开的对话框中输入“cmd”，单击“确定”按钮。

（2）使用 net user 命令为本地计算机建立账户“ntuser1”，并设置密码为“123456”。

（3）使用 net localgroup 命令将“ntuser1”加入到“administrators”工作组。

（4）使用 net user 和 net localgroup 命令查看结果。

2. 查看本地计算机网络环境及配置

（1）使用 ipconfig /all 命令查看本地计算机的当前网络适配器配置。

（2）使用 ping 命令检测本地计算机网关和www.sina.com.cn连通情况，分析输出结果。

（3）使用 tracert www.sina.com.cn 命令，分析输出结果。

（4）使用 arp -a 命令查看当前 ARP 缓存信息，分析输出结果。

3. 使用命令访问 FTP 服务器，并进行文件下载

（1）使用 ftp 命令访问 ftp.pku.edu.cn。

（2）使用匿名账户登录，并输入电子邮箱地址作为密码。

（3）查看当前目录文件和文件夹内容。

（4）下载其中一个文件到本地计算机。

4. 查看当前共享，并建立一个共享文件夹

（1）使用 net share 查看当前共享。

（2）使用 md 命令建立一个名为“software”的文件夹。

（3）使用 net share 命令将“software”文件夹设成共享。

2.7.2　典型任务二　Sniffer 软件的使用

【任务目的】

使用 Sniffer 进行数据包的捕获及数据包结构的分析，理解协议对数据的封装。

【任务实施步骤】

（1）打开 Sniffer 软件，选取实验用的本地网络适配器。

（2）选择“捕获”→“过滤器设置”。

（3）对“地址”进行设置，设置条件为：所有和本地网络适配器通信的数据包。

（4）选择“IP”菜单，选取“ICMP”选项作为要捕获的协议。

（5）单击“捕获开始”按钮，选中“解码”标签。

（6）对捕获报文进行分析。

练　习

1．简述 OSI 参考模型的安全体系结构中定义了哪些安全服务和安全机制。

2．简述 TCP/IP 参考模型中的 Internet 层安全和应用层安全是如何实现的。