

# Adresszuweisung für das private Internet

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Privater Adressbereich](#)

[Vorteile und Nachteile der Verwendung von privaten Adressräumen](#)

[Überlegungen zum Design](#)

[Sicherheitsüberlegungen](#)

[Schlussfolgerung](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument basiert auf [RFC 1597](#) und hilft Ihnen, IP-Adressraum zu sparen, indem Sie privaten Hosts in Ihrem Netzwerk keine global eindeutigen IP-Adressen zuweisen. Sie können weiterhin eine vollständige Netzwerkschichtverbindung zwischen allen Hosts im Netzwerk und zwischen allen öffentlichen Hosts im Internet zulassen.

Hosts, die IP verwenden, fallen in drei Kategorien:

- Hosts, die keinen Zugriff auf Hosts in anderen Unternehmen oder auf das Internet im Allgemeinen benötigen. Diese Hosts können IP-Adressen verwenden, die innerhalb ihres Netzwerks einzigartig sind, aber unter externen Netzwerken nicht eindeutig sind.
- Hosts, die Zugriff auf eine begrenzte Anzahl von externen Diensten benötigen (z. B. E-Mail, FTP, Netnews, Remote-Anmeldung), die über Gateways der Anwendungsschicht verwaltet werden können. Viele dieser Hosts benötigen oder möchten aus Datenschutzgründen keinen uneingeschränkten externen Zugriff (über IP-Verbindungen). Wie Hosts in der ersten Kategorie können sie IP-Adressen verwenden, die innerhalb ihres Netzwerks einzigartig sind, aber nicht innerhalb externer Netzwerke.
- Hosts, die über IP-Verbindungen Zugriff auf die Netzwerkebene außerhalb des Unternehmens benötigen. Nur diese Hosts benötigen global eindeutige IP-Adressen.

Viele Anwendungen benötigen nur Verbindungen innerhalb eines Netzwerks und keine externe Verbindung für die meisten internen Hosts. In größeren Netzwerken verwenden Hosts häufig TCP/IP, wenn sie keine Netzwerkanbindung außerhalb des Netzwerks benötigen. Im Folgenden sind einige Beispiele aufgeführt, bei denen keine externe Verbindung erforderlich ist:

- Ein großer Flughafen mit Ankunft und Abflug wird einzeln über TCP/IP adressierbar angezeigt. Es ist sehr unwahrscheinlich, dass diese Displays direkt von anderen Netzwerken

aus zugänglich sein müssen.

- Große Unternehmen wie Banken und Einzelhandelsketten, die TCP/IP für ihre interne Kommunikation verwenden. Eine große Anzahl lokaler Arbeitsplätze, wie Kassen, Geldautomaten und Einrichtungen an Büropositionen, benötigt selten externe Verbindungen.
- Netzwerke, die Application-Layer-Gateways (Firewalls) verwenden, um eine Verbindung zum Internet herzustellen. Das interne Netzwerk verfügt in der Regel nicht über direkten Zugriff auf das Internet, sodass nur ein oder mehrere Firewall-Hosts vom Internet aus sichtbar sind. In diesem Fall kann das interne Netzwerk nicht eindeutige IP-Nummern verwenden.
- Zwei Netzwerke, die über ihre eigene private Verbindung kommunizieren. In der Regel ist über diese Verbindung nur eine sehr begrenzte Anzahl von Hosts gegenseitig erreichbar. Nur diese Hosts benötigen global eindeutige IP-Nummern.
- Schnittstellen von Routern in einem internen Netzwerk.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

## Privater Adressbereich

Die Internet Assigned Numbers Authority (IANA) hat die folgenden drei Blöcke von IP-Adressraum für private Netzwerke reserviert:

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

Der erste Block besteht aus einer Netzwerknnummer der Klasse A, der zweite Block aus 16 zusammenhängenden Netzwerknnummern der Klasse B und der dritte Block aus 255 zusammenhängenden Netzwerknnummern der Klasse C.

Wenn Sie sich für den privaten Adressbereich entscheiden, müssen Sie sich nicht mit IANA oder einer Internet-Registrierung abstimmen. Die Adressen in diesem privaten Adressbereich sind nur innerhalb Ihres Netzwerks eindeutig. Wenn Sie einen global eindeutigen Adressbereich benötigen, müssen Sie Adressen aus einer Internet-Registrierung beziehen.

Um privaten Adressraum zu verwenden, bestimmen Sie, welche Hosts keine Netzwerkschichtverbindung mit der Außenwelt benötigen. Diese Hosts sind private Hosts und verwenden privaten Adressraum. Private Hosts können mit allen anderen öffentlichen und privaten

Hosts im Netzwerk kommunizieren, sie können jedoch keine IP-Verbindung zu einem externen Host haben. Private Hosts können weiterhin über Relays auf Anwendungsebene auf externe Dienste zugreifen.

Alle anderen Hosts sind öffentlich und verwenden global eindeutigen Adressbereich, der von einer Internet-Registrierung zugewiesen wird. Öffentliche Hosts können mit anderen Hosts im Netzwerk kommunizieren und IP-Verbindungen mit externen öffentlichen Hosts herstellen. Öffentliche Hosts verfügen nicht über Verbindungen zu privaten Hosts anderer Netzwerke.

Da private Adressen keine globale Bedeutung haben, werden Routing-Informationen über private Netzwerke nicht über externe Links verbreitet, und Pakete mit privaten Quell- oder Zieladressen sollten nicht über diese Links weitergeleitet werden. Router in Netzwerken, die keinen privaten Adressraum verwenden, insbesondere Router von Internetdiensteanbietern, sollten so konfiguriert werden, dass Routing-Informationen über private Netzwerke abgelehnt (herausgefiltert) werden. Diese Ablehnung sollte nicht als Routing-Protokoll-Fehler behandelt werden.

Indirekte Verweise auf solche Adressen (z. B. DNS Resource Records) sollten im Netzwerk enthalten sein. Internetdiensteanbieter sollten Maßnahmen ergreifen, um solche Leckagen zu verhindern.

## Vorteile und Nachteile der Verwendung von privaten Adressräumen

Der offensichtliche Vorteil der Nutzung von privaten Adressräumen für das Internet im Allgemeinen besteht darin, den global einzigartigen Adressraum zu erhalten. Die Verwendung von privaten Adressräumen bietet Ihnen außerdem mehr Flexibilität beim Netzwerkdesign, da Ihnen mehr Adressraum zur Verfügung steht, als Sie aus dem global einzigartigen Pool erhalten könnten.

Der Hauptnachteil bei der Verwendung von privaten Adressräumen besteht darin, dass Sie Ihre IP-Adressen neu nummerieren müssen, wenn Sie eine Verbindung zum Internet herstellen möchten.

## Überlegungen zum Design

Sie sollten zuerst den privaten Teil Ihres Netzwerks entwerfen und für alle internen Verbindungen privaten Adressraum verwenden. Planen Sie dann öffentliche Subnetze, und entwerfen Sie die externe Verbindung.

Wenn ein geeignetes Subnetting-Schema entworfen und von Ihrer Ausrüstung unterstützt werden kann, verwenden Sie den 24-Bit-Block privaten Adressbereichs und erstellen Sie einen Adressierungsplan mit einem guten Wachstumspfad. Wenn Subnetz ein Problem darstellt, können Sie den 16-Bit-Block der Klasse C verwenden.

Um einen Host von privat in öffentlich zu ändern, müssen seine Adresse und in den meisten Fällen seine physische Verbindung geändert werden. An Standorten, an denen solche Änderungen vorhersehbar sind (Maschinenräume usw.), können Sie separate physische Medien für öffentliche und private Subnetze konfigurieren, um diese Änderungen zu vereinfachen.

Router, die mit externen Netzwerken verbunden sind, sollten mit geeigneten Paket- und Routing-

Filtern an beiden Enden der Verbindung eingerichtet werden, um Leckagen zu vermeiden. Sie sollten auch private Netzwerke von eingehenden Routing-Informationen filtern, um mehrdeutige Routing-Situationen zu vermeiden, die auftreten können, wenn Routen zum privaten Adressbereich außerhalb des Netzwerks erfolgen.

Gruppen von Organisationen, die einen Bedarf an gegenseitiger Kommunikation voraussehen, müssen einen gemeinsamen Adressierungsplan entwerfen. Wenn zwei Standorte über einen externen Service Provider verbunden werden müssen, können sie die Verwendung eines IP-Tunnels in Erwägung ziehen, um Paketecks aus dem privaten Netzwerk zu verhindern.

Eine Möglichkeit, das Auslaufen von DNS-RRs zu vermeiden, besteht darin, zwei Namensserver zu betreiben, einen externen Server, der für alle global eindeutigen IP-Adressen des Unternehmens verantwortlich ist, und einen internen Server, der für alle IP-Adressen verantwortlich ist, sowohl öffentliche als auch private. Um Konsistenz zu gewährleisten, sollten beide Server dieselben Daten empfangen, von denen der externe Namensserver nur eine gefilterte Version verwendet.

Die Resolver auf allen internen Hosts, sowohl öffentlichen als auch privaten, fragen nur den internen Namensserver ab. Der externe Server löst Anfragen von externen Resolvern und ist mit dem globalen DNS verknüpft. Der interne Server leitet alle Anfragen nach Informationen außerhalb des Unternehmens an den externen Namensserver weiter, sodass alle internen Hosts auf den globalen DNS zugreifen können. Auf diese Weise erreichen Informationen über private Hosts keine externen Resolver und Namensserver.

## Sicherheitsüberlegungen

Die Verwendung von privaten Adressräumen kann zwar die Sicherheit verbessern, ist jedoch kein Ersatz für dedizierte Sicherheitsmaßnahmen.

## Schlussfolgerung

Bei diesem Schema benötigen viele große Netzwerke nur einen relativ kleinen Adressblock vom global eindeutigen IP-Adressbereich. Das Internet bietet enorme Vorteile durch die Erhaltung von weltweit einzigartigem Adressraum, und die Netzwerke profitieren von der erhöhten Flexibilität eines relativ großen privaten Adressbereichs.

## Zugehörige Informationen

- [Support-Seite für IP Routed Protocols](#)
- [Support-Seite für IP-Routing](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)