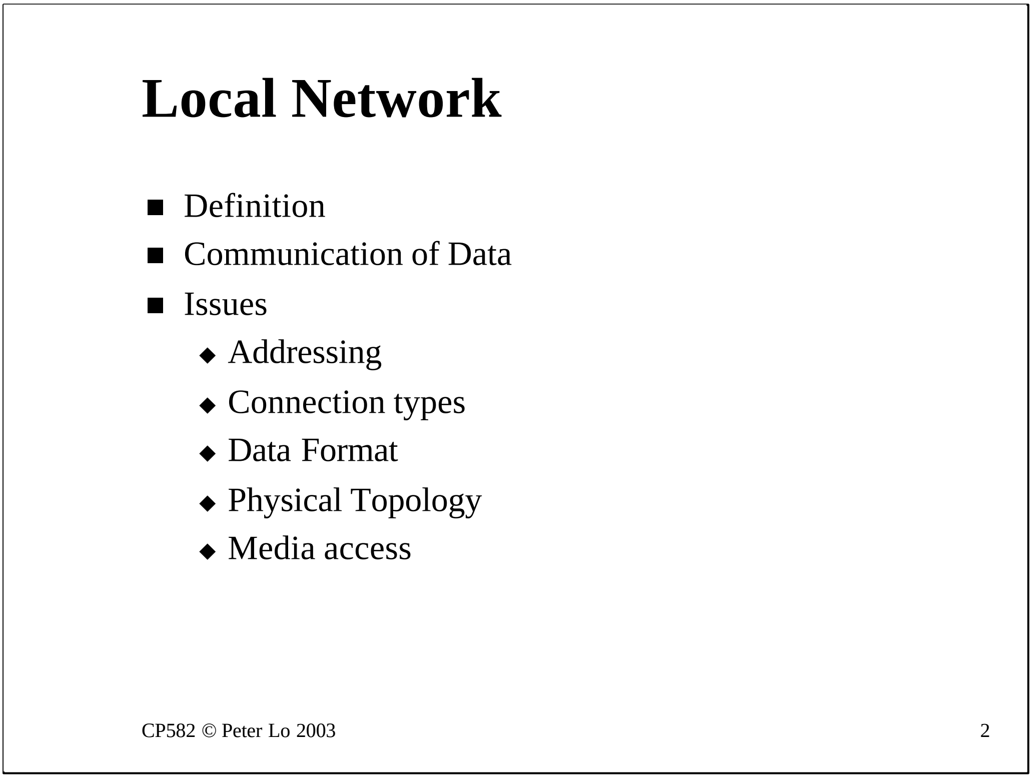
Local Delivery

Peter Lo



Local Network

- Definition
- Communication of Data
- Issues
  - ◆ Addressing
  - ◆ Connection types
  - ◆ Data Format
  - ◆ Physical Topology
  - ◆ Media access

Definition of “Local Network”

How local is local? To define a network as local we need to think about addressing rather than distance. Although in all our labs the local network is just the network in the lab (i.e. “local” = “close”) it would also be reasonable to talk about a satellite link as a local network. The real issue is to consider how you identify the other “nodes” on the network.

If you can identify another node with a simple, one part, address then the network is local.

Consider students in lectures. Within this lecture “Susie James” should identify a student. This lecture is a “local network”. To refer to a student in some other lecture needs a more complex description “T127/James Smith”

Communication of Data

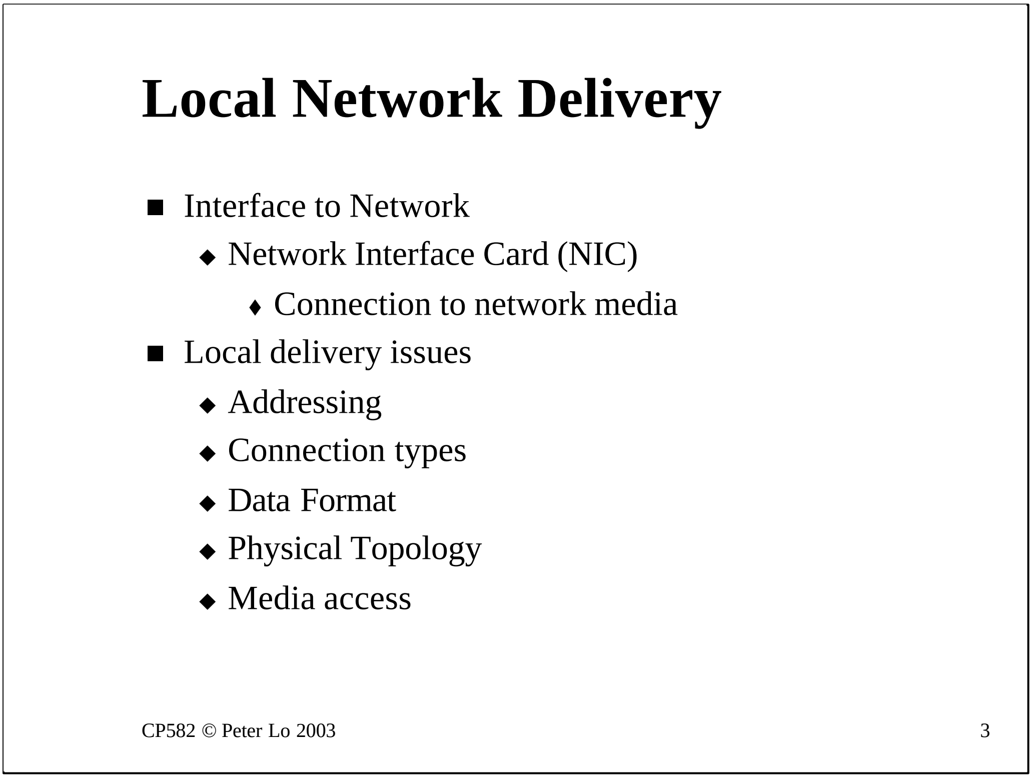
In computer networks this is the whole object of the exercise

Issues for Local Networks

These will be discussed in detail today

Analogies

This unit will make a lot of use of analogies. A telephone system and a mail system are both good analogies of a computer network as will be seen in the next few slides.



Local Network Delivery

- Interface to Network
  - Network Interface Card (NIC)
    - Connection to network media
- Local delivery issues
  - Addressing
  - Connection types
  - Data Format
  - Physical Topology
  - Media access

Local computer networks

Moving away from analogies we are going to look at actual computer networks.

Connecting a computer to a network

A computer that is not connected to a network (A “stand alone” computer) needs something extra to implement the network connection. This extra component is the Network Interface Card. (NIC)

It has two “interfaces” - a connector into the computer and a connector into the network and the components on the card are designed to relay messages back and forth between the two.

Connection to network media

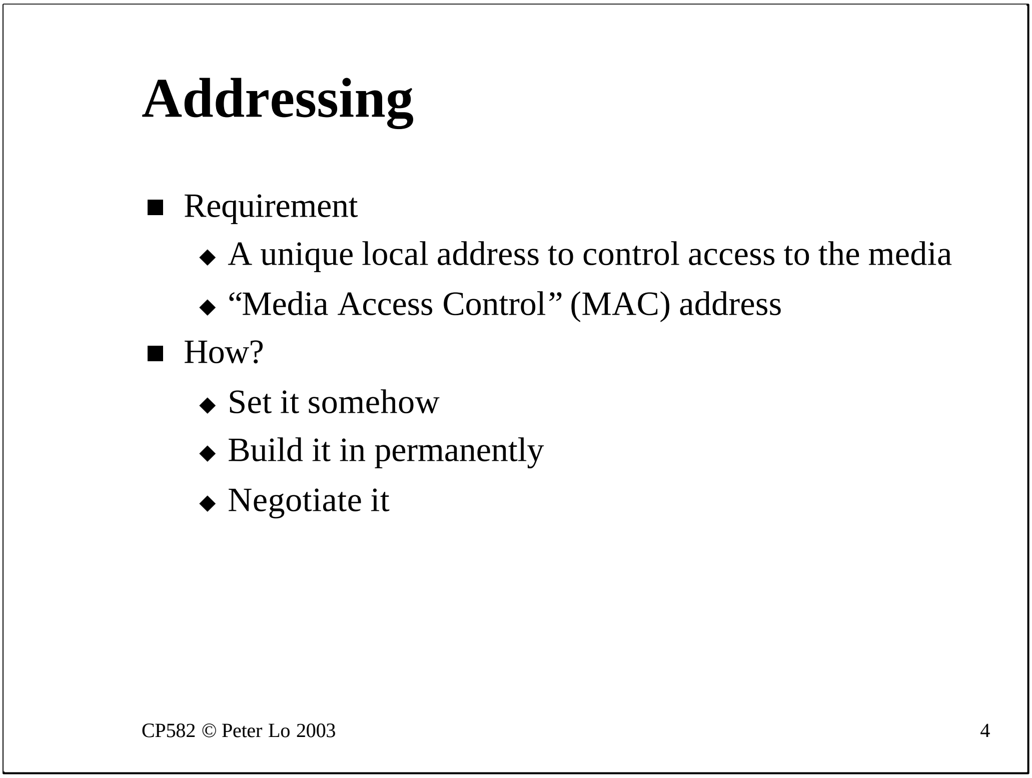
This is the business end of the NIC. There are many kinds of network media

• cables of various types

• radio links

• infra-red links, etc

and each will require its own specially designed NIC



Addressing

- Requirement
  - A unique local address to control access to the media
  - “Media Access Control” (MAC) address
- How?
  - Set it somehow
  - Build it in permanently
  - Negotiate it

Remember, the address only **needs** to be unique locally. How might the NIC be given an address?

Set it somehow

A technician or administrator would be able to set the address of each NIC in some way. They would have a list or a database to make sure that each was unique. **But**

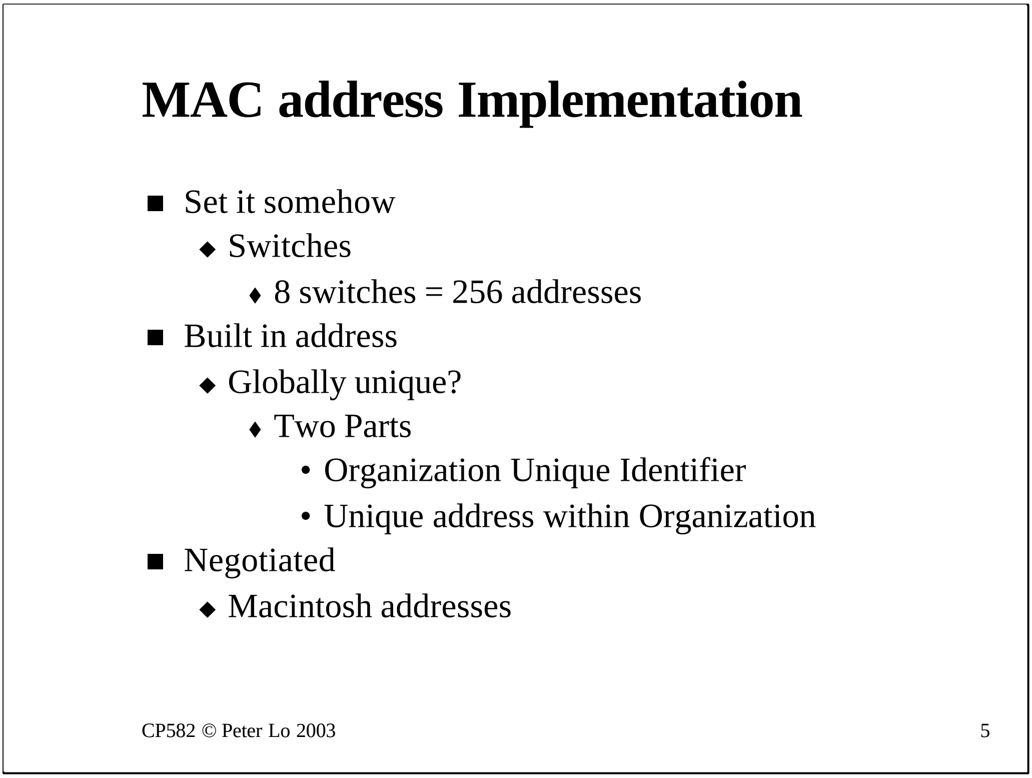
- What if they made a mistake?
- What if you moved your computer to a different local network?

Build it in permanently

The address is “fused” into the NIC. Now we really need to think carefully about what happens when we move our computer. There is no way to resolve a clash if it arises because the address is built right in so we need to think about NIC addresses that are **globally** unique!!

Negotiate it

Maybe the right compromise is to automate the setting of the address and let the NIC set its own address after making sure that the address it is choosing is not going to clash *on this particular local network*



MAC address Implementation

- Set it somehow
  - Switches
    - 8 switches = 256 addresses
- Built in address
  - Globally unique?
    - Two Parts
      - Organization Unique Identifier
      - Unique address within Organization
- Negotiated
  - Macintosh addresses

Set it somehow

Using switches on the NIC but there is a limit to how many switches you can expect someone to set accurately and this may lead to a limit to how many addresses you can have.

Arcnet NICs have 8 switches and this means that there can only be 256 computers on a local Arcnet network.

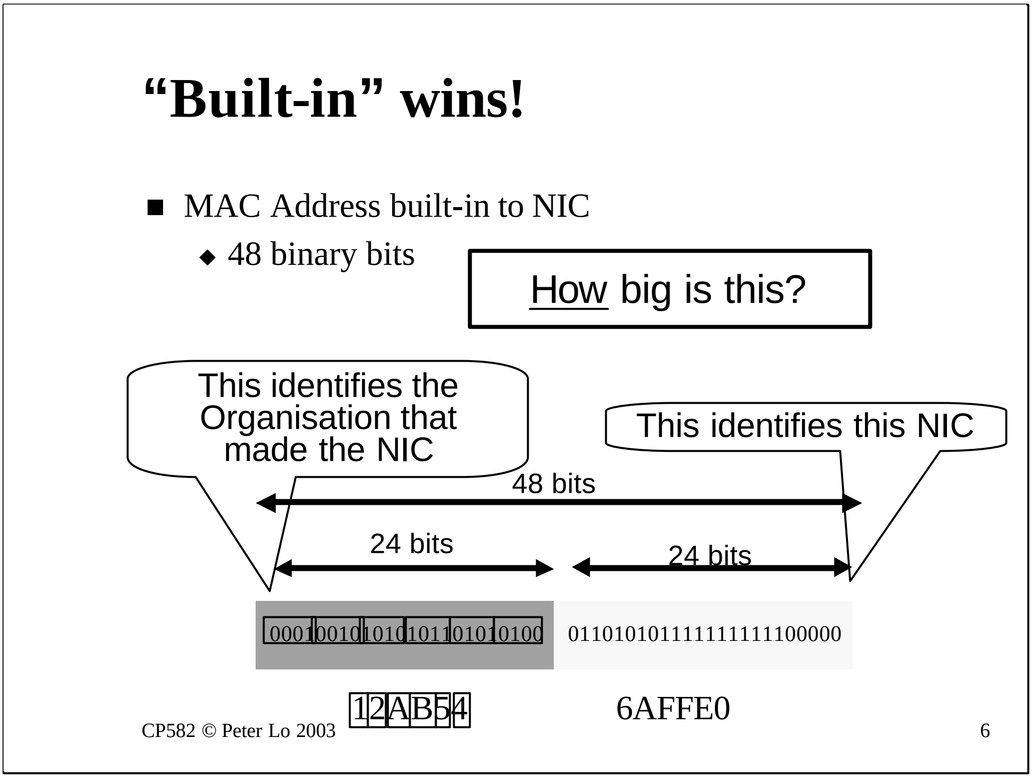
Built-in address

If the address is to be globally unique how can this be administered? An obvious answer is to break the problem down into two parts. Part of the address will identify the company (or “Organisation”) that made the NIC. The company then has the responsibility of making sure that every NIC it produces has the remainder of the address set uniquely.

Unscrupulous or inexperienced companies might not get this right - I have seen whole boxes of NICs with identical addresses - try wiring a network with those!

Negotiated

This was the approach that Apple used with the first Macintosh. When you carry your MAC to a new local network it “talks” to the other computers and figures out what address to use.



“Built-in” wins!

- MAC Address built-in to NIC
  - 48 binary bits

How big is this?

This identifies the Organisation that made the NIC
This identifies this NIC
48 bits
24 bits
24 bits
000100101010101101010100
011010101111111111100000
12AB54
6AFFE0

Most networking today uses the “built in” approach.

48 bit MAC address

This is a pretty general standard in networking today and the IEEE regulate the use of the 48 bits.

The first 24 bits are used to identify the company or organisation who need to apply and be approved and pay to use this value. This then gives the company the right to manufacture cards that have this value for the first 24 bits and then (hopefully!) a unique value for the remaining 24 bits on each and every card the manufacture.

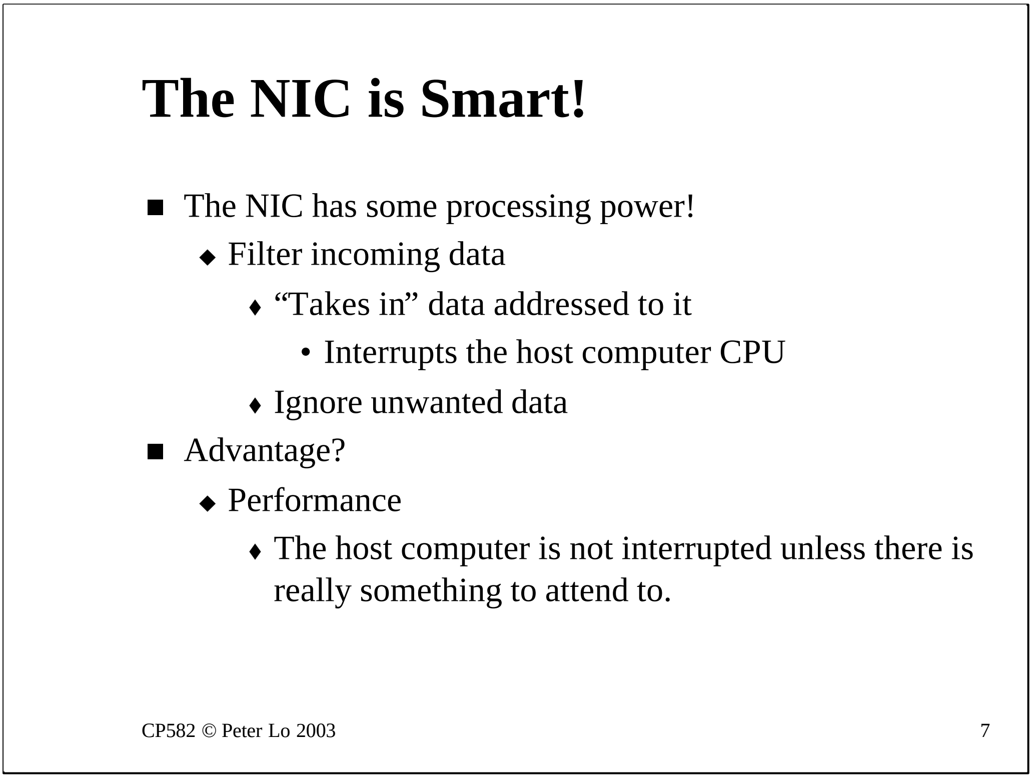
This first 24 bits is called the **Organisation Unique Identifier (OUI)** and in the lab this week you will be finding out what organisations are using certain particular OUIs.

Hexadecimal representation

The remainder of this slide is showing how numbers and letters can be used a shorthand for all those bits. Each number or letter represents exactly 4 bits.

The rest of the unit will be **totally pre-occupied** with this from of representation - you need to live it and breath it (I maintain that I dream in hexadecimal!) - at any rate be completely comfortable with it.

Next week a whole hour will be spent on this so do not worry too much about it today. If this is revision for you then next week you might be able to skip half the lecture!



The NIC is Smart!

- The NIC has some processing power!
  - Filter incoming data
    - “Takes in” data addressed to it
      - Interrupts the host computer CPU
    - Ignore unwanted data
- Advantage?
  - Performance
    - The host computer is not interrupted unless there is really something to attend to.

NIC functionality

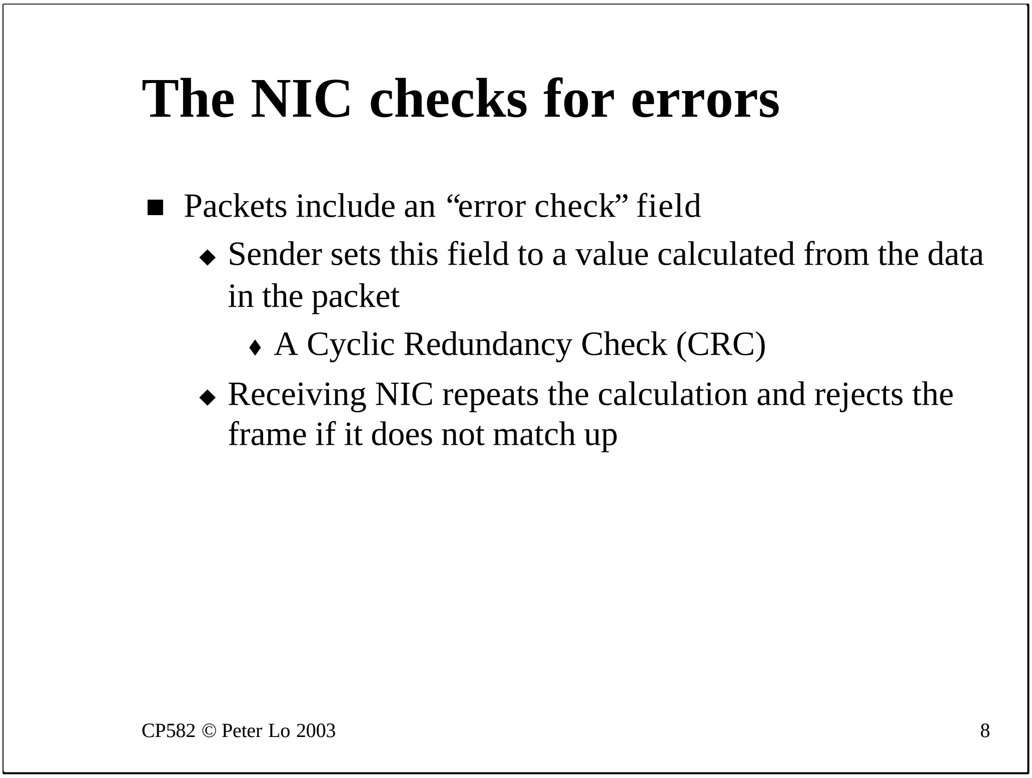
The NIC has an important job to do apart from simply passing messages to and from the “host” computer (the one it is plugged into!)

Each time a message arrives on the network the NIC has to do something with it. The NIC itself has a limited ability to store messages so basically, if the message is not to be lost, the NIC has to tell the host computer CPU to do something with the message - usually, in the first instance, just store it safely in RAM.

There are many thousands of messages on the network and if the host CPU had to store all of them in RAM your computer would grind to a halt.

Fortunately most of those messages are for other computers! The NIC is able to deduce this by taking a quick peek at the destination address in each packet. If the NIC finds that the packet is “not for me” it can ignore the rest of that packet.

By this means the host CPU is only interrupted when there is something meaningful to do. The NIC acts as a filter.



The NIC checks for errors

- Packets include an “error check” field
  - Sender sets this field to a value calculated from the data in the packet
    - A Cyclic Redundancy Check (CRC)
  - Receiving NIC repeats the calculation and rejects the frame if it does not match up

The another thing that NICs do with packets is to keep a check on the integrity of the data. If there are failures in this local delivery it will affect the overall sending and receiving of messages and the NICs are equipped to make sure that only undamaged packets make it through. How does this work?

CRC (Cyclic Redundancy Check)

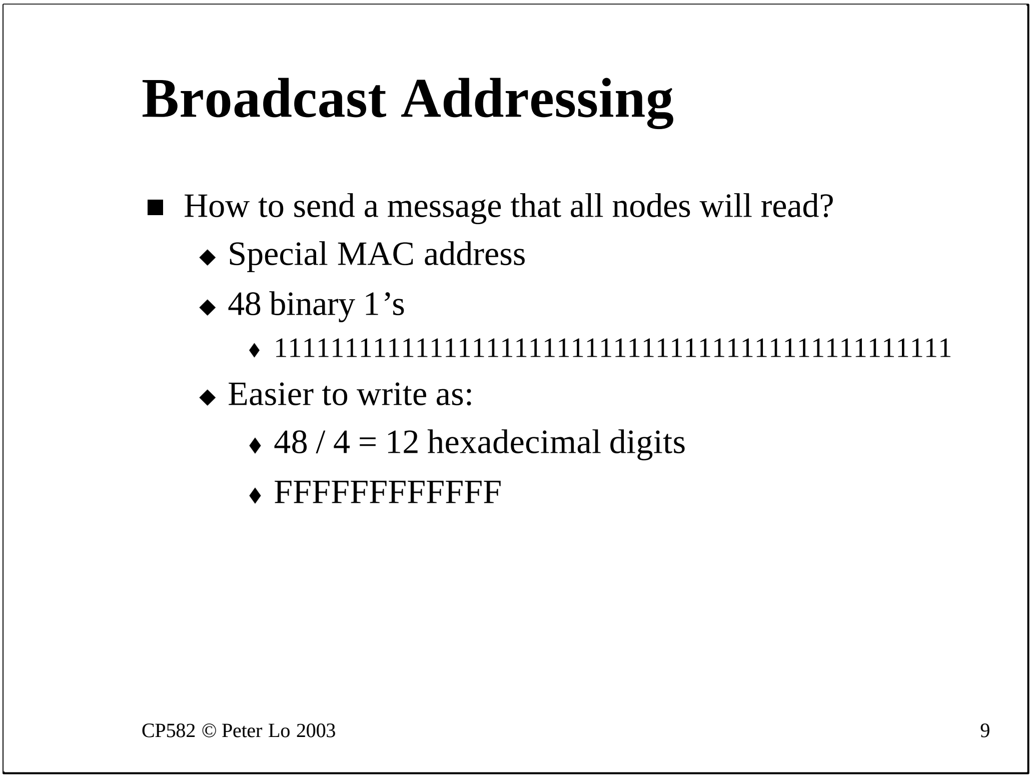
Each chunk of data has a CRC attached to it. The CRC is computed by combining all the bytes of the data in a special calculation. If a byte of the data changes in value the CRC will change.

Sending NIC

Presumably the sender has a good copy of the data. The CRC is computed, and attached to the packet before it is sent.

Receiving NIC

Once the packet has made it through the address check filter the receiving NIC repeats the CRC calculation using the received, but possibly corrupted, data bytes. If the result does not match the packet is rejected.



Broadcast Addressing

- How to send a message that all nodes will read?
  - Special MAC address
  - 48 binary 1’s
    - 111111111111111111111111111111111111111111111111
  - Easier to write as:
    - 48 / 4 = 12 hexadecimal digits
    - FFFFFFFFFFFF

Broadcast Addressing

Having just said that the NIC filters packets we have left ourselves with a problem. What if we want **all** nodes to receive a message (“The building is on fire!”) - what if we do not know the MAC address of all the nodes?

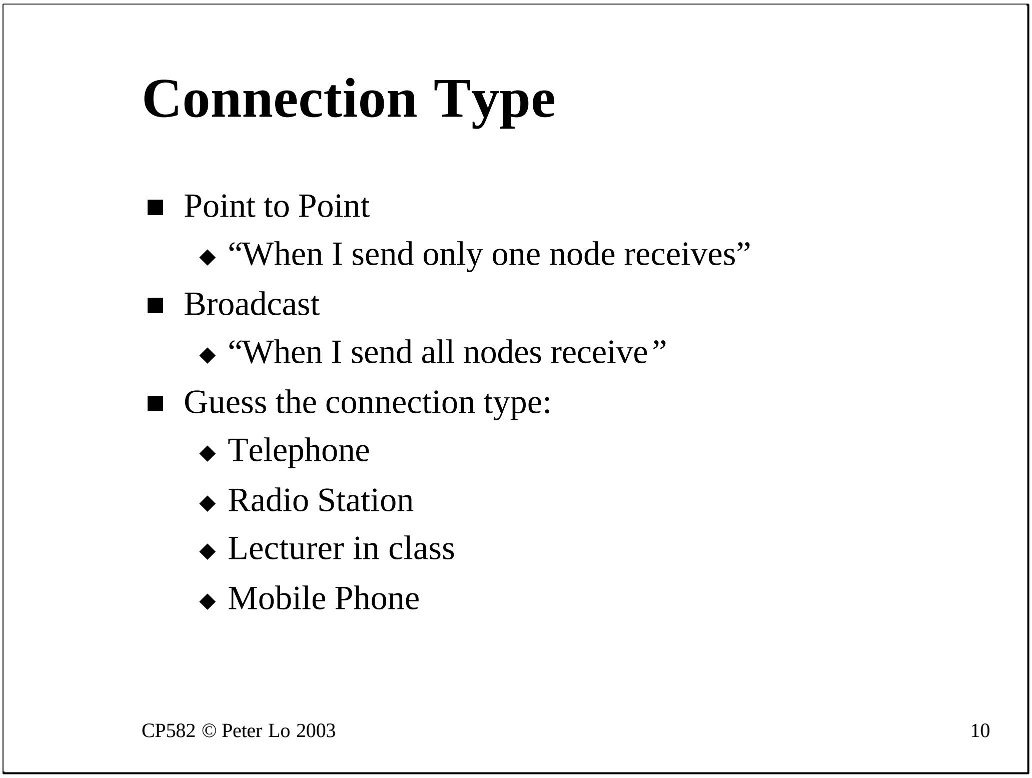
There needs to be a way to exceptionally address a packet so that all the NICs in all the computers will immediately take it in and interrupt their host CPUs.

This address is the “broadcast address” and it simply consists of a MAC address that is all binary 1’s - 48 of them.

So we need to modify our notion of the NIC as a filter - it is a filter that will let through-

a) Packets that are addressed to the NIC

b) Broadcast addressed packets



Connection Type

- Point to Point
  - “When I send only one node receives”
- Broadcast
  - “When I send all nodes receive”
- Guess the connection type:
  - Telephone
  - Radio Station
  - Lecturer in class
  - Mobile Phone

Connection Type

This is the second major issue in Local Delivery.

When a node sends a message how many other nodes immediately “see” it?

If the answer is “1” then we have a “point-to-point” network.

If the answer is “many” then we have a broadcast network.

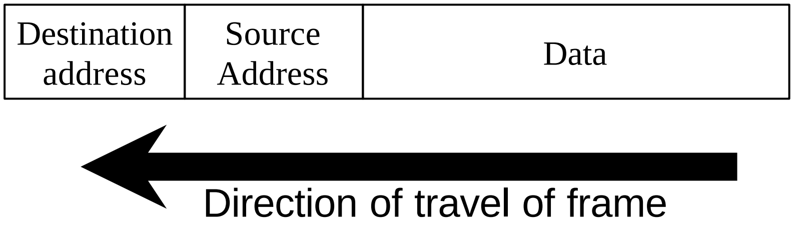
Different cabling systems or media simply **are** one or the other. It should be fairly obvious that a network that uses radio waves would be a broadcast connection type. It is not so obvious when the computers are connected together with wires - you need to know what is going on inside the wires to say what connection type is being used.

Some computer networks are wired up by having a single cable that leads from one computer to the next and the next and so on. What connection type would you guess was being used here?

There is a lot of scope for confusion between “broadcast address” and “broadcast connection type”. Because of the filtering ability of the NIC we **need** to use a broadcast address to speak to all nodes, **whatever the connection type.**

Data Format

- Names for the “chunks” of data on the network?
  - Message - general purpose, non-networking term
  - Packet - general purpose, networking term
  - Frame - specific, local delivery networking term
- Frame format



Destination address	Source Address	Data

Data format

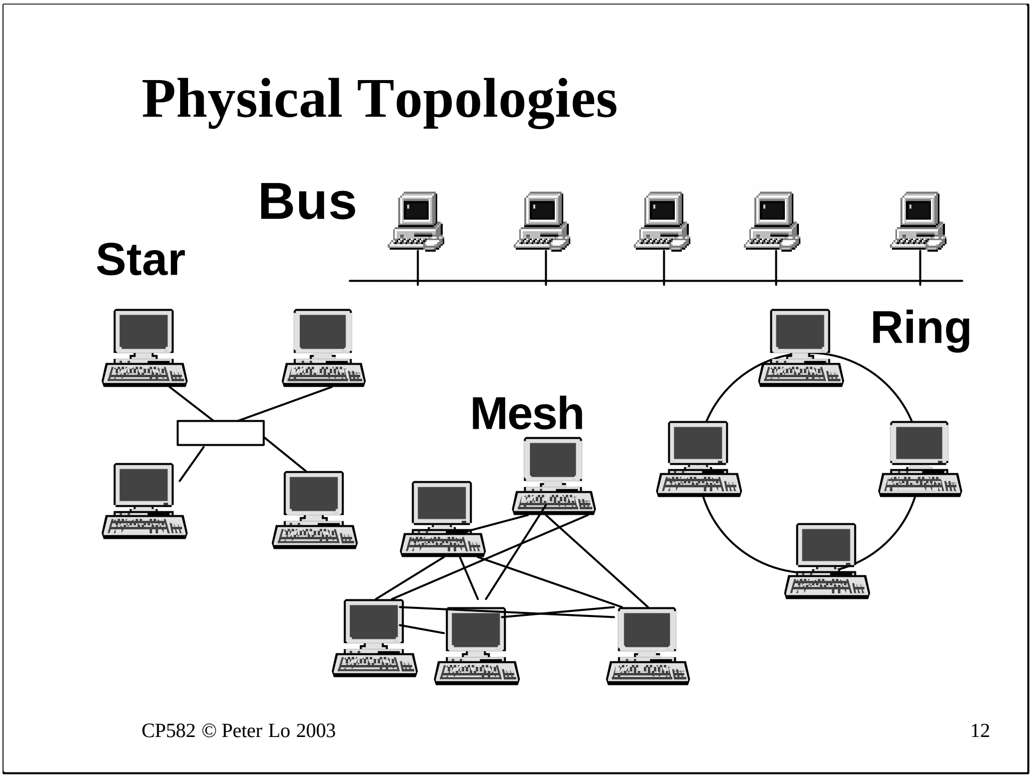
The third major local delivery issue is the format of the data as it is sent across the wire. In this context we use the word “frame” to refer to one message or packet. So what is shown in this slide is the format of a frame.

It is important to remain clear about which direction the frame is travelling along the wire.

Frames are laid out so that their destination address **always** travels at the front. This makes it easier for the receiving NIC to perform its filtering role. If the destination MAC does not match the frame can be immediately discarded without reading any more of it!

The second slot in the frame is for the source (MAC) address. Every single frame must have this filled out otherwise the receiving node will not know where to send the reply. This is like the return address that we write on the backs of our envelopes (in Canada it is written on the front - in the top left-hand corner)

The letter itself, of course, is inside the envelope and in the networking context the data is stored “inside” the frame - in other words immediately after the source and destination MAC addresses. This is sometimes referred to as the “payload” of the packet.



Physical Topologies

The first thing to think about when looking at physical topologies is the **connection type** that is being used. Simply by looking at the physical arrangement you can pick out **point-to-point** and **broadcast** based networks.

Other issues to think about are:

- Ease of installation

How much cable, and therefore disruption of the site, is involved?

- Ease of reconfiguration

What is involved in moving, or adding, a computer?

- Reliability

If a cable breaks how many computers are down?

Bus

A single cable pair is connected to every computer. It can only work at all if the whole cable is complete and undamaged. The NICs need a way to share the cable.

Star

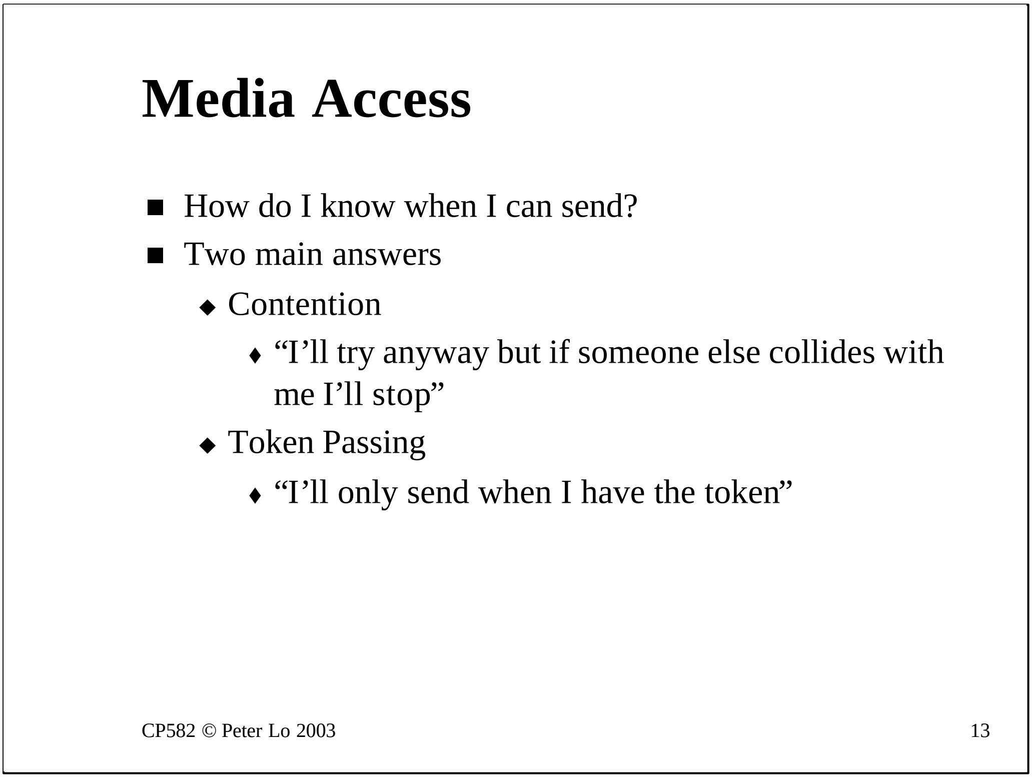
A cable pair links each computer to a central hub. If a computer can talk to the hub then messages will be relayed to the other computers. If a single wire breaks only one computer is affected.

Mesh

Every computer is connected to every other computer. There are many redundant connections.

Ring

Computers are connected directly to neighbours. Messages flow around the ring. If the ring breaks there is no communication at all.



Media Access

- How do I know when I can send?
- Two main answers
  - Contention
    - "I'll try anyway but if someone else collides with me I'll stop"
  - Token Passing
    - "I'll only send when I have the token"

The last issue is termed "media access". Whatever the physical arrangement of the network there have to be rules for deciding when a node can initiate a conversation. The two broad categories of rule are shown in this slide.

Contention

Most networks are based on this simple procedure that is followed when a node needs to send data:

- Node listens to network
- If silent then it starts to send - but keeps listening while it sends
- If the node senses a collision with another node it stops sending
- Wait for a random time and try again

This is easy, and therefore cheap, to implement but tends to bog down when the network gets really busy. There end up being more collisions than successful sends!

Such a network is termed "probabilistic" because, under stress, a message might, or might not, get through. Would you recommend this for controlling a 10 ton crane?

Token passing

To solve that problem there can be a strict order imposed by passing round a "token". The rule is that a node can only send when it has the token and this makes sure that there can never be any collisions.

The token is passed around methodically from node to node so every node is guaranteed to get a chance to send.

This is a "deterministic" solution. Much better for controlling that 10 ton crane!

Contention Based Networks

- CSMA/CD
  - **C**arrier **S**ense (listen first)
  - **M**ultiple **A**ccess (broadcast based)
  - **C**ollision **D**etection (how to resolve contention)
- Ethernet
  - The most common
- Appletalk
  - Uses collision **avoidance** (CSMA/CA)

Ethernet

Most networks you will use are Ethernet networks.

Until recently these were 10 Mbit/sec networks but 100 Mbit/sec is the emerging standard.

Ethernet can be used on a bus (usually black wires) or star topology (usually blue wires). Each approach has the pros & cons that you would expect from the topology. We use ethernet star in the labs - the whole lab no longer hangs when there is a single cable fault.

Appletalk

The network in the original Macintosh computers. It was slow (230KBits/sec) but this was 1982.

Collisions were **avoided** rather than detected. Nodes avoided collisions affecting data packets by sending a tiny "probe" message first. If the probe did not collide it could reserve the wire for the larger, data packet. This is sometimes referred to as a "little brother" technique - before crossing a busy road you send your little brother across. If he makes it then you can go!

Token-passing networks

- Token-ring
  - IBM is main example
  - Expensive NICs
- Arcnet
  - Early cheapo network
  - Now obsolete

Token Ring

Banks, defence establishments & stock brokers often insist on token-ring. In exchange for much more expensive NICs organisations with a lot of money and high security concerns can have a deterministic network.

The NICs are more complex because they must manage two point to point connections simultaneously. For the token passing to be fast the NIC must receive on one side and simultaneously transmit on the other whilst, at the same time, receiving or sending data. Token Ring NICs are powerful computers in their own right!

Speeds are 4 or 16 Mbit/sec

Arcnet

In the early days of networks (when an Ethernet NIC cost $400 - $40 now) Arcnet - with $60 NICs was popular because of its cost.

It was slower (4 Mbit/sec) but very easy to work with physically. The token passing was based on receiving, then sending the token on a broadcast network. This would make things even slower but is obviously cheaper to do in terms of NIC hardware.