Private network

From Wikipedia, the free encyclopedia

In Internet networking, a **private network** is a computer network that uses a private address space of IP addresses. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments. Both the IPv4 and the IPv6 specifications define **private IP address** ranges.[1][2]

Most Internet service providers (ISPs) allocate only a single publicly routable IPv4 address to each residential customer, but many homes have more than one computer, smartphone, or other Internet-connected device. In this situation, a network address translator (NAT/PAT) gateway is usually used to provide Internet connectivity to multiple hosts. Private addresses are also commonly used in corporate networks which, for security reasons, are not connected directly to the Internet. Often a proxy, SOCKS gateway, or similar devices are used to provide restricted Internet access to network-internal users.

Private network addresses are not allocated to any specific organization. Anyone may use these addresses without approval from regional or local Internet registries. Private IP address spaces were originally defined to assist in delaying IPv4 address exhaustion. IP packets originating from or addressed to a private IP address cannot be routed through the public Internet.

Private addresses are often seen as enhancing network security for the internal network, since use of private addresses internally makes it difficult for an external host to initiate a connection to an internal system.

Private IPv4 addresses[edit]

The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks:[1]:4

RFC 1918 name	IP address range	Number of addresses	Largest CIDR block (subnet mask)	Host ID size	Mask bits	*Classful* description[Note 1]
24-bit block	10.0.0.0 – 10.255.255.255	16777216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network
20-bit block	172.16.0.0 – 172.31.255.255	1048576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks
16-bit block	192.168.0.0 – 192.168.255.255	65536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks

In practice, it is common to subdivide these ranges into smaller subnets.

Dedicated space for carrier-grade NAT deployment[edit]

Main article: IPv4 shared address space

In April 2012, IANA allocated the *100.64.0.0/10* block of IPv4 addresses specifically for use in carrier-grade NAT scenarios.[4]

IP address range	Number of addresses	Largest CIDR block (subnet mask)	Host ID size	Mask bits
100.64.0.0 – 100.127.255.255	4194304	100.64.0.0/10 (255.192.0.0)	22 bits	10 bits

This address block should not be used on private networks or on the public Internet. The size of the address block was selected to be large enough to uniquely number all customer access devices for all of a single operator's points of presence in a large metropolitan area such as Tokyo.[4]

Private IPv6 addresses[edit]

Main article: Unique local address

The concept of private networks has been extended in the next generation of the Internet Protocol, IPv6, and special address blocks are reserved.

The address block *fc00::/7* is reserved by IANA for unique local addresses (ULAs).[2] They are unicast addresses, but contain a 40-bit random number in the routing prefix to prevent collisions when two private networks are interconnected. Despite being inherently *local* in usage, the IPv6 address scope of unique local addresses is global.

The first block defined is *fd00::/8*, designed for */48* routing blocks, in which users can create multiple subnets, as needed.

RFC 4193 Block	Prefix/L	Global ID (random)	Subnet ID	Number of addresses in subnet
	48 bits		16 bits	64 bits
fd00::/8	fd	xx:xxxx:xxxx	yyyy	18446744073709551616

Examples:

Prefix /L	Global ID (random)	Subnet ID	Interface ID	Address	Subnet

fd	xx:xxxx:xxxx	yyyy	zzzz:zzzz:zzzz:zzzz	fdxx:xxxx:xxxx:yyyy:zzzz:zzzz:zzzz:zzzz	fdxx:xxxx:xxxx:yyyy::/64
fd	12:3456:789a	0001	0000:0000:0000:0001	fd12:3456:789a:1::1	fd12:3456:789a:1::/64

A former standard proposed the use of *site-local* addresses in the *fec0::/10* block, but because of scalability concerns and poor definition of what constitutes a *site*, its use has been deprecated since September 2004.[5]

Link-local addresses[edit]

Main article: Link-local address

Another type of private networking uses the link-local address range. The validity of link-local addresses is limited to a single link; e.g. to all computers connected to a switch, or to one wireless network. Hosts on different sides of a network bridge are also on the same link, whereas hosts on different sides of a network router are on different links.

IPv4[edit]

In IPv4, the utility of link-local addresses is in zero-configuration networking when Dynamic Host Configuration Protocol (DHCP) services are not available and manual configuration by a network administrator is not desirable. The block *169.254.0.0/16* was allocated for this purpose.[6][7] If a host on an IEEE 802 (Ethernet) network cannot obtain a network address via DHCP, an address from *169.254.1.0* to *169.254.254.255*[Note 2] may be assigned pseudorandomly. The standard prescribes that address collisions must be handled gracefully.

IPv6[edit]

In IPv6, the block *fe80::/10* is reserved for IP address autoconfiguration.[8] The implementation of these link-local addresses is mandatory, as various functions of the IPv6 protocol depend on them.[9]

Loopback interface[edit]

A special case of private link-local addresses is the loopback interface. These addresses are private and link-local by definition, since packets never leave the host device.

IPv4 reserves the entire class A address block *127.0.0.0/8* for use as private loopback addresses. IPv6 reserves the single address *::1*.

Misrouting[edit]

It is common for packets originating in private address spaces to be misrouted onto the Internet. Private networks often do not properly configure DNS services for addresses used internally and attempt reverse DNS lookups for these addresses, causing extra traffic to the Internet root nameservers. The AS112 project attempted to mitigate this load by providing special *blackhole* anycast nameservers for private address ranges which only return negative result codes (*not found*) for these queries.

Organizational edge routers are usually configured to drop ingress IP traffic for these networks, which can occur either by misconfiguration, or from malicious traffic using a spoofed source address. Less commonly, ISP edge routers drop such egress traffic from customers, which reduces the impact to the Internet of such misconfigured or malicious hosts on the customer's network.

Merging private networks[edit]

Since the private IPv4 address space is relatively small, many private IPv4 networks unavoidably use the same address ranges. This can create a problem when merging such networks, as some addresses may be duplicated for multiple devices. In this case, networks or hosts must be renumbered, often a time-consuming task, or a network address translator must be placed between the networks to translate or masquerade one of the address ranges.

IPv6 defines unique local addresses,[2] providing a very large private address space from which each organization can randomly or pseudo-randomly allocate a 40-bit prefix, each of which allows 65536 organizational subnets. With space for about one trillion (10^{12}) prefixes, it is unlikely that two network prefixes in use by different organizations are the same, provided each of them was selected randomly, as specified in the standard. When two such private IPv6 networks are connected or merged, the risk of an address conflict is therefore virtually absent.

RFC documents[edit]

- RFC 1918 – *Address Allocation for Private Internets*
- RFC 2036 – *Observations on the use of Components of the Class A Address Space within the Internet*
- RFC 7020 – *The Internet Number Registry System*
- RFC 2101 – *IPv4 Address Behaviour Today*
- RFC 2663 – *IP Network Address Translator (NAT) Terminology and Considerations*
- RFC 3022 – *Traditional IP Network Address Translator (Traditional NAT)*
- RFC 3330 – *Special-Use IPv4 Addresses* (superseded)
- RFC 3879 – *Deprecating Site Local Addresses*
- RFC 3927 – *Dynamic Configuration of IPv4 Link-Local Addresses*
- RFC 4193 – *Unique Local IPv6 Unicast Addresses*
- RFC 5735 – *Special-Use IPv4 Addresses* (superseded)
- RFC 6598 – *Reserved IPv4 Prefix for Shared Address Space*
- RFC 6890 – *Special-Purpose IP Address Registries*

See also[edit]

- Heartbeat network
- Intranet

- Localhost
- Reserved IP addresses
- Top-level domain § Reserved domains
- Virtual private network