高等学校计算机课程规划教材

网络与信息安全综合实践

王盛邦　编著

清华大学出版社

高等学校计算机课程规划教材

网络与信息安全综合实践

王盛邦　编著

清华大学出版社
北京

内 容 简 介

本书主要介绍网络与信息安全面临的问题和采用的技术。全书共10章，内容包括实验基础(常用的网络命令、TCP/UDP/ICMP协议、常用工具软件等)、网络扫描与嗅探技术、防火墙技术、木马技术、Web安全技术、入侵检测与蜜罐技术、VPN技术、数据加密技术、认证技术和信息隐藏技术。本书内容丰富，实例众多，实例针对性强，叙述和分析透彻，每章都配有相关实验习题，具有可读性、可操作性和实用性强的特点。

本书适合作为计算机网络工程、信息安全等专业本专科教材，也可供网络工程技术人员参考。

图书在版编目(CIP)数据

网络与信息安全综合实践/王盛邦编著. --北京：清华大学出版社，2016
高等学校计算机课程规划教材
ISBN 978-7-302-42342-3

Ⅰ. ①网…　Ⅱ. ①王…　Ⅲ. ①计算机网络－信息安全－高等学校－教材　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2015)第296276号

责任编辑：汪汉友　战晓雷
封面设计：傅瑞学
责任校对：时翠兰
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954

印 装 者：三河市金元印装有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：19.5　　**字　　数**：472千字
版　　次：2016年3月第1版　　**印　　次**：2016年3月第1次印刷
印　　数：1～2000
定　　价：39.50元

产品编号：064101-01

前　言

随着计算机网络在政治、军事、金融、商业等领域的广泛应用，人类社会对计算机网络的依赖性越来越强。网络系统如果遭到破坏，不仅会引起社会混乱，还将带来巨大的经济损失。加快网络安全保障体系的建设、培养高素质的网络安全人才队伍迫在眉睫。编者根据教研实践编写了本书。本书以通俗易懂的形式向读者介绍网络与信息安全技术和研究成果。本书着重于理论知识与实践相结合，希望能对网络工程类、信息安全专业的学生和其他感兴趣的读者提供实质性的帮助。

本书主要介绍网络与信息安全面临的问题和采用的多种技术。第 1 章是本书的基础，介绍常用的网络命令、TCP/UDP/ICMP 协议、常用工具软件(网络包分析工具 Wireshark、网络扫描器 Nmap、漏洞扫描器 Nessus、数学软件 MATLAB 的图像函数等)，这些知识将会在后续内容中用到；第 2 章介绍网络扫描的主机存活扫描(ping)、端口扫描、操作系统探测、漏洞探测、防火墙规则探测五大主要扫描技术以及嗅探技术的原理等；第 3 章介绍包过滤型、状态检测型、应用代理型防火墙的技术原理与应用，涉及 Linux 的防火墙工具 iptables、Windows 的自带防火墙等；第 4 章介绍木马的技术原理，通过实例分析木马的危害；第 5 章介绍 Web 面临的主要威胁，包括 SQL 注入、跨站脚本攻击、网页挂马等攻击类型，提出一些防御措施；第 6 章介绍入侵检测和蜜罐两种重要技术；第 7 章介绍 VPN 技术；第 8 章介绍加密技术，如 DES、RSA、混沌加密等；第 9 章介绍多种认证技术，包括口令身份、PKI 数字证书技术、数字签名技术、SSL 技术、智能卡认证、基于生物特征认证；第 10 章主要介绍数字水印技术中的空间数字水印、频率数字水印。本书提供了大量的应用实例，每章都配有相当数量、类型多样的习题。

本书由王盛邦编写，谢逸、农革审阅。审阅者对本书内容提出了很多宝贵的修改意见，编者在此表示感谢。

在本书编写过程中，编者参阅了大量书籍资料，包括网络上论坛、博客，借鉴了许多网络工程经验。中山大学公共教学实验中心刘树郁博士对本书的编写给予了大力支持。清华大学出版社相关人员为本书的顺利出版做了大量的工作。在此对所有为本书的顺利出版提供帮助的人士及所有参考文献的作者表示衷心的感谢。

由于编者水平有限，不足之处在所难免，读者在使用本书的过程中，如果发现错误和不当之处，敬请与编者联系，编者的联系方式为 wangshb@mail.sysu.edu.cn。

编　者

2015 年 12 月

目　录

第1章 实验基础

本章主要介绍与实验有关的基础知识，包括常用的网络命令、网络包分析工具Wireshark、网络扫描分析工具Nmap、漏洞扫描分析工具Nessus、数学软件MATLAB的图像函数以及实验报告的书写要求等。

1.1 常用网络命令

Windows操作系统中有一个命令行解释器，它类似于MS-DOS的命令解释程序，可以在其中输入一些命令，实现用户和操作系统之间的直接通信。命令行解释器提供基于字符的应用程序和实用程序的用户界面，可通过选择“开始”→“所有程序”→“附件”→“命令提示符”方式进入命令行解释器（即命令提示符窗口），或通过单击“开始”菜单，在“搜索和文件”对话框中输入cmd命令快速进入命令提示符窗口。然后在提示符>后通过键盘输入命令，可以通过在命令后加/？来获得使用帮助。

在网络与信息安全实践中，命令行命令是非常实用的工具，需要熟练掌握。由于网络命令较多，本章仅介绍常用的命令。

1.1.1 ping命令

在进行网络实验、调试的过程中，ping是最常用的一个命令。ping命令全称Packet Internet Grope（因特网包探测器），一般用来测试源主机到目的主机网络的连通性。ping命令是在IP层中利用回应请求/应答ICMP报文来测试目的主机或路由器的可达性的。不同操作系统对ping命令的实现有所差异。通过执行ping命令主要可获得如下信息：

（1）监测网络的连通性，检验与远程计算机或本地计算机的连接。

（2）确定是否有数据包被丢失、复制或重传。ping在所发送的数据包中设置唯一的序列号，以此检查其接收到的应答报文的序列号。

（3）ping在其所发送的数据包中设置时间戳（timestamp），根据返回的时间戳信息可以计算数据包往返的时间（Round Trip Time，RTT）。

（4）ping校验每一个收到的数据包，据此可以确定数据包是否损坏。

在Windows环境下，ping命令语法如下：

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count]
[[-j host-list] | [-k host-list]] [-w timeout] [-R] [-S srcaddr] [-4] [-6] target
_name
```

其中：

-t　　ping指定的主机，直到停止。若要查看统计信息并继续操作，按Ctrl+Break键；若要停止，按Ctrl+C键。

-a	将地址解析成主机名。
-n count	要发送的回显请求数。
-l size	发送缓冲区大小。
-f	在数据包中设置“不分段”标志(仅适用于 IPv4)。
-i TTL	生存时间。
-v TOS	服务类型(仅适用于 IPv4。该设置已不建议使用,且对 IP 标头中的服务字段类型没有任何影响)。
-r count	记录计数跃点的路由(仅适用于 IPv4)。
-s count	计数跃点的时间戳(仅适用于 IPv4)。
-j host-list	与主机列表一起的松散源路由(仅适用于 IPv4)。
-k host-list	与主机列表一起的严格源路由(仅适用于 IPv4)。
-w timeout	等待每次回复的超时时间(毫秒)。
-R	同样使用路由标头测试反向路由(仅适用于 IPv6)。
-S srcaddr	要使用的源地址。
-4	强制使用 IPv4。
-6	强制使用 IPv6。

在这些参数中,用得较多的有 t、l、s 等。t 表示不停地 ping 目的主机,直到按下 Ctrl+C 键时手动停止;l 表示发送缓冲区大小(默认值为 32B);s 表示使用时间戳选项(仅适用于 IPv4)。ping 命令的许多选项实际上是指定因特网如何处理和携带回应请求/应答 ICMP 报文的 IP 数据包。

1. 发送 ping 测试报文

发送 ping 测试报文可以不用选项。如执行命令“ping IP 地址”或“ping 域名”,则向指定的 IP 地址的主机或域名发送 ping 测试报文,这是最常用的一种使用方法。

【例 1-1】 ping 搜狐公司的域名。

```
C:\>ping www.sohu.com
Pinging pgderbjt01.a.sohu.com [118.228.148.143] with 32 bytes of data:
Reply from 118.228.148.143: bytes=32 time=69ms TTL=48
Reply from 118.228.148.143: bytes=32 time=69ms TTL=48
Reply from 118.228.148.143: bytes=32 time=64ms TTL=48
Reply from 118.228.148.143: bytes=32 time=67ms TTL=48

Ping statistics for 118.228.148.143:
    Packets: Sent=4, Received=4, Lost=0(0%loss),
Approximate round trip times in milli-seconds:
    Minimum=64ms, Maximum=69ms, Average=67ms
```

【例 1-2】 ping 搜狐公司的 IP 地址。

```
C:\>ping 118.228.148.143
Pinging 118.228.148.143 with 32 bytes of data:
Reply from 118.228.148.143: bytes=32 time=67ms TTL=48
Reply from 118.228.148.143: bytes=32 time=64ms TTL=48
```

```
Reply from 118.228.148.143: bytes=32 time=67ms TTL=48
Reply from 118.228.148.143: bytes=32 time=65ms TTL=48

Ping statistics for 118.228.148.143:
    Packets: Sent=4, Received=4, Lost=0(0%loss),
Approximate round trip times in milli-seconds:
    Minimum=64ms, Maximum=67ms, Average=65ms
```

在例 1-1 中，我们知道了域名 www.sohu.com 的 IP 地址是 118.228.148.143，所以在例 1-2 中改用 ping IP 地址，结果是一样的。此例说明，可以利用该命令从域名查找对应的 IP 地址。

在例 1-1(或例 1-2)命令显示的结果中都返回了 4 个测试数据包，其中 bytes=32 表示测试中发送的数据包大小是 32B，time=67ms 表示与对方主机往返一次所用的时间是 67ms。信息显示，这 4 个数据包中返回速度最快的为 64ms，最慢的为 69ms，平均速度为 67ms。ping 能够以毫秒为单位显示发送回送请求和收到回送应答之间的时长。如果应答时间短，表示数据包没有通过太多的路由器或者网络连接速度较快。

TTL=48 表示当前测试使用的 TTL 值为 48。因为 ping 命令使用网络层协议 ICMP，所以 TTL(Time to Live，生存时间)指的是一个网络层的数据包(package)的生存周期。

TTL 的作用是在过长路径或有环路情况下令设备抛弃 ICMP Request 包。因为一个包从一台机器到另一台机器中间可能需要经过很长的路径，这个路径可能是很复杂的，并且很可能存在环路。假设一个数据包在传输过程中进入了环路，如果不终止它，它会一直循环下去，如果很多个数据包都这样循环，将会严重影响网络的正常运行。所以需要在包中设置生存时间，并且在包每经过一个结点时，将这个值递减 1，最终包在这个值还是正数的时候到达目的地，或者是在经过一定数量的结点后，这个值减为 0。前者代表完成了一次正常的传输；后者代表包可能选择了一条非常长的路径，甚至是进入了环路，所以在这个值为 0 的时候，网络设备将不会再传递这个包，而是直接将其抛弃，并发送一个通知给包的源地址。

2. 连续发送 ping 测试报文

在网络调试过程中，有时需要连续发送 ping 测试报文，一旦配置正确，测试主机可以立即报告目的地可达信息。连续发送 ping 测试报文可以使用-t 选项。如执行命令

```
ping 192.168.1.100 -t
```

表示连续向 IP 地址为 192.168.1.100 的主机发送 ping 测试报文，可以使用组合键 Ctrl+Break 显示发送和接收回应请求/应答 ICMP 报文的统计信息，此时 ping 仍然继续。要结束 ping 命令，可以使用 Ctrl+C 键。

3. 自选数据长度的 ping 测试报文

在默认情况下，ping 命令使用的测试报数据长度为 32B，使用-l Size 选项可以指定测试数据的长度。

【例 1-3】 将 ping 的数据报长度设为 1560B：

```
C:\ >ping 92.168.1.100 -l 1560
Pinging 192.168.1.100 with 1560 bytes of data:
Reply from 192.168.1.100: bytes=1560 time<1ms TTL=128
```

```
Reply from 192.168.1.100: bytes=1560 time<1ms TTL=128
Reply from 192.168.1.100: bytes=1560 time<1ms TTL=128
Reply from 192.168.1.100: bytes=1560 time<1ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent=4, Received=4, Lost=0(0%loss),
Approximate round trip times in milli-seconds:
    Minimum=0ms, Maximum=0ms, Average=0ms
```

虽然-l 参数可以自定义，但是最大值限制为 65 500B。

在 ping 的使用中，还常用 ping 127.0.0.1 来检测 TCP/IP 协议是否工作正常，其中 127.0.0.1 是本地环回地址，如发现本地地址无法 ping 通，就表明本地机器 TCP/IP 协议不能正常工作。

在排除网络连通性故障时 ping 命令非常有用，但是它也存在局限性。在一些场合需要使用 tracert 命令，它可以显示网络响应时间和路径信息。

黑客的攻击往往是从 ping 开始的，一般用它判断主机是否在线。历史上 ping 曾被作为一款攻击工具使用，即所谓的 ping of death(死亡之 ping)，它通过多台 PC 发送特大 ping 数据包(65 500B)导致目标机器崩溃。

1.1.2 tracert 命令

tracert(trace route，跟踪路由)是路由跟踪实用程序，用于获得 IP 数据报访问目标时从本地计算机到目的主机的路径信息。tracert 通过发送数据报到目的设备，根据应答报文(ICMP)得到路径和延迟信息(TTL)。对于一条路径上的每个设备 tracert 要测 3 次，因而有 3 个探测包的回应时间。一般在网络状态稳定的情况下，3 个时间差不多；如果这 3 个时间相差比较大，说明网络状态变化较大。

tracert 通过向目的地发送具有不同 IP 生存时间（TTL）值的 Internet 控制消息协议(ICMP)回送请求报文，以确定到达目的地的路由。所显示的路径是源主机与目标主机间的路径中的路由器的近侧路由器接口列表。近侧接口是距离路径中的发送主机最近的路由器的接口。tracert 先发送 TTL 为 1 的回应数据包，并在随后的每次发送过程中将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。这一点与 ping 命令不同，ping 时 TTL 是递减的，数据包上的 TTL 减为 0 时，路由器应该将“ICMP 已超时”的消息发回源系统。某些路由器不经询问直接丢弃 TTL 过期的数据包，这在 tracert 实用程序中是看不到的。在这种情况下，将为该跃点(hop)显示一行星号(*)。

tracert 命令在执行时会很缓慢，这主要是 tracert 试图将中间路由器的 IP 地址解析为它们的名称。如果使用-d 选项，则 tracert 实用程序不在每个 IP 地址上查询 DNS，这样可加速显示 tracert 的结果。tracert 的输出结果中包括每次测试的时间和设备的名称或 IP 地址。

在 Windows 环境下，tracert 命令语法如下：

```
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] [-R] [-S srcaddr] [-4]
[-6] target_name
```

其中：

-d	不将地址解析成主机名。
-h maximum_hops	搜索目标的最大跃点数。
-j host-list	与主机列表一起的松散源路由(仅适用于 IPv4)。
-w timeout	等待每个回复的超时时间(以毫秒为单位)。
-R	跟踪往返行程路径(仅适用于 IPv6)。
-S srcaddr	要使用的源地址(仅适用于 IPv6)。
-4	强制使用 IPv4。
-6	强制使用 IPv6。

【例 1-4】 如果数据包必须通过两个路由器(10.10.10.1 和 192.168.0.1)才能到达主机 172.16.0.88，主机的默认网关是 10.10.10.1，那么 192.168.0.1 网络上的路由器的 IP 地址是 192.168.0.1。

```
C:\>tracert 172.16.0.88 -d
Tracing route to 172.16.0.88 over a maximum of 30 hops
1  30ms   35ms   30ms   10,10.10,1
2  45ms   55ms   50ms   192.168.0.1
3   *      *      *     Request timed out.
4  63ms   66ms   60ms   172.16.0.88
Trace complete.
```

第 1 列是经过路由节点的顺序编号。第 2～4 列表示一个路由节点到另外一个路由节点的通信时间，单位是毫秒。其中 * 表示超时，没有解析出正确地址。这是由于这些路由器对于 tracert 命令不可见(可能基于安全考虑，路由节点隐蔽了其信息)。在这种情况下，将为该跃点显示一行星号。最后一列是途经路由器的 IP 地址。

【例 1-5】 跟踪 www.sina.com 路由。

```
C:\>tracert www.sina.com
Tracing route to newssy.sina.com.cn [218.60.32.23]
over a maximum of 30 hops:
1  1 ms    <1 ms   <1 ms   218.25.120.49
2  <1 ms   1 ms    1 ms    218.25.3.209
3  <1 ms   <1 ms   <1 ms   218.25.2.125
4  1 ms    <1 ms   <1 ms   218.25.2.98
5  6 ms    5 ms    9 ms    cncln.online.ln.cn [218.60.20.250]
6  *       *       *       Request timed out.
7  1 ms    <1 ms   <1 ms   cncln.online.ln.cn [218.60.22.246]
8  <1 ms   <1 ms   <1 ms   cncln.online.ln.cn [218.60.32.23]
Trace complete.
```

结果显示，5 和 6 路由节点之间在 tracert 测试下超时。但是因为后面 7、8 能返回正确结果，说明网络仍然是畅通的。

tracert 命令虽然可以查看路由信息，但是目前大多数路由器都对 tracert 命令做了限制，导致 tracert 命令没有解析出正确地址。黑客软件 x-firewalk.exe(下载地址是 http://

www. xdoors. net/)也可用于在 Windows 环境下查看路由信息，且比 tracert 实用。

1.1.3 ipconfig 命令

ipconfig 命令可以显示所有当前的 TCP/IP 网络配置值(如 IP 地址、网关、子网掩码)、刷新动态主机配置协议 (DHCP) 和域名系统 (DNS) 设置。

在 Windows 环境下，ipconfig 命令的语法格式如下：

```
ipconfig [/allcompartments] [/? | /all | /renew [adapter] | /release [adapter] |
                                  /renew6 [adapter] | /release6 [adapter] |
                                  /flushdns | /displaydns | /registerdns |
                                  /showclassid adapter |
                                  /setclassid adapter [classid] |
                                  /showclassid6 adapter |
                                  /setclassid6 adapter [classid] ]
```

其中：

/?	显示此命令的帮助消息。
/all	显示完整配置信息。
/release	释放指定适配器的 IPv4 地址。
/release6	释放指定适配器的 IPv6 地址。
/renew	更新指定适配器的 IPv4 地址。
/renew6	更新指定适配器的 IPv6 地址。
/flushdns	清除 DNS 解析程序缓存。
/registerdns	刷新所有 DHCP 租约并重新注册 DNS 名称。
/displaydns	显示 DNS 解析程序缓存的内容。
/showclassid	显示适配器的所有允许的 DHCP 类 ID。
/setclassid	修改 DHCP 类 ID。
/showclassid6	显示适配器允许的所有 IPv6 DHCP 类 ID。
/setclassid6	修改 IPv6 DHCP 类 ID。

ipconfig 命令最适用于配置为自动获取 IP 地址的计算机。它使用户可以确定哪些 TCP/IP 配置值是由 DHCP、自动专用 IP 寻址和其他配置方式设置的。

如果 adapter(适配器名称)中包含空格，要在该适配器名称两边使用引号(即"适配器名称")。

对于适配器名称，ipconfig 可以使用星号(*)通配符字符指定名称为指定字符串开头的适配器或名称包含有指定字符串的适配器。例如，Local* 可以匹配所有以字符串 Local 开头的适配器，而 *Con* 可以匹配所有包含字符串 Con 的适配器。

下面是一些使用实例。

(1) 显示所有适配器的基本 TCP/IP 配置：

```
ipconfig
```

(2) 显示所有适配器的完整 TCP/IP 配置：

```
ipconfig /all
```

(3) 仅更新“本地连接”适配器的由 DHCP 分配 IP 地址的配置：

```
ipconfig /renew
```

(4) 在排除 DNS 的名称解析故障期间刷新 DNS 解析器缓存：

```
ipconfig /flushdns
```

(5) 仅更新 Local Area Connection 适配器的由 DHCP 分配 IP 地址的配置：

```
ipconfig /renew "Local Area Connection"
```

(6) 在排除 DNS 的名称解析故障期间刷新 DNS 解析器缓存：

```
ipconfig /flushdns
```

(7) 显示名称以 Local 开头的所有适配器的 DHCP 类别 ID：

```
ipconfig /showclassid Local *
```

(8) 要将 Local Area Connection 适配器的 DHCP 类别 ID 设置为 TEST：

```
ipconfig /setclassid "Local Area Connection" TEST
```

其中，(1) 和(2)是 ipconfig 命令两种最常用的使用形式。

在 IPv6 协议下，ipconfig /all 命令显示的内容包括所有接口的 IPv6 地址、默认路由器和 DNS 服务器。

1.1.4 netstat 命令

netstat 命令可以显示当前活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息(对于 IP、ICMP、TCP 和 UDP 协议)以及 IPv6 统计信息(对于 IPv6、ICMPv6、通过 IPv6 的 TCP 以及通过 IPv6 的 UDP 协议)。

在 Windows 环境下，netstat 的语法格式如下：

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

其中：

-a　　显示所有连接和侦听端口。

-b　　显示在创建每个连接或侦听端口时涉及的可执行组件。在某些情况下，已知可执行组件拥有多个独立组件，此时，显示创建连接或侦听端口时涉及的组件序列，可执行组件的名称位于底部[]标记中，它调用的组件位于顶部，直到 TCP/IP 部分。注意，此选项可能很耗时，并且在没有足够权限时可能失败。

-e　　显示以太网统计。此选项可以与 -s 选项结合使用。

-f　　显示外部地址的完全限定域名(FQDN)。

-n　　以数字形式显示地址和端口号。

-o　　显示拥有的与每个连接关联的进程 ID。

-p proto　　显示 proto 指定的协议的连接；proto 可以是下列任何一个：TCP、UDP、TCPv6 或 UDPv6。如果与 -s 选项一起用来显示每个协议的统计，proto 可以是下列任何一个：IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6。

-r　　显示路由表。

-s　　显示每个协议的统计。默认情况下，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息。-p 选项可用于指定默认的子网。

-t　　显示当前连接卸载状态。

interval　　重新显示选定的统计信息，各个显示间暂停的间隔秒数。按 Ctrl+C 键停止重新显示统计。如果省略 interval，则 netstat 将打印当前的配置信息一次。

下面是一些使用实例。

(1) 显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口：

```
netstat -an
```

(2) 显示以太网统计信息，如发送和接收的字节数、数据包数：

```
netstat -e -s
```

(3) 仅显示 TCP 和 UDP 协议的统计信息：

```
netstat -s -p tcp udp
```

(4) 每 5s 显示一次活动的 TCP 连接和进程 ID：

```
netstat -o 5
```

(5) 以数字形式显示活动的 TCP 连接和进程 ID：

```
netstat -n -o
```

netstat 命令的一个重要作用是端口占用查询，据此可以发现本机开放的端口是否被植入了木马或其他黑客程序。

1.1.5 arp 命令

arp(address resolution protocol，地址解析协议)命令是把基于 TCP/IP 的软件使用的 IP 地址解析成 LAN 硬件使用的介质访问控制地址(一般指网卡地址，也称 MAC 地址)。执行 arp 命令对同一物理网络上的主机提供以下协议服务：

(1) 通过使用网络广播请求获得介质访问控制地址(即由厂商为设备编入的唯一地址，通常用十六进制表示，如 00-AA-00-3F-89-4A)，询问“配置成包含 IP 地址的设备的介质访问控制地址是什么?”

(2) 回应 ARP 请求时，ARP 回复的发送方和原始 ARP 请求方都将彼此的 IP 地址及介质访问控制地址记录成被称为 ARP 缓存的本地表中的项目，以便将来引用。

为使广播量最小，ARP 维护 IP 地址到介质访问控制地址映射的缓存以便将来使用。ARP 缓存可以包含动态和静态项目。动态项目随时间推移自动添加和删除；静态项目一直

保留在缓存中，直到重新启动计算机为止。

每个动态 ARP 缓存项目的潜在生存时间是 10min。新加到缓存中的项目带有时间戳。如果某个项目添加后 2min 内没有再使用，则此项目过期并从 ARP 缓存中删除。如果某个项目已在使用，则又增加 2min 的生存时间。如果某个项目始终在使用，则会继续维持 2min 的生命周期，一直到 10min 的最长生存时间。

arp 命令的语法格式如下：

```
arp -s inet_addr eth_addr [if_addr]
arp -d inet_addr [if_addr]
arp -a [inet_addr] [-N if_addr] [-v]
```

其中：

-a	通过询问当前协议数据，显示当前 ARP 项。如果指定 inet_addr，则只显示指定计算机的 IP 地址和物理地址。如果不止一个网络接口使用 ARP，则显示每个 ARP 表的项目。
-g	与 -a 相同。
-v	在详细模式下显示当前 ARP 项。所有无效项和环回接口上的项都将显示。
inet_addr	指定 Internet 地址。
-N if_addr	显示 if_addr 指定的网络接口的 ARP 项。
-d	删除 inet_addr 指定的主机。inet_addr 可以是通配符 *，即删除所有主机。
-s	添加主机并且将 Internet 地址 inet_addr 与物理地址 eth_addr 相关联。物理地址是用连字符分隔的 6 个十六进制字节，该地址是永久的。
eth_addr	指定物理地址。
if_addr	如果存在，此项指定地址转换表应修改的接口的 Internet 地址。如果不存在，则使用第一个适用的接口。

表中 inet_addr 和 if_addr 的 IP 地址用点分十进制记数法表示。物理地址 eth_addr 长度为 6B，这些字节用十六进制记数法表示并且用连字符隔开（比如，00-AA-00-5E-3B-6D）。

下面是一些使用实例。

(1) 显示所有接口的 ARP 缓存表：

```
arp -a
```

(2) 显示 IP 地址为 192.168.1.100 的接口 ARP 缓存表：

```
arp -a -N 192.168.1.100
```

(3) 要将 IP 地址 10.0.0.80 与物理地址 00-AA-00-4F-2A-9C 绑定(静态 ARP 缓存项)：

```
arp -s 10.0.0.80 00-AA-00-4F-2A-9C
```

(4) 删除所有接口的 ARP 缓存表：

```
arp -d
```

值得注意的是，在 IPv6 协议下，已经取消了 ARP 协议，代之以 NDP(邻居发现)协议。