Internet网关及其实现策略

郑州1001信箱 450002 李艳霞

本文以较浅显的语言概述了Internet的网关概念及其实现策略。包括网关模型、网关特性、网关相关协议（特别是ICMP协议）、网关算法以及O&M的要求几个方面，旨在让读者对Internet网关从整体上有一个大概了解，为以后更深入的研究和工作打下基础。

前言

随着国际互联网的日益发展，人们在网络技术的领域内不断探索。其实网络技术的发展，根本目的是提高网络的服务质量，即让网络提供尽可能高的带宽，尽可能少的出错率，尽可能低的延迟，以及人们越来越关注的更高的网络安全需求。而Internet网关技术在这一系列的问题中处于不可忽视的地位，因此，我们将在这里对Internet网关的相关技术作一个简明的阐述。

首先，需要对一些可能引起混淆的术语作一下定义：

数据包（Packet）：数据包是物理网络上的一个传输单元。

数据报（Datagram）：数据报是IP协议的一个传输单元，为了穿过一个特定的网络，一个数据报将被打包进一个数据包中。

路由器（Router）：一个路由器是一个交换器（switch），它负责从输入接口接收数据传输单元，并根据这些单元中的地址将它们“路由”到适当的输出接口。路由器可设置在不同的协议层上，比如IMPs（Interface Message Processors）就是数据包层（packet-level）路由器。

网关（Gateway）：网关与路由器的概念上的区别已日益模糊。过去，网关被定义成在较低层上实现，仅实现简单交换（与路由器相比，没有智能的功能）的网络设备。现在，就有建立在应用层上的应用网关，比如我们常说的代理服务器，而上述路由器也有在链路层上实现的，如IMPs。并且，随着第三层交换概念的出现，网关、路由器思想覆盖的范围更广大了。

网络与网关

传统上，我们将网络分为LAN（局域网，Local-area Network）和WAN（广域网，Wide-area Network）两类。在Internet模型中，构成的网络由被称为“网关”或IP路由器的IP数据报发送者（forwarders）相互联接在一起。在当前的应用中，网关通常由数据包交换软件来体现，这个软件运行在一个通用CPU上，同时需要特殊的硬件支持。一个网关联接着两个或更多网络，在每个网络上表现为一台在联主机。因此，它在每个相联的网络上有一个物理接口和一个IP地址。发送一个IP数据报通常需要选择下一跳网关或目标主机的地址，这就是“路由”，它依赖于网关内的一个路由数据库（Routing data-base）。这个路由数据库可以是个静态表，也可以是根据当前的网络拓扑动态更新的表。

Internet网关模型

互联LAN和WAN有两种基本模型。第一种，一个LAN被设置成一个网络地址，Internet上的所有网关必须都知道如何路由到这个网络。第二种，这个LAN占用WAN的一块地址空间，支持这种模型的网络称为“地址共享网关”或“透明网关”。我们将着重阐述第一种网关。

1.Internet网关（Internet Gateways）

这是一个IP-level路由器，它完成下列功能：

(1)与Internet协议相一致，这些协议包括IP，ICMP等。

(2)具有两个或两个以上的包交换网络（packet networks）的接口，它必须为每个相连的网络实现其所要求功能（functions），这些功能一般包括：

①打包、拆包（en/decapsulate）由相连网络建立的IP数据报（比如以太网包头和校验和）

②接收、发送网络所支持的最大尺寸的IP数据报，这个大小称为网络的MTU（Maximum Transmission Unit）。

③将IP目标地址转换成适当的网络层（network-level）地址（比如以太网硬件地址）

④负责网络的流控制和差错指示。

(3)接收并向前发送（forward）Internet 数据报。重点是缓冲器管理、拥塞控制和公平性。

①识别各种错误条件并按需产生ICMP差错和信息报文。

②丢弃TTL（time-to-live） 域为零的数据报。

③必要时将数据报分段，以适应下一跳网络的MTU。

(4)参照它的路由数据库信息，为每个IP数据报选择下一跳的目标。

(5)支持IGP（内部网关协议）实现与同一自治系统（Autonomous System)中其他网关的分布式路由和可达算法。另外，一些网关还需要支持EGP（外部网关协议）以完成与其他自治系统的拓扑信息交换。

(6)提供系统支持的功能，包括加载（load）、调试（debug）、状态报告（status report）、意外报告和控制（exception report and contol）。

2. 内嵌式网关（Embedded Gateways）

一个网关可以是一台独立的计算机系统，只完成路由功能；它也可以将路由功能内嵌到

一个联接多个网络的主机操作系统中。内嵌式网关好象使互联更简单了，但它却带来了一系列的隐患。

(1)如果一台主机只有一个网络接口，那么它不能作为网关。

(2)如果一台多宿主（multihomed）主机用作网关，它必须处理“所有”相关的网关需求。这种网关的管理员通常要求能够维护和更新网关的代码。

(3)一旦一台主机运行了内嵌式网关代码，它就成为互联网系统的一部分。因此，软件错误或主机配置错误将阻碍与其他主机间的通信。

(4)如果一台运行着内嵌式网关的主机现在用于其他服务，两种应用模式的O&M（Operation and Maintenance）需求可能产生致命冲突。

3. 透明网关（Transparent Gateways）

它的基本思想是位于透明网关“后面（behind)”的LAN主机占用位于网关“前面（infront)”的WAN的地址。这种方式只适于物理上（和拓扑上）有限的环境。它需要某种形式的WAN网络层的逻辑地址（也就是说，LAN环境下的所有IP地址映射到一些（通常为一个）WAN物理地址）。

网关的特性

每个Internet网关必须完成前面所述的功能。但是，一个供应商可以在强度、复杂度和部件上为不同的网关产品进行不同的选择。出于技术和物理的原因，人们渐渐倾向于在四周（edge）带着LAN“边缘”（LAN-fringe）的全球互联系统。位于全球互联系统的网关通常需要：

(1)先进的路由和发送（forwarding）算法：这些网关需要高度动态并提供服务类型（typeof service）选项的路由算法。

(2)高可用性：这些网关应该具有高可靠性，提供每天24小时、每周7天的服务。如果 出现错误必须快速恢复。

(3)先进的O&M特性：网关通常由一个区域或国家监视中心远程操作，它需要为监视、流 量测定、错误诊断等事件提供相应的手段。

(4)高性能：远程线路由全双工的56Kbps到DS1（1.5Mbps）到DS3(45Mbps)，LAN也从10Mbps（ETHERNET）到FDDI（100Mbps)。网络媒体工艺在不断提高，未来将会出现更高的速度。用于“LAN fringe”（如校园网）的网关通常对诸如性能、可提供性和可维护性要求不太严格，这类网关的设计就注重较低的平均延迟和较好的健壮性能，以及对延迟和服务类型敏感的资源管理。在这种环境下，O&M较不正式，对特殊情况有较多的手工静态配置，有较多功能依赖其他供应商的网关；路由机制需要非常灵活，但不需要特别地动态。

网关所需协议

互联网结构使用数据报网关互联网络，下面描述一个网关需要实现的各种协议。

1. Internet Protocol（IP）IP是应用于Internet系统中的最基本的数据报协议。按照当前的网关需求，以下的IP组件可被忽略（尽管它们可能在将来时需要）：服务类型域，安全选项，流ID选项。对网关而言，实现松散的（loose）和严格（strict）的源路由是很重要的，而记录路由（Record Route） 和时间戳（Timestamp）选项是有用的诊断工具，是所有网关必须支持的功能。Internet 模型要求一个网关能够在需要的时候分段（fragment）数据报，以匹配下一网络的MTU。虽然这时的重组工作由上层完成，但是网关也通常收到一些发给它本身的IP数据报（如ICMP请求/应答报文）。相对这些数据报，网关相当于目标主机，则重组由网关来执行。因

此，每个网关必须有一个重组缓冲器（Reassembly buffer），它的大小应不小于MTU的最大值或者576，这个缓冲器用于重组发给网关的ICMP Request/Reply报文（它是用于支持象无盘工作站这样的自配置系统，使它能够在启动时刻找到它的IP网络地址，这个功能由RARP实现更好）、路由更新报文、监视和控制报文。

一个发向网关的数据报的目标地址可以使用网关的任何一个地址，而不管这个数据报从哪个接口进入。在五类IP地址中，网关一般忽略所有目标为D类和E类IP地址的数据报（除非该网关用于实验），ICMP的目标不可达报文和重定向报文也不会因此而产生。

2. 网际控制报文协议（ICMP）

ICMP是一个用于传送建议和差错报文的辅助协议。由于网关需要对它们进行处理，这里详细介绍一下它的种类。

(1)ICMP差错报文

①目标不可达（destination unreachable）：一个数据报由于目标不可达或主机下机而不能发送，网关发送此报文，并指明是主机不可达还是网络不可达。如果是网络不可达，则表明该网关的路由数据库没有给出下一跳目标，或所有的路径不可用。如果是主机不可达，则表明该主机下机，或者是没有可用的路径到达目标主机所在的子网。

②重定向报文（redirected）：网关发送重定向报文给同一网络上的主机，用于改变主机上为特定数据报指定的网关路由。

③报源抑制报文（source quench）：所有的网关必须能够在由于拥塞不得不丢弃IP数据报的之前发送ICMP源抑制报文。这会增加反向带宽开销和网关CPU时间，因此，网关必须能控制发源抑制报文的频率。注意：如果一个网关发送一个数据报给另一个网关而产生了报源抑制报文，那么这个数据报可能是一个EGP更新信息。

④时间超时（time exceeded）：当网关由于一个数据报的TTL为零而丢弃它时，或当一个被分段的数据报不能在一定时间限制内完成重组时发送。

⑤参数问题（parameter）：当一个ICMP报文的某个选项自变量不正确时，产生该报文。

(2)ICMP信息请求/回答报文

①地址掩码(address mask)：主机和网络为了知道自己的（子网）掩码，发送一个请求报文给网关，然后接收一个回答报文获得信息。

②时间戳（timestamp）：它在网络问题诊断中非常有用。它的标准度量是从GMT午夜开始以毫秒计。

③信息请求/回答（information）：它们用于支持自配置系统（如无盘工作站）在启动时找到自己的网络地址。

④应答请求/回答（echo）：网关必须支持ICMP Echo报文，因为它是一个极为有用的诊断工具。一个网关必须能够接收、重组、应答一个ICMP应答请求数据报。

3. 外部网关协议（EGP）

它是一个用于在网关自治系统（AS）之间交换可达信息的协议。当一个自治系统的网关采用动态路由算法时，它的路由数据库必须与EGP应用相结合。当一个网络根据路由算法被确定为不可达后，通过EGP，该网络就不会向其他自治系统报告为可达，这将最小化发向“黑洞（black hole）”的可疑流量，并确保对其他系统的资源的公平利用。

4. 地址解析协议（ARP）

ARP是用于完成在LAN硬件地址和Internet地址之间的动态地址转换。它基于本地网络广播机制。

5. 内部网关协议（IGP）

在Internet网关中最常用的IGP有：

(1)GGP（网关到网关协议）：它的度量以网关间的跳数计，采用分布式最短路径算法。

(2)SPF（最短路径优先协议）：它的路由数据库是复制的而不是分布式的，不会产生分布式算法的全球汇聚（globle convergency）问题。

(3)RIP（路由信息协议）：它非常简单，接近“开放式IGP”（即可用于不同厂家的网关间），但尚未成为标准。它以跳为计量，并象GGP那样定期广播路由信息。

(4)IGMP（网际组管理协议）：IP协议的一个扩展是提供网际多点播送（multicasting），这个传播者称为“多点播送代理”，而接收的这组主机称为“主机组”，这样的主机代理协议称为IGMP，它负责一个主机的加入和离开、或创建一个组。每个主机组都由一个D类IP地址区分。

(5)此外还有HELLO协议和监视（monitor）协议。

构成的网络类型

一个网关必须能够在普遍类型的网络上传输IP数据包，必须能够发送和接收任何大小直到任一相联网络的MTU的IP数据报。这些网络包括：X.25上的公共数据网，1822LH、DH或HDH上的ARPANET，DDN标准X.25上的ARPANET，IEEE802上的以太网，串行线协议。关于这些网络的介绍从略。■