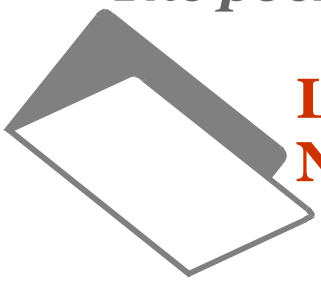
Case Communications

The pocket book of



LOCAL AREA NETWORKS

CONTENTS

1. INTRODUCTION

A definition of LANs

Local area network (LAN) is not a precise term but one definition could be as follows.

"A local area network provides a system for inter-communication between computer terminals, PCs and related equipment operating within the same general area."

The initial introduction of LANs was based on the sharing of information and resources within a local work group or department. While this still continues to be the main use for LANs, it is perhaps better to regard them as a tiered system of work group networks. For example, where a small department has a LAN to connect its PC, printers and fileservers, they may also wish to share information with users in another department, connected on another LAN. Therefore a backbone LAN links these, and possibly other departmental LANs together. In addition, it may still be necessary to access some larger, mini computers or central computers. This can also be achieved using the backbone LAN, allowing any user, on the backbone or any departmental LAN access if so authorised.

During the late 1980's and early 1990's LANS were more complex and it was not simply a matter of choosing the right cable to be able to inter-work. Equipment protocols and even applications needed to be carefully chosen to ensure that not just compatibility, but also optimum network performance, was achieved. Over the last few years for better or worse the world has gone towards the Internet Protocol (IP), making the issue of protocol selection almost redundant. The drive to IP was largely due to the fact it was supplied free with Unix, and more powerful and complex protocols, such as OSI, fell by the wayside.

A brief history of LANs

In recent years a major change has occurred in computer use. In the first half of the 1970s in the major industrialised countries there were more companies than computers. By the middle of the 1980's there were more computers than companies. This phenomenon was due to the advent of the small Personal Computer (PC).

What the PC did was to change the perspective of the manager, from using a central computer, designed for a specific set of jobs, towards using a desktop tool assimilating information, supporting decisions and, more recently, improving the quality of personal output and hence productivity.

The advent of department computers, or distributed processing, generated new needs in computer communications. Previously these had centred on attaching terminals to a large central computer (mainframe), often over large distances. The advent of the PC began to introduce needs for sharing information and resources, such as high quality printers and shared servers, within the local area, and usually involved operation at higher speeds than had been traditional in data communications.

This need drove the development of the local area network – a term which was originally coined in America by the Xerox Corporation. In fact the word 'Local' is a misnomer as LANs can operate between buildings and even internationally.

Initially it was envisaged that a LAN would extend across one floor of a building or possibly throughout a building. Since that time, and in response to the meteoric growth in LAN implementation, many new capabilities have been developed. These have extended the operation of LANs to the level of one of the most sophisticated transportation methods available today.

Unfortunately, as with many developments, market growth left standards organisations lagging behind the development programmes of commercial organisations. As a consequence, in the earlier days of LANs several different types appeared which could not be linked to one another, thereby creating confusion in the marketplace.

Fortunately the standards organisations managed to recoup much of the lost ground using the Open Systems Interconnection (OSI) reference model; the majority of the necessary standards were produced and implemented by most suppliers.

Some confusion still remains, however, as there are several distinct types of standards networks and protocols. These are explained in detail in the following section.

2. MAIN TYPES OF LAN

The operation of a LAN can usually be separated into two main aspects.

Firstly – the physical medium (connector types, voltage and electrical signals) and the method of placing data onto the network. In OSI systems this corresponds to layer 1 and the lower part of layer 2 of the reference model.

Secondly – the operating software which establishes end-to-end transmission with guaranteed data delivery between two devices, communicating across the network. In OSI systems this corresponds to the upper part of layer 2, layer 3 and layer 4 of the reference model.

Carrier Sense Multiple Access with Collision Detect (CSMA/CD) – Ethernet

'Ethernet' is one of the most widely known terms in LAN technology. The term derives from the original network which was defined by Xerox and adopted by several other organisations including DEC (Digital Equipment Corporation) and Intel. The original published specifications were known as DIX (Dec, Intel and Xerox) Ethernet Specifications Versions 1 and 2. The Institute of Electrical and Electronic Engineers (IEEE) adopted, improved and modified the DIX version 2 specification and this has become the IEEE 802.3 standard, which equates to the ISO 8802/3 standard.

Carrier Sense Multiple Access with Collision Detect (CSMA/CD) networks operate using a bus structure, that is a single strand of cable to which all devices connect. It uses baseband communications (i.e. only one signal can travel on the cable at one time) at 10Mbps (10,000,000) bits per second, although the original 10Mbps gone on to become 100Mbps and now Gbps. Most Servers and Ethernet switches support links of 1Gbps, with higher end devices supporting 10Gbps with 100Gbps expected soon.

Carrier Sense Multiple Access with Collision Detection

Using Carrier Sense Multiple Access with Collision Detection means all devices on the LAN are free to communicate whenever they need to without any precedence or order. A device wishing to send monitors the network (Carrier Sense) and, if no other device is sending, begins to transmit. It is possible that another device will also start to transmit at that moment (Multiple Access), so the device checks for a collision (Collision Detect). If a collision occurs, (this is the transmitting station detects another station on the LAN) then all devices involved in the collision stop, the device that was transmitting the frame, transmits a jam signal, and pauses for a period, of time known as the 'back off delay' (which is determined using the truncated binary exponential backoff algorithm) before trying to send that frame again.
All devices monitor the network continuously, copying and acknowledging all packets addressed to that device.

Accessing a network in this way is known as probabilistic or non-deterministic. Probabilistic because the ability of any one station to transmit on the network is based on the level of activity on the network: The higher the level of activity the lower the chance. Non-deterministic because the designer is unable to guarantee the level of performance or delay which will be experienced by any one station on the network under particular loading conditions.

The original 10 Base 5 (Thick Ethernet) topology of Ethernet is that of a branching tree structure with interconnecting segments (see figure 1). A loop in the interconnection segments must be avoided. Each segment can be up to 500 metres in length with a maximum number of 100 network nodes (or taps) per segment. To extend beyond the maximum length or number of devices, segments are linked together with repeaters or half repeaters. These simply extend the length of the network by effectively regenerating and repeating the signal. A repeater connects two local network segments. A half-repeater implements a transmission line between two segments therefore enabling a greater distance to be spanned between two segments. There is a limit of four repeaters or half repeaters, which can be supported between any two points on the network. To extend the network further bridges and routers can be used.

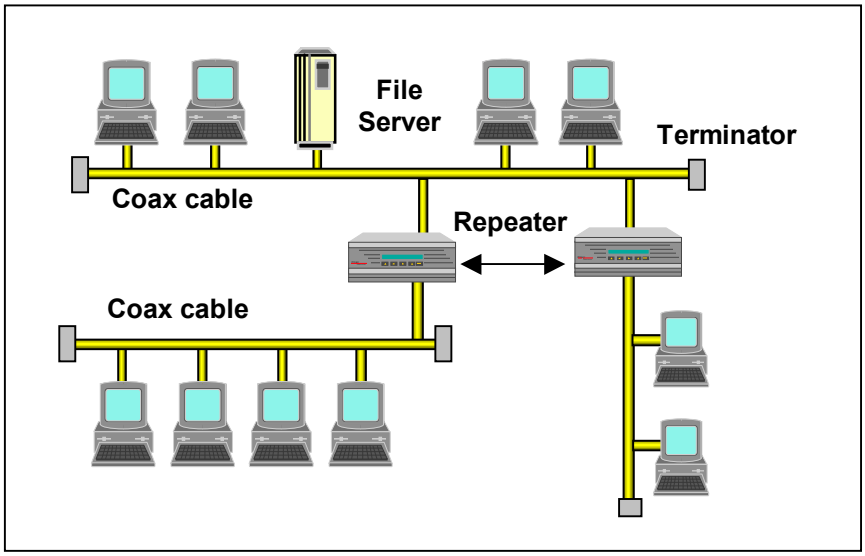


Figure 1: *CSMA/CD Tree Structure*

A significant factor of original Ethernet or CSMA/CD networks was the cost of the co-axial cable. The IEEE standard specifies the use of quality coaxial cable ("Yellow cable") or a thinner cheaper co-axial cable (RG58 specification). These are termed 10 Base 5 and 10 base 2, referring to 10 Megabits per second (MBPS) BASEband transmission 500 metres maximum segment length, and 10 Mbps BASEband transmission 200 metres maximum segment length respectively. 10 Base 2 is often referred to as "Cheapernet" and has an actual maximum segment length of 185 metres and a maximum of 30 taps per segment.

At the time of writing this booklet 10 Base 5 and 10 Base 2 are less common and it is far more common to see 10BASE T (10/100 Mbps BASEBand transmission on twisted pair cable). This has a maximum segment length of 100 metres and 1 tap, i.e. it is point-to-point only.
Ethernet is the most common form of LAN technology installed today due to its early arrival in the marketplace. Originally there were two important concerns regarding this type of technology.

Firstly – the term Ethernet does not guarantee compatibility of hardware, as there are three different standards:

- DIX Version 1
- DIX Version 2
- IEEE 802.3

Previously it was imperative to see confirmation before installing some of the older DIX network components on IEEE type networks. However it would be unusual to purchase any non-802.3 devices today, so the issue of incompatibility is less likely to arise nowadays.

Secondly – degradation of performance under loading is non-linear and the performance of most networks can degrade significantly under sustained heavy network loads.

Because the term 'Ethernet' was in generic usage, it was important that specifiers defined exactly what level of standards compliance was required (e.g. IEEE 802.3/ISO 8802-3). Today it would be unusual to purchase products which do not conform to IEEE 802.3.

CSMA/CD Efficiency

CSMA/CD has a minimum frame size of 64 bytes, (if the payload is smaller the network will pad the frame out to 64 bytes) in order for the collision detection mechanism to work, and a maximum frame size of 1518 bytes (1522 bytes when running Tagged VLANs).

Token Ring

Token Ring is based on a closed loop philosophy so that eventually a station will receive its own transmission. The token is a single special sequence, which circulates around the loop, with each station on the ring receiving and regenerating the token. When a station wishes to transmit data, it waits for the token, adds addressing information plus the data, marks the token busy and then sends the token to the next station. All the stations on the network continue to receive and regenerate frames, but if a station wishes to send data it must wait for the token to become free. A station, which receives a token addressed to itself, copies the data and regenerates the frame. Eventually the sending station detects the return of its busy frame, removes it and then transmits a free token, giving the next station an opportunity to send.

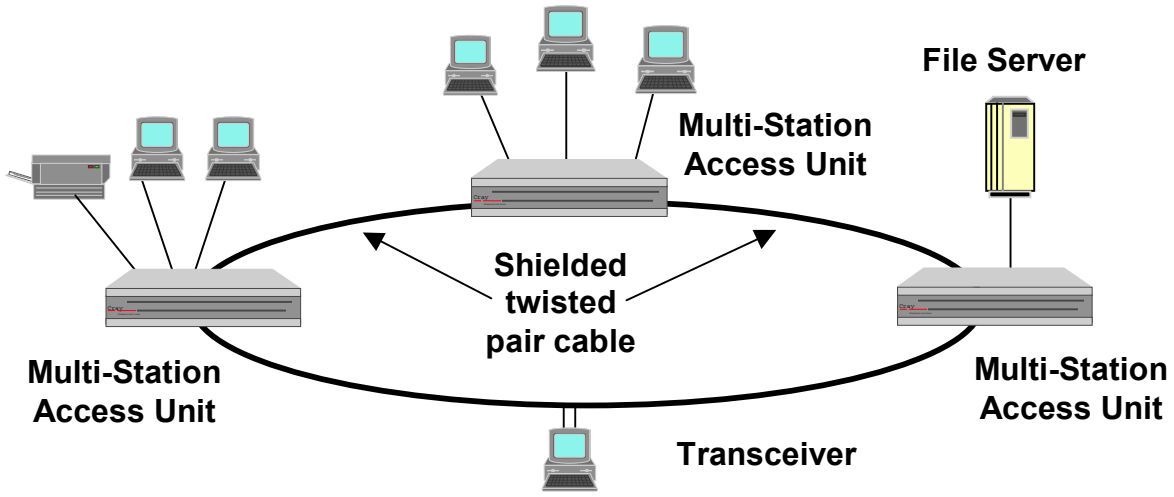


Figure 2: *IBM Token Ring Structure*

A new form of token passing was developed to improve network efficiency. It was called 'early token release' and allowed the token to be released immediately after a data frame had been transmitted. This reduced the delay time, as the station no longer had to wait for its data packet to return, which could take a considerable time on a network with many devices.

There are many types of network employing Token Ring – The IEEE 802.5 standard. The most common is the IBM Token Ring System originally operating at 4Mbps, and then 16Mbps.

The standard specification uses a twisted pair cable running baseband communication at 4Mbps. This offers a cost advantage over the original Ethernet, which operated on co-ax cable, as twisted pair cabling is cheaper. However the IBM full specification screened cabling can be expensive. The introduction of 10Base T Standards for Ethernet (Ethernet operating on twisted pair cable) has effectively addresses this difference by allowing transmission over unscreened cable.

While Token Ring is the architecture of this type of LAN, the IBM Token Ring network need not be a physical ring topology (see figure 2). A device called a Multi-Station Access Unit (MAU) will act as the centre of a star-based ring topology. Unlike Ethernet, Token Ring is not naturally resilient and the removal of a station in the ring would cause all data to stop. To protect against this, the MAU monitors each attached device and heals the ring should a break occur. A MAU supports a number of attached devices (usually seven) and then attaches to other MAUs in the network. In fact the MAU may support one or more sub rings on any of its connections rather than a single device. As with CSMA/CD network repeaters can be used to extend the ring, possibly between two buildings, although repeaters do not increase the maximum number of devices, which can be supported by the network.

As previously stated, the main limitation of a ring topology is that a break in the ring causes the whole network to fail. The MAU maintains an active configuration path so that any failure is detected and circumvented immediately, causing the ring to recover gracefully, so that all users, except those on the failed section, will be unaware that the failure occurred. One of the consequences of this type of fault is that a device could fail or become disconnected while it still has the token, and the token may become lost, or a device may fail after transmitting a busy token and therefore be unable to release the token. In both cases an arbiter is responsible for detecting the anomalous condition and taking corrective action.

Where MAUs are not used, a device is available for connection between the ring and attached device, which produces the same recovery function as the MAU.

The main limitation on the topology is a maximum distance of 100 metres between stations (this allows for the failure of a station at 200 metres, which can be supported during failure). A ring supports a maximum of 33 MAUs and 260 stations, although the network can be extended past these limitations by using bridges and routers to link the rings.

The benefit of Token Ring is that a station can only hold the token for a predetermined period, thus giving all stations an opportunity to transmit on a regular basis whatever the level of traffic on the network. Another benefit over CSMA/CD or Ethernet is that there are no collisions and therefore the performance degrades linearly under heavy loading.

Token Bus

Token Bus combines the bus structure of Ethernet type networks and the token system in Token Ring. The standard form of transmission uses broadband communication on co-axial cable. Broadband communication divides the signals on the network into different frequencies, allowing more than one signal to travel on the cable at any one time. This can be compared with the use of co-axial cable for carrying several television signals simultaneously. Signals are normally generated in pairs and one cable may support several different pairs. A

variety of speeds may be used, four 1 Mbps pairs, one 5 Mbps pair or one 10Mbps pair. The most common form currently is the 5 Mbps pair.

The network needs to be able to transmit to all devices on the bus. Therefore the signal is divided, and two channels – forward and reverse – are implemented. When a signal reached the head end of the network the signal on one channel is re-modulated (i.e. the frequency is changed) and then output on the other channel. This allows any station to broadcast to any other station, regardless of its position on the network. As token passing is implemented, and the network does not form a ring, a logical ring is implemented. This uses the addresses of the devices on the network and each device transmits the token to the next logical address on the bus.

The use of broadband requires a more complicated signalling system and involves a form of modem for each device attached to the network. The network also requires a device at the head end to re-modulate and regenerate the signals. It can therefore be more expensive to implement than baseband.

The specification is covered by the IEEE 802.4 standard. While Token Bus is not widely used, the most common implementation is in Manufacturing Automation Protocol (MAP) networks.

The benefits of Token Bus are that cabling is far easier to implement than a ring topology and superior performance to CSMA/CD can be achieved under high loading conditions by collision avoidance, as token passing is implemented. However, as a logical loop is employed, the token must be captured and regenerated before it can be sent to the next device in the logical loop, which produces large overhead on the network. To reduce this overhead, multiple transmissions can be implemented during token capture by the device seizing the token. However, this only partially resolves the problem as the token can only be held for a limited period.

Fibre Distributed Data Interface (FDDI)

FDDI is a standard issued by the American National Standards Institute (ANSI). It is based on Fibre optic cable, token passing access methods and a ring topology. It is effectively a token ring network, which can be up to 100km in length, and operates at 120Mbps, but after removing overheads, provides useable bandwidth of 100Mbps.

With a maximum distance of 100km this network belies the term local area network. The network should perhaps be regarded as a backbone, linking buildings and central resources to a series of small, lower cost LANS in each department or floor as required. Such reasonable capacity, long distance, backbone networks are often referred to as Metropolitan Area Networks (MANs). Another application area for FDDI could be for, more specialised workstations such as those used in Computer Aided Design (CAD) where large amounts of data may need to be transferred from host computer to terminals on a frequent basis, (See figure 3 ‘FDDI Structure’)

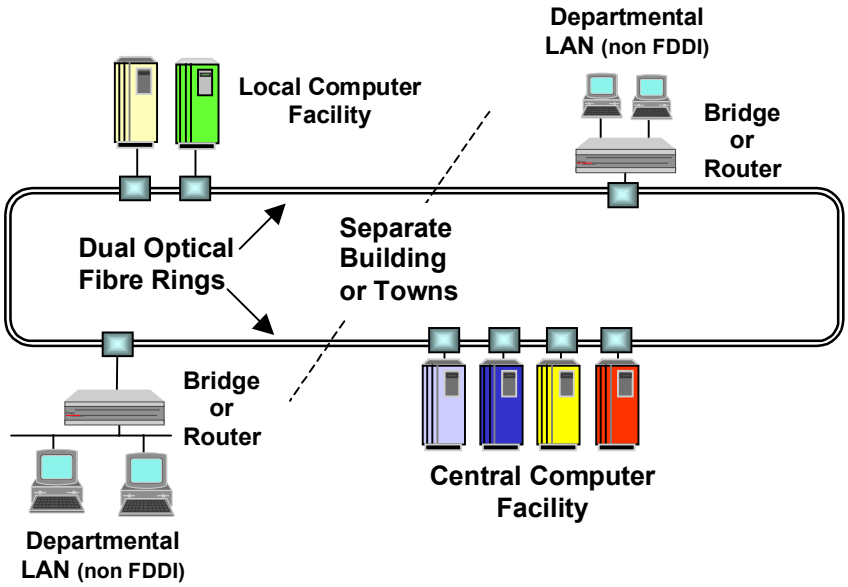


Figure 3: *FDDI Structure*

FDDI offers several key benefits over conventional networks.

Firstly – the specifications implements dual counter rotating optical rings bestowing fault tolerance to the ring and attached nodes.

Secondly – more than one packet can travel the network at the same time, allowing better use of the large size of the network and capability of the optical cable.

Thirdly – the maximum packet size is much larger than other networks, thus enabling efficient data transfer, especially for devices using particularly large amounts of data, such as graphics workstations.

Fourthly- since fibre optic cable uses light it is free from all normal forms of electrical interference. Errors in the data are therefore very low and few retransmissions are required, increasing the bandwidth available for attached devices.

Finally – the use of token passing eliminates collision problems and this has been further developed to allow different devices to be prioritised for network usage. Therefore, key devices and those with high data volumes can be given priority, eliminating possible delays.

The four standards for FDDI are:

- ANSI X3T9.5, containing Physical Media Dependent (PMD) specifications
- ANSI X3T9.5, containing the Physical (PHY) specifications
- ANSI X3.139, containing Media Access Control (MAC) specifications
- ANSI X39.5, containing the Station Management (SMT) specifications.

Other types of LAN

Many proprietary networks were developed the most common of which was Apple Talk and ARCnet. Some proprietary networks offered ‘standards conformance’ but this phrase may be misleading as they may have been developed using a model similar to the OSI model, but not

one, which is fully conformant. The only guarantee of standards conformance is certification by an independent testing body.

Apple Talk

Apple Talk is a proprietary networking protocol designed by Apple Computers. The Apple Talk protocol, which is layered, has been published so that companies wishing to produce products to work over Apple talk can do so.

When Apple first released Apple Talk, the term encompassed all levels of the protocol stack, including the physical media. Subsequently Apple redefined the physical layer as Local Talk, and the upper layers as AppleTalk. This was then followed by an Ethernet implementation called EtherTalk, and recently Token Ring implementation called Token Talk.

LocalTalk utilises a bus topology using baseband transmission. The physical cabling is shielded twisted pair operating at 230 Kilobits per second (kbps), significantly slower than the main standard network types. The maximum length of a network is 300 metres. The method of accessing the bus is a variant of CSMA/CD, termed Carrier Sense Multiple Access with Collision Avoidance.

Local Talk can be easily installed at a very low cost. Every Apple system is automatically equipped with the necessary hardware to communicate across the network, the software is supplied as standard with each system, and therefore only the cable and a link point, commonly called a ‘Rats Tail’, is required for connection.

Ethernet Talk and TokenTalk both require an additional card in each Macintosh, but allow network operation at higher speeds (10 Mbps and 4Mbps respectively). With Ethernet it was possible to implement an OSI solution for Macintosh networking, and now an IP solution.

ARCnet

(An acronym for Attached Resource Computer NETwork) ARCnet was developed by the Datapoint Corporation and is a proprietary LAN. ARCnet was the first commercially available LAN and was introduced in 1977. The network uses baseband transmission at a speed of 2.5Mbps. Token passing is used as the access method and either a ring or bus topology can be used. The system was originally designed to operate on thin co-axial cable but later developments have incorporated both twisted pair and optical fibre support.

The network is relatively inexpensive to install and, due to its early entry in the market, it has established a large installed base. However it is rarely chosen today.

The network is not standards-based and is also a lot slower than the standard networks of today. ARCnet usage will decline quickly as standards and speed begin to dominate the marketplace. In the early 90’s, Thomas-Conrad Corporation developed a 100 Mbit/s topology called TCNS based on the ARCNET protocol, which also supported RG-62, twisted-pair, and fibre optic media. TCNS enjoyed some success until the availability of affordable 100 Mbit/s Ethernet put an end to the general deployment of ARCNET.

3. PHYSICAL MEDIA

For Local Area Networks to function they require a physical media over which to operate, which might be seen as the first layer or physical layer in the OSI model. In the past this would have been 10Base 5, or 10 Base 2 Coax, but the most common type of cabling at the time of writing is UTP (Unshielded Twisted Pair). Alternate media that are also used are fibre optic, or wireless systems which have become more popular in recent years The following paragraphs provide an overview various media options.

Copper Cabling

Co-axial

Co-axial cable (sometimes referred to as 'co-ax), is based on a central copper core encased in a plastic sheath which is then surrounded in a plastic coating.

The signal is carried on the central core with the outer conductor or mesh forming a screen to outside electrical noise. The most common example of co-axial is television aerial cable. Originally this form of cable was the most common form of LAN cable due to its high capacity and resistance to interference.

Its main disadvantage is its thickness, which means it is limited in its ability to be run through small cable ducts and around tight angles. Also, the cost of co-ax is relatively high in comparison to more traditional forms of data cabling.

While coax, both thick and thin is rarely used, most of the networks, which specified this cable type, are now able to operate on other types such as unshielded twisted pair (UTP) or on fibre.

Thick Ethernet

This form of cabling, often known as "Yellow Cable" was the original co-axial cable used by most networks, with Ethernet being the main champion of such cable. Its capacity in terms of distance is great, but the cost of cabling is high and its thickness prohibitive in tight cable runs and cabling ducts, which may already be relatively full.

Thin Coax

Thin coax (RG58) was introduced to reduce the cost of cabling networks. This was mainly associated with Ethernet and became known as 'Cheapernet'. Its main sacrifice over Ethernet is the distance that a single branch can run. However the cable is much cheaper and thinner, and therefore overcomes some of the disadvantages of the original cable.

Twisted Pair

Today twisted pair cabling is the most common form of cabling. It originated as the method for connecting telephones to the local PABX with the same wiring used to connect data terminals to computers around a building.

The pairs are twisted to reduce the interference between adjacent pairs in the cable. Usually a series of pairs are encased in a single sheath and colour coded to reduce the numbers of physical cables, which need to be pulled through the ducting.

Twisted Pair – Unscreened

The main advantage of this type of cable is that its lower cost, easy to handle and cables already laid for other devices can often be re-used to implement a LAN.
The main drawbacks are its relatively high error rate and the short distances which can be run without signal regeneration.

Twisted Pair – Screened

Screened twisted pair has been introduced to reduce the number of errors due to outside interference. The wire is encased in a metallic braid, somewhat similar to co-axial cable. This reduces errors but also raises costs.

Categories of Twisted Pair Cable

Category 5 cable – Cat 5
Commonly known as Cat 5, this is an unshielded twisted pair cable designed for high signal integrity. The actual standard defines specific electrical properties of the wire, but it is most commonly known as being rated for its Ethernet capability of 100 Mbit/s. Its specific standard designation is EIA/TIA-568. Cat 5 cable typically has three twists per inch of each twisted pair of 24 gauge copper wires within the cable. Another important characteristic is that the wires are insulated with a plastic (FEP) that has low dispersion, that is, the dielectric constant of the plastic does not depend greatly on frequency. Special attention also has to be paid to minimizing impedance mismatches at connection points.

It is often used in structured cabling for computer networks such as Fast Ethernet, although it is often used to carry many other signals such as basic voice services, token ring, and ATM (at up to 155 Mbit/s, over short distances).

Category 5 (Cat 5) Patch Leads
Patch leads created from Cat 5 are often terminated with RJ-45 electrical connectors. Normal Cat 5 cables are wired “straight through” and connect a computer to a hub or switch. In other words, pin 1 is connected to pin 1, pin 2 to pin 2, etc. The RJ-45 pinout for a Cat 5 cable can either be TIA-568A or TIA-568B. TIA-568A is used by some phone systems and Token Ring. Most everything else, such as the Ethernet standards 10BASE-T and 100BASE-TX, use TIA-568B.

In Ethernet, “crossover” Cat 5 cables are cables in which pairs two and three are reversed. (For 100BASE-T4 a more complex connection layout is needed.) These are most often used to connect two PC’s NICs directly (with no intervening hub). They can also be used to connect two hubs or switches together. However most hubs and switches either have an uplink port, a button to change a port to uplink or one or more ports with autosense (most modern switches now have autosense on every port). These features eliminate the need for crossover cables when connecting them.

Category 5e Cable (CAT5e)
Cat 5e cable is an enhanced version of Cat 5 for use with 1000 Base-T networks, or for long-distance 100 Base-T links (350 m, compared with 100 m for Cat 5). It must meet the EIA/TIA 568A-5 specification.

Category 6 Cable (CAT 6)
Cat 6 is a cable standard for Gigabit Ethernet and other interconnect that is backward compatible with Category 5 cable, Cat-5e and Cat-3. Cat-6 features more stringent specifications for crosstalk and system noise. The cable standard is suitable for 10BASE-

T/100BASE-TX and 1000BASE-T (Gigabit Ethernet) connections. It is suitable for 1000 Base-T (gigabit) Ethernet up to 100 M.

The cable contains four twisted copper wire pairs, just like earlier copper cable standards. When used as a patch cable, Cat-6 is normally terminated in RJ-45 electrical connectors. If components of the various cable standards are intermixed, the performance of the signal path will be limited to that of the lowest category.

Category 7 cable (CAT7)
Cat 7 (ISO/IEC 11801: 2002 category 7/class F), is a cable standard for Ultra Fast Ethernet and other interconnect technologies that can be made to be backwards compatible with traditional CAT5 and CAT6 Ethernet cable. CAT7 features even more stringent specifications for crosstalk and system noise than CAT6. To achieve this, shielding has been added for individual wire pairs and the cable as a whole.

The CAT7 cable standard has been created to allow 10-Gigabit Ethernet over 100M of copper cabling. The cable contains four twisted copper wire pairs, just like the earlier standards. CAT7 can be terminated in RJ-45 compatible GG45 electrical connectors which incorporate the RJ-45 standard, and a new type of connection to enable a smoother migration to the new standard. When combined with GG-45 connectors, CAT7 cable is rated for transmission frequencies of up to 600 MHz.

EIA/TIA-568A and EIA/TIA-568B Pin Outs

EIA/TIA-568A and EIA/TIA-568B are closely related joint Electronic Industries Alliance (EIA), Telecommunications Industry Association (TIA), and International Telecommunications Union (ITU) standards for twisted pair wiring. They define the pinout, or order of connections, for wires in RJ-45 8-pin modular connector plugs and jacks used with Category 3, Category 5 and Category 6, 4-pair cables.

Both TIA-568A and TIA-568B are used by many modern computer LAN media on twisted pair cable, such as Ethernet 10BASE-T, 100BASE-TX and 1000BASE-T. They are also used by many digital telephone PBX systems.

The reason there are two conflicting standards is that the EIA/TIA produced TIA-568A long after AT&T developed its own, different convention known as 258A. By the time TIA-568A was published, AT&T 258A had become so widespread that it could not easily be discarded. So the EIA/TIA blessed the AT&T 258A convention as TIA-568B.

Some advocate that TIA-568A be preferred to TIA-568B in new installations because the mapping of pair numbers to telephone line numbers is more consistent with TIA-568A. However, the TIA-568B (AT&T 258A) convention is solidly entrenched and seems to show no signs of going away.

Pairing and colours

The eight wires in the cable are grouped into four pairs. According to telephony tradition dating from the days of manual switchboards, one wire in each pair is the *tip* and the other is the *ring*. Each wire pair is twisted within the cable to reduce crosstalk with the other pairs. The pairs *must* be used as such; if a cable is incorrectly wired to group wires from different pairs into a single pair, the network will almost certainly malfunction. In telephony, hum, noise and crosstalk may be present. This is known as a *split pair* error.

The cable pairs are assigned the first four entries in the AT&T standard for colour codes in 25-pair and larger cables. The ring wire is assigned the primary color with a stripe of the secondary color, and the tip wire is assigned the secondary color with a stripe of the primary color. In many cables, the tip wire lacks the secondary color stripe; the solid primary color is used.

The primary color of pair 1 is blue, pair 2 is orange, pair 3 is green and pair 4 is brown. The secondary color for all four pairs is white. It is important to note that because these wire color codes come from an old AT&T standard, they are the same for all 8-pin termination standards, TIA-568A, TIA-568B, and USOC-8 (RJ-61). Only the specific assignments of pairs to connector pins varies among these standards.

Wiring

Regardless of the wiring standard, RJ-45 modular jack pins are numbered 1 through 8 as shown:

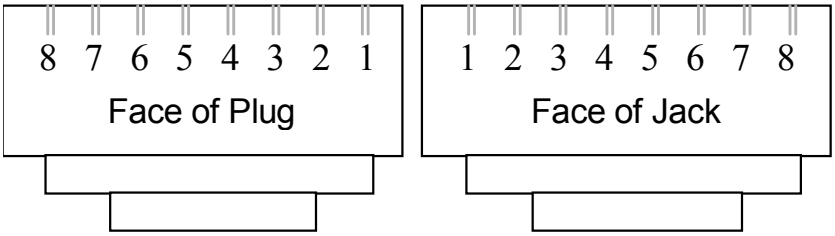


Figure 4: *RJ45 Modular Jack Wiring*

The assignments of wire pairs to plug and jack pins are as follows:

RJ-45 Wiring (EIA/TIA-568A/B)					
Pin	**-568A Pair**	**-568B Pair**	**Wire**	**-568A Color**	**-568B Colour**
1	3	2	tip	white/green stripe	white/orange stripe
2	3	2	ring	green/white stripe	orange/white stripe
3	2	3	tip	white/orange stripe	white/green stripe
4	1	1	ring	blue/white stripe	blue/white stripe
5	1	1	tip	white/blue stripe	white/blue stripe
6	2	3	ring	orange/white stripe	green/white stripe
7	4	4	tip	white/brown stripe	white/brown stripe
8	4	4	ring	brown/white stripe	brown/white stripe

Figure 5: *Assignment of Wire Pairs*

Note that the only difference between TIA-568A and TIA-568B is that pairs 2 & 3 (orange and green) are swapped. Both standards wire the pins “straight through”, i.e., pins 1 through 8 on one end are connected to pins 1 through 8 on the other end. Also, the same sets of pins are paired in both standards: pins 1&2 form a pair, as do 3&6, 4&5 and 7&8. Since electricity doesn’t care about wire insulation color, only about pin connections and pairings, cables wired to either standard are interchangeable.

In other words, *the choice between TIA-568A and TIA-568B is arbitrary* as long as both ends of each cable follow the same standard (except for crossover cables, see below). Different cables may follow different standards.

So if your wiring consists entirely of connectorised cables (i.e., cables that terminate directly in a RJ-45 jack or plug), especially if you buy pre-connectorised cables, then you don't really need to choose a standard.

But if you make a lot of cables yourself, and especially if you have punch-block cross-connects or patch panels, then it becomes important to pick one standard and make it the local site convention to avoid confusion. Both standards are widespread, and neither shows signs of going away although there seems to be a trend to TIA-568A in new equipment and construction.

Crossover wiring

10BASE-T and 100BASE-TX use one pair for transmission in each direction. The Tx+ line from each device connects to the tip conductor and the Tx- line is connected to the ring. This requires that the transmit pair of each device be connected to the receive pair of the device on the other end. When a terminal device is connected to a switch or hub, this crossover is done internally in the latter. A standard *straight through* cable is used for this purpose where each pin of the connector on one end is connected to the corresponding pin on the other connector. Because the connector pin pairings are the same in TIA-568A and TIA-568B, any given cable may be wired to either standard and it will work; the choice between TIA-568A and TIA-568B is arbitrary.

One terminal device may be connected directly to another without the use of a switch or hub, but in that case the crossover must be done externally in the cable. Since 10BASE-T and 100BASE-TX use pairs 2 and 3, these two pairs must be swapped in the cable. This is a *crossover cable*. A crossover cable must also be used to connect two internally crossed devices (e.g., two hubs or switches) as the internal crossovers cancel each other out.

Because the only difference between TIA-568A and TIA-568B are that pairs 2 and 3 are swapped, a crossover cable is just a cable with one connector following TIA-568A and the other TIA-568B.

Many newer Ethernet NICs, switches and hubs automatically apply an internal crossover when necessary. This feature is known by various vendor-specific terms, e.g., Netgear calls it *Auto uplink*™ and other common vendor terms include *Auto-MDI/MDI-X*, *Universal Cable Recognition* and *Auto Sensing*. This eliminates the need for crossover cables, obsoletes the uplink/normal ports and manual selector switches found on many older hubs and switches, and vastly reduces installation errors, especially by non-technical users.

Crossover cables are never necessary in 1000BASE-T (Gigabit)as all four pairs are used bidirectionally. All 1000BASE-T connections should be made with straight-through cables using Category 5e cable or better that provides all four pairs.

Backwards compatibility

Because pair 1 connects to the center pins (4&5) of the RJ-45 jack in both TIA-568A and TIA-568B, both standards are compatible with the first line of RJ-11, RJ-14 RJ-25 and RJ-61 connectors that all have the first pair in the center pins of these connectors.

If the second line of a RJ-14, RJ-25 or RJ-61 plug is used, it connects to pair 2 (orange/white) of jacks wired to TIA-568A but to pair 3 (green/white) in jacks wired to TIA-568B. This makes TIA-568B potentially confusing in telephone applications.

Because of different pin pairings, the RJ-25 and RJ-61 plugs cannot pick up lines 3 or 4 from either TIA-568A or TIA-568B without splitting pairs. This would most likely result in unacceptable levels of hum, crosstalk and noise.

Because 10BASE-T and 100BASE-TX use only pairs 2 and 3, pairs 1 and 4 need not even be present in the cable. It is also common in some networks to use one 4-pair Category 5 cable to provide two separate 10BASE-T or 100BASE-TX links, assigning only two pairs to each link. However, such jacks cannot be used with 1000BASE-T as it requires all four pairs for each link. They are also incompatible with direct use by single-line telephones with standard RJ-11 plugs as nothing is connected to pair 1 in the jack. However, a separate telephone line could be connected to pair 1, thus allowing a single jack to be used for either voice or Ethernet without reconfiguration.

Power over Ethernet

Power over Ethernet or **PoE** technology describes any system to transmit electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. This technology is useful for powering IP telephones, wireless LAN access points, webcams, hubs, computers, and other appliances where it would be inconvenient or infeasible to supply power separately. The technology is somewhat comparable to POTS telephones, which also receive power and data (although analog) through the same cable. It works with an unmodified Ethernet cabling infrastructure.

Power over Ethernet is standardized in IEEE 802.3af. There are several earlier, techniques, but the IEEE standard will probably become dominant.

IEEE 802.3af provides 48 volts DC over two pairs of a four-pair cable at a maximum current of 350 mA for a maximum load power of 16.8 watts. A “phantom” technique is used so that the powered pairs may also carry data. This permits its use not only with 10BASE-T and 100BASE-TX, which use only two of the four pairs in the cable, but also with 1000BASE-T (Gigabit Ethernet), which uses all four pairs for data transmission. This is possible because all versions of Ethernet over twisted pair cable specify differential data transmission over each pair with transformer coupling; the DC supply and load connections can be made to the transformer centre-taps at each end. Each pair thus operates in “common mode” as one side of the DC supply, so two pairs are required to complete the circuit. The polarity of the DC supply is unspecified; the powered device must operate with either polarity with the use of a bridge rectifier.

As of May 2005 there is discussion about increasing the amount of power available on the cable. This may be done by sending power through all four pairs of wire which would double the amount of power. Other discussions include increasing the amount of current.

Before applying power, an IEEE 802.3af power source first “probes” the remote device to determine if it can accept power, and if so, which pairs should be used to supply it. Two modes, A and B, are available. In mode A, pins 1&2 (pair #2 in TIA-568B wiring) form one side of the 48VDC supply, and pins 3&6 (pair #3 in TIA-568B) provide the 48VDC return.

These are the same two pairs used for data transmission in 10BASE-T and 100BASE-TX, allowing the provision of both power and data over only two pairs in such networks.

In mode B, pins 4&5 (pair #1 in both TIA-568A and TIA-568B) form one side of the DC supply and pins 7&8 (pair 4 in TIA-568A and TIA-568B) provide the return; these are the "spare" pairs in 10BASE-T and 100BASE-TX. Mode B therefore requires a 4-pair cable.

A load may choose either mode A or B, but not both. It does so by connecting a nominal 25 kilo-ohm resistor between the desired pair of pairs. The supply detects this resistor and applies power in the selected mode. If the supply detects either an open or a short circuit, no power is applied, thus protecting devices that do not support IEEE 802.3af.

Fibre Optic Cabling

Fibre optic cable is made up of one or more continous strands of glass. Each is surrounded by cladding and then re-inforcing material to protect the fibre, and the whole cable is clad in sheath.

Rather than using electrical pulses, light is uses to transmit information, which is read at the receiving end and converted into electrical pulses for th eprocessing device.

The advantages of fibre optic cable are that it can carry much higher quantities of data and it is immune to normal interference, making errors negligible. Similarly, the signals do not attentuate or weaken to any great degree and much longer distances can be run before signals need to be regenerated. Fibre also offers the advantage of security as it is almos impossible to tap in to it without being detected. The cable is light in weight and small in size for the capacity it can handle.

Its principle disadvantage is its cost. Due to the quality of glass necessary and its fagility the cost of production is high. Termination of fibre cables is a skilled task requiring care, and so installation costs will also be higher. However while it is unlikely to compete directly with coax and twisted pair as demand and and use of optical fibre increases the cost will undoubtedly drop.

Types of Fibre

Multi-Mode Fibre

Multi-mode fibre is a type of optical fibre mostly used for shorter distances, e.g. on campus. It can carry 100 Mbit/s for typical campus distances; the actual maximum speed (given the right electronics) depends upon the actual distance. It is easier to connect to than single-mode optical fibre, but its limit on speed x distance is lower. Multi-mode fibre has a larger centre core than single-mode fibre.

The earliest fibre optic cables used a technique termed multi-mode transmission. This is where the light signals from the laser are broken up into a number of paths along the length of the fibre and is reflected off the fibre wall. The amount of reflection, which occurs, dictates the quality of the signal.

Multi-mode optical fibre is less expensive than Single-mode optical fibre. Current transmission speeds and distances are 100Mb/s up to 10km and 1Gb/s for distances up to 1km. Multi-mode optical fibre has two categories. They are Step Index and Graded Index.

Single Mode Fibre

A single-mode optical fibre is an optical fibre in which only the lowest order bound mode can propagate at the wavelength of interest. Single mode fibres are best at retaining the fidelity of each light pulse over longer distances and exhibit no dispersion caused by multiple modes; thus more information can be transmitted per unit time giving single mode fibres a higher bandwidth in comparison with multi-mode fibres. A typical single mode optical fibre has a core radius of 5-10 micrometers and a cladding radius of 120 micrometers. Currently, data rates of up to 1 Gigabits/second are possible at distances of 60 km and over 6 Gigabits/second at distances of up to 10km. Typically single mode fibre is used within the Wide Area Network rather than the Local Area Network.

Structured Wiring

Structured wiring has come to encompass many differet ideas but at best can be descried as a wiring system designed in a logical hierachy that accommodate all current data cabling and future requirements in a single system.

Structured wiring is a concept which regards the communications wiring of a building as an asset rather than a task to be undertaken when equipment is installed. In a similar way to telephone wiring, which is installed when a building is being furbished, data wiring should be installed at the outset and designed with the intention of obtaining a typical capital life-span of seven to ten years.

Wiring requirements change as equipment capabilities improve or the organisation reorganises its office or technology requirements. Structured wiring is able to accommodate these changes with very little disruption and without the cost of rewiring the building. Also, as the wiring becomes more and more important to the business's operation, the management, control and fault detection within that wiring needs to be more sophisticated.

A simple way of achieving structured wiring may be to install a backbone network between the floors of a building. Ideally this should be fibre due to potential voltage difference between the electricity supply on the floors.

Each floor may then have twisted pair cable to connect the different desks, printers and servers to a central point on that floor, or to a local device if the floor is very large. Originally devices were connected to Hubs, but these days its very difficult to find hubs, as Ethernet switches provide far better functionality (prevent collisions, allow speed mis-matching, provide security etc.) and are now less expensive than hubs.

Typically a large organisation may use a chassis based Ethernet switch for the backbone and then stackable or Edge devices as they get closer to the workgroups. Each network connection is then made by connecting the appropriate cable in the wiring closet for that floor. When people move, the most that will need to be done is to run a new cable from the desk to the wiring closet or to the nearest edge or workgroup switch. Figure 6 below provides a typical example of structured wiring.

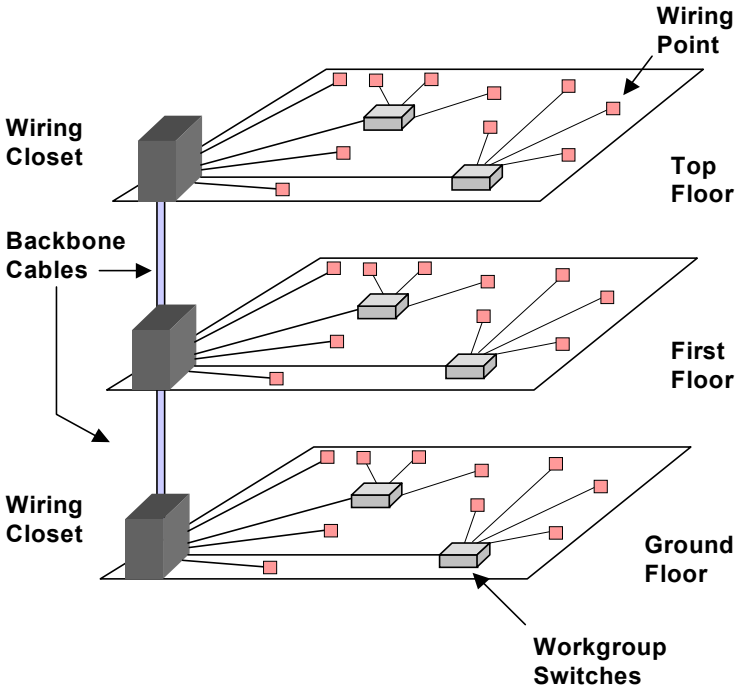


Figure 6: *Example of Structured Wiring*

The above plan, although simplified, shows the principle of structured wiring. When people move only the wiring between the desk and the local access point should need to be changed and when a new computer is introduced to the organisation it simply needs to be connected to its local network. To gain access all the users need to do is to obtain the correct authorisation for the computer, regardless of which network they are connected to.

Typically, a system of flood wiring is employed, so that cables will be in place already whenever a device is added or moved. All that is required is an adjustment to the patch panel in the local wiring closet.

Wireless LAN

Introduction

When this book was first published Local Area Networks used Thick cable to communicate, and within the space of 15 years, have gone from Thick Coax (10 Base 5) to thin coaxial (10 Base 2) to twisted pair (10 base T) cable, and now to wireless as a means of providing an infrastructure.

A Wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier: the last link with the users is wireless, to give a network connection to all users in the surrounding area. Areas may range from a single room to an entire campus. The backbone network usually uses cables, with one or more wireless access points connecting the wireless users to the wired network. Having said this, there are also point to point wireless systems which are used to build single links,although strictly speaking these systems tend to use Microwave or Infrared.

WLAN is expected to continue to be an important form of connection in many business areas. The market is expected to grow as the benefits of WLAN are recognized. So far WLANs have been installed in universities, airports, and other major public places. Decreasing costs of

WLAN equipment has also brought it to many homes. However, in the UK the exorbitant cost of using such connections *in public* has so far limited use to airports' Business Class lounges, etc. Large future markets are estimated to be in health care, corporate offices and the downtown area of major cities. New York City has even begun a pilot program to cover all five boroughs of the city with wireless Internet. BT's Openzone is one such example of a public Wireless LAN.

Originally WLAN hardware was so expensive that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Such places could be old protected buildings or classrooms, although the restricted range of the 802.11b (typically 30ft.) limits its use to smaller buildings. WLAN components are now cheap enough to be used in the home, with many being set-up so that one PC (a parent's PC, for example) can be used to share an Internet connection with the whole family (whilst retaining access control at the parents' PC).

802.11

802.11 legacy

The original version of the standard IEEE 802.11 released in 1997 specifies two raw data rates of 1 and 2 megabits per second (Mbit/s) to be transmitted via infrared (IR) signals or in the Industrial Scientific Medical frequency band at 2.4 GHz. IR remains a part of the standard but has no actual implementations.

The original standard also defines Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the media access method. A significant percentage of the available raw channel capacity is sacrificed (via the CSMA/CA mechanisms) in order to improve the reliability of data transmissions under diverse and adverse environmental conditions.

At least five different, somewhat-interoperable, commercial products appeared using the original specification, from companies like Alvarion (PRO.11 and BreezeAccess-II), Netwave Technologies (AirSurfer Plus and AirSurfer Pro) and Proxim (OpenAir). A weakness of this original specification was that it offered so many choices that interoperability was sometimes challenging to realise. It is really more of a "meta-specification" than a rigid specification, allowing individual product vendors the flexibility to differentiate their products. Legacy 802.11 was rapidly supplemented (and popularized) by 802.11b.

802.11b

The 802.11b amendment to the original standard was ratified in 1999. 802.11b has a maximum raw data rate of 11 Mbit/s and uses the same CSMA/CA media access method defined in the original standard. Due to the CSMA/CA protocol overhead, in practice the maximum 802.11b throughput that an application can achieve is about 5.9 Mbit/s over TCP and 7.1 Mbit/s over UDP.

802.11b products appeared on the market very quickly, since 802.11b is a direct extension of the DSSS modulation technique defined in the original standard. Hence, chipsets and products were easily upgraded to support the 802.11b enhancements. The dramatic increase in throughput of 802.11b (compared to the original standard) along with substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

802.11b is usually used in a point-to-multipoint configuration, wherein an access point communicates via an omni-directional antenna with one or more clients that are located in a coverage area around the access point. With high-gain external antennas, the protocol can also be used in fixed point-to-point arrangements, typically at ranges up to eight kilometers (km)

although some report success at ranges up to 80–120 km where line of sight can be established. This is usually done in place of costly leased lines or very cumbersome microwave communications equipment.

802.11b cards can operate at 11 Mbit/s, but will scale back to 5.5, then 2, then 1 Mbit/s, if signal quality becomes an issue. Since the lower data rates use less complex and more redundant methods of encoding the data, they are less susceptible to corruption due to interference and signal attenuation. Extensions have been made to the 802.11b protocol (e.g., channel bonding and burst transmission techniques) in order to increase speed to 22, 33, and 44 Mbit/s, but the extensions are proprietary and have not been endorsed by the IEEE. Many companies call enhanced versions "802.11b+". These extensions have been largely obviated by the development of 802.11g, which has data rates up to 54 Mbit/s and is backwards-compatible with 802.11b.

802.11a

The 802.11a amendment to the original standard was ratified in 1999. The 802.11a standard uses the same core protocol as the original standard, with a maximum raw data rate of 54 Mbit/s, which yields realistic achievable throughput in the mid-20 Mbit/s. The data rate is reduced to 48, 36, 24, 18, 12, 9 then 6 Mbit/s if required. 802.11a has 12 non-overlapping channels, 8 dedicated to indoor and 4 to point to point. It is not interoperable with 802.11b, except if using equipment that implements both standards.

Since the 2.4 GHz band is heavily used, using the 5 GHz band gives 802.11a the advantage of less interference. However, this high carrier frequency also brings disadvantages. It restricts the use of 802.11a to almost line of sight, necessitating the use of more access points; it also means that 802.11a cannot penetrate as far as 802.11b since it is absorbed more readily, other things (such as power) being equal.

802.11g

In June 2003, a third modulation standard was ratified: 802.11g. This flavour works in the 2.4 GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbit/s, or about 24.7 Mbit/s net throughput like 802.11a. It is fully backwards compatible with "b" and uses the same frequencies. Details of making "b" and "g" work well together occupied much of the lingering technical process. In older networks, however, the presence of an 802.11b participant significantly reduces the speed of an 802.11g network.

The 802.11g standard swept the consumer world of early adopters starting in January 2003, well before ratification. The corporate users held back and Cisco and other big equipment makers waited until ratification. By summer 2003, announcements were flourishing. Most of the dual-band 802.11a/b products became dual-band/tri-mode, supporting "a", "b", and "g" in a single mobile adaptor card or access point.

While 802.11g held the promise of higher throughput, actual results were mitigated by a number of factors: conflict with 802.11b-only devices, exposure to the same interference sources as 802.11b, limited channelization (only 3 fully non-overlapping channels like 802.11b) and the fact that the higher data rates of 802.11g are often more susceptible to interference than 802.11b, causing the 802.11g device to reduce the data rate to effectively the same rates used by 802.11b. The move to dual-mode/tri-mode products also carries with it economies of scale (e.g. single chip manufacturing). The use of dual-band/tri-mode products ensures the best possible throughput in any given environment.

A new proprietary feature called Super G is now integrated in certain access points. These can boost network speeds up to 108 Mbit/s by using channel bonding. This feature may interfere with other networks and may not support all b and g client cards. In addition, packet bursting techniques are also available in some chipsets and products which will also considerably increase speeds. Again, they may not be compatible with some equipment.

802.11n

In January 2004 IEEE announced that it had formed a new 802.11 Task Group (TGn) to develop a new amendment to the 802.11 standard for local-area wireless networks. The real data throughput will be at least 100 Mbit/s (which may require an even higher raw data rate at the physical layer), and should be up to 4–5 times faster than 802.11a or 802.11g, and perhaps 20 times faster than 802.11b. It is projected that 802.11n will also offer a better operating distance than current networks.

There are two competing proposals of the 802.11n standard, expected to be ratified: WWiSE (**W**orld-**Wi**de **S**pectrum **E**fficiency), backed by companies including Broadcom, and TGn Sync backed by Intel and Philips. TGnSync and WWiSE are holding discussions to determine how the proposals may be merged. The standardization process is expected to be completed by the end of 2006.

802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output).

MIMO

MIMO stands for multiple-input multiple-output, an abstract mathematical model for some systems. In radio communications if multiple antennas are employed, the MIMO model naturally arises. MIMO exploits phenomena such as multipath propagation to increase throughput, or reduce bit error rates, rather than attempting to eliminate effects of multipath. MIMO can also be used in conjunction with OFDM and it will be part of the IEEE 802.11n High-Throughput standard, which is expected to be finalized in early 2007.

MIMO and information theory

It has been shown that the channel capacity (a theoretical measure of throughput) for a MIMO system is increased as the number of antennas are increased, proportional to the minimum of number of transmit and receive antennas. This basic result in information theory is what lead to a spur of research in this area.

Benefits of MIMO

MIMO will offer up to eight times the coverage, and up to six times the speed, of current 802.11g networks. Most manufacturers have released “pre-n” hardware in anticipation of the eventual standard.

Wireless LAN In PCs

The use of Windows XP as the ‘standard’ in home PCs makes it very easy to setup a PC as a Wireless LAN ‘basestation’ and (using XP built in Internet Connection Sharing mode) allows all the PCs in the home to access the Internet via the ‘base’ PC. However, lack of expertise in setting up such systems often means that someone nearby, such as a next-door neighbour, may also share the Internet connection. This is typically without the wireless network owner’s knowledge; it may even be without the knowledge of the user (the neighbour) if the user’s computer automatically selects a wireless network.

The future of wireless networks

The 802.11n (MIMO) standard is still being discussed, but one prototype can offer up to (under optimal conditions) 250 Mbit/second. This is over four times the speed of existing 802.11g hardware.

Other new enhancements will include the arrival of 802.11e and 802.11i. 802.11e will prioritize important information on the network (i.e. a voice message takes precedence over email or a webpage). 802.11i will give an increase in security by using WPA2.

4. NETWORK COMPONENTS

Once an appropriate LAN infrastructure (such as structured wiring for example) is in place, the LAN still needs the connection of terminals, printers, PC's and servers to create the network. The following paragraphs outlines some of the devices that might be seen ona typical LAN.

PC Cards

Most PC systems are equipped with an asynchronous communications port which allows data to be sent and received at low speed (up to 115Kbps.). This is quite adequate for text based systems, but nowadays with the advent of the Graphical User Interface (GUI) the bulk of data is in the form of file transfers, and a connection via a low speed serial port is no longer adequate. Usually a corporate user will require large amounts of data to be transferred either to a laser printer or to or from a file server both of which require a much faster operation, and this means connecting those users to a LAN.

To achieve this, a card needs to be added to the PC system which then allows the PC to connect directly to the LAN. This offers the advantage that the card is sitting on the main communications path of the computer, (which operates at high speed), so data can be transferred directly to disk or memory without disabling the computer for extended periods of time.

Intelligent PC cards

In the earlier days of PC LANs the processing power of the PC was such that the PC NICs (Network Interface Cards) drained a significant amount of resources from the PC. Thus activity not directly related to an individuals PC (such as broadcast messages operating in the background) would affect that users PC's performance.

A number of communications vendors (such as Case Communications) developed intelligent cards with their own processors and memory which could handle these background tasks without impeding on the PC's performance. However as PC's grew ever more powerful the need for such sophisticated cards, became a thing of the past, today the majority, if not all NIC cards use the main PC procesor to handle LAN activity.

It should be noted that not all computers need cards. Apple Macintosh machines, for instance have all the necessary hardware to communicate wth other Local Talk devices built in, so that all that is required is a relatively cheap network adapter.

Terminal Servers

For customers with traditional terminals (such as a DEC VT100 for example), which communicate via their serial port, its necessary to use a Terminal Server in order to allow these devices to talk to devices on the LAN. Within TCP/IP terminal emulation is handled by Telnet, and thus Async terminals connected to a terminal server would tend to look like PC's running Telnet sessions to the IP Host.

Host Servers

Mini-Computers were originally designed to have a number of terminals connected each having one port permanently assigned to the computer. The advent of LANs has changed the

need and while some computers are still designed to operate in this manner, additional capabilities have been incorporated for LAN connections.

The most sophisticated computers in terms of LAN connections simply link directly to the network and can handle many terminals working across the network at the same time.

Resources

Network resources are any devices which can be shared by more than one user. These may be computers, file servers, gateways or printers.

File Servers

The disadvantage of LANs were that, unlike a central computer, users could not share information easily. The file server was designed to overcome this by offering a central disk drive that any authorised user could access, both to send and receive files. This meant that information could be shared without having to pass floppy disks around.

As file servers became more sophisticated, it became possible to access information on and update it while another user was also looking but unable to update. Similarly some users could be restricted to viewing but would not be able to change or copy files. File servers typically offer sophisticated resource management and accounting facilities, and can provide network managers with powerful administrative tools. In addition the use of RAID and dual power supplies allow file servers to offer high levels of resilience and redundancy.

Printers

The most typical application of early LANs was the sharing of expensive high quality printers. These were very often laser printers which require a great deal more information per page than earlier ‘Dot matrix’ printers which received one byte of data and produced one character.

Typically a network can support several printers, each of which is given a different name or address on the network. This is then used to identify the information being sent to the printer.

File servers can also act as spooling devices for printers. This eliminates the need for users to contend for printers and therefore the need to wait for an available printer during busy periods.

5. NETWORKING LANS

Since the advantage of LANs became apparent to users, the need to extend networks further and further has arisen. This capability has grown to such an extent that many networks can no longer really be termed “local”, and the following paragraphs outline some of the devices used to extend the local area network.

Network Repeaters

These devices simply connect two lengths of cable, possibly some distance apart and regenerate the signal so that the two parts form one LANs. These days Hubs and Ethernet switches include the repeaters on each port.

Network Hubs

An Ethernet hub or concentrator is a device for connecting multiple twisted pair or fibre optic Ethernet devices together, making them act as a single segment. It works at the physical layer of the OSI model, repeating the signal that comes into one port and out on each of the other ports. If a signal comes into two ports at the same time a collision occurs, so every attached device shares the same collision domain. Hubs support only half duplex Ethernet, providing bandwidth which is shared among all the connected devices. Ethernet hubs have been largly replaced by network switches, which operate at the data link layer and improve performance by separating the connected devices into separate collision domains.

Network Bridges

Bridges are simply devices which bridge the gap between two remote LANs. The distance between the two LANs depends upon the bridges capabilities. Today its more common to use ethernet switches to inter-connect different LAN segments and thus if a bridge is used its more likely to extend the LAN over a wide area network, either via a leased circuit or by a dial up service such as ISDN. With a bridge the network is the same at each end of the network, with the same addressing scheme, therefore bridges allow the network to become one large network. Care must be taken to ensure no two devices on the network have the same IP Address.

The intelligence of the bridge can vary, but usually a bridge will examine the address of each packet of information on the network. Often bridges have a learning capability so they can develop a knowledge of all addresses and whether they are local or remote. Any locally addressed packets are ignored, and all packets with remote addresses related to that bridge will be passed across to the remote bridge which will place them on its network.

A Bridge operates at the data link level of the LAN, usually the Media Access Control (MAC) level. Operation is not as efficient as a router as all the lower level information must also be passed over the link between the networks. However,a benefit of operating at level 2 in the OSI stack is that it is possible to bridge two different networks, for example TCP/IP and OSI, as the bridge simply passes data packets and ignores the higher level protocols.

Spanning Tree

The principle limitations of remote bridges are that a ring cannot be formed in the network (This is no duplication of trunks or links between bridges) and two bridges cannot connect the same two networks for resilience, as the same data packet could be forwarded in an endless

loop. However, a standard has been defined called the “Spanning Tree Algorithm” which allows bridges to form loops. What this does is create a protocol for bridges to use when starting up or when failure is detected.

This is based on a learning or listening stage when bridges will intercommunicate with each other but will not transmit live data. This allows each bridge to determine its position and ‘priority’ in the network. Any bridge which detects that it is linking the same two network segments, or is causing a loop and is the lowest priority bridge in that structure, will block its link between the two segments thus preventing duplication of data on the network. After a specified time period, the bridges will start sending live data. Periodically a bridge will then send data to other bridges, and any failure of one of these transmissions will automatically start a new learning process to re-establish the network structure, which may have changed due to the failure of some equipment in the network. Any new bridge introduced into the network will similarly start by listening to determine its position in the network. While this facility increases the flexibility of bridges, care should be taken in selection of systems, as not all devices will have this facility implemented.

Network Routers

Routers operate in a similar way to bridges except that they operate at a higher level, the Network Layer, in the OSI model. This provides the great advantage of allowing dissimilar networks , for instance CSMA/CD and Token Ring, to interwork. Today routers are mainly used to inter-connect two or more LANS over a wide area network.

Apart from interconnection of dissimilar networks, routers also allow high performance and resilience to be built into network through triangulation, multiple links between the same two networks and additional features such as traffic analysis and accounting. As routers operate at the Network Layer, they have access to the addressing information of data packets and sophisticated routers can select a path between networks, such as the fastest or cheapest route.

The principle limitation of routers is that, as they operate at the Network Layer, it is impossible for them to interwork between dissimilar Network Layer protocols, without the relevant software. For example a TCP/IP router cannot route OSI, DECLAT or any other non TCP/IP protocols without having a software stack for each protocol, and this means a reduction of performance. However as TCP/IP is almost universal today its is no longer such a problem and most routers no longer need to support anything other than TCP/IP.
Many routers also provide Bridging facilties for protocols they don’t recognise, that is to say they will route TCP/IP but if they encounter OSI on the LAN they will bridge it.

Transport of WAN Protocols Over Routers

As the world moves towards TCP/IP and major Telecos move away from pure digital circuits to IP transport only, a new breed of router has to emerge to provide support for non IP devices.

X25 Over IP (XOT)

Where legacy X.25 systems existed, X.25 Over TCP/IP allows the IP Router to emulate an X.25 network, and for the router to transport X.25 over the IP network.

HDLC Over TCP (HOT)

Case Communications HOT (HDLC Over TCP) technology uses a card which fits into routers allowing legacy products which utilise HDLC (such as X.25, Frame Relay and stat muxes etc.) to be transported over an IP network, completely transparently.

Voice Over IP

More common are Voice Over IP Routers which transport telephone calls and faxes over an IP network, saving the cost of expensive long distance calls.

TDM Over IP

A newer but fast growing technology is TDM Over IP (Time Division Multiplexing) which allows virtually any serial devices to operate over an IP network, and which emulate a traditional PDH/SDH Time Division Multiplexer network, over IP.

TDM Over IP, as a technology, has been trademarked by the Israeli firm RAD and therefore, because firms developing and selling this technology are not allowed to use the terminology 'TDM Over IP' in marketing and advertising materials, we will often see these products referred to as Circuit Emulation Over IP (CEO IP) instead of TDM Over IP.

Ethernet Switches

Ethernet Switch Introduction

A network switch is a computer networking device that connects network segments. It uses the logic of a Network bridge but allows a physical and logical star topology. It is often used to replace network hubs. A switch is also often referred to as an intelligent hub.
Originally Ethernet switches switched data at layer two, but increasingly switch at layer 3, 4 and beyond. This means that not only can Ethernet switches switch between LAN segments but they can join two different LANs and switch by traffic type.

Switch Operation

A switch can connect Ethernet, Token Ring, or other types of packet switched network segments together to form a heterogeneous network operating at OSI Layer 2. While a number of switches can switch at Layer 3 and beyond, for the purpose of this section we will focus on more common layer two switches. For more detailed information on Ethernet Switching, please refer to the 'Case Communications pocket book of Ethernet Switches'.

Layer Two Switching

As a frame comes into a switch, the switch saves the originating MAC address and the originating port in the switch's MAC address table. The switch then selectively transmits the frame from specific ports based on the frame's destination MAC address and previous entries in the MAC address table. If the MAC address is unknown, or a broadcast or multicast address, the switch simply floods the frame out of all of the connected interfaces except the incoming port. If the destination MAC address is known, the frame is forwarded only to the corresponding port in the MAC address table. If the destination port is the same as the originating port, the frame is filtered out and not forwarded.

Switches, unlike hubs, use divide collision domains, one per connected segment. This way, only the NICs which are directly connected via a point-to-point link, or directly connected hubs are contending for the medium.

By eliminating the possibility of collisions, full-duplex point-to-point connections on the switch become possible.

Virtual LANs can be used in switches to reduce the size of the broadcast domains and at the same time increase security.

In redundant architectures, spanning tree protocol can be used in switches to prevent loops.

Forwarding Methods

There are four forwarding methods a switch can use:

1. Cut through – starts forwarding the frame (or packet) before the whole frame has been received, normally as soon as the destination address is processed. This technique reduces latency through the switch. In packet switched networks such as Ethernet, cut-through switching can only be used where the outgoing interface is equal in speed to, or slower than the incoming interface.

Cut through routing in IP networks presents some problems since the IP checksum in the packet is supposed to be checked by every router in the path. Since the checksum of a packet cannot be checked until the entire packet has been received, the cut-through router is at risk of forwarding a packet with an incorrect checksum. Provided that there are other routers in the path which are not doing cut-through routing, or that the end system is correctly verifying checksums, this should only result in the occasional loss of a small amount of traffic capacity.

Cut through routing was one of the important features of ATM networks since the edge routers of the ATM network were able to use cell switching through the core of the network with low latency at all points. With higher speed links, this has become less of a problem since packet latency has become much smaller.

2. Store and forward – the switch, unlike cut through, buffers and typically, performs a checksum on each frame before forwarding it on. Store and Forward is typically has greater latency as the switch has to look at and process the packets, but it also provides more reliable data transmission as errors can be removed, and it also allows for speed mis-matching. This is useful where, for example a server could sit on a 1 Gbps port of an Ethernet switch and be connected to by a number of users residing on 10Mbps and 100Mbps ports.

3. Fragment-free switching – is suitable for backbone applications in a congested network, or when connections are allocated to a number of users. The switching device checks the source and destination MAC address of a packet, and sends the packet to the port corresponding to the destination.

The packets are sent through the switch as a continuous flow of data, and the transmit and receive rates are always the same. Because of this, fragment-free switching cannot pass packets to higher speed networks, for example, to forward packets from a 10 Mbit/s to a 100 Mbit/s Ethernet network. Therefore, if you opt for fragment-free switching, you cannot make direct connections to higher speed networks from that port.

Fragment-free switching offers a compromise between cut through (which offers the fastest possible forwarding at the expense of any error checking) and store-and-forward (which offers maximum error checking at the expense of latency), to provide an average latency of approximately 60µs and sufficient error checking to eliminate most common errors.

4. Adaptive switching – mode is a user-defined facility to maximize the efficiency of the switch. Adaptive switching starts in the default switch forwarding mode you have selected (cut-through if you selected adaptive mode as the default switching mode). Depending on the number of runts and CRC errors at that port, the mode changes to the "best" of the other two switching modes. As the numbers of runts and CRC errors change, so does the forwarding mode.

An Adaptive switch will automatically switch between the various modes, and will adopt the best method of operation according to the prevailing conditions. The table below gives an example of this.

Switching mode:	Defects:	Then, adaptive mode changes the switching mode to:
Cut-through	High numbers of CRC errors	Store-and-forward
	High numbers of runts	Fragment-free
Fragment-free	High numbers of CRC errors	Store-and-forward
	Low numbers of runts	Cut-through
Store-and-forward	Low numbers of CRC errors	Fragment-free
	Low numbers of CRC errors and runts	Cut-through

Flaws

Switches provide difficulties in monitoring traffic because each port is isolated until it transmits data, and even then only the sending and receiving ports are connected.

Two popular methods that are specifically designed to allow a network manager to monitor traffic are:

- Port mirroring – the switch sends a copy of network packets to a monitoring network connection.
- SMON – "Switch Monitoring" is described by RFC 2613 and is a protocol for controlling facilities such as port mirroring.

Other "methods" (a.k.a. attacks) have been devised to allow snooping on another computer on the network without the cooperation of the switch:

- ARP spoofing – fooling the target computer into using your own MAC address for the network gateway, or alternatively getting it to use the broadcast MAC.

MAC flooding – overloading the switch with a large number of MAC addresses, so that it drops into a "failopen mode".

Gateways

While not strictly used to connect two LANs or LAN segments Gateways can be used to connect a LAN to a host computer or even to a WAN service.

A Gateway is a specialised form of access device. It is designed to create access between systems or environments running different, often proprietary protocols. It may also enable proprietary systems to be connected to a common backbone LAN, running TCP/IP for instance. For example the Case Communications 'T.Gate' interconnects an Ethernet LAN operating TCP/IP to an X.25 network,and the X.25 network to the TCP/IP network.

This may be confusing, but reference to the OSI model is helpful. A Gateway is often a device which operates at a high layer in the OSI model. (Usually above layer 3, and thus beyond the capability of repeaters, bridges and routers.). Alternatively, a Gateway may operate at any level of the model with a dissimilar level at each side of the Gateway. There is no hard and fast rule as to what forms a true Gateway, but principally it is a device concerned with conversion of incompatible protocols, networks and applications.

6. LIMITATIONS OF LANS

Whilst LANs are extremely wide-ranging in their applications, as with most technologies they do have some limitations. Principally these centre on two areas: capacity and compatibility, most of these can be overcome by good design and careful product selection.

Capacity

Many people familiar with earlier forms of data communications may consider a network operating at 10 or 100 Megabits a second a great luxury. However there can still be throughput problems because the data volumes that are being considered are huge in comparision to the data rates used by terminals with async serial ports.

Consider that a standard VDU (Visual Display Unit) connected to a computer would receive a normal screen full of characters to display. This is typically about 800 characters or 800 bytes which on a 9,600 bps line would take about 0.8 of a second to transfer (800 x 10 bits =8000 bits)/9600). A PC on a LAN would usually transfer a file across from a server, rather than transfer a screen. Files vary greatly in size, but assume that a five page document is being transferred which also has a small graphic included. This may be as much as 20,000 bytes long, 25 times as large as the screen of information. On the LAN even with all the protocol overheads, this may take one quarter of a second to transfer. If the original 9,600 bps line were used the transmission would take 21 seconds.

On looking at the above example it would appear that while volumes of data are much greater this does not cause a problem. However, it should be remembered that there is more than one device on the LAN and therefore, although there is more capacity, there are also more users contending for it.

Capacity problems will become evident during the heaviest loading or “peak loading” of the network. This may be first thing in the morning when every user connects to the network and collects the information for the day or, even more commonly, towards the end of the day, possibly as people are contending for the printers to produce letters for the final post.

To the network user capacity problems become apparent in two ways.

Firstly – when trying to connect to a resource on the network they will not be able to gain access because other users are already connected. This can usually be resolved by adding another resource, such as an extra printer, or adding extra access, such as an additional host server for the computer.

Secondly – response across the network begins to degrade. Files take longer to transfer, connections take longer to set up or even in some cases transfers fail to complete due to the protocol reaching a timeout. (Timeouts occur when one device waits for a preset period to receive something, but does not receive it.)

This type of problem can be more difficult to correct. The easiest method is usually to split the LAN into two parts and use an Ethernet switch or bridge between them. However unless the connection patterns are known accurately, allowing the correct devices to be placed on each LAN to spread the loading, little may be achieved.

RMON

RMON stands for Remote Monitoring. It is a standard used in network equipment which implement a MIB (Management Information Base) which allows for remote monitoring and management of that equipment. RMON uses an agent running on the device being monitored to supply information over SNMP to a management workstation (or some other system).

The current RMON standard is RFC 2819. It is extended by several RFCs, including RFC 2021 which extends it towards the application layer.

The standard describes functions, messages and data structures to support the nine RMON groups of:

1. Statistics
2. History
3. Alarms
4. Hosts
5. Host Top N
6. Traffic Matrix
7. Filters
8. Packet Capture
9. Events

Each of these groups provides specific sets of data to meet common network-monitoring requirements. Each group is optional so that vendors do not need to support all the groups within the Management Information Base (MIB). Some RMON groups require support of other RMON groups to function properly.

The use of RMON aids the network manager with not only fault finding but it allows the manager to predict future trends and identify potential problems.

7. SOFTWARE ARCHITECTURES

While most LANS use TCP/IP and Microsoft, Unix or Linux Operating systems on their servers, a number of alternate operating systems have been used over the last few years and a number still exist. The following paragraphs outline some of the better known LANs.

Netware

Netware was developed by the Novell corporation and is primarily a suite of application oriented interfaces rather than LAN-based protocols. Netware provides workstation (PC, Macintosh etc.) access to a network file server, which runs the Netware operating system. Netware will operate with a variety of LANs including Ethernet, Cheapernet, Token Ring, Local Talk and ARCNet. Basically Netware adds a programme termed a 'shell' to the PC. Every command issued by the PC goes to the shell. If it is a local command it is then passed to the local operating system. If the command relates to the network then the command is processed by Netware and sent onto the network.

While the suite is not standards-based it was widely used and supported due to its level of sophistication and the speed of operation. Its popularity has led many companies to develop software that will operate with Netware.

Netware was originally based on the Xerox network Systems (XNS) stack, but today runs on both IPX/SPX as well as TCP/IP. NetWare was one of a series of XNS-based systems, which also included Banyan Vines and Ungerman-Bass Net/One. Unlike these products, and XNS itself, NetWare established a strong presence in the market in the early 1990s, and barely managed to survive the onslaught of Microsofts Windows NT which killed off the other players.

Netware evolved from a very simple concept : one or more dedicated servers were connected to the network, and shared disk space in the form of *volumes*. Clients running MS-DOS would run a special Terminate and Stay Resident (TSR) program that allowed them to *map* a volume as if it were a local hard disk. Clients had to log-in, to be allowed to map volumes, and access could be restricted according to the log-in name. Similarly, clients could connect to shared printers on the dedicated server, and print as if the printer was connected locally. While early Netware systems did entirely trust all modules (any misbehaving module could bring the whole system down), it was very stable. There are reports of Netware servers running for years without any human intervention.

IBM APPC

Advanced Program-to-Program Communications (APPC) is a protocol suite originally designed by IBM as part of SNA (Systems Network Architecture). APPC uses LU 6.2 (LU stands for Logical Unit or device on the network and 6.2 is the number assigned to the particular level for program to program communication)

With the advent of LANs, IBM have implemented APPC on the Token Ring network operating above 802.5 (Token Ring) and 802.2 (Logical Link Control) standards.

Netbios

Netbios is similar to Netware in that it is a form of application interface rather than a network protocol. In MS/DOS, the main PC operating system, Basic Input Output System (BIOS) controls access to various devices such as the keyboard, screen and communications port. Netbios similarly handles the input and output of applications in coordination with the network.

Originally introduced in 1984, Netbios was designed to operate on IBM networks. Following the publication of the Netbios interface other non-IBM products were introduced and adaptations for Ethernet TCP/IP and OSI standards have been implemented.
Due to its association with IBM this system is widely used. However, it is somewhat restricted in its addressing capability and its maximum capacity for simultaneous sessions.

LAN Manager

LAN Manager, developed by Microsoft and 3Com, is a network operating system originally designed to run on the OS/2 operating system. OS/2 was written by Microsoft for IBM to exploit the enhanced facilities of its second generation of personal computers, the PS/2. The operation is no longer limited to OS/2 systems and versions were and available for MS-DOS, and Xenix (an earlier version of Unix for PC's, now replaced by Linux). There was also LAN Manager/X (LMX) for UNIX based systems. In 1990 Microsoft announced LAN Manager 2.0 with a lot of improvements. The latest version LAN Manager 2.2 which included an MS-OS/2 1.31 base operating system remained to be Microsoft's strategic server system until the release of Windows NT Advanced Server in early 1994.

Windows NT

When development started in 1988, Windows NT (using protected mode (the 286 architecture introduced protected mode allowing for (among other things) hardware-level memory protection)) was to be known as OS/2 3.0, the third version of the operating system developed jointly by Microsoft and IBM.

In addition to working on three versions of OS/2, Microsoft continued parallel development of the DOS-based and less resource demanding Windows environment (using Real mode (an operating mode of 80286 and later x866-compatible CPUs)).

When Windows 3.0 was released in May 1990 it was so successful that Microsoft decided to change the primary API (application programming interface) for the still-unreleased NT OS/2 (as it was then known) from an extended OS/2 API to an extended Windows API. This decision caused tension between Microsoft and IBM, and the collaboration ultimately fell apart. IBM continued OS/2 development alone, while Microsoft continued work on the newly-renamed Windows NT. Though neither operating system would be as immediately popular as Microsoft's DOS or Windows products, Windows NT would eventually be far more successful than OS/2.

OSI – Open Systems Interconnection

Introduction

At one time it was generally accepted that TCP/IP would be superseded by OSI, due to the more advanced facilities available with OSI. For example OSI has such as a much larger addressing field. Companies such as Case Communications even developed Gateways, which converted other LAN protocols such as TCP/IP into OSI. However the complexity of OSI

increased cost of the products, and the proliferation of TCP/IP ensured it became virtually the only network protocol by the end of the millennium.

OSI Standards

Following the publication of the OSI model the International Standards Organisations (ISO) developed the protocols for the seven layers of the model. As with all such monumental tasks, a great deal of time has been spent in the determination and agreement of these standards. To speed up the process and to encourage the implementation of the OSI protocols, many standards developed by the Institutes of Electrical and Electronic engineers (IEEE) and by the Comite Consultatif Internationale de Telegraphique et Telephonique (CCITT now ITU (International Telecommunications Union after 1992) were developed.

The bottom two layers, Physical and Data Link are addressed by the standard LAN types such as CSMA/CD, Token Ring and Token Bus.

Level 2 – the Data Link is constructed of two sub layers. The lower of these is the Media Access Control (MAC), layer. This is regarded as part of the physical standard of the network and different variants are specified with the standards such as 802.3, 802.4 and 802.5. The higher section of level 2 is Logical link Control (LLC) covered by the IEEE 802.2 standards. Effectively LLC is designed to enable multiple links to multiple stations on a single physical network. This part of the standard is software-based but typically resides on hardware units, such as PC cards. There are two distinct classes of LLC.

Class I – is a form of connectionless communication. There is no link establishment, acknowledgement of Protocol Data Units (PDUs), flow control or error recovery.

Class II – operates a connection-oriented communication. Links are established between LLCs prior to data transfer. The link then maintains flow control and error recovery.

LANs usually use Class I LLC because of the relatively low rate of errors on such networks. Class II would reduce the effective throughput of the network because of the connection overheads. Connection control usually resides within the Level 4, (the transport layer, of the OSI model.)

The next two layers, (The Network and Transport Layers), have both connectionless and connection oriented protocols specified. Basically these two forms of communication can be summarised as follows.

Connectionless – protocol allows transmission of blocks of data (datagrams) across the network. There is no previous contact necessary between the sending and receiving devices. Datagrams can arrive in any order or even be missing: the connectionless protocol has no concern over this.

Connection – oriented protocol ensures that the sending and receiving terminals are aware of the communications before transmission of data actually begins. Data is then sent sequentially and errors reported before the next block of data is sent.

Layer three – (the Network Layer), in LANs usually implements a connectionless protocol called Connectionless Network Service (CLNS). The advantage of this is that, due to the low failure rate of LANs, there is no overhead on the network regarding setting up connections

and handling data. Also in failure situations, no restoration of connections is necessary, thus simplifying the restart, saving time and maximising data throughput.

Layer four – (the Transport Layer), in LANs usually implements a connection-oriented protocol called the Transport Protocol (TP4). This exploits the capabilities of CLNS and simply collates the data as it is received, re-sequences the datagrams, checking for errors and requesting retransmissions where necessary. Using this method the connection is handled by the sending and receiving machines but no 'connection; data is sent across the network except for retransmissions due to errors, thus minimising the overheads on the network.

Layers five and six – (the Session and Presentation Layers) both have connection-oriented protocols specified. These protocols are designed to allow applications to interface rather than network components. Their implementation is therefore more dependent upon the actual use of the network rather than its operation. Examples of such levels in the pre-OSI environment are Netware and Netbios.

Layer seven – (the Application Layer), is the area, where the main user inter-working takes place. Layer seven OSI standards include X.400 (Electronic Mail), X500 (Directory Services), Virtual Terminal and FTAM (File Transfer Access Management). Had OSI replaced TCP/IP then these would have been the basic building blocks which would have allowed different business applications to inter-work without any reprogramming or redesign.

Some of the major initiatives in OSI implementation were MAP, TOP and GOSIP.

MAP – Manufacturing Automation Protocol

The Manufacturing Automation Protocol – was pioneered by General Motor's in 1983. It began as an initiative to develop inter-working between equipment on the manufacturing floor. The 1987 release, MAP 3.0, provides a range of protocols, wide enough for commercial implementation.

A mix of standards within the OSI definitions has been chosen as the most suitable for manufacturing purposes. This involved the selection of Token Bus as the LAN (802.4) and an Application layer protocol Manufacturing Message Format Standard (MMFS) was added to the OSI suite.

TOP – Technical and Office Protocols

TOP is similar to MAP. Originally proposed by Boeing Computer Services, the standard follows the OSI form and is concerned with exchanging office documents and graphics in a suite of international standards.

GOSIP (Government Open Systems Interconnection Profile)

GOSIP was a U.S. government mandate first published as FIPS 146-1 in 1990, that after August 15, 1990, all new network procurements must comply with OSI. Testing is performed at the NIST, which maintains a database of OSI-compliant commercial products.

In 1995 FIPS 146-2 was published, which removed the procurement requirement for the GOSIP OSI protocols, by permitting acquired products to implement ISO, ITU-T or IETF standards. Interest in OSI implementations declined, and subsequent civilian government agency deployments of networking services are predominately based on the Internet Protocol Suite, which led GOSIP to evolve into POSIT (Profiles for Open Systems Internetworking

Technologies), which is a set of non-mandatory standards that acknowledge the widespread use of TCP/IP.The Defence Messaging System continued to be based on the OSI protocols X400 and X.500 due to their integrated security capabilities. GOSIP also allows TCP/IP protocols to be used.

GOSIP was also pioneered by the UK government and defined that all suppliers must conform to the OSI model when public sector procurements were being made.

8. ETHERNET & TCP/IP – DE FACTO STANDARDS

Introduction

As the use of TCP/IP began to grow, so more companies adopted it within their products and networks. Such growth in demand resulted in TCP/IP becoming a de facto standard within the LAN environment.

TCP/IP is not OSI compliant but the protocols do parallel the OSI model. Internet Protocol (IP) is similar to ISO Connection Less Network Service (CLNS), (ISO 8473). IP is a connectionless datagram service: that is, it divides the data into small units and puts them onto the network being used for transmission. Transmission Control Protocol (TCP) is similar to the ISO Transport Layer Class 4 (ISO 8073). TCP provides a connection oriented, error free transmission service for applications. It basically collates all the datagrams that IP puts onto the network, re-sequences the data, checks for errors and requests retransmissions for any corrupted or lost data.

The advantage of TCP/IP is its historical status as a de facto standard for LAN operation. Therefore more flexibility is offered for inter-working and compatibility than with any other non-ISO protocol.

The disadvantages are that it is not OSI conformant and was originally designed to operate on a Wide Area Network and not a LAN. WANs generally have a much higher error rate than LANs due to the lower quality of network links. Therefore TCP/IP operates a great deal of checking, which reduces performance although some of this has been overcome by better design in recent developments.

TCP/IP Architectures

Transmission Control Protocol

Transmission Control Protocol/Internet Protocol (TCP/IP) is part of the Internet Protocol Suite, a suite of software which operates across a network to enable communications. TCP/IP began as a non-commercial project in the 1970s. The Defence Advanced Research Projects Agency within the American Government began to develop a wide area network, ARPANET, to link all its research centres. From this, and experiments with packet-based radio, emerged TCP/IP which preceded OSI standards by several years even though it used a layered structure similar in principle to the OSI model.

When commercial organisations began to develop networks they encountered the same problems that ARPANET had addressed and, as the TCP/IP protocol suite was fully tested, a ready-made solution was available.

The use of TCP/IP was also promoted by its inclusion in American Government contracts and its adoption within the UNIX operating system for workstation communication. However, the main reason for its meteoric growth was the fact that TCP/IP included a number of higher level application protocols which became widely used by network developers. TCP/IP uses a layered approach and the following sections provide an overview of the layers within the TCP/IP.

Application layer	HTTP, HTTPS, SMTP, FTP, UUCP, NNTP, SSH, IRC, SNMP, SIP,RTP, Telnet
Transport layer	TCP, UDP,SCTP, DCCP
Network layer	IPV4, IPV6, ICMP, ARP, IGMP
Data Link layer	Ethernet, Token Ring, PPP, Wire Fi, FDDI
Physical layer	RS232, X.21, Fibre, Twisted Pair, Coax

Figure 5: *TCP/IP Layers*

Layer 1 – The Physical Layer

The physical layer refers to the physical media and this could be any of a number of physical interfaces from RS 232, to X.21 V.11 RS 449 etc. As this book is about LANs the physical media is more likely to be coax, fibre or twisted pair cable, but routers and bridges would utilise serial interfaces to connect the LANs over the Wide Area Network.

Layer 2 – The Data Link Layer

The Data Link Layer may also be any of a number of technologies from Ethernet, to Token Ring, to FDDI (described previously) to Wireless to PPP.

Layer 3 – The Network Layer

IPv4 – Internet Protocol version 4

Internet Protocol version 4, was the first version of the Internet Protocol to be widely deployed, and forms the basis for most of the current Internet (as of 2004).
It is described in IETF RFC 791, which was first published in September, 1981.

IPv4 uses 32-bit addresses, limiting it to 4,294,967,296 unique addresses, many of which are reserved for special purposes such as local networks or multicast addresses, reducing the number of addresses that can be allocated as public Internet addresses. Consequently DHCP (Dynamic Host Configuration Protocol) was introduced to loan devices IP addresses while they used the network. This is commonly used on the Internet where your assigned an IP address for the duration of your time on line, and once your off-line the same address maybe used by another user.

As the number of addresses available is consumed, an IPv4 address shortage appears to be inevitable in the long run.This limitation has helped stimulate the push towards IPv6, which is currently in the early stages of deployment, and may eventually replace IPv4.

Ipv6 – Internet Protocol version 6

Internet Protocol version 6, is a network layer standard; i.e., it governs the addressing and routing of data packets through a network. IPv6 is intended to replace the IPv4 standard, whose limits on network addresses are beginning to restrict Internet growth and use.

IPv6 supports about 3.4×10^{38} (340 undecillion) addresses.

Adopted by the Internet Engineering Task Force in 1994 (when it was called “IP Next Generation” or IPng), IPv6 accounts so far for just a few percent of the IP networks in use.

ICMP – Internet Control Message Protocol

The Internet Control Message Protocol is one of the core protocols of the Internet Protocol suite. It is chiefly used by networked computers' operating systems to send error messages indicating, for instance, that a requested service is not available or that a host or router could not be reached.
ICMP differs in purpose from TCP and UDP in that it is usually not used directly by user network applications. One exception is the ping tool, which sends ICMP Echo Request messages (and receives Echo Response messages) to determine whether a host is reachable and how long packets take to get to and from that host.

ARP – Address Resolution Protocol

The Address Resolution Protocol is a method for finding a host's Ethernet (MAC) address from its IP address. The sender broadcasts an ARP packet containing the Internet address of another host and waits for it (or some other host) to send back its Ethernet address. Each host maintains a cache of address translations to reduce delay and loading. ARP allows the Internet address to be independent of the Ethernet address but it only works if all hosts support it.

IGMP – Internet Group Management Protocol

The Internet Group Management Protocol is a communication protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections.

Layer 4 – Transport Layer

TCP – Transmission Control Programme

The Transmission Control Protocol is one of the core protocols of the Internet protocol suite. Using TCP, programs on networked computers can create *connections* to one another, over which they can send data. The protocol guarantees that data sent by one endpoint will be received in the same order by the other, and without any pieces missing. It also distinguishes data for different applications (such as a Web server and an email server) on the same computer.

TCP supports many of the Internet's most popular applications, including HTTP, SMTP, and SSH.

TCP ports

TCP uses the notion of port numbers to identify sending and receiving applications. Each side of a TCP connection has an associated 16-bit unsigned port number assigned to the sending or receiving application. Ports are categorized into three basic categories:

Well Known Ports

The well known ports are assigned by the Internet Assigned Numbers Authority (IANA) and are typically used by system-level or root processes. Well known applications running as servers and passively listening for connections typically use these ports. Some examples include: FTP (21), TELNET (23), SMTP (25) and HTTP (80).

Registered

Registered ports are typically used by end user applications as ephemeral source ports when contacting servers, but they can also identify named services that have been registered by a third party.

Dynamic/private

Dynamic/private ports can also be used by end user applications, but are less commonly so. They do not contain any meaning outside of any particular TCP connection. There are 65535 possible ports officially recognised

UDP – User Datagram Protocol

The User Datagram Protocol is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages known as *datagrams* to one another. UDP does not provide the reliability and ordering guarantees that TCP does; datagrams may arrive out of order or go missing without notice. However, as a result, UDP is faster and more efficient for many lightweight or time-sensitive purposes.Common network applications that use UDP include the Domain Name System (DNS), streaming media applications, Voice Over IP, and online games.

SCTP – Stream Control Transmission Protocol

The Stream Control Transmission Protocol is a transport layer protocol defined in 2000 by the IETF Signalling Transport (SIGTRAN) working group. The protocol is defined in RFC 2960, and an introductory text is provided by RFC 3286.As a transport protocol, SCTP is equivalent in a sense to TCP or UDP. Indeed it provides some similar services as TCP, ensuring reliable, in-sequence transport of messages with congestion control. While TCP is byte-oriented, SCTP deals with framed messages.

DCCP – Datagram Congestion Protocol

The Datagram Congestion Control Protocol is a message-oriented transport layer protocol that is currently (2005) under development in the IETF. Applications that might make use of DCCP include those with timing constraints on the delivery of data such that reliable in-order delivery, when combined with congestion control, is likely to result in some information arriving at the receiver after it is no longer of use. Such applications might include streaming media and Internet telephony. Congestion control is the way that a network protocol discovers the available network capacity on a particular path. The primary motivation for the development of DCCP is to provide a way for such applications to gain access to standard congestion control mechanisms without having to implement them at the application layer.

Layer 7 – Application layer

HTTP – HyperText Transfer Protocol – Port 80

HTTP is the primary method used to convey information on the World Wide Web. The original purpose was to provide a way to publish and receive HTML pages.

HTTPS – HyperText Transfer Protocol Secure – Default Port 443

HTTPS is the secure version of HTTP, the communication protocol of the World Wide Web. It was invented by Netscape Communications Corporation to provide authentication and encrypted communication and is used in electronic commerce. Instead of using plain text socket communication, HTTPS encrypts the session data using either a version of the SSL (Secure Socket Layer) protocol or the TLS (Transport Layer Security) protocol, thus ensuring reasonable protection from eavesdroppers, and man in the middle attacks.

SMTP – Simple Mail Transfer Protocol – Port 25

SMTP is the *de facto* standard for email transmission across the Internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred. It is quite easy to test a SMTP server using the telnet program. To determine the SMTP server for a given domain name, use the MX (Mail eXchange) DNS record.

FTP – File Transfer Protocol – Port 21

FTP allows the transfer of files either in ASCII (American Standard Code for Information Interchange) or Binary form. It should be noted that ASCII defines a standard set of codes used to represent alphanumeric characters. Therefore a file could be transferred from a machine using Extended Binary Coded Decimal Interchange Code (EBCDIC) to an ASCII-based machine or vice versa.

TELNET – Port 23

Telnet which provides an ASCII Virtual Terminal Interface. For a terminal it allows logon to remote hosts from another host or terminal server. To the host it simulates a directly connected terminal, such as a VT 100.

UUCP – Unix to Unix Copy Protocol – If port not defined default Port 540

UUCP is a computer program and protocol allowing remote execution of commands and transfer of files, email and netnews between Unix computers not connected to the Internet proper. The UUCP package consists of several programs including uucp, uuxqt (front ends for remote copy and execution), uucico (communication program), uustat, and uuname. Nowadays it is rarely used for Modem communications, but is still used sometimes over TCP/IP.

NNTP – Network News Transfer Protocol – TCP port 119 is reserved for NNTP

NNTP is an Internet application protocol used primarily for reading and posting Usenet articles, and transferring news among servers.

Usenet was originally designed around the UUCP network, with most article transfers taking place over direct computer-to-computer telephone links. Readers and posters would log into the same computers that hosted the servers, reading the articles directly from the local disk.

As local area networks and the Internet became more commonly used, it became desirable to allow newsreaders to be run on personal computers, and a means of employing the Internet to handle article transfers was desired. Because networked Internet-compatible filesystems were not yet widely available, it was decided to develop a new protocol that resembled SMTP, but was tailored for reading newsgroups.

TCP port 119 is reserved for NNTP. When clients connect to a news server with SSL, TCP port 563 is used. This is sometimes referred to as NNTPS.

SSH – Secure Shell Port 22

SSH is both a computer program and an associated network protocol designed for logging into and executing commands on a networked computer. The designers of SSH aimed to replace the earlier rlogin, telnet and rsh protocols, and the resultant protocol provides secure encrypted communications between two untrusted hosts over an insecure network. Users of SSH can also use it for tunnelling, forwarding X11 connections and arbitrary TCP ports over

the resultant secure channel; and can transfer files using the associated scp or sftp programs. An ssh server, by default, listens on the standard TCP port 22.

A later version of the protocol appeared under the name **SSH-2**. The IETF "secsh" working group has started to standardise SSH-2, which features both security and feature improvements over SSH-1. Better security, for example, comes through Diffie-Hellman key exchange and strong integrity checking via MACs. New features of SSH-2 include the ability to run any number of shell sessions over a single SSH connection.

IRC – Internet Relay Chat

IRC is a form of instant communication over the Internet. It is mainly designed for group (many-to-many) communication in discussion forums called channels, but also allows one-to-one communication. IRC is an open protocol that uses TCP and optionally SSL. An IRC server can connect to other IRC servers to expand the IRC network. Users access IRC networks by connecting a client to a server. There are many client and server implementations. Most IRC servers do not require users to log in, but a user will have to set a nickname before being connected.

IRC is a plaintext protocol, which means that it is fully possible (though quite inconvenient) to use IRC via a basic byte-stream client such as netcat or telnet. However, the protocol only uses a slightly modified version of ASCII, and does not originally provide any support for non-ASCII characters in text, with the result that many different, incompatible character encodings (such as ISO 8859-1 and UTF-8) are used.

SNMP – Simple Network Management Protocol

SNMP is a standard set of rules, which allow devices supporting this protocol to be managed from a common device, usually a network management system. At the time of writing there are three versions of SNMP, these are.

SNMP V1

The first RFC for SNMP version 1, appeared in 1988 and has been criticized for its poor security. Authentication of clients is performed only by a "community string", in effect a type of password, which is transmitted in clear text.

SNMP V2

Version 2 was not widely adopted due to serious disagreements over the security framework in the standard. SNMP v2 or SNMP v2p, revises version 1 and includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. It introduced GETBULK, an alternative to iterative GETNEXTs for retrieving large amounts of management data in a single request. However, the new party-based security system in SNMP v2, viewed by many as overly complex, was not widely accepted.

SNMP v2u, is defined in RFC 1909-RFC 1910. This is a compromise that attempts to offer greater security than SNMP v1, but without incurring the high complexity of SNMP v2. A variant of this was commercialised as SNMP v2*, and the mechanism was eventually adopted as one of two security frameworks in SNMP v3.

SNMP V3

As of 2004 the Internet Engineering Task Force recognised Simple Network Management Protocol version 3 as defined by RFC 3411-RFC 3418 (also known as STD0062) as the

current standard version of SNMP. The IETF considers earlier versions as “Obsolete” or “Historical”.

In practice, SNMP implementations often support multiple versions: typically SNMPv1, SNMPv2c, and SNMPv3.

H.323

H.323 is an umbrella recommendation from the ITU-T, that defines the protocols to provide audio-visual communication sessions on any packet network. It is currently implemented by various Internet real-time applications as NetMeeting and GnomeMeeting (the latter using the OpenH323 implementation). It is a part of the H.32x series of protocols which also address communications over ISDN, PSTN or SS7. Challengers to H.323 are SIP, a standard from the IETF and the new Skype protocol. All these are used in Voice over IP (VoIP, Internet Telephony, or IP Telephony). One strength of H.323 was the relatively early availability of a set of standards, not only defining the basic call model, but in addition the supplementary services, needed to address business communication expectations. H.323 was the first VoIP standard to adopt the IETF standard RTP to transport audio and video over IP networks.

H.323 is based on the ISDN Q.931 protocol and is suited for interworking scenarios between IP and ISDN, respectively between IP and QSIG. A call model, similar to the ISDN call model, eases the introduction of IP Telephony into existing networks of ISDN based PBX systems. A smooth migration towards IP based PBX systems becomes plannable.

SIP – ‘Session Initiation Protocol’

SIP is a protocol developed by the IETF MMUSIC Working Group and proposed standard for setting up sessions between one or more clients. It is currently (2005) the leading signaling protocol for VOIP (Voice over IP), gradually replacing H.323 in this role.

A goal for SIP was to provide a superset of the call processing functions and features present in the public switched telephone network (PSTN). As such, features that permit familiar telephone-like operations are present: dialing a number, causing a phone to ring, hearing ringback tones or a busy signal. Implementation and terminology are different.

Although many other VoIP signaling protocols exist, SIP is characterized by its roots in the IP community rather than the telecom industry. SIP is being standardized and governed by the IETF while older, more complex VoIP protocols were proposed by the ITU.

SIP works in concert with several other protocols and is only involved in the signaling portion of a communication session. SIP acts as a carrier for the Session Description Protocol (SDP), which describes the media content of the session, e.g. what IP ports to use, the codec being used etc. In typical use, SIP “sessions” are simply packet streams of the Real Time Transport Protocol (RTP). RTP is the carrier for the actual voice or video content itself.

RTP – Real-time Transport Protocol

RTP defines a standardized packet format for delivering audio and video over the Internet. It was developed by the Audio-Video Transport Working Group of the IETF and first published in 1996 as RFC 1889. It was originally designed as a multicast protocol, but has since been applied in many unicast applications. It is frequently used in streaming media systems (in conjunction with RTSP) as well as videoconferencing and push to talk systems (in conjunction with H.323 or SIP), making it the technical foundation of the Voice over IP

industry. It goes along with the RTP Control Protocol (RTCP) and it's built on top of User Datagram RTP ensures consistent delivery order of voice packets in an IP internetwork.

RTCP – Real Time Control Protocol

RTCP is a sister protocol of the Real-time Transport Protocol (RTP). It is defined in RFC 3550 (which obsoletes RFC 1889).

RTCP, which stands for Real-time Transport Control Protocol, provides out-of-band control information for an RTP flow. It partners RTP in the delivery and packaging of multimedia data, but does not transport any data itself. It is used periodically to transmit control packets to participants in a streaming multimedia session. The primary function of RTCP is to provide feedback on the quality of service being provided by RTP.

It gathers statistics on a media connection and information such as bytes sent, packets sent, lost packets, jitter, feedback and round trip delay. An application may use this information to increase the quality of service perhaps by limiting flow, or maybe using a low compression codec instead of a high compression codec. RTCP is used for QoS reporting

9. NETWORK FEATURES

Quality of Service

In the fields of packet-switched networks and computer networking, the traffic engineering term Quality of Service (QoS) refers to the probability of the network meeting a given traffic contract, or in many cases is used informally to refer the probability of a packet passing between two points in the network. While most of the issues involving QoS relate to wide area networking, with todays high levels of traffic running over Local Area Networks QoS is becoming more of an issue within the LAN, and is often supported by Ethernet switches.

There is a school of thought which says why bother with a QOS mechanism. If the network is that busy that it needs to start dropping packets then its better to add more bandwidth, because eventually the priority packets will be discarded due to too much traffic.

Why do we require a Quality of Service?

When the Internet was first being created, there was no perceived need for a QoS application. In fact the entire internet ran on a "best effort" system. There were 4 "type of service" bits and three "precedence" bits provided in each message, but they were largely unused. There are many things that can happen to packets as they travel from origin to destination and they result in the following problems, as seen from the point of view of the sender and receiver:

- **dropped packets** – the routers might fail to deliver (*drop*) some packets if they arrive when their buffers are already full. Some, none, or all of the packets might be dropped, depending on the state of the network, and it is impossible to determine what happened in advance. The receiving application must ask for this information to be retransmitted, possibly causing severe delays in the overall transmission.
- **delay** – it might take a long time for a packet to reach its destination, because it gets held up in long queues, or takes a more indirect route to avoid congestion. Alternatively, it might follow a fast, direct route. The delay is very unpredictable.
- **out-of-order delivery** – when a collection of related packets are routed through the internet, different packets may take different routes, each resulting in a different delay. The result is that the packets arrive in a different order than the one with which they were sent. This problem necessitates special additional protocols responsible for rearranging out-of-order packets once they reach their destination.
- **error** – sometimes packets are misdirected, or combined together, or corrupted, while en route. The receiver has to detect this and, just as if the packet was dropped, ask the sender to repeat itself.

Applications requiring QoS

A Quality of Service may be required for certain types of network traffic, for example:

- streaming multimedia may require guaranteed throughput
- IP telephony may require strict limits on jitter and delay
- dedicated link emulation requires both guaranteed throughput and imposes limits on maximum delay
- a safety-critical application, such as remote surgery may require a guaranteed level of availability (this is also called *hard QoS*).

These types of service are called *inelastic*, meaning that they require a certain level of bandwidth to function – if they get more than that they can't use it, and if they get less, then they can't function at all. By contrast, *elastic* applications can take advantage of however much or little bandwidth is available.

Obtaining QoS

There are essentially two ways to provide QoS guarantees. The first is simply to provide *lots* of resources, enough to meet the expected *peak* demand with a substantial safety margin. This is nice and simple, but some people believe it to be expensive in practice, and can't cope if the peak demand increases faster than predicted: deploying the extra resources takes time.
The second one is to require the network to make reservations for certain traffic types.

Types of QOS

IntServ

In computer networking IntServ or integrated services is a system that attempts to guarantee quality of service (QoS) on networks. In other words, IntServ is designed to allow video and sound to reach the user without interruption.

It is a fine-grained system which is often contrasted with DiffServ's coarse-grained system. The idea of IntServ is that every router in the system implements IntServ, and every application that requires some kind of guarantee has to make an individual reservation. "Flow Specs" describe what the reservation is for, while "RSVP" is the underlying mechanism for making them.

Flow Specs

There are two parts to a flow spec:

- What does the traffic look like? Done in the Traffic SPECification or TSPEC part.
- What guarantees does it need? Done in the service Request SPECification or RSPEC part.

RSVP

The Resource ReSerVation Protocol (RSVP) is described in RFC 2205. All machines on the network capable of sending QoS data send a PATH message every 30 seconds, which spreads out through the network. Those who want to listen to them send a corresponding RESV (short for "Reserve") message which then traces the path backwards to the sender. The RESV message contains the flow specs.

The routers between the sender and listener have to decide if they can support the reservation being requested, and if they cannot then send a reject message to let the listener know about it. Otherwise, once they accept the reservation they have to carry the traffic.

The routers then store the nature of the flow, and also police it. This is all done in soft state, so if nothing is heard for a certain length of time, then the reader will time out and the reservation will be cancelled. This solves the problem if either the sender or the receiver crash or are shut down incorrectly without first cancelling the reservation. The individual routers may, at their option, police the traffic to check that it conforms to the flow specs.
In summary, RSVP has the following attributes:

- RSVP makes resource reservations for both unicast and many-to-many multicast applications, adapting dynamically to changing group membership as well as to changing routes.
- RSVP is simplex, i.e., it makes reservations for unidirectional data flows.
- RSVP is receiver-oriented, i.e., the receiver of a data flow initiates and maintains the resource reservation used for that flow.
- RSVP maintains "soft" state in routers and hosts, providing graceful support for dynamic membership changes and automatic adaptation to routing changes.
- RSVP is not a routing protocol but depends upon present and future routing protocols.
- RSVP transports and maintains traffic control and policy control parameters that are opaque to RSVP.

Problems

The problem with IntServ is that many states must be stored in each router. As a result, IntServ works on a small-scale, but as you scale up to a system the size of the Internet, it is difficult to keep track of all of the reservations. As a result, IntServ is not very popular.

DiffServe

DiffServ or differentiated services is a method of trying to guarantee quality of service on large networks such as the Internet, but it is increasingly being used within the LAN on higher end Ethernet switches.

DiffServ deals with bulk flows of data rather than single flows and single reservations. This means that a single negotiation will be made for all of the packets from, for example, a single ISP, or a single university. The contracts resulting from these negotiations are called "service level agreements". These service level agreements will specify what classes of traffic will be provided, what guarantees are needed for each class, and how much data will be sent for each class.

A "DiffServ cloud" is a collection of DiffServ routers. When packets enter a DiffServ cloud they are first classified by the sender. The sender sets the "type of service" field (which hence is also called DiffServ Code Point – DSCP), in the IP header according to the class of the data, so that the better classes get higher numbers.

As the packets enter the DiffServ cloud they are policed by the receiver. If there is so much traffic that it breaches the service level agreement, then the sender may be liable for fines, according to the details of the contract. Within the DiffServ cloud, all the individual routers need to do is to give highest priority to the packets with the highest value in the type of service field, which is simple to implement. There may also be a discard policy on the frequencies with which each type of packet is discarded if the router runs out of buffer space.

Example

There are many ways to split up traffic into classes. For example, the traffic may be split into first, second, and third classes. In each router, First class traffic takes precedence over second class traffic, which takes precedence over third class.

Special handling may be done in at least two different ways:

- preferential forwarding, where more recent higher precedence packets are allowed to jump the queue over old lower precedence packets

- preferential discarding, where buffer space for higher-preference packets is allowed to grow at the expense of lower precedence packets which are discarded

There are also many other schemes involving hybrids of these and other Quality of Service strategies.

- Usually it is done by the router which connects a local area network to the Internet. The router then decides for example, to put interactive traffic like remote shells or online games to maximum priority in order to reduce ping time. Other traffic like HTTP or SMTP then get some lower priority while usual downloads like FTP or peer to peer networks are getting the lowest priority.
- The decision about which traffic should get high priority usually depends on the intended usage of the network connection. Another approach for deciding which traffic is important is the TOS/DiffServ field in the IP header.

Advantages of DiffServ

One advantage of DiffServ, is that all the policing and classifying is done at the boundaries between DiffServ clouds. This means that in the core of the Internet, routers can get on with doing the job of routing, and not care about the complexities of collecting payment or enforcing agreements.

Disadvantages of DiffServ

One disadvantage is that the details of how individual routers deal with the type of service field is somewhat arbitrary, and it is difficult to predict end-to-end behaviour. This is complicated further if a packet crosses two or more DiffServ clouds before reaching its destination.
From a commercial viewpoint, this is a major flaw, as it means that it is impossible to sell different classes of end-to-end connectivity to end users, as one provider's first class packet may be another's third class packet. Internet operators could fix this, by enforcing standardised policies across networks, but are not keen on adding new levels of complexity to their already complex peering agreements.

MultiLayer Network Equipment

Network equipment, that supports DiffServ and perhaps IntServ, are called multilayer network equipment. A switch that supports DiffServ and perhaps IntServ is called a multilayer switch.

However, the market has not yet favoured QoS services. Some people believe that this is because a "dumb" network that offers sufficient bandwidth for most applications, most of the time, is already economically stable, with little incentive to deploy non-standard stateful QoS-based applications.

Internet peering arrangements are already complex, and there appears to be no enthusiasm among providers for supporting QoS across peering connections, or agreement about what policies should be supported in order to do so.

QoS sceptics further point out that if you are dropping many packets on elastic low-QoS connections, you are already dangerously close to the point of congestion collapse on your inelastic high-QoS applications, without any way of further dropping traffic without violating traffic contracts.

MPLS (Multiprotocol Label Switching)

Multiprotocol Label Switching (MPLS) is a data-carrying mechanism, operating at a layer below protocols such as IP. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model. It can be used to carry many different kinds of traffic, including both voice telephone traffic and IP packets.

With MPLS the edge routers assign a lable to the packet which defines its path through the network, in much the same way Frame Relay assigns a DLCI. This allows the various routers in the core of the network to pass the packets through without the need to refer to a routing table, thus eliminating the delays associated with making routing decisions at each stage.

Comparison of MPLS versus IP

Unlike IP, MPLS does not define a directly usable end-point protocol. It only defines a way of encapsulating other layer 2 and layer 3 protocols. In this regard, it is similar to a protocol like PPP. Also unlike IP, MPLS explicitly decouples routing from forwarding, although it can fall back to using IP-style routing if necessary

10. VIRTUAL LANS

Introduction

A virtual LAN, commonly known as a VLAN, is a logically segmented network mapped over physical hardware. IEEE 802.1Q is the predominant protocol. Prior to this, Cisco was one of many companies which had a proprietary protocol: Cisco used a variant of IEEE 802.10 called Inter-Switch Link (ISL).

VLAN technology allows network managers to group switch ports and users connected to them into logically defined communities of interest. These groupings can be co-workers within the same department, a cross-functional product team, or diverse users sharing the same network application or software (such as Lotus Notes users). Grouping these ports and users into communities of interest, referred to as VLAN organizations, can be accomplished within a single switch, or more powerfully, between connected switches within the enterprise. By grouping ports and users together across multiple switches, VLANs can span single building infrastructures, interconnected buildings, or even wide-area networks (WANs).

Early VLANs were often configured to reduce the size of the collision domain in a large single Ethernet segment to improve performance. When Ethernet switches made this a non-issue (because they have no collision domain), attention turned to reducing the size of the broadcast domain at the MAC layer. Another purpose of a virtual network is to restrict access to network resources without regard to physical topology of the network, although the strength of this method is debatable.

Virtual LANs operate at layer 2 of the OSI model. However, a VLAN is often configured to map directly to an IP network, or subnet, which gives the appearance it is involved in layer 3. Switch to switch links and switch to router links are called trunks. A router serves as the backbone for traffic going across different VLANs.

VLANs can be configured in various ways:

- Protocol level, IP, IPX, LAT, etc
- MAC address based.
- IP subnet based.
- Port based, and therefore real world based, say by accounting versus marketing departments.

VLAN Standards

IEEE 802.1Q was a project in the IEEE 802 standards process to develop a mechanism to allow multiple bridged networks to transparently share the same physical network link without leakage of information between networks. IEEE 802.1Q is also the name of the standard issued by this process, and in common usage the name of the encapsulation protocol used to implement this mechanism over Ethernet networks.

IEEE 802.1Q defines the meaning of a virtual LAN or VLAN with respect to the specific conceptual model underpinning bridging at the MAC layer and to the IEEE 802.1D spanning tree protocol.

Types of VLAN

VLANs can be static, dynamic, or port-centric and there are two methods of establishing a VLAN: frame-tagging and frame-filtering. Frame-tagging changes the information that is contained within the layer 2 frame, so that switches may forward the VLAN traffic to their correct VLAN destination and return the frame to its normal format. Frame-filtering involves the switch looking for certain criteria in the layer 2 frame and using this matching system to forward the traffic to its correct VLAN and destination.

A layer 2 device can implement VLANs in different ways:

- Open VLANs have a single MAC address database for all VLANs
- Closed VLANs have a separate MAC address database for each VLAN
- Mixed Mode VLANs can be configured as Open or Closed on a VLAN basis.

Closed VLANs are generally considered more secure than Open VLANs.

Virtual Private Networks

What is a VPN?

Where LANs are interconnected via a common IP network (such as over the Internet) a common cost saving method is to form a Virtual Private Network, or VPN. In effect this is a tunnel through the Internet, which emulates a private network for the organisation.

Types of VPN

Secure VPNs use cryptographic tunneling protocols to provide the necessary confidentiality (preventing snooping), sender authentication (preventing identity spoofing), and message integrity (preventing message alteration) to achieve the privacy intended. When properly chosen, implemented, and used, such techniques can provide secure communications over unsecured networks.

Because such choice, implementation, and use are not trivial, there are many insecure VPN schemes on the market.

Secure VPN technologies may also be used to enhance security as a ‘security overlay’ within dedicated networking infrastructures.

Secure VPN protocols include the following:

- Ipsec (IP security), an obligatory part of IPv6.
- SSL used either for tunneling the entire network stack, such as in OpenVPN, or for securing what is essentially a web proxy. Allthough the latter is often called a “SSL VPN” by VPN vendors, it is not really a fully-fledged VPN.
- PPTP (point-to-point tunneling protocol), developed by Microsoft.

Trusted VPNs do not use cryptographic tunneling, and instead rely on the security of a single provider’s network to protect the traffic. Multi-protocol label switching (MPLS) is commonly used to build trusted VPNs. Other protocols for trusted VPNs include:

- L2F (Layer 2 Forwarding), developed by Cisco.
- L2TP (Layer 2 Tunnelling Protocol), including work by both Microsoft and Cisco.

- L2TPv3 (Layer 2 Tunnelling Protocol version 3).

IP Sec- IP Security

Introduction to Ipsec

IPSec is an abbreviation of IP security, is a standard for securing IP communications by encrypting and authenticating all IP packets. IPsec provides security at the network layer. IPsec is a protocol suite (i.e., a set of interdependent protocols) consisting of

1. Protocols for securing packet flows

There are two:

a. **Encapsulating Security Payload** (ESP) provides authentication, data confidentiality and message integrity;

b. **Authentication Header** (AH) provides authentication and message integrity, but does not offer confidentiality (which is why it is not used as pervasively as ESP).

So why keep AH if EPS can do the same and even more? The answer lies in the past. Originally AH was only used for integrity and ESP was used for encryption.

2. Key exchange protocols used for setting up those secure flows

Currently only one key exchange protocol is defined, the IKE protocol.

IP Sec and IPV6

IPsec is an obligatory part of IPv6 the new IETF Internet standard for Internet Protocol packet traffic, and is optional for use with IPv4. As a result, IPsec is expected to become more widely deployed as IPv6 becomes more popular. IPsec protocols are defined by RFCs 2401-2412. Work is progressing to release updated replacement documents.

IP Sec Protocols Operate at Layer 3

IPsec protocols operate at layer 3 of the OSI model, which makes them suitable for protecting both TCP and UDP-based protocols when used alone. This means that, compared with transport layer and above protocols such as SSL (OSI Layer 6), which cannot protect UDP level traffic, the IPsec protocols must cope with reliability and fragmentation issues, adding their complexity and processing overhead. SSL/TLS, in contrast, rely on a higher level layer TCP (OSI Layer 4) to manage reliability and fragmentation.

11. ENCRYPTION

Introduction

Security over the WAN and within the LAN is becoming an issue and encryption of data is becoming almost a mandatory. This section outlines some of the encryption systems commonly used today.

What is encryption?

Encryption is the process of obscuring information to make it unreadable without special knowledge. While encryption has been used to protect communications for centuries, only organisations and individuals with an extraordinary need for secrecy have made use of it. In the mid-1970s, strong encryption emerged from the sole preserve of secretive government agencies into the public domain, and is now employed in protecting widely-used systems, such as Internet e-commerce, mobile telephone networks and bank automatic teller machines.

Encryption can be used to ensure secrecy, but other techniques are still needed to make communications secure, particularly to verify the integrity and authenticity of a message; for example, a message authentication code (MAC) or digital signatures. Another consideration is protection against traffic analysis.

Types of Cipher

Stream cipher

A stream Cipher is a symmetric cipher in which the input digits are encrypted one at a time, and in which the transformation of successive digits varies during the encryption. An alternative name is a state cipher, as the encryption of each digit is dependent on the current state. In practice, the digits are typically single bits or bytes.

Stream ciphers represent a different approach to symmetric encryption from block ciphers. Block ciphers operate on large blocks of digits with a fixed, unvarying transformation. This distinction is not always clear-cut: some modes of operation use a block cipher primitive in such a way that it then acts effectively as a stream cipher. Stream ciphers typically execute at a higher speed than block ciphers and have lower hardware complexity. However, stream ciphers can be susceptible to serious security problems if used incorrectly.

Well know stream ciphers are – RC4, A5/1, A5/2, Chameleon, FISH, Helix, ISAAC, LEVIATHAN, MUGI, Panama Pike, SEAL, SOBER, SOBER-128, WAKE.

Block cipher

A block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed *blocks*, with an unvarying transformation. When encrypting, a block cipher might take a (for example) 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext. The exact transformation is controlled using a second input — the secret key. Decryption is similar: the decryption algorithm takes a 128-bit block of ciphertext together with the secret key, and yields the original 128-bit block of plaintext.To encrypt messages longer than the block size (128 bits in the above example), a mode of operation is used. The distinction between the two types is not always clear-cut: a block cipher, when used in certain modes of operation, acts effectively as a stream cipher.

An early and highly influential block cipher design was the Data Encryption Standard (DES), developed at IBM and published as a standard in 1977. A successor to DES, the Advanced Encryption Standard (AES), was adopted in 2001.

Some algorithms that make use of block cipher – 3-Way AES, Blowfish, CAST-128, CAST-256, DEAL, DES, DES-X, FEAL, MAGENTA, RC2, RC5, RC6, SAFER, Serpent, Triple DES, Twofish,

Encryption Algorithms

There are a good many encryption algorithms and its outside the scope of this book to detail all of the algorithms. However we have provided a brief overview of some of the better know algorithms here.

DES

The Data Encryption Standard (DES) is a cipher selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally. The algorithm was initially controversial, with classified design elements, a relatively short key length, and suspicions about a National Security Agency (NSA) backdoor. DES consequently came under intense academic scrutiny, and motivated the modern understanding of block ciphers and their cryptanalysis.

DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours. There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES).

Triple DES

Triple DES (also 3DES) is a block cipher formed from the Data Encryption Standard (DES) cipher. It was developed by Walter Tuchman (the leader of the DES development team at IBM) and is specified in FIPS Pub 46-3. There are several ways to use DES three times; not all are Triple-DES and not all are as secure. Triple-DES is defined as performing a DES encryption, then a DES decryption, and then a DES encryption again.

Triple-DES has a key length of 168-bits (three 56-bit DES keys), but because of an attack it has an effective key size of 112 bits. A variant reduces the key size to 112 bits. This mode is susceptible to some attacks, though.

DES is not a group; if it were one, the Triple-DES construction would be equivalent to a single DES operation and no more secure. Veteran 3DES stands unbroken to this day (according to publicly available information), but its demise is inevitable due to the cipher's miserably slow speed. The original DES design was meant for hardware-only use and it lends itself particularly poorly to implementation on modern 32-bit operating systems. An appliance capable of 3 Mbit/s VPN throughput over 3DES could easily achieve 10-22 Mbits when using the Blowfish block cipher.

Blowfish

Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. While no effective

cryptanalysis of Blowfish has been found to date, more attention is now given to block ciphers with a larger block size, such as AES or Twofish.

Schneier designed Blowfish as a general-purpose algorithm, intended as a replacement for the aging DES and free of the problems associated with other algorithms. At the time, many other designs were proprietary, encumbered by patents or kept as government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone." Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits.

Advanced Encryption Standard – AES

Advanced Encryption Standard also known as Rijndael, is a block cipher adopted as an encryption standard by the US government, and is expected to be used worldwide and analysed extensively, as was the case with its predecessor, the Data Encryption Standard (DES). It was adopted by National Institute of Standards and Technology (NIST) as US FIPS PUB 197 in November 2001after a 5-year standardisation process.

The cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen AES is fast in both software and hardware, is relatively easy to implement, and requires little memory. As a new encryption standard, it is currently being deployed on a large scale.

Strictly speaking, AES is not precisely Rijndael (although in practice they are used interchangeably) as Rijndael supports a larger range of block and key sizes; AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits, whereas Rijndael can be specified with key and block sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits. As of 2005, no successful attacks against AES have been recognised. The National Security Agency (NSA) reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for US Government non-classified data. In June 2003, the US Government announced that AES may be used for classified information:

TwoFish

Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the AES contest, but was not selected for standardisation. Twofish is related to the earlier block cipher Blowfish.

Twofish's distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. Twofish borrows some elements from other designs; for example, the *Pseudo-Hadamard Transform* (PHT) from the SAFER family of ciphers. Twofish uses the same Feistel structure as DES.

On most software platforms Twofish is slightly slower than Rijndael (the chosen algorithm for AES) for 128-bit keys, but somewhat faster for 256-bit keys.
As of 2004, there is no known attack on Twofish more efficient than brute force key search.

SAFER

SAFER (Secure And Fast Encryption Routine) is the name of a family of block ciphers designed primarily by James Massey (one of the designers of IDEA) on behalf of Cylink Corporation. The early SAFER K and SAFER SK designs share the same encryption function, but differ in the number of rounds and the key schedule. More recent versions — SAFER+ and SAFER++ — were submitted as candidates to the AES process and the NESSIE

project respectively. All of the algorithms in the SAFER family are unpatented and available for unrestricted use.

The first SAFER cipher was SAFER K-64, published by Massey in 1993, with a 64-bit block size. The “K-64” denotes a key size of 64 bits. There was some demand for a version with a larger 128-bit key, and the following year Massey published such a variant incorporating new key schedule designed by the Singapore Ministry for Home affairs: SAFER K-128. However, both Lars Knudsen and Sean Murphy found minor weaknesses in this version, prompting a redesign of the key schedule to one suggested by Knudsen; these variants were named SAFER SK-64 and SAFER SK-128 respectively.

Serpent

Serpent is a symmetric key block cipher which was a finalist in the Advanced Encryption Standard contest, where it came second to Rijndael.

Like other AES submissions, Serpent has a block size of 128 bits and supports a key size of 128, 192 or 256 bits. The cipher is a 32-round substitution-permutation network operating on a block of four 32-bit words. Each round uses 32 copies of the same 4-bit to 4-bit S-box. Serpent was designed so that all operations can be executed in parallel, using 32 1-bit slices. This maximises parallelism, but also makes use of the extensive cryptanalysis work performed on DES.

Serpent was widely viewed as taking a more conservative approach to security than the other AES finalists, opting for a larger security margin: the designers deemed 16 rounds to be sufficient against known types of attack, but specified 32 rounds as insurance against future discoveries in cryptanalysis.

12. PRODUCT TRENDS

When this book was first written some 15 years ago, LANS could use any of a number of operating systems and protocols, and the complexities that arose were in ensuring the various different systems could co-exist and communicate.

Today with IP becoming the de fatco standard inter-working is rarely an issue, and LANs have become less complex. However the border between LAN and WAN is also becoming clouded. The technologies are starting to merge, and its common to see new Metro Ethernet networks providing rings around towns and cities at Gigabit speeds, and providing the same facilities as are found within the WAN.

Many of the technologies used within the WAN are now being used within the LAN. A glaring example is QOS (Quality of Service), the X.25 networks from the early 1980's used to provide classes of service, which can be seen as a predecessor to Quality of Service today.

As LANS and WANs merge the differentiation between vendors will dissapear and performance and flexibility will be the key to the future.

Industry Standard Hardware and Open Source Software

We are also witnessing a major change in the way vendors are developing products. The major brand leaders have invested millions of dollars and taken two or three years to design their proprietary products from the ground up. The result is an expensive, inflexible product which is outdated before its launch.

There is a new breed of vendor emerging that uses industry standard hardware, and open source software (for example Unix or Linux) to bring products to market very quickly and at a fraction the cost of the proprietary vendors. These products can be seen within the Router and Ethernet switching market-places, where standard 'off the shelf' components are being used to develop very high peformance, high functionality and sophisticated products, costing a fraction the price of the acknowledged brand leaders.

The benefits of this approach are the very rapid time to market, the ease of migration from one hardware platform to another, and the low cost.

Why Don't All Organisations Purchase Open Source products?

While enlightened organisations, such as Internet Service Providers and Academic organisations move towards 'Open Source' products, the more conservative organisations, still insist on purchasing a brand name rather than high performance, and value for money. If the IT manager is sufficiently technical or has a good enough team to be able to evaluate products, then the 'Open Source' vendor will have little difficulty in beating the traditional dinosaurs, however, as was said back in the 1980's 'No One Gets fired for buying IBM' and currently most IT managers don't have the confidence or knowledge to move away from a brand name. The move to 'Open Source' will happen eventually but it will probably take another few years before these products are truly accepted by the mass market.

13. SUMMARY

Although it's not within the scope of this book to go too deeply into any of the topics covered in this book we hope we have provided an informative introduction to the subject of 'Local Area Networks'. There are other Pocket Books within the range which cover subjects such as Ethernet Switching, Telecommunications and ISDN in more detail, and which can be found on the Case Communications web site.

IT and Networking has always been a fast moving area and we can witness this by looking at the different focus of this book from when it was first published, and OSI was the panacea to this current edition where IP is the dominant protocol and OSI is a guiding framework.

In due course Case Communications hope to expand the range of Pocket Books to cover specific areas of interest, such as Security, Wireless LANs etc.

If in the meantime you have any comments or suggestions please mail to admin@casecomms.com

GLOSSARY

10BASE-2

A form of Ethernet and IEEE 802.3 network cabling, using thin co-axial cable. The term refers to 10Mbps (speed) BASEband (transmission) 200 metres (maximum length actually 185 metres). Commonly known as “Cheapernet”.

10BASE-5

A form of Ethernet and IEEE 802.3 network cabling, using thick co-axial cable. The refers to 10Mbps (speed) BASEband (transmission) 500 metres (maximum length).

10BASE-T

A form of Ethernet and IEEE 802.3 network cabling, using twisted-pair cabling. The term refers to 10Mbps (speed) BASEband (transmission) twisted-pair cable. 10 BASE T recommends a segment length of 100 metres. In almost all applications in use today this technology is run at 100Mbps.

Advanced Encryption Standard – AES

Advanced Encryption Standard also known as Rijndael, is a block cipher adopted as an encryption standard by the US government, and is expected to be used worldwide and analysed extensively, as was the case with its predecessor, the Data Encryption Standard (DES). It was adopted by National Institute of Standards and Technology (NIST) as US FIPS PUB 197 in November 2001after a 5-year standardisation process.

ANSI

American National Standards Institute.

AppleTalk

A proprietary network system designed by Apple Computer, principally used with Macintosh systems.

Application Layer

OSI standard for reading, writing, sharing and administering files on different machines.

ARCnet

A proprietary network system designed by Data-point Corporation using token Bus techniques.

ARPANET

The Defence Advanced Research Projects Agency Network. A network in America which was used to develop the Internet Protocol Suite, source of TCP/IP protocols and many others such as OSI.

ASCII

American Standard Code for Information Interchange

ATM

Asynchronous Transfer Mode, a high-speed, scaleable cell-switching protocol that breaks packets down into fixed 53-byte cells.

AUI

Attachment Unit Interface. Defined in IEEE 802.3 as the interface between the transceiver and the network device.

Back Pressure

A technique for preventing buffer overload by sending a jam signal when a station tries to send to an overloaded port. The sending station will interpret the signal as a collisions, stop sending and try again later.

Baseband

A transmission technique employed in LANs. Only one device can communicate at one time and a device simply sends its digital signal on to the cable without any modification.

Blowfish

Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. While no effective cryptanalysis of Blowfish has been found to date, more attention is now given to block ciphers with a larger block size, such as AES or Twofish.

Bridge

A device which connect two separate networks at the MAC layer and passes data between the two networks, filtering local communications.

Broadband

Analogue transmission technique employed in LANs. The signals on the network are divided, (usually by frequency division), to allow more than one (usually pairs of signals) on the cable at any one time. This form of communication requires modems for all devices wishing to access the network.

Bus

A form of network structure based on a single length of cable to which all network devices are connected. Ethernet is an example of such a network structure.

Bit

An abbreviated form of Binary digit used to represent a single transition on a data line, or a fraction of a byte.

Byte

A unit of computer information, consisting of eight bits (binary digits).

CAD

Computer Aided Design.

CCITT

Comite Consultatif Internationale de Telegraphique et Telephonique. A standards body concentrating on the definition of European Communications Standards.

Cheapernet

A term generated following a revised specification for Ethernet using a thin, lower cost, co-axial cable.

CLNS

ConnectionLess-mode. Networking Service as defined in ISO 8473, operating at level 3, Network, of the OSI reference model.

Co-axial cable

A cable consisting of a single inner core surrounded by insulators and a stranded metal sheath, all encased in a single insulating outer cover.

Comite Consultatif Internationale de Telegraphique et Telephonique

See CCITT

CONS

Connection-mode Network Service. Operates at the Network Layer (layer 3) and implements a connection-oriented networking system using X.25.

Connection Oriented Protocol

A form of transmission where a connection is established across a network proper to the first transmission of data taking place. The connection handles checking and error recovery during transmission thus incurring a connection overhead on the transmission.

ConnectionLess Network Service

See CLNS

Connectionless Protocol

A form of transmission where no communication takes place prior to the first transmission of data. Therefore no connection is made on the network and no checking takes place during transmission thus reducing the connection overhead on the transmission.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance. A method of network access not covered by OSI standards. This technique is implemented on AppleTalk networks.

CSMA/CD

Carrier Sense Multiple Access with Collision Detect. The technical reference to the standard LAN transmission network utilising a bus structure, conforming to IEEE 802.3 and ISO 8802-3, which were based on the Ethernet network standard.

Cut-through Switching

A switch forwarding method designed to minimise delay. A packet is forwarded to the output port as soon as the destination address is known.

Data Link

Layer 2 of the OSI 7-layer model.

Datagram

A unit or packet of data sent across a network. A datagram is self contained, with source and destination address, but is not necessarily a complete communication, which may require many such datagrams.

DDCMP

Digital Data Communications Message Protocol. A form of transmission for wide area connectivity over DECnet.

DECnet

A network architecture produced by Digital Equipment Corporation encompassing local and wide area connectivity.

DES

The Data Encryption Standard (DES) is a cipher selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally.

DiffServe

DiffServ or differentiated services is a method of trying to guarantee quality of service on large networks such as the Internet, but it is increasingly being used within the LAN on higher end Ethernet switches.

Distributed Systems Gateway

DSG. A device which operates at layer 4 of the OSI reference model and allows interconnection of dissimilar networks.

DIX DEC, Intel and Xerox

These terms are used in relation to the published Ethernet Specifications.

Early Token Release

A modified version of token passing where a device does not have to wait for its communication to circle a network before transmitting the token on around the network.

Ethernet

A LAN transmission network utilising a bus structure, first produced by Xerox in the USA, later adopted by both DEC and Intel as well (see DIX). This was later adapted to create the IEEE 802.3 and ISO 8802-3 standards (see CSMA/CD).

EtherTalk

An Ethernet implementation of the lower two layers of the AppleTalk protocol suite. EtherTalk complies with 802.3.

FDDI

Fibre Distributed Data Interface. A token passing ring network specification developed by ANSI, implementing dual optical fibre rings. The network operates at 100Mbps and can be up to 100 kilometres in length.

Fibre Distributed Data Interface

See FDDI

Fibre Optic Cable

A cable type based on a continuous strand of very fine glass which uses light to carry information. This type of cable is able to carry very high levels of data for great distances without interference.

File Server

A device, usually a PC, offering on-line storage and management of files for more than one device on a network. File servers offer storage and recall of data files and applications. Additionally they may offer sharing of files and applications, protocol conversion and central facilities such as electronic mail.

File Transfer Protocol

See FTP.

Fragment Free

A switch forwarding method that offers fixed delay whilst ensuring only valid frames are forwarded.

FTAM

File Transfer, Access and Management

FTP

File Transfer Protocol. A Protocol from the Internet Protocol Suite which provides transfer of files between two dissimilar machines.

Full-duplex

Two-way communication in which a station can send and receive data simultaneously, therefore doubling the bandwidth.

Gateway

A device used to allow conversion on LAN networks. Normally operating a layer 4 or above in OSI terms. Gateways convert information between two different networks, computers or applications.

Half-duplex

A communication method in which a station can either send or receive data, not both at the same time.

Half Repeater

A device which extends the distance a LAN can cover by joining two lengths of cable over another communication medium, such as a dial-up circuit, and regenerating the signal.

Head End

A device used with Broadband networks. This is positioned at one end of the cable to convert the signal from one channel and output it on the other channel.

Host Servers

A device which connects to a LAN and then allows a computer, which cannot directly support LAN protocols, to connect to it providing all necessary LAN support.

IEEE

Institute of Electrical and Electronic Engineers. An American Institute responsible for developing and publishing many communications standards (see section listing Standards).

Institute of Electrical and Electronic Engineers

See IEEE

Integrated Services Digital Network

See ISDN

Interworking

A term extending beyond communication any relating to hardware and software compatibility not just to allow connection but to maximise operational efficiency.

International Standards Organisation

A suite of network protocols originally designed for ARPANET in America and since adopted as the main de facto protocols for LANs.

IntServ

In computer networking IntServ or integrated services is a system that attempts to guarantee quality of service (QoS) on networks

ISDN

A form of public network that is designed to handle voice and data at high speed in digital format.

ISO

International Standards Organisation. An organisation devised to create standards which will promote internetworking between different vendors equipment. The main focus of communications is implementation of the Open Systems Interconnection (OSI) reference model.

LAN

See Local Area Network.

LAN Manager

A networking communication system operating on OS/2-based PCs, plus other systems produced by Microsoft and 3Com.

Laser Printer

A high quality printing device capable of producing totally free format image output.

Latency

The time delay introduced by a network device. The time taken for the device to receive a frame and begin sending it out again.

LF

Line field used to identify the protocol in use.

LLC

Logical Link Control. The upper of the two sub-layers in layer 2 of the OSI 7 layer model.

Local Area Network

A system for intercommunication between computer terminals, PCs and related equipment operating within the same general area.

LocalTalk

A twisted pair transmission system used with Macintosh networks, designed by Apple Computer.

Logical Link Control

See LLC.

Logical Ring

When token passing is implemented on a Token Bus network, the token cannot circulate as on a Token Ring network. A Logical Ring is implemented where each device is given a sequential address. When a taken is relayed on the network each receiving address attaches the next logical device address thus ensuring circulation of the data.

MAC

Media Access Control. The lower of the two sub-layers in layer 2 of the OSI 7 layer model.

MAN

Metropolitan Area Network. A term often used to describe the latest, high speed and long distance LANs, such as FDDI.

MAP

Manufacturing Automation Protocol. An OSI initiative pioneered by General Motors to create a series of standards for computer and communication s equipment interworking on the production floor, for example central computer to production line robot.

MAU

Multi-station Access Unit. A device for use on IBM Token Ring networks that allows terminals, PCs, printer and other devices to be connected in a star-based configuration.

Media Access Control

See MAC.

Metropolitan Area Network

See MAN.

MMFS

Manufacturing Message Format Standard. An OSI Application Layer standard devised for MAP type networks.

Multi-station Access Unit

See MAU.

MPLS (Multiprotocol Label Switching)

Multiprotocol Label Switching (MPLS) is a data-carrying mechanism, operating at a layer below protocols such as IP. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model

Netbios

A network communication system operating on MS/DOS PC networks.

Netware

A suite of application oriented interface protocols designed for use on LANs and produced by Novell.

Network Layer

Layer 3 of the OSI reference model, which allows interconnection of dissimilar networks (see Distributed Systems Gateway).

Non-deterministic

A term relating to the inability of a designed being able to predict the performance or delay on a network where collision is possible.

Open Systems Interconnection

See OSI

OSI

Open Systems Interconnection. The term defined by the International Standards Organisation as a basis for standards to enable different vendor systems to interwork without modification.

PC

Personal Computer.

PDU

Protocol Data Unit. Protocol Data Units are the datagrams relating to Logical Link Control (LLC) transmissions.

Physical Layer

Layer 1 of the OSI reference model Presentation Layer, Layer 6 of the OSI reference model Probabilistic. A term relating to the ability of any one device being able to communicate on a network where collision is possible.

Protocol Data Unit

See PDU.

POE

Power over Ethernet or PoE technology describes any system to transmit electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. The standard for POE is IEEE 802.3af

PSU

Power Supply Unit.

QOS

Quality of service, a method of assigning priority to packets carrying traffic which is more critical to delays than other traffic.

RAM

Random access memory used to temporarily store data in a CPU.

Rat's Tail

A term used to describe the network adaptor used to connect Apple Macintoshes to a LocalTalk LAN.

Repeater

A device which extends the distance a LAN can cover by joining two lengths of cable and regenerating the signal.

RG58

A co-axial cable, often referred to as "Thin" coax. This was introduced to reduce the costs of cabling early networks, particularly Ethernet. This version became known as "Cheapernet".

Router

A device which connects two separate networks at the Network Layer. It operates in a similar way to a bridge but also has the ability to choose routers through a network. Because a router operates at the Network Layer it is protocol-dependent.

SAFER

SAFER (Secure And Fast Encryption Routine) is the name of a family of block ciphers designed primarily by James Massey (one of the designers of IDEA) on behalf of Cylink Corporation. All of the algorithms in the SAFER family are unpatented and available for unrestricted use.

Segment

In bus structure network this refers to a single length of cable and attached devices which would normally be linked to another segment by a repeater.

Session Layer

Layer 5 of the OSI reference model.

Simple Mail

See SMTP

Store-and-Forward

A forwarding technique designed to avoid propagating bad frames. The frame is full loaded and checked before any of it is sent out again.

Transfer Protocol SMTP

Simple Mail Transfer Protocol.
A protocol from the Internet Protocol Suite, which provides electronic mail transfer across a network.

TwoFish

Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the AES contest, but was not selected for standardisation. Twofish is related to the earlier block cipher Blowfish.

SNA

Systems Network Architecture. An architecture and suite of protocols designed and produced by IBM for hierarchical computer networks.

Structured Wiring

A cabling philosophy which endeavours to minimise cable changes once a building has been wired.

TAP

A connection into the Local Area Network cable.

TCP/IP

Transmission Control Protocol/Internet Protocol. Two main network communication protocols, part of the Internet Protocol Suite.

Technical and Office Protocols

See TOP.

TELNET

A protocol from the Internet Protocol Suite which provides a Virtual Terminal interface for communicating devices.

Terminal Servers

A device which connects to a LAN and then allows one or more terminals, which cannot directly support LAN protocols, to connect to it providing all necessary LAN support.

Token

A token is a special sequence of data which is passed around a network sequentially. When the token is captured by a device it flags it as busy and adds data to the frame. Once the transmission has circled the network the busy token is replaced by a free token which the next device can then capture and transmit.

Token Bus

A LAN transmission network utilising a bus structure and implementing token passing access. This network is detailed by the IEEE 802.4 and ISO 8802-4 standards.

Token Ring

A LAN transmission network utilising a ring structure. The most common form is IBM Token Ring. This network type is detailed by the IEEE 802.5 and ISO 8802-5 standards.

TokenTalk

A Token Ring implementation of the lower two layers of the AppleTalk protocol suite.

TOP

Technical and Office Protocols. An OSI initiative pioneered by Boeing Computer Services to create a series of standards for computer and communications equipment interworking in the office environment.

Transmission Control Protocol/Internet Protocol

See TCP/IP.

Transport Layer

Layer 4 of the OSI reference model.

Triple DES

Triple DES (also 3DES) is a block cipher formed from the Data Encryption Standard (DES) cipher. There are several ways to use DES three times; not all are Triple-DES and not all are as secure. Triple-DES is defined as performing a DES encryption, then a DES decryption, and then a DES encryption again.

Twisted Pair Cable

The most common form of communication cabling used by telephones, computer terminals and LANs. A pair of wires, coated in a plastic sheath are twisted together. In most cases several pairs are then bound in a single sheath and then laid as a single cable using multiple twisted pairs.

VDU

Visual Display Unit.

Video Conferencing

A form of communication requiring very high capacity networks, which transmits pictures of all parties as well as voice.

Virtual Network

A form of network where communication and access is a achieved without any knowledge of the network structure or location of a specific resource.

VLAN

A virtual LAN, commonly known as a VLAN, is a logically segmented network mapped over physical hardware. IEEE 802.1Q is the predominant protocol.

WAN

Wide Area Network. A network which uses public or private circuits to link terminals, PCs and computers over long distances that also often allows some user choice in destination. Followings the implementation of routers, bridges and gateways many LANs are becoming Wide Area Networks, but more typically networks such as X.25 are classed as WANs.

X.400

An Application Layer OSI standard for transferring electronic mail on a store and forward basis between different machines.

XNS

Xerox Networking Systems. An Ethernet network produced by the Xerox Corporation.

Yellow cable

A co-axial cable, often referred to as “Thick” coax. This was the first cable used on many early LANs.

SUMMARY OF STANDARDS AND RECOMMENDATIONS

IEEE

802.1 Network Management
This standard conforms to the OSI network management model.

802.1d The spanning tree network protocol provides a loop free topology for any LAN or bridged network. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1D

802.1Q Defines the meaning of a virtual LAN or VLAN with respect to the specific conceptual model underpinning bridging at the MAC layer and to the IEEE 802.1D spanning tree protocol.

802.2 Logical link Control

802.3 Carrier Sense Multiple Access with Collision Detect (CSMA/CD) – Commonly known as Ethernet.

802.4 Token Bus –combines the bus structure of Ethernet Type and the token passing system in the token ring.

802.5 Token Ring – is based on a closed loop, philosophy, and runs at 4Mbps or 16Mbps.

802.11a Wireless LAN operating at 54 Mbps (Net 20 Mbps) using 5Ghz

802.11b Wireless LAN operating at 11 Mbps using 2.4ghz

802.11g Wireless LAN operating at 54 Mbps (Net 24.7 Mbps) using 2.4ghz

802.1X Is an IEEE standard for port-based network access control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. It is often used for wireless access points, and is based on the EAP, Extensible Authentication Protocol

ISO

646 Information Processing System OSI Seven Bit Coded Character Set for Information Interchange

2022 Information Processing System OSI Seven Bit and Eight Bit Coded Character Sets. Code Extension Techniques.

2375 Data Processing Procedure for registration of Escape Sequences.

4873 Information Processing Systems OSI Eight Bit Code for Information Interchange Structure and Rules for Implementation.

6429 Information Processing Systems OSI Seven Bit and Eight Bit Coded Character Sets. Additional Control Functions for Character Imaging Devices.

7498 Information Processing Systems OSI Basic Reference

7498 AD1 Information Processing Systems OSI Basic Reference Model. Addendum 1: Data Processing Connectionless Mode Transmission.

7498-2 Information Processing System OSI Basic Reference Model, Part2: Security Architecture.

7498-3 Information Processing System OSI Basic Reference Model, Part3: Naming and Addressing

8072 Information Processing Systems OSI Transport Service Definition

8073 Information Processing Systems OSI Connection Oriented Transport Protocol Specification

8073 DAD1 Information Processing Systems OSI Connection Oriented Transport Protocol Specification Addendum 1: Network Connection Management Sub protocol

8208 Information Processing System Data Communications Interface between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DTE) for a Terminal Operating in the Packet Mode on Public Data Network.

8326 Information Processing Systems OSI Basic Connection Oriented Session Service Definition.

8326 DAD1 Information Processing Systems OSI Basic Connection Oriented Session Service Definition Addendum 1: Session Symmetric Synchronisation Protocol

8326 DAD2 Information Processing Systems OSI Basic Connection Oriented Session Service Definition Addendum 2: Incorporation of unlimited user data.

8327 Information Processing Systems OSI Basic Connection Oriented Session Protocol Specification.

8327 DAD1 Information Processing System OSI Basic Connection Oriented Session Protocol Specification. Addendum 1: Sessions Symmetric Synchronisation for the Session Protocol

8327 DAD2 Information Processing Systems OSI Basic Connection Oriented Session Protocol Specification. Addendum 2: Incorporation of unlimited user data.

8348 Information Processing Systems Data Communication Network Service Definition

8348 AD1 Information Processing Systems Data Communication Addendum to Network Service Definition covering Connectionless Mode Transmission

8348 Information Processing Systems Data Communication Addendum to Network

AD2 Service Definition covering Network Layer Addressing

8348 DAD3 Information Processing Systems Data Communication Additional features of the Network Service.

8473 Information Processing Systems Data Communication for providing the Connectionless Mode Network Service.

8505 Information Processing Systems Text Communication Functional Description and Service Specification for Message Oriented Text Interchange Systems

8571 Information Processing Systems OSI File Transfer Access and Management (FTAM). Part 1: General Introduction. Part 2: The Virtual File Store. Part 3: The File Service Definition. Part 4: The File protocol Specification.

8602 Information Processing Systems OSI Protocol for providing the Connectionless Mode Transport Service.

8648 Information Processing Systems OSI Internal Organisation of the Network Layer

8649-2 Information Processing Systems OSI Service Definition for Common Application Service Elements. Part 2: Association Protocol.

8650-2 Information Processing Systems OSI Service Definition for Common Application Service Elements. Part 2: Association Control.

8802 Information Processing Systems Local Area Networks Logical Link Control (LLC)

8802-3 Information Processing Systems Local Area Networks Carrier Sense Multiple Access with Collision Detect (CSMA/CD) (See IEEE 802.3)

8802-4 Processing Systems Local Area Networks Token Bus (See IEEE 802.4)

8802-5 Processing Systems Local Area Networks Token Ring (See IEEE 802.5)

8821 Information Processing Systems OSI Specification of Basic Encoding Rules for Abstract Syntax Notation One (ANS.I)

8822 Information Processing Systems OSI Connection Oriented Presentation Service Definition.

8823 Information Processing Systems OSI Connection Oriented Presentation Protocol Specification.

8824 Information Processing Systems OSI Specification of Abstract Syntax Notation One (ANS.I)

8831 Information Processing Systems OSI Job Transfer and Manipulation Concepts and Services.

8832 Information Processing Systems OSI Specification of Basic Class Protocol for Job Transfer and Manipulation.

8859 Information Processing Systems Eight Bit Single Byte Coded Graphics Character Sets. Part 3. Latin Alphabet No 3. Part 4: Latin Alphabet No 4.

8878 Information Processing System Data Communication Use of X.25 to provide the OSI Connection Mode Network Service.

8880-1 Information Processing Systems Protocol Combinations to provide and support the OSI Network Service. Part 1: General Principals.

8880-2 Information Processing Systems Protocol Combinations to provide and support the OSI Network Service. Part 2: Provision and Support of the Connection Mode Network Service.

8880-3 Information Processing Systems Protocol Combinations to provide and support the OSI Network Service. Part 3: Provision and support of the Connectionless Mode Network Service.

8881 Information Processing Systems Data Communication Use of X.25 Packet Level Protocol in Local Area Networks.

8883 Information Processing System Text Communication Message Oriented Text Interchange System, Message Transfer Sub layer, Message Interchange Service and Message Transfer protocol.

8886 Information Processing Systems Data Communication Data Link Service Definition for OSI.

9040 Information Processing Systems OSI Virtual Terminal Service Basic Class.

9041 Information Processing Systems OSI Virtual Terminal Protocol Basic Class.

9542 Information Processing Systems Data Communication End System to Intermediate System Routing Exchange Protocol for use in conjunction with the Protocol for the provision of the Connectionless Mode Network Service.

BIBLIOGRAPHY

The Pocket Book of Computer Communications

A General guide to the principles and techniques of data communications, assuming a minimum of prior knowledge. Originally published in 1976, this pocket book is probably one of the most successful reference guides ever produced with more than a million copies circulated in many different languages.

This book is now somewhat dated but the principles still apply. An updated version will be produced in the not too distant future.

Available from Case Communications.

The Pocket Book of OSI

This book introduces the reader to the concepts and jargon on Open Systems Interconnection, again assuming very little prior knowledge.

First published in 1990 – available from Case Communications.

Introduction to Data Communications and LAN technology

An introduction to datacomms for the non technical. It covers all the basics of communications networks as well as LANs. A number of case studies are included as illustrations.

Ed da Silva

Local Area Networking with Micro Computers

This book, sub-titled 'A guide for the business decision-maker' is intended as a guide to the selection, use and management of local area networks. The book ranges from the reasoning behind LANs to network topology, standards and security.

Stevanne Ruth Lehrman.

Communications with the IBM PC Series

A Wide ranging reference book on communications for IBM PC and compatibles. It extends to all forms of communication network types but covers LANs in some detail. Practical examples are also used to illustrate different communications options.

Gilbert Held.

Low Cost Local Area Networks

A guide to the selection and implementations of a LAN. Technology, standards and functionality are covered plus methods for analysing users requirements and purchase criteria. The pros and cons of several proprietary networks are also discussed, plus LAN trends.

Stephen Bridges.

Local Area Network and their Applications

A detailed technical book aimed at the communications student or network designer. An in-depth study of all the main techniques and technology is included centring on Ethernet and IBM Token Ring.

Brendan Tangney and Donal O'Mahony published 1988.

Local Area Networks: Architectures and Implementations

A review of the concepts and standards underpinning LAN technology. Several implementations are discussed highlighting implementation of formal standards and de-facto standards. This is a good book for students or network designers, covering the subject in some detail.

James martin – published 1989.

Mapping the 802.11 Protocol

As part of the release of the second edition of *802.11 Wireless Networks: The Definitive Guide*, this guide provides a visual map of the relationship between the various components of the 802.11 standard and related security standards. The authors learning style is visual, so he tends to draw out diagrams to fit complex relationships together.
by Matthew Gast, author of 802.11

Wireless Networks: The Definitive Guide, 2nd Edition

Web references

http://en.wikipedia.org

http://standards.ieee.org

http://www.wildpackets.com

http://www.tutorial-reports.com