# 專用網的地址分配

## 目錄



## 簡介

本檔案基於RFC 1597 ，它不會將全球唯一的IP位址分配至網路中的私人主機，因此可協助您節省IP位址空間。您仍然可以允許網路中所有主機之間以及Internet中所有公共主機之間的完整網路層連線。

使用IP的主機分為三類：

- 不需要訪問其他企業中的主機或整個Internet的主機。這些主機可以使用其網路中唯一的IP地址，但在外部網路中可能不是唯一的IP地址。
- 需要訪問應用層網關可處理的有限外部服務（例如，電子郵件、FTP、網路新聞、遠端登入）的主機。出於隱私或安全原因，其中很多主機可能不需要或不需要不受限制的外部訪問（通過IP連線提供）。與第一類中的主機一樣，它們可以使用網路內唯一的IP地址，但外部網路之間不能使用。
- 需要通過IP連線提供的企業外部網路層訪問的主機。只有這些主機需要全域性唯一的IP地址。

許多應用程式只需要一個網路中的連線，甚至不需要大多數內部主機的外部連線。在大型網路中，當主機不需要網路層連線時，通常使用TCP/IP。以下是一些可能不需要外部連線的示例：

- 一個大型機場，它的到達和離開顯示可通過TCP/IP單獨定址。這些顯示器幾乎不需要從其他網路直接訪問。
- 銀行和零售連鎖店等大型組織使用TCP/IP進行內部通訊。大量的本地工作站，如收銀機、貨幣機和文書崗位裝置，很少需要外部連線。
- 使用應用層網關（防火牆）連線到Internet的網路。內部網路通常不能直接訪問Internet，因此Internet中只能看到一個或多個防火牆主機。在這種情況下，內部網路可以使用非唯一的IP號。
- 通過自己的專用鏈路進行通訊的兩個網路。通常只有非常有限的一組主機可通過此鏈路相互訪問。只有這些主機需要全域性唯一的IP號。
- 內部網路中路由器的介面。

# 必要條件

## 需求

本文件沒有特定需求。

## 採用元件

本文件所述內容不限於特定軟體和硬體版本。

## 慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

# 專用地址空間

Internet編號指派機構(IANA)為專用網路預留了以下3塊IP地址空間：

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

第一塊是單個A類網路號，第二塊是16個連續的B類網路號的集合，第三塊是255個連續的C類網路號的集合。

如果您決定使用專用地址空間，則無需與IANA或Internet登錄檔協調。此私有地址空間內的地址僅在網路中是唯一的。請記住，如果您需要全域性唯一的地址空間，您必須從Internet登錄檔獲取地址。

要使用私有地址空間，請確定哪些主機不需要與外部建立網路層連線。這些主機是專用主機，並使用專用地址空間。私有主機可以與網路中的所有其它主機通訊，包括公有主機和私有主機，但是它們不能與任何外部主機建立IP連線。專用主機仍可通過應用層中繼訪問外部服務。

所有其他主機都是公共的，並且使用由Internet登錄檔分配的全域性唯一地址空間。公共主機可以與網路中的其他主機通訊，並且可以與外部公共主機建立IP連線。公共主機無法連線到其他網路的專用主機。

由於私有地址不具有全域性含義，因此有關私有網路的路由資訊不會在外部鏈路上傳播，具有私有源地址或目標地址的資料包也不應通過此類鏈路轉發。網路中不使用私有地址空間的路由器（尤其是Internet服務提供商的路由器）應配置為拒絕（過濾掉）有關私有網路的路由資訊。不應將拒絕視為路由協定錯誤。

網路應包含對此類地址的間接引用（如DNS資源記錄）。網際網路服務提供商應採取措施防止此類洩露。

# 使用私有地址空間的優缺點

為整個網際網路使用私有地址空間的明顯優勢是保留了全域性唯一地址空間。使用專用地址空間還為您提供了更大的網路設計靈活性，因為您將擁有比從全域性唯一地址池所能獲得的更多地址空間

。

使用私有地址空間的主要缺點是，如果要連線到Internet，您必須對IP地址重新編號。

## 設計注意事項

您應該首先設計網路的專用部分，並為所有內部鏈路使用專用地址空間。然後規劃公共子網並設計外部連線。

如果可以設計合適的子網劃分方案並且您的裝置支援該方案，請使用24位塊私有地址空間，並制定具有良好增長路徑的編址計畫。如果存在子網劃分問題，您可以使用16位C類塊。

將主機從私有更改為公有需要更改其地址，在大多數情況下還需要更改其物理連線。在可以預知此類更改的位置（機房等），您可能希望為公共子網和專用子網配置單獨的物理介質，以簡化這些更改。

連線外部網路的路由器應該在鏈路兩端設定適當的資料包和路由過濾器，以防止洩漏。您還應該從入站路由資訊中過濾任何私有網路，以防止出現路由不明的情況（如果通往私有地址空間的路由指向網路外部）。

預測需要相互溝通的組織團隊必須設計一個通用編址計畫。如果需要使用外部服務提供商連線兩個站點，則可以考慮使用IP隧道來防止來自專用網路的資料包洩漏。

避免DNS RR洩漏的一種方法是運行兩個名稱伺服器，一個外部伺服器負責企業的所有全域性唯一IP地址，一個內部伺服器負責所有IP地址，包括公有地址和私有地址。為了確保一致性，這兩個伺服器應該接收相同的資料，其中外部名稱伺服器僅使用篩選後的版本。

所有內部主機（包括公共主機和專用主機）上的解析程式只查詢內部名稱伺服器。外部伺服器解析來自外部解析器的查詢，並連結到全域性DNS。內部伺服器將企業外部的所有資訊查詢轉發到外部名稱伺服器，以便所有內部主機都可以訪問全域性DNS。這樣，有關專用主機的資訊不會到達外部解析器和名稱伺服器。

## 安全注意事項

雖然使用私有地址空間可以提高安全性，但它不能替代專用安全措施。

## 結論

使用此方案，許多大型網路只需要來自全域性唯一IP地址空間的相對較小的地址塊。Internet一般通過全球唯一地址空間的保護而受益，而網路則受益於相對較大的私有地址空間所提供的更大的靈活性。

## 相關資訊

- IP 路由通訊協定支援頁面
- IP 路由支援頁面
- 技術支援與文件 - Cisco Systems