计算机百科知识

计算机网络基础

(二)

本书编写组　编

山东科学技术出版社

图书在版编目(CIP)数据

计算机百科知识/本书编写组编．—济南：山东科学技术出版社，2003

ISBN 7-5331-1651-8
Ⅰ．计… Ⅱ．本… Ⅲ．计算机网络—基本知识—汇编
Ⅳ．TP39
中国版本图书馆 CIP 数据核字(2003)第 004271 号

山东科学技术出版社出版发行
(济南市玉函路 16 号 250001)
全国各地新华书店经销 莒县新华印刷厂印刷
开本：787×1092 1/32 印张：240 字数：4 000 千字
2003 年 7 月第 1 版 2003 年 7 月第 1 次印刷
印数：1～1 000 册
书号：ISBN 7-5331-1651-8/D·112
定价：698.00 元

目　录

IE 地址栏技巧点滴

IE 是大家使用最多的浏览器，而地址栏是浏览器最主要的部分之一，这里介绍几个容易被大家忽略的 IE 地址栏技巧。

1.浏览网页时，经常使用键盘。这时要输入网址，还要动用鼠标去点一下地址栏，太麻烦了。其实只要按一下地址栏快捷键 Alt+D 就可以了。

2.输错网址后要修改。移动光标时只能以一个字母为单位，如果能像 Word 一样整词移动就好了。其实在 IE 中按住 Ctrl 键就可以整词移动了。

3.输入地址时，一般不需要输入“http://”，比如“网易”只要输入“www.163.com”就可以了。其实还有一个更简捷的方法，比如在地址栏输入“163”，然后按一下 Ctrl+Enter 键，瞧，IE 就自动给加上“http://www”和“com”。

4.要显示所有输入过的地址，可以按 Ctrl+F4 组合键，然后可以用上下方向控制键选择

“宽带中国河南”应用平台使用指南

如何登录“宽带中国河南”门户网站

一、我可以使用“宽带中国河南”（www.kuandaiha.cn）门户网站提供的应用服务吗？

答：可以使用“宽带中国河南”网站服务的用户

有以下三种：

1.宽带注册用户：指的是通过宽带接入帐号方式接入河南通信宽带互联网的宽带用户，且已经购买了河南通信应用业务。

2.应用注册用户：指的是到河南通信营业前台申请办理应用注册帐号的用户。

3.应用卡用户：指的是通过购买河南通信发行的“河南通信应用卡”进行应用内容消费的用户。

二、登录方式有哪两种？

答：1 从门户站点直接登录，即访问www.kuandaiha.cn；

2 从宽带中国河南加盟网站直接登录，步骤见第四条。

三、如何从门户站点直接登录？

答:1.输入“宽带中国河南”网址（http://www.kuandaiha.cn），进入“宽带中国河南”首页。

2.在网站右上角选择登录方式：快捷登录和正常登录。快捷登录方式只限于宽带注册用户；正常登录方式包含：宽带注册用户、应用注册用户和应用卡用户，即所有宽带中国河南用户。

3.对于宽带注册用户，直接点击“快捷登录”按

钮进行登陆；若要使用其他帐号，可选择登录方式为：“正常登录”，录入帐号、密码即可。

4.对于应用卡用户和应用注册用户，点击“正常登录”按钮，录入相应的帐号、密码即可。

5.登陆成功之后，应用计费系统后台返回结果“您已经登录”，并显示用户类型、用户帐号信息。

6.登录成功之后，用户从门户网站点击加盟网站的链接或者直接输入加盟 ICP 的网址，即可开始访问加盟网站提供的内容；也可直接点击网站上方的各个频道访问相关内容。

四、如何从加盟网站登录？

答：步骤如下：

1.用户在浏览器中输入加盟网站网址，在页面上点击登陆按钮，如有必要同时选择用户身份为“宽带中国河南用户”。

2.重复第三条 2—4 步操作进行登录，登录成功之后会直接返回原加盟网站。

五、我未登录就直接访问收费内容结果怎样？

答：1.用户未登录就直接点击相关收费内容，提示用户登录；

2.按照第三条完成登录，登录成功之后会直接返回到登录之前访问内容所在的位置，即可开始访问所

有内容。

用户如何对网站内容进行消费

一、应用内容消费的方式有那些？

答：应用内容的消费方式如下所示：

说明：用户可根据页面提示自行选择消费方式，收费标准以各个网站的标价为准。

二、用户包月定购要注意些什么？

1 如何进行栏目包月？

（1）点击栏目链接，用户进入收费栏目页面，页面会在包月信息区显示当前用户是否已经对栏目进行包月。如果用户还没有对当前栏目进行包月，则包月信息区会显示包月按钮，并提示用户可以对当前栏目进行包月。

（2）用户点击“订购”按钮，看到提示信息：决定包月，点击“确定”按钮。对于预付费用户系统将检查卡中余额，若余额足够，则包月成功；反之则提示：“余额不足”。如果用户不想包月，点击“取消”按钮，返回上一页，不会扣除任何费用。

2、如何进行会员服务包月？

1）用户点击网站会员服务定购的链接，进入会员服务包月定购页面。

2)会员服务包月定购页面包含了会员的介绍以

及定购包月的注意事项。用户点击“我要订购”按钮，看到提示信息：决定包月，点击“确定”按钮。对于预付费用户，系统将检查卡中余额。若余额足够，则包月成功；反之则提示：“余额不足”。如果用户不想包月，点击“取消”按钮，返回上一页，不会扣除任何费用。

3、包月定购注意事项有哪些？

（1）包月成功以后，用户再访问所包栏目或网站所有的内容将不再收费。

（2）完成包月以后，系统将在每个帐务周期开始(每月的 21 日)自动扣除下一个帐务周期的包月费用。

（3）定购时间与收费标准：用户于上月 21 日到本月5日前定购的包月费将一次性扣除一个月的费用，本月 6 日到 20 日前定购的包月费将一次性扣除半个月的费用。以此类推。

（4）如果用户下一个月不想对此栏目或网站继续包月，则需要在下一个帐务周期开始之前（每月 20 日前）在用户自维护页面当中取消会员定购。用户确认取消包月当时，访问该栏目每次都需要付费。如果该包月栏目属于会员服务，则不能继续访问。

（5）包月服务只对所包栏目或所包网站所属内

容生效，访问其他栏目或网站仍要按照相应的计费方式付费。

（6）对于加盟网站推出的会员服务，用户必须先定购，才能访问其内容。会员服务的收费方式为包月制，每月收取固定的费用。

访问中常遇到的问题

一、用户通过认证后，点击内容时（包月用户已定购）被告知“用户已在线”，如何解决？

答：可能存在以下两种问题：

1、用户当前的帐号、密码正被他人使用。由于系统要求同一帐号同时只允许在线一人，为了避免此类情况的发生，建议用户勿与他人共用同一帐号。

2、用户同时点击 2 部及以上收费内容。建议用户关掉其中一个播放器（如：mediaplay 等）。

二、用户观看在线电影时对计算机配置有什么要求？

答：因为现有的影片图像清晰并且采用了边看边解压的方式，所以为了保证观看效果，对机器的处理器和显卡有一定要求。最低配置如下：赛扬 550Mhz,，内存 64-128MB，显卡 8M 以上。推荐配置：奔 417GHZ，内存 256MB，显卡 32M。

三、用户点击影片后为什么要等待一段时间才能

观看？

答：因为影片需要缓冲，以便用户顺利在线观看，故需等待一段时间。

四、用户拿到初始帐号、密码后，是否应及时修改密码？

答：为了防止帐号、密码被盗用，请您及时在“用户自维护”栏内修改您的初始密码，建议密码不少于6位。

如何办理应用业务

一、应用业务处理种类有哪些？

答：包括开通和变更两种。

1、开通业务：特指用户新申请办理应用注册帐号业务。

2、变更业务：已拥有宽带注册用户帐号、应用注册帐号的用户办理关闭应用服务或开放应用服务的业务。

二、应用业务办理

1、应用业务受理方式有哪些？

答：两种办理方式：营业厅办理和网上办理。

2、营业厅主要受理哪些业务？

答：用户到各市通信公司营业厅现场办理应用业务，主要包括：

（1）应用注册帐号开通、变更业务；

（2）宽带注册用户帐号变更业务；

（3）应用卡的销售。

3、到营业厅如何办理应用注册帐号开通业务？

答：(1)拨号用户需携带《拨号新装机业务登记表》、宽带注册用户需携带《宽带新装机业务登记单》中登记的机主身份证、申请人身份证原件及上月缴费话单，单位用户需在申请表中加盖公章。

（2）用户填写《应用注册帐号申请登记表》，核查无误后，立即开通用户申请帐号。以上业务均不收取任何受理费用。

（3）用户通过此帐号可以单独使用河南通信应用服务，应用费用将最终计入此帐号。

4、到营业厅如何办理应用注册帐号变更业务？

答：(1)拨号用户需携带《拨号新装机业务登记表》、宽带注册用户需携带《宽带新装机业务登记单》中登记的机主身份证、申请人身份证原件及上月缴费话单，单位用户需在申请表中加盖公章。

（2）用户填写《应用业务变更登记表》，核查无误后，立即根据用户要求开通或关闭此应用注册帐号下应用业务。以上业务均不收取任何受理费用。

5、到营业厅如何办理宽带注册用户帐号变更业

务？

答：（1)宽带注册用户需携带《宽带新装机业务登记单》中登记的机主身份证、申请人身份证原件及上月缴费话单，单位用户需在申请表中加盖公章。

（2）用户填写《应用业务变更登记表》，核查无误后，立即根据用户要求开通或关闭此应用注册帐号下应用业务。以上业务均不收取任何受理费用。

6、具备受理条件的用户应用帐号开通时限如何？

答：宽带注册用户帐号：即开即通；

应用注册帐号：即开即通；

应用卡帐号：即开即通。

三、是否可通过网上办理应用帐号？

答：网上办理帐号目前尚未开通，具体开通时间将另行通知。开通后用户网上受理流程如下：

1、用户登录应用业务网上受理点，输入基本的信息，包括用户姓名、性别、身份证件号码、所在地区、出生年月、联系电话、电子信箱等。

2、用户选择需要购买的服务，即应用服务。

3、资料提交之后，显示确认信息，用户可以确认或取消。

4、用户确认之后系统自动为用户分配一个应用

卡帐号和密码，并提示用户进行充值。

四、对新受理的宽带注册用户，若不想继续使用应用服务怎么办？

答：对新受理的宽带注册用户（ADSL 和 LAN），除非有用户的特别说明，系统将为其同时开通互联网接入和应用内容两项服务。用户需要变更服务项目时（关闭应用内容服务或开放应用内容服务）需要到营业前台填写《应用业务变更登记表》申请办理（具体操作见第六部分）。

五、专线用户如何使用应用业务？

答：使用专线接入的用户只能使用应用卡或者另行申请应用注册帐号才能消费“宽带中国河南”网站上提供的所有有偿及无偿服务。

费用计收问题

一、应用内容以什么价格收费？

答：应用内容的价格由内容提供商制定，并在网页上有明确标注。如果您选择了对栏目进行包月计费，那么在所包的帐务月内每次使用包月栏目不需支付包月费以外的费用。

二、如果选择与固定电话捆绑缴费，那么帐单包括几项？

答：河南通信宽带用户通过其宽带用户帐号消费

的应用内容费用将直接计入此帐号。其话单分两部分：应用费用和接入费用。若为联机付费电话缴费，则用户月帐单上为三项：固定电话费用、应用费用和接入费用。

三、内容消费金额是否包含在接入包月费中？

答：不包含。您在“宽带中国河南”消费有偿内容产生的费用将单独计算，不包含在网络使用费之中。如：某宽带包月用户其所付的宽带接入包月费用是 100 元/月，当月在“宽带中国河南”上消费的有偿内容费用总计 20 元，则此用户当月应付的实际上网费用应是 120 元。

四、用户如何缴费？

答：三类用户缴费方式如下：

1、宽带注册用户：内容服务采用后付费方式，服务费用将全部计入宽带注册用户帐号，并与宽带接入费捆绑缴费。

说明：目前所有已开通的河南通信宽带用户均已开通应用业务，用户不需再到营业前台办理相关手续。若用户想要取消应用业务，需到营业前台办理应用业务变更。

2、应用注册用户：内容服务计费采用后付费和预付费两种方式，费用全部计入用户的应用业务注册

帐号。

说明：（1）对于选择预付费方式缴费的应用注册用户帐号，只能购买邮箱业务，不允许购买接入或应用等其它业务。对于可购买的邮箱业务的数量不做限制。

（2）对于选择后付费方式缴费的应用注册用户帐号，可以同时购买邮箱业务和应用业务，不允许购买接入业务。对于可购买的邮箱业务的数量不做限制。

3、应用卡用户：内容服务计费采用预付费方式，应用服务的消费费用将实时从应用卡中扣除。

如何查询及投诉

一、用户可通过自维护对其消费情况进行查询

1、自维护的登录

（1）用户登录成功以后，直接点击首页右上方的“用户自维护”链接进入。屏幕提示：“您好，XXX用户，您已经登录成功”；

（2）点击右侧的“互联网应用自服务”按钮进入。

注意事项：

（1）如果用户未登录直接点击“用户自维护”链接，则页面提示用户登录。

（2）除了“宽带中国河南”首页，每个加盟网站的页面上均有“用户自维护”链接，用户可以通过这些页面直接进入。

（3）点击“退出”会导致退出“宽带中国河南”网站，再访问收费内容，仍需重新登录。

2、点击右边“余额查询”，根据提示进行相关操作。

3、点击右边“修改密码”，填写当前密码，输入新密码两次，点击“确认”按钮，提示操作成功。

4、点击右边“帐务查询”，根据提示进行相关操作。

5、点击右边“余额转账”，根据提示进行相关操作。

6、点击右边“基本信息”，查看相关信息。

7、包月内容操作：

（1）点击右边“包月内容”链接，进入包月内容查询页面；

（2）输入查询条件，点击“确定”按钮；

（3）如果用户准备取消对已包月栏目的包月订购，选择该栏目后点击“取消包月”按钮，再点击“确定”按钮后，即可取消包月。

（4）用户取消包月以后，访问该栏目每次都需

要付费。如果该包月栏目属于会员服务，则不能继续访问。

8、用户反馈操作

（1）点击右边“用户反馈”连接进入。

（2）输入需要填写的信息，点击“确定”按钮，成功提交反馈信息。

计算机网络基础知识(一)

计算机网络就是计算机之间通过连接介质互联起来，按照网络协议进行数据通信，实现资源共享的一种组织形式。

什么是连接介质呢？连接介质和通信网中的传输线路一样，起到信息的输送和设备的连接作用计算机网络的连接介质种类很多，可以是电缆、光缆、双绞线等“有线”的介质，也可以是卫星微波等“无线”介质，这和通信网中所采用的传输介质基本上是一样的。

在连接介质基础上，计算机网络必须实现计算机间的通信和计算机资源的共享，因此它的结构，按照其功能可以划分成通信子网和资源子网两部分。当然，根据硬件的不同，将它分成主机和通信子网两部分也是正确的。

主机的概念很重要，所为主机就是组成网络的各

个独立的计算机。在网络中，主机运行应用程序。这里请注意区别主机与终端两个要领终端指人与网络打交道时所必需的设备，一个键盘加一个显示器即可构成一个终端，显然，主机由于要运行应用程序，只有一个键盘和显示器是不够的，还要有相应的软件和硬件才行。因此，不能把终端看成主机，但有时把主机看成一台终端是可以的。

协议是什么？拿电报来做比较，在拍电报时，必须首先规定好报文的传输格式，多少位的码长，什么样的码字表示启动，什么样的码字又表示结束，出了错误怎么办，怎地方发报人的名字和地址等，这种预先定好的格式及约定就是协议。

这样就也网络协议的定义：为了使网络中的不同设备能进行下沉的数据通信而预先制定一整套通信双方相互了解和共同遵守的格式和约定。

协议对于计算机网络而言是非常重要的，可以说没有协议，就不可能有计算机网。每一种计算机网络，都有一套协议支持着。由于现在在计算机网种类很多，所以现有的网络通信协议的种类也很多。典型的网络通信协议有开放系统互连（OSI）协议1、X 25 协议等。TCP/IP 则是为 Internet 互联的各种网络之间能互相通信而专门设计的通信协议。

可见，由于连接介质的不同，通信协议的不同，计算机网络的种类名目繁多。但一般来讲，计算机网络可以按照它覆盖的地理范围，划分成局域网和广域网。局域网一般指分布于几公里范围内的网络，常见的局域中校园网、大楼网等；广域网则在分范围很区域内提供数据通信服务，前面提到的 NSFnet，国内的如中国公用分组交换网（CHINAPAC）、中国公用数字数据网（CHINADDA）,以及建议中的国家教育和科研网(CERnet)等都属于广域网，建设好的 CHINANET 也将是一个广域网。

计算机网络基础知识（二）

计算机网络就是计算机之间通过连接介质互联起来，按照网络协议进行数据通信，实现资源共享的一种组织形式。

什么是连接介质呢？连接介质和通信网中的传输线路一样，起到信息的输送和设备的连接作用计算机网络的连接介质种类很多，可以是电缆、光缆、双绞线等“有线”的介质，也可以是卫星微波等“无线”介质，这和通信网中所采用的传输介质基本上是一样的。

在连接介质基础上，计算机网络必须实现计算机间的通信和计算机资源的共享，因此它的结构，按照

其功能可以划分成通信子网和资源子网两部分。当然，根据硬件的不同，将它分成主机和通信子网两部分也是正确的。

主机的概念很重要，所为主机就是组成网络的各个独立的计算机。在网络中，主机运行应用程序。这里请注意区别主机与终端两个要领终端指人与网络打交道时所必需的设备，一个键盘加一个显示器即可构成一个终端，显然，主机由于要运行应用程序，只有一个键盘和显示器是不够的，还要有相应的软件和硬件才行。因此，不能把终端看成主机，但有时把主机看成一台终端是可以的。

协议是什么？拿电报来做比较，在拍电报时，必须首先规定好报文的传输格式，多少位的码长，什么样的码字表示启动，什么样的码字又表示结束，出了错误怎么办，怎地方发报人的名字和地址等，这种预先定好的格式及约定就是协议。

这样就也网络协议的定义：为了使网络中的不同设备能进行下沉的数据通信而预先制定一整套通信双方相互了解和共同遵守的格式和约定。

协议对于计算机网络而言是非常重要的，可以说没有协议，就不可能有计算机网。每一种计算机网络，都有一套协议支持着。由于现在在计算机网种类很

多，所以现有的网络通信协议的种类也很多。典型的网络通信协议有开放系统互连（OSI）协议1、X25协议等。TCP/IP则是为Internet互联的各种网络之间能互相通信而专门设计的通信协议。

可见，由于连接介质的不同，通信协议的不同，计算机网络的种类名目繁多。但一般来讲，计算机网络可以按照它覆盖的地理范围，划分成局域网和广域网。局域网一般指分布于几公里范围内的网络，常见的局域中校园网、大楼网等；广域网则在分范围很区域内提供数据通信服务，前面提到的NSFnet，国内的如中国公用分组交换网（CHINAPAC)、中国公用数字数据网（CHINADDA),以及建议中的国家教育和科研网(CERnet)等都属于广域网，建设好的CHINANET也将是一个广域网。

路由基础

一、什么是路由

路由是把信息从源穿过网络传递到目的的行为，在路上，至少遇到一个中间节点。路由通常与桥接来对比，在粗心的人看来，它们似乎完成的是同样的事。它们的主要区别在于桥接发生在OSI参考协议的第二层（链接层），而路由发生在第三层（网络层）。这一区别使二者在传递信息的过程中使用不同的信息，从

而以不同的方式来完成其任务。

路由的话题早已在计算机界出现，但直到八十年代中期才获得商业成功，这一时间延迟的主要原因是七十年代的网络很简单，后来大型的网络才较为普遍。

二、路由的组成

路由包含两个基本的动作：确定最佳路径和通过网络传输信息。在路由的过程中，后者也称为（数据）交换。交换相对来说比较简单，而选择路径很复杂。

1、路径选择

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，如路径长度。为了帮助选路，路由算法初始化并维护包含路径信息的路由表，路径信息根据使用的路由算法不同而不同。

路由算法根据许多信息来填充路由表。目的/下一跳地址对告知路由器到达该目的最佳方式是把分组发送给代表“下一跳”的路由器，当路由器收到一个分组，它就检查其目标地址，尝试将此地址与其“下一跳”相联系。

路由表还可以包括其它信息。路由表比较 metric 以确定最佳路径，这些 metric 根据所用的路由算法而不同，下面将介绍常见的 metric。路由器彼此通信，

通过交换路由信息维护其路由表，路由更新信息通常包含全部或部分路由表，通过分析来自其它路由器的路由更新信息，该路由器可以建立网络拓扑细图。路由器间发送的另一个信息例子是链接状态广播信息，它通知其它路由器发送者的链接状态，链接信息用于建立完整的拓扑图，使路由器可以确定最佳路径。

2、交换

交换算法相对而言较简单，对大多数路由协议而言是相同的，多数情况下，某主机决定向另一个主机发送数据，通过某些方法获得路由器的地址后，源主机发送指向该路由器的物理（MAC）地址的数据包，其协议地址是指向目的主机的。

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。当分组在网络中流动时，它的物理地址在改变，但其协议地址始终不变，如下图所示。

上面描述了源系统与目的系统间的交换，ISO 定义了用于描述此过程的分层的术语。在该术语中，没

有转发分组能力的网络设备称为端系统（ES—end system），有此能力的称为中介系统（IS—intermediatesystem）。IS 又进一步分成可在路由域内通信的域内 IS（intradomainIS）和既可在路由域内有可在域间通信的域间 IS（interdomainIS）。路由域通常被认为是统一管理下的一部分网络，遵守特定的一组管理规则，也称为自治系统（autonomoussystem）。在某些协议中，路由域可以分为路由区间，但是域内路由协议仍可用于在区间内和区间之间交换数据。

三、路由算法

路由算法可以根据多个特性来加以区分。首先，算法设计者的特定目标影响了该路由协议的操作；其次，存在着多种路由算法，每种算法对网络和路由器资源的影响都不同；最后，路由算法使用多种 metric，影响到最佳路径的计算。下面的章节分析了这些路由算法的特性。

1、设计目标

路由算法通常具有下列设计目标的一个或多个：

优化简单、低耗健壮、稳定快速聚合灵活性

优化指路由算法选择最佳路径的能力，根据 metric 的值和权值来计算。例如有一种路由算法可能使用跳数和延迟，但可能延迟的权值要大些。当然，

路由协议必须严格定义计算 metric 的算法。

路由算法也可以设计得尽量简单。换句话说，路由协议必须高效地提供其功能，尽量减少软件和应用的开销。当实现路由算法的软件必须运行在物理资源有限的计算机上时高效尤其重要。

路由算法必须健壮，即在出现不正常或不可预见事件的情况下必须仍能正常处理，例如硬件故障、高负载和不正确的实现。因为路由器位于网络的连接点，当它们失效时会产生重大的问题。最好的路由算法通常是那些经过了时间考验，证实在各种网络条件下都很稳定的算法。

此外，路由算法必须能快速聚合，聚合是所有路由器对最佳路径达成一致的过程。当某网络事件使路径断掉或不可用时，路由器通过网络分发路由更新信息，促使最佳路径的重新计算，最终使所有路由器达成一致。聚合很慢的路由算法可能会产生路由环或网路中断。

在下图中的路由环中，某分组在时间 t1 到达路由器 1，路由器 1 已经更新并知道到达目的的最佳路径是以路由器 2 为下一跳，于是就把该分组转发给路由器 2。但是路由器 2 还没有更新，它认为最佳的下一跳是路由器 1，于是把该分组发回给路由器 1，结

果分组在两个路由器间来回传递直到路由器2收到路由更新信息或分组超过了生存期。

路由算法还应该是灵活的，即它们应该迅速、准确地适应各种网络环境。例如，假定某网段断掉了，当知道问题后，很多路由算法对通常使用该网段的路径将迅速选择次佳的路径。路由算法可以设计得可适应网络带宽、路由器队列大小和网络延迟。

2、算法类型

各路由算法的区别点包括：

静态与动态、单路径与多路径、平坦与分层主机智能与路由器、智能域内与域间、链接状态与距离向量

(1)静态与动态

静态路由算法很难算得上是算法，只不过是开始路由前由网管建立的表映射。这些映射自身并不改变，除非网管去改动。使用静态路由的算法较容易设计，在网络通信可预测及简单的网络中工作得很好。

由于静态路由系统不能对网络改变做出反映，通常被认为不适用于现在的大型、易变的网络。九十年代主要的路由算法都是动态路由算法，通过分析收到的路由更新信息来适应网络环境的改变。如果信息表示网络发生了变化，路由软件就重新计算路由并发出

新的路由更新信息。这些信息渗入网络，促使路由器重新计算并对路由表做相应的改变。

动态路由算法可以在适当的地方以静态路由作为补充。例如，最后可选路由（routero flastresort），作为所有不可路由分组的去路，保证了所有的数据至少有方法处理。

(2)单路径与多路径

一些复杂的路由协议支持到同一目的的多条路径。与单路径算法不同，这些多路径算法允许数据在多条线路上复用。多路径算法的优点很明显：它们可以提供更好的吞吐量和可靠性。

(3)平坦与分层

一些路由协议在平坦的空间里运作，其它的则有路由的层次。在平坦的路由系统中，每个路由器与其它所有路由器是对等的；在分层次的路由系统中，一些路由器构成了路由主干，数据从非主干路由器流向主干路由器，然后在主干上传输直到它们到达目标所在区域，在这里，它们从最后的主干路由器通过一个或多个非主干路由器到达终点。

路由系统通常设计有逻辑节点组，称为域、自治系统或区间。在分层的系统中，一些路由器可以与其它域中的路由器通信，其它的则只能与域内的路由器

通信。在很大的网络中，可能还存在其它级别，最高级的路由器构成了路由主干。

分层路由的主要优点是它模拟了多数公司的结构，从而能很好地支持其通信。多数的网络通信发生在小组中（域）。因为域内路由器只需要知道本域内的其它路由器，它们的路由算法可以简化，根据所使用的路由算法，路由更新的通信量可以相应地减少。

(4)主机智能与路由器智能

一些路由算法假定源结点来决定整个路径，这通常称为源路由。在源路由系统中，路由器只作为存贮转发设备，无意识地把分组发向下一跳。其它路由算法假定主机对路径一无所知，在这些算法中，路由器基于自己的计算决定通过网络的路径。前一种系统中，主机具有决定路由的智能，后者则为路由器具有此能力。

主机智能和路由器智能的折衷实际是最佳路由与额外开销的平衡。主机智能系统通常能选择更佳的路径，因为它们在发送数据前探索了所有可能的路径，然后基于特定系统对“优化”的定义来选择最佳路径。然而确定所有路径的行为通常需要很多的探索通信量和很长的时间。

(5)域内与域间

一些路由算法只在域内工作，其它的则既在域内也在域间工作。这两种算法的本质是不同的。其遵循的理由是优化的域内路由算法没有必要也成为优化的域间路由算法。

(6)链接状态与距离向量

链接状态算法（也叫做短路径优先算法）把路由信息散布到网络的每个节点，不过每个路由器只发送路由表中描述其自己链接状态的部分。距离向量算法（也叫做 Bellman-Ford 算法）中每个路由器发送路由表的全部或部分，但只发给其邻居。也就是说，链接状态算法到处发送较少的更新信息，而距离向量算法只向相邻的路由器发送较多的更新信息。

由于链接状态算法聚合得较快，它们相对于距离算法产生路由环的倾向较小。在另一方面，链接状态算法需要更多的 CPU 和内存资源，因此链接状态算法的实现和支持较昂贵。虽然有差异，这两种算法类型在多数环境中都可以工作得很好。

3、路由的 metric

路由表中含有由交换软件用以选择最佳路径的信息。但是路由表是怎样建立的呢？它们包含信息的本质是什么？路由算法怎样根据这些信息决定哪条路径更好呢？

路由算法使用了许多不同的 metric 以确定最佳路径。复杂的路由算法可以基于多个 metric 选择路由，并把它们结合成一个复合的 metric。常用的 metric 如下：

路径、长度可靠性、延迟带宽、负载通信代价

路径长度是最常用的路由 metric。一些路由协议允许网管给每个网络链接人工赋以代价值，这种情况下，路由长度是所经过各个链接的代价总和。其它路由协议定义了跳数，即分组在从源到目的的路途中必须经过的网络产品，如路由器的个数。

可靠性，在路由算法中指网络链接的可依赖性（通常以位误率描述），有些网络链接可能比其它的失效更多，网路失效后，一些网络链接可能比其它的更易或更快修复。任何可靠性因素都可以在给可靠率赋值时计算在内，通常是由网管给网络链接赋以 metric 值。

路由延迟指分组从源通过网络到达目的所花时间。很多因素影响到延迟，包括中间的网络链接的带宽、经过的每个路由器的端口队列、所有中间网络链接的拥塞程度以及物理距离。因为延迟是多个重要变量的混合体，它是个比较常用且有效的 metric。

带宽指链接可用的流通容量。在其它所有条件都

相等时，10Mbps 的以太网链接比 64kbps 的专线更可取。虽然带宽是链接可获得的最大吞吐量，但是通过具有较大带宽的链接做路由不一定比经过较慢链接路由更好。例如，如果一条快速链路很忙，分组到达目的所花时间可能要更长。

负载指网络资源，如路由器的繁忙程度。负载可以用很多方面计算，包括 CPU 使用情况和每秒处理分组数。持续地监视这些参数本身也是很耗费资源的。

通信代价是另一种重要的 metric，尤其是有一些公司可能关系运作费用甚于性能。即使线路延迟可能较长，他们也宁愿通过自己的线路发送数据而不采用昂贵的公用线路。

四、网络协议

可被路由的协议（RoutedProtocol）由路由协议(RoutingProtocol）传输，前者亦称为网络协议。这些网络协议执行在源与目的设备的用户应用间通信所需的各种功能，不同的协议中这些功能可能差异很大。网络协议发生在 OSI 参考模型的上四层：传输层、会话层、表示层和应用层。

术语 routedprotocol（可被路由的协议）和 routingprotocol（路由协议）经常被混淆。routedprotocol 在网络中被路由，例如 IP、DECnet、

AppleTalk、NovellNetWare、OSI、BanyanVINES 和 XeroxNetworkSystem(XNS)。而路由协议是实现路由算法的协议，简单地说，它给网络协议做导向。路由协议如：IGRP、EIGRP、OSPF、EGP、BGP、IS-IS 及 RIP 等。我们将陆续介绍上述的各种协议。

论 ARP 冲突

每台主机进入 LAN 时会向整个子网发送免费 ARP 通知报文，即该 request 包是利用广播方式请求解析自己的 IP 地址，但源和目标 IP 已经就位了。

免费 ARP(源 IP 和目标 IP 一致)请求意味着一个包就影响了整个子网，如果一个错误的免费 ARP 请求出现，整个子网都被搅乱了。

即使主机不发送免费 ARP 报文，也会因为后续的 request 请求导致自己的 IP-MAC 对进入 LAN 上所有主机的 ARPCache 中，所以冲突与否与免费 ARP 包没有必然联系。这个结论可以这样理解，一台 Linux 主机与 pwin98 争夺 IP 地址，Linux 主机将争夺成功，pwin98 却一直在报告 IP 冲突，显然后面所有的 IP 冲突报告都与免费 ARP 包没有关系了。

in_arpinput()函数是 4XBSD-Lite2 中的经典实现

1 如果针对本机某个 IP 地址的请求到达，响应被

送出。ARP 入口被建立(如果相应入口不存在)。这个优化避免过多的 ARP 报文交换。

2 如果 ARP 响应到达,相应的 ARP 入口建立完成,异己主机的 MAC 地址存储在 sockaddr_dl 结构中,队列中目标是该异己主机的报文现在可以发送了。

3 假如异己主机发送了一个 ARP 请求包或者响应包,包中源 IP 地址等于自己的 IP 地址,那么两台之中必有一台错误配置了 IP 地址。Net/3 侦测到这个错误并向管理员报告。

4 主机接收到来自异己主机的 ARP 包,该异己主机的 ARP 入口已经存在,若包中异己主机的 MAC 地址已经改变,则相应的 ARP 入口中的 MAC 地址得到更新。

5 主机可以配置成 proxyARPserver。这意味着它代替目标主机响应 ARP 请求。卷 I 的 46 节讨论了 proxyARP。用 arp 命令可以配置一台主机成为 proxyARPserver。

双绞线

一、概述

双绞线(TP:TwistedPairwire)是综合布线工程中最常用的一种传输介质。双绞线由两根具有绝缘保护层的铜导线组成。把两根绝缘的铜导线按一定密度互相绞在一起,可降低信号干扰的程度,每一根导线

在传输中辐射的电波会被另一根线上发出的电波抵消。双绞线一般由两根 22--26 号绝缘铜导线相互缠绕而成。如果把一对或多对双绞线放在一个绝缘套管中便成了双绞线电缆。在双绞线电缆(也称双扭线电缆)内,不同线对具有不同的扭绞长度,一般地说,扭绞长度在 381cm 至 14cm 内,按逆时针方向扭绞,相临线对的扭绞长度在127cm以上。与其他传输介质相比,双绞线在传输距离、信道宽度和数据传输速度等方面均受到一定限制,但价格较为低廉。目前,双绞线可分为非屏蔽双绞线(UTP:UnshildedTwistedPair)和屏蔽双绞线(STP:ShieldedTwistedPair)。

虽然双绞线主要是用来传输模拟声音信息的,但同样适用于数字信号的传输,特别适用于较短距离的信息传输。在传输期间,信号的衰减比较大,并且产生波形畸变。采用双绞线的局域网的带宽取决于所用导线的质量、长度及传输技术。只要精心选择和安装双绞线,就可以在有限距离内达到每秒几百万位的可靠传输率。当距离很短,并且采用特殊的电子传输技术时,传输率可达 100Mbps--155Mbps。由于利用双绞线传输信息时要向周围幅射,信息很容易被窃听,因此要花费额外的代价加以屏蔽。屏蔽双绞线电缆的外层由铝泊包裹,以减小幅射,但并不能完全消除辐射。屏

蔽双绞线价格相对较高,安装时要比非屏蔽双绞线电缆困难。类似于同轴电缆,它必须配有支持屏蔽功能的特殊连结器和相应的安装技术。但它有较高的传输速率,100 米内可达到 155Mbps。

另外,非屏蔽双绞线电缆具有以下优点:

(1)无屏蔽外套,直径小,节省所占用的空间;

(2)重量轻、易弯曲、易安装;

(3)将串扰减至最小或加以消除;

(4)具有阻燃性;

(5)具有独立性和灵活性,适用于结构化综合布线。

二、规格型号

EIA/TIA 为双绞线电缆定义了五种不同质量的型号。计算机网络综合布线使用第三、四、五类。这五种型号如下:

1、第一类:主要用于传输语音(一类标准主要用于八十年代初之前的电话线缆),不用于数据传输。

2、第二类:传输频率为 1MHz,用于语音传输和最高传输速率 4Mbps 的数据传输,常见于使用 4Mbps 规范令牌传递协议的旧的令牌网。

3、第三类:指目前在 ANSI 和 EIA/TIA568 标准中指定的电缆。该电缆的传输频率为 16MHz,用于语音传

输及最高传输速率为 10Mbps 的数据传输，主要用于 10base-T。

4、第四类:该类电缆的传输频率为 20MHz,用于语音传输和最高传输速率 16Mbps 的数据传输，主要用于基于令牌的局域网和 10base-T/100base-T。

5、第五类:该类电缆增加了绕线密度,外套一种高质量的绝缘材料,传输频率为 100MHz,用于语音传输和最高传输速率为 100Mbps 的数据传输，主要用于 100base-T 和 10base-T 网络,这是最常用的以太网电缆。

双绞线分为屏蔽双绞线与非屏蔽双绞线两大类。在这两大类中又分 100 欧姆电缆、双体电缆、大对数电缆、150 欧姆屏蔽电缆。具体型号有多种。

三、性能指标

对于双绞线,用户最关心的是表征其性能的几个指标。这些指标包括衰减、近端串扰、阻抗特性、分布电容、直流电阻等。

(1)衰减

衰减(Attenuation)是沿链路的信号损失度量。衰减与线缆的长度有关系,随着长度的增加,信号衰减也随之增加。衰减用“db”作单位,表示源传送端信号到接收端信号强度的比率。由于衰减随频率而变

化,因此,应测量在应用范围内的全部频率上的衰减。

(2)近端串扰

串扰分近端串扰和远端串扰(FEXT),测试仪主要是测量 NEXT,由于存在线路损耗,因此 FEXT 的量值的影响较小。近端串扰(NEXT)损耗是测量一条 UTP 链路中从一对线到另一对线的信号耦合。对于 UTP 链路,NEXT 是一个关键的性能指标,也是最难精确测量的一个指标。随着信号频率的增加,其测量难度将加大。

NEXT 并不表示在近端点所产生的串扰值,它只是表示在近端点所测量到的串扰值。这个量值会随电缆长度不同而变,电缆越长,其值变得越小。同时发送端的信号也会衰减,对其它线对的串扰也相对变小。实验证明,只有在 40 米内测量得到的 NEXT 是较真实的。如果另一端是远于40米的信息插座,那么它会产生一定程度的串扰,但测试仪可能无法测量到这个串扰值。因此,最好在两个端点都进行 NEXT 测量。现在的测试仪都配有相应设备,使得在链路一端就能测量出两端的 NEXT 值。

293 以上两个指标是 TSB67 测试的主要内容,但某些型号的测试仪还可以给出直流电阻、特性阻抗、衰减串扰比等指标。

(3)直流电阻

TSB67 无此参数。直流环路电阻会消耗一部分信号,并将其转变成热量。它是指一对导线电阻的和,11801 规格的双绞线的直流电阻不得大于 192 欧姆。每对间的差异不能太大(小于 01 欧姆),否则表示接触不良,必须检查连接点。

(4)特性阻抗

与环路直流电阻不同,特性阻抗包括电阻及频率为 1~100MHz 的电感阻抗及电容阻抗,它与一对电线之间的距离及绝缘体的电气性能有关。各种电缆有不同的特性阻抗,而双绞线电缆则有 100 欧姆、120 欧姆及 150 欧姆几种。

(5)衰减串扰比(ACR)

在某些频率范围,串扰与衰减量的比例关系是反映电缆性能的另一个重要参数。ACR 有时也以信噪比(SNR:Signal-Noiceratio)表示,它由最差的衰减量与 NEXT 量值的差值计算。ACR 值较大,表示抗干扰的能力更强。一般系统要求至少大于 10 分贝。

(6)电缆特性

通信信道的品质是由它的电缆特性描述的。SNR 是在考虑到干扰信号的情况下,对数据信号强度的一个度量。如果 SNR 过低,将导致数据信号在被接收时,

接收器不能分辨数据信号和噪音信号,最终引起数据错误。因此,为了将数据错误限制在一定范围内,必须定义一个最小的可接收的 SNR。

四、测试数据

100 欧姆 4 对非屏蔽双绞线有 3 类线、4 类线、5 类线和超 5 类线之分。主要的性能指标为衰减、分布电容、直流电阻、直流电阻偏差值、阻抗特性、返回损耗、近端串扰。

五、常用的双绞线电缆

综合布线中最常用的双绞线电缆有以下几种:

1、5 类 4 对非屏蔽双绞线

它是美国线缆规格为 24 的实芯裸铜导体,以氟化乙烯做绝缘材料,传输频率达 100MHz。。其中,“938 欧姆 MAXPer100m@20℃”是指在 20℃的恒定温度下,每 100 米的双绞线的电阻为 938 欧姆。

342、5 类 4 对 24AWG100 欧姆屏蔽电缆

它是美国线规为 24 的裸铜导体,以氟化乙烯做绝缘材料,内有一 24AWGTPG 漏电线。传输频率达 100MHz,导线组成,屏蔽项“0002[0051]铝/聚酯带最小交叠@20℃及一根 24AWGTPC 漏电线”的含义是:

- 屏蔽层厚度为 0002 厘米或 0051 英寸。
- @20℃代表在 20℃恒定温度下。

它由4对线和一根26AWGTPC漏电线组成,传输频率达100MHz。

超5类布线系统是一个非屏蔽双绞线(UTP)布线系统,通过对它的“链接”和“信道”性能的测试表明,它超过TIA/EIA568的5类线要求。与普通的5类UTP比较,其衰减更小,串扰更少,同时具有更高的衰减与串扰的比值(ACR)和信噪比(SRL)、更小的时延误差,性能得到了提高。它具有四大优点:

(1)提供了坚实的网络基础,可以方便转移、更新网络技术。

(2)能够满足大多数应用的要求,并且满足低偏差和低串扰总和的要求。

(3)被认为是为将来网络应用提供的解决方案。

(4)充足的性能余量,给安装和测试带来方便。

与5类线缆相比,超5类在近端串扰、串扰总和、衰减和信噪比四个主要指标上都有较大的改进。

近端串扰(NEXT)是评估性能的最重要的标准。一个高速的LAN在传送和接收数据时是同步的。NEXT是当传送与接收同时进行时所产生的干扰信号。NEXT的单位是db,它表示传送信号与串扰信号之间的比值。

在普通应用中,衡量NEXT的标准方法是用一对线

进行传送，另一对线用于接收，如 10BASET 和 TokenRing,甚至 100BASET 和 155MbpsATM。但是,有时候也可以使用另外两对线,并接到另一工作站,这样可以加快 LAN 的速度,如 622MbpsATM 和 1000BASE-T,不只用一对(可能用全部的 4 对线)来传送和接收。在一根线缆中使用多对线进行传送会增加这根线缆的串扰。现在的四对 5 类双绞线没有考虑这种情况。

串扰总和(PowerSumNEXT)是从多个传输端产生 NEXT 的和。如果一个布线系统能够满足 5 类线在 PowerSum 下的 NEXT 要求,那么就能处理从应用共享到高速 LAN 应用的任何问题。超 5 类布线系统的 NEXT 只有 5 类线要求的 1/8。

信噪比(StructuralReturnLoss)是衡量线缆阻抗一致性的标准,阻抗的变化引起反射。一部分信号的能量被反射到发送端,形成噪声。SRL 是测量能量变化的标准,由于线缆结构变化而导致阻抗变化,使得信号的能量发生变化。反射的能量越少,意味着传输信号越完整,在线缆上的噪声越小。

比起普通 5 类双绞线,超 5 类系统在 100MHz 的频率下运行时,为用户提供 8db 近端串扰的余量,用户的设备受到的干扰只有普通 5 类线系统的 1/4,使系统具有更强的独立性和可靠性。

什么是网络什么是 INTERNET

简单的来讲,网络就是在一定的区域内两个或两个以上的计算机以一定的方式连接,以供用户共享文件、程序、数据等资源。

Internet,即全球信息网（WorldWideWeb，简称 WWW），是基于超文本(Hypertext)的信息检索工具，它通过超链接把世界各地不同 Internet 节点上的相关的信息有机地组织在一起，用户只需发出检索请求，它就能自动地进行相应的定位，找到相应的检索信息。

下面就几种常见的网络类型及分类方法作简单的介绍。

按网络的地理位置分类

局域网（LocalAreaNetwork,简称 LAN）

一般限定在较小的区域内，小于 10km 的范围，通常采用有线的方式连接起来。

城域网（MetropolisAreaNetwork,简称 MAN）

规模局限在一座城市的范围内，10--100km 的区域。

广域网（WideAreaNetwork,简称 WAN）

网络跨越国界、洲界，甚至全球范围。

目前局域网和广域网是网络的热点。局域网是组

成其他两种类型网络的基础，城域网一般都加入了广域网。广域网的典型代表是 Internet 网。

按网络的拓扑结构分类

网络的拓扑结构是指网络中通信线路和站点（计算机或设备）的几何排列形式。

星型网络

各站点通过点到点的链路与中心站相连。特点是很容易在网络中增加新的站点，数据的安全性和优先级容易控制，易实现网络监控，但中心节点的故障会引起整个网络瘫痪。

环形网络

各站点通过通信介质连成一个封闭的环形。环形网容易安装和监控，但容量有限，网络建成后，难以增加新的站点。

总线型网络

网络中所有的站点共享一条数据通道。总线型网络安装简单方便，需要铺设的电缆最短，成本低，某个站点的故障一般不会影响整个网络。但介质的故障会导致网络瘫痪，总线网安全性低，监控比较困难，增加新站点也不如星型网容易。

树型网、簇星型网、网状网等其他类型拓扑结构的网络都是以上述三种拓扑结构为基础的。

按传输介质分类

有线网

采用同轴电缆和双绞线来连接的计算机网络。

同轴电缆网是常见的一种连网方式。它比较经济，安装较为便利，传输率和抗干扰能力一般，传输距离较短。

双绞线网是目前最常见的连网方式。它价格便宜，安装方便，但易受干扰，传输率较低，传输距离比同轴电缆要短。

光纤网

光纤网也是有线网的一种，但由于其特殊性而单独列出，光纤网采用光导纤维作传输介质。光纤传输距离长，传输率高，可达数千兆 bps，抗干扰性强，不会受到电子监听设备的监听，是高安全性网络的理想选择。不过由于其价格较高，且需要高水平的安装技术，所以现在尚未普及。

无线网

采用空气作传输介质，用电磁波作为载体来传输数据，目前无线网联网费用较高，还不太普及。但由于联网方式灵活方便，是一种很有前途的连网方式。

局域网通常采用单一的传输介质，而城域网和广域网采用多种传输介质。

按通信方式分类

点对点传输网络：数据以点到点的方式在计算机或通信设备中传输。星型网、环形网采用这种传输方式。

广播式传输网络：数据在共用介质中传输。无线网和总线型网络属于这种类型。

按网络使用的目的分类

共享资源网：使用者可共享网络中的各种资源，如文件、扫描仪、绘图仪、打印机以及各种服务。Internet 网是典型的共享资源网。

数据处理网：用于处理数据的网络，例如科学计算网络、企业经营管理用网络。

数据传输网：用来收集、交换、传输数据的网络，如情报检索网络等。

目前网络使用目的都不是唯一的。

按服务方式分类

客户机/服务器网络

服务器是指专门提供服务的高性能计算机或专用设备，客户机是用户计算机。这是客户机向服务器发出请求并获得服务的一种网络形式，多台客户机可以共享服务器提供的各种资源。这是最常用、最重要的一种网络类型。不仅适合于同类计算机联网，也适

合于不同类型的计算机联网，如 PC 机、Mac 机的混合联网。这种网络安全性容易得到保证，计算机的权限、优先级易于控制，监控容易实现，网络管理能够规范化。网络性能在很大程度上取决于服务器的性能和客户机的数量。目前针对这类网络有很多优化性能的服务器称为专用服务器。银行、证券公司都采用这种类型的网络。

对等网

对等网不要求文件服务器，每台客户机都可以与其他每台客户机对话，共享彼此的信息资源和硬件资源，组网的计算机一般类型相同。这种网络方式灵活方便，但是较难实现集中管理与监控，安全性也低，较适合于部门内部协同工作的小型网络。

其他分类方法

如按信息传输模式的特点来分类的 ATM 网，网内数据采用异步传输模式，数据以 53 字节单元进行传输，提供高达 12Gbps 的传输率，有预测网络延时的能力。可以传输语音、视频等实时信息，是最有发展前途的网络类型之一。

另外还有一些非正规的分类方法：如企业网、校园网，根据名称便可理解。

从不同的角度对网络有不同的分类方法，每种网

络名称都有特殊的含意。几种名称的组合或名称加参数更可以看出网络的特征。千兆以太网表示传输率高达千兆的总线型网络。了解网络的分类方法和类型特征，是熟悉网络技术的重要基础之一。

如何保证电缆性能

许多用户和安装商面临着如何在园区网环境里进行楼间廉价高效数据传输的问题。

路由的选择、传输距离和应用环境都将影响对电缆介质的选择，不正确或不恰当的选择将会导致布线投资的有限期缩短，而重新安装也会导致网络系统运行的停止。

如果是室外应用，通常对于园区网连接的选择是光纤系统。光纤真正的开销在光纤布线系统的端接和光电设备上，当用户只需要在楼间 50 米的距离内传达输 10Mbps 或 100Mbps 时，一般不采用光纤。

将常规5类铜缆埋入地下或架空铺设将可能会导致某一网络沿布线线路的传输失败，所以选择现有的室外直埋增强型 5 类电缆会带来廉价的链路。在决定选择这些室外局域网电缆之前应对它的设计进行充分理解。

多年来防潮保护网在通信电缆中一直应用，这些铝聚合材料有重叠封口作为保护，降低水蒸汽的渗透

路径来地阻止水的进入。然而一个无保护的干燥电缆将需要遭受长达半年到一年由于浸润而产生的的液化，一个带防潮保护网的干燥电缆才会得到彻底保护。这样设计的电缆大约与箔屏蔽局域网电缆类似，端接通用简单。所以，布线系统设计者必须考虑到应用环境，这包括下列环境及影响电缆的参数。

电缆是否放置于：屋檐下。电缆只要不直接暴露在阳光照射或超高温下，标准局域网电缆就可以应用，建议使用管道；外墙上。避免阳光直接照射墙面及人为损坏；

管道里（塑料或金属的）。如在管道里，注意塑料管道的损坏及金属管道的导热；

悬空应用/架空电缆。考虑电缆的下垂和压力。打算采用哪种捆绑方式？电缆是否被阳光直接照射；

直接在地下电缆沟中铺设，这种环境是控制范围最小的。电缆沟的安装要定期进行干燥或潮湿程度的检查；

地下管道。为便于今后的升级、电缆更换以及与表面压力和周围环境相隔离，铺设管道是一个较好的方法。但不要寄希望于管道会永远保持干燥，这将影响对电缆种类的选择。

影响电缆性能的因素包括:

紫外线（UV）——不要将无紫外线防护的电缆应用于阳光的直射环境内，应选择黑色聚乙烯或 PVC 外皮的电缆，如奔瑞公司（Brand-Rex)的 4 对增强型 5 类 MegaOutdoor 室外电缆，它带有金属网防潮保护层及黑色聚乙烯外皮，适用于绝大多数楼间连接，不管是架空铺设、地面安装还是管道内施工均可以采用；

热度——电缆在金属管道或线槽内的温度很高，许多聚合材料在这种温度下会降低使用寿命，应选择黑色聚乙烯或 PVC 外皮；

水——水是局域网电缆的真正杀手。在局域网双绞线电缆内的水分会增加电缆的电容，从而降低了阻抗并引起近端串扰问题。若要有效防止潮湿和水蒸气，需要采用金属屏蔽网保护层；

机械损坏（修复费用）——光缆的修复是十分昂贵的，在每一个间断点至少需要两次端接；

接地——如果电缆的屏蔽层需要接地，则必须遵守相应的标准；

路由总长度（不仅仅指楼间）——大楼间采用室外级的局域网双绞线电缆，其总长度要限制在 90 米之内。对于 100Mps 或 1000Mbps 网络，其铺设距离不能超过这一限定。如果铺设的距离在 100 米到 300 米

之间，则应该选择光缆。

可用下列的简单实验自测一下布线投资是否安全：用 20 米增强型 5 类 UTP 电缆分别在两端进行端接；在电缆中点的位置小心拨开电缆外皮，露出一小段铜缆（1 厘米）；按照 AN/NZSD 级标准测试电缆；将电缆的切割部分浸泡在水中 1-2 分钟，然后再重新测试。

使用 LINUX 作硬盘克隆

源盘：IBM20G5400RPMFAT16 分区 1；Linuxnative 分区 1；FreeBSD 分区 1，内又分为一个主 Sillice 和一个 SwapSillice；扩展分区 1，4 个逻辑分区，其中最后一个是 LinuxSwap 分区。

IDE1Master

目标盘：西部数据 30G7200RPM，空白盘。IDE2Master

进入 Linux，运行：ddif=/dev/hdaof=/dev/hdc

dd 就是 Linux/Unix 下通用的克隆、镜像程序，if=输入的文件 of=输出的文件。由于在 Linux 下所有的硬件都表示为文件，所以可以进行任何复制、克隆。比如还可以把/dev/hda 克隆到 MO、磁带以及映像文件中，当然，目标“文件”必须比原“文件”大，不然就会溢出。

20G 的硬盘复制了大约不到 2 个小时，在整个过程中，使用 K6-2500CPU，UDMA2 打开的情况下，CPU 占用率只有 18%-19%，从来没有超过 20%。在此期间还可以玩玩扫雷、国际象棋等游戏，也可以看看文档、帮助什么的，但是最好不要作写操作。当然你可以估计时间，在复制进程还没有到 Linux 分区，或者已经过了 Linux 分区的时候，也可以进行写操作，但是要当心！

最后，dd 会报告一共复制了多少字节，这就是源盘的实际大小。完成以后，30G 的西部数据硬盘就跟原来的 IBM 硬盘“一模一样”了，只不过是后面有 10G 的空空间，你可以在份一个分区（我的硬盘不能在分主分区了，因为 4 个 Primray 分区已满，只能在芬逻辑分区），或者用 PQ、Fips 扩大原有的分区。如果你什么都不做，那么从新启动 Win98 以后，跟原来是一模一样的。如果启动 Linux，就有了一些问题，因为对于新硬盘来说，相当于运行完了 dd 程序就切断了电源，因此文件系统处于 unclean 状态，在启动的时候会报错，不要怕，输入 root 密码，然后运行：fsck/ 这就启动了文件系统检测程序，相当于 Windows 下的磁盘检测，对于所有的问题都回答“y”，大部分都是 /tmp 的问题，无关紧要的。修复完毕，输入：reboot

就可以安全的启动 Linux 了！

总的来说，Linux 下的 dd 相对于 Ghost 各有所长。dd 的复制是完全基于二进制的物理复制，从硬盘的第一个字节道最后一个字节，完全一样的克隆了一边，所以是最保险、最准确的。而且由于 dd 是物理复制，所以只要是硬盘上存在的分区，无论 Linux 是否认识，甚至是 Linux 认不出是什么的一段数据，都可以原原本本的复制，例如 FreeBSD 分区、其他操作系统的分区，甚至加密扇区什么的，就连逻辑坏块也原样复制！因此除非出现物理问题，不然 dd 是绝对不会出错的！而 Ghost 则比较“高级”一些，可以在复制的时候改变分区大小（他认识的分区格式），压缩映像文件（dd 本身不具有压缩功能，但是可以用 gzip、bzip2 等工具压缩生成的文件），在 Windows 下还有 explore 软件可以单独提取文件出来，还有网络功能，而且速度也要比 dd 快一些（好像 Ghost 使用了较大的缓存）。另外一点 dd 的优势在于，在克隆的同时还可以干些别的事情，不像 Ghost 那样只能干等。因此从这方面来看，dd 的速度又要比 Ghost 快，因为它完全占用系统的时间是零！

其它 Unix 下的 dd 操作跟 Linux 下的雷同，只不过是/dev/hda 的称谓变化一下。我在 FreeBSD42 下试

验过，效果跟 Linux 下完全相同，时间稍微长一点点，但是在 FreeBSD 下，dd 的 CPU 占用率有时会达到 30%以上。

如果你的源盘是 IDE，而目标盘是 SCSI 的，这时要注意了，虽然对于硬件来说是没有什么问题，因为现在的 Linux 还是 FreeBSD 都支持即插即用；但是，/etc/fstab 文件需要修改，在 dd 之前要把所有的 hda 改成 sda，然后再改回来

ICMP 详解

TCP 和 UDP 能承载数据，但 ICMP 仅包含控制信息。因此，ICMP 信息不能真正用于入侵其它机器。Hacker 们使用 ICMP 通常是为了扫描网络，发动 DoS 攻击，重定向网络交通。(这个观点似乎不正确，可参考 shotgun 关于木马的文章，译者注)

一些防火墙将 ICMP 类型错误标记成端口。要记住，ICMP 不象 TCP 或 UDP 有端口，但它确实含有两个域：类型(type)和代码(code)。而且这些域的作用和端口也完全不同，也许正因为有两个域所以防火墙常错误地标记了他们。更多关于 ICMP 的知识请参考 InfosecLexiconentryonICMP。

关于 ICMP 类型/代码的含义的官方说明请参阅 http://wwwisiedu/in-notes/iana/assignments/ic

mp-parameters。该文献描述官方含义，而本文描述Hacker的企图，详见下文。

类型代码名称含义

0Echoreplay对ping的回应

3DestinationUnreachable主机或路由器返回信息：一些包未达到目的地

0NetUnreachable路由器配置错误或错误指定IP地址

1HostUnreachable 最后一个路由器无法与主机进行ARP通讯

3Portunreachable 服务器告诉客户端其试图联系的端口无进程侦听

4FragmentationNeededbutDFset 重要：如果你在防火墙丢弃记录中发现这些包，你应该让他们通过否则你的客户端将发现TCP连接莫名其妙地断开

4SourceQuenchInternet阻塞

5Redirect有人试图重定向你的默认路由器，可能Hacker试图对你进行“man-in-middle”的攻击，使你的机器通过他们的机器路由。

8EchoRequestping

9RouterAdvertisementhacker 可能通过重定向你的默认的路由器DoS攻击你的Win9x或Solaris。

邻近的 Hacker 也可以发动 man-in-the-middle 的攻击11TimeExceededInTransit因为超时包未达到目的地 0TTLExceeded 因为路由循环或由于运行 traceroute,路由器将包丢弃 1 Fragmen treassembly timeout 由于没有收到所有片断，主机将包丢弃 12ParameterProblem 发生某种不正常,可能遇到了攻击。

(一)type=0(Echoreply)

发送者在回应由你的地址发送的 ping,可能是由于以下原因：

有人在 ping 那个人：防火墙后面有人在 ping 目标。

自动 ping：许多程序为了不同目的使用 ping，如测试联系对象是否在线，或测定反应时间。很可能是使用了类似 VitalSign ‘sNetMedic 的软件，它会发送不同大小的 ping 包以确定连接速度。

诱骗 ping 扫描：有人在利用你的 IP 地址进行 ping 扫描，所以你看到回应。

转变通讯信道：很多网络阻挡进入的 ping(type=8)，但是允许 ping 回应(type=0)。因此，Hacker 已经开始利用 ping 回应穿透防火墙。例如，针对 internet 站点的 DdoS 攻击，其命令可能被嵌入

ping 回应中，然后洪水般的回应将发向这些站点而其它 Internet 连接将被忽略。

(二)Type=3(DestinationUnreachable)

在无法到达的包中含有的代码(code)很重要

记住这可以用于击败“SYN 洪水攻击”。即如果正在和你通讯的主机受到“SYN 洪水攻击”，只要你禁止 ping(type=3)进入，你就无法连接该主机。

有些情况下，你会收到来自你从未听说的主机的 ping(type=3)包，这通常意味着“诱骗扫描”。攻击者使用很多源地址向目标发送一个伪造的包，其中有一个是真正的地址。Hacker 的理论是：受害者不会费力从许多假地址中搜寻真正的地址。

解决这个问题的最好办法是：检查你看到的模式是否与“诱骗扫描”一致。比如，在 ICMP 包中的 TCP 或 UDP 头部分寻找交互的端口。

1)Type=3,Code=0(DestinationNetUnreachable)

无路由器或主机：即一个路由器对主机或客户说，：“我根本不知道在网络中如何路由！包括你正连接的主机”。这意味着不是客户选错了 IP 地址就是某处的路由表配置错误。记住，当你把自己 UNIX 机器上的路由表搞乱后你就会看到“无路由器或主机”的

信息。这常发生在配置点对点连接的时候。

2)Type=3,Code=3(DestinationPortUnreachable)

这是当客户端试图连击一个并不存在的UDP端口时服务器发送的包。例如，如果你向 161 端口发送 SNMP 包，但机器并不支持 SNMP 服务，你就会收到 ICMPDestinationPortUnreachable 包。

解码的方案

解决这个问题的第一件事是：检查包中的端口。你可能需要一个嗅探器，因为防火墙通常不会记录这种信息。这种方法基于 ICMP 原始包头包含 IP 和 UDP 头。以下是复制的一个 ICMPunreachable 包：

0000BA5EBA1100609707C0FF08004500

00386FDF00008001B4120A00010B0A00

01C90303C2D200000000450000 4707F0

000080111BE30A0001C90A00010B08A7

79190033B836

其中字节 0303 是 ICMP 的类型和代码。最后 8 个字节是原始 UDP 头，解码如下：

08A7UDP 源端口 port=2215，可能是临时分配的，并不是很重要。

7919UDP 目标端口 port=31001，很重要，可能原

来用户想连接 31001 端口的服务。

0033UDP 长度 length=51，这是原始 UDP 数据的长度，可能很重要。

B836UDP 校验和 checksum=0xB836，可能不重要。

你为什么会看到这些？

“诱骗 UDP 扫描”：有人在扫描向你发送 ICMP 的机器。他们伪造源地址，其中之一是你的 IP 地址。他们实际上伪造了许多不同的源地址使受害者无法确定谁是攻击者。如果你在短时间内收到大量来自同一地址的这种包，很有可能是上述情况。检查 UDP 源端口，它总在变化的话，很可能是 Scenario。

“陈旧 DNS”：客户端会向服务器发送 DNS 请求，这将花很长时间解析。当你的 DNS 服务器回应的时候，客户端可能已经忘记你并关闭了用于接受你回应的 UDP 端口。如果发现 UDP 端口值是 53，大概就发生了这种情况。这是怎么发生的？服务器可能在解析一个递归请求，但是它自己的包丢失了，所以它只能超时然后再试。当回到客户时，客户认为超时了。许多客户程序(尤其是 Windows 中的程序)自己做 DNS 解析。即它们自己建立 SOCKET 进行 DNS 解析。如果它们把要求交给操作系统，操作系统就会一直把端口开在那里。

“多重 DNS 回应”：另一种情况是客户收到对于一个请求的多重回应。收到一个回应，端口就关闭了，后序的回应无法达到。此外，一个 Sun 机器与同一个以太网中的多个 NICs 连接时，将为两个 NICs 分配相同的 MAC 地址，这样 Sun 机器每桢会收到两个拷贝，并发送多重回复。还有，一个编写的很糟糕的客户端程序(特别是那些吹嘘是多线程 DNS 解析但实际上线程不安全的程序)有时发送多重请求，收到第一个回应后关闭了 Socket。但是，这也可能是 DNS 欺骗，攻击者既发送请求由发送回应，企图使解析缓存崩溃。

“NetBIOS 解析”：如果 Windows 机器接收到 ICMP 包，看看 UDP 目标端口是否是 137。如果是，那就是 windows 机器企图执行 gethostbyaddr()函数，它将将会同时使用 DNS 和 NetBIOS 解析 IP 地址。DNS 请求被发送到某处的 DNS 服务器，但 NetBIOS 直接发往目标机器。如果目标机器不支持 NetBIOS，目标机器将发送 ICMPunreachable。

“Traceroute”：大多数 Traceroute 程序(Windows 中的 Tracertexe 除外)向关闭的端口发送 UDP 包。这引起一系列的背靠背的 ICMP Port Unreachable 包发回来。因此你看到防火墙显示这样 ICMP 包，可能是防火墙后面的人在运行 Traceroute。你也

会看到 TTL 增加。

3)Type=3,Code=4(FragmentationNeededandDon‘tFragmentwasSet)

这是由于路由器打算发送标记有(DF,不允许片断)的 IP 报文引起的。为什么？IP 和 TCP 都将报文分成片断。TCP 在管理片断方面比 IP 有效得多。因此，饯堆趋向于找到“PathMTU”(路由最大传输单元)。在这个过程将发送这种 ICMP 包。

假设 ALICE 和 BOB 交谈。他们在同一个以太网上(maxframesize=1500bytes)，但是中间有连接限制最大 IP 包为 600byte。这意味着所有发送的 IP 包都要由路由器切割成 3 个片断。因此在 TCP 层分割片断将更有效。TCP 层将试图找到 MTU(最大传输单元)。它将所有包设置 DF 位(Don‘tFragment)，一旦这种包碰到不能传输如此大的包的路由器时路由器将发回 ICMP 错误信息。由此，TCP 层能确定如何正确分割片断。

你也许应该允许这些包通过防火墙。否则，当小的包可以通过达到目的地建立连接，而大包会莫名其妙的丢失断线。通常的结果是，人们只能看到 Web 页仅显示一半。

路由最大传输单元的发现越来越整合到通讯中。

如 IPsec 需要用到这个功能。

(三)Type=4(SourceQuench)

这种包可能是当网络通讯超过极限时由路由器或目的主机发送的。但是当今的许多系统不生成这些包。原因是现在相信简单包丢失是网络阻塞的最后信号(因为包丢失的原因就是阻塞)。

现在 sourcequenches 的规则是(RFC1122):

路由器不许生成它们

主机可以生成它们

主机不能随便生成它们

防火墙应该丢弃它们

但是，主机遇到 SourceQuench 仍然减慢通讯，因此这被用于 DoS。防火墙应该过滤它们。如果怀疑发生 DoS，包中的源地址是无意义的，因为 IP 地址肯定是虚构的。

已知某些 SMTP 服务器会发送 SourceQuench。

(四)Type=8(EchoakaPING)

这是 ping 请求包。有很多场合使用它们；它可能意味着某人扫描你机器的恶意企图，但它也可能是正常网络功能的一部分。参见 Type=0(EchoResponse)

很多网络管理扫描器会生成特定的 ping 包。包括 ISS 扫描器，WhatsUp 监视器等。这在扫描器的有

效载荷中可见。许多防火墙并不记录这些，因此你需要一些嗅探器捕捉它们或使用入侵检测系统(IDS)标记它们。

记住，阻挡 ping 进入并不意味着 Hacker 不能扫描你的网络。有许多方法可以代替。例如，TCPACK 扫描越来越流行。它们通常能穿透防火墙而引起目标系统不正常的反应。

发送到广播地址(如xxx0或xxx255)的ping可能在你的网络中用于 smurf 放大。

(五)Type=11(TimeExceededInTransit)

这一般不会是 Hacker 或 Cracker 的攻击

1)Type=11,Code=0(TTLExceededInTransit)

这可能有许多事情引起。如果有人从你的站点 traceroute 到 Internet，你会看到许多来自路由器的 TTL 增加的包。这就是 traceroute 的工作原理：强迫路由器生成 TTL 增加的信息来发现路由器。

防火墙管理员看到这种情况的原因是 Internet 上发生路由循环。路由器 Flapping(持续变换路由器)是一个常见的问题，常会导致循环。这意味着当一个 IP 包朝目的地前进时，这个包被一个路由器错误引导至一个它曾经通过的路由器。如果路由器在包经过的时候把 TTL 域减一，这个包只好循环运动。实际上当

TTL 值为 0 时它被丢弃。

造成这种情况的另一个原因是距离。许多机器(Windows)的默认 TTL 值是 127 或更低。路由器也常常会把 TTL 值减去大于 1 的值，以便反应诸如电话拨号或跨洋连接的慢速连接。因此，可能由于初始 TTL 值太小，而使站点无法到达。此外，一些 Hacker/Cracker 也会使用这种办法使站点无法到达。

2)Type=11,Code=1(FragmentReassemblyTimeExceeded)

当发送分割成片断的 IP 报文时，发送者并不接收所有片断。通常，大多数 TCP/IP 通讯甚至不分割片断。你看到这种情况必定是采用了分割片断而且你和目的地之间有阻塞。

(六)Type=12(ParameterProblem)

这可能意味着一种进攻。有许多足印技术会生成这种包。

制作 W2K 启动盘

此秘籍针对普通硬件配置的机器。

1.用 W2K 格式化软盘！

2.把下面四个文件复制到软盘上：

bootini

IOsys

ntldr
ntdetectcom
3.编辑 bootini，尽量多加启动项，比如：
[bootloader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operatingsystems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="1-1"
/fastdetect
multi(0)disk(0)rdisk(0)partition(2)\WINNT="1-2"
/fastdetect
multi(0)disk(0)rdisk(0)partition(3)\WINNT="1-3"
/fastdetect
multi(0)disk(0)rdisk(0)partition(4)\WINNT="1-4"
/fastdetect
multi(0)disk(1)rdisk(0)partition(1)\WINNT

="2-1"

/fastdetect

multi(0)disk(1)rdisk(0)partition(2)\WINNT

="2-2"

/fastdetect

C:\="Windows9x"

其中"1-1"等等标志是为了自己看着方便，提醒自

己启动哪个分区的系统；最后一行的"C:\"项则是为

了启动 DOS、Win9x 系统。

4.把软盘插入软驱，重启机器，……

如有特殊配置，斟酌调整软盘上的文件即可。

Ifconfig 网络配置工具详解 Linux Aidcomcniama fanifcon fig

无论是Linux自动安装还是我们手工安装，Linux都会向你询问有关网络的问题并配置相关的软件。这个用于配置网卡的基本命令就是 ifconfig。

在执行 ifconfig 命令后，系统将在内核表中设置必要的参数，这样 Linux 就知道如何与网络上的网卡通信。ifconfig 命令有以下两种格式：

※ifconfig[interface]

※ ifcon figinter face [aftype] option |address … ifconfig 的第一种格式（或使用不带任何参数的 ifconfig 命令）可以用来查看当前系统的网络配置情况。

在刚刚安装完系统之后，实际上是在没有网卡或者网络连接的情况下使用 Linux，但通过 ifconfig 可以使用回绕方式工作，使计算机认为自己工作在网络上。

现在我们运行一下 ifconfig 命令，不带参数的 ifconfig 命令可以显示当前启动的网络接口，其输出结果为：

```
[root@machine1/sbin]#ifconfig
eth0Linkencap:EthernetHwaddr52:54:AB:DD:6F:61
inetaddr:21034689Bcast:210346127Mask:255255255128
UPBROADCASTRUNNINGMULTICASTMTU:1500Metric:1
RXpackets:46299errors:0dropped:0overruns:0frame:189
TXpackets:3057errors:0dropped:0overruns:0carrier:0
```

collisions:0txqueuelen:100

Interrupt:5Baseaddress:0xece0

loLinkencap:LocalLoopback

inetaddr:127001Mask:255000

UPLOOPBACKRUNNINGMTU:3924Metric:1

RXpackets:44errors:0dropped:0overruns:0frame:0

TXpackets:44errors:0dropped:0overruns:0carrier:0

collisions:0txqueuelen:0

其中以 eth0 为首的部分是本机的以太网卡配置参数，这里显示了网卡在下的设备名/dev/eth0 和硬件的 MAC 地址 52:54:AB:DD:6F:61，MAC 地址是生产厂家定的，每个网卡拥有的唯一地址。

不过我们可以手工改动网卡的 MAC 地址，只要我们在/etc/rcd/initd/中的 network 中加入：

ifconfigeth 0h wether xx:xx:xx:xx:xx:xx

然后重启，此时再用 ifconfig 命令查看一下，我们就会发现网卡的 MAC 地址已经变成 xx:xx:xx:xx:xx:xx 了。

下一行显示本机的 IP 地址信息，分别是本机的 IP 地址，网络广播地址和子网掩码。必须确认这些信

息都是正确无误的，否则 Linux 服务器无法与其它网络设备建立连接。我们也可以手工实现 IP 与 Mac 地址的捆绑，命令是

arp-ieth0-sxxxxxxxxxxxx(IP)xxxxxxxxxx(MAC)

接下来显示的是设备的网络状态。MTU（最大传输单元）和 Metric（度量值）字段显示的是该接口当前的 MTU 和度量值的值。按照惯例，度量值供某些操作系统所用，用于计算一条路由的成本。

再下来显示接口通信的网络统计值。RX 和 TX 分别表示接收和传送的数据包。如果你的网卡已经完成配置却还是无法与其它设备通信，那么从 RX 和 TX 的显示数据上可以简单地分析一下故障原因。在这种情况下，如果你看到接收和传送的包的计数(packets)增加，那有可能是系统的 IP 地址出现了混乱；如果你看到大量的错误(errors)和冲突(Collisions)，那么这很有可能是网络的传输介质出了问题，例如网线不通或 hub 损坏。

再下面的 Interrupt:5Baseaddress:0xece0 显示的是网卡的中断调用号和端口号，这是两个非常重要的硬件配置信息。如果您的网卡是 PCI 的，那么 Linux 在引导时有可能会自动配置这些信息（也很有可能会

让您手工配置）但目前绝大多数网卡都是 PnP 的，这就需要我们进行手工配置了。如果您的网卡还没有配置好，那么运行：

[root@machine1/sbin]#ifconfig

系统只会输出以 lo 为首的部分。lo 是 look-back 网络接口，从 IP 地址 127001 就可以看出，它代表“本机”。无论系统是否接入网络，这个设备总是存在的，除非你在内核编译的时候禁止了网络支持，这是一个称为回送设备的特殊设备，它自动由 Linux 配置以提供网络的自身连接。IP 地址 127001 是一个特殊的回送地址（即默认的本机地址），您可以在自己的系统上用 telnet 对 IP 地址 127001 进行测试。如果有 inetd 进程在运行的话您会从自己的机器上获得登录提示符。Linux 可以利用这个特征在进程与仿真网络之间进行通信。（您有兴趣的话还可以试试本机的实际 IP 地址，如这里的机器就是 21034689，或者试试“localhost”，或者“127001”，同样可以模拟网络通信。这可是 Linux 一个非常突出的优点！）

如果你只是关心某个设备是否正常，可以在 ifconfig 后面加上接口名字：

[root@machine1/sbin]#ifconfigeth0

eth0Linkencap:EthernetHWaddr52:54:AB:DD:6

F:61

inetaddr:21034689Bcast:210346127Mask:2552
55255128

UPBROADCASTRUNNINGMULTICASTMTU:1500Metric
:1

RXpackets:50568errors:0dropped:0overruns:
0frame:198

TXpackets:3200errors:0dropped:0overruns:0
carrier:0

collisions:0txqueuelen:100

Interrupt:5Baseaddress:0xece0 表示 eth0 设备已经正常工作。

有时需要为某个设备接口配置多个 IP 地址，办法是使用设备别名，例如，eth0 设备可以有 eth0，eth0:0，eth0:1 多个别名，每个都可以有一个独立的 IP 地址：

ifconfigeth021034689netmask255255255128br
oadcast210346127

ifconfigeth0:021034688netmask255255255128
broadcast210346127

这样，21034689 和 21034688 都会被绑定在 eth0 设备上，使用同样的网络设备，不同的 IP 地址。

如果你要暂停某个网络接口的工作，使用 down 参数：

ifconfigeth0down

将取消 eth0 网络接口。与之对应的是有一个参数 up，不过由于是缺省值，所以从来不用。

如果我们使用了带有参数的 ifconfig 命令，那就可以手动设置网卡的配置参数了。有效的 ifconfig 命令参数及其意义为(选项对应的特性可以打开也可以取消，只在选项名前加一个破折号（-）即可)：

Interface 网络设备名，如 eth0 就表示本机的第一块网卡。

up 标志接口处于“up”状态，也就是说，IP 层可以对其进行访问。这个选项用于命令行上给出一个地址之时。如果这个接口已被“down”选项临时性取消的话（与该选项对应的标记是 UPRUNNING），还可以用于重新启用一个接口。

down 标标志接口处于“down”状态，也就是说，IP 层不能对其进行访问。这个选项有效地禁止了 IP 通信流通这个接口。注意，它并没有自动删除利用该接口的所有路由信息。如果永久性地取消了一个接口，就应该删除这些路由条目，并在可能的情况下，提供备用路由。

netmask 标分配子网掩码，供接口所用。要么给一个前面是 0x 的 32 位十六进制号码，要么采用只适用于两台主机所用的点分四段式号码。对 SLIP 和 PLIP 接口来说，这个选项是必须配置的。

address 设置指定接口设备的 IP 地址。

Dstaddr adderss 为 PPP 设置远程 IP 地址，此关键字可用 point opoint 代替。

Irq address 设置指定接口设备使用的中断行。

Pointt opoint address 该选项用于只涉及两台主机的点到点链接。对 SLIP 和 PLIP 接口来说，这个选项是必须配置的（如果已经设置了一个点到点地址，ifconfig 就会显示出 POINTTPOINT 标记）。

Broadcast address 广播地址通常源于网络编号，通过设置主机部分的所有位得来。有的 IP 采用的方案有所不同：这个选项可适用于某些奇怪的环境（如果已经设置了广播地址，ifconfig 就会显示出一个 BROADCAST 标记）。

Hwclass addr 设置指定接口设备的 MAC 地址，关键字的后面必须跟硬件名或者与之等价的 ASCII 码。目前支持的硬件类有 ether,ax25,ARCnet 和 netrom。

Metric number 该选项可用于为接口创建的路由表分配度量值。路由信息协议（RIP）利用度量值来

构建网络路由表。ifconfig 所用的默认度量值是 0。如果不运行 RIP 程序，就没必要采用这个选项。如果要运行RIP程序,就尽量不要改变这个默认的度量值。

Mtu bytes 该选项用于设置最大传输单元，也就是接口一次能处理的最大字节数。对以太网接口来说，MTU 的默认设置是 1500 个字节；对 SLIP 接口来说，则是 296 个字节。

arp 标这个选项专用于以太网或包广播之类的广播网络。它启用 ARP（地址解析协议）来保护网络上各台主机的物理地址。对广播网来说，默认设置是“on”(开)。

promisc 将接口置入 promiscuous（混乱）模式。广播网中，这样将导致该接口接收所有的数据包，不管其目标是不是另一台主机。该选项允许利用包过滤器和所谓的以太网窥视技术，对网络通信进行分析。通常情况下，这对揪出网络故障的元凶来说，是相当有用的。但另一方面，如果有人蓄意攻击你的网络，也可浏览到 s 通信数据，进而获得密码，破坏你的网络。一项重要的保证措施是杜绝任何人将他们的计算机接入你的以太网。另一个选项用于保护某些身份验证协议的安全，比如 Kerberos 或 SRA 登录套件（该选项对应的标记是 PROMISC)。

trallers 开或关闭跟踪器。目前在某些 Linux 系统中还无法实现此功能。

allmulti 多播地址即是向不在同一个子网上的一组主机广播数据。多播地址尚未获得内核支持（该选项对应的标记是 ALLMULTI）

tx queuelen len 设置指定接口设备的发送队列长度。由此可以看出有大量的参数可用于配置网卡，下面是在这台计算机上使用 ifconfig 命令的实例：

if configeth 021034689net mask255255255128 broadcast 210346127

该命令的作用是设置网卡 eth0 的 IP 地址，网络掩码和网络的本地广播地址。同样的方式可以用来配置 eth1，eth2 等等，通常 netmask 和 broadcast 只要设置一个就可以了。Win2000IP 路由应用解析 2002-1-2623:20:48 赛迪网谭永刚 Windows 2000 Server 路由提供多协议 LAN 到 LAN、LAN 到 WAN、虚拟专用网络（VPN）和网络地址转换（NAT）路由服务。Windows2000Server 路由供已经熟悉路由协议和服务以及路由协议（例如：TCP/IP、IPX 和 AppleTalk）的系统管理员使用。

解释 IP 路由在通常的术语中，路由就是在网络之间转发数据包的过程。对基于 TCP/IP 的网络，路

由是部分网际协议（IP）与其他网络协议服务结合使用，提供在基于 TCP/IP 的大型网络中单独网段上的主机之间互相转发的能力。

IP 是 TCP/IP 协议的“邮局”，负责对 IP 数据进行分检和传递。每个传入或传出数据包叫做一个 IP 数据报。IP 数据报包含两个 IP 地址：发送主机的源地址和接收主机的目标地址。与硬件地址不同，数据报内部的 IP 地址在 TCP/IP 网络间传递时保持不变。路由是 IP 的主要功能。通过使用 Internet 层的 IP，IP 数据报在每个主机上进行交换和处理。

在 IP 层的上面，源主机上的传输服务用 TCP 段或 UDP 消息的形式向 IP 层传送源数据。IP 层使用在网络上传递数据的源和目标的地址信息装配 IP 数据报。然后 IP 层将数据报向下传送到网络接口层。在这一层，数据链路服务将 IP 数据报转换成在物理网络的网络特定媒体上传输的帧。这个过程在目标主机上按相反的顺序进行。每个 IP 数据报都包含源和目标的 IP 地址。每个主机上的 IP 层服务检查每个数据报的目标地址，将这个地址与本地维护的路由表相比较，然后确定下一步的转发操作。IP 路由器连接到能够互相转发数据包的两个或更多 IP 网段上。

IP 路由器

TCP/IP 网段由 IP 路由器互相连接，IP 路由器是从一个网段向其他网段传送 IP 数据报的设备，这个过程叫做 IP 路由。IP 路由器将两个或更多物理上相互分离的 IP 网段连接起来。

所有的 IP 路由器都有两个基本特征:

1）IP 路由器是多宿主主机。多宿主主机就是用两个或更多网络连接接口连接每个物理分隔的网段的网络主机。

2）IP 路由器可以对其他 TCP/IP 主机转发数据包。

IP 路由器与其他多宿主主机有一个重要的差别：IP 路由器必须能够对其他 IP 网络主机转发基于 IP 的网间通讯。可以使用各种可能的硬件和软件产品来实现 IP 路由器。基于硬盒的路由器，即指定运行专门软件的硬件设备，是很普遍的。另外，您可以使用基于路由和远程访问服务之类的软件（在运行 Windows2000 Server 的计算机上运行）的路由方案。

不管使用哪种类型的 IP 路由器，所有的 IP 路由都依靠路由表在网段之间通讯。

TCP/IP 主机使用路由表维护有关其他 IP 网络及 IP 主机的信息。网络和主机用 IP 地址和子网掩码来

标识。另外，由于路由表对每个本地主机提供关于如何与远程网络和主机通讯的所需信息，因此路由表是很重要的。

对于 IP 网络上的每台计算机，可以使用与本地计算机通讯的其他每个计算机或网络的项目来维护路由表。通常这是不实际的，因此可改用默认网关（IP 路由器）。当计算机准备发送 IP 数据报时，它将自己的 IP 地址和接收者的目标 IP 地址插入到 IP 报头。然后计算机检查目标 IP 地址，将它与本地维护的 IP 路由表相比较，根据比较结果执行相应操作。该计算机执行以下三种操作之一：

将数据报向上传到本地主机 IP 之上的协议层。

经过其中一个连接的网络接口转发数据报。

丢弃数据报。

IP 在路由表中搜索与目标 IP 地址最匹配的路由。从最精确的路由到最不精确的路由，按以下顺序排列：

与目标 IP 地址匹配的路由（主机路由）。

与目标 IP 地址的网络 ID 匹配的路由（网络路由）。

默认路由。

如果没有找到匹配的路由，则 IP 丢弃该数据报。

Win2000IP 路由表

运行 TCP/IP 的每台计算机都要决定路由。这些决定由 IP 路由表控制。要显示运行 Windows2000 的计算机上的 IP 路由表，请在命令提示行键入 routeprint。

下表就是 IP 路由表的一个典型范例。此范例中的计算机运行 Windows2000，带有一个网卡和以下配置：

IP 地址：1000169

子网掩码：255000

默认网关：10001

注意：上表第一列中的说明实际上不显示在 routeprint 命令的输出中。

路由表根据计算机的当前TCP/IP配置自动建立。每个路由在显示的表中占一行。计算机在路由表中搜索与目标 IP 地址最匹配的项目。

动态 IP 地址的捕获及应用

IP 地址与 IP 地址的动态分配

1IP 地址基本概念

Internet 依靠 TCP/IP 协议，在全球范围内实现不同硬件结构、不同操作系统、不同网络系统的互联。在 Internet 上，每一个节点都依靠唯一的 IP 地址互

相区分和相互联系。

IP 地址是一个 32 位二进制数的地址,由 4 个 8 位字段组成，每个字段之间用点号隔开,用于标识 TCP/IP 宿主机。

每个 IP 地址都包含两部分:网络 ID 和主机 ID。网络 ID 标识在同一个物理网络上的所有宿主机，主机 ID 标识该物理网络上的每一个宿主机，于是整个 Internet 上的每个计算机都依靠各自唯一的 IP 地址来标识。

IP 地址构成了整个 Internet 的基础，它是如此重要，每一台联网的计算机无权自行设定 IP 地址，有一个统一的机构—IANA 负责对申请的组织分配唯一的网络 ID,而该组织可以对自己的网络中的每一个主机分配一个唯一的主机 ID,正如一个单位无权决定自己在所属城市的街道名称和门牌号，但可以自主决定本单位内部的各个办公室编号一样。

静态 IP 与动态 IP

IP 地址是一个 32 位二进制数的地址,理论上讲,有大约 40 亿（2 的 32 次方）个可能的地址组合，这似乎是一个很大的地址空间。实际上，根据网络 ID 和主机 ID 的不同位数规则，可以将 IP 地址分为 A（7 位网络 ID 和 24 位主机 ID）、B（14 位网络 ID 和 16

位主机 ID），C（21 位网络 ID 和 8 位主机 ID）三类，由于历史原因和技术发展的差异，A 类地址和 B 类地址几乎分配殆尽，目前能够供全球各国各组织分配的只有 C 类地址。所以说 IP 地址是一种非常重要的网络资源。

对于一个设立了因特网服务的组织机构，由于其主机对外开放了诸如 WWW、FTP、E-mail 等访问服务，通常要对外公布一个固定的 IP 地址，以方便用户访问。当然，数字 IP 不便记忆和识别，人们更习惯于通过域名来访问主机，而域名实际上仍然需要被域名服务器（DNS）翻译为 IP 地址。例如，你的主页地址是 wwwmyhostcom，用户可以方便地记忆和使用，而域名服务器会将这个域名翻译为 10112123234，这才是你在网上的真正地址。

而对于大多数拨号上网的用户，由于其上网时间和空间的离散性，为每个用户分配一个固定的 IP 地址（静态 IP）是非常不可取的，这将造成 IP 地址资源的极大浪费。因此这些用户通常会在每次拨通 ISP 的主机后，自动获得一个动态的 IP 地址，该地址当然不是任意的，而是该 ISP 申请的网络 ID 和主机 ID 的合法区间中的某个地址。拨号用户任意两次连接时的 IP 地址很可能不同，但是在每次连接时间内 IP 地

址不变。

WIN2k 下几种 FTPServer 的比较

（以下 FTPServer 都是基于 windows 操作系统的。）1Serv_U:最简单小巧的 FTPServer 了，别的不说，仅仅 15M 的身体就让别的 Server 望尘莫及。设置也极为简单，支持更改端口号。可以从 Server 的监控窗口直接看到用户，ip，下载速度等等，缺点：占用系统资源较大，当用户太多的时候就会导致 Server 负担过重，不信你用 Serv_U 做 server 开 1000 个用户试试看，保证死的很难看。没法 mount 目录，所以对于文件搞的到处都是的来说，不是很好的选择。当然，据 flyriver 说可以用别的来代替，没用过，没发言权，总之是不能直接 mount 不爽，。所以建议偶尔使用 FTP 的人使用，而且 Serv_U 不用安装，直接拷贝了就可以使用！

2ArGoFTP:和 Serv_U 类似的东西，也很小巧，这个东西我没有仔细用过，装了一下看了看界面就拉到了。不过想来应该和 Serv_U 差不多吧，这个是免费的！而 Serv_U 则需要注册，所以，，大家心照不宣啦。这个东西我在 2K 下一启动就被 2K 强行关闭了，不知道别人的系统如何？不过我想应该是和 2K 有不兼容的地方，用过的人说说详细的功能和缺点吧。

最新版 1053

3G6FTP:也是一个比较常用的 Server，freeware。这个东西支持每个目录去显示 message，没有长时间的去用，所以对于多用户大负担下性能如何也不是很清楚。

目前能找到的最新版是 20beta6，有 keygen 的。

4VermillionFTP：FTPServer，freeware 来的，缺陷在于所有 mount 的目录都可以看到，但是可以设置访问权限的，可是谁又知道它有没有 bug 会让该目录被访问呢？最新版 131，有 keygen。

最主要的是 mount 目录之后/就变成了/x:/，看起来不好看，所以放弃了。

5War_FTP：可能是我用的比较多的一个 FTPServer 了，这个东西设置起来很烦的，不过对资源占用较小，我用的时候经常有>500 用户在线，

最多到过 1200 多，居然没死机，。但是致命的缺点是不太稳定，在 2K 下经常就 error 了，尤其是负担大的时候，Sysadmin 都连不上去，mount 目录和添加用户也非常方便（如果你熟悉了的话）。

最新版 170beta1released4，免费软件。而且我用的时候用的和 ssb 一样的设置居然 IPallow 不行:-(，难道是和我不兼容？

6WS_FTP:也是一个比较强大的 FTPServer 了，不是因为 WS_FTP 是经常被用到的 FTPClient 吧？要注册才可以使用的。这个东西和 G6 我都是用一下就放弃了，没什么吸引人的地方，或者是我没用到，用过的应该发言，我就不多说了。最新版 10x。

7IIS:微软的东西，性能么，当然不错了，占用系统资源也不错，不过现在却是我在用的，没办法，就它还稳定一些了，据勇哥说是最稳定的 FTPServer 了。从 50 开始支持了续传。Pro 版的有个最大的缺陷是仅能连接 10 个用户，而且这个数目有点问题，那次我重启之后自己都连不进去，当时用户仅2名而已，而且上载续传的问题是你可以对该目录下任何文件进行任何操作！AdvancedServer 版默认是 10000 用户。这个东西确实高效！是一个不错的 Server，我本地下载可以超过 3M/s，别的 FTPServer 都不行。尤其是 War_FTP，仅能到<100K/s，差别极大。管理起来很烦，因为从 Server 上看不到用户的连接情况！你不清楚他们是断线了还是怎么了。否则就太完美了

简单网络管理协议透视——从 SNMPv1 到 SNMPv3

简单网络管理协议（SNMP）是目前 TCP/IP 网络中应用最广泛的网络管理协议，是网络管理事实上的

标准。它不仅指简单的网络管理协议本身，而且代表采用 SNMP 协议的网络管理框架，经历了从 SNMPv1 到 SNMPv3 的发展历程，本文将从下面几个方面探讨其演变过程。SNMPv1 管理模型 SNMPv1 管理模型包括四个关键元素：管理站、管理代理、管理信息库、管理协议。下图显示了上述四个元素的关系。

1、管理站

管理站是网络管理员与网络管理系统的接口，它实际上是一台运行特殊管理软件的计算机。管理站运行一个或多个管理进程，它通过 SNMP 协议在网络上与代理通信，发送命令并接收代理的应答。管理站通过获取 MIB 对象的值来实现网络资源监视，也可以通过修改特殊变量的值来使代理执行一个动作或修改资源的配置。许多管理站的应用进程都具有图形用户界面，提供数据分析、故障发现的功能，网络管理者能方便地检查网络状态并在需要时采取行动。

2、管理代理

网络中的主机、路由器、网桥和交换机等都可配置 SNMP，成为管理代理，以便管理站对它进行管理。每个代理负责维护本地 MIB 来存放被管资源的状态、运行情况等，对来自管理站的信息查询和动作执行的请求作出响应，同时还可以异步地向管理站提供一些

重要的非请求信息。管理站可以访问多个管理代理的MIB对象，接收来自多个代理的Trap，因此从操作和控制的角度看，管理站“管理”着许多代理。同时，管理代理也能对多个管理站的请求作出响应，是一种一对多的关系，管理代理为了控制管理站对它的MIB的使用，保护它自己和它的MIB，避免不希望的或未授权的访问，使用了共同体的概念。管理代理为每一个必要的认证、访问控制和代理特性的联合建立一个共同体。从管理站发往代理的报文都包含共同体名，它起着口令的作用，只要报文发送方知道口令，该报文就被认为是可信的。由此可见，这并不是很安全的方式，所以，很多管理者仅仅提供网络监视的功能（get 和 trap 操作），屏蔽掉了网络控制功能（set操作）。

3、管理信息库

MIB是一个信息存储库，它包含了管理代理中的有关配置和性能的数据，是网络管理的基础。每一个被管资源由一个对象来表示，MIB就是由这样一些对象组成的结构化的集合。在RFC1155中定义的管理信息结构给出了MIB结构的总体框架。4、管理协议

管理站和管理代理之间是通过 SNMP 网络管理协议连接的，通过 SNMP 报文的形式来交换信息。协议

主要支持 Get、Set 和 Trap 三种功能共五种操作，Get 用于管理站获取代理的 MIB 对象值，Set 用于管理站去设置代理的 MIB 对象值，Trap 用于代理向管理站通告重要事件。SNMPv1 存在的问题及 SNMPv2 的改进 SNMPv1 协议以其简单和灵活性，获得了许多厂商的支持，得到广泛应用，但其缺点也很多，功能简单、安全性差。SNMPv1 是基于一种主动轮询的监视机制，轮询间隔短时对网络性能影响很大，不适合大规模的网络管理；SNMPv1 不支持管理站-管理站之间的通信，这样，它不允许一个管理系统去了解由另一个管理系统管理的设备和网络的状况。与 SNMPv1 单纯的集中式管理模式不同，SNMPv2 支持分布式/分层式的网络管理结构，在 SNMPv2 管理模型中有些系统可以同时具有管理器和代理的功能，作为代理，它可以接收上一级管理系统的命令，访问其存储的本地信息，也可以提供它所负责的管理域中其它代理的信息摘要，向上级管理器发送 Trap 信息。SNMPv2 定义了两个 MIB 库，一个相当于 SNMPv1 的 MIB-II，另一个是 Manager－to-Manager(M2M)MIB，提供对分布式管理结构的支持。网络管理的安全威胁和 SNMPv3 体系结构使用 SNMPv1、SNMPv2 进行网络管理时，由于安全功能有限，面临着假冒、信息篡改、报文序列和定时机制的修改、

信息暴露等几种安全威胁。SNMPv3 通过简明的方式实现了加密和验证功能。SNMPv3 结构是由分布的、相互连接的 SNMP 实体组成。每一个实体可以作为一个代理节点、管理器节点或代理和管理器的混合节点。SNMPv3 实体通常由一 SNMP 引擎和一个或多个相关联的应用组成。应用主要有：命令产生器（Command Generator）、通知接收器（Notification Receiver）、代理转发器（Proxy Forwarder）、命令响应器（Command Responder）、通知始发器（Notification Originator）和一些其他的应用。RFC2271 定义的 SNMPV3 体系结构，体现了模块化的设计思想，SNMP 引擎和它支持的应用被定义为一系列独立的模块。SNMP 实体的功能由所在实体的多个模块决定，每个实体仅仅是模块的不同组合，每个模块具有相对独立性，当改进或替换某一模块时，不会影响整个结构，这样可以简单地实现功能的增加和修改。作为 SNMP 实体核心的 SNMP 引擎用于发送和接受消息、鉴别消息、对消息进行解密和加密以及控制对被管对象的访问等功能。SNMPv3 可运用于多种操作环境，可根据需要增加、替换模块和算法，具有多种安全处理模块，有极好的安全性和管理功能，既弥补了前两个版本在安全方面的不足，同时又保持了 SNMPv1 和 SNMPv2 易于理解、易于实现的特

点。随着 SNMPv3 的进一步扩充和完善，必将进一步推动网络管理技术的发展。使用 ICMP 地址掩码请求来鉴定 SUN 机器

对于 ICMP 地址掩码请求，只有少数操作系统会进行响应的回应，这些系统包括 ULT RIX Open VMS，Windows95/98/98SE/ME,NTbelowSP4,和 SUNSolaris 机器。但其中 SUN 机器对碎片 ICMP 地址掩码回答（fragmented ICMP Address Mask Requests）最不一样，所以允许远程用户来鉴定 SUN 机器。

下面是通过由 Alfredo And resomella 写的 SING 对 SUNSOLARIS27 机器正常的地址掩码请求：

```
#/sing-maskIP_Address
SINGingtoIP_Address(IP_Address):12databytes
12bytesfromIP_Address:icmp_seq=0ttl=236mask=2552552550
12bytesfromIP_Address:icmp_seq=1ttl=236mask=2552552550
12bytesfromIP_Address:icmp_seq=2ttl=236mask=2552552550
12bytesfromIP_Address:icmp_seq=3ttl=236mask=2552552550
```

12bytesfromIP_Address:icmp_seq=4ttl=236mask=2552552550

---IP_Addresssingstatistics---

5packetstransmitted,5packetsreceived,0%packetloss

操作系统会回答一个 ICMP 的地址掩码请求并带有其响应的网络地址掩码。

下面我们来看我们发送一些碎片请求，下面的例子是通过发送 8 字节的 IP 数据碎片到同样上面操作的 SUNSOLARIS27 机器上，就可以看到我们获得的回应和刚才的不一样了(-c2 是允许 SING 发送两个 ICMP 地址掩码请求)：

#/sing-mask-c2-F8IP_Address

SINGingtoIP_Address(IP_Address):12databytes

12bytesfromIP_Address:icmp_seq=0ttl=241mask=0000

12bytesfromIP_Address:icmp_seq=1ttl=241mask=0000

---IP_Addresssingstatistics---

2packetstransmitted,2packetsreceived,0%packetloss

这样你就可以看到 SUNSOLARIS 回应的网络地址掩码是 0000。

我们可以使用下面的方法了解决这个问题：

ndd-set/dev/ipip_respond_to_address_mask_broadcast0

ndd-set/dev/ipip_respond_to_echo_broadcast0

ndd-set/dev/ipip_respond_to_timestamp0

ndd-set/dev/ipip_respond_to_timestamp_broadcast0

ndd-set/dev/ipip_forward_directed_broadcasts0

参考：

1）SING 可以到下面的地址去下载：

http://downloadsourceforgenet/sing/SING-10b7tgz

2）更具体的关于 ICMP 的更多使用方法：

http://www.sys-security.com

Arp 理论的实践

这里推荐一个不错的上述理论产物，dsniff，这个软件包中包括了 filesnarf、mailsnarf、msgsnarf、urlsnarf、dnsspoof、macof 等诸多很有特色的组件，

可以捕获网络中的各种敏感数据，但这些不是今天感兴趣的主题，我们只看其中一个组件，arpspoof，这个组件就是上述 arp 理论的一个实践，它的工作原理是这样的：发起 arpspoof 的主机向目标主机发送伪造的 arp 应答包，骗取目标系统更新 arp 表，将目标系统的网关的 mac 地址修改为发起 arpspoof 的主机 mac 地址，使数据包都经由发起 arpspoof 的主机，这样即使系统连接在交换机上，也不会影响对数据包的攫取，由此就轻松的通过交换机实现了网络监听。

举例如下：

主机 a 和 b 连接在交换机的同一个 Vlan 上，

A 机的 ip 地址：192168137

B 机的 ip 地址：192168135，mac 地址为：08-00-20-c8-fe-15

网关的 Ip 地址：192168133，mac 地址为：00-90-6d-f2-24-00

首先在 a 机上看看 a 机的 arp 表

C:\>arp-a

Interface:192168137

InternetAddressPhysicalAddressType

19216813300-90-6d-f2-24-00dynamic

我们看到a机中保留着网关的ip地址192168133

和对应的 mac 地址 00-90-6d-f2-24-00

我们在 B 机上执行 arpspoof，将目标指向 a 机，宣称自己为网关，如下：

HOSTB#arpspoof-t192168137192168133

8:0:20:c8:fe:150:50:ba:1a:f:c0080642:arpreply192168133is-at8:0:20:c8:fe:15

8:0:20:c8:fe:150:50:ba:1a:f:c0080642:arpreply192168133is-at8:0:20:c8:fe:15

8:0:20:c8:fe:150:50:ba:1a:f:c0080642:arpreply192168133is-at8:0:20:c8:fe:15

8:0:20:c8:fe:150:50:ba:1a:f:c0080642:arpreply192168133is-at8:0:20:c8:fe:15

8:0:20:c8:fe:150:50:ba:1a:f:c0080642:arpreply192168133is-at8:0:20:c8:fe:15

8:0:20:c8:fe:150:50:ba:1a:f:c0080642:arpreply192168133is-at8:0:20:c8:fe:15

8:0:20:c8:fe:150:50:ba:1a:f:c0080642:arpreply192168133is-at8:0:20:c8:fe:15

8:0:20:c8:fe:150:50:ba:1a:f:c0080642:arpreply192168133is-at8:0:20:c8:fe:15

8:0:20:c8:fe:150:50:ba:1a:f:c0080642:arpreply192168133is-at8:0:20:c8:fe:15

可以看到 b 机持续向 a 发送 arp 回应包，宣称网关 192168133 的 mac 地址是自己！此时，

我们在 a 机上看看 arp 表的内容，

C:\>arp-a

Interface:192168137

Internet Address Physical Address Type

19216813308-00-20-c8-fe-15dynamic

哈！a 机的 arp 表已经改变了，网关的 mac 地址被更新为了 b 机的 mac 地址，这样，当有数据包发送时，a 机理所当然的会发到它 arp 表中网关对应的 mac 地址 08-00-20-c8-fe-15，然而这个地方的 b 机正在等待着，悄然无声的冒充网关收发着 a 机的数据包。

有一点要说明的是，为了让 a 机能正常使用网络，

b 机还必须打开数据转发，linux 中可以使用 sysctl-wnetipv4ip_forward=1bsd 系统可以使用 sysctl-wnetinetipforwarding=1solaris 系统可以使用 ndd-set/dev/ipip_forwarding1 除了这样打开内核的支持外，也可以选用外部的 fragrouter 等转发软件，如此，就能确保 a 机正常工作了。

此外，ettercap 的作者指出，内核为 24x 的 linux 系统在 arp 实现中，考虑到了 arp 欺骗，不会接受未经请求的 arp 回应，因此直接向这种系统发送 arpreply 也是无效的，不过，有意思的是虽然它不会接受未经请求的 arpreply，但是只要接收到 arp 的 request，它就会更新自己的 arp 缓存，;)，如此就好办了，发送一个伪造的 arprequest 即可！不过，作者在自己实验时没有发现这个问题，作者内核为 247 的系统接受了直接的 arpreply，并更新了自己的 arp 表。如果一切配置正常的话，被重定向的 a 机是不会有什么明显的感觉的，网络照常是通畅的，只是在后台数据都绕了一个小圈子，不是直接到网关,而是先经由 b 机，再由 b 机转发到网关，因为数据包都经过了 b 机，那么在 b 机上起一个网络监听软件，a 机的所有数据必然会被监听到。交换环境下的监听由此实现！

除此之外，dsniff 还提供了 macof 等淹没交换机 arp 表等进行监听的模式，这里就不介绍了，有兴趣的读者可以自己查阅相关资料。

Arp 方式监听的防范

wwwcnsafenet 对付采用 arp 方式的监听也是个比较棘手的问题，有几个不是非常理想的对策。

首先还是上面提到的加密，尽可能的让局域网内的传输的数据都是秘文的，这个可能相对最理想的防范方法，但实施起来可能有一点困难。有一点要注意，ssh1 是不安全的，我们提到的 dsniff 和 ettercap 都可以对 ssh1 实施中间人的监听。

另外，还可以考虑指定静态 arp，如大多数 unix 系统支持 arp 读取指定的 ip 和 mac 地址对应文件，首先编辑内容为 ip 和 mac 地址对照的文件，然后使用命令：arp-f/path/to/ipandmacmapfile 读取文件，这样就指定了静态的 arp 地址，即使接收到 arpreply，也不会更新自己的 arp 缓存，从而使 arpspoof 丧失作用。windows 系统没有-f 这个参数，但有-s 参数，用命令行指定 ip 和 mac 地址对照关系，如 arp-s19216813300-90-6d-f2-24-00，可惜除了 xp 外，其它的版本的 window 平台即使这样做，当接收到伪造的 arpreply 后，依然会更新自己的 arp 缓存，

用新的 mac 地址替换掉老的 mac 地址，所以无法对抗 arpspoof。而且采用静态 arp 有一个缺憾，就是如果网络很大的话，工作量会非常的大。

网际协议

IP,InternetProtocol,(RFC-791)网际协议

ICMP,InternetControlMessageProtocol,(RFC-792)网际报文控制协议

IGMP,InternetGroupMulticastProtocol,(RFC-1112)网际成组多路广播协议

UDP,UserDatagramProtocol,(RFC-768) 用户数据报协议

TCP,TransmissionControlProtocol,(RFC-793) 传输控制协议

TELNET,TelnetProtocol,(RFC-854,855)Telnet 协议

FTP,FileTransferProtocol,(RFC-959) 文件传输协议,计算机网络上主机之间传送

文件的一种服务协议。

SMTP,SimpleMailTransferProtocol,(RFC-821) 简单邮件传输协议

SMTP-SIZE,SMTPServiceExtforMessageSize,(RFC-1870)可处理大信包的扩充的

SMTP 协议

SMTP-EXT,SMTPServiceExtensions,(RFC-1869) SMTP 协议扩充

NTPV2,NetworkTimeProtocol(Version2),(RFC-1119)网络时间协议版本 2

SNMP,SimpleNetworkManagementProtocol,(RFC-1157)简单网络管理协议

NETBIOS,NetBIOSServicesProtocols,(RFC-1001,1002)NetBIOS 服务协议

ECHO,EchoProtocol 应答协议

DISCARD,DiscardProtocol 取消协议

CHARGEN,CharacterGeneratorProtocol 字符发生器协议

QUOTE,QuoteoftheDayProtocol 气象报告协议

USERS,ActiveUsersProtocol 当前用户报告协议

DAYTIME,DaytimeProtocol 日期查询协议

TIME,TimeServerProtocol 标准时间服务器协议

TFTP,TrivialFileTransferProtocol 测试用的文件传输协议

TP-TCP,ISOTransportServiceontopoftheTCP 基于 TCP 的 ISO 传输层服务

ETHER-MIB,Ether-MIB 以太网管理信息库

PPP,Point-to-PointProtocol 点对点协议

PPP-HDLC,PPPinHDLCFramingHDLC 分组的 PPP 协议

IP-SMDS,IPDatagramovertheSMDSService 基于 SMDS 服务的 IP 数据报

RIP,RoutingInformationProtocol 路由信息协议

ARP,AddressResolutionProtocol,(RFC-826) 地址解析协议

RARP,AReverseAddressResolutionProtocol,(RFC-903)逆向地址解析协议

POP3,PostOfficeProtocol,Version3,(RFC-1725)电子邮局协议,版本 3

HTTP,HyperTextTransferProtocol 超文本传输协议

RPC,RemoteProcedureCallProtocol,(RFC-1831)远过程调用协议

NICNAME,WhoIsProtocol,(RFC-954)WhoIs 协议

DHCP,DynamicHostConfigurationProtocol,(RFC-1541)主机动态配置协议

NNTP,NetworkNewsTransferProtocol,(RFC-977)网络新闻传输协议

IARP,InverseAddressResolutionProtocol,(RFC-1293)反向地址解析协议

RAP,InternetRouteAccessProtocol,(RFC-1476)网际路由存取协议

IRCP,InternetRelayChatProtocol,(RFC-1459)网际转发的闲聊协议

RMCP,RemoteMailCheckingProtocol,(RFC-1339)远程邮件检查协议

MTP,MulticastTransportProtocol,(RFC-1301)多路广播传输协议

GOPHER,TheInternetGopherProtocol,(RFC-1436)网际 Gopher 协议

LISTSERV,ListservDistributeProtocol,(RFC-1429)Listserv 分布协议

Arp 方式监听的检测

首先是借助检测 ip 地址和 mac 地址对应的工具，如 arpwatch，安装了 arpwatch 的系统在发生 mac 地址变化时会在系统的日志文件中看到如下提示 Apr 2123:05:00192168135arpwatch:flipflop1921681330:90:6d:f2:24:0(8:0:20:c8:fe:15)Apr2123:05:02192168135arpwatch:flipflop1921681338:0:20:c8:fe:15(0:90:6d:f2:24:0)Apr2123:05:03192168135a

rpwatch:flipflop1921681330:90:6d:f2:24:0(8:0:20:c8:fe:15)

从提示中可以看出 arpwatch 检测到了网关 mac 地址发生了改变。

其次借助于一些入侵检测系统，如 snort，亦可以起到的一定的检测作用。在 snort 的配置文件中打开 arpspoof 的 preprocessor 开关并进行配置即可。

如果采用本地解析时，观测局域网本地的 dns 服务器的反解是一个好的办法，因为发起 arpspoof 的主机会不间断的尝试正反解析冒充的网关 ip，发送数量非常多的重复解析数据包，当怀疑有 arpspoof 时很容易被发现，如下：

nameserver#tcpdump-n-soport53

tcpdump:listeningonhmeo

23:19:22489417192168135417797>19216816853:32611+PTR?3322410

2202in-addrarpa(45)(DF)

23:19:22490467192168135417798>19216816853:32611+PTR?3322410

2202in-addrarpa(45)(DF)

TCP/IP 的安全性

TCP/IP 的层次不同提供的安全性也不同，例如，

在网络层提供虚拟私用网络，在传输层提供安全套接服务。

介绍TCP/IP不同层次的安全性和提高各层安全性的方法

Internet层的安全性

对 Internet 层的安全协议进行标准化的想法早就有了。在过去十年里，已经提出了一些方案。例如，“安全协议 3 号(SP3)”就是美国国家安全局以及标准技术协会作为“安全数据网络系统(SDNS)”的一部分而制定的。“网络层安全协议(NLSP)”是由国际标准化组织为“无连接网络协议(CLNP)”制定的安全协议标准。“集成化 NLSP(I-NLSP)”是美国国家科技研究所提出的包括 IP 和 CLNP 在内的统一安全机制。SwIPe 是另一个 Intenet 层的安全协议，由 Ioannidis 和 Blaze 提出并实现原型。所有这些提案的共同点多于不同点。事实上，他们用的都是 IP 封装技术。其本质是，纯文本的包被加密，封装在外层的 IP 报头里，用来对加密的包进行 Internet 上的路由选择。到达另一端时，外层的 IP 报头被拆开，报文被解密，然后送到收报地点。

Internet 工程特遣组(IETF)已经特许 Internet 协议安全协议(IPSEC)工作组对IP安全协议(IPSP)和

对应的 Internet 密钥管理协议(IKMP)进行标准化工作。IPSP 的主要目的是使需要安全措施的用户能够使用相应的加密安全体制。该体制不仅能在目前通行的 IP(IPv4)下工作，也能在 IP 的新版本(IPng 或 IPv6)下工作。该体制应该是与算法无关的，即使加密算法替换了，也不对其他部分的实现产生影响。此外，该体制必须能实行多种安全政策，但要避免给不使用该体制的人造成不利影响。按照这些要求，IPSEC 工作组制订了一个规范：认证头(AuthenticationHeader，AH)和封装安全有效负荷(Encapsulating Security Payload，ESP)。简言之，AH 提供 IP 包的真实性和完整性，ESP 提供机要内容。

IP AH 指一段消息认证代码(Message Authentication Code，MAC)，在发送 IP 包之前，它已经被事先计算好。发送方用一个加密密钥算出 AH，接收方用同一或另一密钥对之进行验证。如果收发双方使用的是单钥体制，那它们就使用同一密钥；如果收发双方使用的是公钥体制，那它们就使用不同的密钥。在后一种情形，AH 体制能额外地提供不可否认的服务。事实上，有些在传输中可变的域，如 IPv4 中的 time-to-live 域或 IPv6 中的 hoplimit 域，都是在 AH 的计算中必须忽略不计的。RFC1828 首次规定了加

封状态下 AH 的计算和验证中要采用带密钥的 MD5 算法。而与此同时，MD5 和加封状态都被批评为加密强度太弱，并有替换的方案提出。

IP ESP 的基本想法是整个 IP 包进行封装，或者只对 ESP 内上层协议的数据(运输状态)进行封装，并对 ESP 的绝大部分数据进行加密。在管道状态下，为当前已加密的 ESP 附加了一个新的 IP 头(纯文本)，它可以用来对 IP 包在 Internet 上作路由选择。接收方把这个 IP 头取掉，再对 ESP 进行解密，处理并取掉 ESP 头，再对原来的 IP 包或更高层协议的数据就象普通的 IP 包那样进行处理。RFC1827 中对 ESP 的格式作了规定，RFC1829 中规定了在密码块链接(CBC)状态下 ESP 加密和解密要使用数据加密标准(DES)。虽然其他算法和状态也是可以使用的，但一些国家对此类产品的进出口控制也是不能不考虑的因素。有些国家甚至连私用加密都要限制。

AH 与 ESP 体制可以合用，也可以分用。不管怎么用，都逃不脱传输分析的攻击。人们不太清楚在 Internet 层上，是否真有经济有效的对抗传输分析的手段，但是在 Internet 用户里，真正把传输分析当回事儿的也是寥寥无几。

1995 年 8 月，Internet 工程领导小组(IESG)批

准了有关 IPSP 的 RFC 作为 Internet 标准系列的推荐标准。除 RFC1828 和 RFC1829 外，还有两个实验性的 RFC 文件，规定了在 AH 和 ESP 体制中，用安全散列算法(SHA)来代替 MD5(RFC1852)和用三元 DES 代替 DES(RFC1851)。

在最简单的情况下，IPSP 用手工来配置密钥。然而，当 IPSP 大规模发展的时候，就需要在 Internet 上建立标准化的密钥管理协议。这个密钥管理协议按照 IPSP 安全条例的要求，指定管理密钥的方法。

因此，IPSEC 工作组也负责进行 Internet 密钥管理协议(IKMP)，其他若干协议的标准化工作也已经提上日程。其中最重要的有：

IBM 提出的“标准密钥管理协议(MKMP)”

SUN 提出的“Internet 协议的简单密钥管理(SKIP)”

PhilKarn 提出的“Photuris 密钥管理协议”

Hugo Krawczik 提出的“安全密钥交换机制(SKEME)”

NSA 提出的“Internet 安全条例及密钥管理协议”

HilarieOrman 提出的“OAKLEY 密钥决定协议”

在这里需要再次强调指出，这些协议草案的相似点多于不同点。除 MKMP 外，它们都要求一个既存的、

完全可操作的公钥基础设施(PKI)。MKMP 没有这个要求，因为它假定双方已经共同知道一个主密钥(MasterKey)，可能是事先手工发布的。SKIP 要求 Diffie-Hellman 证书，其他协议则要求 RSA 证书。

1996 年 9 月，IPSEC 决定采用 OAKLEY 作为 ISAKMP 框架下强制推行的密钥管理手段，采用 SKIP 作为 IPv4 和 IPv6 实现时的优先选择。目前已经有一些厂商实现了合成的 ISAKMP/OAKLEY 方案。Photuris 以及类 Photuris 的协议的基本想法是对每一个会话密钥都采用 Diffie-Hellman 密钥交换机制，并随后采用签名交换来确认 Diffie--Hellman 参数，确保没有“中间人”进行攻击。这种组合最初是由 Diffie、Ooschot 和 Wiener 在一个“站对站(STS)”的协议中提出的。Photuris 里面又添加了一种所谓的“cookie”交换，它可以提供“清障(anti-logging)”功能，即防范对服务攻击的否认。

Photuris 以及类 Photuris 的协议由于对每一个会话密钥都采用 Diffie-Hellman 密钥交换机制，故可提供回传保护(back-traf ficprotec tion，BTP)和完整转发安全性(perfect-for ward secrecy，PFS)。实质上，这意味着一旦某个攻击者破解了长效私钥，比如 Photuris 中的 RSA 密钥或 SKIP 中的

Diffie-Hellman 密钥,所有其他攻击者就可以冒充被破解的密码的拥有者。但是，攻击者却不一定有本事破解该拥有者过去或未来收发的信息。

值得注意的是，SKIP 并不提供 BTP 和 PFS。尽管它采用 Diffie-Hellman 密钥交换机制，但交换的进行是隐含的，也就是说，两个实体以证书形式彼此知道对方长效 Diffie--Hellman 公钥，从而隐含地共享一个主密钥。该主密钥可以导出对分组密钥进行加密的密钥，而分组密钥才真正用来对 IP 包加密。一旦长效 Diffie-Hellman 密钥泄露，，则任何在该密钥保护下的密钥所保护的相应通信都将被破解。而且 SKIP 是无状态的，它不以安全条例为基础。每个 IP 包可能是个别地进行加密和解密的，归根到底用的是不同的密钥。

SKIP 不提供 BTP 和 PFS 这件事曾经引起 IPSEC 工作组内部的批评，该协议也曾进行过扩充，试图提供 BTP 和 PFS。但是，扩充后的 SKIP 协议版本其实是在 BTP 和 PFS 功能的提供该协议的无状态性之间的某种折衷。实际上，增加了 BTP 和 PFS 功能的 SKIP 非常类似于 Photuris 以及类 Photuris 的协议，唯一的主要区别是 SKIP(仍然)需要原来的 Diffie-Hellman 证书。这一点必须注意:目前在 Internet 上，RSA 证

书比其他证书更容易实现和开展业务。

大多数 IPSP 及其相应的密钥管理协议的实现均基于 Unix 系统。任何 IPSP 的实现都必须跟对应协议栈的源码纠缠在一起，而这源码又能在 Unix 系统上使用，其原因大概就在于此。但是，如果要想在 Internet 上更广泛地使用和采纳安全协议，就必须有相应的 DOS 或 Windows 版本。而在这些系统上实现 Internet 层安全协议所直接面临的一个问题就是，PC 上相应的实现 TCP/IP 的公共源码资源什么也没有。为克服这一困难，Wagner 和 Bellovin 实现了一个 IPSEC 模块，它象一个设备驱动程序一样工作，完全处于 IP 层以下。

Internet 层安全性的主要优点是它的透明性，也就是说，安全服务的提供不需要应用程序、其他通信层次和网络部件做任何改动。它的最主要的缺点是：Internet 层一般对属于不同进程和相应条例的包不作区别。对所有去往同一地址的包，它将按照同样的加密密钥和访问控制策略来处理。这可能导致提供不了所需的功能，也会导致性能下降。针对面向主机的密钥分配的这些问题，RFC1825 允许(甚至可以说是推荐)使用面向用户的密钥分配，其中，不同的连接会得到不同的加密密钥。但是，面向用户的密钥分配

需要对相应的操作系统内核作比较大的改动。

虽然 IPSP 的规范已经基本制订完毕，但密钥管理的情况千变万化，要做的工作还很多。尚未引起足够重视的一个重要的问题是在多播(multicast)环境下的密钥分配问题，例如，在 Internet 多播骨干网(MBone)或 IPv6 网中的密钥分配问题。

简而言之，Internet 层是非常适合提供基于主机对主机的安全服务的。相应的安全协议可以用来在 Internet 上建立安全的 IP 通道和虚拟私有网。例如，利用它对 IP 包的加密和解密功能，可以简捷地强化防火墙系统的防卫能力。事实上，许多厂商已经这样做了。RSA 数据安全公司已经发起了一个倡议，来推进多家防火墙和 TCP/IP 软件厂商联合开发虚拟私有网。该倡议被称为 S-WAN(安全广域网)倡议。其目标是制订和推荐 Internet 层的安全协议标准。

二、传输层的安全性

在 Internet 应用编程序中，通常使用广义的进程间通信(IPC)机制来与不同层次的安全协议打交道。比较流行的两个 IPC 编程界面是 BSDSockets 和传输层界面(TLI)，在 Unix 系统 V 命令里可以找到。

在 Internet 中提供安全服务的首先一个想法便是强化它的 IPC 界面，如 BSDSockets 等，具体做法

包括双端实体的认证，数据加密密钥的交换等。Netscape 通信公司遵循了这个思路，制定了建立在可靠的传输服务(如 TCP/IP 所提供)基础上的安全套接层协议(SSL)。SSL 版本 3(SSLv3)于 1995 年 12 月制定。它主要包含以下两个协议：

SSL 记录协议它涉及应用程序提供的信息的分段、压缩、数据认证和加密。SSLv3 提供对数据认证用的 MD5 和 SHA 以及数据加密用的 R4 和 DES 等的支持，用来对数据进行认证和加密的密钥可以通过 SSL 的握手协议来协商。

SSL 握手协议用来交换版本号、加密算法、(相互)身份认证并交换密钥。SSLv3 提供对 Deffie-Hellman 密钥交换算法、基于 RSA 的密钥交换机制和另一种实现在 Fortezzachip 上的密钥交换机制的支持。

Netscape 通信公司已经向公众推出了 SSL 的参考实现(称为 SSLref)。另一免费的 SSL 实现叫做 SSLeay。SSLref 和 SSLeay 均可给任何 TCP/IP 应用提供 SSL 功能。Internet 号码分配当局(IANA)已经为具备 SSL 功能的应用分配了固定端口号，例如，带 SSL 的 HTTP(https)被分配的端口号为 443，带 SSL 的 SMTP(ssmtp)被分配的端口号为 465，带 SSL 的 NNTP(snntp)被分配的端口号为 563。

微软推出了 SSL2 的改进版本称为 PCT(私人通信技术)。至少从它使用的记录格式来看，SSL 和 PCT 是十分相似的。它们的主要差别是它们在版本号字段的最显著位(TheMostSignificantBit)上的取值有所不同:SSL 该位取 0，PCT 该位取 1。这样区分之后，就可以对这两个协议都给以支持。

1996 年 4 月，IETF 授权一个传输层安全(TLS)工作组着手制定一个传输层安全协议(TLSP)，以便作为标准提案向 IESG 正式提交。TLSP 将会在许多地方酷似 SSL。

前面已介绍 Internet 层安全机制的主要优点是它的透明性，即安全服务的提供不要求应用层做任何改变。这对传输层来说是做不到的。原则上，任何 TCP/IP 应用，只要应用传输层安全协议，比如说 SSL 或 PCT，就必定要进行若干修改以增加相应的功能，并使用(稍微)不同的 IPC 界面。于是，传输层安全机制的主要缺点就是要对传输层 IPC 界面和应用程序两端都进行修改。可是，比起 Internet 层和应用层的安全机制来，这里的修改还是相当小的。另一个缺点是,基于 UDP 的通信很难在传输层建立起安全机制来。同网络层安全机制相比，传输层安全机制的主要优点是它提供基于进程对进程的(而不是主机对主机的)

安全服务。这一成就如果再加上应用级的安全服务，就可以再向前跨越一大步了。

三、应用层的安全性

必须牢记(且须仔细品味)：网络层(传输层)的安全协议允许为主机(进程)之间的数据通道增加安全属性。本质上，这意味着真正的(或许再加上机密的)数据通道还是建立在主机(或进程)之间，但却不可能区分在同一通道上传输的一个具体文件的安全性要求。比如说，如果一个主机与另一个主机之间建立起一条安全的 IP 通道，那么所有在这条通道上传输的 IP 包就都要自动地被加密。同样，如果一个进程和另一个进程之间通过传输层安全协议建立起了一条安全的数据通道，那么两个进程间传输的所有消息就都要自动地被加密。

如果确实想要区分一个具体文件的不同的安全性要求，那就必须借助于应用层的安全性。提供应用层的安全服务实际上是最灵活的处理单个文件安全性的手段。例如一个电子邮件系统可能需要对要发出的信件的个别段落实施数据签名。较低层的协议提供的安全功能一般不会知道任何要发出的信件的段落结构，从而不可能知道该对哪一部分进行签名。只有应用层是唯一能够提供这种安全服务的层次。

一般来说，在应用层提供安全服务有几种可能的做法，第一个想到的做法大概就是对每个应用(及应用协议)分别进行修改。一些重要的 TCP/IP 应用已经这样做了。在 RFC1421 至 1424 中，IETF 规定了私用强化邮件(PEM)来为基于 SMTP 的电子邮件系统提供安全服务。由于种种理由，Internet 业界采纳 PEM 的步子还是太慢，一个主要的原因是 PEM 依赖于一个既存的、完全可操作的 PKI(公钥基础结构)。PEMPKI 是按层次组织的，由下述三个层次构成：

顶层为 Internet 安全政策登记机构(IPRA)

次层为安全政策证书颁发机构(PCA)

底层为证书颁发机构(CA)

建立一个符合 PEM 规范的 PKI 也是一个政治性的过程，因为它需要多方在一个共同点上达成信任。不幸的是，历史表明，政治性的过程总是需要时间的，作为一个中间步骤，PhilZimmermann 开发了一个软件包，叫做 PGP(prettyGoodPrivacy)。PGP 符合 PEM 的绝大多数规范，但不必要求 PKI 的存在。相反，它采用了分布式的信任模型，即由每个用户自己决定该信任哪些其他用户。因此，PGP 不是去推广一个全局的 PKI，而是让用户自己建立自己的信任之网。这就立刻产生一个问题，就是分布式的信任模型下，密钥废

除了怎么办。

S-HTTP 是 Web 上使用的超文本传输协议(HTTP)的安全增强版本，由企业集成技术公司设计。S-HTTP 提供了文件级的安全机制，因此每个文件都可以被设成私人/签字状态。用作加密及签名的算法可以由参与通信的收发双方协商。S-HTTP 提供了对多种单向散列(Hash)函数的支持，如:MD2，MD5 及 SHA;对多种单钥体制的支持，如：DES，三元 DES，RC2，RC4，以及 CDMF;对数字签名体制的支持，如:RSA 和 DSS。

目前还没有 Web 安全性的公认标准。这样的标准只能由 WWWConsortium，IETF 或其他有关的标准化组织来制定。而正式的标准化过程是漫长的，可能要拖上好几年，直到所有的标准化组织都充分认识到 Web 安全的重要性。S-HTTP 和 SSL 是从不同角度提供 Web 的安全性的。S-HTTP 对单个文件作“私人/签字”之区分，而 SSL 则把参与通信的相应进程之间的数据通道按“私用”和“已认证”进行监管。Terisa 公司的 SecureWeb 工具软件包可以用来为任何 Web 应用提供安全功能。该工具软件包提供有 RSA 数据安全公司的加密算法库，并提供对 SSL 和 S-HTTP 的全面支持。

另一个重要的应用是电子商务，尤其是信用卡交易。为使 Internet 上的信用卡交易安全起见，

MasterCard 公司(同 IBM,Netscape,GTE 和 Cybercash 一道)制定了安全电子付费协议(SEPP)，Visa 国际公司和微软(和其他一些公司一道)制定了安全交易技术(STT)协议。同时，MasterCard，Visa 国际和微软已经同意联手推出 Internet 上的安全信用卡交易服务。他们发布了相应的安全电子交易(SET)协议，其中规定了信用卡持卡人用其信用卡通过 Internet 进行付费的方法。这套机制的后台有一个证书颁发的基础结构，提供对 X509 证书的支持。

上面提到的所有这些加安全功能的应用都会面临一个主要的问题，就是每个这样的应用都要单独进行相应的修改。因此，如果能有一个统一的修改手段，那就好多了。通往这个方向的一个步骤就是赫尔辛基大学的 TatuYloenen 开发的安全 shell(SSH)。SSH 允许其用户安全地登录到远程主机上，执行命令，传输文件。它实现了一个密钥交换协议，以及主机及客户端认证协议。SSH 有当今流行的多种 Unix 系统平台上的免费版本，也有由 DataFellows 公司包装上市的商品化版本。

把 SSH 的思路再往前推进一步，就到了认证和密钥分配系统。本质上，认证和密钥分配系统提供的是一个应用编程界面(API)，它可以用来为任何网络应

用程序提供安全服务，例如:认证、数据机密性和完整性、访问控制以及非否认服务。目前已经有一些实用的认证和密钥分配系统，如:MIT 的 Kerberos(V4 与 V5)，IBM 的 CryptoKnight 和 Netwrok Security Program，DEC 的 SPX，Karl sruhe 大学的指数安全系统(TESS)等，都是得到广泛采用的实例。甚至可以见到对有些认证和密钥分配系统的修改和扩充。例如，SESAME 和 OSFDCE 对 KerberosV5 作了增加访问控制服务的扩充，Yaksha 对 KerberosV5 作了增加非否认服务的扩充。

关于认证和密钥分配系统的一个经常遇到的问题是关于它们在 Internet 上所受到的冷遇。一个原因是它仍要求对应用本身做出改动。考虑到这一点，对一个认证和密钥分配系统来说，提供一个标准化的安全 API 就显得格外重要。能做到这一点，开发人员就不必再为增加很少的安全功能而对整个应用程序大动手术了。因此，认证系统设计领域内最主要的进展之一就是制定了标准化的安全 API，即通用安全服务 API(GSS-API)。GSS-API(v1 及 v2)对于一个非安全专家的编程人员来说可能仍显得过于技术化了些，但德州 Austin 大学的研究者们开发的安全网络编程(SNP)，把界面做到了比 GSS-API 更高的层次，使同

网络安全性有关的编程更加方便了。

局域网在网络层有什么不安全的地方

不安全的地方

由于局域网中采用广播方式，因此，若在某个广播域中可以侦听到所有的信息包，黑客就对可以对信息包进行分析，那么本广播域的信息传递都会暴露在黑客面前。

网络分段

网络分段是保证安全的一项重要措施，同时也是一项基本措施，其指导思想在于将非法用户与网络资源相互隔离，从而达到限制用户非法访问的目的。

网络分段可分为物理分段和逻辑分段两种方式：

物理分段通常是指将网络从物理层和数据链路层（ISO/OSI 模型中的第一层和第二层）上分为若干网段，各网段相互之间无法进行直接通讯。目前，许多交换机都有一定的访问控制能力，可实现对网络的物理分段。逻辑分段则是指将整个系统在网络层（ISO/OSI 模型中的第三层）上进行分段。例如，对于 TCP/IP 网络，可把网络分成若干 IP 子网，各子网间必须通过路由器、路由交换机、网关或防火墙等设备进行连接，利用这些中间设备（含软件、硬件）的安全机制来控制各子网间的访问。在实际应用过程

中，通常采取物理分段与逻辑分段相结合的方法来实现对网络系统的安全性控制。

VLAN 的实现

虚拟网技术主要基于近年发展的局域网交换技术(ATM 和以太网交换)。交换技术将传统的基于广播的局域网技术发展为面向连接的技术。因此，网管系统有能力限制局域网通讯的范围而无需通过开销很大的路由器。

以太网从本质上基于广播机制，但应用了交换器和 VLAN 技术后，实际上转变为点到点通讯，除非设置了监听口，信息交换也不会存在监听和插入（改变）问题。

由以上运行机制带来的网络安全的好处是显而易见的：

信息只到达应该到达的地点。因此、防止了大部分基于网络监听的入侵手段。通过虚拟网设置的访问控制，使在虚拟网外的网络节点不能直接访问虚拟网内节点。

但是，虚拟网技术也带来了新的安全问题：

执行虚拟网交换的设备越来越复杂，从而成为被攻击的对象。基于网络广播原理的入侵监控技术在高速交换网络内需要特殊的设置。基于 MAC 的 VLAN 不

能防止 MAC 欺骗攻击。

采用基于 MAC 的 VLAN 划分将面临假冒 MAC 地址的攻击。因此，VLAN 的划分最好基于交换机端口。但这要求整个网络桌面使用交换端口或每个交换端口所在的网段机器均属于相同的 VLAN。

VLAN 之间的划分原则

VLAN 的划分方式的目的是保证系统的安全性。因此，可以按照系统的安全性来划分 VLAN;可以将总部中的服务器系统单独划作一个 VLAN,如数据库服务器、电子邮件服务器等。也可以按照机构的设置来划分 VLAN，如将领导所在的网络单独作为一个 LeaderVLAN(LVLAN),其他司局（或下级机构）分别作为一个VLAN,并且控制LVLAN与其他VLAN之间的单向信息流向，即允许 LVLAN 查看其他 VLAN 的相关信息，其他 VLAN 不能访问 LVLAN 的信息。VLAN 之内的连接采用交换实现，VLAN 与 VLAN 之间采用路由实现。由于路由控制的能力有限,不能实现 LVLAN 与其他 VLAN 之间的单向信息流动，需要在 LVLAN 与其他 VLAN 之间设置一个 Gauntlet 防火墙作为安全隔离设备，控制 VLAN 与 VLAN 之间的信息交流。

win2ksrvoradv 单网卡实现

以前试过 n 次都失败了，于是就认为 win2k 无法

实现单网卡构架vpn+nat代理服务器今天搞了半天才搞出来了，原来没有问题的完全可能实现的

过程如下：

启用路由与远程访问，使用默认配置配置路由与远程访问这时候路由与远程访问中已经设置好了 vpn 服务器及路由器需要做的就是设置 nat 服务在 ip 路由选择中右键点击常规，然后添加新的路由选择协议

选择 nat 协议

然后在nat中添加新接口，如果是单块网卡的话，且你没有猫，isdn 之类的东西，也没有创建什么什么拨号接口的话，只有一个本地连接可以添加，也没有创建什么什么拨号接口的话，只有一个本地连接可以添加将本地连接添加上，并且将其设置为公用接口连接至 internet，加上转换 tcp/udp 报头显然 nat 只有一个接口是不能工作的，另一个接口就应该加上 vpn 的那个接口了vpn服务器的那个接口就是那个名称为“内部”的接口，如果没有人任何人联接过你的 vpn 服务器的话，这个接口不显示 ip 的，一旦有人连接过，这个接口就会得到一个 ip，具体 ip 是多少要看你怎么设置的 vpn 服务器。在 win2k 中是无法将此接口添加到 nat 中的，而在 winxp 中是可以的其实呢，在 win2k 中也是可以添加此接口的，因为这也是个接

口，没有理由无法添加的只不过 win2k 还留下了一点点小 bug。要想添加此接口，要用到命令行工具 netshexe。

运行 netshexe 后出现以下提示符

netsh>

然后按顺序输入以下命令即可

setmachine 你的机器名

routing ip nat addinterfacename=“内部” mode=private

然后就万事大吉了，注意不同语言版本的操作系统，接口名称不一样的另外有些情况下，添加了 nat 会默认的给你加上内部接口但无论如何，在 nat 里面，你怎么也不会看到这个内部接口，而在 winxp 中就能看到好了，这样就可以工作了，其他有关的配置我就不讲了。

重装了五次有三个网卡 win2kadv 系统才搞定了，最后还发现根本没有必要弄三个网卡，真是大分特啊。

另外,netshexe 是个好东东，网络管理基本上全搞定了，如在网卡多绑定个地址啊，删除个地址啊，设置 dns 服务器啊，设置路由啊，设置远程访问啊，设置过滤器啊全可以，有兴趣的人好好研究一下吧。

然后就万事大吉了，注意不同语言版本的操作系统，接口名称不一样的另外有些情况下，添加了 nat 会默认的给你加上内部接口但无论如何，在 nat 里面，你怎么也不会看到这个内部接口，而在 winxp 中就能看到好了，这样就可以工作了。

局域网

局域网（LocalAreaNetwork）是区别于广域网（WideAreaNetwork）的一种地理范围有限各种设备互连在一起的计算机网络。

一、局域网的特点：

1．局域网络是包含低三层功能的通信网络。

2．连接到局域网的数据通信设备是广义的，包括计算机、终端、各种外设等。

3．其覆盖的地理范围可以是一个建筑物、一个校园或者大至几十公里直径的区域。

二、局域网的典型特性

1．高数据速率（0．1~100Mbps）

2．短距离（0．1—25km）

3．低误码率（10-8~10-11）

三、局域网分类

1．局域网 LAN，是最普遍的一种局域网

2．计算机交换机（CBX 或 PABX），这是采用线路

交换的局域网

四、局域网主要技术

1．传输媒体。

2．拓朴结构。

3、媒体访问控制方法（MAC）。

其中最重要是媒体访问控制方法，它对网络特性起着十分重要的作用。将传输媒体的频带有效地分配给网上各站点的方法，称为媒体访问控制协议。

在 LAN 和 WAN 之间是城市区域网 MAN（MetropolitanAreaNetwork），MAN 是一个覆盖整个城市的网络，但它使用 LAN 的技术。针对这一目标在 IEEE8036 中定义了一种分布式队列双总线 DQDB 的标准（DistributedQueueDualBus）。

局域网的选择

在描述不同类型 LAN 的结构和操作之前，首先要了解选择 LAN 必须考虑的有关课题，

这些课题的有关内容可用关系图概括。下面将详细讨论各个课题。

一、局域网的拓扑

局域网常用的拓扑有三种，星型、环型和总线／树型，有关网络拓朴的概念已在第一章中作了介绍，本节针对局域网的拓扑适用范围作一些说明。

星型拓扑局域网的典型实例就是计算机交换机CBX。

环型拓扑局域网的典型实例便是光纤分布数据接口 FDD1。

总线／树型拓扑是用来实现 LAN 的最通用的拓扑，并且在 LAN 中使用两种传输技术：基带和宽带。采用数字信号传输的基带，可以使用双绞线或同轴电缆。采用无线电频率范围内的模拟信号传输的宽带，使用同轴电缆。

二、传输媒体

本节着重说明局域网中适宜的传输媒体

1．基带系统

使用数字信号传输的 LAN 定义为基带 LAN，数字信号以曼彻斯特编码的电压脉冲形式加到链路上，媒体的整个频谱用于构成信号，因此，不能采用频分多路复用 FDM 传输，其传输是双向的，媒体上任意一点加入的信号沿两个方向传输到其端点，在那里被吸收。

数字信号传输要求用总线形拓扑，数字信号不易传过树型拓朴所要求的分裂器和连接器。基带系统只能延伸有限的距离，最多约一公里，这是由于信号的衰减引起脉冲模糊和信号减弱以致无法实现更大距

离上的通信。

基带总线 LAN 的常见形式采用同轴电缆，大部分是用特殊的 50Ω电缆，而不是标准的 CATV75Ω电缆，这是因为对于数字信号，，50Ω电缆受到来自接头插入容抗的反射不那么强，而且对低频电磁噪声有较好的抗干扰性。

最简单的基带同轴电缆 LAN 是由一段无分支的同轴电缆构成，两端接有防反射的端接器（是一个终端阻抗器），推荐的最大长度为 500 米。站点通过接头接入主电缆，任何两接头间的距离为 25 米的整数倍，这是为了保证来自相邻接头的反射在相位上不致于叠加，推荐的最多接头数目为 100 个。每个接头包括一个收发机，它含有发送和接收用的电子线路。

为了延伸网络的长度，可以采用转发器。转发器由组合在一起的两个收发机组成，连到不同的两段同轴电缆上。转发器在两段电缆间，向两个方向传送数字信号，在信号通过时，将信号放大和复原。因而，转发器对于系统的其余部分来说是透明的。由于它不做缓冲存储操作，所以并没有将这一段与另一段隔开，因此如果不同段上的两个站同时发送的话，它们的分组将互相干扰（冲突）。为了避免多路径的干扰，在任何两个站之间只允许有一条包含分段和转发器

的路径。802 标准中，在任何两个站之间的路径中最多只允许四个转发器，这就将有效的电缆长度延伸到25km。

双绞线基带LAN用于低成本、低性能要求的场合，安装容易，往往限制在 1km 的长度以内，数据速率为1Mbps～10Mbps。用超五类双绞线可达 100Mbps。

2．宽带系统

在 LAN 范围内，宽带是指采用模拟信号技术。因而可用频分多路复用 FDM 传输技术，即

把电缆的频道分成多个信道或频段，这些模拟载波信号工作在高频范围（通常为 10～400MHz）。宽带系统可以采用总线和树型拓扑结构，可以达到比基带大得多的传输距离（达几十公里），这是因为携带数字数据的模拟信号，在噪声和衰减损害数据之前，可以传播较长的距离。

宽带同基带一样，系统中的站点是通过接头接入电缆。然而，与基带不同的是宽带本质上是一种单方向的媒体，加到媒体上的信号只能沿一个方向传播。这是因为要制作能在两个方向上传递同一频率信号的放大器是不可能的。这种单向性质，意味着只有在发送站的“下游”的那些站才可以收到它的信号。

由此可见，需有两条数据路径，这些路径在网络

的端头处接在一起。对于总线拓扑，端头就是总线的一端；对于树形拓扑，端头是有分枝的树根。所有站沿一条路径（入径）向端头传输，在端头接收到的信号，沿另一条数据路径（出径）离开端头传输，所有的站在出径上接收。物理上，可用两种不同的构造来实现输入和输出的通路。

在双电缆构造中，入径和出径是分开的电缆，而端头只是两者问的一个无源连接装置。每个站以相同的频率发送和接收。

在分叉构造中，入径和出径是同一电缆上的不同频率。双向放大器传送较低频率的人径和较高频率的出径。端头包含一种称为频率转换器的装置，将入径频率转换为出径频率。端头上的频率转换器可以是模拟或数字装置。模拟装置只要把信号转换成一个新的频率并重发。数字装置则在端头恢复数字数据，然后在新的频率上重发净化了的数据。有一种“中分”(midsplit)系统，在 300MHz 的频谱中，将 5 到 116MHz 作为入径，而 168 到 300MHz 作为出径。

三、媒体访问控制方法

当两个站点经过星型网建立信道时，由交换机确保这两个端点在呼叫期间专用该传输信道。而在环型或总线型拓扑中，只有一条物理传输通道连接所有的

设备。因此，连到网络的所有设备必须遵循一定的规则，才能确保传输媒体的访问和使用。常用的媒体访问控制方法有：具有冲突检测的载波监听多路访问（CSMA／CD）、控制令牌（ControlToken）以及时槽环（SloitedRing）三种技术。

1、具有冲突检测的载波监听多路访问

具有冲突检测的载波监听多路访问（CSMA／CD）技术只用于总线型网络拓朴结构，这种结构将所有的设备都直接连到同一条物理信道上，该信道负责任何两个设备之间的全部数据传送。因此称信道是以多路访问方式进行操作的。站点以帧的形式发送数据，帧的头部含有目的地和源点的地址，帧通过信道的传输是广播传输。所有连接在信道上的设备随时都能检测到该帧。当目地站点检测到目的地址为本站地址的帧时，就继续阅读帧中包含的数据，并按定义的链路协议给源站点返回一个响应。用这种操作方法，在信道上可能有两个或更多的设备在同一瞬间都发送帧，从而在信道上造成帧的重叠，而出现差错，这种现象称为冲突。

为减少这种冲突，源站点在发送帧之前，首先监听信道是否忙，如监听到信道上有载波信号，则推迟发送，直到信道恢复到安静（空闲）为止。这种方法

称为载波监听多路访问（CSMA）。对于传播时延远小于传输时延的网络，CSMA 能降低冲突次数，并减少冲突时间；而对于传播时延远大于传输时延的网络，CSMA 就变得毫无价值，此外，还要采用边发送边监听的技术，因为监听到干扰信号，就表示检测到冲突，于是就立即停止发送。为了确保冲突的其它站点知道发生了冲突，首先在短时间里坚持连续发送一串阻塞（Jam）码，卷入冲突的站点则继续等待一随机时间，然后准备重发受到冲突影响的帧，这种具有冲突检测的 CSMA 称为 CSMA／CD 技术，它对发生冲突的传输能迅速发现并立即停止发送，因此能明显减少冲突次数和冲突时间。有关 CSMA／CD 技术的具体实现在 6．4 节中将会详细讨论。

2．控制令牌

控制令牌是另一种传输媒体访问控制方法。它是按照所有站点共同理解和遵守的规则，可以从一个站点到另一个站点传递控制令牌，一个站点只有当它占有令牌时，才能发送数据帧，发完帧之后，即把令牌传递给下一个站点，其操作次序如下：

首先建立逻辑环，将所有站点同物理媒体相连，然后产生一个控制令牌。

令牌由一个站点沿逻辑环传递到另一个站点，直

到等待发送帧的那个站点接收。

该站点把要发送的帧利用物理媒体发送出去，然后将控制令牌沿逻辑环传递给下一站点。

控制令牌方法除了用于环型网拓扑结构之外，也可以用于总线网拓扑结构，这两类结构建立的逻辑环，对于一个物理环（见图 66（a)），令牌传递的逻辑结构和物理环的结构是相同的，令牌传递的次序和站点连接的物理次序也是一致的。然而对于图 66（b）所示的总线网，逻辑环次序则不必和电缆上的站点连接次序相对应。并且，对于总线网上的令牌访问方法，所有站点没有必要均按逻辑环连接。

3．时槽环

时糟环只用于环形网的控制访问。这种方法首先由环中被称为监控站的特定节点起动环，并产生一个固定位数的二进制数字比特串。这个比特串不停地绕环从一个站点到另一个站点传递。当一个站点收到这一串二进制数时，由站点的接口阅读，并将其传送到环的下一个站点，如此循环下去。监控站确保总有一个固定的比特数绕环传送，而不考虑组成环的站点数目。整个环配置有若干个固定的时槽数，每个时槽由一串比特组成，并且能携带一个固定尺寸的信息帧。时槽帧的格式。

起始时，由监控站将每个时槽开头的满／空（Full／Empty）位置于空状态。当某个站点想要发送帧时，首先等待，直至监测到一个空时槽后，将时槽置为满，并将帧的内容插入时槽中，同时在帧的头部插入目的地址和源地址，并将帧尾部的两个响应位全置为 1，然后发送该时槽帧，使它绕物理环从一个站点至下一个站点传送。环中每个站对任何置满的时槽头部的目的地址进行检测，如果检测到是自己的地址，则认为该时槽的帧是要接受的帧，它就从时槽中阅读该帧数据内容，同时通过环将它转发。阅读该帧内容后，修改时槽尾部的一对响应位，表明它已读过该帧。如果目的地站点忙或者拒收，则响应位作相应的标记，或保留不作改变。源站点在起动一个帧发送之后，要等到该帧绕环一周，由于每个站均知道环上时槽总数，由环接口对时槽转发计数可知道所发帧的到来。之后，源站点一收到发送该帧所用时槽的第一个比特时，它就重新标记该时槽为空，并等待阅读时槽尾部的响应位，以确定是否应舍弃已被发送的该帧拷贝，或者重发该帧。由于采用了响应位，就不需要独立的响应帧。

监控站传递位是由监控站用来监测各个站点发送的帧是否有差错或站点有无故障。该位由源站点在

发送帧时置“0”。当满时槽在环接口上转发时，由监控站对每一•个满时槽的该位（M）置“1”。如果监控站往其转发某个满时槽时，测得监控站传递位（M）已被置为 1，就认为源站点有故障，就将该帧的满／空位置为空，并释放时槽。监控站把经过它的帧拷贝保留下来，如果同一个帧多次经过，它就认为该帧有错，监控站就删除该帧，重新产生一个新的空时槽。时槽尾部的两个控制位是提供给 DTE 高层协议使用的，在媒体访间控制层没有意义。

需特别指出，对于时槽环媒体访问方法，每个站点每次只能传送一个帧，并在想要传送另一个帧之前，首先必须释放传输前一帧所有的时槽。由此可见，对环的访问体现出公平性，并被各个互连的站点所共享。

时槽环的主要缺点如下：

（1）为保持基本环结构而需要一个特定的监控站节点。

（2）一个完整的链路层帧通常需要多个时槽传送，因为每个时槽只能携带 16 位有用数据，而总长 40 位，故开销大，效率较低。

（3）在绕环一周时间内，每站只能发一帧信息，如只有上一个站点有多帧信息要发送，则许多时糟是

空循环。

时槽环的主要优点是结构简单，节点间相互干扰少、可靠性高。

对于前面所述的令牌环，一旦某个站点得到控制令牌，就可以把包括多个字节的信息帧作为一个整体进行发送，所以效率较高。

四、IEEE802 系列标准和 ISO8802 系列标准

局域网 LAN 最初开始发展时，提出了许多不同类型的网络产品，但这些网络产品一般只能用于特定厂商的计算机或工作站之间的互连，称这类 LAN 为闭合系统。为了改变这种情况，一些国家的标准化组织制定了一组能被共同接受的 LAN 标准。首先由 IEEE 制定了 IEEE802 系列标准。现已被 ISO 采纳，作为国际标准 ISO8802 系列标准。在这些标准中，根据 LAN 的多种类型，规定了各自的拓扑结构、媒体访问控制方法、帧的格式和操作。

局域网络参考模型

我们已介绍了局域网的协议结构和局域网和城市区域网的参考模型（L&MAN／RM），以及与 OSI 提出的参考模型 OSI／RM 的关系。IEEE802 标准包括了 OSI／RM 最低两层（物理层和链路层）的功能，也包括网间互连的高层功能和管理功能。还有一种实现模型

L&MAN／IM 与参考模型（L&MAN／RM）是有区别的，它比参考模型更特殊，它允许实现方法上有差别。

一、服务访问点 SAP

在参考模型中，每个实体和另一系统的同等实体按协议进行通信。在一个系统中，上下层之间则通过接口进行通信，用服务访问点 SAP 来定义接口。

为了对多个高层实体提供支持，在 LLC 层的顶部有多个 LLC 服务访问点（LSAP），为图中的实体 A 和 B 提供接口端。在网络层的顶部有多个网间服务访问点（NSAP），为实体 C、D 和 E 提供接口端。媒体访问控制服务访问点（MSAP）向 LLC 实体提供单个接口端。物理服务访问点（PSAP）向 MAC 实体提供单个接口端。

二、逻辑链路控制 LLC 子层

IEEE802 规定两种类型的链路服务：

1、无连接 LLC（类型 l）。

2、面向连接 LLC（类型 2）；

在类型 1 的操作中，是一种数据报服务，信息帧在 LLC 实体间交换，无需在同等层实体间事先建立逻辑链路，对这种 LLC 帧既不确认，也无任何流量控制或差错恢复。支持点对点、多点和广播式通信。

在类型 2 的操作中，提供服务访问点之间的虚电路服务，在任何信息帧交换前，在一对 LLC 实体间必

须建立逻辑链路，在数据传送过程中，信息帧依次发送，并提供差错恢复和流量控制功能。

三、媒体访问控制 MAC 子层

MAC 子层在支持 LLC 子层中完成媒体访问控制功能，可以提供多个可供选择的媒体访问控制方式。在使用 MSAP 支持 LLC 子层时，MAC 子层实现帧的寻址和识别。MAC 到 MAC 的操作通过同等层协议来进行，MAC 还产生帧检验序列和完成帧检验等功能。

逻辑键路控制协议

IEEE8022 是在 IEEE802 系列协议中描述逻辑链路控制（LLC）子层的功能、特性和协议，描述 LLC 子层与网络层、MAC 子层及 LLC 子层管理功能的界面服务规范。它提供了同等层协议的描述，这些协议是为了在 LAN 上任何数据链路层服务访问点对之间信息的传输而定义的。LLC 协议与具体的局域网所采用的某个媒体访问控制方法类型是无关的。

IEEE8022 对 LLC 子层规定了三个界面的服务规范：

1）网络层／LLC 子层界面服务规范，用于描述从网络层看，LLC 子层和其下各层提供的服务。

2）LLC／LLC 子层界面服务规范，描述提供给 LLC 子层的管理服务。

3）LLC／MAC 子层管理功能的界面服务规范，用于描述 LLC 子层对 MAC 子层所要求的服务。

以下对上述三种界面的服务规范进行进一步说明。

一、网络层／LLC 子层界面服务规范

在这一界面服务规范中提供了两种服务方式：

1）无确认无连接方式服务：它是在不建立数据链路级连接的方式下提供网络层实体交换链路服务数据单元（LSDU）的手段。这是一种数据报服务，支持点一点，多点式或广播式数据传输。

2）面向连接方式服务：它提供了建立、使用、复位以及终止数据链路层连接的手段，这些连接是通过 LLC 服务访问点之间的点点式连接，并提供数据链路层的定序、流控和差错恢复。这是一种虚电路服务。

对应于 LLC 子层的两种服务类型，LLC 定义了两种操作：Ⅰ型操作：在该类操作中，在 LLC 之间交换 PDU 时不需建立数据链路连接，PDU 不需确认，也没有流控和差错恢复。Ⅱ型操作：在 LLC 之间交换 PDU 之前，必须建立数据链路连接。正常通信包括从源 LLC 到目的 LLC 发送带有信息的 PDU，和相反方向 PDU 的确认；前述定义的 LLC1 类仅支持Ⅰ型操作，LLC2 类既支持Ⅰ型操作，也支持Ⅱ型操作。

二、LLC 子层／MAC 子层界面服务规范

这一个界面服务规范说明了逻辑链路控制（LLC）子层对媒体访问控制（MAC）子层的服务要求，以便本地 LLC 子层实体与对等层 LLC 子层实体交换 LLC 数据单元。

LLC 子层／LLC 子层管理功能的界面服务规范有待进一步研究解决。

三、LLC 协议数据单元 PDU 的结构

IEEE802 标准中所采用的帧格式类似于大多数专用网络中采用的格式。而 LLC 层采用单独格式的帧，然后嵌入相应的 MAC 帧中。

DSAP 地址字段包含一个字节，其中七位实际地址，一位为地址类型标志，用来标识 DSAP 地址为单个地址或组地址，SSAP 地址字段也包含一个字节，其中七位实际地址，一位为命令／响应标志位，用来识别 LLCPDU 是命令或响应。定义 DSAP 字段中全“1”是全局地址，由 MAC 服务访问地址所实际服务的全部 DSAP 组成，定义 DSAP 或 SSAP 地址字段中全“0”为空地址。该空服务访问点地址表示与 MAC 服务访问点地址有关的 LLC，不识别网络层的任何服务访问点或有关层管理的任何服务访问点。

但有一点需指出：地址信息在 LLC 和 MAC 帧中是

分开的，这是因为为了把数据传送到所连结的站用源和目的地址指出这是 MAC 的功能。而源或目的服务访问点只需在 LLC 层知道就行了。

LLCPDU 中的控制字段是效仿 HDLC 平衡模式制定的，具有相似的格式和功能。图 610 表示了 LLCPDU 控制字段的格式。定义了三种格式：用来完成带编号的信息帧传输、带编号的监视帧的传输和无编号的控制和无编号信息帧传输。

带编号的信息传输帧（I 一格式 PDU）用来在连接方式下发送数据。N（s）、N（R）是帧序列号用以支持流控和差错控制。站发送帧时都按模 128 编号，并将编号值置于 N（S）中，N（R）是向发送站指示希望下一次接收的帧的编号，也以模 128 编号，并以捎带的方式作回答响应，P/F 置 1 用以指示探询和发送终止。

监视帧用来作响应和流控，SS 域用以指示三个命令：接收准备好（RR）、接收未准备好（RNR）和拒收（REJ）。RR 帧在 N（R）中指示希望下一次接收的帧的编号，用在无反向通信捎带响应的场合。RNR 与 RR 一样作为响应，同时还要求发送站立即终上发送。REJ 用以指示编号为 N（R）帧被拒收，必须重新发送。带编号的监视帧只能用于 II 型操作。

无编号帧（U 一格式 PDU）用于无编号信号传输和控制信号传输。

第一类 LLC 和第二类 LLC 及 I 型操作和 II 型操作所支持的命令和响应 PDU 见表 6．2 所示。

CSMA／CD 媒体访问控制

CSMA／CD 是用争用的方法来决定对媒体的访问权。而这种争用协议一般用于总线网。在总线系统中，每个站都能独立地决定帧的发送，如两个或多个站同时发送，就会产生冲突，同时发送的所有帧都会出错。因此一个用户发送信息成功与否在很大程度上取决于总线是否空闲的算法以及当两个不同节点同时发送的分组发生冲突时所使用和中断传输的方法，总线争用技术可分为载波监听多路访问和具有冲突检测的载波监听多路访问这两大类。

一、载波监听多路访问（CSMA）

载波监听多路访问（CSMA）的技术，也叫做先听后说（LBT），希望传输的站首先对媒体进行监听以确定是否有别的站在传输。如果媒体空闲，该站可以传输，否则，该站将避让一段时间后再尝试。需要有一种退避算法来决定退让时间。常用的有三种算法。

1、非坚持 CSMA

1）如果媒体是空闲的，则可以发送。

2）如果媒体是忙的，则等待由概率分布决定的、一定量的重发延迟时间，然后重复步骤 1。

采用随机的重发延迟时间可以减少冲突的可能性。其缺点是：即使有几个站有数据要发送，媒体仍然可能处于空闲状态，媒体的利用率较低。

坚持协议。

1）如果媒体是空闲的则可以发送。

2）如果媒体是忙的，则继续监听，直至检测到媒体空闲，立即发送。

3）如果有冲突（在一段时间内未收到肯定的回复），则等待一随机量的时间，重复步骤 1。

这种方法的优点是：只要媒体空闲，站点就立即发送，其缺点：假如有两个或两以上的站点有数据要发送，冲突就不可避免。

试图又能象非坚持算法那样减少冲突而又能象 1一坚持算法那样减少媒体空闲的时间的一种折中方案是：

P 一坚持协议

1）监听总线，如果媒体是空闲的，则以 P 的概率发送，而以（1 一 p）的概率延迟一个时间单位。时间单位通常等于最大的传播延迟的 2 倍。

2）如果媒体是忙的，继续监听直至媒体空闲并

重复步骤 1。

3)如果传输延迟了一个时间单位,则重复步骤 1。

问题在于如何选择P的有效值？需考虑的主要因素是想避免重负载下系统处于的不稳定状态。假如媒体忙时，有 N 个站有数据等待发送，一旦当前的发送完成时，将要试图传输的站的期望数为 NP。如果选择 P 过大，使 NP＞1，表明有多个站试图发送，冲突就不可避免。最坏的情况是,随着冲突概率的不断增大，而使吞吐率降到 0。所以必须选择 P 值使 NP＜1。当然 P 值选得过小，则媒体利用率会大大降低。

二、载波监听多路访问／冲突检测(CSMA/CD)

在 CSMA 中，由于通道的传播延迟，当两个站点监听到总线上没有存在信号而发送帧时，仍会发生冲突。在传播延迟期间，站点 2 有帧发送，就会和站点 1 发送的帧冲突，由于 CSMA 算法没有冲突检测功能，即使冲突已发生，仍然要将已破坏的帧发送完，使总线的利用率降低。

一种 CSMA 的改进方案是使站点在传输时间继续监听媒体，一旦检测到冲突，就立即停止发送，并向总线上发一串阻塞信号，通知总线上各站冲突已发生，这样通道容量不致因白白传送已受损的帧而浪费，可以提高总线的利用率，这就称作载波监听多路

访问／冲突检测协议，简写为 CSMA／CD，这种协议已广泛应用于局域网中。

此时，浪费掉的带宽就减少为用检测冲突所花费的时间。那么，怎么来估算所需的冲突检测时间呢？对于基带总线而言，此时用于检测一个冲突的时间等于任意两个站之间最大的传播延迟的两倍，

对于宽带总线而言，冲突检测时间等于任意两个站之间最大传播延迟的四倍，

三、退避算法

在 CSMA／CD 算法中，一旦检测到冲突，并发完阻塞信号后，为了降低再冲突的概率，需要等待一个随机时间，然后再次使用 CSMA 方法试图传输。为了保证这种退避维持稳定，采用了一种称为二进制指数退避的技术，其算法的过程如下：

1）对每个帧，当第一次发生冲突时，设置参量 L=2。

2）退避间隔取 1 到 L 个时间片中的一个随机数。1 个时间片等于 2a。

3）当帧重复发生一次冲突，则将参量 L 加倍。

4）设置一个最大重传次数，超过这个次数，则不再重传；并报告出错。

这个算法是按后进先出的次序控制的，即未发生

冲突，或很少发生冲突的帧，具有优先发送的概率，而发生过多次冲突的帧，发送成功的概率反而小。Ethernet 网就是采用 CSMA／CD 算法，并用二进制指数退避和 1 一坚持算法。这种算法在低负荷时，如媒体空闲时，要发送帧的站点能立即发送。在重负荷时，仍能保证系统稳定。它是基带系统，采用曼彻斯特编码，通过检测总线上的信号存在与否来实现载波监听。发送站的收发器同时检测冲突，如果发生冲突，收发器的电缆上的信号超过收发器本身发送信号的幅度，就判断出冲突。由于在媒体上传播的信号会衰减，为了正确地检测出冲突信号，Ethernet 网限制电缆的最大长度为 500 米。

四、CSMA／CD 媒体访问控制协议

1．CSMA／CD 总线的实现模型

IEEE8023 是一个使用 CSMA／CD 媒体访问控制方法的 LAN 的综合性标准。CSMA／CD 总线的实现模型

从逻辑上可以划分为两大部分：数据链路层的媒体访问控制子层（MAC）和物理层。它严格对应于 ISO 开放系统互连模式的最低两层。LLC 子层和 MAC 子层在一起完成 OSI 模式的数据链路层的功能。

在物理层中把依赖于媒体的特性分离出来，使得 LLC 子层和 MAC 子层能适用于一系列媒体。在物理层

内定义了两个重要的兼容接口，即依赖于媒体的媒体相关接口 MDI 和访问单元接口 AUI。MDI 是一个同轴电缆接口，所有站都必须严格遵守 IEEE8023 定义的物理媒体信号的确切技术规范，严格遵守站点正确动作的规程，要求这个物理媒体接口完全兼容；AUI 为第二兼容接口，大多数站点都设在离开同轴电缆的连接处有一段距离的地方，在与同轴电缆靠近的 MAC 中只有少量电路，而大部分硬件和全部软件都在站点中，对于确保通信来说，符合这个接口并不是绝对必要的，但是由于它允许在 MAC 和站配合使用时有极大的灵活性，所以推荐这个接口。

MAC 子层和 LLC 子层之伺的接口，包括发送和接收帧的设施，并提供每个操作的状态信息，以供高一层差错恢复规程之用，MAC 子层和物理层之间的接口，包括成帧、载波监听、起动传输和解决争用（冲突控制）的信号，在两层间传送一对串行比特流（发送、接收）的设施和用于定时等待的功能。

2．MAC 的帧结构

MAC 帧是在 MAC 子层实体间交换的协议数据。

为：前导码、帧起始定界符、目的地址、源地址、表示信息字段长度的长度字段、要发送的以 LLC 数据、需要进行填充的字段和帧校验序列字段。这 8 个字段

除 LLC 数据和填充字段外，长度都是固定的。

前导码字段包含 7 个字节，它用于使 PLS（物理收发信号）电路和收到的帧达到稳态同步。帧起始定界符（SFD）字段是 10101011 序列，它紧跟在前导码后，表示一帧的开始。地址字段包括目的地址字段和源地址字段。目的地址字段规定该帧发往的目的地。源地址字段用于标识起始发送该帧的站。MAC 子层有两类地址：即单个地址和成组地址，单个地址说明该地址与网络上一个特定站有关，成组地址说明是多目的地的地址，它与给定网络上的一个或多个站有关。也可以是广播地址，即表示网络上所有站的一组地址。

长度字段是两个字节字段，其值表示数据字段中 LLC 数据的字节数量，数据字段包含数据序列，为了 CSMA／CD 协议的正常操作需要一个最小帧长度，必要时可在 LLC 数据字段之后，FCS 之前以字节为单位加以填充。帧校验序列（FCS）字段是发送和接收都要使用循环冗余校验码（CRC）算法所产生的 FCS 字段的 CRC 码，帧的长度为 64 个字节到 1518 字节之间。

3．MAC 子层的功能

IEEE8023 标准提供了 MAC 子层的功能说明，主要有数据封装和媒体访问管理两个方面。数据封装（发

送和接收数据封装）包括成帧（帧定界和帧同步）、编址（源地址及目的地址的处理）和差错检测等。媒体访问管理包括媒体分配和竞争处理。

（1）发送数据封装部分的功能

当 LLC 子层请求发送一帧时，MAC 子层的发送数据封装部分用 LLC 子层所提供的数据结构组帧，它将一个前导码 P 和一个帧起始定界符 SFD 附加到帧的开头部分，还将 PAD 附加到结尾部分，以确保传送帧的长度满足最小帧长的要求，它还要附加目的地址和源地址，长度计数字段和帧校验序列，然后把组成的帧交给 MAC 子层的发送媒体访问管理部分以供发送。

（2）发送媒体访问管理部分的功能

借助于监视物理层收发信号（PLS）部分提供的载波监听信号，发送媒体访问管理设法避免发送信号与媒体上其它信息发生冲突。在媒体空闲时，经短暂的帧间延迟（提供给媒体恢复时间）之后，就启动帧发送，然后，MAC 子层将串行位流送给 PLS 接口以供发送，PLS 完成产生媒体上电信号的任务。同时，监视媒体和产生冲突检测信号。在没有争用的情况下，即完成发送。完成发送后，MAC 子层通过 LLC 与 MAC 间的接口通知 LLC 子层，等待下一个发送请求。假如产生冲突，PLS 接通冲突检测信号，接着发送媒体访

问管理开始处理冲突。首先，它发送一个称为阻塞（Jam）的位序列来强制冲突，这就保证了有足够的冲突持续时间，以使其它与冲突有关的发送站都得到通知，在阻塞信号结束时，发送媒体访问管理就停止发送。

发送媒体访问管理在随机选择的时间间隔后再进行重发尝试，在重复的冲突面前反复进行重发尝试，发送媒体访问管理用二进制指数退避算法调整媒体负载。然后，或者重发成功，或者媒体故障或过载的情况下，放弃重发尝试。

（3）接收媒体访问管理部分的功能

首先由 PLS 检测到达帧，使接收与前导码同步，并接通载波监听信号。接收媒体访问管理部件要检测到达的帧是否错误，帧长是否超过最大长度，是否为 8 位的整倍数，还要过滤冲突的信号，即把小于最小长度的帧过滤掉。

（4）接收数据解封部分的功能

这一部分检验帧的目的地址字段，决定本站是否应该接收该帧，如地址符合，将送到 LLC 子层，并进行差错检验。

下面列出 1EEE8023MAC 协议的 10Mbps 实现方案的参数值。

参数数值：

SlotTime（时间片）512 比特时间

InterFrameGap（帧问间隔）9．6 微秒

attemptlimit（尝试极限）16

Backofflimit（退避极限）10

Jamsize（人为干扰长）32 比特

maxFramesize（最大帧长）1518 字节

minFramesize（最小帧长）512 字节

addresssize（地址字段长）48 比特

65 令牌环（TokenRing）媒体访问控制

IEEE8025 标准规定了令牌环的媒体访问控制子层和物理层所使用的协议数据单元格式和协议，规定了相邻实体间的服务，规定了连接令牌环物理媒体的方法。

一、令牌环工作原理

令牌环由一组用传输媒体串联成一个环的站组成。对媒体具有访问权的某个已知站将信息一个比特一个比特地附加到环上。在网上的信息将从一个站至下一个站地环行。所寻址的目的站在信息经过时拷贝此信息，最后由发送该信息的站从环上撤除此信息。这种媒体访问使用一个沿着环循环的令牌，当各站都没有帧发送，令牌的形式为 01111111，称空令牌。希

望发送帧的站必须等待，直到它检测到一个空令牌的到来，此时通过改变令牌的比特组合，将空令牌改为忙令牌，其形式为 01111110。该站紧接着忙令牌的后面，传输一个数据帧，由于在环上没有空令牌，因而其它希望发送数据帧的站必须等待，图 618 表示令牌环的工作原理。发送的帧沿环循环一周后再回到发送站，并被发送站将该帧从环上移去，同时忙令牌改为空令牌，传至后面的站，使之获得发送帧的许可权。

接收帧的过程是当帧经过站时，该站将帧的目的地址和本站的地址相比较，如地址相符合，则将帧放入接收缓冲器，再输入站，同时将帧送回至环上。如地址不符合，则将数据帧重新送入。

环的长度往往是折算成比特数来度量。环上每个中继器引入一位延时，把环看作一个循环缓冲器。环上的比特数等于传播延迟（5μs／km）×发送媒体长度×数据速率+中继器延迟。例如：lkm 长 1Mbps 速率、20 个站点，每个中继器引入 1 位延迟的环，其环的位长度＝5×10-6×1×1×106+1×2=5＋20=25 位。

令牌环的故障处理功能主要体现在对令牌和数据帧的维护。环上至关重要的差错是没有空令牌循环和持续的忙令牌，为解决这些问题，指定一个站为主动令牌管理站。该管理站通过采用一超时机制来检测

令牌丢失的情况，该超时值比最长的帧为完全遍历该环所需要的时间还要长一些。如果在这一段时间里没有检测到令牌，就认为令牌已经丢失。为恢复令牌，管理站将清除环上的任何残余数据并发出一个空令牌。

为了检测到一个持续循环的忙令牌，管理站在经过的任何一个忙令牌上置其管理比特为 1。如果管理站看到一个忙令牌的管理比特已经置为 1，它就知道有某个站未能清除自己发出的帧，管理站就将忙令牌改为空令牌。

环上其它的站都具有被动管理站的功能和作用，它们的主要工作是检测出主动管理站的故障并承担起主动管理站的职能。

二、令牌环帧格式

（1）令牌环有两个基本的格式：令牌和帧。在 IEEE8025 标准中，帧的传输是从最高位开始一位一位发送，而 IEEE8023 和 IEEE8024 正好相反，帧的传输是从最低位开始一位一位发送的，这一点对于不同协议的局域网互连时，要考虑进行转换。

（2）访问控制（AC）域格式

AC 字节的格式：

PTMR

P:指示令牌的优先级。

T：指示空令牌还是忙令牌

M：监视位

R：预约位，允许具有较高优先权的站申请下一个令牌。

三、令牌环媒体访问控制协议

1、令牌环的体系结构

令牌环局域网协议标准包括四个部分，即逻辑链路控制（LLC）、媒体访问控制（MAC）、物理层（PHY）和传输媒体。IEEE8025 规定了后面三个部分的标准。LLC 和 MAC 等效于 OSI 的第二层——数据链路层，PHY 相当于 OSI 的第一层——物理层。

2、媒体访问控制功能

1）帧发送：采用沿环传递令牌的方法来实现对媒体的访问控制。取得令牌的站具有发送一帧或一系列帧的机会。

2）令牌发送：在完成帧发送后，该站就要查看本站地址是否已在 SA 字段中返回，若未查看到，则该站就发送填充，否则就发送令牌。令牌发送之后，该站仍保持在发送状态，直到该站发送的所有的帧从环上移去为止。

3）帧接收：若帧的类型为 MAC 帧，如果帧的 DA

字段与站的单个地址、相关组地址或广播地址匹配，则把 FC、DA、SA、INFO 以及 FS 字段拷贝到接收缓冲区中，并随后转至适当的子层。

4）优先权操作：访问控制字段中的优先权位（PPP）和预约位（RRR）配合工作，使环路服务优先权与环上准备发送的 PDU 最高优先级匹配。

NOVELL 网络

NOVELL 公司开发的 NOVELLNetware 网络操作系统是一个可使 PC 机网络取代小型机系统的多任务网络操作系统，它以一流的性能和可靠性遥遥领先子其它局域网软件产品，开创了工作站/服务器的结构。在一个 NOVELL 网络中允许有多个文件服务器，每个服务器可适用于不同类型的网络接口卡（NIA）。Netware 适用于多种微机和 200 种左右的网络接口板，具有十分灵活的拓扑构，如总线型、星型、环型和混合型的拓扑结构，并可以和其它网络（如 3+网、TCP/IP）在同一网络下工作，Novell 网还提供了不同种类的网间连接器。Novell／Netware 由文件服务器软件、工作站软件、网桥软件、加值程序（VAP）以及帮助信息组成，其中文件服务器软件和工作站软件是建网不可缺少的软件，安装时需要根据硬件的配置生成。

由于 Novell／Netware 是直接对微处理器编程，因而它总是可以和最新的徽处理器一起发展，并能充分利用微处理器的高性能，形成高效的网络操作系统。

一、Netware 的核心结构

NovellNetware 是在局域网的基础上建立的网络操作系统，因此它不同于一般网络协议所需的完整的协议和通信传输功能，它具有所有操作系统的职能，如任务管理、缓冲区管理、文件管理、磁盘、打印机等外设管理，因而结构相当复杂。它是一个围绕核心调度的多用户共享资源的操作系统，它包括磁盘处理、打印机处理、控制台命令处理及网络通信处理等面向用户的处理程序和一个在多用户时的核心调度程序。

二、Netware 网络层次结构

如果将 Netware 和标准的网络层次模型作比较，其层次结构的相应关系。从物理层和数据链路层看，Netware 可支持多种网络接口卡，它包括 Novell 公司自己的各种网卡 3Com 公司及别的厂家的网卡。其中有基于总线的，也有基于令牌环的及支持星型网络的 ARCNET 网卡。

Novell 网不仅可以使用相同协议的网络接口板，

也能使用不同协议的网络接口板。对不同协议的网络接口板如何建立 Novell 网络呢？首先将使用相同协议的网络接口板分别连成网，然后将这几个网用网桥连接起来，形成更大的 Novell 网络。Novell 的网桥可用于完全不同的通信协议，在桥接网络上的用户可以跨桥访问另一网络的文件服务器，无需知道网络的具体配置和通信协议。Novell 的网桥可分为内桥、外桥和远程桥。

从网络层次结构的第三～七层来看，Netware 和标准网络协议有较大差别。因为 Netware 是一个基于服务器的网络操作系统，因而 Netware 的侧重点在于服务器的网络文件系统以及网络管理功能，这与以数据通信为主要目的的网络软件有很大区别。

三、Novell／Netware 的主要特点

1、Novell 网络为用户使用提供完善的安全措施

网络安全对用户是十分重要的，它包括用户口令、目录的权限、文件和目录的属性，以及对用户登录工作站点及时间的限制。此外，管理员对用户的帐户进行管理，被取消帐户的用户不能登录进网，用户使用共享盘中的目录时，由于各用户的身份不同，它们对目录的使用权限也不同，因此，对各用户要使用文件服务器的·目录就有个授权问题。此外，目录本

身也有个权限问题。Novell 网络为目录提供 8 种权限设置。这 8 种权限是读权、写权、打开权、创建权、删除权、授权权、列目权和修改权。一般来说，共享盘目录的创建和授权是由管理员用户执行的，这样有利于网络的统一管理和安全。一般用户在共享盘的自己目录中，可以创建子目录和给其它用户授权。

目录除了有权限还有属性。目录的属性有四种：正常、隐含、系统和专用，Novell 网对文件可以设置只可执行、只读、可读写、允许共享、不可共享、不可共享且可读写、隐文件、索引，上次备份后又已修改、系统文件和允许事务跟踪等属性。由此可见，Novell 网对目录和文件管理十分完善，确保了网络的安全。

2、具有系统容错（SFT）的可靠性措施

局域网的可靠性在很大程度上取决于对服务器硬件故障的查错和纠锗能力。因此，对文件服务器的共享硬盘采取了较多的可靠性措施，具体又分为几个级别。

第一级是硬盘目录和文件分配表（FAT）的保护、Netware 在硬盘的不同区域保存双份的目录和文件分配表，如果一处损坏，系统会自动转向另一处，并在硬盘中另找一处安排副本。每次启动文件服务器都要

例行检查目录和文件分配表的副本，以确认其一致性，目录和文件分配表的复制均由系统自动完成。

第二级是硬盘表面损坏时的数据保护。为了防止将数据写入磁盘的不可靠块，采用了热调整（HotFix）及写后读验证这两个互补技术进行数据保护。热调整技术首先在磁盘上划一小部分区域（默认值为硬盘容量的 2%）作为“热调整重定向区”，用于存放因硬盘上的主数据存储区损坏而被“重定向”的数据块。

第三级是 SFTNetware 采用磁盘镜象的方法实现硬盘驱动器损坏的保护。所谓磁盘镜象，即在一个磁盘通道上有两个成对的磁盘驱动器，同一数据分别写在两台硬盘上，如果一台硬盘驱动器损坏，另一台硬盘能单独运行，不会造成数据丢失和系统停止。磁盘镜象仅适用硬盘驱动器损坏的保护，磁盘通道控制板的损坏不能得到保护。

第四级是采用磁盘双工，对磁盘通道或硬盘驱动器损坏时起到保护作用。磁盘双工是采用二个磁盘通道，每个磁盘通道接磁盘镜象对中的一个硬盘。用户应该选择磁盘双工保护，这不仅在通道发生损坏时有保护功能，而且传送数据速度也比单纯的磁盘镜象快得多。无论是磁盘双工还是磁盘镜象都需要增加一台价格昂贵的硬盘。

第五级是 Netware 的一个附加容错功能：事务跟踪系统 TTS（TransactionTrackingSystem），用以防止当数据在写到数据库时，因系统故障而造成的数据库损坏，TTS 起作用时，SFTNetware 把数据库变更的整个过程看作是单个“事务”，必须整个完成或整个“返回”（完全复原），仅在所有文件正确更正之后，事务才算整个完成。如果在一个事务执行期间发生系统故障，TTS 执行一个“自动返回”，TTS 放弃这一事务已做的所有数据库修改并返回到数据库的原始状态，数据库的数据和系统信息均恢复至这一事务执行前的样子。

虽然 TTS 可以用来保护任何数据文件，但 TTS 主要用于数据库、帐户系统和库存清单维护等的数据文件。

3、开放的网络软件开发环境

首先是开放的数据链路接口 ODI（OpenData 一 1inkInterface），这是 Novell/Netware 的一项重要网络互连技术。它的实现方法是以 Netware 作为开放式服务器，支持多种通信协议和多种设备驱动程序，构成异构的计算机网络，ODI 允许在 Netware 工作站上不增加网络接口卡，使用多种网络协议（如 IPX/SPX,Apple，Talk,TCP／IP 等）来扩展网络。ODI

可用同一网络卡，建立不同的“逻辑网卡”，对不同的网络连接，使用不同的逻辑网卡,使用不同类型的信包。

用 ODI 可实现不同工作站、文件服务器、主机、不同网络协议的通信，在工作站上加上网卡和 ODI 系统就可构成 ODI 工作站。

其次 NetwareStreams 流提供了操作系统和网络通协议（如 IPX／SPX，TCP／IP、SNA、OSI 等）之间的通用接口，它允许在单个文件服务器上，存放和使用多种网络协议。

Streams 由一组可加载模块组成，若在编程时使用了如 CLIB 等接口，则必须有相应的 Streams 接口模块。常用的 Streams 模块有 StreamsNLM，SPXSNLS，IPXSNLM，CLSNLM，TLINLM。

第三，Netware 为了使用户在程序级使用网络资源，给用户提供了有关网络功能的 C 应用库函数和灵活的高级语言接口。用户可以在自己的应用环境中，使用 Netware 的网络功能，建立自身的网络开发环境。Netware 开放系统结构给用户使用和扩充自己的网络功能提供了极大方便。

计算机局域网络基础知识简介

作为信息技术基础——计算机网络（局域网和远

程网）是当今世界上最为活跃的技术因素之一。70年代末期出现的计算机局域网(LAN－LocalAreaNetwork)，在80年代获得了飞速发展和大范围的普及，90年代正步入更高速的阶段。目前LAN的使用已相当普遍，其主要用途是：

①共享打印机、绘图机等费用很高的外部设备；

②通过公共数据库共享各类信息；

③向用户提供诸如电子邮件之类的高级服务。

在一座办公大楼、一栋大厦、一个校园或一个企业内实现这种互连的网络方法有：Ethernet网(以太网),也称为8023LAN;令牌环网,也称为8025LAN;令牌总线网,也称为8024LAN以及光纤分布数据接口(FDDI)等。

什么是LAN

为了完整地给出LAN的定义，必须使用两种方式：一种是功能性定义,另一种是技术性定义。前一种将LAN定义为一组台式计算机和其它设备,在物理地址上彼此相隔不远，以允许用户相互通信和共享诸如打印机和存储设备之类的计算资源的方式互连在一起的系统。这种定义适用于办公环境下的LAN、工厂和研究机构中使用的LAN。

就LAN的技术性定义而言,它定义为由特定类型

的传输媒体(如电缆、光缆和无线媒体)和网络适配器(亦称为网卡)互连在一起的计算机,并受网络操作系统监控的网络系统。

功能性和技术性定义之间的差别是很明显的,功能性定义强调的是外界行为和服务;技术性定义强调的则是构成 LAN 所需的物质基础和构成的方法。

局域网(LAN)的名字本身就隐含了这种网络地理范围的局域性。由于较小的地理范围的局限性。由于较小的地理范围,LAN 通常要比广域网(WAN)具有高的多的传输速率,例如,目前 LAN 的传输速率为 10Mb/s,FDDI 的传输速率为 100Mb/s,而 WAN 的主干线速率国内目前仅为 64kbps 或 2048Mbps,最终用户的上线速率通常为 144kbps。

LAN 的拓扑结构目前常用的是总线型和环行。这是由于有限地理范围决定的。这两种结构很少在广域网环境下使用。

LAN 还有诸如高可靠性、易扩缩和易于管理及安全等多种特性。

LAN 的简史

在计算机应用的初期,人们使用的都是大中型计算机,通常简称为主机。需要使用计算机的人必须向计算机操作人员提交请求,而且在获准上机后,必须

等待数小时或几天才能得到结果。后来,随着电子技术的发展,通过终端连到了主机上,从而人们不必进入机房,只需从办公室的终端上便可提交请求。再后来又出现了中小型计算机，操作系统也随之出现。这时用户已经能够以交互操作方式向中心机提交请求。然而，计算机的普及使用只是在 70 年代出现了个人计算机(PC)后才得以实现的。

1981 年出现的 IBMPC 机的处理能力和存储能力已经可同早几年的大型机相媲美。随着 PC 的大量投入市场,人们发现,每台 PC 配置一台磁盘驱动器和打印机，当时在费用上实在难以承受。于是出现了资源共享的方式:磁盘服务器和共享打印机。这是一种硬件和软件的组合,它可使几个PC用户很方便地对公共硬盘驱动器进行共享式访问。第一个磁盘服务器是在CP/M 操作系统下运行的。

早期的 LAN，用户对硬盘驱动器的共享访问是经过连到共享驱动器的计算机实现的。计算机中的软件将公享的硬盘驱动器分成称为“卷”的区域，每个用户一个。在用户看来,用户分得的“卷”犹如他自己的专用盘驱动器。硬盘通常还包括公用卷,使用户共享信息。

在目前 LAN 中，磁盘服务器已经由文件服务器取

代。文件服务器无论在使用户共享文件方面,还是帮助用户跟踪他们的文件方面都优于磁盘服务器。有些 LAN 能支持多个文件服务器,每个服务器又有多个硬盘驱动器与之相连,从而使 LAN 很容易扩充。

除硬盘驱动器为 PC 用户共享外,第二个供 PC 用户共享的设备是打印机。目前,每种 LAN 都能有这种能力,而且在多数情况下,打印服务器已成了整个 LAN 软件包的一部分,而不是一台独立的计算机。

利用 LAN 打印服务器,用户仅可使用与一定文件服务器相连的打印机,或使用与网络上任何用户工作站相连的打印机。LAN 管理器可以限制对一定打印机的访问。用户也可将几个文件发送到同一个打印机。这些特点和其它特点取决于使用的 LAN 软件特性。

其它类型的服务器也已出现,如通讯服务器、数据库服务器等,将在以后的专题中介绍。需要强调的是,LAN 是通过将一组 PC 连接到指定为服务器的机器上来实现的,连接媒体可有多种,如同轴电缆等。

为什么需要 LAN

LAN 的最初目的是在若干用户间共享资源,并能维持连入网络的各种机器本身原有的重要功能。当然,现在共享资源的方法比以前更加完善了。例如,LAN 可使多台 PC 机共享一台费用较高的激光打印机。

LAN 还可使用户共享公共数据。正是由于这种共享特性，出现了很多更加完善的技术。LAN 的最初方法是将网上 PC 机的共享数据放入一个中心文件服务器中。服务器通常由一台 PC 机组成,代表 LAN 上的用户专门管理数据。这种方法效率较低,而且服务器和 PC 机之间的数据流随 PC 机的增加,或工作量的增大而可能使 LAN 产生阻塞。产生这种问题的原因是,每当用户希望访问服务器上的一个记录时,便进行搜索,数据库中的每个记录经过LAN从文件服务器发送到请求信息的 PC 机,直到接到所需的文件记录为止。

这个问题可使用客户/服务器技术来避免。客户/服务器方式能使 LAN 和其上的 PC 机操作更为有效。从本质上说,应用可分为两部分,一部分运行在用户的微机上,另一部分运行在中心服务器上。如果用户希望访问某一个记录,他便向服务器发送请求，中心服务器将在自己的机器上定位用户请求的那个记录,并响应用户请求，将记录发往请求它的 PC 机。因为这种方式不再需要将其它记录发到 LAN 上,所以具有较高的效率,并能减少 LAN 上的信息阻塞。

即使在较小的LAN上,客户/服务器计算方式也越来越重要,这是因为在开发 LAN 各种应用时将会利用这种技术。用户的 PC 机随后只需集中到它要处理的

任务上,如信息表示和在用户控制下的诸如字处理和电子表格之类的服务。中心服务器则集中到由若干LAN用户共享的服务上,如管理公共数据。

应该指出,如果在较小的LAN上专门设置一个服务器,在成本上是不大合算的。在这种情况下,有些PC机要负担起双重作用,即作为数据库服务器,也作为客户。这样形成的小型LAN,各PC机能以灵活和有效的方法相互通信和共享信息。

LAN的基本部件

要构成LAN,必须有其基本部件。

①计算机(特别是PC机);

②传输媒体;

③网络适配器;

④网络连接设备;

⑤网络操作系统。

LAN的网络拓扑结构

目前大多数LAN使用的拓扑结构有3种

①星行拓扑结构

②环行拓扑结构

③总线型拓扑结构

网络操作系统

网络操作系统(NOS)是网络的心脏和灵魂,是向

网络计算机提供服务的特殊的操作系统它在计算机操作系统下工作,使计算机操作系统增加了网络操作所需要的能力。例如象前面已谈到的当你在 LAN 上使用字处理程序时,你的PC机操作系统的行为象在没有构成 LAN 时一样，这正是 LAN 操作系统软件管理了你对字处理程序的访问。网络操作系统运行在称为服务器的计算机上,并由连网的计算机用户共享,这类用户称为客户。

NOS 与运行在工作站上的单用户操作系统或多用户操作系统由于提供的服务类型不同而有差别。一般情况下，NOS 是以使网络相关特性最佳为目的的。如共享数据文件、软件应用以及共享硬盘、打印机、调制解调器、扫描仪和传真机等。一般计算机的操作系统，如 DOS 和 OS/2 等,其目的是让用户与系统及在此操作系统上运行的各种应用之间的交互作用最佳。

为防止一次由一个以上的用户对文件进行访问，一般网络操作系统都具有文件加锁功能。如果没有这种功能,将不会正常工作。文件加锁功能可跟踪使用中的每个文件,并确保一次只能一个用户对其进行编辑。文件也可由用户的口令加锁,以维持专用文件的专用性。

NOS 还负责管理 LAN 用户和 LAN 打印机之间的连

接。NOS 总是跟踪每一个可供使用的打印机以及每个用户的打印请求,并对如何满足这些请求进行管理,使每个端用户的操作系统感到所希望的打印机犹如与其计算机直接相连。

NOS 还对每个网络设备之间的通信进行管理,这是通过 NOS 中的媒体访问法来实现的。

NOS 的各种安全特性可用来管理每个用户的访问权利,确保关键数据的安全保密。因此,NOS 从根本上说是一种管理器,用来管理连接、资源和通信量的流向。

局域网的主要技术 411 局域网的特点

区别于一般的广域网(WAN),局域网(LAN)具有以下一些特点:

(1)地理分布范围较小,一般为数百米至数公里。可以覆盖一幢大楼、一所校园或者一个企业。

(2)数据传输速率高,一般为 01~100Mbps,目前已出现速率高达 1000Mbps 的局域网。可交换各类数字和非数字(如语音、图像、视频等)信息。

(3)误码率低,一般在 10-11~10-8 以下。这是因为局域网通常采用短距离基带传输,可以使用高质量的传输媒体,从而提高了数据传输质量。

(4)以 PC 机为主体,包括终端及各种外设,网中一

般不设中央主机系统。

(5)一般仅包含岱I参考模型中的低三层功能,即仅涉及通信子网的内容。

(6)协议简单、结构灵活、建网成本低、周期短、便于管理和扩充。局域网可分成三大类:一类是平时常说的局域网 LANE 另一类是采用电路交换技术的局域网,称计算机交换机 CBX(Computer Branche Xchange)或 PBX(Private Branche Xchange)还有一类是新发展的高速局域网 HSLN(High SpeedLocal Network)。

在 LAN 和 WAN 之间的是城市区域网 MAN(Metropolitan Area Net work),简称城域网。MAN 是一个覆盖整个城市的网络,但它使用 LAN 的技术。

局域网的特性主要涉及拓扑结构、传输媒体和媒体访问控制(Meditm Access Contro,MAC)等三项技术问题,其中最重要的是媒体访问控制方法。

局域网的技术特性

拓扑结构总线、环形、星形

传输媒体双绞线、同轴电缆、光纤、无线通信

媒体访问控制 CSMA/CD、TokenRing、TokenBus、FDDI

局域网标准化组织 ISO、IEEE802 委员会、NBS、

EIA、ECMA、

应用领域办公自动化、企业自动化、校园、医院等

局域网的拓扑结构

网络的拓扑结构对网络性能有很大影响。选择网络拓扑结构,首先要考虑采用何种媒体访问控制方法,因为特定的媒体访问控制方法一般仅适用于特定的网络拓扑结构;其次要考虑性能、可靠性、成本、扩充灵活性、实现的难易程度及传输媒体的长度等因素。局域网常用的拓扑结构有总线、环形、星形三种。有关网络拓扑结构的概念已在第 2 章中做了介绍,这里再针对局域网的拓扑适用范围做一些说明。

总线网一般采用分布式媒体访问控制方法。总线网可靠性高、扩充性能好、通信电缆长度短、成本低,是用来实现局域网的最通用的拓扑结构,著名的以太网(Ethernet)就是总线网的典型实例。总线拓扑网可采用两种协议,一种是以太网采用的 CSMA/CD;另一种是总线拓扑网与令牌环相结合的变型,其在物理连接上是总线拓扑结构,而在逻辑上则采用令牌环,兼有了总线结构和令牌环的优点。总线网的缺点是若主干电缆某处发生故障,整个网络将瘫痪;另外,当网上站点较多时,会因数据冲突增多而使效率降低。

环形网也采用分布式媒体访问控制方法。环形网控制简单、信道利用率高、通信电缆长度短、不存在数据冲突问题,在局域网中应用较广泛,典型实例有IBM 令牌环(TokenRing)网和剑桥环(CambridgeRing)网。另外还有一种 FDDI 结构,它是采用光纤作为传输媒体的高速通用令牌环网,常用于高速局域网HSLN和城域网 MAN 中。环形网的缺点是?对节点接口和传输线的要求较高,一旦接口发生故障可能导致整个网络不能正常工作。

星形网往往采用集中式媒体访问控制方法。星形网结构简单、实现容易、信息延迟确定。其缺点是通信电缆总长度长、传输媒体不能共享。星形网的典型实例是计算机交换机 CBX。

局域网的传输媒体 LAN 中使用的传输方式有基带和宽带两种

基带用于数字信号传输,常用的传输媒体有双绞线或同轴电缆。宽带用于无线电频率范围内的模拟信号的传输,常用同轴电缆。

给出了这两种传输方式的比较。

基带、宽带传输方式的比较

基带宽带

数字信号传输

全部带宽用于单路信道传输
双向传输
总线拓扑
距离达数公里
模拟信号传输（需用 MODEM)
使用 FDM 技术，多路信道复用
单向传输
总线或树形拓扑
距离达数十公里 1 基带系统

使用数字信号传输的 LAN 定义为基带 LAN。数字信号通常采用曼彻斯特编码传输,媒体的整个带宽用于单信道的信号传输,不采用频分多路复用技术。数字信号传输要求用总线形拓扑,因为数字信号不易通过树形拓扑所要求的分裂器和连接器。基带系统只能延伸数公里的距离,这是由于信号的衰减会引起脉冲减弱和模糊,以致无法实现更大距离上的通信。基带传输是双向的,媒体上任意一点加入的信号沿两个方向传输到两端的端接器(即终端阻抗器),并在那里被吸收。总线 LAN 常采用 500 的基带同轴电缆。对于数字信号来说,500 电缆受到来自接头插入容抗的反射不那么强,而且对低频电磁噪声有较好的抗干扰性。最简单的基带同轴电缆 LAN 由一段无分校的同轴电缆

构成,两端接有防反射的端接器,推荐的最大长度为500米。站点通过接头接入主电缆,任何两接头间的距离为25米的整倍数,这是为了保证来自相邻接头的反射在相位上不致于叠加。推荐的最多接头数目为100个,每个接头包括一个收发器,其中包含发送和接收用的电子线路。

为了延伸网络的长度,可以采用中继器。中继器由组合在一起的两个收发器组成,连到不同的两段同轴电缆上。中继器在两段电缆间向两个方向传送数字信号,在信号通过时将信号放大和复原。因而,中继器对于系统的其余部分来说是透明的。由于中继器不做缓冲存贮操作,所以并没有将两段电缆隔开,因此如果不同段上的两个站同时发送的话,它们的分组将互相干扰(冲突)。为了避免多路径的干扰,在任何两个站之间只允许有一条包含分段和中继器的路径。802标准中,在任何两个站之间的路径中最多只允许有4个中继器,这就将有效的电缆长度延伸到25公里。是一个具有3个分段和两个中继器的基带系统例子。双绞线基带LAN用于低成本、低性能要求的场合,双绞线安装容易,但往往限制在1公里距离以内,数据速率为1Mbps—10Mbps。

宽带系统

在LAN范围内,宽带一般用于传输模拟信号,这些模拟载波信号工作在高频范围(通常为10—400MHz),因而可用FDM技术把宽带电缆的带宽分成多个信道或频段。宽带系统采用总线/树形拓扑结构,可以达到比基带大得多的传输距离(达数十公里),这是因为携带数字数据的模拟信号,在噪声和衰减损害数据之前,可以传播较长的距离。

宽带同基带一样,系统中的站点是通过接头接入电缆的。但是,与基带不同的是宽带本质上是一种单方向传输的媒体,加到媒体上的信号只能沿一个方向传播。这种单向性质,意味着只有处于发送站“下游”的站点才能收到发送站的信号。因此需有两条数据路径,这些路径在网络的端头处接在一起。对于总线拓扑,端头就是总线的一端;对于树形拓扑,端头是有分校的树根。所有站沿一条路径(人径)向端头传输,在端头接收到的信号,再沿另一条数据路径(出径)离开端头传输,所有的站点都在出径上接收。

在物理上,可用双电缆和中分(Midsplit)两种不同的结构来实现输入和输出的通路。在双电缆结构中,人径和出径是分开的两根电缆,两者间的端头只是一个无源连接装置,每个站以相同的频率发送和接收。在中分构造中,人径和出径是同一电缆上的不同频率,

双向放大器传送较低频率(5—116MHz)的入径和较高频率(168~300MHz)的出径。端头包含一个称为频率转换器的装置,将入径频率转换为出径频率。频率转换器可以是模拟装置也可以是数字装置,模拟装置只要把信号转换成一个新的频率并重发就可以了,而数字装置则先要在端头恢复数字数据,然后再在新的频率上重发净化了的数据。414 局域网的媒体访问控制方法

环形或总线拓扑中,由于只有一条物理传输通道连接所有的设备,因此,连到网络上的所有设备必须遵循一定的规则,才能确保传输媒体的正常访问和使用。常用的媒体访问控制方法有:具有冲突检测的载波监听多路访问

CSMA/CD(CarrierSenseMultipleAccess/CollSionDetection)、控制令牌(ControlToken)及时槽环(SlottedRing)三种技术。

1.具有冲突检测的载波监听多路访问 CSMA/CD

具有冲突检测的载波监听多路访问CSMA/CD采用随机访问和竞争技术,这种技术只用于总线拓扑结构网络。CSMA/CD 结构将所有的设备都直接连到同一条物理信道上,该信道负责任何两个设备之间的全部数据传送,因此称信道是以“多路访问”方式进行操作

的。站点以帧的形式发送数据,帧的头部含有目的地和源点的地址。帧在信道上以广播方式传川输,所有连接在信道上的设备随时都能检测到该帧。当目的地站点检测到目的地址为本端地址的帧时,就接收帧中所携带的数据,并按规定的链路协议给源站点返回一个响应。

采用这种操作方法时,在信道上可能有两个或更多的设备在同一瞬间都发送帧,从而在信道上造成帧的重叠而出现差错,这种现象称为冲突。为减少这种冲突,源站点在发送帧之前,首先要监听信道上是否有其它站点发送的载波信号(即进行“载波监听”),若监听到信道上有载波信号则推迟发送,直到信道恢复到安静(空闲)为止。另外,还要采用边发送边监听的技术(即“冲突检测”),若监听到干扰信号,就表示检测到冲突,于是就要立即停止发送。为了确保冲突的其它站点知道发生了冲突,首先在短时间里持续发送一串阻塞(Jam)码,卷入冲突的站点则等待一随机时间,然后准备重发受到冲突影响的帧。这种技术对发生冲突的传输能迅速发现并立即停止发送,因此能明显减少冲突次数和冲突时间。CSMA/CD 媒体访问控制的具体实现,将在本章第 43 节中再详细介绍。

2.控制令牌

控制令牌是另一种传输媒体访问控制方法。它是按照所有站点共同理解和遵守的规则,从一个站点到另一个站点传递控制令牌,一个站点只有当它占有令牌时,才能发送数据帧,发完帧之后,即把令牌传递给下一个站点。其操作次序如下:

(1)首先建立一个逻辑环,将所有站点同物理媒体相连,然后产生一个控制令牌。

(2)控制令牌由一个站点沿着逻辑环顺序向下一个站点传递。

(3)等待发送帧的站点接收到控制令牌后,把要发送的帧利用物理媒体发送出去,然再将控制令牌沿逻辑环传递给下一站点。

控制令牌方法除了用于环形网拓扑结构(即令牌环)之外,也可以用于总线网拓扑结

对于一个物理环,令牌传递的逻辑结构和物理环的结构是相同的,令牌传递的次序和站点连接的物理次序也是一致的;而对于总线网,逻辑环次序则不必和电缆上的站点连接次序相对应,所有站点没有必要均按逻辑环连接。

3.时槽环时槽环只用于环形网的媒体控制访问,这种方法对每个节点预先安排一个特定的时间片段(即时槽段),每个节点只能在时槽内传输数据。若数

据较长,可用多个时槽来传输。

时槽环采用集中控制方式,这种方法首先由环中被称为监控站的特定节点起动环,并产生若干个固定长度的比特串,这种比特串即称为时槽。时槽不停地绕环从一个站点传递到另一个站点。当一个站点收到时槽时,由该站点的接口阅读后再将其转发到环的下一个站点,如此一直循环下去。监控站确保总有一个固定数目的时槽绕环传送,而不考虑组成环的站点数目。每个时槽能携带一个固定尺寸的信息帧,时槽帧的格式。

时槽环初始化时,由监控站将每个时槽开头的满/空位置为空状态。某个站点要发送数据前,首先要得到一个空时槽,然后将该时槽的满/空位置为满状态,将数据的内容插入时槽中,同时在帧的头部填入目的地地址和源地址,并将帧尾部的两个响应位全置为 1,然后发送该时槽,使它绕物理环从一个站点至另一个站点传送。

环中每个站对任何置满的时槽头部的目的地址进行检测,如果检测到是自己的地址,便从时槽中阅读所携带的数据内容,并修改时槽尾部的一对响应位,然后通过环再将它转发出去。如果目的地站点忙或者拒收,则响应位做相应的标记,或保留不做改变。源站

点在起动一个帧发送之后,要等到该帧绕环一周。由于每个站均知道环上时槽的总数,由环接口对时槽转发计数可知道所发时槽的到来。此后,源站点将所用时槽重新标记为主空状态,并阅读时槽尾部的响应位,以确定是否应舍弃已被发送的该帧备份,或者重发该二帧。由于采用了响应位,就不需要设置独立的响应帧。

监控站传递位由监控站用于监测各个站点发送的帧是否有差错或站点有无故障,该位由-源站点在发送帧时置“0”。当满时槽在环接口上转发时,由监控站对每一个满时槽的该位置“1”。如果监控站在其转发某个满时槽时,测得监控站传递位已被置为 1,就认为源站点有故障,便可将该帧的满/空位置为空,并释放空时槽。时槽尾部的两个控制位是提供给 urE 高层协议使用的,在媒体访问控制层中没有意义。

需要特别指出的是,在时槽环媒体访问控制方法中,每个站点每次只能传送一个帧,若想要传送另一个帧,则首先必须释放传输前一帧所用的时槽。这种对环的访问方法体现了公平性,并被各个互连的站点所共享。时槽环的优点是结构简单,节点间相互干扰少、可靠性高。但是,时槽环为保持基本环结构需要一个特定的监控站节点:由于绕环一周时间内,每个

站点只能占用一个时槽,若某站点发送的数据较长要占用多个时槽,而此时环上只有该站点有数据要发送,则许多时槽都是空循环;另外,每个 40 位长的时槽只能携带 16 位有效数据,开销大、效率较低。相比之下,令牌环中的某个站点得到控制令牌后,就可将包括多个字节的信息帧作为一个整体进行发送,所以效率比时槽环高。

局域网的参考模型与协议标准

局域网的标准化工作,能使不同生产厂家的局域网产品之间有更好的兼容性,以适应各种不同型号计算机的组网需求,并有利于产品成本的降低。国际上从事局域网标准化工作的机构主要有国际标准化组织 ISO、美国电气与电子工程师学会 IEEE 的 802 委员会、欧洲计算机制造商协会 ECMA、美国国家标准局 NBS、美国电子工业协会 EIA、美国国家标准化协会 ANSI 等。

局域网的参考模型

局域网是一个通信网,只涉及到相当于 OSI 很 M 通信子网的功能。由于内部大多采用共享信道的技术,所以局域网通常不单独设立网络层。局域网的高层功能由具体的局域网操作系统来实现。

IEEE802 标准的局域网参考模型与 OSI 很 M 的对

应关系,该模型包括了 OSI/RM 最低两层(物理层和链路层)的功能,也包括网间互连的高层功能和管理功能。从,图中可见,OSI/RM 的数据链路层功能,在局域网参考模型中被分成媒体访问控制 MAC(Medium Access Control)和逻辑链路控制 LLC(Logical Link Control)两个子层。

在 OSI/RM 中,物理层、数据链路层和网络层使计算机网络具有报文分组转接的功能。对于局域网来说,物理层是必需的,它负责体现机械、电气和过程方面的特性,以建立、维持和拆除物理链路;数据链路层也是必需的,它负责把不可靠的传输信道转换成可靠的传输信道,传送带有校验的数据帧,采用差错控制和帧确认技术。

但是,局域网中的多个设备一般共享公共传输媒体,在设备之间传输数据时,首先要解决由哪些设备占有媒体的问题。所以局域网的数据链路层必须设置媒体访问控制功能。由于局域网采用的媒体有多种,对应的媒体访问控制方法也有多种,为了使数据帧的传送独立于所采用的物理媒体和媒体访问控制方法,IEEE802 标准特意把 LLC 独立出来形成一个单独子层,使 LLC 子层与媒体无关,仅让 MAC 子层依赖于物理媒体。由于设立了 MAC 子层,IEEE802 标准就具有了

可扩充性,有利于接纳新的媒体和媒体访问控制方法。

由于穿越局域网的链路只有一条,不需要设立路由选择和流量控制功能,如网络层中的分组寻址、排序、流量控制、差错控制等功能都可以放在数据链路层中实现。因此,局域网中可以不单独设置网络层。当局限于一个局域网时,物理层和链路层就能完成报文分组转接的功能。但当涉及网络互连时,报文分组就必须经过多条链路才能到达目的地,此时就必须专门设置-个层次来完成网络层的功能,在IEEE802标准中这一层被称为网际层。

在参考模型中,每个实体和另一个系统的同等实体按协议进行通信;而一个系统中上下层之间的通信,则通过接口进行,并用服务访问点 SAP(Service Access Point)来定义接口。为了对多个高层实体提供支持,在 LI层的顶部有多个 LLC 服务访问点(LSAP),为图中的实体A和B提供接口端;在网际层的顶部有多个网间服务访问点(NSAP),为实体C、D和E提供接口端;媒体访问控制服务访问点(MSAP)向 LLC 实体提供单个接口端,物理服务访问点(PSAP)也向MAC 实体提供单个接口端。

LLC 子层中规定了无确认无连接、有确认无连接

和面向连接三种类型的链路服务。确认无连接服务是一种数据报服务,信息帧在LLC实体间交换时,无需在同等层实体间事先建立逻辑链路,对这种 LLC 帧既不确认,也无任何流量控制或差错恢复;有确认无连接服务除了对 LLC 帧进行确认外,其它类似于无确认无连接服务;面向连接服务提供服务访问点之间的虚电路服务,在任何信息帧交换前,一对LLC实体之间必须建立逻辑链路,在数据传送过程中,信息帧依次发送,并提供差错恢复和流量控制功能。

MAC 子层在支持 LLC 子层完成媒体访问控制功能时,可以提供多个可供选择的媒体访问控制方式。使用 MSAP 支持 LLC 子层时,MAC 子层实现帧的寻址和识别。MAC 到 MAC 的操作通过同等层协议来进行,MAC 还产生帧检验序列和完成帧检验等功能。

IEEE802 标准

IEEE 在 1980 年 2 月成立了局域网标准化委员会(简称IEEE802委员会),专门从事局域网的协议制订,形成了一系列的标准,称为 IEEE802 标准。该标准已被国际标准化组织 ISO 采纳,作为局域网的国际标准系列,称为 ISO8802 标准。在这些标准中,根据局域网的多种类型,规定了各自的拓扑结构、媒体访问控制方法、帧的格式和操作等内容。IEEE8021 是局域网的

体系结构、网络管理和网际互连协议。IEEE8022 集中了数据链路层中与媒体无关的 LLC 协议。涉及与媒体访问有关的协议,则根据具体网络的媒体访问控制方法分别处理,其中主要的 MAC 协议有:EEE8023 载波监听多路访问/冲突检测 CSMA/CD 访问方法和物理层协议、IEEE8024 令牌总线(TokenBus)访问方法和物理层协议、IEEE8025 令牌环(TokenRing)访问方法和物理层协议,IEEE8026 关于城域网的分布式队列双总线以主 DB(Distri buted Queue Dual Bus)的标准等。

IEEE802 标准定义了 LLC 子层和 MAC 子层的帧格式。数据传输过程中,LLC 子层将高层递交的报文分组作为 LLC 的信息字段,再加上 LLC 子层目的服务访问点(DSAP)、服务访问点(SSAP)及相应的控制信息以构成 LLC 帧。LLC 帧格式及其控制字段定义见图(48)LLC 的链路只有异步平衡方式(ABM),而不用正常响应方式(NRM)和异步响应方式(ARM)。也即节点均为组合站,它们既可作为主站发送命令,也可作为从站响应命令。IEEE8022 标准定义的 LLC 帧格式与 HDLC 的帧格式有点类似,其控制字段的格式和功能完全效仿 HDLC 的平衡方式制定。LLC 帧也分为信息帧、监控帧和无编号帧三类。信息帧主要用于信息数据传输,监控帧主要用于流量控制,元编号帧用于在 LLC 子层传输控

制信号以对逻辑链路进行建立与释放。LLC 帧的类型取决于控制字段的第 1、2 位,信息帧和监控帧的控制字段均为 2 字节长,无编号帧的控制字段为 1 字节。监控帧控制字段中的第5--8位为保留位,一般设置为0。控制字段中的其它位含义与 EELC 控制字段中的含

载波监听多路访问 CSMA

载波监听多路访问CSMA的技术,也称做先昕后说LBT(ListenBeforeTall○。要传输数据的站点首先对媒体上有元载波进行监听,以确定是否有别的站点在传输数据。如果媒体空闲,该站点便可传输数据;否则,该站点将避让一段时间后再做尝试。这就需要有一种退避算法来决定避让的时间,常用的退避算法有非坚持、1-坚持和 P-坚持三种。

非坚持算法

算法规则为:

(1)如果媒体是空闲的,则可以立即发送。

(2)如果媒体是忙的,则等待一个由概率分布决定的随机重发延迟后,再重复前一步骤。

采用随机的重发延迟时间可以减少冲突发生的可能性。非坚持算法的缺点是:即使有几个站点都有数据要发送,但由于大家都在延迟等待过程中,致使媒体仍可能处于空闲状态,使利用率降低。

坚持算法

算法规则为:

(1)如果媒体是空闲的,则可以立即发送。

(2)如果媒体是忙的,则继续监听,直至检测到媒体空闲,立即发送。

(3)如果有冲突(在一段时间内未收到肯定的回复),则等待一随机量的时间,重复步骤(1)~(2)。

这种算法的优点是:只要媒体空闲,站点就立即可发送,避免了媒体利用率的损失;其缺点是:假如有两个或两个以上的站点有数据要发送,冲突就不可避免。

3P-坚持算法

算法规则为:

(1)监听总线,如果媒体是空闲的,则以 P 的概率发送,而以(1-P)的概率延迟一个时间单位。一个时间单位通常等于最大传播时延的 2 倍。

(2)延迟了一个时间单位后,再重复步骤(1)。

(3)如果媒体是忙的,继续监听直至媒体空闲并重复步骤(1)。

P-坚持算法是一种既能像非坚持算法那样减少冲突,又能像 1 一坚持算法那样减少媒体空闲时间的折中方案。问题在于如何选择 P 的有效值,这要考虑

到避免重负载下系统处于的不稳定状态。假如媒体忙时,有 N 个站有数据等待发送,一旦当前的发送完成时,将要试图传输的站的总期望数为 NP。如果选择 P 过大,使 NP>1,表明有多个站试图发送,冲突就不可避免。最坏的情况是,随着冲突概率的不断增大,而使吞吐率降到零。所以必须选择适当 P 值使 NP<1。当然 P 值选得过小,则媒体利用率又会大大降低。

具有冲突检测的载波监听多路访问 SMA/CD

在 CSMA 中,由于信道传播时延的存在,即使总线上两个站点没有监听到载波信号而发送帧时,仍可能会发生冲突。由于 CSMA 算法没有冲突检测功能,即使冲突已发生,仍然要将已破坏的帧发送完,使总线的利用率降低。一种 CSMA 的改进方案是使发送站点在传输过程中仍继续监听媒体,以检测是否存在冲突。如果发生冲突,信道上可以检测到超过发送站点本身发送的载波信号的幅度,由此判断出冲突的存在。一旦检测到冲突,就立即停止发送,并向总线上发一串阻塞信号,用以通知总线上其它各有关站点。这样,通道容量就不致因白白传送已受损的帧而浪费,可以提高总线的利用率。这种方案称做载波监听多路访问/冲突检测协议,简写为 CSMA/CD,这种协议已广泛应用于局域网中。CSMA/CD 的代价是用于检测冲突所花费

的时间。对于基带总线而言,最坏情况下用于检测一个冲突的时间等于任意两个站之间最大传播时延的两倍。从一个站点开始发送数据到另一站点开始接收数据,也即载波信号从一端传播到另一端所需的时间,称为信号传播时延。信号传播时延(us)=两站点间的距离(m)/信号传播速度(200m/us)。假定 A、B 两个站点位于总线两端,两站点之间的最大传播时延为 tp。当 A 站点发送数据后,经过接近于最大传播时延 tp 时,B 站点正好也发送数据,此时冲突便发生。发生冲突后,B 站点立即可检测到该冲突,而 A 站点需再经过一份最大传播时延 tp 后,才能检测出冲突。也即最坏情况下,对于基带 CSMA/CD 来说,检测出一个冲突的时间等于任意两个站之间最大传播时延的两倍(2tp)。

数据帧从一个站点开始发送,到该数据帧发送完毕所需的时间称为数据传输时延;同理,数据传输时延也表示一个接收站点开始接收数据帧,到该数据帧接收完毕所需的时间。数据传输时延(s)=数据帧长度(bit)/数据传输速率(bps)。若不考虑中继器引人的延迟,数据帧从一个站点开始发送,到该数据帧被另一个站点全部接收所需的总时间,等于数据传输时延与信号传播时延之和。

由上述分析可知,为了确保发送站点在传输时能

检测到可能存在的冲突,数据帧的传输时延至少要两倍于传播时延。换句话说,要求分组的长度不短于某个值,否则在检测出冲突之前传输已经结束,但实际上分组已被冲突所破坏。由此引出了 CSMA/CD 总线网中最短帧长的计算关系式:

最短数据帧长(bit)/数据传输速率(Mbps)=2x 任意两站点间的最大距离(m)/200(m/us)

计算时要注意单位的统一。

由于单向传输的原因,对于宽带总线而言,冲突检测时间等于任意两个站之间最大传播时延的 4 倍。所以,对于宽带CSMA/CD来说,要求数据帧的传输时延至少 4 倍于传播时延。

在 CSMA/CD 算法中,一旦检测到冲突并发完阻塞信号后,为了降低再次发生冲突的概率,需要等待一个随机时间,然后再使用 CSMA 方法试图传输。为了保证这种退避操作维持稳定,采用了一种称为二进制指数退避的算法,其规则如下:

(1)对每个数据帧,当第一次发生冲突时,设置一个参量 L=2;

(2)退避间隔取 1 到 L 个时间片中的一个随机数,1 个时间片等于两站点之间的最大传播时延的两倍;

(3)当数据帧再次发生冲突,则将参量 L 加倍;

(4)设置一个最大重传次数,超过该次数,则不再重传,并报告出错。

二进制指数退避算法是按后进先出 LIFO(LastIn First Out)的次序控制的,即未发生冲突或很少发生冲突的数据帧,具有优先发送的概率;而发生过多次冲突的数据帧,发送成功的概率就更小 0。

EEE8023 就是采用二进制指数退避和 1-坚持算法的 CSMA/CD 媒体访问控制方法。这种方法在低负荷时,如媒体空闲时,要发送数据帧的站点能立即发送;在重负荷时,仍能保证系统的稳定性。由于在媒体上传播的信号会衰减,为确保能检测出冲突信号,CSMA/CD 总线网限制一段元分支电缆的最大长度为 500 米。

IEEE8023 媒体访问控制协议

1CSMA/CD 总线的实现模型

IEEE8023 是一个使用 CSMA/CD 媒体访问控制方法的局域网标准。CSMA/CD 总线的实现模型它对应于 OSI/RM 的最低两层。从逻辑上可以将其划分为两大部分:一部分由 LLC 子层和 MAC 子层组成,实现岱 I 很 M 的数据链路层功能,另一部分实现物理层功能。

把依赖于媒体的特性从物理层中分离出来的目的,是要使得 LLC 子层和 MAC 子层能适用于各类不同

的媒体。

物理层内定义了两个兼容接口:依赖于媒体的媒体相关接口 MDI 和访问单元接口 AUIoMDI 是一个同轴电缆接口,所有站点都必须遵循 IEEE8023 定义的物理媒体信号的技术规范,与这个物理媒体接口完全兼容。由于大多站点都设在离电缆连接处有一段距离的地方,在与电缆靠近的 MAC 中只有少量电路,而大部分硬件和全部的软件都在站点中,AUI 的存在为 MAC 和站点的配合使用带来了极大的灵活性。

MAC 子层和 LLC 子层之间的接口提供每个操作的状态信息,以供高一层差错恢复规程所用。MAC 子层和物理层之间的接口,提供包括成帧、载波监听、启动传输和解决争用、在两层间传送串行比特流的设施及用于定时等待等功能。

2EEE8023MAC 帧格式

MAC 帧是在 MAC 子层实体间交换的协议数据单元,IEEE8023MAC 帧的格式。IEEE8023MAC 帧中包括前导码 P、帧起始定界符 SFD、目的地址 DA、源地址 SA、表示数据字段字节数长度的字段 LEN、要发送的数据字段、填充字段 PAD 和帧校验序列配 S 等 8 个字段。这 8 个字段中除了数据字段和填充字段外,其余的长度都是固定的。前导码字段 P 占 7 个字节,每个字节

的比特模式为“10101010”,用于实现收发双方的时钟同步。帧起始定界符字段 SFD 占 1 个字节,其比特模式为“10101011”,它紧跟在前导码后,用于指示一帧的开始。前导码的作用是使接收端能根据“1”、“0”交变的比特模式迅速实现比特同步,当检测到连续两位“1”(即读到帧起始定界符字段 SFD 最未两位)时,便将后续的信息递交给 MAC 子层。

地址字段包括目的地址字段 DA 和源地址字段 SA。目的地址字段占 2 个或 6 个字节,用于标识接收站点的地址,它可以是单个的地址,也可以是组地址或广播地址。DA 字段最高位为“0”表示单个地址,该地址仅指定网络上某个特定站点;DA 字段最高位为“1”、其余位不为全“1”表示组地址,该地址指定网络上给定的多个站点;DA 字段为全“1”,则表示广播地址,该地址指定网络上所有的站点。源地址字段也占 2 个或 6 个字节,但其长度必须与目的地址字段的长度相同,它用于标识发送站点的地址。在 6 字节地址字段中,可以利用其48位中的次高位来区分是局部地址还是全局地址。局部地址是由网络管理员分配,且只在本网中有效的地址;全局地址则是由 IEEE 统一分配的,采用全局地址的网卡出厂时被赋予惟一的 IEEE 地址,使用这种网卡的站点也就具有了全球独一

无二的物理地址。

长度字段 LEN 占两个字节,其值表示数据字段的字节数长度。数据字段的内容即为,LLC 子层递交的 LLC 帧序列,其长度为 0~1500 个字节。

为使 CSMA/CD 协议正常操作,需要维持一个最短帧长度,必要时可在数据字段之后、帧校验序列 FCS 之前以字节为单位添加填充字符。这是因为正在发送时产生冲突而中断的帧都是很短的帧,为了能方便地区分出这些元效帧,IEEE8023 规定了合法的 MAC 帧的最短帧长。对于 10Mbps 的基带 CSMA/CD 网,MAC 帧的总长度为 64~1518 字节。由于除了数据字段和填充字段外,其余字段的总长度为 18 个字节,所以当数据字段长度为 0 时,填充字段必须有 46 个字节。

帧校验序列 FCS 字段是 32 位(即 4 个字节)的循环冗余码(CRC),其校验范围不包括前导码字段P及帧起始定界符字段 SFD。

3EEE8023MAC 子层的功能

IEEE8023 标准提供了 MAC 子层的功能说明,内容主要有数据封装和媒体访问管理两个方面。数据封装(发送和接收数据封装)包括成帧(帧定界和帧同步)、编址(源地址及目的地址的处理)和错检测(物理媒体传输差错的检测)等;媒体访问管理包括媒体分配和

竞争处理。当 LLC 子层请求发送一数据帧时,MAC 子层的发送数据封装部分便按 MAC 子层的数据帧格式组帧。首先将一个前导码 P 和一个帧起始定界符 SFD 附加到帧的开头部分,填上目的地址和源地址,计算出 LLC 数据帧的字节数,填人数据长度计数字段 LEN。必要时还要将填充字符 PAD 附加到 LLC 数据帧后,以确保传送帧的长度满足最短帧长的要求。最后求出 CRC 校验码附加到帧校验序列 FCS 中。完成数据封装后的 MAC 帧,便可递交 MAC 子层的发送媒体访问管理部分以供发送。

借助于监视物理层收发信号(PLS)部分提供的载波监昕信号,发送媒体访问管理设法避免发送信号与媒体上其它信息发生冲突。在媒体空闲时,经短暂的帧间延迟(提供给媒体恢复时间)之后,就启动帧发送。然后,MAC 子层将串行位流送给 PLS 接口以供发送。PLS 完成产生媒体上电信号的任务,同时监视媒体和产生冲突检测信号。在没有争用的情况下,即可完成发送。发送完成后,MAC 子层通过 LLC 与 MAC 间的接口通知 LLC 子层,等待下一个发送请求。假如产生冲突,PLS 接通冲突检测信号,接着发送媒体访问管理开始处理冲突。首先,它发送一串称为阻塞(Jam)码的位序列来强制冲突,由此保证有足够的冲突持续时间,

以使其它与冲突有关的发送站点都得到通知。在阻塞信号结束时,发送媒体访问管理就暂停发送,等待一个随机选择的时间间隔后再进行重发尝试。发送媒体访问管理用二进制指数退避算法调整媒体负载。最后,或者重发成功,或者在媒体故障、过载的情况下,放弃重发尝试。

接收媒体访问管理部分的功能是,首先由 PLS 检测到达帧,使接收时钟与前导码同步,并接通载波监听信号。接收媒体访问管理部件要检测到达的帧是否错误,帧长是否超过最大长度,是否为 8 位的整倍数。还要过滤因冲突产生的碎片信号(即小于最短长度的帧)。

接收数据解封部分的功能,用于检验帧的目的地址字段,以确定本站点是否应该接收该帧。如地址符合,将其送到 LLC 子层,并进行差错检验。

IEEE8023 物理层规范

IEEE8023 委员会在定义可选的物理配置方面表现了极大的多样性和灵活性。为了区分各种可选用的实现方案,该委员会给出了一种简明的表示方法:

〈数据传输速率(Mbps)〉〈信号方式〉〈最大段长度(百米)〉如 10BASE5、i10BASE2、10BROAD36。但 10BASE-T 和 10BASE-F 有些例外,其中的 T 表示双绞

线、F 表示光纤。IEEE8023 的 10Mbps 可选方案见表 43。IEEE8023 的 10Mbps 可选方案

10BASE510BASE210BASE-T10BROAD3610BASE=F

传输媒体基带同轴电缆基带同轴叫缆非屏蔽双绞线宽带同轴电缆 850mm 光纤对

编码技术曼彻斯特码曼彻斯特码曼彻斯特码差分 PSK 码曼彻斯特码

拓扑结构总线总线里形总线/树形星形

最大段长 500m 185m 100m 1800m 500m

每段节点 10030----33

(1)10BASE5 和 10BASE2。前面介绍 IEEE8023 时所涉及的物理规范,实际上说的就是基于以太网的 10BASE5。

与 10BASE5 一样,10BASE2 也使用 50 瓯姆同轴电缆和曼彻斯特编码,数据速率为 10Mbps。两者的区别在于 10BASE5 使用粗缆(Φ10mm),10BASE2 使用细缆(5mm)。由于两者数据速率相同,所以可以使 10BASE5 电缆段和 10BASE2 电缆段共存于一个网络中。

(2)10BASE-T。10BASE-T 定义了一个物理上的星形拓扑网,其中央节点是一个集线器,每个节点通过一对双绞线与集线器相连。集线器的作用类似于一个转发器,它接收来自一条线上的信号并向其它的所有

线转发。由于任意一个站点发出的信号都能被其它所有站点接收,若有两个站点同时要求传输,冲突就必然发生。所以,尽管这种策略在物理上是一个星形结构,但从逻辑上看与 CSMA/CD 总线拓扑的功能是一样的。

(3)10BROAD36。10BROAD36 是 8023 中惟一针对宽带系统的规范,它采用双电缆带宽或中分带宽的 75 瓯姆 CATV 同轴电缆。从端出发的段的最大长度为 1800m,由于是单向传输,所以最大的端一端距离为 3600m。

(4)10BASE-F。10BASE-F 是 8023 中关于以光纤作为媒体的系统的规范。该规范中,每条传输线路均使用一对光纤,每条光纤采用曼彻斯特编码传输一个方向上的信号。每一位数据经编码后,转换为一对光信号元素(有光表示高、无光表示低),所以,一个 10Mbps 的数据流实际上需要 20Mbaud 的信号流。

令牌环工作原理

令牌环的结构

令牌环在物理上是一个由一系列环接口和这些接口间的点一点链路构成的闭合环路,各站点通过环接口连到网上。对媒体具有访问权的某个发送站点,通过环接口出径链路将数据帧串行发送到环上;其余各站点边从各自的环接口人径链路逐位接收数据帧,

同时通过环接口出径链路再生、转发出去,使数据帧在环上从一个站点至下一个站地环行,所寻址的目的站点在数据帧经过时读取其中的信息:最后,数据帧绕环一周返回发送站点,并由其从环上撤除所发的数据帧。

由点一点链路构成的环路虽然不是真正意义上的广播媒体,但环上运行的数据帧仍能被所有的站点接收到,而且任何时刻仅允许一个站点发送数据,因此同样存在发送权竞争问题。为了解决竞争,可以使用一个称为令牌(Token)的特殊比特模式,使其沿着环路循环。规定只有获得令牌的站点才有权发送数据帧,完成数据发送后立即释放令牌以供其它站点使用。由于环路中只有一个令牌,因此任何时刻至多只有一个站点发送数据,不会产生冲突。而且,令牌环上各站点均有相同的机会公平地获取令牌。

令牌环的操作过程

(1)网络空闲时,只有一个令牌在环路上绕行。令牌是一个特殊的比特模式,其中包含一位“令牌/数据帧”标志位,标志位为“旷”表示该令牌为可用的空令牌,标志位为“1”表示有站点正占用令牌在发送数据帧。

(2)当一个站点要发送数据时,必须等待并获得

一个令牌,将令牌的标志位置为“1”,

随后便可发送数据。

(3)环路中的每个站点边转发数据,边检查数据帧中的目的地址,若为本站点的地址,便读取其中所携带的数据。

(4)数据帧绕环一周返回时,发送站将其从环路上撤消。同时根据返回的有关信息确定所传数据有无出错。若有错则重发存于缓冲区中的待确认帧,否则释放缓冲区中的待确认帧。

(5)发送站点完成数据发送后,重新产生一个令牌传至下一个站点,以使其它站点获得发送数据帧的许可权。

环长的比特度量

环的长度往往折算成比特数来度量,以比特度量的环长反映了环上能容纳的比特数。假如某站点从开始发送数据帧到该帧发送完毕所经历的时间,等于该帧从开始发送经循环返回到发送站点所经历的时间,则数据帧的所有比特正好布满整个环路。换言之,当数据帧的传输时延等于信号在环路上的传播时延时,该数据帧的比特数就是以比特度量的环路长度。

实际操作过程中,环路上的每个接口都会引人延迟。接口延迟时间的存在,相当于增加了环路上的信

号传播时延,也即等效于增加了环路的比特长度。所以,接口引人的延迟同样也可以用比特来度量。一般,环路上每个接口相当于增加 1 位延迟。由此,可给出以比特度量的环长计算式:

环的比特长度=信号传播时延×数据传输速率+接口延迟位数

=环路媒体长度×5(us/Km)×数据传输速率+接口延迟位数

式中 5us/km 即信号传播速度 200m/us 的倒数。例如,某令牌环媒体长度为 10Km,数据传输速率为 4Mbps,环路上共有 50 个站点,每个站点的接口引人 1 位延迟,则可计算得:

环的比特长度=10(Km)×5(μs/km)×4(Mbps)+1(bit)×50

=10×5×10-6×4×106+1×50

=200+50=250(bit)

如果由于环路媒体长度太短或站点数太少,以至于环路的比特长度不能满足数据帧长度的要求,则可以在每个环接口引人额外的延迟,如使用移位寄存器等。

令牌环的维护

令牌环的故障处理功能主要体现在对令牌和数

据帧的维护上。令牌本身就是比特串,绕环传递过程中也可能受干扰而出错,以至造成环路上元令牌循环的差错;另外,当某站点发送数据帧后,由于故障而无法将所发的数据帧从网上撤消时,又会造成网上数据帧持续循环的差错。令牌丢失和数据帧无法撤消,是环网上最严重的两种差错,可以通过在环路上指定一个站点作为主动令牌管理站,以此来解决这些问题。

主动令牌管理站通过一种超时机制来检测令牌丢失的情况,该超时值比最长的帧为完全遍历环路所需的时间还要长一些。如果在该时段内没有检测到令牌,便认为令牌已经丢失,管理站将清除环路上的数据碎片,并发出一个令牌。

为了检测到一个持续循环的数据帧,管理站在经过的任何一个数据帧上置其监控位为 1,如果管理站检测到一个经过的数据帧的监控位已经置为 1,便知道有某个站未能清除自己发出的数据帧,管理站将清除环路上的残余数据,并发出一个令牌。

令牌环的特点

令牌环网在轻负荷时,由于存在等待令牌的时间,故效率较低;但在重负荷时,对各站公平访问且效率高。

考虑到帧内数据的比特模式可能会与帧的首尾

定界符形式相同,可在数据段采用比特插入法或违法码法,以确保数据的透明传输。

采用发送站点从环上收回帧的策略,具有对发送站点自动应答的功能;同时这种策略还具有广播特性,即可有多个站点接收同一数据帧。

令牌环的通信量可以加以调节,一种方法是通过允许各站点在其收到令牌时传输不同量的数据,另一种方法是通过设定优先权使具有较高优先权的站点先得到令牌。