

Address Allocation for Private Internets

Document ID: 13789

Introduction

Prerequisites

Requirements

Components Used

Conventions

Private Address Space

Advantages and Disadvantages of Using Private Address Space

Design Considerations

Security Considerations

Conclusion

Related Information

Introduction

This document is based upon RFC 1597 , and it will help you conserve IP address space by not allocating globally unique IP addresses to private hosts in your network. You can still permit full network layer connectivity between all hosts in the network and between all public hosts in the Internet.

Hosts that use IP fall into three categories:

- Hosts that do not require access to hosts in other enterprises or the Internet at large. These hosts can use IP addresses that are unique within their network but may not be unique among outside networks.
- Hosts that need access to a limited set of outside services (for example, email, FTP, netnews, remote login) which can be handled by application layer gateways. Many of these hosts may not need or want unrestricted external access (provided via IP connectivity), for privacy or security reasons. Like hosts in the first category, they can use IP addresses that are unique within their network but not among outside networks.
- Hosts that need network layer access outside the enterprise provided via IP connectivity. Only these hosts require IP addresses that are globally unique.

Many applications require connectivity only within one network and do not even need external connectivity for most internal hosts. In larger networks, hosts often use TCP/IP when they do not need network layer connectivity outside the network. Here are some examples where external connectivity might not be required:

- A large airport which has its arrival and departure displays individually addressable via TCP/IP. It is very unlikely that these displays need to be directly accessible from other networks.
- Large organizations like banks and retail chains that use TCP/IP for their internal communication. Large numbers of local workstations like cash registers, money machines, and equipment at clerical positions rarely need outside connectivity.
- Networks that use application layer gateways (firewalls) to connect to the Internet. The internal network usually does not have direct access to the Internet, so only one or more firewall hosts are visible from the Internet. In this case, the internal network can use non-unique IP numbers.
- Two networks that communicate over their own private link. Usually only a very limited set of hosts is mutually reachable over this link. Only those hosts need globally unique IP numbers.
- Interfaces of routers on an internal network.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP address space for private networks:

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

The first block is a single class A network number, the second block is a set of 16 contiguous class B network numbers, and the third block is a set of 255 contiguous class C network numbers.

If you decide to use private address space, you don't need to coordinate with IANA or an Internet registry. Addresses within this private address space will only be unique within your network. Remember, if you need globally unique address space, you must obtain addresses from an Internet registry.

In order to use private address space, determine which hosts do not need to have network layer connectivity to the outside. These hosts are private hosts, and use private address space. Private hosts can communicate with all other hosts within the network, both public and private, but they cannot have IP connectivity to any external host. Private hosts can still have access to external services via application layer relays.

All other hosts are public and use globally unique address space assigned by an Internet registry. Public hosts can communicate with other hosts within the network, and can have IP connectivity to external public hosts. Public hosts do not have connectivity to private hosts of other networks.

Because private addresses have no global meaning, routing information about private networks is not propagated on outside links, and packets with private source or destination addresses should not be forwarded across such links. Routers in networks that do not use private address space, especially those of Internet service providers, should be configured to reject (filter out) routing information about private networks. This rejection should not be treated as a routing protocol error.

Indirect references to such addresses (like DNS Resource Records) should be contained within the network. Internet service providers should take measures to prevent such leakage.

Advantages and Disadvantages of Using Private Address Space

The obvious advantage of using private address space for the Internet at large is to conserve the globally unique address space. Using private address space also gives you greater flexibility in network design, since you will have more address space available than you could get from the globally unique pool.

The primary disadvantage of using private address space is that you have to renumber your IP addresses if you want to connect to the Internet.

Design Considerations

You should design the private part of your network first and use private address space for all internal links. Then plan public subnets and design the external connectivity.

If a suitable subnetting scheme can be designed and is supported by your equipment, use the 24-bit block of private address space and make an addressing plan with a good growth path. If subnetting is a problem, you can use the 16-bit class C block.

Changing a host from private to public requires changing its address and, in most cases, its physical connectivity. In locations where such changes can be foreseen (machine rooms, and so forth) you might want to configure separate physical media for public and private subnets, to make these changes easier.

Routers that connect to external networks should be set up with appropriate packet and routing filters at both ends of the link in order to prevent leakage. You should also filter any private networks from inbound routing information in order to prevent ambiguous routing situations which can occur if routes to the private address space point outside the network.

Groups of organizations that foresee a need for mutual communication must design a common addressing plan. If two sites need to be connected using an external service provider, they can consider using an IP tunnel to prevent packet leaks from the private network.

One way to avoid leaking of DNS RRs is to run two name servers, one external server responsible for all globally unique IP addresses of the enterprise and one internal server responsible for all IP addresses, both public and private. In order to ensure consistency both these servers should receive the same data, of which the external name server only uses a filtered version.

The resolvers on all internal hosts, both public and private, query only the internal name server. The external server resolves queries from outside resolvers and is linked into the global DNS. The internal server forwards all queries for information outside the enterprise to the external name server, so all internal hosts can access the global DNS. This way, information about private hosts does not reach outside resolvers and name servers.

Security Considerations

While using private address space can improve security, it is not a substitute for dedicated security measures.

Conclusion

With this scheme many large networks only need a relatively small block of addresses from the globally unique IP address space. The Internet at large benefits through conservation of globally unique address space, and the networks benefit from the increased flexibility provided by a relatively large private address space.

Related Information

- [IP Routed Protocols Support Page](#)
 - [IP Routing Support Page](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 18, 2005

Document ID: 13789
