

路由器和网络互联

陈虹 芦康俊 (郑州解放军信息工程学院通信工程系 450002)

摘要:本文介绍了网络互联的关键设备——路由器的内部结构和工作过程。介绍了网络互联原理及路由器所起的作用。

关键词:路由器 网络互联 IP协议 路由算法 网络安全

路由器在网络互联中起着至关重要的作用。全球最大的计算机网络 Internet 就是由路由器连接起来的众多计算机网络组成的。可以说,没有路由器,就没有今天的 Internet。

路由器和中继器、网桥、网关等同属网络互联设备。不同的是:中继器工作于物理层;网桥工作于数据链路层;路由器工作于网络层;而网关则工作于运输层之上。

一、路由器种类

路由器种类繁多,有不同的分类方法。

按结构形式分有:插卡式及独立机箱式路由器。

按支持的网络层协议分有:IP路由器、IPX路由器、CLNP路由器、多协议路由器。

按在网络中所处的位置分有:主干路由器、区域边界路由器、区内路由器、局域网路由器。

二、路由器如何连接异种网络

路由器有很强的异种网互联能力。它所连接的网络其最低二层的协议可互不相同,它们通过路由器的第三层得到统一。

为了实现网络的互联,路由器必须完成以下功能:

1. 地址映射

实现不同的网络地址与子网物理地址的映射。如 IP 地址和以太网地址之间的映射。

路由器在网上传输数据包的过程一般如下:路由器检查信息包的协议地址(如 IP 地址),对于知道下一站该往哪儿去的信息包,路由器将其目的地址改为下一站的物理地址(MAC 地址),发送给下一站。对于不知道下一站该往哪儿去的信息包,路由器一般将其丢弃。该过程又称“交换”。下一站如仍是路由器,则执行同样过程,直到信息包到达最终的目的主机。信息包在网络中传递

时,它的物理地址不断改变,而协议地址不变。

那么,路由器是如何根据协议地址知道下一站的物理地址的呢?

对于支持 IP 协议的路由器来说,IP 层的 ARP 子协议负责把 IP 地址转换为物理地址。ARP 动态寻找物理地址的过程如下:假设网上 A 机已知下一目标为 B 机,并已知 B 机的 IP 地址。A 机广播一含有 B 机 IP 地址的 ARP 包,由于是广播方式,网上所有机器都收到了该 ARP 请求,但是只有 B 机识别出是自己的 IP 地址,予以接收和响应,向 A 机发回 ARP 响应,送回 B 机的物理地址。ARP 只适用于具有广播功能的网络。

IP 层的 RARP 子协议负责把物理地址转换为 IP 地址。网络在使用无盘工作站时,无盘站有自己的物理地址,但并不知道自己的 IP 地址。为了从物理地址找 IP 地址,在网络上至少要设置一台 RARP 服务器,网络管理员必须事先把网卡的物理地址和相应的 IP 地址加入到 RARP 数据库中。无盘站要寻找自己的 IP 地址,经广播一个 RARP 请求包给网络上所有主机,而由 RARP 服务器予以响应。有的边界路由器,其 IP 寻址依赖于中心路由器,所以也要用 RARP 向中心路由器请求 IP 地址。

2. 数据转换

路由器应实现数据的分段。不同的网络所支持的最大帧长不同,互联网协议必须提供分段和重组功能。若无分段和重组功能,整个互联网就只能按照所允许的某个最短分组进行传输,这就要大大降低其他一些网络的效率。

路由器承担数据分段工作,它把较长的 IP 数据报的数据部分分成几个较小的单元,加上适当的报头,以便信宿机完成数据重组。路由器不承担重组工作。

3. 协议转换

实现不同的网络之间协议转换的功能。路由器连接的可能是异种网络,因此它必须能对其互联的两个异构

网络的帧格式进行转换。如图所示为 Token ring 网上的主机 A 经公共 WAN(帧中继)与 Ethernet 网上主机 B 的通信过程。路由器完成了不同的网络之间协议转换。

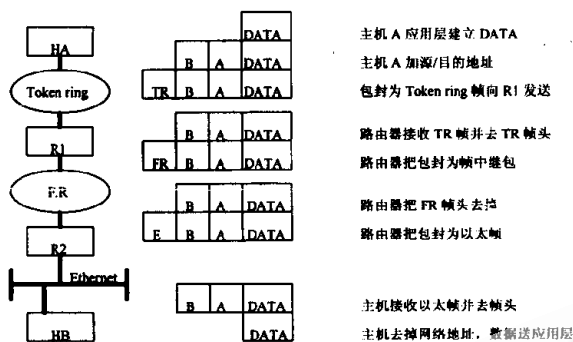


图 1 路由器实现协议转换

三、路由算法和路由协议

路由器主要担负着互联网间的最佳寻径及数据报的传送工作。后者又称为“交换”,其过程和原理都较简单,路由选择则很复杂。

路由选择可以基于各种不同的开销(如网络时延等)或几种开销的综合。所谓最佳路径,是指在特定开销意义上的最佳。

在路由器中设置某种路由协议后,路由器就能按照一定的路由算法建立并维护路由表,根据路由表的信息选择路径。路由表的维护是通过传递路由更新信息进行的。路由更新信息可定期发送,或当网络拓扑发生变化,影响了路径后发送。路由更新信息包括路由表的部分或全部信息。

路由协议种类很多,如 Rip, OSPF, EGP, BGP 及 Cisco 公司的 IGRP, EIGRP 和 ISO/OSI 的 ES-IS, IS-IS, IDRP 等。

有两种基本的路由算法:链路状态法(L-S 算法)和距离矢量法(V-D 算法)。每种路由协议都采用其中的一种算法,如 Rip, EGP 采用 V-D 算法,OSPF 采用 L-S 算法,或同时采用两种算法,如 EIGRP。

链路状态法利用“洪泛法”将路由信息发向网络各节点。每个路由器只发送与它相连的那一部分链路状态的路由表。距离矢量法要求每个路由器发送它整张路由表,但仅发送给相邻的路由器。距离矢量法更易产生路由循环;链路状态法则大大增加了控制通信量,而且更难

计算。撇开它们的不同之处,这两种算法在很多场合运行良好。

路由协议可以分为非分级和分级两类。如 OSPF 是分级的, Rip 是非分级的。在分级系统中,有些路由器组成路由干线,并将局部的节点群划分成域。来自非干线的信息包被传递至干线路由器,在干线上传输,直到到达终点所在的域,这时它们经过最后一个干线路由器,再经若干非干线路由器达到最终目的地。非干线路由器仅需同域内路由器通信,这样就简化了路由算法,也减少了路由更新的通信量。非分级算法则所有路由器平等,均需密切注视其他路由器的情况。

路由器还支持对两个不同路由协议之间的相互学习。当路由器跨越运行不同路由协议的两个网络系统时,路由器可以通过对两个异构协议用相互学习的办法得到统一。

四、路由器的其他功能

由于路由器具有网络层智能,因此它还具有分组过滤、流量控制、网络管理、数据压缩、优先、加密等功能。

路由器具有分组过滤功能,是防火墙的主要组件。路由器逐一审查每份数据报,判断它是否与分组过滤规则匹配,以决定对收到的分组的取舍。

对某种服务的过滤:分组过滤规则允许路由器取舍以一个特殊服务为基础的信息流。例如 Internet 服务器在 TCP port 23 端口等待远程连接,若要封锁输入 Telnet 连接,路由器只需舍弃 TCP 目的端口值为 23 的所有分组。

对某些攻击的过滤:有些类型的攻击难以用基本分组头信息加以鉴别,因为这些攻击不属于某种服务。防止这类攻击,过滤规则要加些信息。这些信息源于:研究路由表,检查特定 IP 选项,检查特殊片段偏移等。

如源 IP 地址欺骗攻击,入侵者从伪装成一台内部主机的外部节点传送信息分组,这些分组似乎包含了内部系统的一个源 IP 地址。当这些分组到达路由器的外部接口时,只要丢弃每个含有源 IP 地址的分组就制止了这种攻击。

对源路由攻击,源站指定了一个信息分组穿越 Internet 时应取的路径。这类攻击企图绕过安全措施,并使分组沿另一路径到达目的地。只要丢弃所有包含源路由选择的分组,就可制止这种攻击。

对残片攻击,入侵者利用 IP 残片特性生成一个极小

的片断,并将 TCP 报头信息肢解成一个分离的信息分组片断。丢弃所有协议类型为 TCP/IP 片断偏移量为 1 的信息分组,就可制止这种攻击。

此外,有的路由器提供了多条传输通路的方法,从而增加了互联网的冗余度和容错性。有的路由器具有网络管理能力,使网络管理人员在集中式管理控制台上监控路由器,并查找路由器故障。

五、路由器内部结构和工作过程

工作过程:

1. 网络接口模块将收到的数据帧拷贝到接口缓冲区。
2. 查表 Fast cache 中是否有目的主机网络地址。
3. 若无,则查路由表,并初始化 Fast cache。
4. 重新封装数据帧。
5. 发往相应的网络接口模块,并由网络接口模块计算 CRC。

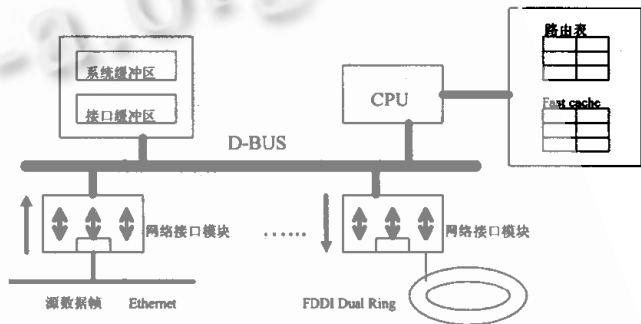


图 2 路由器内部结构框图

参考文献

- [1] Internet Protocol RFC:791
- [2] Transmission Control Protocol RFC:793
- [3] Cisco Router Architecture and Performance Analysis
- [4] 《Computer Networks 计算机网络》Aporew S Tanenbaum 清华大学出版社

(来稿时间:1998 年 1 月)