Layer 1 - Devices and Their Functions
Layer 1 defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems. Some common examples are Ethernet segments and serial links like **Frame Relay** and **T1**.
Repeaters that provide signal amplification are also considered Layer 1 devices.
The **physical interface on the NIC** can also be considered part of Layer 1.

Definition

The **LAN (Local Area Network) card** is a 'door' to the network from a computer. Any type of network activity requires a LAN card: the Internet, network printer, connecting computers together, and so on. Today many devices contain a network card, including televisions for their Internet apps, Blu-ray players, mobile phones, VoIP, desk phones, and even refrigerators. LAN cards are hardware devices that can be added to a computer, or they can be integrated into the main hardware of the computer.

LAN Card Types

What does a LAN card look like? Some LAN cards look like credit cards.

Some cards, such as a PCMCIA card, can be used in a laptop. There are many other ways of connecting the LAN card to a computer. Some cards are connected via the **USB port**, some via the **PCI port** inside of the computer, and some are even embedded inside of the computer. Most laptops today have integrated LAN cards both for wired and wireless networking.

A PCI card goes inside of a PC computer. The card shows an **Ethernet port**, which is the spot where you plug in a network cable. The LAN card you select often determines the **protocols** that are used on the network. For example, an Ethernet card will allow communication via the Ethernet protocol. A coax card would allow for a bus topology network and a new set of protocols. A fiber cable would have a different cable plugin, and it would likely work with **Wide Area Network** protocols. The Ethernet port on a LAN card looks like a phone jack, but it is wider and has more pins.

A typical Ethernet cable, or network cable, is the plugin that goes into the LAN card, or the Network Interface Controller (NIC).

Function

The purpose of a LAN card is to create a **physical connection to the network** - to provide an open 'door,' as it were. The first interface supported by a LAN card is a physical interface through which the cable plugs into the card. The interface is well-defined in technical documentation, which is why standard network cables fit most standard LAN cards.

The second function of a LAN card is **to provide a data link**. There is a theoretical model in computer networking called **OSI (Open Systems Interconnection)**. This model, or way of explaining networks, includes seven layers. The first two layers are the physical layer and the data link. Each layer of the OSI model allows for other layers to be independent. Upgrading or changing one layer does not affect the others. This means that if plugins change for all LAN cards, other elements, like the protocols, don't have to change.

The data link function of a LAN card provides hardware-level sending and receiving of network binary data. Zeros and ones flow from the network into the network card. The card can recognize this flow and it can even check for errors. When you turn on a computer with a LAN card, it will have two lights, **one green and one orange**. The **orange** light will come on **when the data link layer is activated**. This means that the cable works, there is a network connected, and data bits are flowing. The second light, the **green light**, comes on once **the next layer, the network layer (such as an IP network), is activated.**

Modem

The word "modem" is a contraction of the words **modulator-demodulator**. A modem is typically used to send digital data over a phone line.

The sending modem **modulates** the data into a signal that is compatible with the phone line, and the receiving modem **demodulates** the signal back into digital data. **Wireless modems** convert digital data into radio signals and back.

Modems came into existence in the 1960s as a way to allow terminals to connect to computers over the phone lines. A typical arrangement is shown below:

A **modem** (**mo**dulator-**dem**odulator) is a device that modulates signals to encode digital information and demodulates signals to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used with any means of transmitting analog signals, from light emitting diodes to radio. A common type of modem is one that turns the digital data of a computer into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

Modems are generally classified by the amount of data they can send in a given unit of time, usually expressed in bits per second (symbol **bit/s**, sometimes abbreviated "bps"), or bytes per second (symbol **B/s**).

What Are The Different Types or Kinds of Modems?

There are a couple of different modems, and the one that will work for your situation depends on the internet connection that you have.

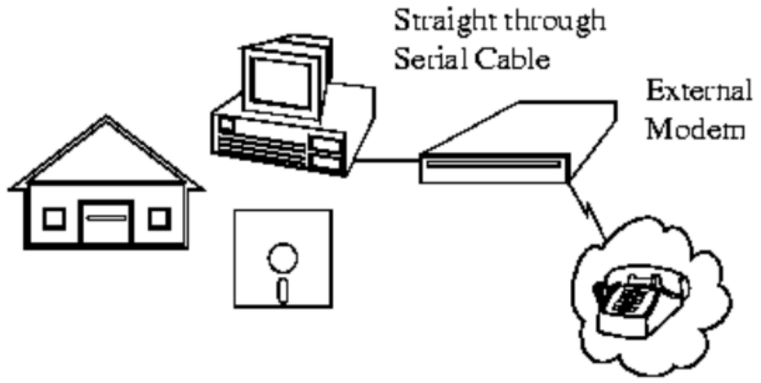
- **Cable** – Cable modems use coaxial cables. One end connects to the back of the modem and the other end connects to your wall or to the back of your cable box. Cable internet is considered to be "high speed" internet.
- **DSL** – DSL can either connect to an external modem (like cable, but a different plug-in), or your computer will already have an internal modem that will dial-in through your phone line. Unlike dial-up, you can still access the internet while talking on the phone.
- **Dial-Up** – Dial-up is the oldest form of internet connection. It uses your phone line to connect to your ISP. Dial-up modems are much slower compared to cable and DSL. Also, if you only have one phone line you won't be able to access the internet at the same you're talking on the phone.

A dialup connection to an ISP uses **circuit switching**, just like an ordinary phone call. But if you're using broadband to get a faster connection, you'll use your phone line in an entirely different way, using a data-handling technique called **packet switching**—and you'll need an entirely different kind of modem. (Read more about circuit and packet switching in our article about the Internet.) If you want to use broadband (packet switching) on a cellophane network, you'll need yet another kind of modem (known as an HSDPA modem).

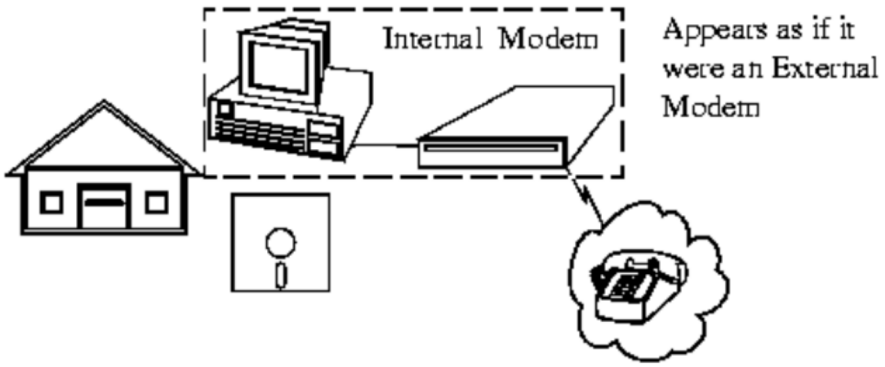
If you link to the Internet without using a telephone line, either by using a wired Ethernet connection or Wi-Fi (wireless Ethernet), you won't need a modem at all: your computer sends and receives all its data to and from the network in digital form, so there's no need to switch back and forth between analog and digital with a modem.

Dialup modems have another handy feature: they can communicate with fax machines at high speed. That's why they're sometimes called **fax modems**. If you have fax software on your computer, you can use your modem to fax out word-processed documents and receive incoming faxes.

There are 2 basic physical types of modems: Internal & External modems. External modems sit next to the computer and connect to the serial port using a straight-through serial cable.



An internal modems is a plug-in circuit board that sits inside the computer. It incorporates the serial port on-board. They are less expensive than external modems because they do not require a case, power supply and serial cable. They appear to the communication programs as if they were an external modem for all practical purposes.

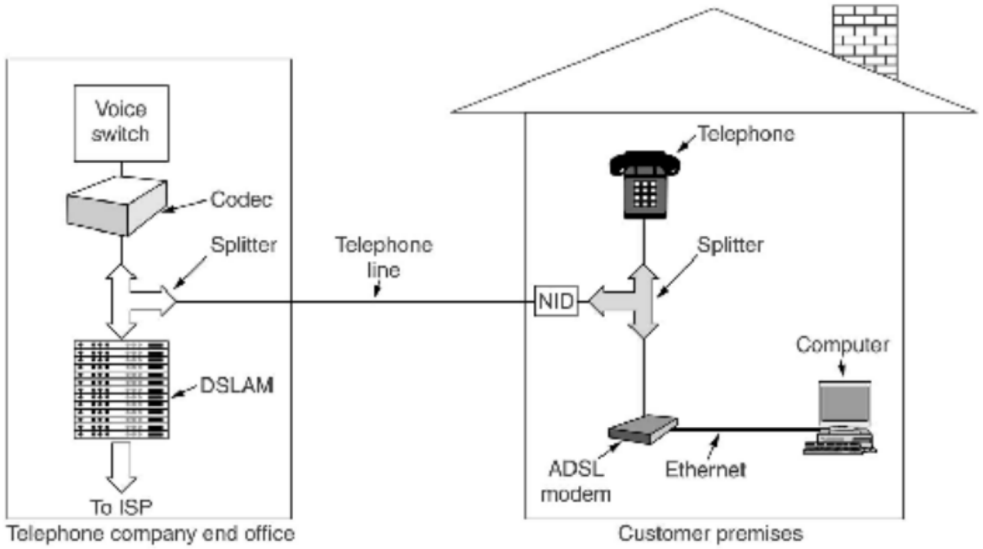


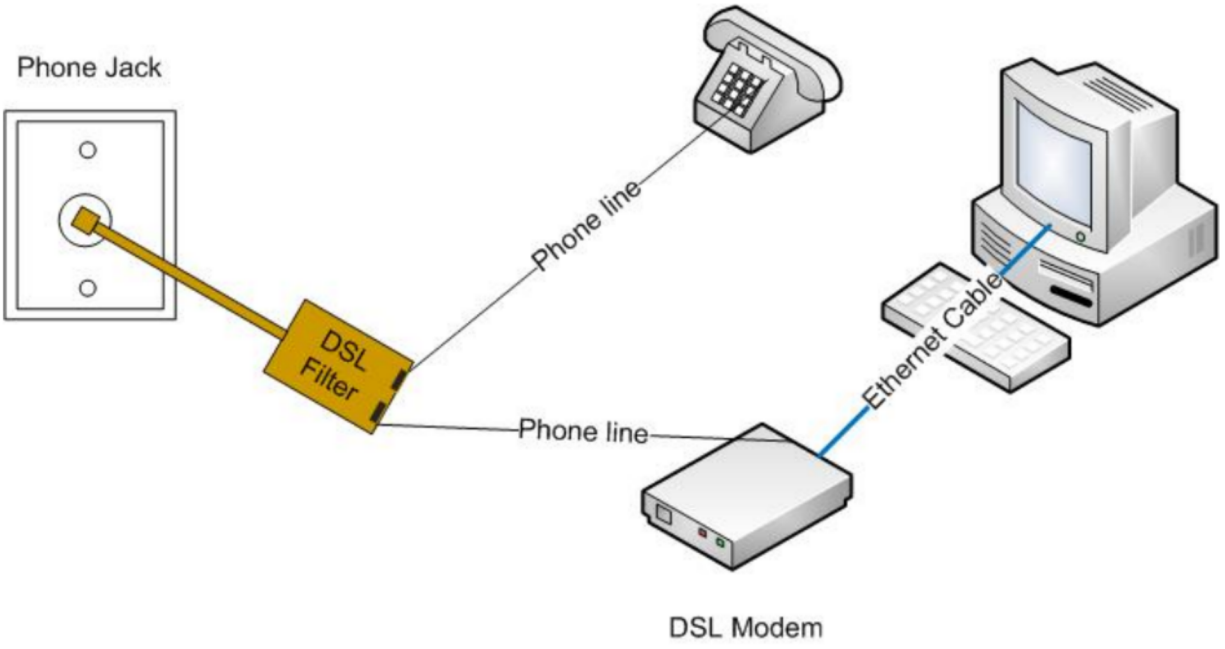
Modem Types

There are many types of modems, the most common of which are:

i. Optical Modem - Uses optical fiber cable instead of wire. The modem converts the digital signal to pulses of light to be transmitted over optical lines (more commonly called a media adapter or transceiver).
ii. Short Haul Modem - A modem used to transmit data over 20 miles or less. Modems we use at home or to connect computers together among different offices in the same building are short haul modems.
iii. Acoustic Modem - a modem that couples to the telephone handset with what looks like suction cups that contain a speaker and microphone. Used by traveling salespeople to connect to hotel phones.
iv. Smart Modem - A modem with a CPU (microprocessor) on board that uses the Hayes AT command set. This allows auto-answer & dial capability rather than manually dialing & answering.
v. Digital Modem - Converts the RS-232 digital signals to digital signals more suitable for transmission. (also called a media adapter or transceiver)

vi. V.32 Modem - a milestone modem that uses a 2400 baud modem with 4 bit encoding. This results in a 9600 bps (bits per second) transfer rate. It brought the price of high speed modems below $5,000.





What is DSL?

DSL (Digital Subscriber Line), also referred as xDSL (x stands for the different techniques used), is a group of technologies that provide high-speed Internet access, by using the ordinary telephone lines. It converts the ordinary telephone line into a high-speed passage for digital audio, video, and data. It is widely used for business and personal purposes. The technology is simple as the setup required for networking already exists. It does not keep the telephone line busy as is the case in the Internet access used in the Dial-up connection. However, the speed depends on the distance between the Internet service provider and the user. More the distance, less will be the speed of the Internet access.

How does DSL work?

POTS (Plain Old Telephone Service) uses copper wired (twisted cable) network, for the exchange of voice information. It uses analog signal transmission and requires a very low bandwidth (0-3400Hz), thus a wide bandwidth remains unused. DSL uses this unused bandwidth to provide Internet service. In this technique, the unused high range of frequency is used for broadband Internet access and the low range is used for voice transmission. In this technique, there is no analog to digital and digital to analog conversion. Digital data is directly fed into the computer using a modem, thus allowing a wider range of bandwidth to be used. Splitters are used to split the low and high frequency signals into two bands. Filters are installed in phones to avoid interference between the range of frequencies used for DSL and telephonic conversion.

Difference between DSL and other Internet Services

Internet Service	Upstream Speed	Downstream Speed
DSL	128 Kbps to 384 Kbps	3 Mbps to 6 Mbps
Dial Up	56 Kbps	56 Kbps
Cable	768 Kbps to 1.5 Mbps	8 Mbps to 16 Mbps
Satellite	128 Kbps to 256 Kbps	512 Kbps to 1.5 Mbps
Wireless	128 Kbps to 768 Kbps	384 Kbps to 2.0 Mbps

Types of DSL Techniques

There are basically two types -

Asymmetric DSL: ADSL, RADSL, VDSL are types of Asymmetric DSL

Symmetric DSL: SDSL, HDSL, SHDSL are types of Symmetric DSL

In Asymmetric DSL, the bandwidth allotted for upstream and downstream is unequal, whereas in Symmetric DSL, it's equal. Let us look into the concept of upstream and downstream to understand the broad uses of the technologies.

Downstream: Data transfer from the server to the user is called downstream. For e.g., downloading a song from any website.

Upstream: Data transfer from the user to the server is called upstream. For e.g., uploading an image to a website.

Difference between DSL Techniques

Type	Upstream Speed	Downstream Speed	Distance Limit
ADSL - Asymmetric Digital Subscriber Line	16 Kbps to 640 Kbps	1.5 Mbps to 6.1 Mbps	9,000 feet to 18,000 feet
VDSL - Very High Speed Digital Subscriber Line	1.5 Mbps to 2.3 Mbps	1.6 Mbps to 52.8 Mbps	1000 feet to 4500 feet
HDSL - High Data Rate Digital Subscriber Line	1.544 Mbps	2.048 Mbps	12,000 feet
SDSL - Symmetric Digital Subscriber Line	1.544 Mbps to 2.048 Mbps	1.544 Mbps to 2.048 Mbps	12,000 feet
RADSL - Rate Adaptive Digital Subscriber Line	272 Kbps to 1.088 Mbps	640 Kbps to 202 Mbps	9,000 feet to 18,000 feet

What is ADSL?

ADSL allots more bandwidth for downstream than upstream. The downstream speed (1.5-9 Mbps) is higher than the upstream speed (1.5 Mbps). The downstream speed depends on the distance of the user from the service provider. The speed increases with decrease in the distance. 1.5 Mbps downstream speed can be achieved for 18,000 feet distance; while 9 Mbps speed is

possible for distance of 9,000 feet. Most of the Internet users aim for a high downloading speed, as compared to uploading. ADSL is widely used for Internet connections at homes and small businesses. With its use, large unused bandwidth of the copper wired network can be utilized for high speed data transfer. With the help of ADSL, one can talk on the telephone and simultaneously access the Internet. Following are other types of Asymmetric Digital Subscriber Line:

RADSL: The speed of data transfer is adjusted automatically depending on the quality of telephone line and distance from the service provider. The downstream speed is adjusted higher than the upstream speed. RADSL provides a faster speed for premises close to the service provider.

VDSL: It provides a high speed of data transfer for short distance, by connecting to ONU (Optical Network Unit), which is a combination of fiber optic and copper wire networks.

The most important advantage of Digital Subscriber Line technology, is that it uses existing telephonic network for high speed Internet access, without keeping the phone line busy.

Read more at Buzzle: http://www.buzzle.com/articles/difference-between-dsl-and-adsl.html

Hubs have become an integral part of the contemporary business and networking systems. In the networking technology sphere, a special type of network device called hub is increasingly being used. From homes to small and major businesses and networks, hubs have become an integral part for smooth conduct of business operations. Usually, hubs are considered of three types namely passive, active and intelligent hubs.

Hubs are the layer 1 devices while switches and routers are layer 2 and layer 3 devices respectively. All kinds of hubs have some common features that are determined primarily by the types of cabling attached to the system. Usually, it could be regarded as a network device that works within the standard parameters of the specific network that it actually is working within.

Active, passive and intelligent hubs are the three of the most commonly know hubs. An active hub possesses all the usual features of a passive hub besides having some more. An active hub takes a larger role in Ethernet communications with the help of technology called store & forward.

Here the hub actually goes through the data before they are transmitted. In cases wherever needed, an active hub repair the data and reschedule the distribution of databases accordingly.

In a situation of data received being weak but readable, the active hub restores the signal before rebroadcasting the same. It enables a certain number of devices which are not operating at their optimal capacity still to be used in the network. Another aspect of an active hub is that it provides information on devices on the network which are not yet fully functional. An active hub also provides certain performance advantages in addition to, certain diagnostic capabilities.

A passive hub on the other hand, do very little to enhance the performance of the network. Neither, it helps in any way in the troubleshooting operations which have become an integral part of the networking operations in recent times. From the cost perspective, most of the passive hubs are easily obtainable at a lesser cost, usually less than US $200. A passive hub when upgraded from 10base-2 then the performance becomes quite impressive and can match with the best.

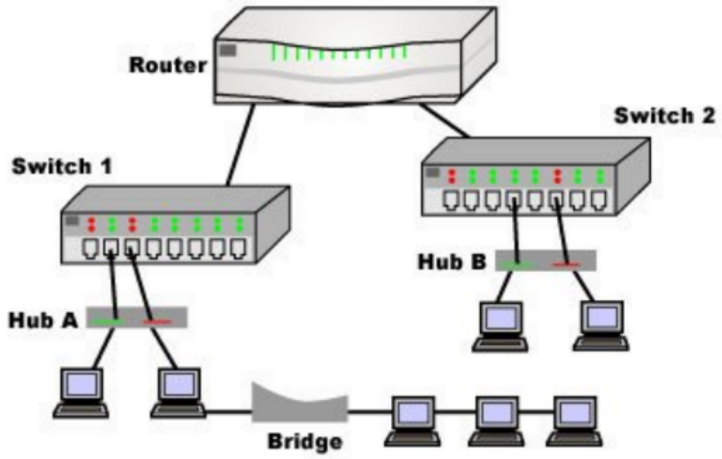
Intelligent hub is another form of hub that is increasingly being used. An advanced version that comprises the best of both active and passive hubs, it provides with the ability to manage the network from one central location. With the help of an intelligent hub, one can easily identify, diagnose problems and even come up with remedial solutions. This troubleshooting of a large enterprise scale network is possible with the help of an intelligent hub. In addition to, an intelligent hub can offer flexible transmission rates to various devices. With standard transmission rates of 10, 16 and 100Mbps to desktop systems using popular technologies like Ethernet, FDDI or Token Ring, an intelligent hub easily incorporates the better of the other two hubs in terms of features and benefits. No wonder, hubs have become an integral part of the current networking systems.

Hub

A Hub is the simplest of these devices. In general, a hub is the central part of a wheel where the spokes come together. Hubs cannot filter data so data packets are sent to all connected devices/computers and do not have intelligence to find out best path for data packets. This leads to inefficiencies and wastage.

As a network product, a hub may include a group of modem cards for dial-in users, a gateway card for connections to a local area network (for

example, an Ethernet or a token ring), and a connection to a line. Hubs are used on small networks where data transmission is not very high.



Bridge

In telecommunication networks, a bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol. Having a single incoming and outgoing port and filters traffic on the LAN by looking at the MAC address, bridge is more complex than hub. Bridge looks at the destination of the packet before forwarding unlike a hub. It restricts transmission on other LAN segment if destination is not found.

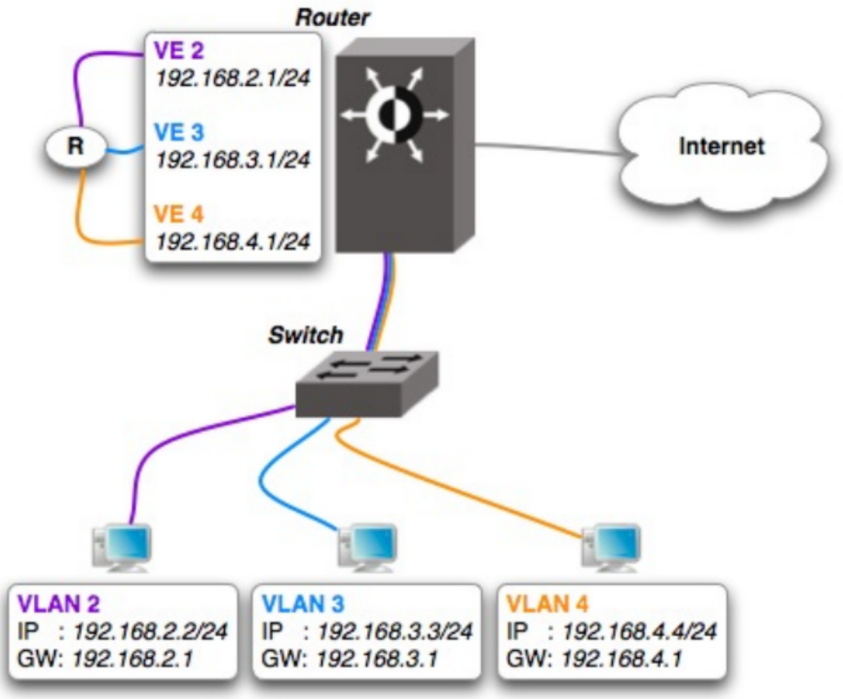
A bridge works at the data-link (physical network) level of a network, copying a data frame from one network to the next network along the communications path.

Bridge Mode	Router Mode
• Does not block any broadcast or multicast	• Blocks and provide protection against broadcast storms
• Transparent bridge and can pass Non-IP protocols	• Only IP protocol is supported
• PPPOE protocol Pass-through	• No PPPOE protocol pass-through
• Able to transport VLAN tagging	• Doesn't supports VLAN
• No network segmentation. One broadcast domain	• Network segmentation (Clients can be on different IP subnet)
• Can only relay the DHCP client's request to the external DHCP server	• Can Act as DHCP server & relay which Prevents IP conflict & DHCP Injection
• Bridges maintains bridging table (Mac) & STP can be used to avoid loops	• No STP feature; maintains routing table
• External bandwidth Controller can be used to control the speed of the clients by Mac or IP address	• External bandwidth Controller can be used to control the speed of the clients by IP only
• In client device, it uses MAC address to associate which requires WDS compatible AP	• Use SSID to associate, work with any 802.11a/b/g AP

Switch

A switch when compared to bridge has multiple ports. Switches can perform error checking before forwarding data, which are very efficient by not forwarding packets that error-end out or forwarding good packets selectively to correct devices only.

Switches can support both layer 2 (based on MAC Address) and layer 3 (Based on IP address) depending on the type of switch. Usually large networks use switches instead of hubs to connect computers within the same subnet.



Router

A router, like a switch forwards packets based on address. Usually, routers use the IP address to forward packets, which allows the network to go across different protocols. Routers forward packets based on software while a switch (Layer 3 for example) forwards using hardware called ASIC (Application Specific Integrated Circuits). Routers support different WAN technologies but switches do not.

Besides, wireless routers have access point built in. The most common home use for routers is to share a broadband internet connection. As the router has a public IP address which is shared with the network, when data comes through the router, it is forwarded to the correct computer.

How do wireless routers transmit data?

The primary purpose of a wireless router is to share an internet connection in the home, but it can also transfer data from one computer to another or to a peripheral device such as a printer. Wireless routers and any computers connected to the network use a transmitter and a receiver to send data back and forth. Information is sent via radio waves, usually at a frequency of 2.4GHz, though sometimes the 3.6GHz and 5GHz bands are used. The wireless router has its own DNS

(domain name system) registry, so it can process requests to view certain websites or pages. Once you enter the URL of a website you wish to visit into the address bar on your computer's browser, the router uses its DNS registry to convert it into an IP (internet protocol) address to direct you to the correct site.

Many new computers come with wireless networking functions as standard, but older laptops and desktop PCs may not and will require further hardware such as a USB dongle or a PCMCIA (Personal Computer Memory Card International Association) card to connect. These can be picked up for as little as 15.

What are the antennae for?

These aren't just for show - they really do play a part in relaying signals from the router to your computers and vice versa. If you're having a problem with a slow connection then you should try setting the antennae to a different position to see if this helps. If it doesn't, you can buy devices that extend the range of your wireless network such as the dLAN Wireless Extender Starter Kit from Devolo (www.devolo.co.uk), which costs around 70. It works by taking advantage of your home's electricity circuits - you plug one of the extender devices into a wall socket and connect it to your wireless router. Then you can plug a second device into another wall socket elsewhere in the house, creating a new wireless access point.

Can I connect wired devices to a wireless router?

Yes - and if your main computer is within a short distance of your wireless router you should definitely connect the two devices using an Ethernet cable to a spare LAN (local area network) port on the router. This will increase the security of the connection between the PC and the router, as well as the speed at which the two can send data to each other.

USB ports on your router let you connect other devices, such as a NAS (network-attached storage) devices and printers, so you can share the storage and printing facilities between all the computers on your network.

Which wireless standard should I use?

There are several standards, all beginning with the code IEEE802.11. The first commonly used standard was 802.11b, which has a maximum data transfer speed of 11Mbps. The 802.11a standard, which was released at the same time, offered faster data transfers, but didn't have as good a range. A few years later, the 802.11g standard emerged, which offered the 54Mbps data transfer of 802.11a with the range of 802.11b. It was also backwards compatible to work with the 802.11b standard, but has since been superseded by the 802.11n standard.

Although this standard hasn't officially been ratified yet by the IEEE (Institute of Electrical Electronics Engineers), most new wireless routers support it. In addition to much higher transfer speeds - up to 600Mbps (in theory, at least) - 802.11n also uses MIMO (multiple input, multiple output) technology, which allows for multiple antennae in both the transmitter and receiver, improving the reliability of the communication between the two. If you are buying a new router, look for one that supports 802.11n, which is also backwards compatible with the other more common standards.

Are there any associated health risks?

Though some scare stories claimed that the radio waves used in Wi-Fi could cause cancer, several of the scientists pushing the theory, such as Professor Olle Johansson of the Karolinska Institute in Sweden, have since been discredited. The UK's Health Protection Agency (HPA) has passed Wi-Fi equipment as safe to use in schools, saying that radio frequency exposures from wireless networks are likely to be less than those from mobile phones.

HOW TO SECURE YOUR WIRELESS ROUTER

The first thing you should do when setting up your wireless network is change the name of your router as well as the default login name and password. If a criminal knows the model name of your router, there is a good chance they can find out what the default login and password are with a quick web search. If they can do this, then they'll be able to use the connection for their own purposes or even alter the DNS to redirect you to websites containing malware.
Secondly, you should ensure you choose an appropriate level of encryption. WEP (Wired Equivalent Privacy) has been shown to be easily cracked and should be avoided if possible. WPA (Wi-Fi Protected Access) is a more secure method though not entirely uncrackable, but WPA II, the latest generation of this encryption standard, is recommended. Any device that connects to your wireless network - whether a laptop, mobile phone or media-streaming device - will need to support WPA II as well. Some older gadgets will not be compatible.