第 3 章　网络分析实验

3.1　网络分析原理

3.1.1　TCP/IP 原理

TCP/IP 是一个 4 层协议系统，TCP/IP 是一组不同的协议组合在一起构成的协议族。

(1) 数据发送时自上而下，层层加码；数据接收时自下而上，层层解码。

如图 3.1.1 所示，当应用程序用 TCP 传送数据时，数据被送入协议栈中，然后逐层通过，直到被当作一串比特流送入网络。每一层对收到的数据都要增加一些首部信息(有时还要增加尾部信息)。TCP 传给 IP 的数据单元称作 TCP 报文段。IP 传给网络接口层的数据单元称作 IP 数据报。通过以太网传输的比特流称作帧。

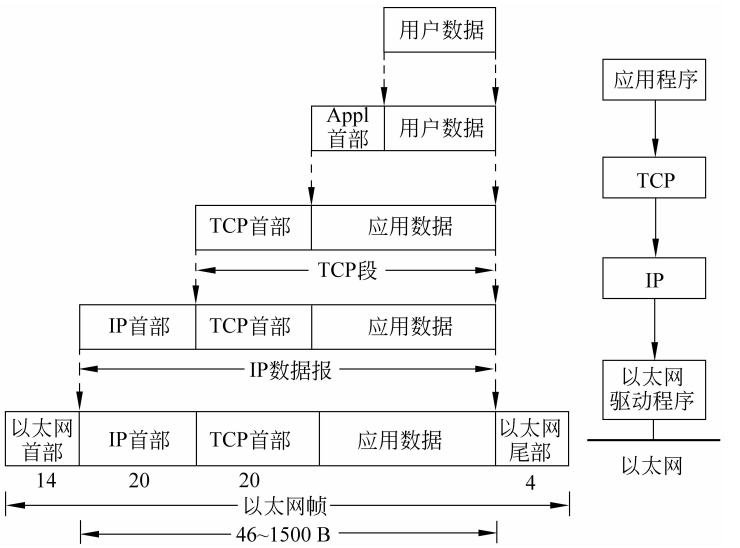

图 3.1.1　TCP/IP 系统

(2) 逻辑通信在同层完成。

数据沿垂直方向(即数据在各层间依次传递)传递是当今人们普遍认可的数据处理的功能流程。每一层都有与其相邻层的接口。为了通信，系统必须在各层之间传递数据、指令、地址等信息，通信的逻辑流程与真正的数据流不同，虽然通信流程垂直通过各层次，但每一层逻辑上都能够与远程计算机系统的相应协议层直接通信。如图 3.1.2 所示，通信实际上是按垂直方向进行的，但在逻辑上通信是在同层进行的。

3.1.2　交换技术

所谓交换，就是将分组(或帧)从一个端口转移到另一端口的动作。交换机在操作过程

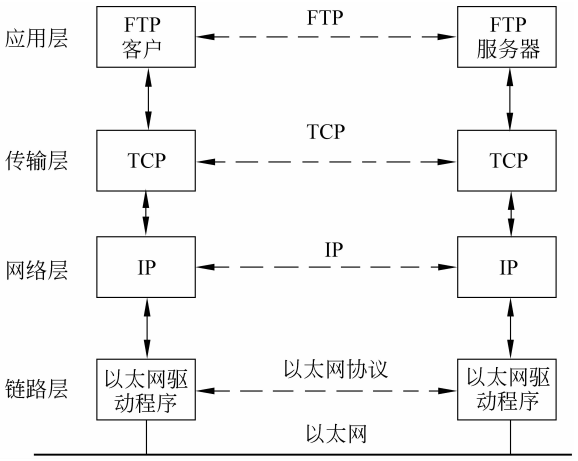

图 3.1.2　逻辑通信结构

中会不断地收集资料建立它本身的一个地址表，MAC 地址表显示了主机的 MAC 地址与以太网交换机端口的映射关系，指出数据帧去往的目标主机。

当以太网交换机收到一个数据帧时，将数据帧的目的 MAC 地址与 MAC 地址表进行查找匹配。如果在 MAC 地址表中没有相应的匹配项，则向除接收端口外的所有端口广播该数据帧。当 MAC 地址表中有匹配项时，该匹配项指定的交换机端口与接收端口相同则表明该数据帧的目的主机和源主机在同一广播域中，不通过交换机可以完成通信，交换机将丢弃该数据帧。否则，交换机把该数据帧转发到相应的端口。

交换机检查收到数据帧的源 MAC 地址，并查找 MAC 地址表中与之匹配的项。如果没有，交换机将记录该 MAC 地址和接收该数据帧的端口，并激活一个定时器。这个过程被称作地址学习；如果接收的数据帧的源 MAC 地址在地址表中有匹配项，交换机将复位该地址的定时器。如果交换机不能正确学习 MAC 地址，则有可能造成数据包丢失以及泛洪现象的发生，影响交换机的转发性能。

局域网交换技术作为对共享式局域网提供有效网段划分的解决方案，可以使用户尽可能地分享到最大带宽。交换技术在 OSI 参考模型中的第二层，即在数据链路层进行操作，交换机对数据包的转发建立在 MAC 地址基础上，对于 IP 网络协议来说，它是透明的，即交换机在转发数据包时，无须知道信源机和目标机的 IP 地址，只知其物理地址即可。

3.1.3　路由技术

路由是指通过相互连接的网络把信息从源地点移动到目标地点的过程。在路由过程中，信息至少会经过一个或多个中间节点。路由和交换实现的功能类似，但它们二者的区别是明显的，交换发生在 OSI 参考模型的第二层（数据链路层），而路由发生在第三层，即网络层。这一区别决定了路由和交换在传输信息的过程中需要使用不同的控制信息。

当 IP 子网中的一台主机发送 IP 分组给同一子网的另一台主机时，它直接把 IP 分组送到网络上，对方就能收到。当发送给不同子网上的主机时，它要选择一个能到达目的子网上的路由器，把 IP 分组传递给该路由器，由路由器负责把 IP 分组送到目的地。如果没有这样的路由器，主机就把 IP 分组送给一个被称为“默认网关”的路由器。“默认网关”是每台主机

上的一个配置参数，它是同一个网络上的某个路由器端口的 IP 地址。

同主机一样，路由器也要判定端口连接的是否为目的子网，如果是，就直接把分组通过端口送到网络上，否则也要选择下一个路由器传送分组。路由器也有它的默认网关，用来传送 IP 分组，通过逐级传送，IP 分组最终将送到目的地，否则 IP 分组被网络丢弃。

路由器不仅负责 IP 分组转发，还需与其他路由器联络，确定网络的路由选择和维护路由表。路由包含两个基本动作：选择最佳路径和通过网络传输信息。在路由过程中，后者也称为(数据)交换。交换相对来说比较简单，而选择最佳路径很复杂。

路径选择是判定到达目的地的最佳路径，由路由选择算法实现。由于会涉及不同的路由选择协议和路由选择算法，所以相对复杂一些。为了判定最佳路径，路由选择算法必须启动并维护包含路由信息的路由表，其中路由信息依赖于所用的路由选择算法。

Metric 是路由算法用以确定到达目的地的最佳路径的计量标准。路由算法根据许多信息填充路由表。路由器查看了数据包的目的协议地址后，确定是否知道如何转发该包，如果路由器不知道如何转发，通常就将之丢弃。如果路由器知道如何转发，就把目的物理地址变成下一跳的物理地址并向之发送。下一跳可能就是最终的目的主机，如果不是，通常为另一个路由器，它将执行同样的步骤。

3.1.4 网络嗅探技术

1. 嗅探技术简介

嗅探(sniffer)技术是一种重要的网络安全攻防技术。对黑客来说，通过嗅探技术能以非常隐蔽的方式攫取网络中的大量敏感信息，与主动扫描相比，嗅探行为更难被察觉，也更容易操作。对安全管理人员来说，借助嗅探技术，可以对网络活动进行实时监控，发现各种网络攻击行为。嗅探技术最初作为网络管理员检测网络通信的必备技术，既可以是软件，又可以是一个硬件设备。软件 Sniffer 应用方便，针对不同的操作系统平台有多种不同的软件 Sniffer；硬件 Sniffer 通常被称作协议分析器，其价格一般都很高。

在局域网中，以太网的共享式特性决定了嗅探能够成功。因为以太网是基于广播方式传送数据的，所有的物理信号都会被传送到每一个主机节点，此外，网卡可以被设置成混杂接收模式，在这种模式下，无论监听到的数据帧目的地址如何，网卡都能予以接收。而 TCP/IP 栈中的应用协议大多数明文在网络上传输，这些明文数据中往往包含一些敏感信息(如密码、账号等)，使用 Sniffer 可以监听到所有局域网内的数据通信，并得到这些敏感信息。

Sniffer 的隐蔽性好，它只是被动接收数据，不向外发送数据，所以在传输数据过程中，根本无法觉察。Sniffer 的局限性是只能在局域网的冲突域中或者在点到点连接的中间节点上进行监听。

2. 网络嗅探器

网络嗅探器在当前网络技术中使用得非常广泛。网络嗅探器既可以作为网络故障的诊断工具，也可以作为监听工具。传统的网络嗅探技术是被动地监听网络通信、用户名和口令。新的网络嗅探技术开始主动地控制通信数据。大多数的嗅探器至少能够分析下面的协议：标准以太网、TCP/IP、IPX、DECNET 等。

根据功能不同，嗅探器可以分为通用网络嗅探器和专用嗅探器。前者支持多种协议，如

tcpdump、Snifferit 等；后者一般针对特定软件或提供特定功能，如专门针对 MSN 等即时通信软件的嗅探器、专门嗅探邮件密码的嗅探器等。

3. 嗅探技术分类

根据工作环境和工作原理的不同，嗅探技术又可以分为本机嗅探、广播网嗅探、交换机嗅探等类型。

1）本机嗅探

本机嗅探是指在某台计算机内，嗅探程序通过某种方式，获取发送给其他进程的数据包的过程。例如，当邮件客户端在收发邮件时，嗅探程序可以窃听到所有的交互过程和其中传递的数据。

2）广播网嗅探

广播网基于集线器（Hub）的局域网络，其工作原理是基于总线方式的，所有的数据包在该网络中都会被广播发送（即发送给所有端口）。在广播网中，每一个网络数据包都被发送到所有的端口，然后由各端口连接的网卡判断是否需要接收，所有目的地址与网卡实际地址不符的数据包将被网卡驱动自动丢弃，这确保了广播网中每台主机只接收到以自己为目标的数据包。

广播网嗅探利用了广播网“共享”的通信方式。在广播网中，所有的网卡都会收到所有的数据包，只要将本机网卡设为混杂模式，就可以使嗅探工具支持广播网或多播网的嗅探。

3）交换机嗅探

交换机的工作原理与 Hub 不同，它不再将数据包转发给所有端口，而是通过“分组交换”的方式进行单对单的数据传输，即交换机能记住每个端口的 MAC 地址，根据数据包的目的地址选择目的端口，只有对应该目的地址的网卡能接收到数据。

基于交换机的嗅探是指在交换环境中通过某种方式进行的嗅探。由于交换机基于“分组交换”的工作模式，因此，简单地将网卡设为“混杂”模式并不能嗅探到网络上的数据包，必须采用其他方法实现基于交换机的嗅探。

4）端口镜像嗅探

端口镜像也称作巡回分析端口（roving analysis port），它从网络交换机的一个端口转发每个进出分组的副本到另一个端口，分组将在此端口进行分析，端口镜像是监视网络通信量和通信内容的一种方法。网络管理员将端口镜像作为一种诊断或调试的工具，尤其是在分析网络情况的时候，它使管理员能跟踪交换机的性能，并在必要时对其进行更改。

端口镜像是交换机为调试预留的功能。通过端口镜像，可以将交换机中任意端口的数据复制给镜像端口。通过端口镜像，本机嗅探工具就可以嗅探交换机上的任意端口了。

基于端口镜像的嗅探受限于交换机能够支持的镜像功能，能够镜像多少端口、镜像出来的协议如何都取决于交换机的型号和配置。由于进行基于端口镜像的嗅探必须拥有交换机的管理权限，因此，基于端口镜像的嗅探往往是网络管理员常用的嗅探方式。

5）通过 MAC 泛滥进行交换机嗅探

这种方式往往被攻击者使用。网络交换机为了能够进行分组交换，必须在内部维护一个转换表，将不同的 MAC 地址转换成交换机上的物理端口。由于交换机的工作内存有限，如果用虚假的 MAC 地址对交换机不断进行攻击，直到交换机的工作内存被占满，交换机就进入了所谓的“打开失效”模式，开始了类似于集线器的工作方式，向网络上所有的机器广播

数据包。在这种情况下，交换机嗅探同样可以采用广播网嗅探的方式实现。

4. 嗅探的安防作用

1）网络安全审计

网络安全审计是指通过网络嗅探工具，将网络数据包捕获、解码并加以存储，以备后期查询或提供即时报警。通过嗅探技术，网络安全审计可以实现上网行为审计、网络违规数据的监控等功能。利用网络嗅探技术开发的网络行为审计类软件是运行在关键的网络节点，对网络传输的数据流进行合法性检查的工具。

2）蠕虫病毒的控制

采用嗅探技术，对蠕虫病毒的控制可起到以下作用。

（1）基于网络嗅探的流量检测，及时发现网络流量异常，并根据已经建成的流量异常模型初步判断出网络蠕虫病毒爆发的前兆。

（2）基于网络嗅探的网络协议分析，进一步确认蠕虫病毒的发作，并及时给出预警信息。

（3）基于网络嗅探技术的蜜罐，尽早捕获蠕虫病毒的样本，并通过对其进行详细的分析，制定出有效的防御方案和清除方案。

（4）通过基于网络嗅探技术的入侵检测，能够准确定位局域网络中的蠕虫病毒传播源，从而及时扼杀病毒蠕虫的传播行为。

3）网络布控与追踪

针对网络犯罪，如黑客入侵、拒绝服务攻击等，通过嗅探技术进行追踪，协助执法部门定位网络犯罪分子。现代网络犯罪往往采用跳板进行，即通过一台中间主机进行网络攻击和犯罪活动，这对犯罪分子的捕获造成了很大的障碍，而嗅探技术可以有效地帮助执法人员解决这一问题。

网络追踪是针对伪造 IP 地址攻击的一种追查方法。由于网络攻击往往采用虚假的 IP 地址（特别是大规模的拒绝服务攻击），因此，从被攻击机嗅探获取的数据无法直接判断攻击源，需要采用移动的网络嗅探器，以溯源的方式从终点逐个前溯，直到发现攻击的起源点。

当发现某网络犯罪行为是通过中间跳板主机进行时，暂时不对该主机进行明显的操作，而是运行网络嗅探器对其进行 24 小时监控，一旦犯罪分子远程登录该主机，网络嗅探器就会记录该犯罪分子的 IP 地址，从而协助定位和追踪。目前，国内已经有多个通过网络布控和追踪的方式抓获犯罪分子的案例，其中涉及嗅探技术的应用。

4）网络取证

基于嗅探的网络取证工具可以运行在需要取证的犯罪分子使用的计算机上（如个人计算机或公共场所的计算机），并可以将该犯罪分子的网络行为（如邮件、聊天信息、上网记录等）加以实时记录，从而协助案件的侦破和起诉证据的获取。为了确保利用嗅探工具获得的网络证据具备不可篡改性，网络取证工具中还需要内置数字签名工具，防止操作人员人为修改或误删数字证据。

嗅探技术在黑客攻防技术及信息安全体系建设中都起到了非常重要的作用，而反嗅探技术也是确保网络私密性的关键之一。同时，嗅探技术在网络安全管理工作中也具有很大的帮助。但是，在进行嗅探技术的合法应用的同时，还需要关注嗅探技术滥用带来的泄密和破坏个人隐私问题。未来，随着网络技术的发展，嗅探技术和反嗅探技术还将不断进步，目

前在高速化、可视化、针对加密的嗅探和无线切入技术 4 个方向上都可以看到新技术。

3.2 网络分析基础实验

3.2.1 Sniffer Pro 简介

Sniffer Pro 软件是 NAI 公司推出的功能强大的协议分析软件。利用 Sniffer Pro 网络分析器的强大功能和特征，解决网络问题。本书使用的软件版本为 Sniffer Pro_4_70_530。

Sniffer Pro 软件的主要作用可以体现在以下 6 个方面。

(1) Sniffer 可以评估业务运行状态，如各种应用的响应时间、一个操作需要的时间、应用带宽的消耗、应用的行为特征、应用性能的瓶颈等。

(2) Sniffer 能够评估网络的性能，如各链路的使用率、网络性能趋势、消耗最多带宽的具体应用、消耗最多带宽的网络用户、各分支机构的流量状况、影响网络性能的主要因素。

(3) Sniffer 可以快速定位故障，monitor、expert、decode 等功能都可以快速定位故障。

(4) Sniffer 可以排除潜在的威胁，如病毒、木马、扫描等，并且发现攻击的来源，为控制提供根据，对类似蠕虫病毒一样对网络影响大的病毒有效。作为即时监控工具，Sniffer 通过发现网络中的行为特征判断网络是否有异常流量，所以 Sniffer 发现病毒的速度可能比防病毒软件快。

(5) Sniffer 可以做流量的趋势分析，通过长期监控，可以发现网络流量的发展趋势，为将来的网络改造提供建议和依据。

(6) 应用性能预测。Sniffer 能够根据捕获的流量分析一个应用的行为特征，可以提供量化的预测，准确率较高，误差不超过 10%。

Sniffer 包括了 4 大功能：监控(monitor)、显示(display)、数据包捕捉(capture)和专家分析系统(expert)。

3.2.2 程序安装实验

实验器材

Sniffer Pro 软件系统，1 套。

PC(Windows XP/Windows 7)，1 台。

预习要求

(1) 做好实验预习，复习网络协议有关的内容。

(2) 熟悉实验过程和基本操作流程。

(3) 做好预习报告。

实验任务

通过本实验，掌握以下技能。

(1) 学会在 Windows 环境下安装 Sniffer。

(2) 能够运用 Sniffer 捕获报文。

实验环境

本实验采用一个已经连接并配置好的局域网环境。在 PC 上安装 Windows 操作系统。

预备知识

(1) TCP/IP 原理及基本协议。
(2) 数据交换技术的概念及原理。
(3) 路由技术及实现方式。

实验步骤

按照常规安装方法双击 Sniffer 软件的安装图标按顺序进行,如图 3.2.1 所示。本书选用的软件版本为 Sniffer Portable 4.7.5。

图 3.2.1 软件安装界面

如图 3.3.2 所示,选择 Sniffer Pro 的安装目录时,默认安装在 C:\Program Files\NAI\SnifferNT 目录中,为了更好地使用,建议用默认路径进行安装。

图 3.2.2 安装目录选择界面

注册用户时，需要填写必要的注册信息。在出现的 Sniffer Pro User Registration 的 3 个对话框中依次填写个人信息。如图 3.2.3 所示，最后一行的 Sniffer Serial Number 需要填入购买软件时提供的注册码。

图 3.2.3　用户注册界面

如图 3.2.4 所示，完成注册操作后，需要设置网络连接状况。从上至下，依次有 3 个选项："Direct Connection to the Internet(直接连接)""Connection to the Internet through a Proxy(通过代理服务器连接)""Not connected to network or dial-up print & fax option(拨号、传真或无连接)"。一般情况下，用户选择第一项——"Direct Connection to the Internet"。

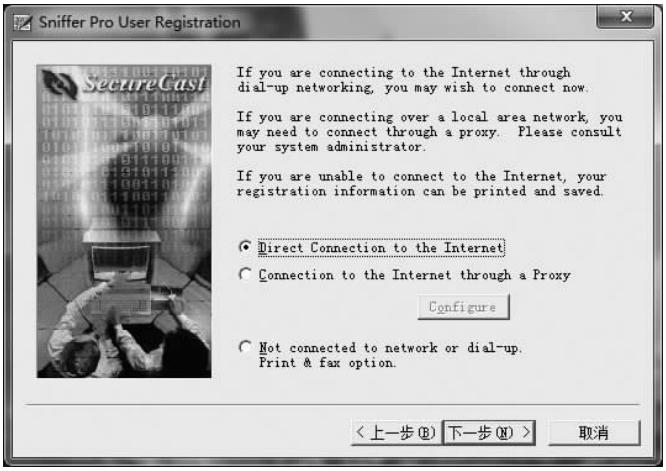

图 3.2.4　网络连接状况设置界面

如图 3.2.5 所示，若通过代理服务器连接，则需要输入代理服务器地址、用户名和账号等信息。

接下来系统会自动定位并连接到最近的网络服务器 Mercury. nai. com，完成必要的注册信息提交和注册码认证工作。当用户的注册信息验证通过后，系统会转入如图 3.2.6 所示的界面，用户被告知系统分配的身份识别码，以便用户进行后续的服务和咨询。

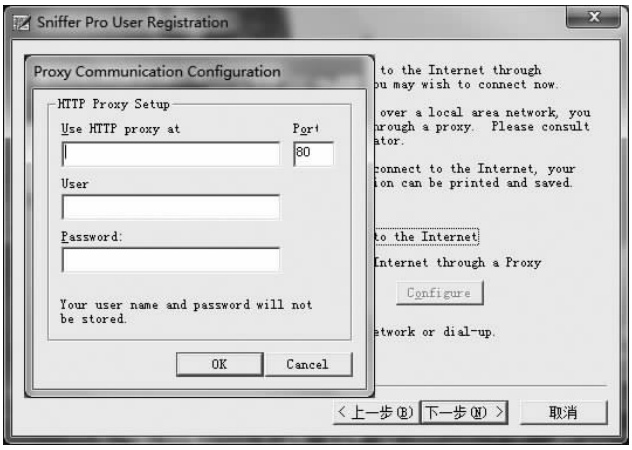

图 3.2.5　代理服务器设置界面

图 3.2.6　注册信息验证界面

如图 3.2.7 所示，此时用户单击【下一步】按钮，系统会提示用户保存关键性的注册信息，并生成一个文本格式的文件 Registration Summary.txt。该文件主要包括以下几个重

图 3.2.7　注册信息保存提示

要部分，详细内容可参照图 3.2.8。

图 3.2.8　注册文件内容

- 用户身份识别码(Customer Identification Number)。
- 服务器连接信息(Contact Info)。
- 用户填写的身份注册信息(Product Sniffer Pro)。

由于 Sniffer Pro 软件的运行环境需要 Java 环境支撑，因此，在软件使用前安装程序会提示用户安装并设置 Java 环境，如图 3.2.9 所示。

图 3.2.9　设置 Java 环境

接下来，系统在完成关键文件复制和安装的工作后，会出现 setup complete 提示，由于 Sniffer Pro 需要将网卡的监听模式切换为混杂，所以需要重新启动计算机完成网卡的工作模式切换，当软件提示重新启动计算机时，按照提示操作即可。

重新启动计算机后，可以通过运行 Sniffer Pro 监测网络中的数据包。通过【开始-程序-Sniffer pro-Sniffer】启动程序。进入主界面后，首先要配置监听网卡。一般情况下，Sniffer Pro 初次运行时会自动选择机器网卡进行监听。如果本地计算机有多个网卡，则需要手工指定。具体方法如下。

(1) 选择软件【文件(file)】下的【选定设置(select settings)】选项。

(2) 在【当前设置(settings)】窗口中选择监听的网卡，同时勾选 Log Off，单击【确定】按钮，如图 3.2.10 所示。

图 3.2.10　设置提示

(3) 如果存在多个网卡，则需要确定最终的监听网卡，如图 3.2.11 所示。

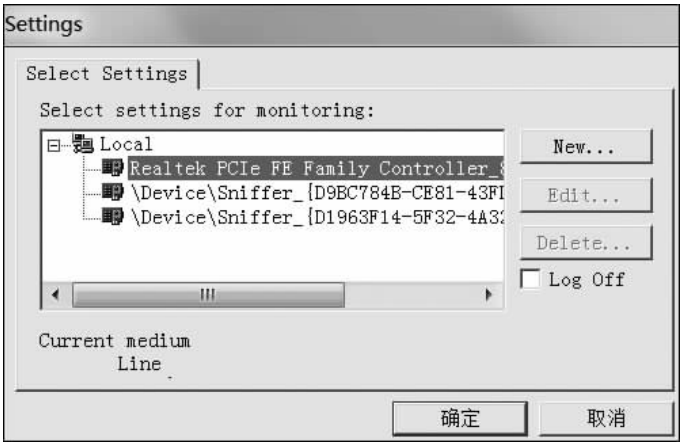

图 3.2.11　多网卡设置提示

完成上述操作后，就可以使用 Sniffer Pro 对目标机器进行网络监听了，如图 3.2.12 所示。快捷操作功能主要包括报文捕获及网络性能监视，主要监控目标机器的网络流量和错误数据包的情况。主要的参考信息包括网络使用率(utilization)、数据包传输率(packets/s)、错误数据情况(error/s)。

图 3.2.12　快捷操作菜单

实验报告要求

- 写明实验目的。
- 附上实验过程的截图和结果截图。
- 阐述碰到的问题以及解决方法。
- 阐述收获与体会。

思考题

(1) 网卡的工作模式有几种?
(2) 描述监听模式的具体工作情况。

3.2.3　数据包捕获实验

实验器材

Sniffer Pro 软件系统,1 套。
PC(Windows XP/Windows 7),1 台。

预习要求

(1) 做好实验预习,复习网络协议有关的内容。
(2) 熟悉实验过程和基本操作流程。
(3) 做好预习报告。

实验任务

通过本实验,熟练掌握 Sniffer 数据包捕获功能的使用方法。

实验环境

本实验采用一个已经连接并配置好的局域网环境。在 PC 上安装 Windows 操作系统。

预备知识

(1) 数据交换技术的概念及原理。
(2) 路由技术及实现方式。

实验步骤

1. 报文捕获

数据包捕捉(capture)是将所有的数据包截取并放在磁盘缓冲区中,便于分析。基本原

理是通过软件手段设置网络适配器(NIC)的工作模式,在这种模式下,网卡接收所有的数据,达到网络监控和网络管理的功能。

如图 3.2.13 所示,报文捕获快捷操作的功能依次为开始、暂停、停止、停止显示、显示、定义过滤器以及选择过滤器。一般情况下,选择默认的捕获条件。

Sniffer 启动后,一般处于脱机模式。在捕获报文前,需要进入记录模式,通过选择【文件】菜单下的【记录于】启动网卡的监听模式。也可以通过【选定设置】勾选"Log On/Off"完成上述操作。此时可根据需要进行局域网的回环测试。选择【捕获】菜单下的【开始】或直接单击捕获快捷菜单中的【开始】按钮,系统开始进行网络报文的捕获。

在捕获过程中,单击快捷菜单中的【捕获面板】或选择【捕获】菜单下的【捕获面板】选项,可以随时查看捕获报文的数量以及数据缓冲区的利用率,如图 3.2.14 所示。

图 3.2.13　捕获报文快捷操作菜单

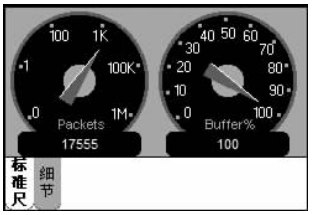

图 3.2.14　报文捕获面板

左侧仪表显示了系统当前捕获到的报文数量,右侧仪表显示了捕获报文的数据缓冲器大小。此外,还可以选择【细节】功能,查看详细的统计信息,如图 3.2.15 所示。

Status			
# 看见	60030	# 已接受的	22003
# Drops	0	# 拒绝	0
缓冲器大小	8 MB	碎片大小	全部
缓冲器动作	覆盖	逝去时间	0:14:31
保存文件#	N/	文件覆盖	N/
标准尺	细节		

图 3.2.15　报文捕获统计信息

捕获到的报文存储在缓冲器内。使用者可以显示和分析缓冲器内的当前报文,也可以将报文保存到磁盘,加载和显示之前保存的报文信息,进行离线分析和显示。

整个捕获过程受【定义过滤器】的约束,选择【捕获】菜单下的【定义过滤器】,单击【缓冲】选项卡,对捕获缓冲区进行设置。

首先,缓冲区的大小由用户自定义,根据实际主机的内存容量进行调整。缓冲区设置过大,容易造成软件运行延迟。

其次,数据包大小应选择适度,截取部分数据包能够节省磁盘空间,保证网络通信流畅,避免丢失帧。

值得一提的是,当禁止【保存到文件】选项时,可以选择停止捕获条件,即缓冲区已满或覆盖原有数据。

此外,也可以通过指定文件名前缀和脱机文件数对捕获信息进行存储,如图 3.2.16 所示。

图 3.2.16　捕获缓冲区设置

以上介绍的是基本捕获方式，若需要捕获特定主机或工作站的数据包，可以通过选择【监视器】菜单中的【主机列表】选项查看工作站信息，并单击单个主机进行数据包捕获。

2. 报文分析

为了有效地进行网络分析，需要借助专家分析系统。首先，应根据网络协议环境对专家系统进行配置。选择【工具】菜单中的【专家选项】，如图 3.2.17 所示。

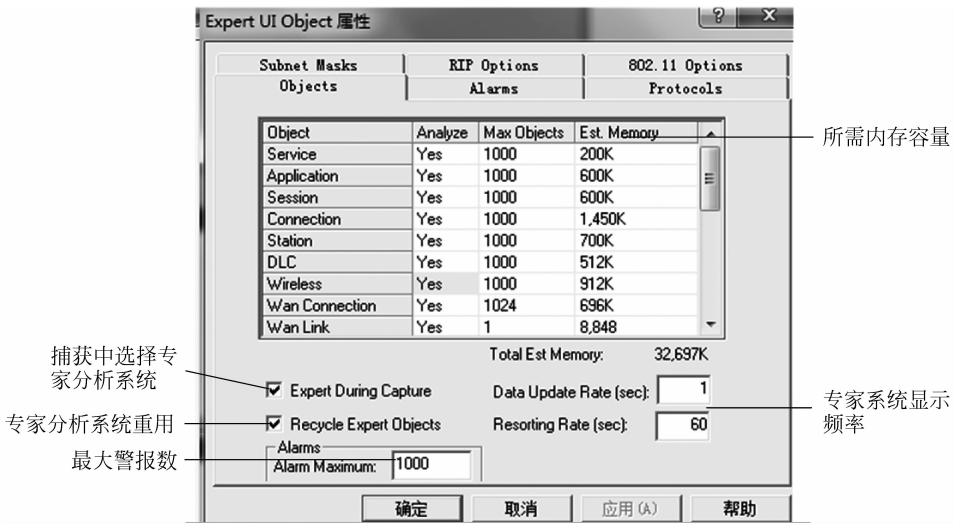

图 3.2.17　专家选项设置

专家系统的配置能够帮助分析人员专注于特定问题，通过排除某些系统层数据，捕获到网络分析所需的特定通信量。同时，根据每层对象所需的内存容量，创建每个系统层的最大对象数。

- 在设置中，【专家分析系统重用】选项定义了当内存不足时专家分析系统需要进行的操作，即覆盖原有数据创建新对象（选中）或停止创建对象，对已有数据进行分析（未选中）。
- 默认情况下，当数据包捕获开始时，专家分析系统就开始分析进入缓冲区的数据包，

并在窗口中实时显示，用户可以在捕获的同时分析网络对象、症状，并做出诊断。用户也可以选择禁用实时分析功能（未选中）。

- 指定可创建的最大警报数。当达到最大警报数时，专家系统会覆盖最早最低级别的警报（选中）或者停止创建警报。
- 专家系统显示的刷新频率，以及专家分析系统数据分析到摘要显示操作之间的延迟。
- 对于专家系统的警报阈值配置，可以通过选择【工具】菜单下的【专家选项】获得，单击【Alarms】设置项。

值得注意的是，系统默认的阈值都是经过精确计算的，可保证系统进行诊断和问题检测需求，对于阈值的修改，可能会导致系统判断失误或运行错误。如图 3.2.18 所示，每一个系统层都存在多个症状诊断的警报阈值信息。

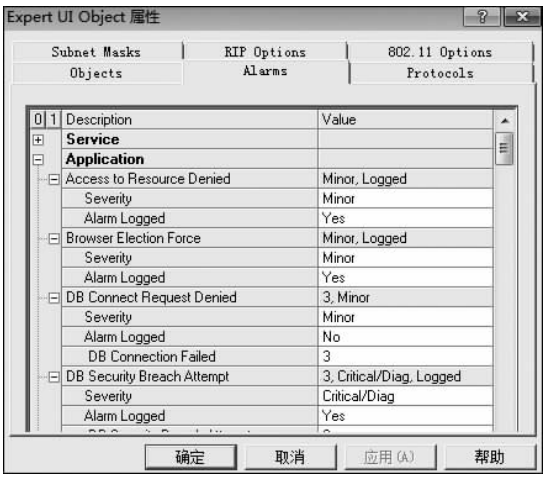

图 3.2.18　专家分析系统阈值设置

对于各类网络协议，用户可以进行选择性的监听和分析，单击【Alarms】右侧的【Protocols】设置项，如图 3.2.19 所示，可按照系统分析层进行协议选择。

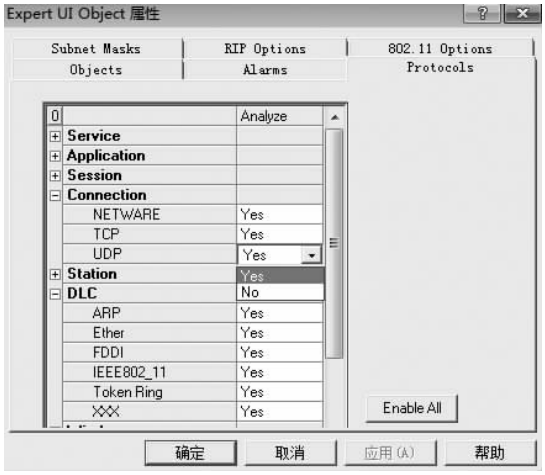

图 3.2.19　指定分析协议设置 1

此外，当网络使用了不规范的子网掩码时，可以通过选择【Subnet Masks】设置项进行更改。

专家分析系统还为用户提供了用于检测路由故障的路由信息协议（RIP）分析，通过分析捕获报文的路由选择协议构建路由表并显示。专家分析系统通常会发现网络上的默认路由器，同时构建一条通向网关的默认静态路由。如果选择使用 RIP 分析方式，则需要将【对象】设置项中的连接层和应用层定义为“分析”，如图 3.2.20 所示。

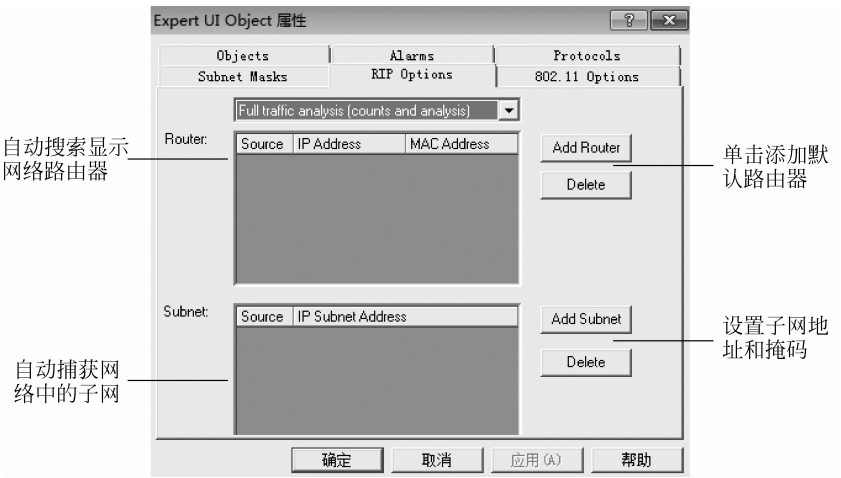

图 3.2.20　指定分析协议设置 2

在专家分析系统属性设置中还特别设定了用于无线网络分析的选项。启用欺诈 AP 查找的选项后，专家系统会对访问主机的 MAC 地址和选项中已存地址进行比较，一旦出现异常，就会生成警报。

通过【显示】菜单下的【显示设置】选项，可以自定义要显示的分析内容。如图 3.2.21 所示，显示设置对话框中主要包括如下几个方面。

图 3.2.21　摘要显示设置

- 【普通】设置可以显示或隐藏“主机列表”“矩阵”“协议分布”“统计数据”等。
- 【摘要显示】可以定义具体显示的专家症状、系统层等内容。

- 【协议颜色】可以改变显示协议使用的字体颜色。
- 【协议使详诉】可以设置每个协议的详细显示设置。
- 【解码字体】可以更改“解码”显示中文字体类型、颜色和大小。

摘要显示选项说明与状态标志说明分别如表 3.2.1 和表 3.2.2 所示。

表 3.2.1　摘要显示选项说明

显 示 选 项	启用功能描述
专家系统症状	为每个帧显示发现的上一个症状
全部层	显示帧中包含的协议层,每个协议层一行
网络地址	显示为网络地址,否则为硬件地址
MAC 地址中的厂商 ID	在 MAC 地址的开头部分显示供应商名称
网络地址的名称解析	显示网络地址的名称,而不是数字地址
地址簿解析名称	如果工作站在地址簿中已命名,则显示其名称,而不是地址
二进制格式	显示将表示为两个窗口,以显示工作站之间的通信情况
可 选 择 区 域	
状态	当数据包出现异常时,显示异常状态表示,见表 3.2.2
绝对时间	显示收到帧的时间
Delta 时间	显示当前帧和上一帧之间的时间间隔
相对时间	显示当前帧和标记帧之间的时间间隔
Len(字节)	显示帧的长度
累计的字节	显示从标记帧开始,到当前帧的所有帧的长度

表 3.2.2　状态标志说明

状态标志	状 态 描 述	状态标志	状 态 描 述
M	数据包已标记	帧不全	数据包小于 64B,无 CRC 错误
A	数据包是端口 A 捕获到的	分段	数据包小于 64B,有 CRC 错误
B	数据包是端口 B 捕获到的	超大	数据包大于 1518B,无 CRC 错误
#	数据包存在症状,或具体诊断内容	冲突	数据包由于冲突而损坏
触发器	数据包是一个数据触发器	对齐	数据包长度不是 8 的整数倍
CRC	具有 CRC 错误大小正常的数据包	地址重复	在环中有地址冲突
超长	具有 CRC 错误大小超长的数据包	帧复制	目的主机未收到数据包

在专家分析系统的解码显示窗口中可以通过【显示】菜单下的【查找帧】获得特定帧信息。【查找帧】包含 4 个选项。

- 文本,即搜索包含特定文本字符信息的帧。
- 数据,即搜索包含特定数据模式的帧。

- 状态，允许搜索具有特定状态标志的帧。
- 专家系统，允许搜索与特定专家系统症状或诊断关联的帧。

专家分析系统能够对缓冲区内的数据包进行综合分析，将捕获内容按照服务、应用、连接、工作站、路由、子网等类别进行分类统计，并对存在安全隐患和问题的服务或连接进行分析，给出确切的结论。对于问题内容，将注明其所属层次(layer)、诊断方式(diagnoses)、基本征兆(symptoms)和目标(objects)。

专家分析平台可以对网络流量进行实时分析，并提供客观翔实的诊断结果，主要包括【专家分析系统】【解码系统】【矩阵】【主机列表】【协议列表】以及【统计分析系统】，只要单击【停止并显示】，就可以查看具体的网络分析数据，如图 3.2.22 所示。

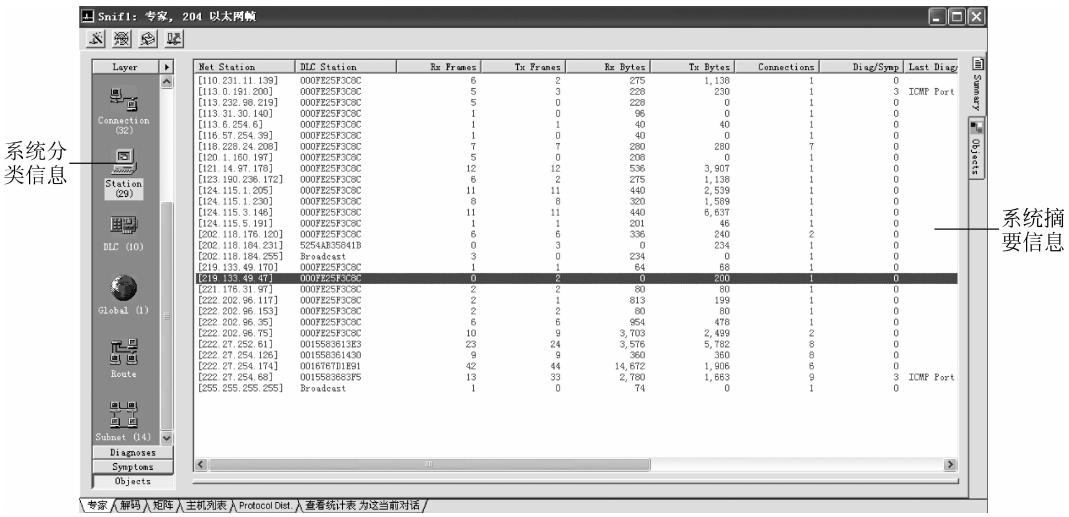

图 3.2.22　报文捕获显示界面

通过专家分析平台，可以捕获在网络会话过程中存在的各类潜在问题。这些问题被定义为症状或诊断。

- 症状：网络会话情况超过专家设定阈值，表示网络存在潜在问题。
- 诊断：多个一起分析的症状、复发率较高的特定症状，对于诊断，必须立即检查。
- 专家系统分类信息：显示网络各个分析层，其层次性与 OSI 参考模型类似。
- 专家系统摘要信息：根据“摘要显示”设定的各层显示数据。

对于某项统计分析，可以通过双击方式查看对应记录的详细统计信息，如图 3.2.23 所示。对于每一项记录，都可以通过查看帮助的方式了解产生的原因。

3. 解码分析

单击专家系统下方的【解码】按钮，就可以对具体的记录进行解码分析，如图 3.2.24 所示。页面自上而下由 3 部分组成：捕获的报文、解码后的内容、解码后的二进制编码信息。

对于解码分析人员来说，只有充分掌握各类网络协议，才能看懂解析出来的报文。利用软件解码分析解决问题的关键是要对各种层次的协议有充分的了解。

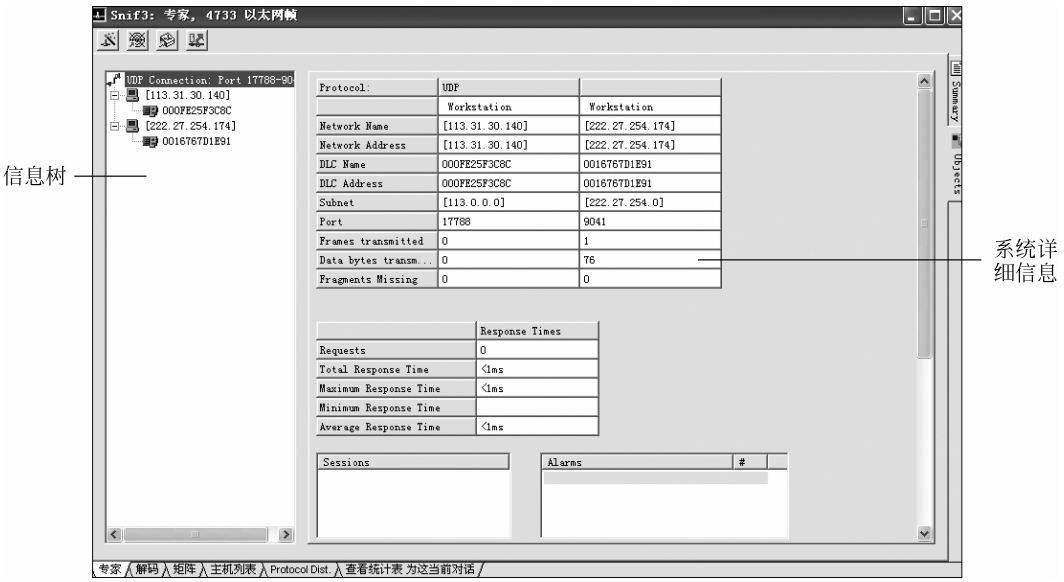

图 3.2.23　报文详细信息

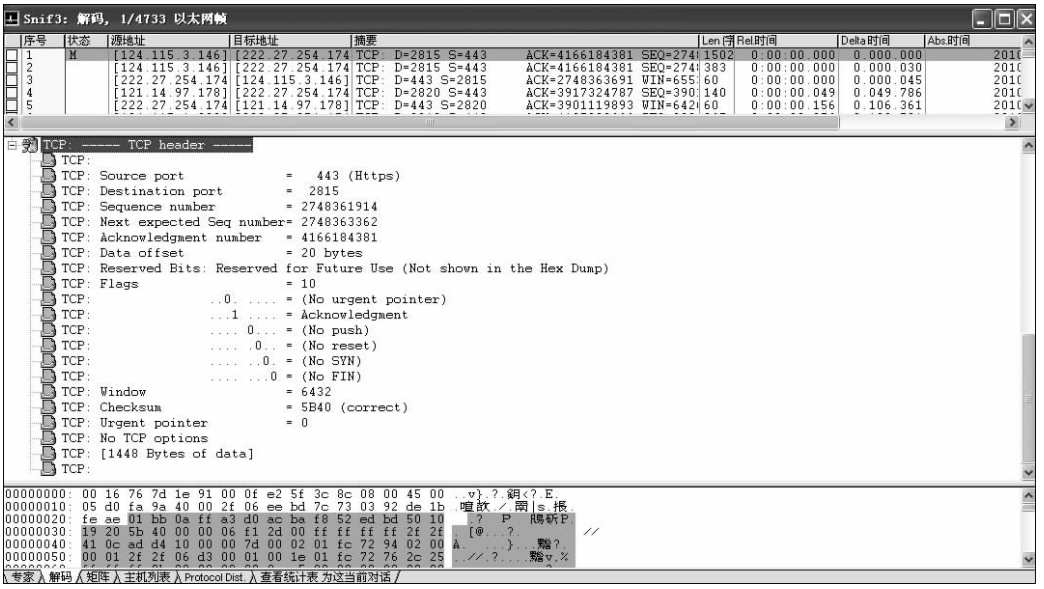

图 3.2.24　报文解码

4. 统计分析

对于各种报文信息，专家系统提供了矩阵分析（见图 3.2.25）、主机列表分析（见图 3.2.26）、协议统计分析（见图 3.2.27）以及会话统计分析（见图 3.2.28）等多种统计分析功能，可以按照 MAC 地址、IP 地址、协议类型等内容进行多种组合分析。

5. 捕获条件设置

在 Sniffer 环境下，可以通过【定义】的方式对捕获条件进行设置，获得用户需要的报文协议信息。基本的捕获条件有两种。

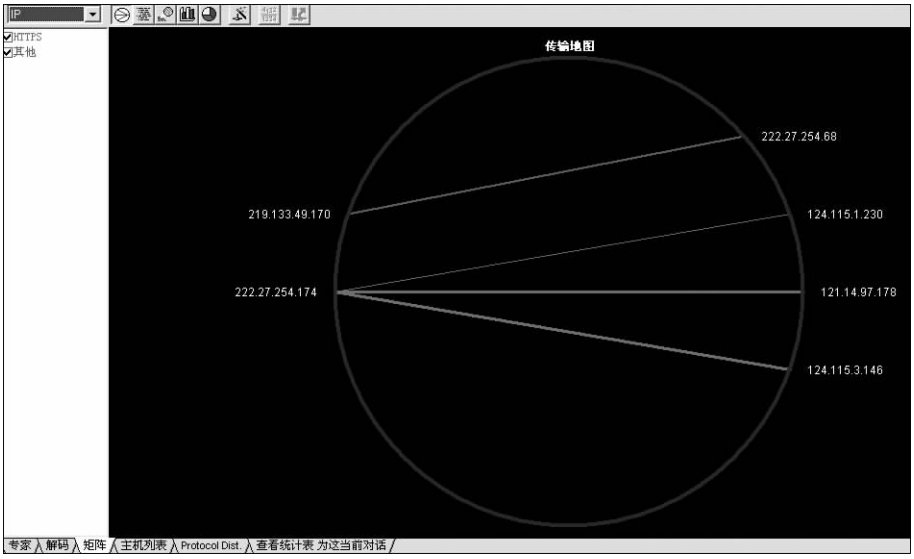

图 3.2.25　矩阵分析

		入埠数据包	入埠字节	出埠数据包	出埠字节	数据包总数	字节总数
	[illegible]	4	1209	5	320	9	1529
IP	000FE25F3C8C	6	402	6	1413	12	1815
	本地	2	204	1	82	3	286

图 3.2.26　主机列表分析

协议	数据包	字节
HTTPS	9	1529
其他	3	286

图 3.2.27　协议统计分析

变量	值
开始捕获次数	2010-06-21 08:27
捕获持续时间	0:00:01.934
字节总数	1815
总数数据包	12
平均数据包大小	151
字节每秒	938
数据包每秒	6
平均利用	0%
线速度	100 Mbps
MAC广播数据包	0
MAC多点传送数据包	0
IP信息包	12
IP字节	1815
IP广播数据包	0
IP多点传送数据包	0
TCP数据包	9
TCP字节	1529
UDP数据包	3
UDP字节	286
ICMP数据包	0
ICMP字节	0
IPX数据包	0
IPX字节	0
IPX广播数据包	0
IPX多点传送数据包	0

图 3.2.28　会话统计分析

(1) 链路层捕获：按照源 MAC 地址和目的 MAC 地址设定捕获条件，输入方式为十六进制 MAC 地址，如 000D98ABCDFE。