



OSW / appiChar Technical Guide for IT Staff

Section 2: Networking

This section explains the benefits of networking, introduces basic concepts which are useful when thinking about a network and describes different ways of connecting to and linking networks.

Contents:

- Introduction to Networking
- Networking in Layers
- Wired Networking
Cable types, LAN cabling
- Wireless Networking
Point to point links



Introduction

Prior to the personal computer, most work was done using mainframe or minicomputers so that all the data was held on a single machine and it was easy for many users to have access to the same data and resources such as printers.

Although the personal computer brought many benefits, there were and are still a number a drawbacks when there is more than one computer all working stand alone, i.e. not networked together. As the use of PCs became more widespread, many users found themselves producing information which they needed to pass on to others in its original form, such as a word-processed document or spreadsheet. In addition, the cost of hardware meant that the idea of buying a printer for each computer so that everyone could produce hard copy was not particularly attractive.

Without a network, documents and other data needs to be put on some sort of transferable storage medium such as a floppy disk for someone on another machine to use.

Networking allows one user or computer to access data stored on a different computer, possibly created by one or more other users, possibly at the same time as those other users, all using some kind of link between the computers. Other potentially expensive resources can also be shared between many users, reducing costs to an acceptable level.

Computers within a networked environment can *share* a range of resources:

- Disk space
- Printers
- Communications links (e.g. an Internet connection.)
- Applications

With a PC networking environment there are two types of network, elements of which are sometimes combined:

- Peer to Peer
With a peer to peer network, all the computers are equal in status as far as the network is concerned. Each computer is able to share resources and access shared resources on other computers. Each computer is responsible for the control of access to the resources it is sharing.
- Server-based
In a server-based network there is a computer (or sometimes a number of them) dedicated to providing shared resources to all the clients on the network.

Networking in Layers

Descriptions of networking systems are often based on the Open Systems Interconnect (OSI) Reference Model, which splits the functions of a communications system into seven layers. For day to day use this isn't something you really need to remember but it's useful to keep in the back of your mind, especially when fault finding.

The OSI reference model is a layered model, with each layer representing a different level of communication within a networked environment. The following diagram shows the seven different layers that make up the model. A number of layers such as this can be referred to as a stack.

7	Application Layer	Services
6	Presentation Layer	
5	Session Layer	
4	Transport Layer	Networking
3	Network Layer	
2	Data Link Layer	Communications
1	Physical Layer	

Except for the Physical layer, each layer only communicates with the layers immediately above and below it. The Physical layer is the one which provides the link between protocol stacks on different machines (or sometimes even the same machine).

When machines communicate with one another, the design of the model allows each layer to act as if it communicates directly with the same layer on the other machine. Each layer therefore doesn't need to understand or know about the process, functions and services that go to actually sending the information to the other machine.

TCP/IP is usually described using fewer layers which map on to those shown above. This is discussed in the next section.

Application Layer

The Application Layer is the uppermost layer of the OSI reference model, and provides the services to the user. The services and functions at this level will be applications such as database servers and clients, electronic mail servers and clients, and specific network utility applications such as FTP and Telnet, etc.

Presentation Layer

The Presentation Layer encodes the data, given by the Application Layer program, into a format suitable for transmission and subsequent re-coding on the target system. It is also able to compress and encrypt data, change or convert the character sets used and expand graphics commands.

Session Layer

The Session Layer allows applications to establish, use and close communication sessions with a remote machine. This session provides any name recognition and communication functions such as security that allow applications to interact over a network. This layer opens, controls and closes communications between the sender and receiver. It is able to do this using three distinct steps.

- Establishing Connections
- Data transfer
- Connection release

This layer also provides a synchronisation of the user tasks by implementing a checkpointing system in the data flow in order to provide network redundancy. If the network fails, then only the data after the last checkpoint must be sent again.

The Transport Layer

The Transport Layer controls data transportation from source to destination; including error checking, flow control, and reconstructing the message packets. It is the Transport Layer that ensures that communication is delivered error-free, in sequence, and with no losses or duplication of data. The Transport Layer packages messages either by breaking larger packets into manageable packet entities, or by building manageable packet entities from small packets. These packets are then unassembled, and the original messages put together at the other end.

The two main functions of the transport layer are addressing and transport control

The Network Layer

The Network Layer handles the network orientation functions, such as routing and buffering. This layer deals with the translation of logical addresses and names into physical addresses, as well as determining the route from the source to the destination computer, taking into consideration packet switching, routing and controlling the congestion of network traffic.

The three main functions of the network layer are:

- Internetworking
- Routing
- Network control

The Data Link Layer

The Data Link Layer deals with the data frames that are passed to and from the Physical Layer (see below). A data frame is an organised, logical structure used to send the information. It is the Data Link Layer that is responsible for providing the error-free communication of these frames between machines utilising the Physical Layer.

The two main functions of the Data Link Layer are frame packaging and error-free transport

The Physical Layer

The Physical Layer provides a physical channel through a coaxial cable medium. It electrically encodes and physically transfers messages between nodes. This layer handles low-level rules for transmitting bits (ones and zeros), defining any of the electrical, optical, mechanical and functional interfaces to the cable over which the signal is transmitted.

The four main areas defined by the Physical Layer are:

- Network structures
- Transmission media
- Transmission devices
- Data signals

Wired Networking

Cable types

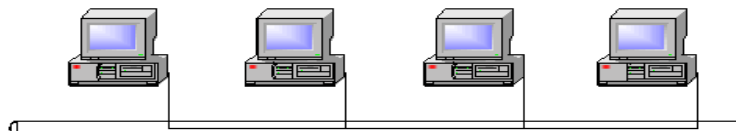
There are three main connection types that you will come across

- Coaxial
Can be thick (typically used for long distances or network backbones) or thin (typically used for LANs)
- Twisted Pair
Can be shielded (STP - used in areas where there might be a lot of interference) and unshielded (UTP - by far the most common cabling type at the moment)
- Fibre optic
Provides immunity from electrical noise, long range and electrical isolation between ends - important when running a connection outside and/or between areas which could be on a different phase for mains electricity.

Generally, there are three network topologies in use: Bus, Ring and Star.

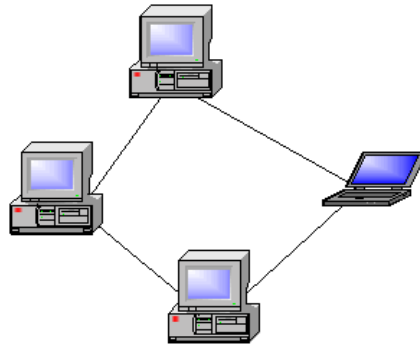
Bus Topology

This is the most widely used topology in early networks, consisting of a length of cable to which the nodes are attached in sequence. The ends of the cable are not joined together but are terminated with end resistors called terminators. If the cable is broken or damaged at any point or either of the terminators are removed then the whole section of cable or segment will stop working. If there's a problem there can be much fun trying to work out which bit of cable or component it is that's actually causing it!



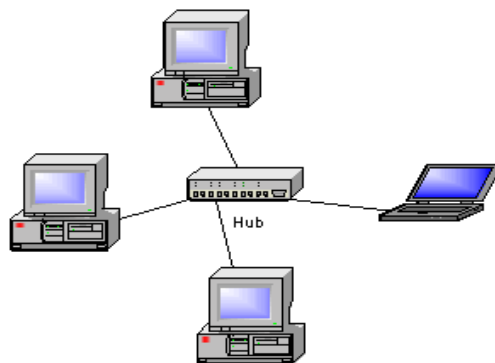
Ring Topology

A Ring topology can be implemented in two ways. The first is the most obviously a ring – cables go from one computer to the next (as with a bus topology) but in this case the ends are joined to form the closed ring. The other and more common option is have a central hub to which all the workstations connect. Physically this looks like a Star topology but the actual data carried on the network still travels in a ring as before. A Ring topology is more resilient to problems with connected nodes than a bus.



Star Topology

In Star topology, each node is connected to a central hub or concentrator. One benefit of this is that if any connection is broken (e.g. a cable fault) between a node and the hub, then no other user is affected. Only failure in the hub will result in more than one user being affected. This kind of topology is the one used by most current LANs.



LAN Cabling

The most common current form of LAN cabling is to use UTP in a Star topology. Each computer or other device connects to a central “hub”. Usually some kind of structured cabling will be used with sockets around a building being wired back to a patch panel in some kind of housing. Patches are then made between the patch panel and the network and possibly the phone system too since both voice and data traffic can be carried over the same kind of cabling.



If you have a patch panel it's a really, really good idea to label at least the important cables. These could include those for the servers, uplinks between hubs/switches, routers and anything else where it might be useful to know where it's plugged in.

It's also worth having a defined colour scheme for cables. For example, grey for workstations, green for voice and red for servers. Patch cables are available in a huge range of colours so there's plenty of scope although don't over do it!

Wireless Networking

There are a number of different standards for wireless links which can be used for/within a LAN and to link LANs together. Most of the LAN options are referred to by their IEEE standard number. The most common is 802.11b which provides for up to 11 Mbps, with steps down to 1 Mbps depending on environment. Others include 802.11a and 802.11g. When buying 802.11b equipment look for the WiFi logo which will guarantee that the equipment will work together.

Groups of 802.11 devices are identified by the SSID which must be the same for all the devices in the same group. 802.11b can be configured in three different ways although not all are supported by every type of device. The three different arrangements are Ad-hoc, Infrastructure and Bridging.

Ad-hoc

Each computer must be configured in to Ad-hoc mode and given the same SSID and channel number (although some drivers may be able to do this automatically). Each computer communicates with every other computer, giving what is effectively a mesh of connections. Because of this, Ad-hoc operation can become very inefficient and so performance will drop if there are more than a few computers.

Infrastructure

This requires what is called an Access Point. Effectively this functions like a hub in a wired network. Each computer just communicates with the Access Point rather than each other which makes the network more efficient with a larger number of computers. Access Points are also often used to provide a bridge between wired and wireless networks. Some computers may be able to take on the role of an access point in what would otherwise be an Ad-hoc network, OS X on the Machintosh can certainly do this.

Bridging

Two access points may be used to provide a bridge between wired networks in different locations. This can be useful in situations where large amounts of bandwidth are not required and it would not be economic to install fibre or one of the other point to point options.

Wireless Security

Wireless networks based solely on 802.11b aren't very secure, even if you do enable WEP (Wired Equivalent Privacy). WEP is at least better than nothing and will stop casual "passers by" from using your network.



<http://arstechnica.com/paedia/w/wireless-security-howto/home-802.11b-1.html>



<http://www.warchalking.org/>

Point to point links

Sometimes it is necessary to link sites or parts of a site but it is usually not possible to run a simple cable between the them. Even if you could run a cable, there could be good reasons, such as the other area being on a different electrical phase, not to do so – in this case you would probably use fibre instead of copper cable. Options also include laser and microwave.

If you're not too concerned about bandwidth between points then you could look at using a pair of 802.11 access points. Be aware though that not all access points support *bridging* which is what this feature will usually be called. Also, most will usually only be an access point *or* a bridge, not both at the same time.