NAT———网络地址翻译

Internet 的飞速发展，网上丰富的资源产生着巨大的吸引力。接入 Internet、访问 Internet 成为当今信息业迫切的需求。

但这受到 IP 地址的许多限制。首先，许多局域网在未联入 Internet 之前，就已经运行许多年了，局域网上有了许多现成的资源和应用程序，但它的 IP 地址分配不符合 Internet 的国际标准，因而需要重新分配局域网的 IP 地址，这无疑是劳神费时的工作；其二，随着 Internet 的膨胀式发展，其可用的 IP 地址越来越少，要想在 ISP 处申请一个新的 IP 地址已不是很容易的事了。这不仅仅是费用的问题，而是 IP 地址的现行标准 IPv4 决定的。当然，随着 IPv6 的出台，这个问题应当能够得到解决。但从 IPv4 到 IPv6 的升级不是一两天就能完成的。

NAT（网络地址翻译）能解决不少令人头疼的问题。它解决问题的办法是：在内部网络中使用内部地址，通过 NAT 把内部地址翻译成合法的 IP 地址，在 Internet 上使用。其具体的做法是把 IP 包内的地址域用合法的 IP 地址来替换。

NAT 功能通常被集成到路由器、防火墙、ISDN 路由器或者单独的 NAT 设备中。NAT 设备维护一个状态表，用来把非法的 IP 地址映射到合法的 IP 地址上去。每个包在 NAT 设备中都被翻译成正确的 IP 地址发往下一级，这意味着给处理器带来了一定的负担。但这对于一般的网络来说是微不足道的，除非是有许多主机的大型网络。

需要注意的是，NAT 并不是一种有安全保证的方案，它不能提供类似防火墙、包过滤、隧道等技术的安全性，仅仅在包的最外层改变 IP 地址。这使得黑客可以很容易地窃取网络信息，危及网络安全。

NAT 有三种类型：静态 NAT（staticNAT）、NAT 池（pooledNAT）和端口 NAT（PAT）。其中静态 NAT 设置起来最为简单，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。而 NAT 池则是在外部网络中定义了一系列的合法地址，采用动态分配的方法映射到内部网络。PAT 则是把内部地址映射到外部网络的一个 IP 地址的不同端口上。根据不同的需要，各种 NAT 方案都是有利有弊。

■使用 NAT 池

使用 NAT 池，可以从未注册的地址空间中提供被外部访问的服务，也可以从内部网络访问外部网络，而不需要重新配置内部网络中的每台机器的 IP 地址。例如，建立在 NT＋IIS 服务器上的内部试验子网 192．168．0．0，其网络地址属于 B 类保留地址。作为企业网的一个子网，其 IP 地址不分配给企业网上的设备而仅仅局限在试验子网的设备上

isco4700 路由器。其中的路由器可以把内部网和企业网连接起来，使之能相互访问。在内部网中不要使用 RIP 协议，因为使用 RIP 后，内部网络相对外部来说变得不可见了。

这样，本地信息可以相互访问了，但由于 192．168．0．0 属于保留地址，故不能直接访问 Internet。所以在路由器中设置一个 NAT 池，用来翻译来自内部网络的 IP 包，把它的 IP 地址映射成地址池（pooledaddresses）中的合法 IP 地址。那么，内部网可以访问 Internet 上的任何服务器，Internet 上的任何主机也能通过 TCP 或 UDP 访问到内部网。

采用 NAT 池意味着可以在内部网中定义很多的内部用户，通过动态分配的办法，共享很少的几个外部 IP 地址。而静态 NAT 则只能形成一一对应的固定映射方式。该引起注意的是，NAT 池中动态分配的外部 IP 地址全部被占用后，后续的 NAT 翻译申请将会失败。庆幸的是，许多有 NAT 功能的路由器有超时配置功能。例如在上述的 Cisco4700 中配置成开始 15 分钟后删除当前的 NAT 进程，为后续的 NAT 申请预留出外部 IP 地址。通过试验表明，一般的外部连接不会很长，所以短的时间阈值也可以接受。当然用户可以自行调节时间阈值，以满足各自的需求。

NAT 池提供很大灵活性的同时，也影响到网络原有的一些管理功能。例如，SN？MP 管理站利用 IP 地址来跟踪设备的运行情况。但使用 NAT 之后，意味着那些被翻译的地址对应的内部地址是变化的，今天可能对应一台工作站，明天就可能对应一台服务器。这给 SNMP 管理带来了麻烦。一个可行的解决方案就是把划分给 NAT 池的那部分地址在 SNMP 管理平台上标记出来，对于这些不响应管理信号的地址不予报警，如同它们被关掉了一样。

■使用 PAT

PAT 在远程访问产品中得到了大量的应用，特别是在远程拨号用户使用的设备中。PAT 可以把内部的 TCP／IP 映射到外部一个注册 IP 地址的多个端口上。PAT 可以支持同时连接 64500 个 TCP／IP、UDP／IP，但实际可以支持的工作站个数会少一些。因为许多 Internet 应用如 HTTP，实际上由许多小的连接组成。

在 Internet 中使用 PAT 时，所有不同的 TCP 和 UDP 信息流看起来仿佛都来源于同一个 IP 地址。这个优点在小型办公室（SOHO）内非常实用，通过从 ISP 处申请的一个 IP 地址，将多个连接通过 PAT 接入 Internet。实际上，许多 SOHO 远程访问设备支持基于 PPP 的动态 IP 地址。这样，ISP 甚至不需要支持 PAT，就可以做到多个内部 IP 地址共用一个外部 IP 地址上 Internet。虽然这样会导致信道的一定拥塞，但考虑到节省的 ISP 上网费用和易管理的特点，用 PAT 还是很值得的。

■基于 NAT 的负载平衡

以上所谈论的均是关于使用 NAT 和 PAT 来把内部 IP 地址转换成外部合法的 IP 地址使用。下面介绍 NAT 的另一个运用：作为用于负载平衡的 DNS 系列服务器（DNSround－robin）的一个替代品。DNS 系列服务器解决了多个 IP 地址共用一个域名的问题。它会在响应 DNS 申请时跳跃式地寻找可用的 IP 地址。达到的效果就是一个域名可以对应多个 IP 地址。这种功能可以应用在一个 HTTP 服务器群中，利用它可以平衡多个服务器的负载。但是这里还有一个问题，IP 客户端会在本地缓冲 DNS／IP 地址解析，从而使它的后续的申请都会到达同一个 IP 地址，减弱了 DNS 系列服务器的作用。

使用基于 NAT 的负载平衡方案，则可以避免这个问题。路由器或其它 NAT 设备把需要负载平衡的多个 IP 地址翻译成一个公用的 IP 地址，每个 TCP 连接被 NAT 送到一个 IP 地址，而后续的 TCP 连接则被 NAT 送到下一个 IP 地址。真正实现了负载平衡。当然，基于 NAT 的负载平衡只能在 NAT 上实现，而不能在 PAT 上实现。

■安全问题

当 NAT 改变包的 IP 地址后，需要认真考虑这样做对安全设施带来的影响。

对于防火墙，它利用 IP 地址、TCP 端口、目标地址以及其它在 IP 包内的信息来决定是否干预网络的连接。当使用了 NAT 之后，可能就不得不改变防火墙的规则，因为 NAT 改变了源地址和目的地址。

在许多配置中，NAT 被集成在防火墙系统之中，提供访问控制和地址翻译的功能。不要把 NAT 设在防火墙之外，因为黑客可以轻易地骗过 NAT，让 NAT 认为它是一个授权用户，从而进入网络。

若企业网中使用了 VPN（虚拟专用网），并用 IPSec 进行加密安全保证，那么错误地设置 NAT 将会破坏 VPN 的功能。把 NAT 放在受保护的 VPN 内部，而不是在中间。因为 NAT 改变 IP 包内的地址域，而 IPSec 规定一些信息是不能被改变的。若 IP 地址被改变了，IPSec 就会认为这个包是伪造的，拒绝使用。

虽然 NAT 带来了许多优越性，例如使现有网络不必重新编址、减少了 ISP 接入费用，还可以起平衡负载的作用，但 NAT 潜在地影响到一些网络管理功能和安全设施，这就需要谨慎地使用它。