



**Postgraduate Diploma  
in  
Strategic Business Information Technology**

**Module 4  
Computer Networking and Management**

**Chapter 5  
The Data Link Layer**

© NCC Education Limited, 2003

## Modification History

Revision	Date	Revision Description
V1.0	January 2003	For issue

© NCC Education Limited, 2003

**All Rights Reserved**

*The copyright in this document is vested in NCC Education Limited. The document must not be reproduced by any means, in whole or in part, or used for manufacturing purposes, except with the prior written permission of NCC Education Limited and then only on condition that this notice is included in any such reproduction.*

*Information contained in this document is believed to be accurate at the time of publication, but no liability whatsoever can be accepted by NCC Education Limited arising out of any use made of this information.*

### **Trademarks**

*NCC Education acknowledge that the trademarks and registered trademarks of products mentioned in this material are held by the companies producing them. Use of a term in this material should not be regarded as affecting the validity of any trademark or service mark.*

*Copyright of any screen captures in this material are the property of the software's manufacturer.*

*This material may contain some clipart, which is copyright to the Corel Corporation.*

# Contents

Introduction – The Data Link Layer.....	5
Link Layer and Local Area Networks.....	5
Reliable Delivery.....	7
Flow Control.....	7
Error Detection.....	7
Error Correction.....	8
Link Layer Implementation.....	8
Error Detection and Correction Techniques.....	9
Error Detection and Correction Scenario.....	9
Parity Checks.....	10
One-Bit Even Parity.....	10
Internet Checksum Technique.....	10
Cyclic Redundancy Check (CRC).....	11
Multiple Access Links and Protocols.....	12
Summary.....	14



## Introduction – The Data Link Layer

### Visual 1 (NCC Course Title Visual)

### Visual 2

### The Data Link Layer

<p><b>Our goals:</b></p> <ul style="list-style-type: none"> <li>□ Understand principles behind data link layer services:                             <ul style="list-style-type: none"> <li>○ error detection, correction</li> <li>○ sharing a broadcast channel: multiple access</li> <li>○ link layer addressing</li> <li>○ reliable data transfer, flow control: <i>done!</i></li> </ul> </li> <li>□ Instantiation and implementation of various link layer technologies</li> </ul>	<p><b>Overview:</b></p> <ul style="list-style-type: none"> <li>□ Link layer services</li> <li>□ Error detection, correction</li> <li>□ Multiple access protocols and LANs</li> <li>□ Link layer addressing, ARP</li> <li>□ Specific link layer technologies:                             <ul style="list-style-type: none"> <li>○ Ethernet</li> <li>○ hubs, bridges, switches</li> <li>○ IEEE 802.11 LANs</li> <li>○ PPP</li> <li>○ ATM</li> </ul> </li> </ul>
--	--

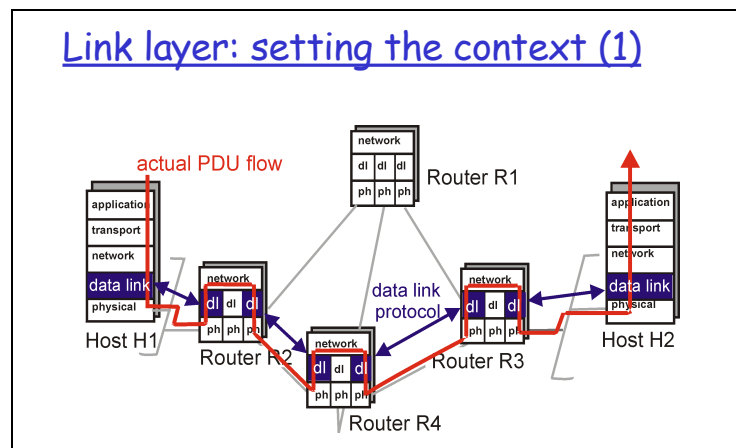
## Link Layer and Local Area Networks

In this chapter we examine the data link layer – its services, the principles underlying its operation, and a number of important data link layer protocols. We learn that the basic service of the data link layer is to move a network-layer datagram from one node (host or router) to an adjacent node.

We investigate the different services a link layer protocol can provide in addition to this basic service, including link access services, delivery services, flow control services and transmission services. These differences are due in part to a wide variety of link types over which data link protocols must operate.

We examine error detection and correction, services that are often present in link-layer protocols. We investigate multiple access protocols, commonly used in LANs (local area networks).

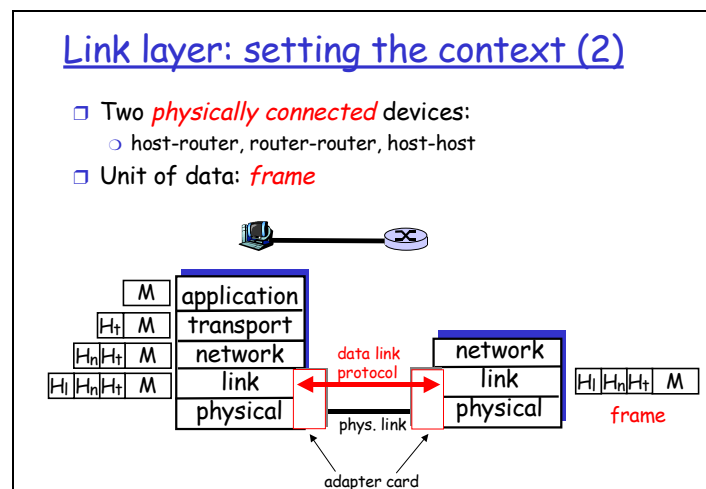
### Visual 3



Almost all link-layer protocols encapsulate each network-layer datagram within a link-layer frame before transmission onto the link. A frame consists of a data field, in which the network-layer datagram is inserted, and a number of header fields. (A frame may also include trailer fields; however, we will refer to both header and trailer fields as header fields.)

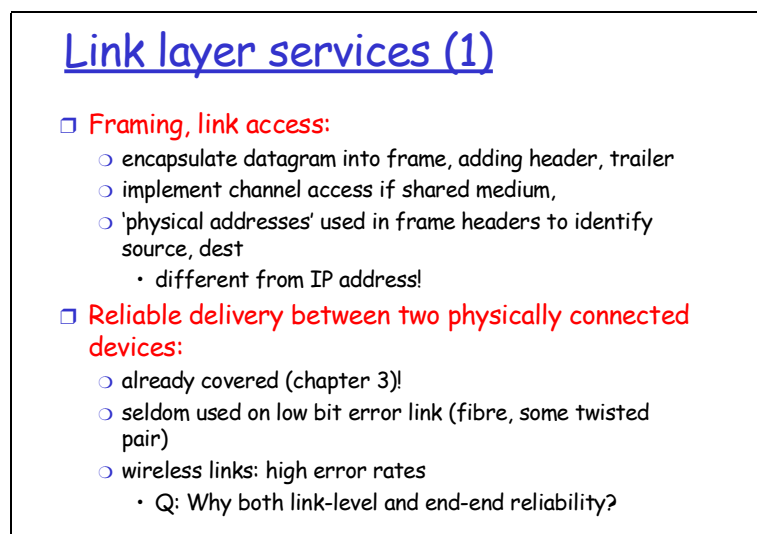
A data-link protocol specifies the structure of the frame, as well as a channel access protocol that specifies the rules by which a frame is transmitted onto the link. For point-to-point links that have a single sender on one end of the link and a single receiver at the other end of the link, the link-access protocol is simple (or non-existent) – the sender can send a frame whenever the link is idle. The more interesting case is when multiple nodes share a single broadcast link – the so-called multiple access problem.

#### Visual 4



Here, the channel access protocol serves to coordinate the frame transmissions of the many nodes; Frame headers also often include fields for a node's so-called physical address, which is completely distinct from the node's network layer (for example, IP) address.

#### Visual 5

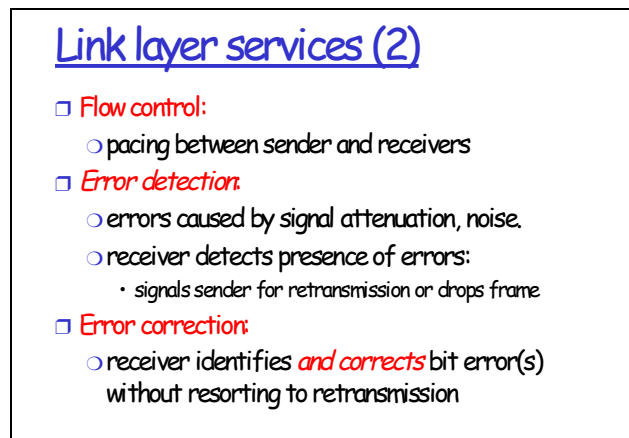


## Reliable Delivery

When a link-layer protocol provides reliable-delivery service, it guarantees to move each network-layer datagram across the link without error. Recall that certain transport-layer protocols (such as TCP) also provide a reliable-delivery service. Similar to a transport-layer reliable-delivery service, a link-layer reliable-delivery service is achieved with acknowledgments and retransmissions.

A link-layer reliable-delivery service is often used for links that are prone to high error rates, such as a wireless link. The goal is to correct an error locally, on the link where the error occurs, rather than forcing an end-to-end retransmission of the data by a transport-layer or application-layer protocol. However, link-layer reliable delivery can be considered an unnecessary overhead for low bit-error links, including fibre, coax, and many twisted-pair copper links. For this reason, many of the most popular link-layer protocols do not provide a reliable-delivery service.

### Visual 6



## Flow Control

The nodes on each side of a link have a limited amount of frame buffering capacity. This is a potential problem, as a receiving node may receive frames at a rate faster than it can process the frames over some time interval. Without flow control, the receiver's buffer can overflow and frames can get lost. Similar to the transport layer, a link-layer protocol can provide flow control in order to prevent the sending node on one side of a link from overwhelming the receiving node on the other side of the link.

## Error Detection

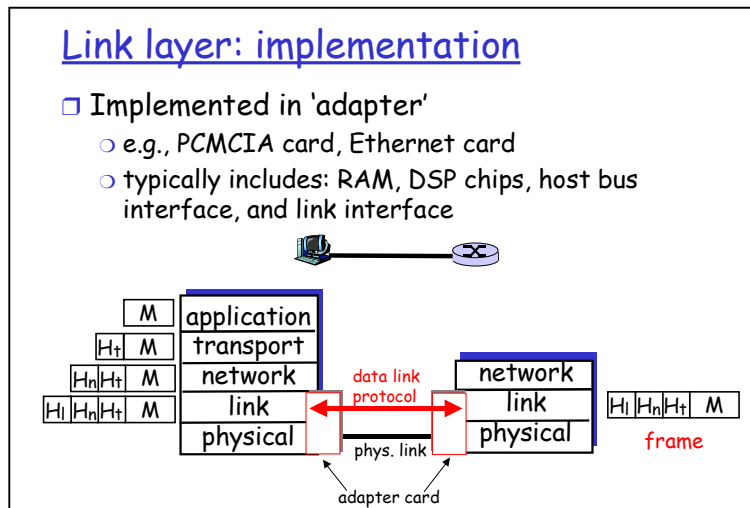
A node's receiver can incorrectly decide that a bit in a frame is zero when it was transmitted as a one, and vice versa. Such bit errors are introduced by signal attenuation and electromagnetic noise. Because there is no need to forward a datagram that has an error, many link-layer protocols provide a mechanism to detect the presence of one or more errors. This is done by having the transmitting node set error-detection bits in the frame, and having the receiving node perform an error check. Error detection is a very common service among link-layer protocols.

## Error Correction

Error correction is similar to error detection, except that a receiver cannot only detect whether errors have been introduced in the frame but can also determine exactly where in the frame the errors have occurred (and hence correct these errors).

## Link Layer Implementation

### Visual 7



For a given communication link, the link-layer protocol is, for the most part, implemented in an adapter. An adapter is a board (or a PCMCIA card) that typically contains RAM, DSP chips, a host bus interface, and a link interface. Adapters are also commonly known as network interface cards or NICs.

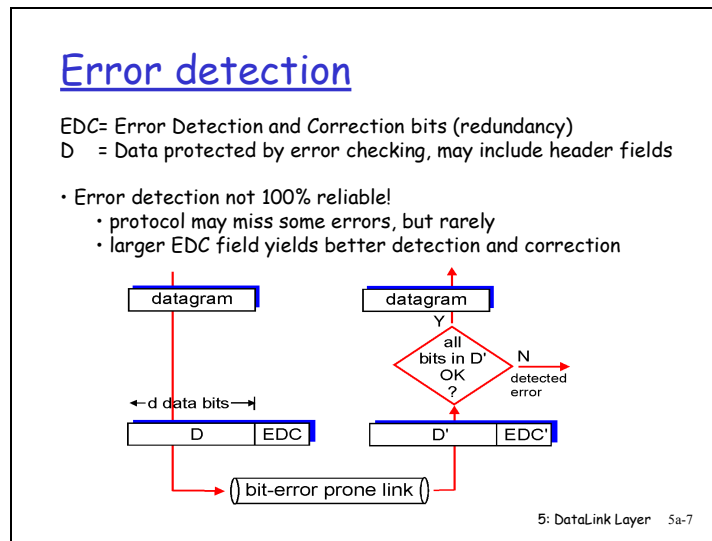
The network layer in the transmitting node (that is, a host or router) passes a network-layer datagram to the adapter that handles the sending side of the communication link. The adapter encapsulates the datagram in a frame and then transmits the frame into the communication link. At the other side, the receiving adapter receives the entire frame, extracts the network-layer datagram, and passes it to the network layer.

If the link-layer protocol provides:

- error detection, then it is the sending adapter that sets the error detection bits and it is the receiving adapter that performs error checking;
- reliable delivery, then the mechanisms for reliable delivery (for example, sequence numbers, timers, and acknowledgments) are entirely implemented in the adapters;
- random access, then the random access protocol is entirely implemented in the adapters.

## Error Detection and Correction Techniques

Visual 8



Error detection and correction services are also often offered at the transport layer as well.

### Error Detection and Correction Scenario

The receiver’s challenge is to determine whether or not D’ is the same as the original D, given that it has only received D’ and EDC’.

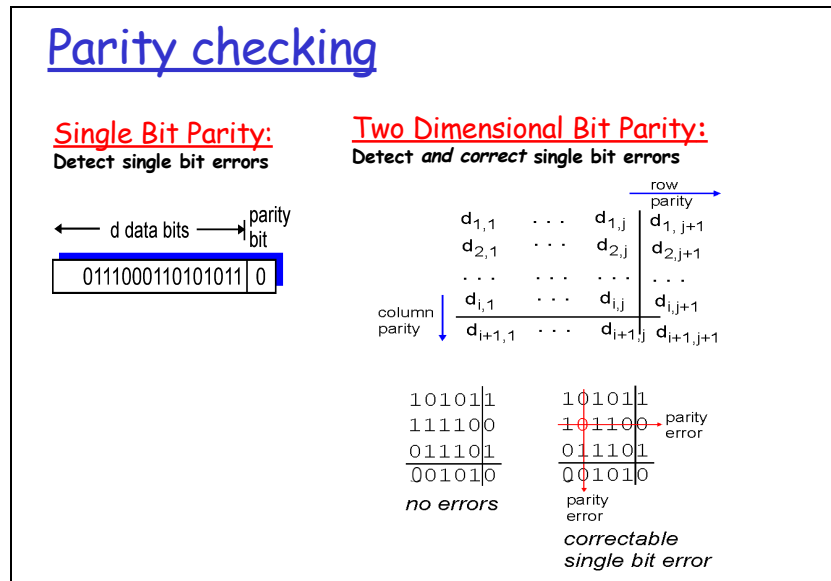
Error-detection and correction techniques allow the receiver to sometimes, but not always, detect that bit errors have occurred. Even with the use of error-detection bits there will still be a possibility that undetected bit errors will occur, that is, that the receiver will be unaware that the received information contains bit errors.

As a consequence, the receiver might deliver a corrupted datagram to the network layer, or be unaware that the contents of some other field in the frame’s header have been corrupted. We thus want to choose an error-detection scheme so that the probability of such occurrences is small.

Generally, more sophisticated error-detection and correction techniques (that is, those that have a smaller probability of allowing undetected bit errors) incur a larger overhead – more computation is needed to compute and transmit a larger number of error-detection and correction bits.

## Parity Checks

Visual 9



Perhaps the simplest form of error detection is the use of a single parity bit. Suppose that the information to be sent,  $D$  has  $d$  bits. In an even parity scheme, the sender simply includes one additional bit and chooses its value such that the total number of 1s in the  $d + 1$  bits (the original information plus a parity bit) is even. For odd parity schemes, the parity bit value is chosen such that there are an odd number of 1s.

### One-Bit Even Parity

Receiver operation is also simple with a single parity bit. The receiver need only count the number of 1s in the received  $d + 1$  bits. If an odd number of 1-valued bits are found with an even parity scheme, the receiver knows that at least one bit error has occurred. More precisely, it knows that some odd number of bit errors have occurred.

However, measurements have shown that rather than occurring independently, errors are often clustered together in 'bursts'. Under burst error conditions, the probability of undetected errors in a frame protected by single-bit-parity can approach 50 percent. Clearly, a more robust error-detection scheme is needed.

### Internet Checksum Technique

In checksumming techniques, the  $d$  bits of data are treated as a sequence of  $k$ -bit integers. One simple checksumming method is to simply sum these  $k$ -bit integers and use the resulting sum as the error detection bits. The so-called Internet checksum is based on this approach – bytes of data are treated as 16-bit integers and their ones-complement sum forms the Internet checksum.

The receiver calculates the checksum over the received data and checks whether it matches the checksum carried in the received packet. RFC 1071 discusses the Internet checksum algorithm and its implementation in detail. In the TCP/IP protocols, the Internet checksum is computed over all fields (header and data fields included). In other protocols, for example, XTP, one checksum is computed over the header, with another checksum computed over the entire packet.

## Visual 10

### Internet checksum

**Goal:** Detect 'errors' (e.g. flipped bits) in transmitted segment (note: used at transport layer *only*)

<p><b>Sender:</b></p> <ul style="list-style-type: none"> <li>□ Treat segment contents as sequence of 16-bit integers</li> <li>□ Checksum: addition (1's complement sum) of segment contents</li> <li>□ Sender puts checksum value into UDP checksum field</li> </ul>	<p><b>Receiver:</b></p> <ul style="list-style-type: none"> <li>□ Compute checksum of received segment</li> <li>□ Check if computed checksum equals checksum field value:             <ul style="list-style-type: none"> <li>○ NO - error detected</li> <li>○ YES - no error detected - <i>but maybe errors nonetheless? More later</i></li> </ul> </li> </ul> <p>....</p>
--	---

## Cyclic Redundancy Check (CRC)

## Visual 11

### Checksumming: cyclic redundancy check

- View data bits,  $D$ , as a binary number
- Choose  $r+1$  bit pattern (generator),  $G$
- Goal: choose  $r$  CRC bits,  $R$ , such that
  - $\langle D, R \rangle$  exactly divisible by  $G$  (modulo 2)
  - receiver knows  $G$ , divides  $\langle D, R \rangle$  by  $G$ . If non-zero remainder: error detected!
  - can detect all burst errors less than  $r+1$  bits
- Widely used in practice (ATM, HDCL)

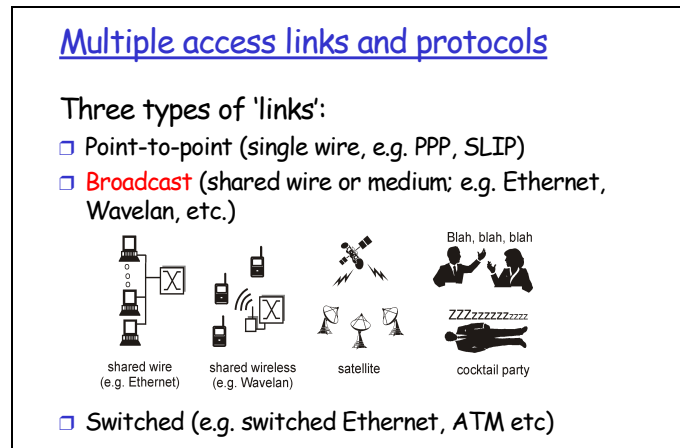
$\overleftarrow{\hspace{1.5cm}} \text{d bits} \hspace{0.5cm} \overleftarrow{\hspace{1.5cm}} \text{r bits} \hspace{0.5cm} \overrightarrow{\hspace{1.5cm}}$   
D: data bits to be sent | R: CRC bits *bit pattern*  
 $D * 2^r \text{ XOR } R$  *mathematical formula*

An error-detection technique used widely in today's computer networks is based on cyclic redundancy check (CRC) codes. CRC codes are also known as polynomial codes, since it is possible to view the bit string to be sent as a polynomial whose coefficients are the 0 and 1 values in the bit string, with operations on the bit string interpreted as polynomial arithmetic.

CRC codes operate as follows. Consider the  $d$ -bit piece of data,  $D$ , that the sending node wants to send to the receiving node. The sender and receiver must first agree on an  $r + 1$  bit pattern, known as a generator, that we will denote as  $G$ . We will require that the most significant (leftmost) bit of  $G$  be a 1. The key idea behind CRC codes is shown in the above visual. For a given piece of data,  $D$ , the sender will choose  $r$  additional bits,  $R$ , and append them to  $D$  such that the resulting  $d + r$  bit pattern (interpreted as a binary number) is exactly divisible by  $G$  using modulo 2 arithmetic. The process of error checking with CRCs is thus simple: The receiver divides the  $d + r$  received bits by  $G$ . If the remainder is nonzero, the receiver knows that an error has occurred; otherwise the data is accepted as being correct.

## Multiple Access Links and Protocols

Visual 12

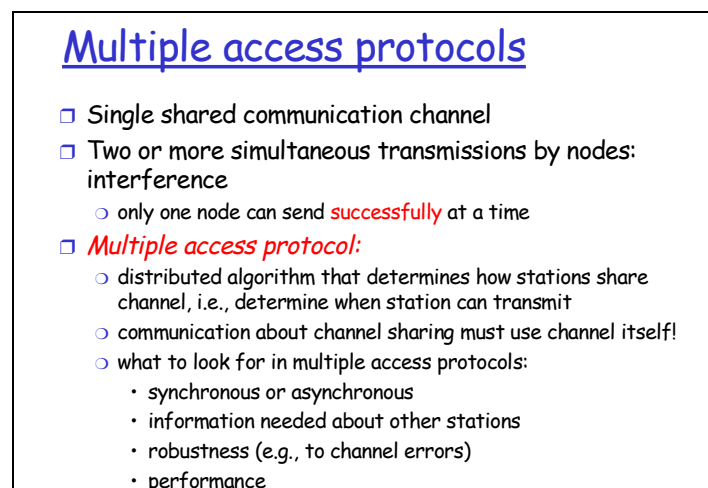


There are two types of network links – point-to-point links, and broadcast links. A point-to-point link consists of a single sender on one end of the link, and a single receiver at the other end of the link. Many link-layer protocols have been designed for point-to-point links; PPP (the point-to-point protocol) and HDLC are two such protocols.

The second type of link, a broadcast link, can have multiple sending and receiving nodes all connected to the same, single, shared broadcast channel. The term broadcast is used here because when any one node transmits a frame, the channel broadcasts the frame and each of the other nodes receives a copy.

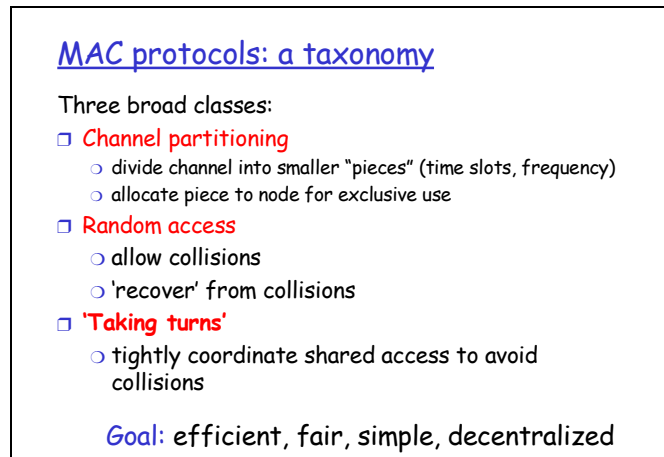
Ethernet is probably the most widely deployed broadcast link technology. In this section we will take a step back from specific link-layer protocols and first examine a problem of central importance to the data-link layer: how to coordinate the access of multiple sending and receiving nodes to a shared broadcast channel – the so-called multiple access problem. Broadcast channels are often used in local area networks (LANs), networks that are geographically concentrated in a single building (or on a corporate or university campus). Thus, we will also look at how multiple access channels are used in LANs at the end of this section.

Visual 13



Computer networks similarly have protocols – so-called multiple access protocols – by which nodes regulate their transmission onto the shared broadcast channel. Multiple access protocols are needed in a wide variety of network settings, including both wired and wireless local area networks, and satellite networks. In practice, hundreds or even thousands of nodes can directly communicate over a broadcast channel.

#### Visual 14



We are all familiar with the notion of broadcasting, as television has been using it since its invention. But traditional television is a one-way broadcast (that is, one fixed node transmitting to many receiving nodes), while nodes on a computer network broadcast channel can both send and receive. Perhaps a more apt human analogy for a broadcast channel is a cocktail party, where many people gather together in a large room (the air providing the broadcast medium) to talk and listen. A second good analogy is something many readers will be familiar with – a classroom, where teacher(s) and student(s) similarly share the same, single, broadcast medium. A central problem in both scenarios is that of determining who gets to talk (that is, transmit into the channel), and when.

As humans, we have evolved an elaborate set of protocols for sharing the broadcast channel:

“Give everyone a chance to speak.”

“Don’t speak until you are spoken to.”

“Don’t monopolize the conversation.”

“Raise your hand if you have a question.”

“Don’t interrupt when someone is speaking.”

“Don’t fall asleep when someone else is talking.”

## Summary

### Visual 15

#### Summary

- The data link layer - services, principles and protocols
- Link layer implementation
  - error detection, reliable delivery, random access
- Error detection and correction techniques
- Parity checks and cyclic redundancy
- Multiple access links and protocols