The IEEE 802.3 Standard (Ethernet):
An Overview of the Technology

Rion Hollenbeck
ICS 620
Dr. Jones
17 September, 2001

Table of Contents

Introduction ……… ………………………………………………………………… 2

Evolution of the IEEE 802.3 Standard …... ………………………………………… 2

IEEE 802.3 Subtypes ………….. …………………………………………………… 3

How Ethernet Works: In Brief .. …………………………………………………… 4

Relation to the OSI Model …… …………………………………………………… 6

Carrier Sensing Multiple Access with Collision Detection (CSMA/CD) …. ……… 7

Data Transmission ... ……………………………………………………………… 8

Frame Collisions ….. ……………………………………………………………… 9

The IEEE 802.3 Data Frame ….. …………………………………………………… 11

Cyclic Redundancy Check ……. …………………………………………………… 14

Manchester Encoding ………... …………………………………………………… 15

IEEE 802.3 Physical Media …... …………………………………………………… 16

Benefits and Limitations of IEEE 802.3 ….. ……………………………………… 18

Conclusions ………. ……………………………………………………………… 20

References

As the 21st century begins, data communications and networking will continue to grow in importance and necessity. With this necessity comes the need for fast and reliable transfer of data from one place to another. Many network protocols have been developed and are in use, but the most widely used in Local Area Networks is the Ethernet standard.

The following discussion will present an overview of the Ethernet (IEEE 802.3) standard. The paper will cover a brief history of the development of the Ethernet standard and how that has evolved to the IEEE 802.3 standard. The evolution from original Ethernet to 1Gb/s Ethernet will be presented with a focus on the 10 Mb/s standard. How the Ethernet standard fits into the OSI network model will be discussed briefly followed by a detailed look at how the Carrier Sensing Multiple Access with Collision Detection (CSMA/CD) standard works. The basis of the Ethernet system, the data frame, will be analyzed and presented. In addition, a brief discussion on the hardware and physical topology of an Ethernet network will be presented. Finally a brief discussion will be presented on the benefits and limitations of the Ethernet system.

The scope of this paper is an elementary look at the Ethernet standard for network protocol. The discussion will focus on an analysis of the 10 Mb/s IEEE.802.3 standard. The term Ethernet will be used interchangeably with IEEE 802.3 understanding that the original Ethernet protocol differs very slightly from the IEEE 802.3 standard.

Evolution of the IEEE 802.3 Standard

Back in the 1970s at the Xerox Palo Alto Research Center, Dr. Robert M. Metcalf developed a network standard that enabled the sharing of printers to personal workstations (Slone, 1998)(Fairhurst, 2001d)(Gilbert, 1995). This original system, entitled the “Alto Aloha Network” (later re-named “Ethernet”), was able to transmit data at a rate of 3 Mb/s between all connected computers and printers (Kaplan & Noseworthy, 2000). Later, in 1980 a multi-vendor consortium consisting of DEC, Intel, and Xerox released the DIX Standard for Ethernet. It was through this effort that Ethernet was able to become an open standard for network operations (Fairhurst, 2000d).

At the same time, the Institute of Electrical and Electronic Engineers (IEEE) created a group designated the 802 Working group to standardize network technologies. This group created standards that they would later number 802.x, where x was the subcommittee developing the particular standard (Pidgeon, 2001b). The subcommittee that developed the standards for the CSMA/CD, functionally very similar to the DIX Ethernet system, was 802.3. Later in 1985, the official standards were released for the IEEE 802.3. The standards were for Carrier Sensing Multiple Access with Collision Detection access method (Pidgeon, 2001b).

It is important at this point to distinguish between original DIX Ethernet and what is termed Ethernet today. Ethernet today refers to the IEEE 802.3 standards. Although functionally similar, there are subtle differences between the two standards. The main differences lay with the frame structure, which will be discussed later, and the data transfer rates. For now, when the term Ethernet is used, it refers to the IEEE 802.3 standards.

IEEE 802.3 Subtypes

There are currently three "versions" of Ethernet available for commercial use. The difference between these types lies in the speed at which they can transmit data. The earliest form of the IEEE 802.3 standard, still in use today by many offices and LANs, is the 10 Mb/s speed. This means that this version can transmit data at 10 Mb/s (1,000,000 bits / second). The

10 Mb/s Ethernet can transmit over thick or thin Coaxial cable, UTP (Unshielded Twisted Pair) wire, or fiber optic cable.

The early Thick and Thin Ethernet, which referred to the type of coaxial cable used, were set up in a bus topology. This means that the machines were all connected directly to the main transmission medium in a linear fashion. However, with UTP as the transmission medium of choice, the topology of Ethernet networks have evolved into the Star topology. In the star topology, all machines are connected to a central hub, router, or switch. This greatly reduces the problems associated with damaged cabling (Cisco Systems, 1999).

The next category is the 100 Mb/s Ethernet or "Fast Ethernet." The only functional difference between these two is the speed of data transmission. With a transfer rate of 100 Mb/s, this system typically uses either Category 5 UTP cable or Fiber Optics for the transmission medium (Cisco Systems, 1999).

The newest form of Ethernet is the 1 Gb/s category. This technology is functionally similar to the 10 and 100 Mb/s technologies, but has subtle differences. The main difference is that the transmission medium for 1 Gb/s Ethernet is the fiber optic cable not UTP (Cisco Systems, 1999). The remainder of the discussion focuses on the technology of the 10 Mb/s Ethernet standard. These standards also apply to the 100 Mb/s Ethernet standard.

How Ethernet Works: In Brief

The Ethernet system works off of the CSMA/CD standard. CSMA/CD simply means that the computers all have access to the transmission medium, and can send and receive data whenever the network is idle. The benefit of Ethernet is that it has the ability to sense collisions on the network (Pidgeon, 2001a). A collision occurs when two or more machines (nodes) try to send data at the same time. There are sophisticated techniques used to keep this from occurring on a regular basis. These techniques will be discussed later.

When a node on an Ethernet network wishes to send information to another node, it first listens to the network to see if there is network traffic. If the station detects no traffic, it will begin sending the frames of data. These frames will be transmitted throughout the network and ALL nodes on the particular Ethernet segment will receive the frames. However, only the node for which it was intended will be able to view the contents of the frame (Pidgeon, 2001a). This is done through source and destination addressing, which will be described later.

If, however, more and more nodes become active on the network the probability of multiple nodes trying to send information at the same time increases. If two or more nodes send data at the same time a collision will occur. When this happens, the sending station will send out a jam sequence alerting all other nodes that there has been a collision and that any data received should be discarded (Spurgeon, 1995e). The node then waits a period of time and re-sends the frame. A mathematical algorithm termed "Truncated Binary Exponential Backoff "determines the amount of time the node waits (Spurgeon, 1995b). This process will be discussed in greater detail later in the discussion.

The CSMA/CD standard can be broken down into its individual parts and applied to the description above. The Carrier Sensing (CS) is the ability of the computers to listen to the network and determine if there is activity. Multiple Access (MA) refers to the fact that all nodes on the network have access to the transmission medium at all times, and finally, the Collision Detection (CD) process was explained above (Pidgeon, 2001a).

Relation to the OSI Model

The IEEE 802.x standards all fall within the first two layers of the Open Systems Interconnection (OSI) Model. The first layer, the Physical Layer, handles the actual transport of the bits from the sender to the receiver. This layer does not know what the bits are, or anything about them. It is solely responsible for transporting the electrical impulses across the physical medium (Kaplan & Noseworthy, 2000).

The real guts of the Ethernet system lie in the Medium Access Control (MAC) standards. The MAC is truly what gives Ethernet its ability to handle collisions and effectively transport data. The Medium Access Control, which is common to all 802.x standards, resides in the Data Link Layer of the OSI Model. Figure 1 illustrates how all of the protocols and standards fit together and how they fit in the OSI Model.

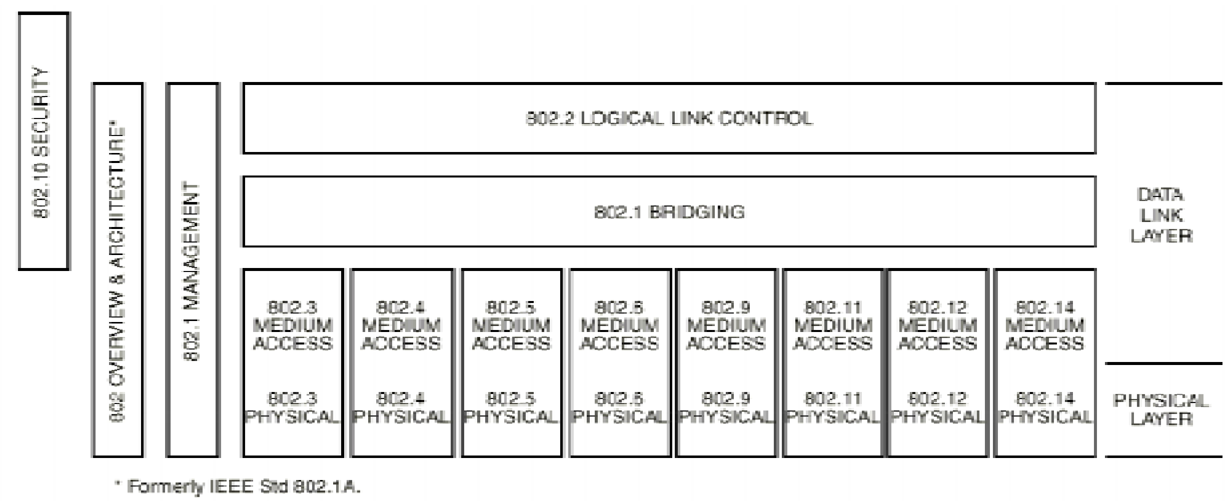

Figure 1. *IEEE 802 and the OSI Model*
Hadriel Kaplan & Bob Noseworthy, 2000

The Data Link layer provides the functional and procedural means to transfer data from one network station to another. It is also in this layer that errors can be detected and possibly corrected. In addition bits are grouped into frames and certain maintenance and timing issues are addressed (Fairhurst, 2001i)(Slone, 1998).

Carrier Sensing Multiple Access with Collision Detection (CSMA/CD)

The following section goes into greater detail explaining how the CSMA/CD standard functions and how it enables the network to transmit data efficiently and with very few errors.

As was explained earlier, CSMA/CD allows machines to send and receive data any time it senses that the network is inactive (IEEE, 2000). This method allows for a much more efficient use of the network resources and transmission medium. First it is necessary to explain how the Ethernet network is set up.

A network can be made up of two or more machines connected together with a transmission medium. These nodes that are connected together form an Ethernet Segment or a Collision Domain (Fairhurst, 2001d). It is called a collision domain because all of the nodes will receive every other nodes traffic. This being the case, the transmission medium is truly shared, therefore collision prone. Machines can be on the same network, but not on the same Collision Domain. This is done through the use of bridges and switches (Slone, 1998).

Each machine or node on the network has a unique MAC (Medium Access Control) address. This MAC address is permanently imprinted on the NIC (Network Interface Card) in the form of a ROM (Read Only Memory) chip (Fairhurst, 2001g). The addresses are globally unique and are assigned to the NIC manufactures in blocks of 8 or 16 million. This ensures that no two network nodes have the same address (Fairhurst, 2001g). It is this address that distinguishes a node from other machines on the network.

Data Transmission

On any collision domain of an Ethernet network any information that is sent out over the network propagates in both directions in order to reach all nodes. All nodes receive every frame that is sent over the network, whether it is intended for that particular node or not. Only if the frame is addressed to that particular node, is the node allowed to accept it. (Fairhurst, 2001a).

When a particular node on the network is ready to send information it goes through a series of steps which are outlined below:

1. The node listens to the network to see whether any other node or machine is transmitting. The node is able to listen by sensing the carrier signals present on the network transmission medium. If there is activity, the node continues to wait.
2. When no signal is detected, the node starts transmission of the message of frame.
3. While the node is transmitting, it also listens to the network. The node compares the received message with what was transmitted. If they are the same, the node continues to transfer, putting a 9.6 μs gap between frames.
4. If what is received is not what was sent, the node assumes it was a collision and stops transmitting.
5. The node transmits a Jam sequence which tells other nodes that a collision has been detected
6. The node waits a random amount of time and then begins again (Reed, 1996)

This is the basic process that each node goes through when it transmits a packet. Figure 2 illustrates this process in detail. It seems very simple, but the truth is that there are a lot of behind-the-scenes processes that enable these simple six steps to take place.

The node "listens" to the transmission medium by use of a transceiver. This transceiver monitors the current flow along the cable. When the transceiver picks up current flow that translates to a bit flow (about 18-20 mA), it says the cable is busy and does not transmit any data (Fairhurst, 2001a). If the transceiver senses no activity, i.e. no current flow, it can begin transmission of data.

Frame Collisions

While the node is transmitting, it also continues to "listen". It monitors all data that it has sent over the network. When it senses a collision on the network it halts transmission. It is able to sense a collision using the same transceiver. When the transceiver detects excess current on the line, it stops transmission of data and transmits a 32-bit jam sequence (Fairhurst, 2001a). This sequence is to let any node that may be receiving the damaged frame, to discard it. The receiving machine knows this because the 32-bit jam sequence is designed to take the place of the 32-bit CRC (Cyclic

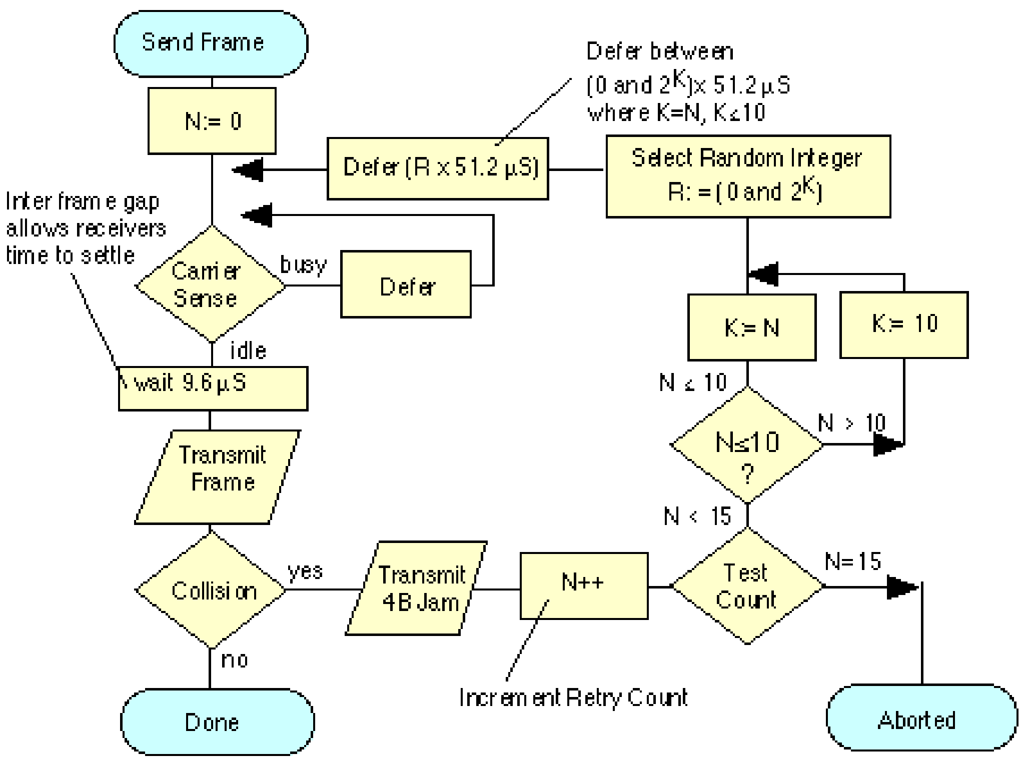

Figure 2. IEEE 802.3 Transmission Algorithm
Garry Fairhurst, 2001

Redundancy Check) error-checking portion of the data frame (See the next section on CRC for more information). When the receiving node gets this jam sequence, it checks it against its CRC and determines it is an error and discards the frame (Fairhurst, 2001).

Following a detection of a collision, the node(s) will wait a random amount of time before transmitting the frame again. This process is known as "Truncated Binary Exponential Backoff (Spurgeon, 1995b)." Simply put, after the collision and jam sequence has been sent and received, each node involved in the collision can either transmit immediately (following the 9.6 μs gap), or it can wait one window period. A window period is defined as the time it takes one frame to propagate the round-trip length of the network. The standard window time has been set to 51.2 μs (Hardy, 1995). This is calculated by the fact that a standard frame is at least 512 bits in length. Since the transmission speed is 10 Mb (10,000,000 bits) / second, it would take 51.2 μs to send one frame.

After a collision, the node will select a multiple of the base window time (51.2 μs) to wait before sending again. This multiple comes from a set of numbers generated by the node with each successive send attempt (Hardy, 1995). For example, if the node encounters a collision, it will either send immediately, or wait one window (51.2 μs). If it encounters another collision, it will then select a multiple of the window from the set of (0, 1, 2, or 3) . Figure *2* illustrates this point. There are four options; therefore there is only a 25% chance that both nodes will choose the same time interval. The set of multiples continues to increase for each repeated attempt. The formula for the set of numbers is simply 2^K where K is the number of attempted resends (Hardy, 1995). So for the first attempt it would be 2^1 for a set of (0 or 1) times the window value. If it was the second attempt, it would be 2^2 for a set of (0, 1, 2, or 3) times the window and so on. This will continue up through fifteen re-sends. At this point, the node will stop attempting to send, and look to higher OSI-level software to decide what to do next (Hardy, 1995). Incidentally, the total of fifteen re-sends corresponds to a set of windows ranging from 0-1023, which corresponds directly with the 1024 maximum number of nodes allowable on any collision domain (Fairhurst, 2001a).

The IEEE 802.3 Data Frame

The CSMA/CD system sends information through the network using MAC (Medium Access Control) data frames. Simply put, a data frame is a small slice of data wrapped in MAC information. This MAC information is what allows the packet to be delivered to the correct place and in one piece (Fairhurst, 2001f).

The reason the system uses data frames is simple. When a single transport medium is shared by many different nodes, each trying to send information to a particular destination, it is much more efficient to break down a large amount of data into small packets and send each packet when the network is clear. This allows every node on the network to have a chance to send a small piece of its data at a time. The concept is very much like multiplexing, where a bit

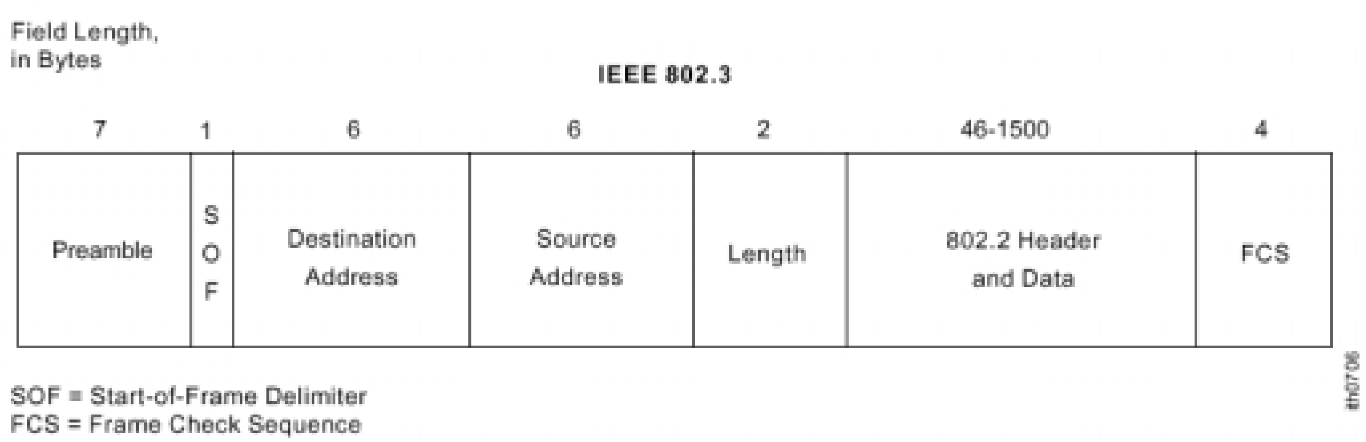

Figure 3. *IEEE 802.3 Data Frame Format*
Cisco Systems, 1999

stream is broken down into individual bits and each gets its place along the cable.

The IEEE 802.3 data frame consists of seven different fields. These fields are put together to form a single data frame. Figure 3 illustrates the seven following fields: Preamble, Start-of-Frame delimiter, Destination Address, Source Address, Length, Data, and Frame Check Sequence (Cisco Systems, 1999). Each is discussed below.

Preamble

The preamble is a field that tells the receiving node that a data frame is coming. This field is simply a 56-bit (7 byte) alternating pattern of 1s and 0s (Cisco Systems, 1999).

Start of Frame Delimiter

The start-of-frame delimiter is used in conjunction with the preamble to synchronize the receiving clock with the transmitting clock though on lock of the Digital Phase Lock Loop (DPLL)(Fairhurst, 2001c). The Digital Phase Lock Loop circuit is used to lock onto the phase timing of the frame which is imbedded in the Manchester Encoding of the data. Manchester Encoding will be discussed later.

Along with the recognized bit pattern supplied by the preamble, the DPLL circuit is able, through the use of shift registers, to lock the receiving clock on to the timing of the sending clock (Fairhurst, 2001c). Figure 4 illustrates this process.

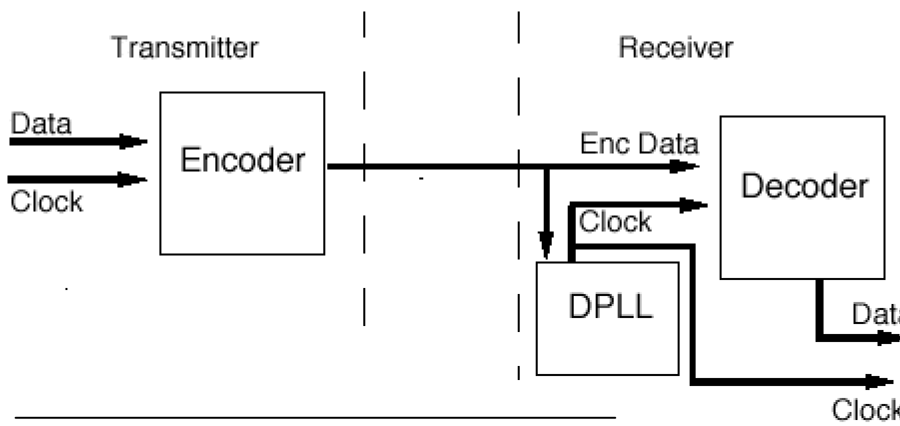

Figure 4. *Digital Phase Lock Loop*
G. Fairhurst, 2001

Destination Address

The destination address is the MAC address of the machine to which the particular frame is to be delivered. As explained earlier, each NIC (Network Interface Card) has a unique MAC address. It is this address that is part of the destination address field, which is a 6 byte or 48-bit address (Cisco Systems, 1999).

The destination address can be one of three types: unicast, multicast, or broadcast (Slone, 1998). A unicast address is addressed to a single node on the network. This is the MAC address of the machine. Multicast is where a single frame can be sent to a number of nodes in a particular group. This is done by programming individual nodes to listen for specific multicast addresses. If one of these addresses is present in the destination address, any node that is set up to receive that address will retrieve that data (Cisco Systems, 1999). The third type of destination address is a broadcast address. When the destination address contains a broadcast address, every node on the network will be able to retrieve the data in that frame. The standard broadcast address is a 48-bit number of all 1s (Spurgeon, 2001d). This addressing scheme allows the network to be very flexible in transmission of data.

Source Address

The source address, like the destination address, is a 48-bit field. However, this value is always a unicast address and always reflects the MAC address of the sending node (Cisco Systems, 1999).

Length

The length field consisting of 16 bits contains the total number of bits of information contained in the following *Data* field.

Data

The data field contains the actual data to be processed by upper level protocols of the recipient node. The length of the data must be between 46 – 1500 bytes. The 46-byte minimum is to ensure that the entire length of the data frame is at least 64 bytes in length (Gilbert, 1995). The 64 bytes equates to 512 bits. This is the minimum size a data frame must be for nodes on either end of the network to be able to detect collisions. This is related to the propagation time of the data frame through the 10 Mb/s network (Cisco Systems, 1999).

Frame Check Sequence

The frame check sequence is a 4 byte, 32 bit Cyclic Redundancy Check (CRC) value. This value is calculated by the transmitting node and appended to the frame (Cisco Systems, 1999). On the receiving end, the receiving node also calculates this value. If the values do not match, there has been a transfer error and the frame is discarded.

Cyclic Redundancy Check

The main error checking method for frames transferred over a CSMA/CD network is the Cyclic Redundancy Check (CRC). This is a 32 bit value that is appended to the end of the data frame as explained above. The CRC is calculated by the transmitting node and then again by the receiving node. If they do not match, i.e. if the receiving node does not calculate the same CRC number as the one in the data frame, there has been a transmission error, and the frame

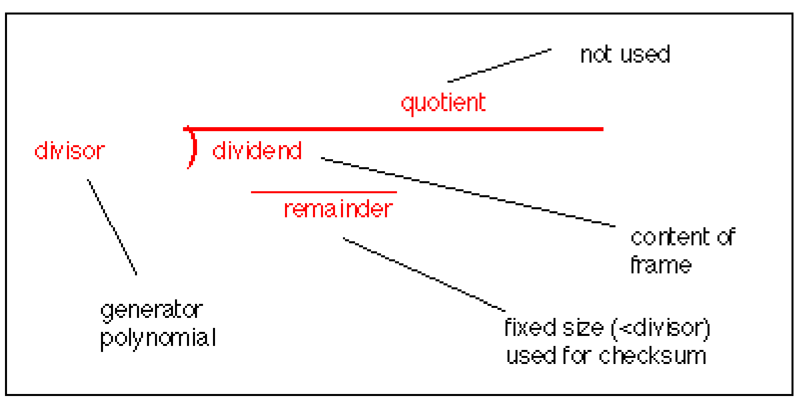

Figure 5. *CRC value calculation*
G. Fairhurst, 2001b

is discarded (Cisco Systems, 1999).

The CRC value is calculated using complex polynomial division. Figure 5 illustrates how the value is calculated.

Depending on the type of CRC used, the polynomials differ. Ethernet (IEEE 802.3) uses 32 bit CRC so the polynomial that would be the divisor for this equation would be:

$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$ (Hardy, 1995). The entire frame contents, from the destination address back through the data, are divided by this polynomial and the remainder is used in the CRC field. Because of the speed at which the Ethernet network can transfer information, when a frame is corrupt or has errors, it is simply discarded and the sending node requests a new one.

Manchester Encoding

Ethernet transmission sends a baseband signal. This means that the signal is not modulated at all, it is simply the data that is being sent. However, the frame is not simply sent as a series of 1s and 0s as they would appear in the data frame. IEEE 802.3 uses an encoding method called Manchester Encoding (Fairhurst, 2001e).

Manchester encoding is used to encode the data as well as to synchronize the two nodes. The actual encoding process interweaves the clock speed into the bit stream. This process makes it very easy for the

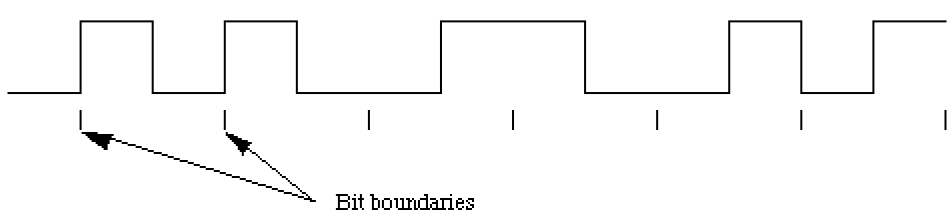

Figure 6. *Manchester Encoding (Biphase Code)*
G. Fairhurst, 2001f

receiving machine to stay in phase with the transmission clock because each transmitted bit is represented by a phase transition between 2 bits of either 90^{o} or -90^{o} (Fairhurst, 2001e). Figure 6 illustrates this encoding process.

The wave form illustrated at the right represents a binary bit flow. There is a transition in the center of each bit boundary. The type of transition determines which logical state, 0 or 1, will be registered. When the flow changes from a logical 1 to a 0 (0 volts to –2.05 volts) in a given bit boundary, a 0 is registered. If the flow changes from a 0 to 1 (transition from –2.05 volts to 0 volts) within a bit boundary, a logical 1 is registered (Hardy, 1995). The main benefit of this is that no matter what the bit value, or how many there are in sequence; there is always a logical bit transition occurring. This enables the receiving clock to always stay synchronized with the sending clock. The synchronizing method was explained earlier as Digital Phase Lock Loop.

IEEE 802.3 Physical Media

The physical components of an Ethernet network, i.e. network cables and network interface cards, are what actually enable the encoded bit stream of data to flow from one node on the network to the next. This section will take a very brief look at the different transmission mediums that are supported by the IEEE 802.3 standard, focusing on the 10BaseT standard.

As far as cabling goes, there are four main types that are used on Ethernet networks. These types are thin coaxial, thick coaxial, Category 5 UTP (Unshielded Twisted Pair) and fiber optics. Table 1 summarizes the specifications for each type of transmission medium. It can be seen that each type of transmission medium has a maximum length that a given segment of that type can be. In addition, the physical topology of the network depends heavily on the type of transport medium used (Cisco Systems, 1999). This was presented earlier in the discussion.

The most common transmission medium for Ethernet is 10BaseT. The name actually

Characteristic	Ethernet Value	IEEE 802.3 Values 10Base5	10Base2	10BaseT	10BaseFL	100BaseT
Data rate (Mbps)	10	10	10	10	10	100
Signaling method	Baseband	Baseband	Baseband	Baseband	Baseband	Baseband
Maximum segment length (m)	500	500	185	100	2,000	100
Media	50-ohm coax (thick)	50-ohm coax (thick)	50-ohm coax (thin)	Unshielded twisted-pair cable	Fiber-optic	Unshielded twisted-pair cable
Topology	Bus	Bus	Bus	Star	Point-to-p oint	Bus

Table 1. *IEEE 802.3 Transmission Medium Specifications*
Cisco Systems, 1999

indicates quite a bit about the type of medium. The 10 stands for 10 Mb/s, the Base indicates that it is a baseband signal, and the T stands for Twisted Pair cabling (Cisco Systems, 1999). The other transmission standards are named in a similar fashion.

10BaseT uses a standard 4-pair UTP cable. This medium, which looks a lot like a fat telephone line, carries eight wires or four pairs. The main difference between the UTP cable and the phone line is that in UTP, the pairs of wires are twisted. This twisting reduces the cross-talk within the cable and cuts down on collision that would be detected due to wire cross-talk (Spurgeon, 1995f). The standard IEEE 802.3 signal uses two pairs of wires, one for transmission and one for

Pin Number	Signal
1	TD+
2	TD-
3	RD+
4	Unused
5	Unused
6	RD-
7	Unused
8	Unused

Table 2. *10BaseT eight-pin connector*
C. Spurgeon, 1995

receiving. Table 2 summarizes the configuration of the pins on the RJ-45 jack for the 10BaseT standard.

For the network to communicate with the node, a network interface card (NIC) is needed. A network card is simply an expansion card that plugs into the motherboard of the machine. This card has a unique MAC address that distinguishes itself from every other node on the network. This addressing process was explained earlier.

The NIC card is the interface between the host node and the transmission medium (Cat 5 UTP Cable). This card usually contains an internal transceiver, the part that "listens" to the network to detect collisions. The card also contains an Ethernet controller and protocol control that enables it to support the Medium Access Control (MAC) protocol used by the IEEE 802.3 standard (Fairhurst, 2001h).

In addition to the network card, the Ethernet network contains many other pieces of hardware including routers, switches, bridges and hubs. These topics are beyond the focus of this paper, but it is important to recognize their participation in Ethernet networking.

Benefits and Limitations of the IEEE 802.3 (Ethernet) Standard

The IEEE 802.3 (Ethernet) networking standard has become the most widely used networking standard in most Local Area Networks (LANs) and Wide Area Networks (WANs). This is due to the flexibility and vendor-neutrality built into the Ethernet system. Most computer manufacturers today equip computers with Ethernet cards that can be connected directly to either 10 Mb/s or 100 Mb/s networks. Because of this fact, it is very easy to connect new nodes and upgrade existing nodes on an Ethernet network.

The cost of standard CAT5 cabling is very cheap compared to the cost of either coaxial cabling or fiber optics. By simply purchasing two or more machines, some CAT5 cabling with RJ-45 connectors, and a simple hub, the Ethernet network can be set up, all within a matter of minutes. This flexibility allows for the easy expansion of the network as the organization grows.

In addition, it becomes very easy to adapt the network to physical changes. If user A moves offices and plugs his/her machine into a different jack, the network still recognizes the MAC address on the NIC and automatically assigns that node back into the group(s) that it was part of before the move. This is real benefit because of the dynamic nature of today's businesses.

However, with all of the benefits of Ethernet, there are some limitations that exist. To begin, there is a limit to the length of a particular Ethernet segment. For standard 10BaseT cabling, the maximum length of any Ethernet segment is 100 m. That may seem like a lot of length, but if a particular segment is to span several floors of an office building, that 100 m may not be sufficient. When it comes to 10BaseFL which is fiber optic cable, the maximum distance is extended to 2000 m, but the cost of fiber over standard CAT5 UTP is substantial.

Another limitation is the number of nodes that can be connected to any single Ethernet Segment or Collision Domain. As eluded to earlier, the maximum number of nodes on any segment or domain is 1024. Simply put, the more nodes on a particular segment, the slower the network will perform. With more nodes sharing the medium, each gets less and less time to send and receive data. This problem however has been overcome by the use of Switched Ethernet, which basically puts each node on its own segment. Each segment is attached to a switch which actually does the routing of the traffic, so the medium is no longer shared. This also means that the Collision Detection is no longer needed in setups such as this because there is no shared medium (Pidgeon, 2001b). However, smaller un-switched networks continue to face the issues of network traffic.

Conclusions

The IEEE 802.3 standards for CSMA/CD have proved to be an invaluable set of standards in the networking world. With a majority of LANs operating on some form of Ethernet, be it 10 Mb/s, 100 Mb/s, or the newest 1Gb/s, the technology provides an environment that is flexible enough to change with today's dynamic market place, but strong enough to provide the level and quality of service that today's networked businesses demand.

In addition, the fact that Ethernet is able to work without proprietary software or hardware, makes it ideal for smaller companies, and those with legacy equipment that must be worked into the network. Because the standards are open, most vendors are able to provide hardware that is compatible with the network.

With today's advancements in fiber optics and wireless technology, Ethernet and CSMA/CD are reaching a new level of applicability. The necessity to have an entire building wired with CAT5 cable is becoming obsolete. Wireless transceivers can provide direct access to the network without the need for expensive cabling.

As network technology continues to advance, we will continue to see Ethernet evolve to maintain its status as one of the easiest and most efficient ways to approach networking.

References

Cisco Systems. (1999, July). Ethernet Technologies.
< http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm>
[2001, September 3].

Fairhurst, G. (2001a, January 1). CSMA/CD.
< http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/csma-cd.html>
[2001, September 3].

Fairhurst, G. (2001b, January 1). Cyclic Redundancy Check.
< http://www.erg.abdn.ac.uk/users/gorry/course/dl-pages/crc.html>
[2001, September 3].

Fairhurst, G. (2001c, January 1). Digital Phase Locked Loop.
< http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/dpll.html>
[2001, September 3].

Fairhurst, G. (2001d, January 1). Ethernet.
< http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/enet.html>
[2001, September 3].

Fairhurst, G. (2001e, January 1). Manchester Encoding.
< http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/man.html>
[2001, September 3].

Fairhurst, G. (2001f, January 1). Medium Access Control.
< http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/mac.html>
[2001, September 3].

Fairhurst, G. (2001g, January 1). Naming and Addressing.
< http://www.erg.abdn.ac.uk/users/gorry/course/intro-pages/addresses.html>
[2001, September 3].

Fairhurst, G. (2001h, January 1). Network Interface Card.
< http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/nic.html>
[2001, September 3].

Fairhurst, G. (2001i, January 1). OSI Reference Model.
< http://www.erg.abdn.ac.uk/users/gorry/course/intro-pages/osi.html>
[2001, September 3].

Gilbert, H. (1995, April 12). Ethernet. <http://www.yale.com/pclt/COMM/ETHER.HTM>
[2001, September 3].

Hardy, J. (1995) Inside Networks. Columbus, OH: Prentice Hall.

IEEE. (2000). Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications. [On-line reproduction]. Available: http://standards.ieee.org/getieee802/802.3.html [2001, September 5].

Kaplan, H. & Noseworthy, B. (2000, September) The Ethernet Evolution. PowerPoint Presentation presented at the Interop Atlanta 2000 Workshop W924. Available: <http://www.iol.unh.edu/training/ge/ethernet_evolution_index.html>. [2001, September 5].

Pidgeon, N. (2001a). CSMA/CD. <http://www.howstuffworks.com/ethernet3.htm> [2001, September 3].

Pidgeon, N. (2001b). Ethernet Today. <http://www.howstuffworks.com/ethernet7.htm> [2001, September 3].

Pidgeon, N. (2001c). Limitations of Ethernet. <http://www.howstuffworks.com/ethernet4.htm> [2001, September 3].

Reed, K. (1996) Data Network Handbook: An Interactive Guide to Network Architecture and Operations. New York: Van Nostrand Reinhold.

Slone, J. Editor. (1998) Handbook of Local Area Networks. Boca Raton: Auerbach.

Spurgeon, C. (1995a). 10-Mps Media Systems. <http://www.ots.utexas.edu/ethernet/ethernet/10quickref/ch2qr_2.html> [2001, September 5].

Spurgeon, C. (1995b). Collisions. <http://www.ots.utexas.edu/ethernet/ethernet/100quickref/ch1qr_8.html> [2001, September 5].

Spurgeon, C. (1995c). Development of Ethernet Standards. <http://www.ots.utexas.edu/ethernet/ethernet/100quickref/ch1qr_4.html> [2001, September 5].

Spurgeon, C. (1995d). Ethernet Frame and Ethernet Addresses. <http://www.ots.utexas.edu/ethernet/ethernet/100quickref/ch1qr_10.html> [2001, September 5].

Spurgeon, C. (1995e). The Ethernet System. <http://www.ots.utexas.edu/ethernet/ethernet/100quickref/ch1qr_2.html> [2001, September 5].

Spurgeon, C. (1995f). Network Medium.
<http://www.ots.utexas.edu/ethernet/ethernet/10quickref/ch5qr_4.html>
[2001, September 5].

Spurgeon, C. (1995g). Twisted-Pair Patch Cables.
<http://www.ots.utexas.edu/ethernet/ethernet/10quickref/ch5qr_7.html>
[2001, September 5].