EECS150 - Digital Design

Lecture 14 - Serial/Audio/Ethernet

March 7, 2013

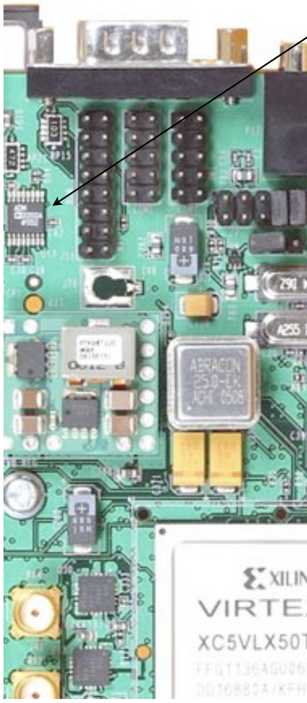
John Wawrzynek

Project Overview

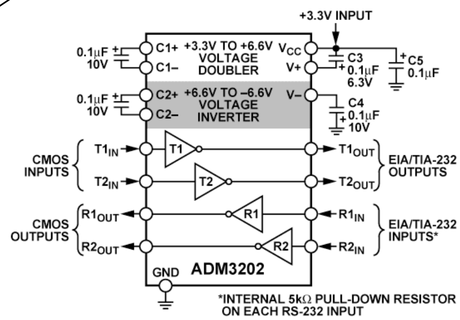
A. Serial Interface
B. Digital Audio
C. Networking and Ethernet

Board-level Physical Serial Port

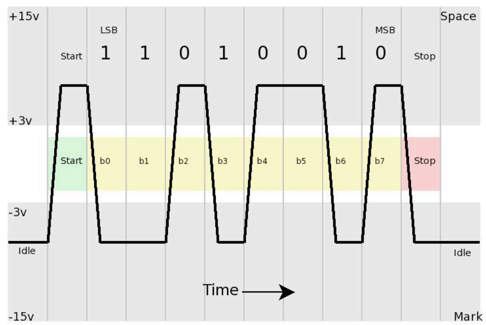
DB-9 connector



RS-232 Transmitter/Receiver

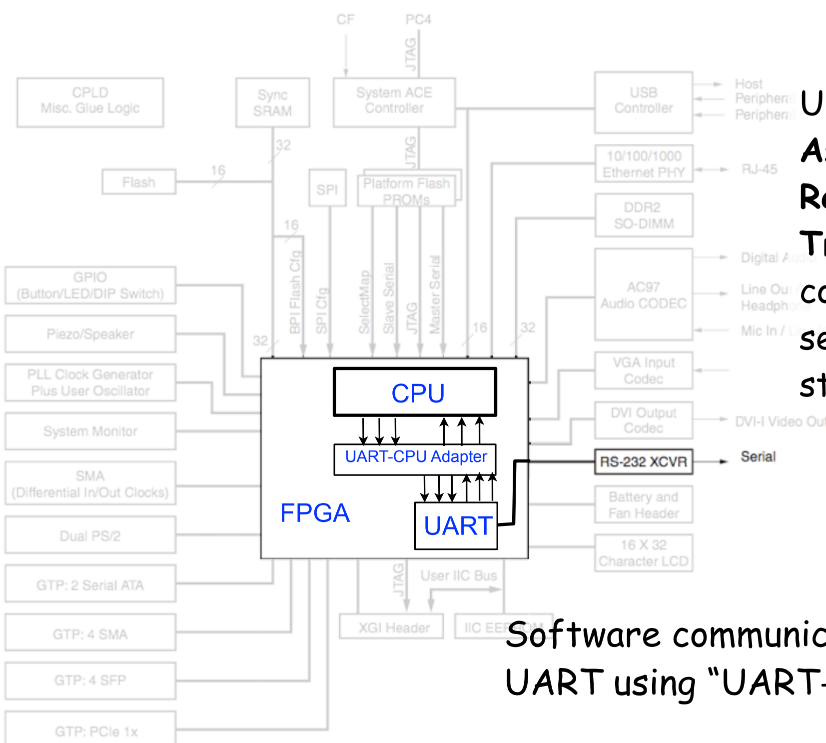


Implements standard signaling voltage levels for serial communication.
Allows FPGA board to communicate with any other RS-232 device.



Oscilloscope trace of ASCII "K" transmission.

FPGA Serial Port

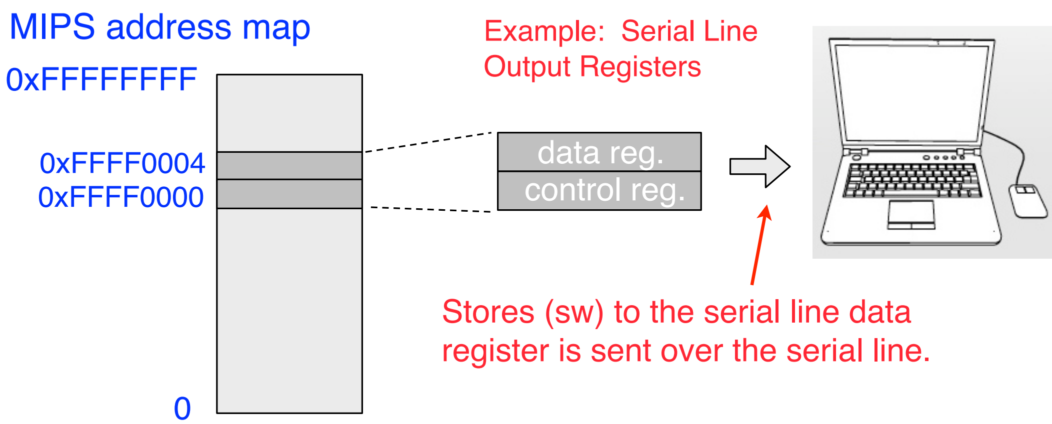


UART: **Universal Asynchronous Receiver and Transmitter** converts to/from serial format with start/stop bits.

Software communicates with UART using "UART-CPU Adapter".

MIPS uses Memory Mapped I/O

- Certain addresses are not regular memory
- Instead, they correspond to registers in I/O devices

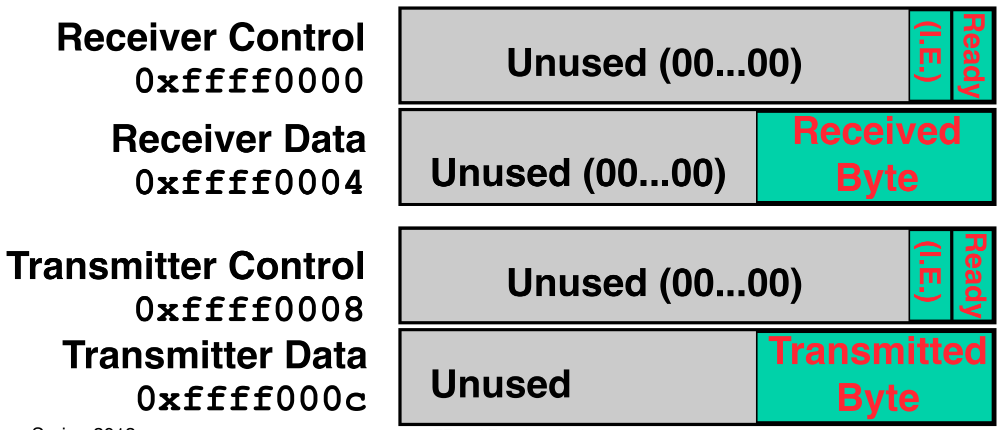


Processor Checks Status before Acting

- Path to device generally has 2 registers:
  - Control Register, says it's OK to read/write (I/O ready) [think of a flagman on a road]
  - Data Register, holds data for transfer
- Processor reads from Control Register in loop, waiting for device to set Ready bit in Control reg ($0 \Rightarrow 1$) to say its OK
- Processor then loads from (input) or writes to (output) data register

MIPS150 Serial Line Interface

- Serial-Line Interface is a memory-mapped device.
- Modeled after SPIM terminal/keyboard interface.
  - Read from keyboard (receiver); 2 device regs
  - Writes to terminal (transmitter); 2 device regs



Serial I/O

- Control register rightmost bit (0): Ready
  - Receiver: Ready==1 means character in Data Register not yet been read;
    1 ⇒ 0 when data is read from Data Reg
  - Transmitter: Ready==1 means transmitter is ready to accept a new character;
    0 ⇒ Transmitter still busy writing last char
    - I.E. bit (not used in our implementation)
- Data register rightmost byte has data
  - Receiver: last char from serial port; rest = 0
  - Transmitter: when write rightmost byte, writes goes to serial port.

"Polling" MIPS code

- Input: Read from keyboard into $v0

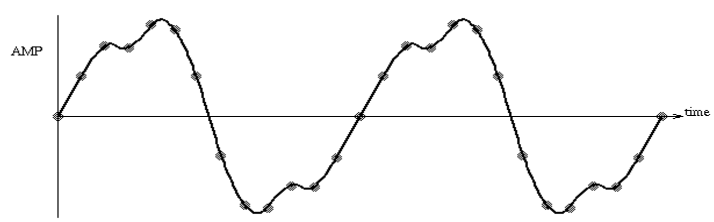
```
              lui  $t0, 0xffff #ffff0000
Waitloop1:    lw   $t1, 0($t0) #control
              andi $t1,$t1,0x1
              beq  $t1,$zero, Waitloop1
              lw   $v0, 4($t0) #data
```

- Output: Write to display from $a0

```
              lui  $t0, 0xffff #ffff0000
Waitloop2:    lw   $t1, 8($t0) #control
              andi $t1,$t1,0x1
              beq  $t1,$zero, Waitloop2
              nop
              sw   $a0, 12($t0) #data
```


Digital Audio

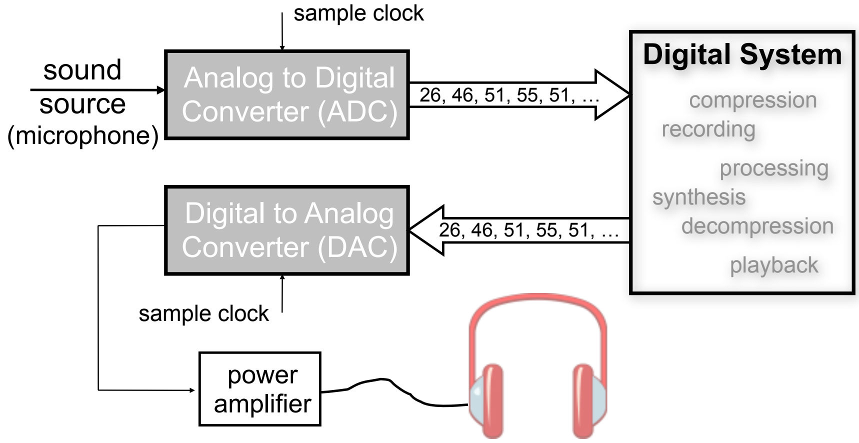
- Music waveform



- **A series of numbers is used to represent the waveform, rather than a voltage or current, as in analog systems.**

- Discrete time: regular spacing of sample values in time. Most digital audio system use 44.1KHz (consumer) sample rate or 48KHz (professional) sample rate.
  - Lower frequency would limit the maximum representable frequency content. (Human hearing max is 20KHz)
- Digital: All inputs/outputs and internal values (signals) take on discrete values (not analog). Most digital audio systems use 16-bit values (64K possible values for any point in waveform). Using much fewer than 16 bits generates noticeable noise from distortion.

Analog / Digital Conversion



- Converters are used to move from/to the analog domain.
- ADC & DAC often combined in a single chip called CODEC (coder/decoder).
- Other types of CODECs perform other functions (ex: video conversion, audio compression/decompression).

Digital Audio Data-rates

44.1K samples/sec x 2 (stereo) x 16 bits/samples
= 1.4 Mbit/sec = 176,400 Bytes/sec

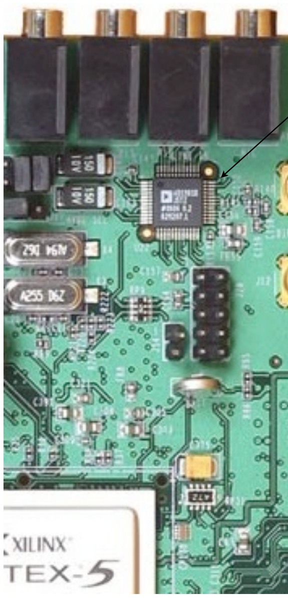
1 minute ≈ 10MByte total

- Relatively small storage devices and network bandwidth limits has prompted the development and application of many compression algorithms for music and speech:
  - Typically compression ratios of 10-100
  - MP3: 32Kbits/sec - 320Kbits/sec (factor of 4x to 44x)
  - These techniques are *lossy;* information is lost. However the better ones (MP3 & AAC for example) used techniques based on characteristics of human auditory perception to drop information of little importance.
- Uncompressed audio is often referred to as PCM (pulse code modulation) . (.wav files in windows)

Board-level Physical Audio Port

Audio Jacks

AC '97 Audio Codec



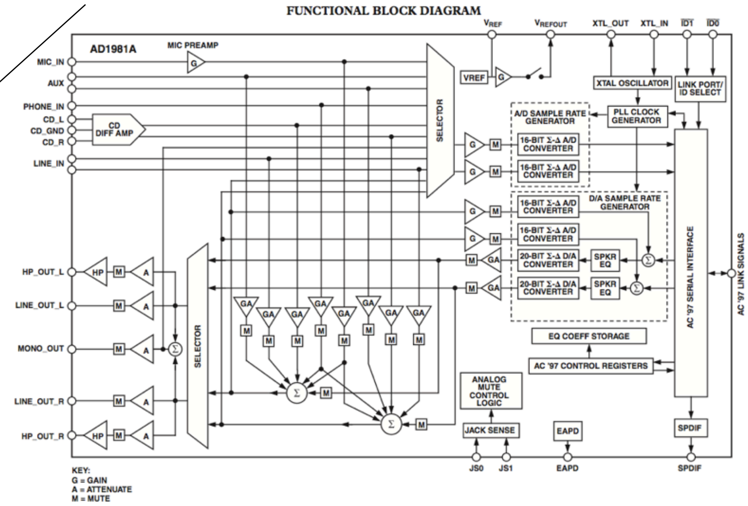


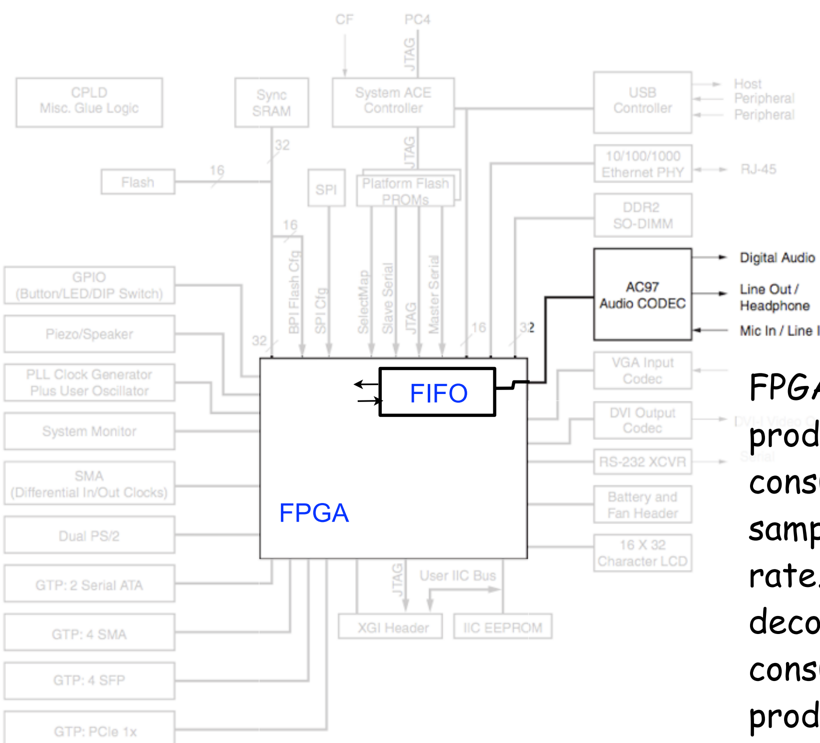
Table 1-12: **Audio Jacks**

Reference Designator	Function
P10	Microphone - In
P11	Analog Line - In
P12	Analog Line - Out
P13	Headphone - Out
P14	SPDIF - Out

Table 1-13: **Audio Codec Control Connections**

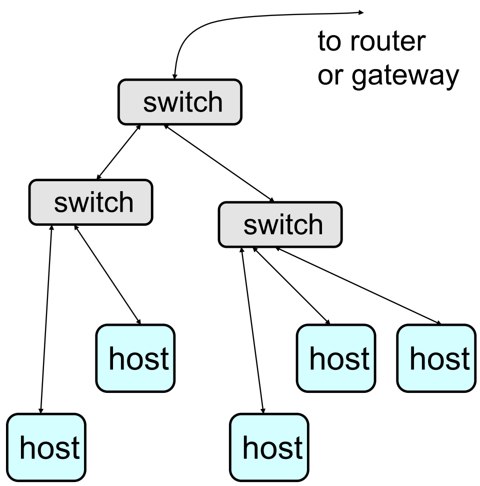
Net Name	FPGA Pin
AUDIO_BIT_CLK	AF18
AUDIO_SDATA_IN	AE18
AUDIO_SDATA_OUT	AG16
AUDIO_SYNC	AF19
FLASH_AUDIO_RESET_B	AG17

FPGA Audio Port



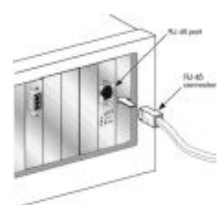
FPGA design produces or consumes audio samples at audio rate. FIFO decouples consumer from producer.

Local Area Network (LAN) Basics

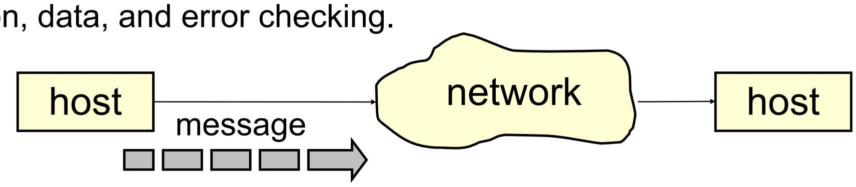


- A LAN is made up physically of a set of switches, wires, and hosts. Routers and gateways provide connectivity out to other LANs and to the internet.
- Ethernet defines a set of standards for data-rate (10/100/1000 Mbps), and signaling to allow switches and computers to communicate (IEEE 802.3)
- Most Ethernet implementations these days are “switched” (point to point connections between switches and hosts, no contention or collisions).

Ethernet



- An Ethernet interface card or Network Interface Card (NIC) is used to bring the network into the host:
- Information travels in variable sized blocks, called Ethernet Frames (or packets), each frame includes preamble, header (control) information, data, and error checking.



- Link level protocol on Ethernet is called the Medium Access Control (MAC) protocol. It defines the format of the packets.
- Frame format:

Preamble (8 bytes)	MAC header	Payload	CRC

  - Preamble is a fixed pattern used by receivers to synchronize their clocks to the data.
  - Payload is the actual information the host is sending.

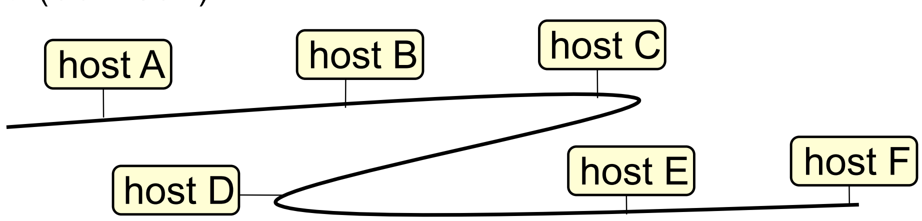
Ethernet (802.3) Frame Format

destination address	source address	length	payload (data)	CRC
14 Bytes			46-1500 Bytes	4 B

- MAC protocol *encapsulates* a payload by adding a 14 byte header before the data and a 4-byte cyclic redundancy check (CRC) after the data.
- Each network hardware device is assigned a unique address (called MAC address), assigned globally.
- A 6-Byte **destination address**, specifies either a single recipient node (unicast mode), a group of recipient nodes (multicast mode), or the set of all recipient nodes (broadcast mode).
- A 6-Byte **source address**, is set to the sender's globally unique node address. Its main function is to allow address learning which may be used to configure the filter tables in switches.
- A 2-byte **length** field, indicates the number of bytes in the payload field.
- The 4-Byte **CRC** provides error detection in the case where line errors result in corruption of the MAC frame. Any frame with an invalid CRC should discarded by the MAC receiver without further processing.

Ethernet Control – old style CSMA/CD

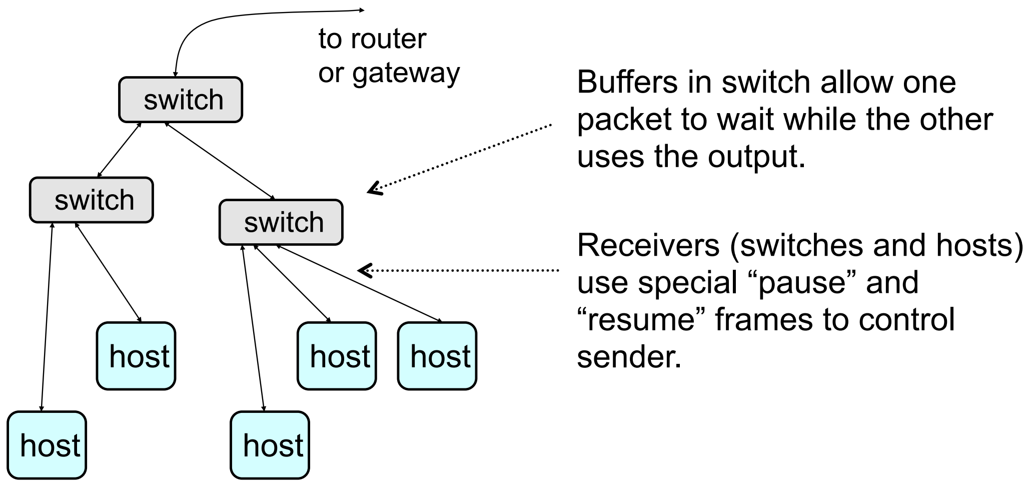
- To keep cost down, inventors of Ethernet wanted no switches – just hosts and Ethernet interfaces.
- They used a protocol called Carrier Sense Multiple Access/Collision Detect (CSMA/CD):



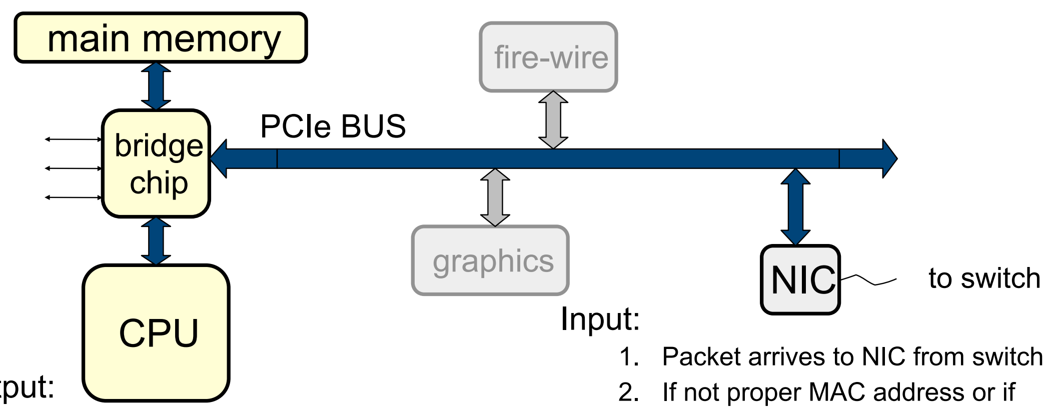
- A host wanting to transmit senses whether the line is idle and therefore available to be used. If it is, the host begins to transmit its frame and listens as it does. If another device has tried to send at the same time, a *collision* occurs and the frames are discarded.
- Each device then waits a random amount of time and retries. If another collision occurs it waits longer before trying again (*exponential backoff*).

Switched Ethernet

- Modern style Ethernet uses *buffering* and *flow-control* to handle collisions in the network.



NIC connection into Machine



Output:

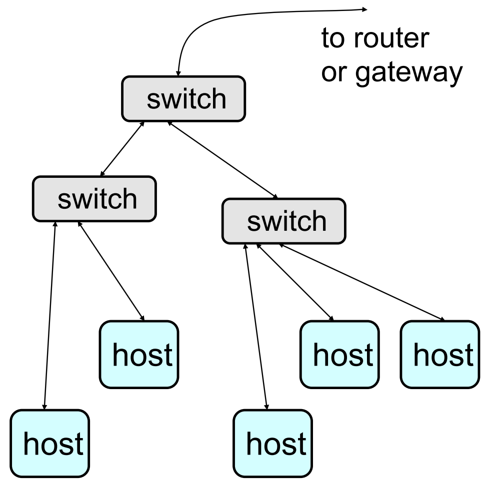
1. CPU prepares payload and leaves in memory buffer.
2. If NIC buffer space available, then initiate DMA transfer to NIC.
3. If no space wait for interrupt.
4. NIC transfers frame out to switch, then interrupts CPU with "buffer space" update.

Input:

1. Packet arrives to NIC from switch.
2. If not proper MAC address or if CRC error ignore
3. Else save payload in buffer and interrupt CPU
4. CPU initiates DMA transfer to memory buffer.
5. DMA finishes and notifies CPU
6. CPU processes packet according to high-level protocol and application.

So far …

- Ethernet (IEEE 802.3):
  - Good for routing within local area network (LAN).
  - **Difficult for truly global routing**, every switch everywhere would need to store all MAC addresses – (we really need some kind of address hierarchy).
  - **Unreliable**:
    - No automatic retransmission on error.
    - No acknowledgements – sender doesn't know if receiver got the data.



TCP/IP

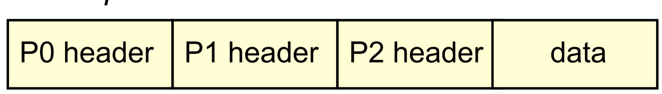
A suite of protocols for global host addressing and reliable transmission on the internet.

- TCP/IP is an example of a layered protocol: each layer builds upon the layer below it, adding new functionality.
- The protocol stack is the collection of protocol that make up the suite:

protocol for transferring files / delivering mail	P2
protocol for routing and reliability	P1
protocol for sending and receiving data using specific hardware	P0

- Each protocol layer *encapsulates* the layer above it:

packet format:



- Stacks are modular, so they can easily change when a new hardware model is adapted or needs of applications change. (Replace one module).

TCP/IP

- TCP/IP is used as part of a 4-layer protocol:

Application layer:	FTP, SMTP, HTTP
Transport layer:	TCP, UDP
Network layer:	IP
Link Layer:	IEEE 802.x, PPP, SLIP

- Link level examples:
  - IEEE 802.3 for Ethernet, 802.5 for token-ring, 802.11 for wireless,
  - Used with dial-up modems: Serial line IP (SLIP), Point-to-Point protocol (PPP).

IP (Internet Protocol)

Extends the idea of host address from MAC to a hierarchical "soft" address. All hosts take on an IP address.

- *The job of IP is to enable data to be transmitted between networks* (adds very little in the context of a LAN over what is possible with MAC addresses).
- Features of IP:
  - *Connectionless* – no concept of a job or session. Every packet treated individually.
  - *In-order delivery not ensured*.
  - *Unreliable* protocol.

The link layer (Ethernet) needs to know the unique address (MAC) of the specific place to next deliver the message. TCP/IP suite include ARP (address resolution protocol) to map from IP address to MAC address. Protocol works by broadcasting a request on the network – if a host sees its IP address, it replies with its MAC. If the IP is outside this subnet, then the router (connecting out) will reply).

IP Packets

<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to live</td><td>Protocol</td><td colspan="2">header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Options (optional)</td></tr>
</table>

← 16 bits → ← 16 bits →

- *Protocol* field: says which high-level protocol sent the data – used by destination to pass packet to right protocol module.
- TTL (time to live): Initialized by the sender (usually 64) then decr. by 1 by every router the packet passes through. When reaches 0, the packet is discarded and the sender is notified with the Internet control message protocol (ICMP). This keeps packets from getting stuck in loops. (Also, used by traceroute).
- *Internet Addressing*: every host directly connected to the internet has a unique address (issued by IANA, iana.org).
- These days many hosts connect *indirectly* with NAT.
- Internet addresses are 32-bits long written as 4-Bytes separated by periods. Range:

1.0.0.1 to 223.255.255.255

IP Routing

- Local routing is done according to the specifics of the LANs own protocol.
- Routing to outside networks is done through <u>routers</u> *(these are either hosts with multiple NICs and special routing software, or special router hardware*.)
  - Each host on the LAN is assigned a default router, used to connect it to outside.

- A router examines every packet and compares the destination address with a table of addresses.
  1. If it finds an exact match, it forwards the packet to the address associated with that entry in the table.
  2. If the router doesn't find a match, it runs through to the table looking for a match just on the network ID. If a match is found, the packet is sent on to the address associated with that entry.
  3. If no match, the router sends it to the default, next-hop router, if present.
  4. If no default router present, the router sends an ICMP "host unreachable" messsage back to the sender.

- Routers build up their tables in multiple ways:
  - Static – read from a file on startup.
  - Dynamically, by broadcasting ICMP router solicitation messages to which other routers respond.
  - Other protocols are used to discover the shortest path to a location.
  - Routers are updated periodically in response to traffic conditions and availability of a route.

Transport Layer

Two most popular transport protocols are TCP and UDP.

← 16 bits →

Source Port	Destination Port
length	Checksum

UDP Header

- UDP – User Datagram Protocol
  - Port numbers represent a software port.
  - They identify which protocol module sent (or is to receive) the data.
  - Standard port numbers exist:

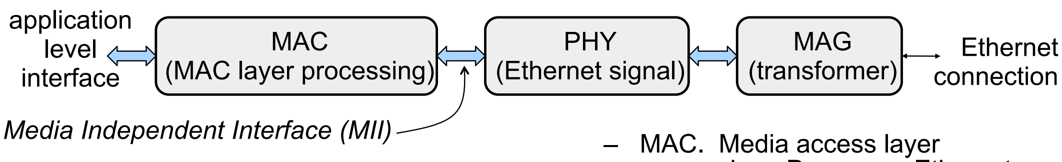
    Telnet: port 23, Simple Mail Transfer Protocol: port 25
  - UDP and TCP use the port numbers to determine which application layer protocol should receive the data.
  - UDP isn't reliable, but appropriate for many applications like real-time audio and video (where if data is lost it is better to do without it than to send it again.) Also, gets used for online games.

TCP – Transmission Control Protocol

- Transport layer protocol used by most internet applications: FTP, HTTP, Telnet, …

- Connection-oriented: 2 hosts, one a client, and the other a server must establish a connection before any data can be transferred between them (SYN/ACK handshake). Once done the connection must be closed (FIN flag).
- TCP sends data using IP in blocks called segments.
- TCP includes mechanisms for ensuring data which arrives out of sequence is put back into the order it was sent.
- TCP implements flow-control, so a sender app. cannot overwhelm a receiver app with data.
- TCP provides reliability: When data is received correctly, TCP sends an acknowledgement back to the sender. If the sender doesn't receive an ack within a certain period, the data is recent. For efficiency, the sender will usually send multiple segments without waiting for acks. It keeps track of what segments have or have not been acked – keeping a copy of those that have not, in case they need to be resent.
- ACKs are piggy-backed on data segments for efficiency.

Standard Hardware-Network-Interface

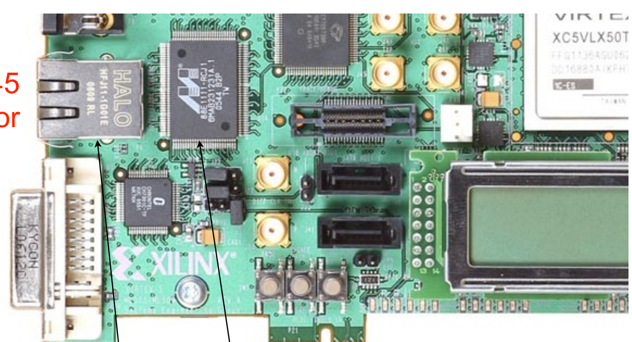


- Usually divided into three hardware blocks. (Application level processing could be either hardware or software.)
  - MAG. "Magnetics" chip is a transformer for providing electrical isolation.
  - PHY. Provides serial/parallel and parallel/serial conversion and encodes bit-stream for Ethernet signaling convention. Drives/ receives analog signals to/from MAG. Recovers clock signal from data input.
  - MAC. Media access layer processing. Processes Ethernet frames: preambles, headers, computes CRC to detect errors on receiving and to complete packet for transmission. Buffers (stores) data for/from application level.
- Application level interface
  - Could be a standard bus (ex: PCI)
  - or designed specifically for application level hardware.
- MII is an industry standard for connection PHY to MAC.

XUP board has no MAC chip, must be handled in FPGA (hardcore).

Board-level Physical Network Port

RJ-45 connector



Marvel Alaska PHY device (88E1111), supports 10/100/1000 Mb/s.

RJ-45 with built-in magnetics