Networking

Networking

How Typical Home Networking Works

Bandwidth - **of a connection is the width of it or the amount of data that can fit through it.**

Broadband - **is a term used today to describe almost any always on, high speed connection to the internet.**

Types of Networks

Local Area Network (LAN)
Wide Area Network (WAN)
Peer-to-peer (P2P) network
Client-Server network

DHCP Server - A server in a network that assigns IP addresses to the multiple stations on the network.

Wired Network Hardware components

Computers (2 or more)
Network Interface Card (NIC) – installed in computer or integrated into motherboard
Ethernet Cable - Category 5 unshielded twisted pair (UTP)
Switch – allow multiple PCs to connect to router
Router – assigns IP addresses to computers (DHCP), provides hardware firewall and NAT
DSL/Cable Modem for internet access

Wireless Network Hardware components

Computers (2 or more)
Wireless Adapter
Wireless Router
Wireless Range Extender (if necessary)

IP - Internet Protocol, handles the address part of each packet so that it gets to the right destination.

TCP - Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message.

Packets - Each packet contains part of the body of your message. A typical packet contains perhaps 1,000 or 1,500 bytes.

NAT – Network Address Translation

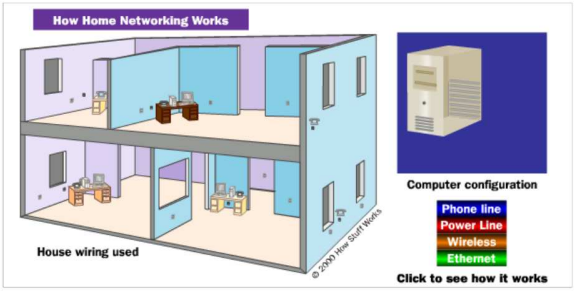
MAC Addresses - Media Access Control (MAC) address

Homework

Handouts - **How Home Networking Works**
How NAT Works
IP address-TCP-IP-Packets
The MAC Address

Online - **Networking Quiz**

How Networking Works



by Tracy V. Wilson and John Fuller Howstuffworks.com

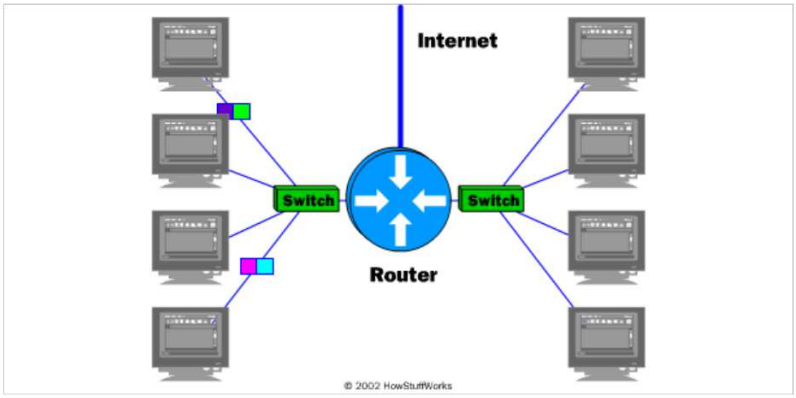
Once, home networks were primarily the realm of technophiles -- most families either didn't need or couldn't afford more than one computer. But now, in addition to using computers for e-mail, people use them for schoolwork, shopping, instant messaging, downloading music and videos, and playing games. For many families, one computer is no longer enough to go around. In a household with multiple computers, a home network often becomes a necessity rather than a technical toy.

A home network is simply a method of allowing computers to communicate with one another. If you have two or more computers in your home, a network can let them share:

- Files and documents
- An Internet connection
- Printers, print servers and scanners
- Stereos, TVs and game systems
- CD burners

The different network types use different hardware, but they all have the same essential components:

- More than one computer
- Hardware (such as a router**)** and software (either built in to the operating system or as a separate application) to coordinate the exchange of information
- A path for the information to follow from one computer to another



If you're thinking of networking the computers in your home, you have several options to explore. In this article, you'll learn about the different types of home computer networks, how they work and what to keep in mind if you're considering creating one. We'll look at the hardware that creates and protects home networks in the next section.

Building a Network

The two most popular network types are **wireless** and **Ethernet** networks. In both of these types, the router does most of the work by directing the traffic between the connected devices. By connecting a router to your dial-up, DSL or cable modem, you can also allow multiple computers to share one connection to the Internet.

If you're going to connect your network to the Internet, you'll need a **firewall**. A firewall is simply a hardware device or software program that protects your network from malicious users and offensive Web sites, keeping hackers from accessing or destroying your data. Although they're essential for businesses looking to protect large amounts of information, they're just as necessary for someone setting up a home network, since a firewall will secure transactions that might include Social Security numbers, addresses, phone numbers and credit card numbers. Most routers combine wireless and Ethernet technology and also include a hardware firewall.

Many software firewalls installed onto your computer block all incoming information by default and prompt you for permission to allow the information to pass. In this way, a software firewall can learn which types of information you want to allow into your network. Symantec, McAfee and Zone Alarm are popular companies that produce software-based firewalls. These companies usually offer some free firewall protection as well as advanced security that you can buy.

A router connects your computers to one another. If you connect it to your modem, it will also connect your network to the Internet.

Wired Networks

Ethernet and wireless networks each have advantages and disadvantages; depending on your needs, one may serve you better than the other. Wired networks provide users with plenty of security and the ability to move lots of data very quickly. Wired networks are typically faster than wireless networks, and they can be very affordable. However, the cost of Ethernet cable can add up -- the more computers on your network and the farther apart they are, the more expensive your network will be. In addition, unless you're building a new house and installing Ethernet cable in the walls, you'll be able to see the cables running from place to place around your home, and wires can greatly limit your mobility. A laptop owner, for example, won't be able to move around easily if his computer is tethered to the wall.

There are three basic systems people use to set up wired networks. An **Ethernet** system uses either a twisted copper-pair or coaxial-based transport system. The most commonly used cable for Ethernet is a **category 5 unshielded twisted pair (UTP)** cable -- it's useful for businesses who want to connect several devices together, such as computers and printers, but it's bulky and expensive, making it less practical for home use. A **phone line**, on the other hand, simply uses existing phone wiring found in most homes, and can provide fast services such as DSL. Finally, **broadband** systems provide cable Internet and use the same type of coaxial cable that gives us cable television.

If you plan to connect only two computers, all you'll need is a **network interface card (NIC)** in each computer and a cable to run between them. If you want to connect several computers or other devices, you'll need an additional piece of equipment: an Ethernet router. You'll also need a cable to connect each computer or device to the router.

This Belkin router (right) provides wireless and Ethernet connections, while also acting as a firewall.

Once you have all of your equipment, all you need to do is install it and configure your computers so they can talk to one another. Exactly what you need to do depends on the type of network and your existing hardware. For example, if your computers came with network cards already installed, all you'll need to do is buy a router and cables and configure your computers to use them. Regardless of which type you select, the routers, adapters and other hardware you buy should come with complete setup instructions.

The steps you'll need to take to configure your computers will also vary based on your hardware and your operating system. User manuals usually provide the necessary information, and Web sites dedicated to specific operating systems often have helpful tips on getting several different computers to talk to each other.

Wireless Networks

The easiest, but most expensive way to connect the computers in your home is to use a wireless network, which uses **radio waves** instead of wires. The absence of physical wires makes this kind of network very flexible. For example, you can move a laptop from room to room without fiddling with network cables and without losing your connection. The downside is that wireless connections are generally slower than Ethernet connections and they are less secure unless you take measures to protect your network.

Most home wireless networks use **802.11g** wireless networking, which transmits data at 2.4 GHz with a speed of 54 megabits. A newer wireless standard is **802.11n,** which is designed to be faster and offer a longer range than 802.11g. However, the 802.11n standard isn't yet final, and early 802.11n hardware has failed to meet expectations in tests.

If you want to build a wireless network, you'll need a **wireless router.** Signals from a wireless router extend about 100 feet (30.5 meters) in all directions, but walls can interrupt the signal. Depending on the size and shape of your home and the range of the router, you may need to purchase a **range extender** or **repeater** to get enough coverage.

You'll also need a **wireless adapter** in each computer you plan to connect to the network. You can add printers and other devices to the network as well. Some new models have built-in wireless communication capabilities, and you can use a **wireless Ethernet bridge** to add wireless capabilities to devices that don't. Any devices that use the Bluetooth standard can also connect easily to each other within a range of about 10 meters (32 feet), and most computers, printers, cell phones, home entertainment systems and other gadgets come installed with the technology.

Definitions

Broadband is a term used today to describe almost any always on, high speed connection to the internet.

Bandwidth of a connection is the width of it or the amount of data that can fit through it. To use an analogy, a ten lane road can fit more cars down it than a five lane road. We express the bandwidth in bits per second (bps). This indicates the number of bits of information that can fit down the line for a second. These days, bits per second doesn't cover many methods of connection so we use kilobits per second (kbps) and megabits per second (mbps) for thousands and millions of bits per second.

Local Area Network (**LAN**) is a computer network covering a small physical area, like a home, office, or small group of buildings, such as a school, or an airport. The defining characteristics of LANs, in contrast to wide-area networks (WANs), include their usually higher data-transfer rates and smaller geographic range.

Ethernet over unshielded twisted pair cabling, and Wi-Fi are the two most common technologies currently used. A local area network is a network that spans a relatively small space and provides services to a small number of people. A peer-to-peer or client-server method of networking may be used.

Peer-to-peer (P2P) network is where each client shares their resources with other workstations in the network. Examples of peer-to-peer networks are: Small office networks where resource use is minimal and a home network.

Client-server network is where every client is connected to the server and each other. Client-server networks use servers in different capacities. These can be classified into two types: Single-service servers and print servers where the server performs one task such as file server, ; while other servers can not only perform in the capacity of file servers and print servers, but they also conduct calculations and use these to provide information to clients (Web/Intranet Server). Computers are linked via Ethernet Cable, can be joined either directly (one computer to another), or via a network switch that allows multiple connections.

Wide Area Network (**WAN**) is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries. Contrast with local area networks (LANs) which are usually limited to a room, building, or campus. The largest and most well-known example of a WAN is the Internet.

WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet. A router connects to the LAN on one side and the WAN on the other.

DHCP Server (Dynamic Host Configuration Protocol). A server in a network or Internet service that assigns IP addresses to the multiple stations on the network.

Network Hardware

Network switch is a small hardware device that joins multiple computers together within one local area network (LAN). Different models of network switches support differing numbers of connected devices. Most consumer-grade network switches provide either four or eight connections for Ethernet devices. Switches can be connected to each other, a so-called *daisy chaining* method to add progressively larger number of devices to a LAN.

Broadband Routers are used to connect 2 networks together. Usually either two LANs (Local Area Networks), two WANs (Wide Area Networks) or a LAN to the internet. If you are going to be connecting more than one computer (such as a network) to the broadband connection then you will need a router. A broadband modem is used to connect just one computer to the broadband connection. A router is required to share the modem's internet connection with multiple computers.

Broadband modem is a type of digital modem used with high-speed DSL or cable Internet service. Cable modems connect a home computer to residential cable TV service, while DSL modems connect to residential public telephone service.

Network interface card (NIC), or **LAN adapter** is a computer hardware component designed to allow computers to communicate over a computer network.

What is an IP address? By Hans Joachim Roy/Dreamstime.com

There are 4.3 billion possible combinations of Internet Protocol (IP) addresses. Every machine on the Internet has a unique identifying number, called an IP Address. A typical IP address looks like this:

- 216.27.61.137

To make it easier for us humans to remember, IP addresses are normally expressed in decimal format as a "*dotted decimal number*" like the one above. But computers communicate in binary form. Look at the same IP address in binary:

- 11011000.00011011.00111101.10001001

The four numbers in an IP address are called **octets**, because they each have eight positions when viewed in binary form. If you add all the positions together, you get 32, which is why IP addresses are considered 32-bit numbers. Since each of the eight positions can have two different states (1 or 0) the total number of possible combinations per octet is 2^8 or 256. So each octet can contain any value between 0 and 255. Combine the four octets and you get 2^{32} or a possible 4,294,967,296 unique values!

What is TCP/IP?

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network. When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer. TCP/IP and the higher-level applications that use it are collectively said to be "stateless" because each client request is considered a new request unrelated to any previous one (unlike ordinary phone conversations that require a dedicated connection for the call duration). Being stateless frees network paths so that everyone can use them continuously. (Note that the TCP layer itself is not stateless as far as any one message is concerned. Its connection remains in place until all packets in a message have been received.)

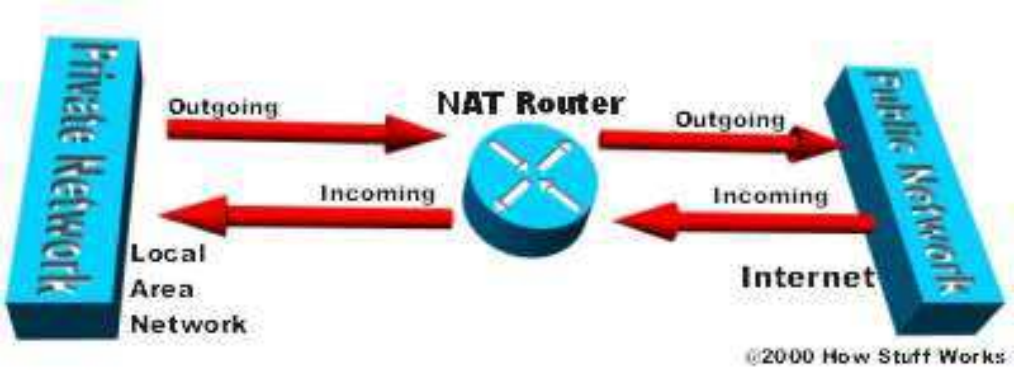
What is a packet?

It turns out that everything you do on the Internet involves **packets**. For example, every Web page that you receive comes as a series of packets, and every e-mail you send leaves as a series of packets. Networks that ship data around in small packets are called **packet switched networks**.

On the Internet, the network breaks an e-mail message into parts of a certain size in bytes. These are the packets. Each packet carries the information that will help it get to its destination -- the sender's IP address, the intended receiver's IP address, something that tells the network how many packets this e-mail message has been broken into and the number of this particular packet. The packets carry the data in the protocols that the Internet uses: Transmission Control Protocol/Internet Protocol (TCP/IP). Each packet contains part of the body of your message. A typical packet contains perhaps 1,000 or 1,500 bytes.

Each packet is then sent off to its destination by the best available route -- a route that might be taken by all the other packets in the message or by none of the other packets in the message. This makes the network more efficient. First, the network can balance the load across various pieces of equipment on a millisecond-by-millisecond basis. Second, if there is a problem with one piece of equipment in the network while a message is being transferred, packets can be routed around the problem, ensuring the delivery of the entire message.

How Network Address Translation Works



By Jeff Tyson

The NAT router translates traffic coming into and leaving the private network.

Network Address Translation helps improve security by reusing IP addresses.

The Internet has grown larger than anyone ever imagined it could be. Although the exact size is unknown, the current estimate is that there are about 100 million hosts and more than 350 million users actively on the Internet. That is more than the entire population of the United States! In fact, the rate of growth has been such that the Internet is effectively doubling in size each year.

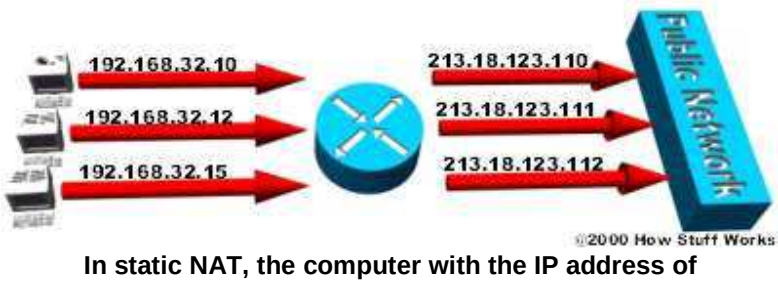
So what does the size of the Internet have to do with NAT? Everything! For a computer to communicate with other computers and Web servers on the Internet, it must have an **IP address**. An IP address (IP stands for Internet Protocol) is a unique 32-bit number that identifies the location of your computer on a network. Basically, it works like your street address -- as a way to find out exactly where you are and deliver information to you.

Network Address Translation allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers.

NAT is like the receptionist in a large office. Let's say you have left instructions with the receptionist not to forward any calls to you unless you request it. Later on, you call a potential client and leave a message for that client to call you back. You tell the receptionist that you are expecting a call from this client and to put her through. The client calls the main number to your office, which is the only number the client knows. When the client tells the receptionist that she is looking for you, the receptionist checks a lookup table that matches your name with your extension. The receptionist knows that you requested this call, and therefore forwards the caller to your extension.

Network Address Translation is used by a device (firewall, router or computer) that sits between an internal network and the rest of the world.

- **Static NAT** - Mapping an unregistered IP address to a registered IP address on a one-to-one basis. Particularly useful when a device needs to be accessible from outside the network.



In static NAT, the computer with the IP address of 192.168.32.10 will always translate to 213.18.123.110.

The MAC Address

An Introduction to MAC Addressing

An Article by your Guide Bradley Mitchell

In computer networking, the Media Access Control (MAC) address is every bit as important as an IP address. Learn in this article how MAC addresses work and how to find the MAC addresses being used by a computer... *(see below)*

What Is a MAC Address?

The MAC address is a unique value associated with a network adapter. MAC addresses are also known as **hardware** addresses or **physical** addresses. They uniquely identify an adapter on a LAN.

MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following two formats:

`MM:MM:MM:SS:SS:SS`

`MM-MM-MM-SS-SS-SS`

The first half of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body (see sidebar). The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer. In the example,
`00:A0:C9:14:C8:29`
The prefix
`00A0C9`
indicates the manufacturer is Intel Corporation.

MAC vs. IP Addressing

It's a slight oversimplification, but one can think of IP addressing as supporting the software implementation and MAC addresses as supporting the hardware implementation of the network stack. The MAC address generally remains fixed and follows the network device, but the IP address changes as the network device moves from one network to another.

IP networks maintain a mapping between the IP address of a device and its MAC address. This mapping is known as the **ARP cache** or **ARP table**. ARP, the Address Resolution Protocol, supports the logic for obtaining this mapping and keeping the cache up to date.

DHCP also usually relies on MAC addresses to manage the unique assignment of IP addresses to devices.

Find a MAC Address in Windows

Use the ipconfig utility (with the /all option) in Windows XP and any newer versions of Windows.

'ipconfig' may display multiple MAC addresses for one computer. One MAC address exists for each installed network card. Additionally, Windows maintains one or more MAC addresses that are not associated with hardware cards.

For example, Windows dial-up networking uses virtual MAC addresses to manage the phone connection as if it were a network card. Some Windows VPN clients likewise have their own MAC address. The MAC addresses of these "virtual" network adapters are the same length and format as true hardware addresses.