专用 Internet 地址分配

目录

简介

本文档基于RFC 1597 ，它不向网络中的专用主机分配全局唯一的IP地址，从而帮助您节省IP地址空间。您仍然可以允许网络中所有主机之间以及Internet中所有公共主机之间的完全网络层连接。

使用IP的主机分为三类：

- 不需要访问其他企业或整个Internet的主机。这些主机可以使用在其网络中唯一但在外部网络中可能不唯一的IP地址。
- 需要访问可由应用层网关处理的有限外部服务（例如，电子邮件、FTP、网络新闻、远程登录）的主机。出于隐私或安全原因，其中许多主机可能不需要或不希望不受限制的外部访问（通过IP连接提供）。与第一类别中的主机一样，它们可以使用在网络中唯一但在外部网络中不唯一的IP地址。
- 需要通过IP连接在企业外部访问网络层的主机。只有这些主机需要全局唯一的IP地址。

许多应用程序只需在一个网络内进行连接，甚至不需要大多数内部主机的外部连接。在大型网络中，主机通常在不需要网络层连接时使用TCP/IP。以下是一些可能不需要外部连接的示例：

- 到达和离开的大型机场通过TCP/IP显示可单独寻址的信息。这些显示器不太可能可以从其他网络直接访问。
- 大型组织，如使用TCP/IP进行内部通信的银行和零售连锁店。大量本地工作站，如收银机、货币机和办公室设备，很少需要外部连接。
- 使用应用层网关（防火墙）连接到Internet的网络。内部网络通常不能直接访问Internet，因此只有一台或多台防火墙主机可从Internet中查看。在这种情况下，内部网络可以使用非唯一IP编号。
- 通过自己的专用链路通信的两个网络。通常只有非常有限的一组主机可以通过此链路相互访问。只有这些主机需要全局唯一的IP编号。
- 内部网络中路由器的接口。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

专用地址空间

互联网编号分配机构(IANA)为专用网络保留了以下三个IP地址空间块：

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

第一个块是单个A类网络号，第二个块是一组16个连续的B类网络号，第三个块是一组255个连续的C类网络号。

如果您决定使用私有地址空间，则无需与IANA或Internet注册表协调。此私有地址空间中的地址在您的网络中是唯一的。请记住，如果需要全局唯一地址空间，必须从Internet注册表获取地址。

要使用私有地址空间，请确定哪些主机不需要与外部建立网络层连接。这些主机是专用主机，使用专用地址空间。私有主机可以与网络内的所有其它主机（公有主机和私有主机）通信，但它们不能与任何外部主机建立IP连接。私有主机仍然可以通过应用层中继访问外部服务。

所有其它主机都是公有的，使用由Internet注册表分配的全局唯一地址空间。公共主机可以与网络内的其他主机通信，并且可以与外部公共主机建立IP连接。公共主机无法连接到其他网络的专用主机。

由于私有地址没有全局意义，因此有关私有网络的路由信息不会在外部链路上传播，并且具有私有源地址或目的地址的数据包不应通过此类链路转发。网络中不使用私有地址空间的路由器，特别是Internet服务提供商的路由器，应配置为拒绝（过滤）有关私有网络的路由信息。此拒绝不应视为路由协议错误。

网络中应包含对此类地址（如DNS资源记录）的间接引用。互联网服务提供商应采取措施防止此类泄露。

使用专用地址空间的优点和缺点

为整个Internet使用私有地址空间的明显优势是节省全球唯一的地址空间。使用私有地址空间也使您在网络设计方面具有更大的灵活性，因为您拥有的地址空间将比从全局唯一池获得的地址空间更多。

使用私有地址空间的主要缺点是，如果要连接到Internet，必须对IP地址重新编号。

设计注意事项

您应首先设计网络的私有部分，并为所有内部链路使用私有地址空间。然后规划公共子网并设计外部连接。

如果您的设备可以设计并支持合适的子网划分方案，请使用24位私有地址空间块，并制定具有良好增长路径的编址方案。如果子网划分存在问题，您可以使用16位C类块。

将主机从私有主机更改为公有主机需要更改其地址，在大多数情况下，还需要更改其物理连接。在可以预见这些更改的位置（机房等）中，您可能希望为公共和私有子网配置单独的物理介质，以便更轻松地进行这些更改。

连接外部网络的路由器应在链路两端设置适当的数据包和路由过滤器，以防止泄漏。您还应从入站路由信息中过滤所有专用网络，以防止在通往网络外部的专用地址空间的路由时出现不明确的路由情况。

预计需要相互沟通的组织组必须设计共同的编址计划。如果两个站点需要使用外部服务提供商进行连接，他们可以考虑使用IP隧道来防止来自专用网络的数据包泄露。

避免DNS RR泄漏的一种方法是运行两个域名服务器，一个外部服务器负责企业的所有全局唯一IP地址，另一个内部服务器负责所有IP地址，包括公有地址和私有地址。为确保一致性，这两台服务器都应接收相同的数据，外部名称服务器仅使用过滤版本。

所有内部主机（公有主机和私有主机）上的解析器仅查询内部名称服务器。外部服务器解析来自外部解析器的查询并链接到全局DNS。内部服务器将企业外部信息的所有查询转发到外部名称服务器，以便所有内部主机都可以访问全局DNS。这样，有关专用主机的信息就无法到达外部解析器和名称服务器。

安全考虑

虽然使用私有地址空间可以提高安全性，但它不能替代专用的安全措施。

结论

使用此方案，许多大型网络只需从全局唯一IP地址空间获得相对较小的地址块。Internet通过节约全球唯一的地址空间而大大受益，而网络则受益于相对较大的私有地址空间所提供的更高的灵活性。

相关信息

- IP 路由协议支持页
- IP 路由 支持页
- 技术支持和文档 - Cisco Systems