Institute of Electrical and Electronic Engineers (IEEE)

- Formed in 1963 by a merger of the American Institute of Electrical Engineers (AIEEE) and the Institute of Radio Engineers (IRE)

- World's largest professional engineering society
  - Membership open to the engineering community

- Developing and disseminating electrotechnical standards is a core activity
  - National & International recognition
  - Publishes standard guides, practices, and reference manuals to define these standards

- Many publications, journals, and newsletters are published by members under the IEEE title, contain various proposals and technology trends

- IEEE Standards process
  - Individual committees develop draft standards
  - Then approved through the IEEE Standards Board
  - Forwarded to ANSI and/or ISO for finalization and adoption
IEEE LAN Standards

• Standards are developed by the IEEE LAN Standards Committees.
  – 802.1 Internetworking
  – 802.2 Logical Link Control
  – 802.3 CSMA/CD local area networks
  – 802.4 Token Bus local area networks
  – 802.5 Token Ring local area networks
  – 802.6 Metropolitan Area Networks
  – 802.7 Broadband Technical Advisory Group
  – 802.8 Fiber Optic Technical Advisory Group
  – 802.9 Integrated voice and data networks
  – 802.10 Network security
  – 802.11 Wireless networks
  – 802.12 Demand Priority Access local area networks

• Committees efforts focus on developing protocol standards for the lower level functions of LAN connectivity
  – Physical and Data-Link layers of the ISO/OSI Reference Model
  – Define how data connections among network devices are made, managed, and terminated
  – Specify physical elements such as cabling and connectors
Consortia and Forums

• **Fast Ethernet Alliance**
  - Over 75 member companies promoting open, cost-effective, and interoperable 100BaseT Ethernet (100Mbps)
  - Formed around common objectives
    • Extend the existing Ethernet standard in response to demand for increased network bandwidth
    • Address customer need for interoperability with Fast Ethernet products

• **100VG-AnyLAN Forum**
  - Formed to promote the IEEE 802.12 (100VG-AnyLAN) standard as the successor to the IEEE 802.3 (10BaseT) protocol

• **ATM Forum**
  - Formed in 1991 with more than 800 member organizations worldwide
  - Represents computer and communications industries, as well as government agencies, research organizations, and end users
  - Chartered to speed the development and deployment of ATM products and services
  - Development and recommendation of interoperability specifications
  - Promotion of industry cooperation and awareness
Consortia and Forums

• **Frame Relay Forum**
  – Association of Frame Relay users, vendors, and service providers
  – Development of Frame Relay standards
  – Made up of committees that create implementation specifications and agreements

• **North American ISDN Users' Forum (NIUF)**
  – Quasi-standards body
  – Proposes standards and works for their adoption

• **SMDS Interest Group (SIG)**
  – Promoter of Switched Multimegabit Data Service
  – Association of SMDS product vendors, service providers, carriers, and end users
  – Working groups that promote SMDS and work on specifications
    • The Technical Working Group works on improvements to the IEEE 802.6 standard
  – Sponsors a user group and a public-relations group that holds seminars and disseminates information
Other Consortia and Forums

- W3C - World Wide Web Consortium
- IETF - Internet Engineering Task Force and the Internet Society
- The Open Group (includes X/Open and OSF)
- The X Consortium
- EWOS - European Workshop on Open Systems - Europe
- OMG - Object Management Group
- ODMG - Object Database Management Group
- NMF - Network Management Forum
- CASE Data Interchange Format
- The Unicode Consortium
Error Detection and Correction

• A level of noise is unavoidable in most communication channels
  – Even optimized digital system have small but non-zero bit errors rates, typically
    • copper wire: in the order of $10^{-6}$
    • optical fiber: in the order of $10^{-9}$ or less
    • Wireless: in the order of $10^{-3}$ or more
  – acceptability of bit error rates depends on the particular application
    • digital speech transmission - fairly high
    • electronic funds transfer - essentially error-free

• Two basic approaches to error control
  – Both involve the detection of errors

• Automatic retransmission request (ARQ) uses a return channel for a retransmission request whenever errors are detected
  – additional bandwidth
  – widely used in systems that use telephone lines
Error Detection and Correction 2

- Forward error correction (FEC) attempts to correct the errors whenever errors are detected
  - requires additional information to be transmitted and processed
  - Used where a return channel is not available
  - Used retransmission requests are not easily accommodated or
  - Used a large amount of data is sent and retransmission to correct a few errors is very inefficient
  - E.g. in satellite and deep space communications.
  - In audio CD recordings to provide clear sound reproduction even in the presence of smudges and scratches on the disk surface

- Two fundamentals of error detection.
  - Error detection requires redundancy
    - Additional data must be transmitted
    - For a single parity check code of length \( k + 1 \): \( 1/(k + 1) \) redundancy
  - Every error detection technique will fail to detect some errors
    - Always fail to detect errors which convert a valid codeword into another valid codeword
    - For the single parity check code, an even number of transmission errors
Error Detection and Correction 3

- **Basic concept of error detection**
  - Application data is encoded to satisfy a specific pattern or condition
  - Transmission through the communication channel
  - Check the received data to see if the pattern is satisfied
  - If not, an error has occurred, then set an alarm

- **Parity Check Codes**
  - Single Parity Check is the simplest code
  - a single check bit (parity bit) is appended to \( k \) information bits and to form a codeword
  - Even Parity Codeword: the parity check ensures that the total number of 1s in the codeword is even
  - Used in ASCII
    - characters represented by seven bits
    - the eighth bit is a parity bit
Error Detection and Correction 4

• “Linear codes” because the parity bit is calculated as the modulo-2 sum of the information bits

\[ B_{k+1} = b_1 + b_2 + \ldots + b_k \mod 2 \]

where \( b_1, b_2, \ldots, b_k \) are the information bits

<table>
<thead>
<tr>
<th>( 0 + 0 )</th>
<th>( 0 + 1 )</th>
<th>( 1 + 0 )</th>
<th>( 1 + 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

• A Single Parity Check will detect transmission errors in a codeword
  – a single error (the output block contains an odd number of 1s)
  – odd number of errors (also generates an odd number of 1s)

• A Single Parity Bit will fail to detect any error patterns which introduce an even number of errors
  – the output block will have even parity

• A single check bit detects half of all possible error patterns, regardless of the value of \( k \)
• An alternative approach to error detection
  – Calculate and transmit a check sum from the information bits
  – Recalculated the checksum based on the received information
  – Compare the received and recalculated checksums, set an alarm if they disagree

Information accepted if check bits match
Error Detection and Correction 6

- Select an error detection code that reduces the chance that channel will convert one valid codeword into another.

- To minimize the probability of error detection failure, select codewords that they are spaced as far away from each other as possible.

- Code effectiveness depends on the types of errors that are introduced by the channel.

A code with poor distance properties

A code with good distance properties

X codewords

0 noncodewords
Error Models

- The effectiveness of an error detection code is measured by the probability that the system fails to detect an error
  - this probability is a function of the probabilities of various errors
  - probabilities depend on the particular properties of the channel

- Three models of channel errors
  - The Random Error Vector Model
  - The Random Bit Error Model
  - Burst Errors

- Transmit a $n$ bit codeword and define an error vector $\mathbf{e} = (e_1, e_2, \ldots, e_n)$
  $e_i = 1$ if an error occurs in the $i^{th}$ bit else $e_i = 0$
Error Models 2

• The **Random Error Vector Model**
  - all \(2^n\) possible error vectors are equally likely to occur
  - the probability of \(e\) does not depend on the number of errors it contains
  - A single parity check code will fail when the error vector has an even number of 1s
  - And have a probability of error detection failure is \(\frac{1}{2}\)

• The **Random Bit Error Model**
  - bit errors occur independently of each other
  - E.g. Satellite communications channels
  - \(P\) is the probability of an error in a single bit
  - The probability of an error vector that has \(j\) errors is \(p^j (1–p)^{n-j}\)
    - each of \(j\) errors occurs with probability \(p\)
    - each of \(n-j\) correct transmissions occurs with probability \(1-p\)
Error Models 3

\[ p[e] = (1 - p)^n \left( \frac{p}{1 - p} \right)^{w(e)} \]

where the weight \( w(e) \) is the number of 1s in \( e \) (the number of errors)

- In an useful communication channel, the probability of bit error is much smaller than 1 (\( p < \frac{1}{2} \) and \( p/(1-p) < 1 \))
  - with random bit errors the probability of \( e \) decreases as the number of errors (1s) increases
  - fewer bit errors is more likely than an error pattern with more bit errors
  - the channel tends to map a transmitted codeword into binary blocks that are clustered around the codeword

- Results in very low probably of error detection failure
  - E.g. \( 5 \times 10^{-6} \) where \( n = 32 \) and \( p = 10^{-4} \)
Error Models 4

• The two channel error models result in a wide gap in the performance
  – Many communications channels combine aspects of the two model so that errors occur in bursts

• Burst Errors reflect periods of low error rate transmission that are interspersed with periods in which clusters of errors occur
  – The periods of low error rate are similar to the random bit error model
  – The periods of error bursts are similar to the random error vector model
  – The probability of error detection failure for the single parity check code is between those of the two channel models
  – Measurement studies are required to characterize the statistics of burst occurrence
Two-dimensional Parity Checks

- Two-dimensional Parity Checks improves the error detection capability of a single parity check code
  - Arrange the information bits in columns
  - The matrix sets a pattern that all rows have even parity and all columns have even parity

```
1 0 0 1 0 0
0 1 0 0 0 1
1 0 0 1 0 0
1 1 0 1 1 0
1 0 0 1 1 1
```

- Bottom row consists of check bit for each column

**Two-dimensional parity check code**

- At least one row or parity check will fail if one, two, or three errors occur anywhere in the matrix of bits during transmission

- Some patterns with four errors are not detectable
### Two-dimensional Parity Checks 2

<table>
<thead>
<tr>
<th></th>
<th>1 error</th>
<th>2 errors</th>
<th>3 errors</th>
<th>4 errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 0 0 1 0</td>
<td>0</td>
<td>1 0 0 1 0</td>
<td>0</td>
<td>1 0 0 1 0</td>
</tr>
<tr>
<td>0 0 0 0 0</td>
<td>1</td>
<td>0 0 0 0 0</td>
<td>1</td>
<td>0 0 0 0 0</td>
</tr>
<tr>
<td>1 0 0 1 0</td>
<td>0</td>
<td>1 0 0 1 0</td>
<td>0</td>
<td>1 0 0 1 0</td>
</tr>
<tr>
<td>1 1 0 1 1</td>
<td>0</td>
<td>1 0 0 1 1</td>
<td>1</td>
<td>1 0 0 1 1</td>
</tr>
<tr>
<td>1 0 0 1 1</td>
<td>1</td>
<td>1 0 0 1 1</td>
<td>1</td>
<td>1 0 0 1 1</td>
</tr>
</tbody>
</table>

**Arrows indicate failed check bits**

Detectable and undetectable error patterns for two-dimensional code

- The two-dimensional parity check code is another a linear code
  - visually identify error detecting capabilities
  - does not have particularly good performance, there are better linear codes
Internet Checksum

- Several Internet protocols (e.g. IP, TCP) use check bits to detect errors
  - IP calculates a checksum for the contents of the header and includes it in a special field
  - Checksum is recalculated at every router
    - algorithm selected for implementation ease rather than for strength in error-detecting

- The algorithm assumes that the header consists of \( L \) number of 16-bit words, \( b_0, b_1, b_2, \ldots, b_{L-1} \), plus a checksum \( b_L \)

<table>
<thead>
<tr>
<th>Version</th>
<th>Header Length</th>
<th>Type of Service</th>
<th>Total Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Identification</td>
<td>Flags</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Time</td>
<td>Protocol</td>
</tr>
</tbody>
</table>

Source IP Address

Destination IP Address

<table>
<thead>
<tr>
<th>Options</th>
<th>Padding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>
Internet Checksum 2

• Checksum calculation:
  1. Each 16-bit word is treated as an integer, and the \( L \) words are added modulo \( 2^{16}-1 \)
    \[
    x = b_0 + b_1 + b_2 + \ldots + b_{L-1} \mod 2^{16}-1
    \]

  2. The checksum then consists of the negative value (1s compliment) of \( x \):
    \[
    b_L = -x
    \]

  3. The checksum \( b_L \) is then inserted in a dedicated field in the header

• The headers and the checksum satisfy this pattern:
  \[
  0 = b_0 + b_1 + b_2 + \ldots + b_{L-1} + b_L \mod 2^{16}-1
  \]

• Each router can check for errors in each received header by calculating the above equation
Networking hardware

- Includes computers, peripherals, interface cards and other equipment which perform data-processing and communications across a network

- Major types of network hardware
  - Network Interface Cards (NICs)
  - Modems
  - Line Drivers
  - Multiplexers ("Muxs")
  - Channel Service Units/Data Service Units (CSUs-DSUs) Digital Data Sets (DDS)
  - Hubs/Concentrators
  - Multistations Access Units (MAUs)
  - Repeaters
  - Bridges
  - Routers
  - Bridge/Routers ("Brouters")
  - Protocol Converters
  - Ethernet Switches
DCE / DTE

• Data Terminal Equipment (DTE)
  – End user equipment
  – dumb terminal or printer
  – computer, or bridge or router that interconnects local area networks

• Data Communication Equipment (DCE)
  – provides a connection between the DTE and the communication network
  – it terminates and provides clocking for a communication circuit
  – when analog telephone lines are the communication media, the DCE is a modem
  – when the lines are digital, the DCE is a Channel Service Unit/Data Service Unit (CSU/DSU)

• DTE / DCE interfaces are defined by the OSI physical layer
Network Interface Cards

- Provides the physical connection between the network and the computer workstation
  - Most NICs are internal
  - Laptops generally use external LAN adapters connected to the parallel port or network cards that slip into a PCMCIA slot

- The three most common network interface connections are:
  - Ethernet cards, Token Ring, and Local Talk

- Ethernet Cards Connections
  - Coaxial (BNC) or twisted pair cables (RJ-45) or both
  - Some also contain have Attachment Unit Interface (AUI) DB-15 connector for an external transceiver or thick Ethernet viper tap
Network Interface Cards 2

- NICs comply with the Physical Layer and the Medium Access Control (MAC) (e.g. CSMA/CD) sublayer of the Datalink Layer

- Each NIC has a unique MAC address stored into a PROM
  - Standardized numbering scheme developed by the IEEE assigned in blocks to NIC manufacturers

- Network Layer addresses, e.g. IP addresses, are assigned to the device in which the NIC is installed
Network Interface Cards 3

- NICs are a major factor in determining the speed and performance of a network

- Dual cards can support two speeds of data transfer, eg. detecting whether data is arriving at 10Mbps or 100Mbps

- Multiport cards - suited for servers where spare expansion slots are at a premium – can have up to four ports on a single card
• Four methods for NICs to interface with minimum disruption to the CPU:
  – After data enters the NIC from the network

• Bus mastering:
  – NIC processor stores data in the NIC's RAM
  – NIC processor sends data to CPU when the network transmission is complete
  – CPU is not interrupted - the NIC processor has ultimate responsibility for data transfer

• Direct Memory Access (DMA):
  – NIC processor interrupts the CPU
  – CPU stops other tasks and transfers the network data into its RAM

• Programmed I/O (input/output):
  – NIC processor loads the data into a I/O address reserved for network data
  – CPU checks the I/O address for any data
  – If data, CPU transfers the data to its RAM

• Shared memory:
  – NIC processor stores the data in the NIC's RAM
  – NIC processor interrupts the computer's CPU
  – CPU stops other tasks and transfers the network data into its RAM
Digital Modulation

- Voice-grade channels permit signals to be transmitted in a limited frequency band
  - These Bandpass channels pass power in some frequency range with bandwidth $W = f_2 - f_1$
  - Any information-bearing signal must place its power density lies within this band

- A modem performs the basic function of producing a signal that contains the information sequence and that occupies frequencies within the bandpass

- Most convenient way of ensuring this is to use sinusoidal signals $A(t)\cos(2\pi f_c t + \theta(t))$
  - $f_c$ is the carrier frequency
  - $A$ and $\theta$ are the time varying amplitude and phase

- Modulation schemes imbed a binary sequence into the transmitted signal by varying, or `modulating', either the amplitude or the phase with time
• **Amplitude Shift Keying (ASK)**
  – Turn the sinusoidal signal on and off according to the information sequence
  – Demodulator determines the presence or absence of a sinusoid in a given time interval
  – Prone to signal attenuation
  – Used in conjunction with Phase Modulation

• **Frequency Shift Keying (FSK)**
  – Vary the frequency of the sinusoid according to the information sequence
  – Binary 0: \( f_1 = f_c - \epsilon \) and Binary 1: \( f_2 = f_c + \epsilon \)
  – Demodulator determines which of two possible frequencies is present at a given time
  – Used with inexpensive 300 and 1,200 bps modems

• **Phase-Shift Keying (PSK)**
  – Alter the phase of the sinusoid according to the information sequence
  – Binary 0: \( \cos(2\pi f_c t) \) & Binary 1: \( \cos(2\pi f_c t + \pi) \)
  – Equivalent to multiplying the sinusoid by +1 for a 1, and by -1 for a 0
  – Demodulator determines the phase of the received sinusoid in respect to some reference phase
– Differential Phase-Shift Keying (DPSK) is an enhanced form normally used in modems
  - Binary value is determined by the degree of the phase shift from the current bit
  - Eliminates some detection problems with phase change methods
  - Demodulator only needs to determine the pattern of the phase change, which is easier to do
Signal Constellations and Telephone Modem Standards

- A Constellation map of signals has a set of points that relate to the phase and amplitude of a signal.
- Each point is a symbol associated with a bit pattern.

<table>
<thead>
<tr>
<th>Constellation</th>
<th>Levels/pulse</th>
<th>Bits/pulse</th>
<th>Bits per second</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2W</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>4</td>
<td>4W</td>
</tr>
</tbody>
</table>

Copyright 2001 ©Roy M. Wnek. All rights reserved.
Signal Constellations and Telephone Modem Standards 2

- **Quadrature Amplitude Modulation (QAM)**
  - *Up* to four bits are encoded in each signal change
    - a 2400 *baud* modem can attain a data rate of 9,600 bps.
  - CCITT (ITU) V29 specifies an encoding method in which a 1,700-Hz carrier is varied in both phase and amplitude, resulting in 16 possible binary values per signal change
  - A four-bit binary value is represented by the position of the wave when a phase change occurs

- **Trellis-Coded Modulation (TCM)**
  - The 14.2 Kbits/sec V32bis standard has 128 points in its constellation
  - A sending modem only needs to transmit one signal to represent a symbol
  - The receiving modem uses a lookup table to determine the symbol associated with the signal and the desired bit pattern
  - TCM combine error correction coding with the modulation
Signal Constellations and Telephone Modem Standards 3

Modem Standards

<table>
<thead>
<tr>
<th>V.32 bis</th>
<th>4800 bps</th>
<th>QAM 4</th>
<th>2400 pulses/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>9600 bps</td>
<td>Trellis 32</td>
<td>2400 pulses/sec</td>
<td></td>
</tr>
<tr>
<td>14,000 bps</td>
<td>Trellis 128</td>
<td>2400 pulses/sec</td>
<td></td>
</tr>
</tbody>
</table>

| V.34 bis   | 2400-33600 bps | Trellis 960 | 2400-3429 pulses/sec |

⇒ **Baud** is the signal rate of a modem
⇒ bps rating is the number of bits transferred on each signal change
⇒ Encoding schemes allow each signal change represents multiple bits
Modems 1

• Modulators/ demodulators (Modems) are DCE devices connecting computers to the public switched telephone network

• Modulate the digital signals into analog signals that can be transmitted over telephone lines
  – A modem at the other end of the link then demodulates the signals back to digital bits
  – Both modems must use compatible communication standards

• Modems can be internal or external
  – Typical external modem connections:
    • RS-232 from the computer to the modem
    • RJ-11C from the modem to the telephone wall jack
  – Typical internal modem connections:
    • Internal circuit board following a standard bus
    • RJ-11C from the modem to the telephone wall jack
Modems 2

• Modems exchange signals, to establish parameters for a communication session
  – The maximum available signaling rate
  – Type of compression being used

• Telephone communication circuits have an approximately 3,300 Hz bandwidth
  – This range is perfect for voice but it imposes some limitation for data communication
  – Not possible to use the entire voice bandwidth for data
  – Two carrier signals are modulated within the bandwidth range to achieve *duplexing* (modems can talk and listen over separate channels)
  – Guard bands are used to separate the two duplexed channels to prevent crosstalk and corruption
Modems 3

- These parameters allow an effective baud rate is 2,400 baud, or 1,200 baud per duplexed channel
  - Based on the Shannon-Hartley Theorem

- Encoding and compression techniques are used to boost the throughput
  - Quadrature amplitude modulation (QAM) is used to attain bit rates above 2,400 bps
    - E.g. a 9,600 bps rate is attained by encoding a 4-bit code into 16 possible phase and amplitude changes.
  - The trellis encoding algorithm is an extension of QAM that has a higher tolerance for line noise
    - Higher bit rates

**Shannon-Hartley Theorem**

The capacity of a communications channel in bps is:

\[ C = W \cdot \log_2 (s/n + 1) \]

W is the bandwidth in hertz and s/n is the signal-to-noise ratio. It is physically impossible to exceed this limit.
Some CCITT (ITU) encoding standards for boosting the bit rates are:
- Modems typically support multiple standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V.8</td>
<td>Standard for the initial handshaking process</td>
</tr>
<tr>
<td>V.22</td>
<td>1,200 bits/sec full-duplex modem standard</td>
</tr>
<tr>
<td>V.22bis</td>
<td>2,400 bits/sec full-duplex modem standard</td>
</tr>
<tr>
<td>V.28</td>
<td>Defines circuits in RS-232 interface</td>
</tr>
<tr>
<td>V.32</td>
<td>Asynchronous and synchronous 4,800/9,600 bits/sec standard</td>
</tr>
<tr>
<td>V.32bis</td>
<td>Asynchronous and synchronous standard up to 14,400 bits/sec; uses a two-dimensional trellis coding technique with 128 points in a signal constellation</td>
</tr>
<tr>
<td>V.35</td>
<td>High data-rates over combined circuits</td>
</tr>
<tr>
<td>V.32terbo</td>
<td>19.2 Kbits/sec interim standard between V.32bis and V.34, uses a two-dimensional trellis coding technique with 256 or 512 points in a signal constellation</td>
</tr>
<tr>
<td>V.34</td>
<td>Standard for 28 Kbits/sec transmission rates; uses a four-dimensional trellis coding technique with up to 768 points in a signal constellation</td>
</tr>
<tr>
<td>V.90</td>
<td>Standard for 56K modems; actual data speeds received vary depending on line conditions</td>
</tr>
</tbody>
</table>

Speculation that V.90 will be the final analog modem speed standard
Modems 5

- The V.34bis modem comes close to the maximum possible transmission rate under Shannon's formula
  - Shannon's formula then gives a max bit rate of 44880 bits per second with a useful bandwidth of 3400 Hz and a maximum SNR of 40 dB
  - The 56 kbps speed of ITU-T V.90 standard is attained only under particular conditions that do not correspond to the normal telephone channel

- Modem standards provide both error control and data compression capabilities
  - Modems must compress and decompress data on-the-fly
  - A modem must use an error control protocol to support data compression
  - E.g. A MNP-5 modem requires MNP 4 error control protocol and a V.42bis modem requires V.42 error control protocol
- The V.42bis standard uses the Link Access Procedure for Modems (LAPM) protocol for error control
- V.42bis uses the Lempel-Ziv scheme for the information compression prior to transmission
  - This scheme can usually provide compression ratios up to 4x = an apparent modem speedup
- V.42 & MNP-4 can provide error-free connections by filtering out the line noise and automatically retransmitting corrupted data

<table>
<thead>
<tr>
<th>Microcom Networking Protocols</th>
<th>Error correction protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNP 2 to 4</td>
<td>Two error control schemes:</td>
</tr>
<tr>
<td>CCITT V.42</td>
<td>Primarily uses Link Access Procedure for Modems (LAP-M);</td>
</tr>
<tr>
<td></td>
<td>Includes MNP-4 as an alternate</td>
</tr>
<tr>
<td>MNP-5</td>
<td>Data compression protocol; maximum compression ratio is 2:1</td>
</tr>
<tr>
<td>V.42bis</td>
<td>Modem compression using the Lempel Ziv method; maximum compression ratio is 4:1</td>
</tr>
</tbody>
</table>
Network Segments

• A network *Segment* is a length of cable
  – Devices can be attached to the cable
  – Has its own unique address
  – Limit on its length and the number of attached devices

• Large networks are made by combining several individual network segments
  – Using appropriate devices like routers and/or bridges

• When network segments are combined into a single large network, paths or “Routes” exist between the individual network segments

• Routers /bridges keep tables which define how to get to a particular path
  – When a packet arrives, Router/bridge looks at the destination address
  – Determines which network segment the packet is to be transmitted on in order to get to its destination
Concentrators/Hubs

- Concentrators or "hubs" provide a central connection point for cables from workstations, servers, and peripherals.
  - Used in star topologies
  - Often configured with 8, 12, or 24 RJ-45 ports
  - May be configured with other physical connections and multi-port cards within an expandable cage

- Concentrators can be passive or active
  - Passive concentrators pass signals through without any change
  - Active concentrators electrically amplify signals that pass through and are used like repeaters to extend the length of a network

![Diagram of Concentrator/Hub]
Concentrators/Hubs

• Provide full bandwidth to each node
  – Unlike bus topologies where the bandwidth is shared
  – Ports can be buffered to allow packets to be held in case the hub or port is busy
  – Can provide filtering so that bad packets are discarded

• In standard Ethernet, all nodes are connected to the same network segment
  – Traffic on the bus is controlled using CSMA
  – Nodes attach to the hub using UTP
  – Ports on the hub are logically combined using a single backplane
  – Backplanes often runs at a much higher data rate than that of the ports

• Nodes do not contend with other workstations for access to the Hub

• The ports on a hub collectively appear as one single Ethernet segment
Concentrators/Hubs

- Hubs can be stacked or cascaded (using master/slave configurations) together, to add more ports per segment

- Hubs do not count as nodes
  - Better option for adding more workstations than a repeater
  - Retains distance limitations

- Hub may be controlled via SNMP (Simple Network Management Protocol) command
  - Allows network management software to remotely administer and configure the hub
  - Detailed statistics related usage and bandwidth may be available from the hub
Multistations Access Units (MAUs)

- Hub device in a token ring networks
  - Contains an internal ring that is extended to an external ring
  - Provides the connection point for multiple nodes

- MAUs automatically bypass failed or absent network cards to maintain the ring

- Multiple MAUs can be daisy-chained in a loop to expand the network
  - Maintains the ring configuration
Repeaters

• Signal quality deteriorates during transmission along a cable
  – Eventually becoming undetectable/mis-read

• A repeater is a device that electrically amplifies and provides retiming to network signal
  – Operates on incoming signal received from one segment and rebroadcasting them to all other attached segments
  – Can be separate devices or
  – Can be incorporated into a concentrators

• Repeaters are used to connect multiple network segments together
  – allows the total cable length to exceed the standards set for the cable type
Repeaters operate at the Physical Layer
Repeaters

- The repeater counts as a single node against the maximum node limit per segment
  - Ethernet standard of 30 for thin coax
  - Example, a thin coax segment may have 29 computers and 1 repeater
  - or a ThickWire segment can have 20 repeaters and 80 computers

- Disconnecting one side of a repeater effectively isolates the associated segments from the network
  - In the event of failures or fault conditions.

- Repeaters simply extend network distance limitations
  - Does not increase bandwidth or network data rate
  - Does not store or buffer data
  - The traffic generated on one segment is propagated onto the other segment
  - Propagates any errors in data transmission
  - In effect, increases total traffic on segments
  - If the network segments are already heavily loaded, it's not a good idea to use a repeater
Repeater

• Other limits on repeater use
  – Cannot loop back to itself (must be unique single paths)
  – Limits on the number of repeaters
  – Cannot be administered or controlled via remote access

• Example application:
  Used in a Star topology LAN with UTP
  – UTP length limit for cable is 100 meters
  – Each workstation is connected to a multi-port active concentrator
  – The concentrator regenerates signals that pass through it allowing for the total length of cable on the network to exceed the 100 meter limit
Bridges 1

- Allows segmentation of a large network into two smaller, more efficient networks
  - Used to connect different types of cabling, or physical topologies.
  - May be used between networks with the different data link protocols

- Originally designed to interconnect Ethernet segments together

- Protocol independence allows bridges to store and forward packets for any data link protocol without regard for information content

- Keeps information flowing on both sides of the network, but unlike a repeater, does not allow unnecessary traffic
Bridges 2

• Each network segment must have a unique address in order for the bridge to be able to forward packets from one segment to the other.

• *Transparent Bridges* (IEEE 802.1 D) make all routing decisions:
  – Operate at the Data Link Level
  – Said to be invisible to network workstation
  – Automatically initialize themselves and configure their own routing information after enabling.

• A new class of bridges, *Etherswitches*, offer limited filtering:
  – Read only enough of a packet to determine the source and destination addresses for retransmission purposes
  – Do not read remainder of packet and do not filter out illegal or bad packets
    • Unless the problem is evident in the first few bytes
    • Speeds throughput
  – Weight speed against need to filter.
Bridges 3

- Bridges operate at the Data Link Layer
- Bridges can be used to:
  - To expand the distance or number of nodes for the entire network
  - To reduce traffic bottlenecks caused by an excessive number of attached nodes
  - To connect different cabling or physical topologies (must be used between networks with the same network layer protocol)
Functions of Bridges

- Learn about the network and the routes during initialization

- Monitor traffic on both sides of the network and determine the address of each node on both sides of the bridge
  - Store the source address of each incoming packet
  - Builds a table of node addresses & segment locations
  - Use this table to determine which segment incoming packets should be forwarded to
  - The size of this table is significant, especially if the network has a large number of nodes

- Inspect each packet and, if necessary, broadcast it on the other side of the network
  - Read an entire packet before they compare it to their address list;
  - Done to automatically filtered out bad packets
    - Short or illegal packets
    - Packets with bad CRCs
    - Packets with late collisions

- Manage the traffic to maintain optimum performance on both sides of the network
  - “Store & forward” individual packets
Bridges 4

• Advantages of bridges:
  – Increase the number of attached workstations and network segments
  – Possible to interconnect different segments which use different Data Link protocols
  – Transparent to higher level protocols
  – Can reduce traffic on other segments
  – Increase fault tolerance by isolating faulty segments and reconfiguring paths if failure
  – Make the network easier to maintain by subdividing the LAN into smaller segments
  – Most allow remote access and configuration with Simple Network Management Protocol (SNMP)
  – Loops can be used (redundant paths) if using spanning tree algorithm

• Disadvantages of bridges:
  – Packet buffering introduces network delays
  – Broadcasts are forwarded to every segment
  – May overload during periods of high traffic
  – Packet modification processing causes delays when bridges accommodate different protocols
  – Not efficient with complex networks
  – Redundant paths to other networks are not used
    • (Useful if the major path was overloaded)
  – Shortest path is not always chosen by spanning tree algorithm
Bridges Applications

• Ideally used in environments where:
  – A number of well defined workgroups
  – Each operating more or less independent of each other
  – Occasional access to nodes outside of their network segment.

• Offers no performance improvements where:
  – Diverse or scattered workgroups
  – Most access occurs outside of a local segment

• Ideally, locate servers and workstations which need access to it on the same segment
  – Minimizes traffic on the other segment
  – Avoids the delay incurred by the bridge
Spanning Tree Algorithm

• The "learning" capabilities of bridges could define network loops
  – Multiple pathways to a segment
  – Multiple perspectives of network configuration
  – Each bridge has its own unique picture of the network
  – Based on what it sees from passing packets

• Network loops are deadly to bridged networks
  – Could cause packets to be sent on incorrect segments
  – Packets could loop around the network, being forwarded on, eventually arriving back, only to be forwarded on, etc..
  – Resulting in network flooding

• The **Spanning Tree Algorithm** is a specification which describes how bridges are to communicate with one another in order to avoid network loops
Spanning Tree Algorithm

- Bridges supporting the Spanning Tree Algorithm establish singular paths between them to avoid loops or multiple pathways from being defined
  - By passing packets called BPDUs between each other
  - A bridge which creates a loop or is on a path which is not being used may be totally excluded from use by other bridges

- The Spanning Tree Algorithm is a continuous process so that if a bridge fails, the remaining devices reconfigure their tables to allow each segment to be reached with new pathways

Network port 2 on Bridge #4 is shut off by the Spanning Tree Algorithm to avoid a bridge loop.
Ethernet Switches

• An expansion of the concept of Ethernet bridging

• Two basic LAN switch architectures:
  – Cut-through
    • Switch only examines destination address an arriving packet forwarding it to destination segment
    • This approach once held speed advantage
  – Store-and-forward
    • Switch accepts and analyzes the entire packet before forwarding it to its destination
    • Takes more time to examine the entire packet, but it allows the switch to catch certain packet errors and keep them from propagating through the network
    • With current faster switches, the speed difference between these two approaches is minimal
  – Hybrid switches
    • mix both cut-through and store-and-forward architectures
Ethernet Switches 2

• Both cut-through and store-and-forward switch allow network segmentation

• Segmentation separates a network into separate collision domains and is the basic reason for using switches
  – breaks one network into many small networks so the design rules of distance and repeater limitations are restarted
  – isolates traffic and reduces collisions relieving network congestion
  – each segment attached to switch can better performance
    • has a full 10 Mbps of bandwidth shared by fewer users
    • (as opposed to hubs that only allow sharing of bandwidth from a single Ethernet)

• Replacing hubs with switches in networks
  – Switches are self learning (install like hubs)
  – Operate on the same layer as a hub (no protocol issues)
  – Switches are somewhat more expensive
  – Not effective in all situations
- Segmentation

1 Collision Domain

2 Collision Domains
Ethernet Switches 4

- All switches add small latency delays to packet processing, deploying switches unnecessarily can actually slow down network performance
  - benefits of switching vary by network
  - understanding traffic patterns is critical to designing switched networks
  - the goal is to eliminate (or filter) as much traffic as possible

- Networks that are not congested can actually be negatively impacted by adding switches

- A switch installed in a location where it forwards almost all the traffic it receives will be as effective as one that filters most of the traffic
Ethernet Switches 5

- Good Candidates for improved performance with switching
  - Utilization more than 35%
    - Utilization load is the amount of total traffic as a percent of the theoretical maximum for the network type, 10 Mbps in Ethernet, 100 Mbps in Fast Ethernet
  - Collision rates more than 10%
    - The collision rate is the number of packets with collisions as a percentage of total packages

- Network response times suffers as the load on the network increases, and under even moderately heavy loads small increases in user traffic often results in significant decreases in performance

- Network utilities found on most server operating systems can identify utilization and collision rates
  - both peak and average statistics should be considered
A network composed of a number of switches linked together via uplinks is termed a "collapsed backbone" network.

Switches offer high-speed links:
- FDDI, Fast Ethernet or ATM can be used to link the switches together or to give added bandwidth to particularly important servers that get a lot of traffic.
Routers 1

- Routers are similar to bridges, except routers are protocol dependent
  - Select the best path to route a message, based on the destination address and origin
  - Translate information from networks
    - Different topologies
    - Different data link protocols

- Routers functioning is based on the particular details of the protocols that they support
  - Allows routers to do more sophisticated packet forwarding and can provide a greater reduction in network traffic by filtering extraneous packets
Routers 2

- Routers operate at the Network Layer
  - Provide logical separation to networks
    - e.g. a TCP/IP router can segment a network based on IP subnets
  - Filtering at this level takes longer than a bridge which only looks at the Data Link layer

- Remote administration and configuration via SNMP
Router Features

- Routers store the addresses of computers, bridges, and other routers on the network.
- Filter out unnecessary traffic by passing packets only to necessary segments.
- Can direct network traffic:
  - Monitor traffic on the entire network to determine which sections are busiest.
  - Smart enough to know when to direct traffic along alternate routes to prevent head-on collisions.
- Routers are usually more expensive and require additional configuration set-up.
Router Applications

• Using a router as the main *Gateway* from a local network to the Internet

• Providing a *Firewall* as barrier in front of a network
  – Configure the router with access lists defining which protocols and nodes have access
  – Prevents unwanted packets from either entering or leaving the network
  – Enforces security by restricted access to either internal or external nodes
  – e.g. external nodes can be allowed IP access to a selected local nodes, but other nodes (which may contain sensitive data) are protected
  – Internal workstations may also be prevented from access selected servers