

NAT (RFC 2663, RFC 2766)

- Many households now have high-speed Internet access via DSL or cable modem.
- The basic service offered by most ISPs includes only one or two computers per customer.
- An additional charge is levied for additional computers and IP addresses.
- Network Address Translation (NAT) - a technology that allows multiple computers on a network to "share" a single IP address.
- NAT completely hides additional computers at the customer's site.

NAT (RFC 2663, RFC 2766)

- To the ISP, the customer appears to have only one computer attached to the Internet.
- A device which implements NAT appears to function like a default router.
- When a computer on the local network generates a datagram, the computer forwards the datagram to the NAT device for delivery.
- NAT is completely transparent; computers on the local network do not need special software.
- Instead, each computer can run a standard OS and standard network software.

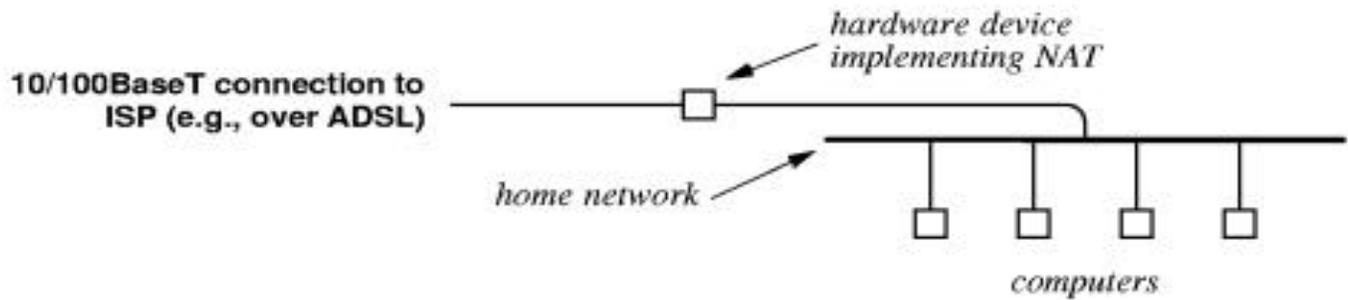
NAT (RFC 2663, RFC 2766)

- NAT combines the advantage of connectivity for multiple computers with the advantage of low-cost Internet service.

Basic NAT Architecture

- A NAT hardware device is inserted between an ISP and the household computers.
- The NAT device acts like an IP router which forwards datagrams between the local network and the Internet.
- Like a router, a NAT device has two network interfaces. One connects to the ISP and the other to the local network.
- Unlike a router, a NAT device does something else which we'll describe later.

Basic NAT Architecture



Basic NAT Architecture

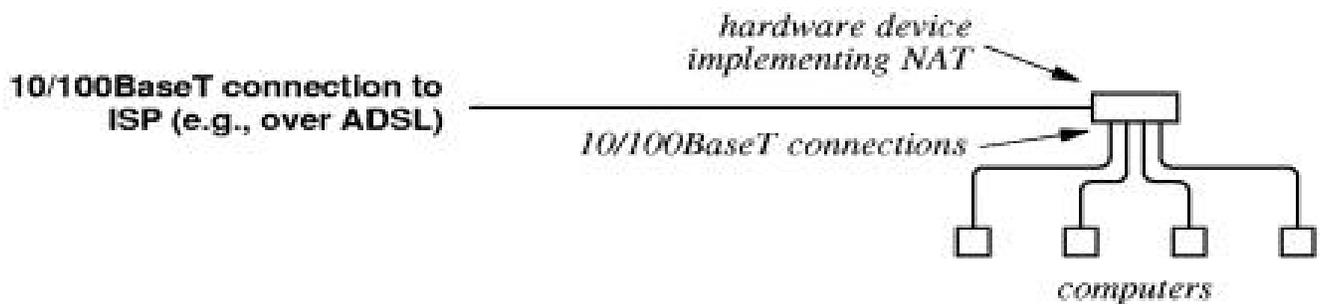
- NAT is available commercially.
 - Software that runs on a conventional PC.
 - A dedicated special-purpose hardware device. Sometimes called a residential gateway or a broadband gateway or a broadband router.

NAT Software

- When a PC is used to run NAT, the PC needs two NICs as shown in the previous diagram.
- One NIC connects to the ISP and the other to the local network.
- Commercial NAT software:
 - *Masquerade* implements NAT for the Linux OS.
 - Microsoft's *Internet Connection Sharing* (ICS) implements NAT for Windows systems.

NAT Hardware

- When a dedicated NAT hardware device is used, the device usually incorporates or comes with a small Ethernet hub (or Ethernet switch) for the home network.



NAT Hardware

- Commercial NAT hardware:
 - D-Link DI-701 Residential Gateway
 - Farallon NetLine Broadband Gateway
 - MaxGate Ugate-3200P
 - Netgear RT314
 - SMC Barricade

NAT Software vs Hardware

- Both provide the same functionality.
- However, a NAT hardware device has several advantages over a PC running NAT software.
 - Much smaller than a PC.
 - Easy to install and configure.
 - Cheaper than a PC.

Costs between \$120 and \$200.

Of course, this advantage is mitigated if you have an old unused PC lying around.

How NAT Works

- The basic idea of NAT is simple.
- Computers on the local network use arbitrary addresses, and NAT translates the local addresses to the customer's valid IP address before sending a datagram to the Internet.
- The customer chooses an arbitrary prefix for the local network and assigns host addresses using that prefix.
 - The IETF recommends 10.0.0.X and 192.168.0.X, addresses never assigned on the Internet.

How NAT Works

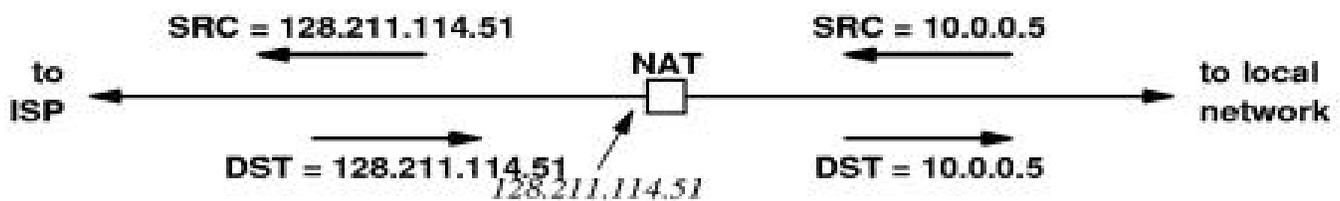
- Here's what happens.
- Suppose a local computer has local IP address 10.0.0.5 on a local network. The customer's valid IP address is 128.211.114.51.

How NAT Works



- The computer generates a datagram with IP source address 10.0.0.5.
- The NAT device replaces the IP source address 10.0.0.5 with the customer's valid IP address 128.211.114.51 and records the translation in a table.
- NAT forwards the datagram toward its destination.

How NAT Works



- When a datagram is received by the NAT device, NAT looks up the source address in the translation table and replaces the destination address with the appropriate internal address. (In practice, NAT also translates protocol port numbers.)
- NAT forwards the datagram over the local network to the correct local computer.

Other Features of NAT Hardware

- Runs a DHCP server for computers on the local network.

Dynamic Host Configuration Protocol (DHCP) (RFC 2131) - a protocol that computers use to obtain configuration information such as IP addresses.

- Acts as a router to the outside world (the Internet).
- Acts as a security firewall.
 - No local computers are connected directly to the Internet.

Other Features of NAT Hardware

- Since all local computers have IP addresses 10.0.0.X or 192.168.0.X, they are invisible to the outside world.
- All the outside world can see is the NAT hardware device.
- Since local IP addresses are masked from others on the Internet, it is difficult for a hacker to target a local computer.
- Specific ports can be blocked and limited services provided.
- The NAT hardware device acts like a decoy on which there's nothing to hack.