

NETWORKING ABBREVIATED

By Mark E. Donaldson

TERMINOLOGY

Protocol - The predefined manner or set of rules by which a function or service is performed.

Standard - Defined by rules and written specifications.

Topology - The physical layout of a network.

Connectivity - Allows hardware and software products to be connected and form a unified networking system.

Architecture - Combines the existing standards, protocols, and topologies needed to create a functioning network. The network defined by the combination of standards, protocols, and topologies is called the network architecture.

A network architecture can be broken into layers, with each layer responsible for a certain task. When these tasks are combined, the result is a service performed by the network. Each layer can communicate with the layer above and the layer below it. Protocols define how this communication between layers occurs. As each layer completes its function, it passes data and control of the service to the layer immediately above or below it.

The layering of protocols to create network architectures is a basic principle of standards based networking. All networks are built on layers of protocols, and these layers are the building blocks used by standards organizations to create network architectures. A network architecture, is therefore, also a standard as it defines the rules of a network and how its components interact.

BASIC COMPONENTS

Hardware

- File Server
- Workstation
- Cabling
- Network Interface Cards (NICs)
- Hub, concentrator or wiring center.

Software

- Network Operating System (NOS)
- Operating System for Workstation
- Workstation Network shell, requester, or redirector

THE OSI MODEL

NETWORKING ABBREVIATED

By Mark E. Donaldson

The OSI (Open Systems Interconnect) Model describes a network architecture that connects dissimilar devices. OSI is concerned with the interconnection between systems, the way they exchange information, rather than the internal functions of particular systems. The OSI Model has a protocol layered structure with seven functional levels.

The Physical Layer transmits bit streams across a particular physical transmission medium. It involves a connection between two or more machines that exchange electrical signals. This is the nuts and bolts layer. Here is where the cable, connector, and signaling specifications are defined.

The Data Link Layer provides reliable data transmission from one node to another and shields the higher layers from concern for the physical transmission medium. It is responsible for the error free transmission of frames of data. This layer is subdivided into the **Media Access Control (MAC) Layer** and the **Logical Link Control (LLC) Layer**. This layer deals with getting data packets on and off the wire, error detection and correction, and retransmission. The LLC, the upper half, does the error checking, and the MAC, on the lower half, deals with getting the data on and off the wire.

The Network Layer routes data from one network node to another. It establishes, maintains, and terminates the network connection between two users and transfers data along that connection. It also does fragmentation and reassemble. This layer makes certain that a packet sent from one device to another actually gets there in a reasonable period of time. Routing and flow control are performed here. This is the lowest layer of the OSI model that can remain ignorant of the physical network.

The Transport Layer provides data transfer between two users at an agreed upon level of quality. When a connection is established between two nodes, this layer selects a particular class of service. That class monitors transmissions to ensure that the appropriate level of quality is maintained and notifies users when transmission quality falls below level. This layer makes sure the lower three layers are doing their job correctly, and provides a transparent, logical data stream between the end user and the network service being used. This is the lower layer that provides local user services.

The Session Layer provides the services necessary to organize and synchronize the dialog that occurs between users and to manage the data exchange. This layer is primarily concerned with controlling when users can send and receive data, based on whether they can send or receive concurrently or alternately. Communications between applications across a network is controlled at this layer. Testing for out-of-sequence packets and two-way communications are managed here.

The Presentation Layer is responsible for presenting information to network users in a meaningful way. This may include character code translation, data conversion, or data compression and expansion. Differences in data representation are dealt with at this level.

NETWORKING ABBREVIATED

By Mark E. Donaldson

For example, UNIX style line endings (CR only) might be converted to MS-DOS style (CRLF), or EBCDIC to ASCII character sets.

The Application Layer lets application processes access the system interconnection facilities to exchange information, including services used to establish and terminate connections between users. It is also used to monitor and manage the interconnected systems and the various resources they use. This is where the user applications software lies. Such issues as file access and transfer, virtual terminal emulation, interprocess communication, and the like are managed here.

NETWORKING ABBREVIATED

By Mark E. Donaldson

OSI MODEL				
Layer		Associated Protocols	Connectivity Devices	Top
7	APPLICATION	X.400 X.500 Shell Redirector		
6	PRESENTATION	RFS SMB NCP NFS		
5	SESSION	TCP IPX NetBIOS FTP/Telnet SMTP TFTP RPC SNMP		
4	TRANSPORT	TCP UDP SPX/IPX	Gateway (Router)	
3	NETWORK	IP IPX ICMP X.25	Router	
2b	DATA LINK - LLC	IEEE 802.2 ODI LABP NDIS		
2a	DATA LINK - MAC	IEEE 802.3 IEEE 802.5 CSMA/CD Token	Switch Bridge	
1	PHYSICAL	IEEE 802.3 IEEE 802.4 IEEE 802.5 RS-232 RS-449 V.35 Topologies	Repeater Transceiver MAU Hub NIC Cabling	

TCP/IP NETWORK CLASSIFICATION & ADDRESSING

NETWORKING ABBREVIATED

By Mark E. Donaldson

There are four different network classifications for IP networks: **A - B - C - D**. They are distinguished by their addressing conventions. All addresses consist of four (4), eight (8) bit header units, or **octets**. The number of network allotted for each classification is dependent upon the number of octets allotted per header. Total number of networks in each class is determined by number of number combinations. They shift upward as the network class decreases.

CLASS A

Bits (1)			= (32) Bits
0	(7) Network Address	(24) Local (Host) Address	
1 to 127	126	16,777,124	

CLASS B

Bits (2)			= (32) Bits
10	(14) Network Address	(16) Local (Host) Address	
128 to 191	16,384	65,534	

CLASS C

Bits (3)			= (32) Bits
110	(21) Network Address	(8) Local (Host) Address	
192 to 223	2,097,152	256	

CLASS D

Bits (4)			= (32) Bits
1110	(28) Network Address		
	?		
	Local (Host) Address		
224 to 264			

CONNECTIVITY

REPEATER - A device which propagates electrical signals from one cable to another without making routing decisions or providing packet filtering. In OSI terminology, a **repeater is a Physical Layer** intermediate system. While a repeater is not used to interconnect different networks, it does connect segments of the same network to form an extended network. Its purpose is to receive a signal and regenerate it or strengthen that signal extending the

NETWORKING ABBREVIATED

By Mark E. Donaldson

cabling distance limits placed on the network by the architecture. When a repeater is used, it must connect to networks of the same architecture type, using the same protocols, media access scheme, and transmission technique. The repeater counts as one node on each trunk segment it connects.

A repeater receives and then immediately retransmits each bit. It has no memory and does not depend on any particular protocol. It duplicates everything, including collisions.

TRANSCEIVER - Transmitter-Receiver. The physical device that connects a host interface to a local area network, such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and sense collisions.

BRIDGE - A device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are repeaters, which simply forward electrical signals from one cable to another, and full fledged routers, which make routing decisions based on several criteria. In OSI terminology, a bridge is a Data Link Layer intermediate system.

A bridge receives the entire message into memory. If the message was damaged by a collision or noise, or if the bridge knows that the message was being sent between two stations on the same cable, then it discards it. Otherwise the message is queued up and will be transmitted on another cable. The bridge has no address and its actions are transparent to the client and server.

A bridge connects disparate networks. The bridge functions at the **Data Link Layer** of the OSI model. Bridges read only the station address of each Ethernet Packet or Token Ring frame and then pass it on to its destination. **Install a bridge if you need to interconnect LANs that are running the same protocols, or isolate certain network traffic. Since a bridge does less to data than a Router, it's frequently faster for local traffic within the same LAN protocol.** It functions as a device on its own but also belongs to the networks it joins. A bridge can either be **local** or **remote**.

Local Bridges connect two similar networks in the same geographical area. It takes packets from one network and places them on another network, then takes packets from the

second network and places them on the first network. Each time the bridge swaps packets between networks, it also functions as a repeater regenerating the signal. Of course, a bridge does more than just regenerate the signal. It can examine the packet header and decide and decide on which of the two networks the packet belongs. This process is known as filtering. Basically the bridge receives all packets on the networks it is connected to and looks at the source and destination addresses of each packet. By preventing a packet from crossing the bridge and moving into the LAN it is not destined for, the bridge decreases the excess traffic on the LAN.

NETWORKING ABBREVIATED

By Mark E. Donaldson

As packets pass through the bridge, it stores the addresses of nodes communicating through it, determining which addresses are on each section of the LAN. Through the learning process, the bridge builds a table containing the addresses of all the nodes on the networks. Each time the bridge filters a packet, it checks the address table against the node address of the packet. If they don't match, the bridge stores the address and forwards the packet. This process is known as **storing and forwarding**. When some bridges, known as **learning bridges**, are attached to an Ethernet network, they immediately send broadcasts asking all the stations on the local network segment to respond. As the stations return the broadcast, the bridge builds a table of local addresses. As nodes are added to the network, it continues to gather node addresses. Bridges that require someone to enter all the node addresses into the bridge are known as **static bridges**.

Multiple bridges can be used, but in such cases the bridge must know all the stations it can reach, not just the stations on the networks to which it is directly connected. When multiple bridges are used, only one path can connect any two networks or duplicate messages may be created, or messages could arrive out of sequence.

In the context of bridging, the term routing refers to the path the packet will travel. This term has no connection with the interconnectivity device called a router. The type of routing used by bridges is called **transparent routing**. Not only are the bridges unaware of the route the packet will take, the packet itself doesn't know the route it will travel. **Source routing** is another type of routing used by bridges, primarily in IBM Token Ring networks. With source routing, the packet itself contains routing information specifying the networks and bridges through which it will travel to its destination. The sending node is responsible for putting this information onto the packet. It determines the various routes available through the process of **route discovery**. Source routing does add some overhead to the network, but its benefits more than make up for it. Another of those benefits is that it can aid in network communication management. Since each node specifies the route, its packet will follow, it can always choose the most efficient path at the time of transmission. Source routing bridges can also be faster than transparent routing bridges because they have to read only the destination information rather than each packet in its entirety.

Bridges are protocol independent. In other words, the bridge doesn't care what protocol is used on either LAN. It treats TCP/IP, SPX/IPX, and other communication protocols equally. The bridge receives packets and either transmits them or ignores them without concern for protocols. The bridge does not translate the packet, but they may be implemented to facilitate the connection of different media types.

Remote Bridges connect two LANs that aren't in the same geographical area. Usually, some type of telecommunications link, such as a telephone line or satellite transmission, is needed to connect remote LAN's. A bridge at one end of the telecommunications link puts packets destined for the other LAN out onto the link. A bridge at the other end of the link receives these packets and passes them on to its LAN. This process works in both

NETWORKING ABBREVIATED

By Mark E. Donaldson

directions. All the other facets of bridges remain the same for remote bridges. The only difference is the telecommunications link.

SWITCH - A switch is essentially a multiport bridge. It operates on OSI level 2 media access control (MAC) level. The switch filters between the port addresses of the switch. Each port on a switch is the entrance to a segment on the network, and each segment has the address of its associated port on the switch. A switch is basically a more sophisticated way of bridging a network. However, they have many advantages. They usually have a high speed backplane that can support a very high rate of throughput. Usually it is the number of paths through the switch multiplied by the throughput of each path. If there are eight paths through the switch, the backbone of the switch can accommodate 80 Mbps of throughput. There are switches available whether the port gives a node a dedicated collision free line. The device attached to this port does not share an address with any other device for this port. It is a dedicated port to that device.

An Ethernet switch provides a different solution for LAN congestion and bottlenecking. The speed of the network is not increased by increased bandwidth, rather it decreases the number of users on a segment and instead of five users fighting for 10 Mbps of bandwidth, one user has a full 10 Mbps. A port on an Ethernet Switch can be connected to a single user as a dedicated port or to a shared segment that serves many users.

The 10 Mbps Ethernet Switch is similar to a MAC Layer bridge that receives Ethernet packets, reads the destination address, and sends it out on the port where the destination device resides. They are much faster than the bridge though. Ethernet Switches use either **Cut Through** or **Store and Forward architectures** to switch an Ethernet packet from one port to another. Cut Through switches are faster, but will circulate bad packets that cause bottlenecks during heavy traffic. Store and Forward Switches buffer the incoming packet first, making sure it is good, and then send it on its way. A Store and Forward Switch generally has a higher latency than a Cut Through Switch. Ethernet Switches are more expensive than 100 Mbps shared hubs.

A Token Ring Switch may be used to break a single ring into smaller segments. A very large ring is often slow, especially if the whole ring is restricted to 4 Mbps. A Token Ring Switch can segment a large ring into two or more smaller rings, increasing throughput to all workstations. To reduce backbone congestion and increase throughput dramatically, a single Token Ring Switch can replace both the bridges and the backbone connecting the rings.

ROUTER - A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this **it uses a routing protocol to gain information about the network**, and algorithms to choose the best route based on several criteria known as routing metrics. In OSI terminology, **a router is a Network Layer** intermediate system.

A Router is more sophisticated than a bridge in terms of their data handling capability. A Router looks deeper within the Ethernet Packet or Token Ring Frame to read the NetBIOS,

NETWORKING ABBREVIATED

By Mark E. Donaldson

IPX, or TCP/IP address. It checks the address against its internal tables for the best way to send the packet or frame to the next Router or the destination network. The Router then strips off the outer layer of the packet and repackages it with a new outer layer for its final network address. Because of this sophisticated data handling ability, routers, unlike bridges, can be used to link networks using different protocols, such as from Ethernet to Token Ring. Because the Router examines the entire packet, errors aren't passed on to the next LAN. Because it rebuilds data into packets or frames appropriate to their final destination, a Router sends very few bits on to the next LAN. This can be an important savings when data is being transferred over expensive leased lines.

A Router acts as an agent to receive and forward messages. The router has an address and is known to the client or server machines. Typically, machines directly send messages to each other when they are on the same cable, and they send the router messages addressed to another zone, department, or subnetwork. Routing is a function specific to each protocol. For IPX, the Novell server can act as a router. For SNA, an APPN Network Node does the routing. TCP/IP can be routed by dedicated routers, UNIX workstations, or OS/2 servers.

Since the router is functioning at the Network Layer, **the communication protocols on both sides of the router must be the same** and must be compatible at higher network layers. The first two OSI Layers may differ without affecting routing. The router is used to pass a message through intermediate nodes. This approach doesn't work well with a single LAN because a transmitted message is sent to all the nodes on that network and receiving node determines from the destination address whether or not it should accept the message and process it. However, when a LAN is connected with other LANs or on a wide area network, the issue of routing becomes more important. With other types of networks, particularly the wide area network, a message is ordinarily sent from one node to another specific node on the network rather than to every node. However, it may pass through a

series of intermediate nodes before arriving at the destination. A message usually also has more than one path or route available to it, thus, there are various paths to choose from when one node sends a message to another. When a message is routed through intermediate nodes, it must contain two addresses, the destination address, which remains constant, and the address of the next node along the route. The latter address changes as new nodes are encountered, until the message finally arrives at the destination node. A route is itself an intermediate system or node. Multiple routers can also be used. They can be connected in a manner that allows for multiple paths or routes between any two networks. Since messages are sent to a specific route node, the existence of multiple paths will not cause the message to be duplicated.

The function of a Router is to determine the next node to receive the message. Two methods are used to do this. Routing information can be defined when the network is designed, then stored in routing tables that are placed manually within routers. Or source routing can be used. Whichever approach is used, a network map is developed for the routers.

NETWORKING ABBREVIATED

By Mark E. Donaldson

GATEWAY - The original Internet term for what is **now called route** or more precisely, IP Route. In modern usage, the terms gateway and application gateway refer to systems which do translations from some native format to another. Examples include x.400 to/from RFC 822 electronic mail gateways.

Gateways are used to connect networks that may have entirely different architectures. Gateways offer the greatest degree of flexibility in network connectivity, but for the developers who must develop the conversion software, they are very complex.

BACKBONE - The backbone network may be used to connect different networks. Users are not directly connected to the backbone network, but instead have their own LAN. The network on which the users are connected is called the **access network**.

Using a backbone to connect several smaller access networks has its advantages over using one large network. Each LAN can continue to operate should one of the other access networks fail. Individual LANs are easier to administer than one large LAN. Because the backbone can do the filtering, only traffic that is meant for other networks needs to pass over the backbone.

A backbone network requires a large bandwidth and should be able to transmit over long distances. Because fiber optics are usually used for these networks, the backbone is often designed as an FDDI network. FDDI networks have a transfer speed of 100 Mbits/sec and are very reliable and secure. Access may require a bridge, route, or gateway to attach to the backbone, depending on the architectures of the various access LANs and the backbone itself.

NETWORKING ABBREVIATED

By Mark E. Donaldson

TOPOLOGIES

- **Star**
- **Ring**
- **Linear Bus**
- **Star Wired**
- **Tree**

OPERATING SYSTEMS

Novell

- NetWare 2.2
- NetWare 3.11
- NetWare 4.1

IBM

- LAN Server 4.0
- OS/2 Warp Connect

Microsoft

- LAN Manager
- Windows 95
- Windows NT
- Windows for Workgroups

Banyan VINES

UNIX

LANtastic

TRANSPORT/COMMUNICATION PROTOCOLS

NetBIOS - Network Basic Input/Output System. A software interface or protocol developed by IBM for network communication. A NetBIOS interface is a programming interface that allows I/O requests to be sent and received from a remote computer. It hides networking hardware from applications. This protocol operates at the network and transport layers, and sometimes at the session layer, of the OSI Model.

IPX/SPX - Internet Packet Exchange/Sequenced Packet Exchange. Transport and communications protocols used in Novell NetWare and other networks. Part of the series of protocols known as **XNS (Xerox Network Systems)**. For Windows 95, the NWLINK.VXD module is used to implement the IPX/SPX compatible protocol. **IPX - Internet Packet Exchange** is the NetWare protocol for the exchange of message packets on an interwork.

NETWORKING ABBREVIATED

By Mark E. Donaldson

IPX passes application requests for network services to the network drives and then to other workstations, servers, or devices on the interwork. **SPX - Sequenced Packet Exchange.** Is a NetWare protocol by which two workstations or applications communicate across the network. SPX uses IPX to deliver the messages, but SPX guarantees delivery of the messages and maintains the order of messages on the packet stream.

XNS - Xerox Network Systems. A suite of protocols developed by Xerox and used by Novell that operate at the network and transport layers, and sometimes at the session layer, of the OSI Model. **IPX (Internet Packet Exchange)** and **SPX (Sequence Packet Exchange)** are parts of XNS

TCP/IP - Transmission Control Protocol/Internet Protocol. A set of routing protocols developed by the Department of Defense as part of the work done on **ARPANET**. The primary wide area network (WAN) transport protocol used to communicate with computers on TCP/IP networks, and to participate in UNIX based bulletin boards and electronic mail services. This suite of protocols operate at the network and transport layers, and sometimes at the session layer, of the OSI Model.

IP - Internet Protocol. The Internet standard protocol that defines the Internet datagram as the unit of information passed across the Internet. Provides the basis for the Internet connectionless best effort packet delivery service. The Internet protocol suite is often referred to as TCP/IP because IP is one of the two fundamental protocols.

PHYSICAL & CONNECTIVITY STANDARDS & PROTOCOLS

IEEE Project 802

802.1 - An overview of the work of the project defining the LAN references model. It also addresses such issues as formats, networks management, and internetworking.

802.2 - Describes the LLC services and primitives to be used in all IEEE specified LANs.

802.3- Defines standards for the MAC and physical layers for a CSMA/CD based bus network.

802.4 - Defines standards for the MAC and physical layers for a baseband token passing bus network.

802.5 - Defines standards for the MAC and physical layers for a baseband token passing ring network.

802.7 - A TAG concerned with broadband networks. It advises the other groups on issues related to broadband transmission.

802.8 - A TAG concerned with fiber optics exploring ways in which fiber optic technology can contribute to the other groups.

NETWORKING ABBREVIATED

By Mark E. Donaldson

CCITT

X.25 - A standard protocol for communication over wide area networks. Mostly used in Europe.

X.400 Message Handling Service (**MHS**).

X.400 A standard protocol for message exchange in electronic mail. System model and service elements.

X.401 Basic service elements and optional user interfaces.

X.408 Encoding information and conversion rules.

X.409 Presentation transfer syntax and notation.

X.410 Remote operations and reliable transfer system.

X.411 Message transfer layer.

X.420 Interpersonal messaging user agent layer.

X.430 Access protocols for teletex terminals.

X.500 A standard for governing worldwide directories for electronic mail.

SNMP

The protocol that allows communication between the console, or **Network Management Station (NMS)**, the network administrator uses and a network device. SNMP allows administrators to monitor and analyze networks and isolate faults. The agent devices have software that places messages into the SNMP protocol. SNMP is actually a protocol suite consisting of three the three specifications, RFC1157 (the SNMP), RFC1156 and RFC1158 (the **management information base**, or **MIB**), and RFC1155 (the **structure of management information**, or **SMI**).

SNMP is the standard for LAN management, particularly in mission critical applications. The **Internet Engineering Task Force (IETF)** governs the SNMP standard. In evaluating network management systems, SNMP compliance has emerged as a crucial factor. SNMP was designed to manage network configuration, performance, faults,, accounting, and security. An SNMP agent must be present at the device level (a route or hub, for example), either built into the unit or as a proxy agent, and is accessed through a remote terminal. SNMP does not follow a polling protocol. It waits to receive data from the remote device. Or it sends data based on operator commands. By using one common set of standards, SNMP allows network administrators to manage, monitor, and control their SNMP compliant network equipment with in management system, and from one management station. If a network device goes down, it's possible to both pinpoint and troubleshoot the problem more efficiently. And a network administrator isn't" limited to equipment from just one vendor when using an SNMP program. However, it is critical that the multivendor equipment fully complies with the SNMP standard for complete network management.

RFC 1157 - The SNMP.

RFC 1156 and 1158 - The Management Information Base (**MIB**).

Revised November 29, 2008

Page 13 of 26

NETWORKING ABBREVIATED

By Mark E. Donaldson

RFC 1155 - The Structure of Management Information (SMB)

DIX (Xerox Standard)

An older, yet refined Ethernet technology often referred to as Ethernet II, developed by Xerox, Intel, and Digital. The earliest versions of Ethernet were developed by Xerox. All DIX standards are controlled by Xerox exclusively. The Ethernet as we know it now is determined by IEEE 802. Standards.

ARCHITECTURES

Ethernet (Types)

See below.

FDDI - Fiber Distributed Data Interface. Network architecture designed to meet the requirements of high speed individual networks and high speed connections between individual networks. The FDDI standard was developed primarily to handle the requirements of back end local networks, high speed office networks, and backbone local networks. The underlying medium is fiber optics, and the topology is a dual attached, counter rotating Token Ring. FDDI networks can often be spotted by the orange fiber cable.

TOKEN RING

Token Ring is a sophisticated LAN technology endorsed by IBM and defined by the IEEE 802.5 standard. Token Ring uses a star wired topology in which all workstations connect to a central Multistation Access Unit (MAU). This makes moving, changing, and adding equipment quick and easy. It's fault tolerant. If, for example, the cable to a networked PC is

damaged or cut, the MAY will automatically bypass that port. Because the logical ring stays intact, the network stays up.

Token Ring is also easy to connect to a mainframe. It can be plugged directly into an IBM AS/400 or 3174 controller (added workstation software or a gateway may be necessary). The Token Ring network topology offers a high speed with up to 16 Mbps. With shielded twisted pair cable, 260 devices can be connected to a local Token Ring network. With unshielded twisted pair cable (Category 3, 4, or 5), the limit is 72 devices.

Type 1 Token Ring networks use Type 1 Token Ring cable (shielded twisted pair) with IBM style universal data connectors, which give greater distances with passive devices. Type 1 also supports greater speeds (16 Mbps), with fewer problems on the network.

Type 3 Token Ring networks use Category 3, 4, or 5 unshielded twisted pair cable with easy to use modular connections. Type 3 cabling is more flexible. It is generally already installed in most buildings. Because the cable is not shielded, less distance is attainable and more network problems occur. Both Type 1 and Type 3 networks can operate at 4 or 16 Mbps.

NETWORKING ABBREVIATED

By Mark E. Donaldson

Token Ring Switching is an inexpensive PnP technology. To take advantage of Token Ring Switching, only one new piece of equipment needs to be added, a Token Ring Switch. Just install a switch in place of a Token Ring MAU or Bridge. Networks speeds can be increased dramatically with Token Ring Switching. Each new LAN segment can now have a dedicated 16 Mbps connection to the switch port. If a workstation needs maximum LAN throughput, it is possible to have only one workstation on each segment, giving each workstation a dedicated 16 Mbps connection to the server. Servers installed with 16/32 Token Ring Adapters can achieve speeds of up to 32 Mbps, receiving 16 Mbps data from one segment while sending 16 Mbps data to another segment. A Token Ring Switch may be used to break a single ring into smaller segments. A very large ring is often slow, especially if the whole ring is restricted to 4 Mbps. A Token Ring Switch can segment a large ring into two or more smaller rings, increasing throughput to all workstations. To reduce backbone congestion and increase throughput dramatically, a single Token Ring Switch can replace both the bridges and the backbone connecting the rings.

FAST ETHERNET 100BASE-T (IEEE 802.3u)

100BASE-T retains the familiar CSMA/CD media access technique used in 10-Mbps Ethernet networks. It also supports a broad range of cabling options: two standards for twisted pair, one for fiber. 100BASE-TX supports 2-pair Category 5 UTP or Type 1 STP cable. 100BASE-T4 uses 4-pair Category 3 or 4 cable. And 100BASE-FX allows fiber optic links via duplex multimode fiber cable. It retains CSMA/CD so existing network management systems don't need to be rewritten. It can easily be integrated into existing 10 Mbps

Ethernet LANs so your previous investment is saved. 100BASE-T also carries data, voice, and video at up to 100 Mbps. Supports CSMA/CD protocol so you can use your existing networking software. Operates over inexpensive Unshielded Twisted-Pair (UTP) cabling. Can be implemented gradually as 10/100-Mbps adapters and hubs where 10- or 100-Mbps bandwidth is software-selectable. Serves as a stepping stone to even faster technologies like ATM.

Fast Ethernet increases the bandwidth on a LAN tenfold. Fast Ethernet is also called 100Base-T because of the protocol operating on the cable, not the cable itself. Only one device at a time can transmit on a LAN, forcing the users to share the available bandwidth. So as traffic increases, the number of collisions increases, making the network less efficient. Increasing bandwidth reduces the number of collisions and bottlenecks.

100VGAnyLAN is a sometimes mistakenly called Fast Ethernet, but it does not have the same proven technology of 100Base-T, nor is it universally supported by vendors. 100Base-T was approved by the IEEE committee in June 14, 1995 as specification 802.3u. 100Base-T should use Category 5 cable. Network topology must be considered, but the basic CSMA/CD logic remains the same. Like standard 10 Mbps hubs, Fast Ethernet hubs perform collision detection, signal reshaping, and partitioning functions. A typical hub provides a maximum of 4 or more ports with RJ-45 connectors.

NETWORKING ABBREVIATED

By Mark E. Donaldson

SWITCHED ETHERNET

Switched Ethernet relies on centralized multiport Switches to provide a physical link between multiple LAN segments. Inside each intelligent Switch, high-speed circuitry supports wire-speed virtual connections between all the segments, for maximum bandwidth allocation on demand. Adding new segments to a Switch increases the aggregate network speed while reducing overall congestion, so Switched Ethernet provides superior configuration flexibility. It also gives you an excellent migration path from 10 to 100 Mbps Ethernet, since both segments can often operate via the same Switch. It is a cost-effective technique for increasing the overall network throughput and reducing congestion on a 10-Mbps network. Other than the addition of the switching hub, the Ethernet network remains the same—the same network interface cards, the same client software, the same LAN cabling.

An Ethernet switch provides a different solution for LAN congestion and bottlenecking. The speed of the network is not increased by increased bandwidth, rather it decreases the number of users on a segment and instead of five users fighting for 10 Mbps of bandwidth, one user has a full 10 Mbps. A port on an Ethernet Switch can be connected to a single user as a dedicated port or to a shared segment that serves many users.

The 10 Mbps Ethernet Switch is similar to a MAC Layer bridge that receives Ethernet packets, reads the destination address, and sends it out on the port where the destination

device resides. They are much faster than the bridge though. Ethernet Switches use either **Cut Through** or **Store and Forward architectures** to switch an Ethernet packet from one port to another. Cut Through switches are faster, but will circulate bad packets that cause bottlenecks during heavy traffic. Store and Forward Switches buffer the incoming packet first, making sure it is good, and then send it on its way. A Store and Forward Switch generally has a higher latency than a Cut Through Switch. Ethernet Switches are more expensive than 100 Mbps shared hubs.

Full Duplex Ethernet

Full Duplex Ethernet more than doubles the throughput of traditional half duplex Ethernet. It combines high speed LAN switching with the use of simultaneous Transmit and Receive over dedicated links. Because Full Duplex Ethernet uses two lines to send data in both directions at the same time, you get 20 Mbps transmission, twice the 10 Mbps speed of half duplex Ethernet. In addition, Full Duplex Ethernet doesn't have the collision problems of half duplex Ethernet, so you get better performance as well as higher speed. Standard Ethernet uses the CSMA/CD protocol to transfer data. Since a network can either transmit or receive data, a station wanting to transmit a packet first listens to the line to ensure that no other stations are transmitting on the same line. The station will only transmit if the line is free.

As on most Ethernet LANs, multiple stations are likely to attempt transmitting data at any given time. Collisions occur when two or more stations transmit at the same time. Collisions destroy data and are an indicator that there is not enough bandwidth to support the overall

NETWORKING ABBREVIATED

By Mark E. Donaldson

network demand. After every collision, the network resets, forcing the relevant nodes to retransmit at a latter time. The traditional half duplex transmission, that is in either direction but not both directions at the same time, tends to operate at only 40% to 60% of the potential 10 Mbps because of collisions. The network interface card is forced to deal with the collision, and this slows down the whole network. Full Duplex Ethernet uses entirely different lines for Transmit and Receive, doesn't experience collisions, and operates more efficiently. It can theoretically sustain a 100% network load at 20 Mbps. In practice, you can expect about a 20% increase in efficiency over half duplex Ethernet., though a 60% increase is possible in heavily loaded environments.

Full Duplex Ethernet is a point to point connection enabling two stations to send and receive (listen and transmit) data at the same time. A major benefit of Full Duplex Ethernet is that the only distance limitation is that of the attached transceiver.

ARCnet

ARCnet, **Attached Resource Computer Network**, was developed by Datapoint Corporation and has been a popular reliable LAN for years. Because of its popularity, standards existed for ARCnet even before IEEE Project 802 was established. The IEEE 802.4 specification, which defines token passing on a bus using broadband technology, is the standard most

similar to ARCnet. However, because ARCnet is a baseband network, it is very inexpensive and easy to install. ARCnet can have a star or bus topology. Often, however, it is considered to have a distributed star or tree topology. Manufacturers consistently follow ARCnet standards, and the products released for ARCnet networks are usually compatible with equipment from other vendors... Because it uses both passive and active hubs, ARCnet is excellent for elaborate wiring configurations.

100VG AnyLAN (IEEE 802.12)

Like Fast Ethernet (100BaseT), 100VG AnyLAN is a 100 Mbps throughput network. It does not have much support as Fast Ethernet, and is mostly championed by Hewlett-Packard. It was originally designed to serve as an upgrade from 16 Mbps Token Ring and Ethernet because it can carry both Token Ring and Ethernet packets. What really sets it apart from Fast Ethernet is the method of access it uses. Unlike Ethernet it uses a deterministic access method, referred to as **demand priority**. The hub scans each port in succession to transmit data. This avoids many of the collisions inherent to CSMA/CD. 100VG AnyLAN complies with the IEEE 802.12 specifications. A provision exists to implement isochronism, or the ability to send timing data, such as video. It can operate over four pair Category 3, 4, or 5 UTP cabling.

100VG AnyLAN uses an encoding scheme called Quartet Signaling to transmit data simultaneously over all four pairs in the network cable, so it achieves a full tenfold increase in transmission speeds over 10 BASE-T. It also replaces the CSMA/CD media access control protocol with Demand Priority to optimize network operation and eliminate the overhead of packet collisions and recovery. Demand Priority works like this: The hub directs all

NETWORKING ABBREVIATED

By Mark E. Donaldson

transmissions, acknowledging higher-priority packet requests before normal-priority requests. This effectively guarantees bandwidth to time sensitive applications like voice, video, and multimedia applications.

The benefits of 100VG AnyLAN are that It uses a transmission frequency very similar to traditional Ethernet, and works on any conventional cabling system (Category 3, 4, or 5 UTP, Type 1 STP, and fiber optics) and uses the same connectors. In addition, 100VG AnyLAN may soon support Token-Ring networks-a potential advantage over its rival standard 100BASE-T.

ATM

A versatile broadband network architecture capable of delivering in varying speeds. The original specification for ATM came from the **International Telecommunications Union (ITU)**, the organization whose standards address the worldwide telecommunications infrastructure. In the early 1980's the ITU defined **Integrated Services Digital Network (ISDN)**, which is now called N-ISDN for narrowband ISDN. N-ISDN had two access interfaces, or transfer rates (Basic 14.4 Kbps and Primary 1.544 Mbps). In the late 1980's,

the ITU further enhanced N-ISDN by bringing out the specifications for B-ISDN, or broadband ISDN. Unlike N-ISDN, B-ISDN offered much higher transmission rates, up to 622 Mbps. The signals generated by B-ISDN are carried by ATM. ATM transmits in what is known as a cell stream. A cell is a term for ATM broadband transmission that can be thought of as a predefined data packet. The data packet, or cell, is 48 bytes long with a 5 byte header for addressing.

Asynchronous Transfer Mode (ATM) is a cell-based fast-packet communication technique that supports data-transfer rates ranging from sub-T1 speeds (less than 1.544 Mbps) up to 10 Gbps. Like other packet-switching services (**Frame Relay, SMDS**), ATM achieves its high speeds in part by transmitting data in fixed-size cells, and dispensing with error-correction protocols. Instead, it relies on the inherent integrity of digital lines to ensure data integrity. ATM networks are extremely versatile. An ATM network can be treated as a single network, whether it connects points in a building or across the country. Its fixed-length cell-relay operation, the signaling technology of the future, offers more predictable performance than variable-length frames. And it can be integrated into an existing network as needed, without having to upgrade the entire LAN.

ISDN

ISDN, or **Integrated System (Services) Digital Network**. Is based on the CCITT model for the eventual integration of voice and data and a universal interface for networks. Transmits at the normal digital rate of 8,000 bytes per second according to phone company transmission standards as opposed to the 28,000 bits per second of a 28.8 modem.

T1

NETWORKING ABBREVIATED

By Mark E. Donaldson

T1 is a digital transmission method for multiplexing multiple voice and data channels over two pairs of wires. By using a technique called **Time Division Multiplexing (TDM)**, T1 interleaves both voice and/or LAN data across DSO subchannels. The primary benefit of T1 is bandwidth (1.544 Mbps) available in 24 allocated 64 Kbps DSO subchannels. T1 sends data in frames made up of 24 eight bit words (one word for each subchannel) and one framing bit for a total of 193 bits per frame. A T1 channel transmits 8000 frames per second. The framing bits on successive frames follow a pattern for a superframe format. The T1 Channel Bank checks this pattern to make sure synchronization is maintained.

T1 is the most flexible end to end digital service option available today. It's the preferred service for interconnecting voice, data, fax, and video signals across an enterprise network. T1 lines are used for high traffic, high bandwidth, and high speed connections are needed. Applications might be: High volume point to point data transfer. Accessing public frame relay networks or public switched telephone networks for voice and fax. Merging voice and data traffic - a single T1 line can give several additional voice and data lines at no additional cost. LAN connections. Bandwidth intensive data transfers such as CAD/CAM, MRI, CAR

scan images, and other graphics with large file sizes. Multiplexing lines from several locations onto one local T1 loop. T1 leased operate at 1544 Mbps, and are simple and reliable.

FRAME RELAY

Frame Relay is a type of packet based switching technology that has been streamlined for speed. It was developed to solve communication problems that other protocols could not, such as large bandwidth efficiency for clumping (bursty) traffic, lower protocol processing, and high speeds. Frame Relay provides a signal and data transfer mechanism between the endpoints, or sites, of a network. It allows many users to share bandwidth, creating instantaneous bandwidth on demand (bonding). It sends information in packets called frames. And each frame contains all the information necessary to route it to the correct destination. So in effect, each endpoint can communicate with many destinations over one access link to the network. And instead of being allocated a fixed amount of bandwidth, Frame Relay traffic gets full bandwidth for short (bursty) transmissions.

The Frame Relay network contains user devices and network devices. The sending user device delivers the frames to the network. The network reads the addressing information on the frames and routes them to the proper destination user devices. Frame Relay assumes that the data is error free,, which cuts out a time consuming step in the processing protocol. Therefore, the data travels much faster that it would have with other, older technologies. Any error correction is done by the user devices (PC's, routers, etc).

The benefits of Frame Relay are lower internetworking costs since you get multiple logical connections over a single physical connection. Equipment costs and access costs are also lower.. Frame Relay has better performance, more network access, and less network complexity.

NETWORKING ABBREVIATED

By Mark E. Donaldson

For additional information on Network Architectures, refer to *White Paper NETWORK ARCHITECTURES*.

LAN IMPLEMENTATION

Study Phase

- **Investigation and Analysis**
 - Collecting Background Information.
 - Defining the Problem.
 - Assessing User Requirements.
 - Identifying Resources and Constraints.

- **Feasibility Study**
 - Costs and Benefits.
 - Study Phase Report.

- **Install or Not**
 - Improved Efficiency.
 - Improved Control.
 - Improved Productivity.
 - Cost Savings.
 - Improved Service.

Selection and Design Phase

- Determine the degree of system security required.
- Determine the proper system management.
- Consult the users.
- Design procedures.
- Develop a chart showing information flow.
- Select the best topology.
- Select the appropriate transmission media.
- Evaluate the available software.
- Evaluate the available hardware.
- Create the most appropriate LAN.
- Prepare a design phase report.

Implementation Phase

NETWORKING ABBREVIATED

By Mark E. Donaldson

- Implementation plan.
- Computer program design.
- Review meeting.
- Equipment installation.
- Computer program development.
- System test.
- Software test.
- Manual development.
- Personnel training.
- Final review meeting.

Operation Phase

- **Changeover**
 - Cold conversion.
 - Parallel conversion.
 - Phased conversion.
- **Routine Operation**
 - Hardware maintenance.
 - Software maintenance
 - Programming maintenance.
- **System Performance Evaluation**
 - Cost analysis.
 - Ease of information retrieval.
 - Data integrity.
 - Personnel in contact with system.
 - Amount of data processed.
 - Security.
 - Maintenance.

DESIGNING AN ETHERNET LAN

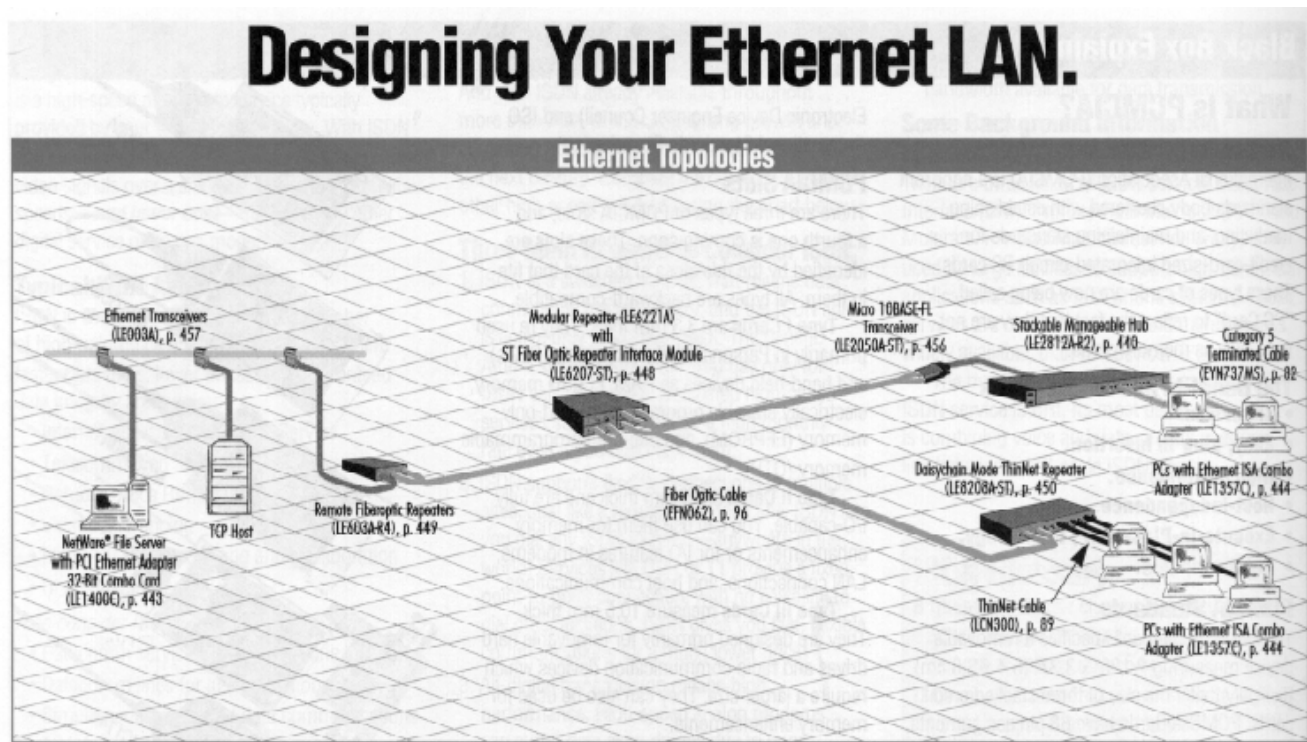
Ethernet is the most widely used network topology. You can choose between bus and star topologies, and coaxial, twisted-pair, or fiber cabling. But with the right connective equipment multiple Ethernet-based LANs (local networks) can be linked together no matter topology and/or cabling system they use. In fact with the right equipment and software, Token Ring, AppleTalk, and wireless LANs can be connected to Ethernet.

NETWORKING ABBREVIATED

By Mark E. Donaldson

The access method Ethernet uses is **CSMA/** (Carrier Sense Multiple Access with Collision Detection). In this method, multiple workstations access a transmission medium (**Multiple Access**) by listening until no signals are detected (**Carrier Sense**). Then they transmit and check to see if more than one signal is present (**Collision Detection**). Each station attempts to transmit when it "believes" the network is free. If there is a collision, each station attempts to retransmit after a preset delay, which is different for each workstation. **Collision detection** is an essential part the CSMA/CD access method. Each station that detects the collision will some period of time and then try again **The two possible topologies for are bus and star.** The **bus** is the simplest (and traditional) topology. Standard Ethernet (10BASE5) and Thin Ethernet (10BASE2), both based on coaxial cable systems, use the bus. In this one-cable LAN, all workstations are connected in succession (a "bus" arrangement) on a single cable. All transmissions go to all the connected workstations.

Each workstation then selects those transmissions it should receive based on the address information contained in the transmission. In a **star** topology, all attached workstations are wired directly to a central hub, which establishes, maintains, and breaks connections between them (in the event of error). The advantage of a star topology is that it is easy to isolate a problem node. The disadvantage is that if the hub fails, the entire system is compromised. Twisted-Pair Ethernet (10BASE-T), based on unshielded twisted pair, and Fiber optic Ethernet (FOIRL and 10BASE-FL), based on fiber optic cable, use the star.



Bus-Standard Ethernet (Coax): 10BASE-5

NETWORKING ABBREVIATED

By Mark E. Donaldson

Star-Twisted-Pair Ethernet (Unshielded Twisted Pair): 10 BASE-T, UTP

- There are two versions of Ethernet over unshielded twisted pair: 10BASE-T (the standard) and its predecessor UTP.
- 10BASE-T and UTP segments can coexist on the same network when each common segment, via a transceiver and transceiver cable or converter.
- The cable used is 2 to 26 AWG unshielded twisted pair (standard telephone wire), at least Category 2 with two twists per foot. Category 3 or 4 is preferred. Category 5 supports 100BASE-T (Fast Ethernet).
- Workstations are connected to a central concentrator ("hub") in a star configuration. Concentrators can be attached to a fiber optic or coax network, and can be concentrated to form larger networks.
- A hub usually also has an AUI port for standard Ethernet connections.
- The maximum distance of a segment (from concentrator to node) is 100 m (328 feet).
- The maximum number of devices per segment is 2. One device is the hub port; the other is the 10BASE-T or UTP device.
- Ethernet network interface cards (NICs) are available with built-in 10BASE-T transceivers.
- Devices with standard AUI ports may be attached with a twisted-pair transceiver.
- Twisted pair is the most economical cable type, especially since it may already be installed, and it is the easiest to work with. But it is not recommended for installations with much EMI/RFI interference (for example, in industrial environments).

Bus-Th!nNet Ethernet (Coax): 10BASE2

- The maximum length of a segment is 185 m (607 feet).
- A maximum of 2 IRL (InterRepeater Links) is allowed between devices; the maximum length of cable is 925 m (3035 feet).
- Typically, devices use Ethernet network interface cards (NICs) with built-in BNC transceivers. This eliminates the need for separate transceivers, as connections can be made directly to the ThinNet cable. Devices are connected to the cable with T-connectors, which must be plugged directly into the card. No cable is allowed between the T and the card. Workstations are daisy chained, with an "in-and-out" cabling system.
- The minimum distance between T-connectors is 0.5 m (1.6 feet).
- If the interface card does not have its own built-in BNC transceiver, a BNC transceiver and transceiver cable are required. The maximum length of a transceiver cable is 50 m (164 feet).
- Up to 30 connections can be attached to a single segment.
- Both ends of each segment should be terminated with a 50-ohm resistor.
- One end of each segment should be grounded to earth.

Star-Fiber Optic Ethernet: FOIRL or 10BASE-FL

NETWORKING ABBREVIATED

By Mark E. Donaldson

- There are two versions of Ethernet over fiber optic cable, meeting the older FOIRL (Fiber Optic InterRepeater Link) and the more recent 10BASE-FL standards.
- FOIRL IRL and 1 10BASE-FL fiber optic Ethernet differ only in how far each will transmit (the maximum length of a segment). For FOIRL it is 1 km (0.6 miles); for 1 10BASE-FL it is 2 km (1.2 miles).
- The maximum number of devices per segment is 2. One device is the hub port, the other device is the 1 10BASE-FL device.
- Fiber optic cable provides the best signal quality as well as the greatest point-to-point distance.
- Fiber optic cable is completely free of EMI/RFI interference.
- Fiber optic cable runs point to point only; it cannot be tapped or daisy chained. A fiber optic hub or multiport repeater is required to carry the signal to multiple devices (for FOIRL, a FOIRL multiport repeater and transceivers).
- Since fiber optic cable does not carry electrical charges, all electrical cable problems disappear. When fiber optic cable (outdoor quality) is used to link buildings, grounding problems and voltage spikes are eliminated. And fiber optic cable is immune to electronic eavesdropping.

CABLES AND CONNECTORS

For additional information on Cables and Connectors, refer to *White Paper CABLES AND CONNECTORS*.