

0x01 Advanced Networking

Core Concepts

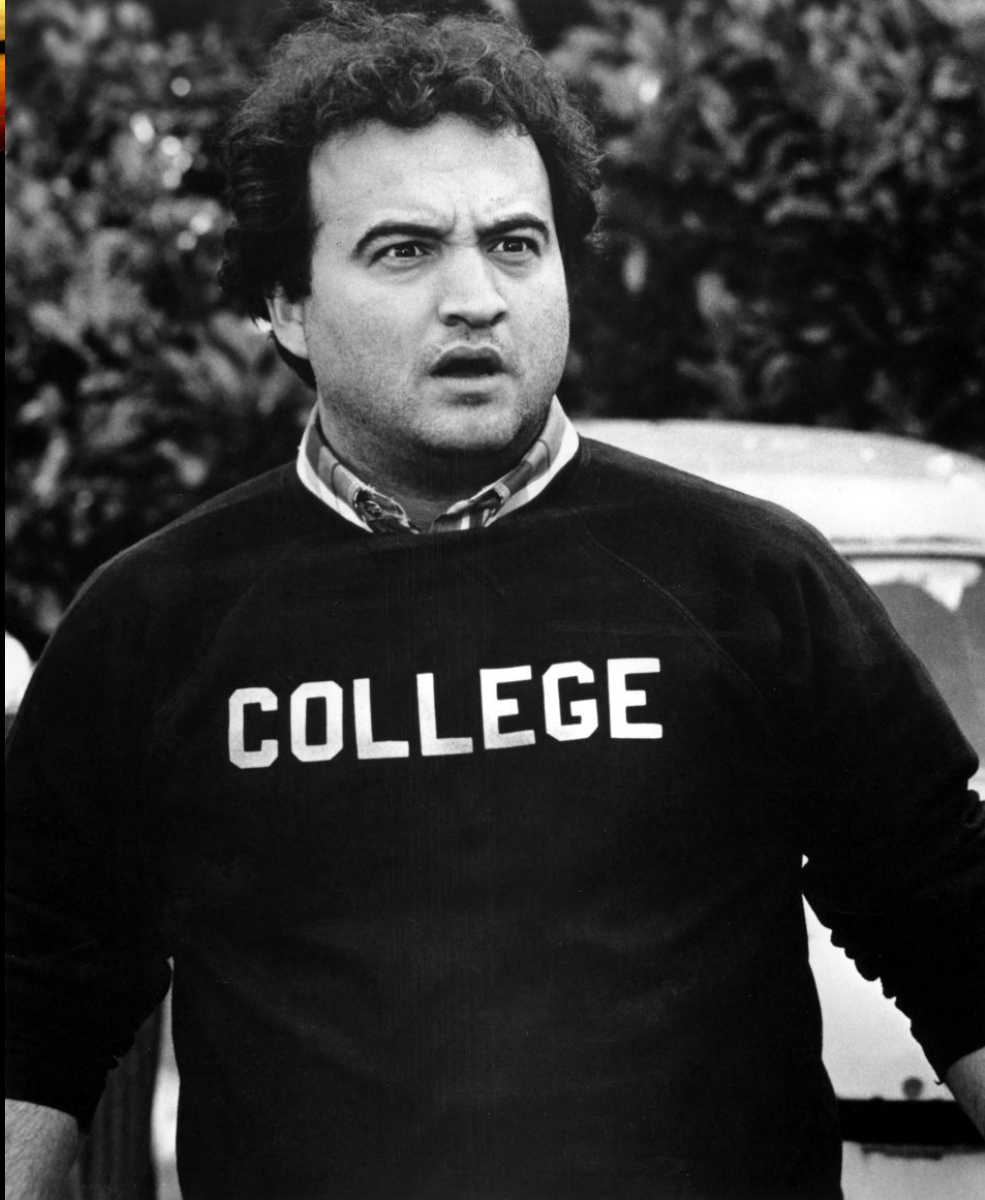
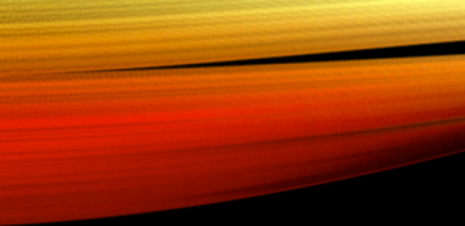


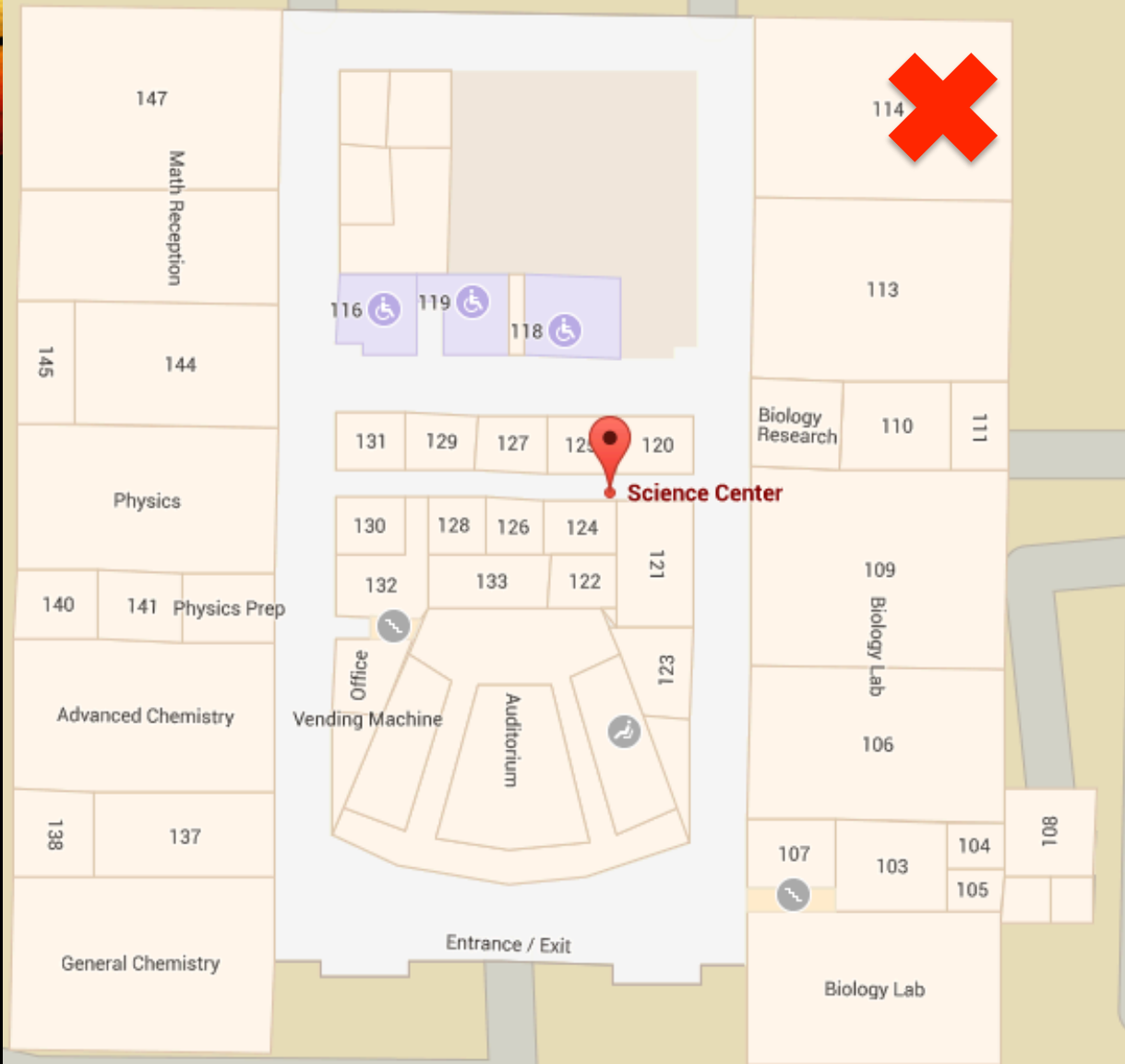
Welcome

Mike Ham

DSU Instructor, Independent Security
Consultant, GenCyber Ninja

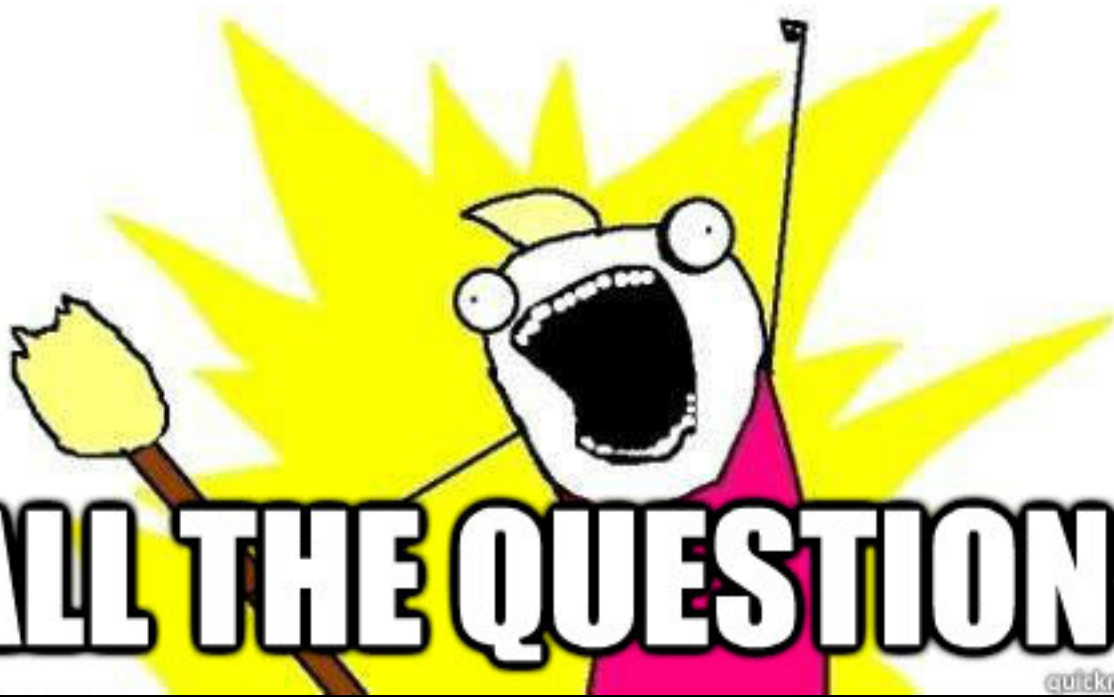
Michael.Ham@dsu.edu





50 minutes

ASK



ALL THE QUESTIONS

Week at a Glance

- Day 1 – Physical hardware, IP/MAC, Binary
- Day 2 – Subnetting 101, DHCP, DNS, Enterprise equipment
- Day 3 – Port scanning, TCP/UDP, SYN Flood
- Day 4 – ARP Poisoning, MITM attacks
- Day 5 – GenCyber Networking Olympics, Mom and Dad come back <3

What is a network?

- Allow us to connect to services and resources
 - HTTP(S), FTP, SSH, ...
- This week should help you to understand why things work
 - What happens when you connect to a Wi-Fi network
 - What happens when you type www.google.com
 - What happens when you download a file

OSI Model

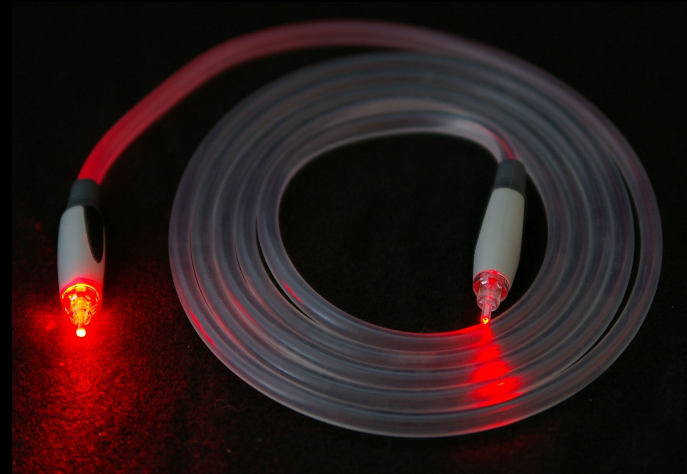
- (Open Systems Interconnection model)
- Standard conceptual model
- Telecomm or computer systems
- No representation of the underlying tech
- Help to understand how everything works together

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	G A T E W A Y Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	F I L T E R I N G TCP/SPX/UDP	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		Routers IP/IPX/ICMP
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Can be used on all layers Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	Hub Land Based Layers	

The First Layer

- Physical Layer
- All of the physical parts of a network are here
- We're mostly concerned with:
 - Cables
 - Connectors



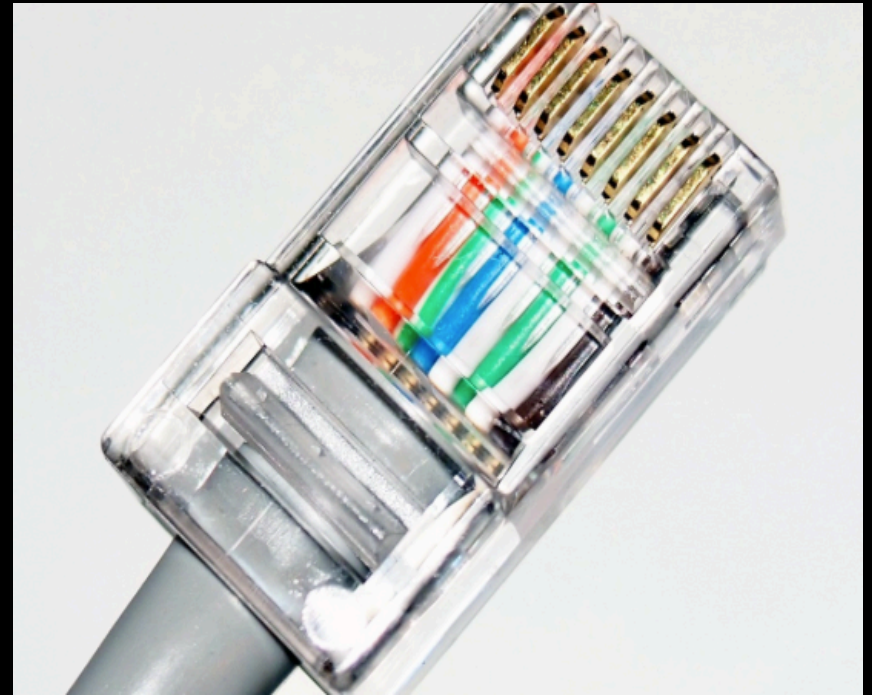
Cables

- **Fiber Optic**- Speed of Light!
- Runs HUGE distances
 - Actually crosses oceans
- www.submarinecablemap.com
- Current record speed: 255 Tb/s
 - That's 255,000 Gb/s
 - Or: 255,000,000 Mb/s
- **Twisted Pair**
 - Other Names: Cat5, Ethernet
- Fairly common/cheap
- 100 meters/328 feet max length
- Typical max speed: 10Gb/s

Cat 5e vs. Cat 6



Twisted Pair Cabling



Why are cables twisted?

- To eliminate crosstalk
- Crosstalk is essentially is where a signal transmitted on one channel is interfering with another transmission channel
- This can be eliminated or reduced by twisting the pairs of cabling together and separating out each pair

Multimode Fiber

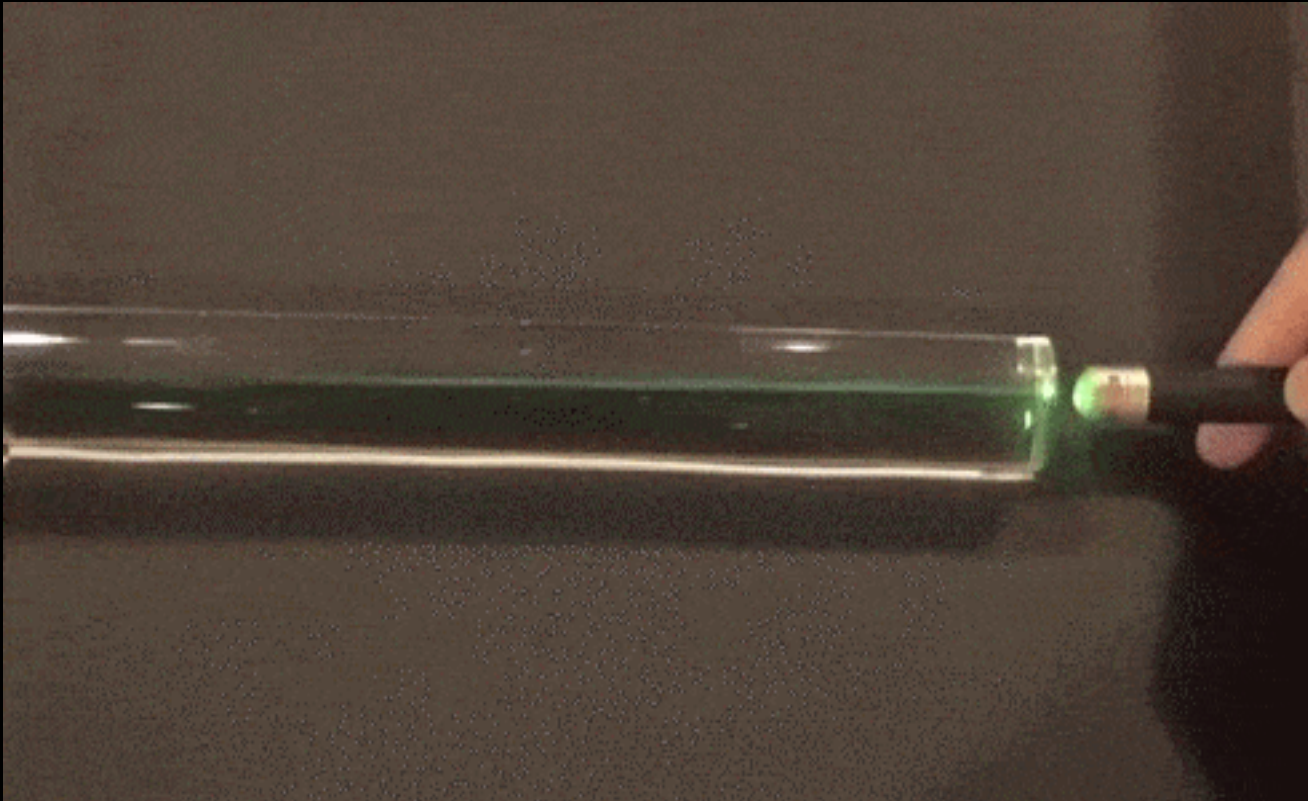
- Light can be sent as regular light or with lasers
- Most multimode fiber uses LEDs
- Changes the angle of transmission down the core of the fiber cable
- Multiple reflection angles tend to disperse over long distances, so multimode fiber optic cables are used for relatively short distances
- A typical multimode network runs at 10, 100, or 1000 Mbps
- Distances for multi-mode runs generally top out at ~600 meters

Single Mode Fiber

- Uses Lasers
- High transfer rate
- Long distances
- Better choice if budget is not an issue



Fiber Cabling Demo



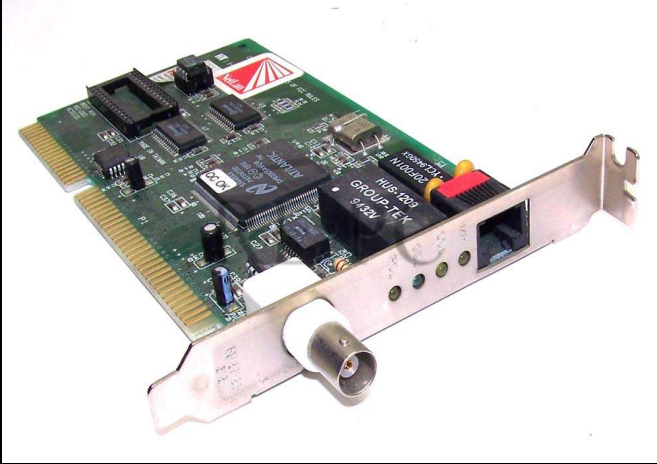
Network Interface Controller (NIC)

- What you plug your computer/device into for network access
 - Can also be wireless
- Uses physical (layer 1) and data link (layer 2) layers of OSI
- Provides a base for the full network protocol stacks
- Pretty much every computer you buy has one built in
 - Servers can have 4 or more (redundancy)

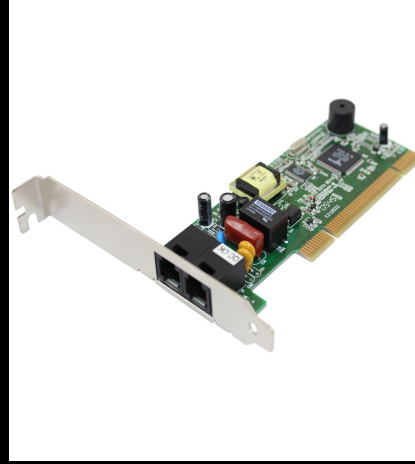
Activity: NIC

- How to find what network card and network you are using:
 1. Click the Start Button and then click the "Programs" folder.
 2. Next, click the "Accessories" and then the "System Information" folder.
 3. Within the System Information window, click the + symbol next to Components.
 4. Click the "+" next to "Network" and highlight "Adapter", in the right side of the window you should be able to locate complete information about the network card.

Legacy NICs



BNC and Ethernet
NIC



56K NIC (dial-up)

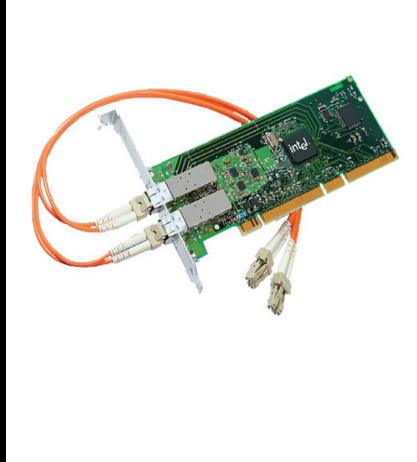


Token Ring

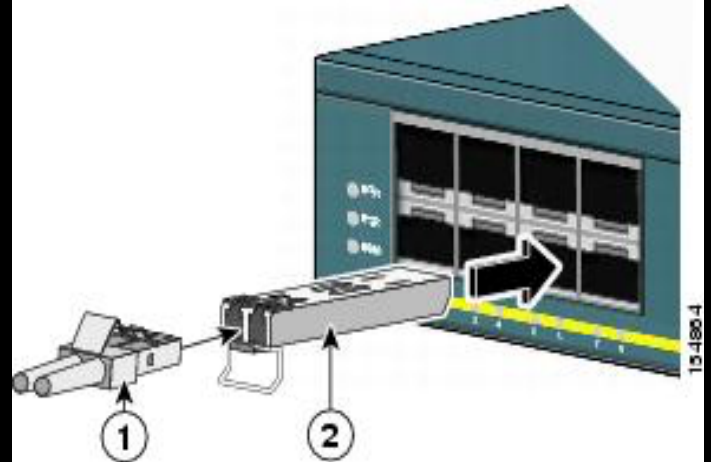
Modern NICs



10/100/1000 NIC



Dual Fiber NIC



SFP into Switch



SFP



SFP

Media Converter



So Cables connect us... now what?

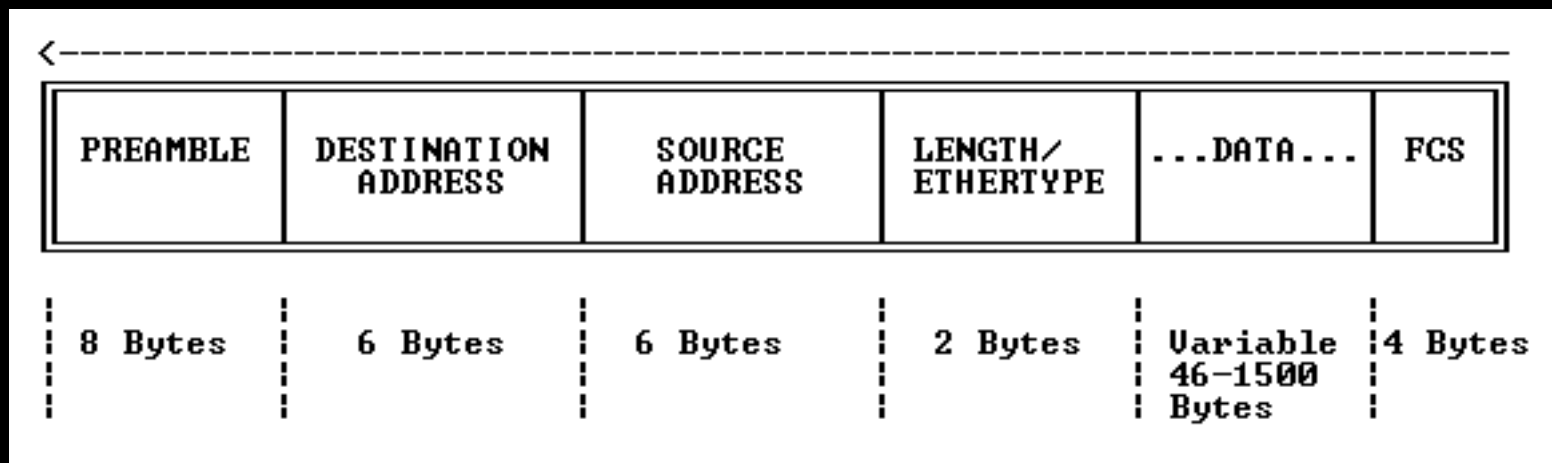
- Cables are our physical connection
- Allows signals to get sent and converted
- What do these signals look like? It depends!
 - Could be Ethernet, USB, Bluetooth, Firewire, etc
 - We'll just focus on Ethernet

So What's Next?

- Cables are our physical connection
- Allows signals to get sent and converted
- What do these signals look like? It depends!
 - Could be Ethernet, USB, Bluetooth, Firewire, etc
 - We'll just focus on Ethernet

Layer 2- Ethernet

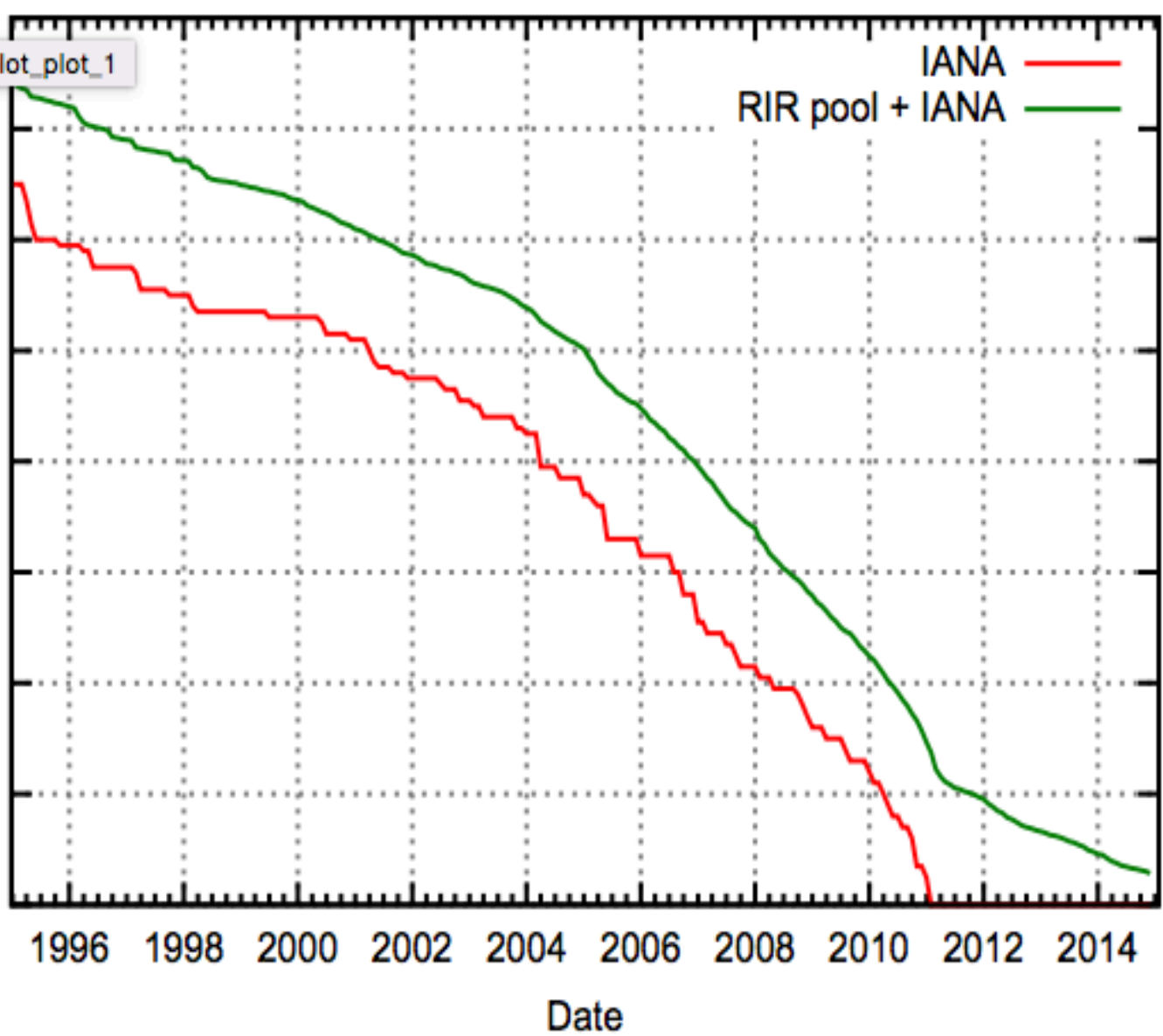
- We've converted our signal from the wire, what does it have?
- Ethernet Pieces:
 - Destination MAC Address
 - Source MAC Address
 - Length
 - Data
- What's a MAC Address?
 - Unique address
 - Every adapter has one
 - It "can't change"
- Media Access Control
- Let's go find it!



Layer 3; One More Address!

- MAC address: Used to identify yourself to your neighbor
 - Kind of like your name; never changes even if you move
- IP Address: Used to identify yourself to the world
 - Changes as you move, just like your mailing address
- IPv4
 - 192.168.1.1
 - 4,294,967,296 addresses possible
- IPv6
 - 2001:0db8:85a3:0042:1000:8a2e:0370:7334
 - 3.4×10^{38} possible addresses

plot_plot_1



What does an IPv4 address consist of?

- Dotted-decimal notation, divide out octets
- 192.168.10.1

192

168

10

1

11000000

10101000

00001010

00000001

- How do the 0's and 1's create that number?

128

64

32

16

8

4

2

1

1

1

0

0

0

0

0

1

Activity: What are these in binary?

- 5
- 24
- 99
- 223
- 255

Activity: Find your IP address

- How do you find your IP?

Activity: Wireshark

Lets go look at some packets!