Forgetting the Fundamentals?

Data Communications: Physical and Logical Explanation

PREPARED FOR DEFCON 32

BY: KEVIN MANNA, MBA, CISSP, CCNA

Objectives

- Introduction
- Communication Process
- Analyze the layered models
- Review some common protocols
- Data link and physical layers
- Understand the encapsulation process
- Reliability issues
- How does my data get to its destination?

About Me

- I am retired!
- Professor Emeritus, Networking and InfoSec, Northampton Community College
- Current degrees/certs: MBA, CISSP, CCNA, Cisco CyberOps. Past cert: CCNP-Routing
- Skills include: Business Planning, Cisco Routing and Switching, Advanced Routing Technologies, International Business, Business Process Improvement, Network Design, Network and Business Consulting, and System Security and Administration.
- Primary Investigator for the Wall Street West Dept. of Labor grant at Northampton Community College.
- Past workshop topics: basic networking, wireless fundamentals, information security, time management, and leadership development.

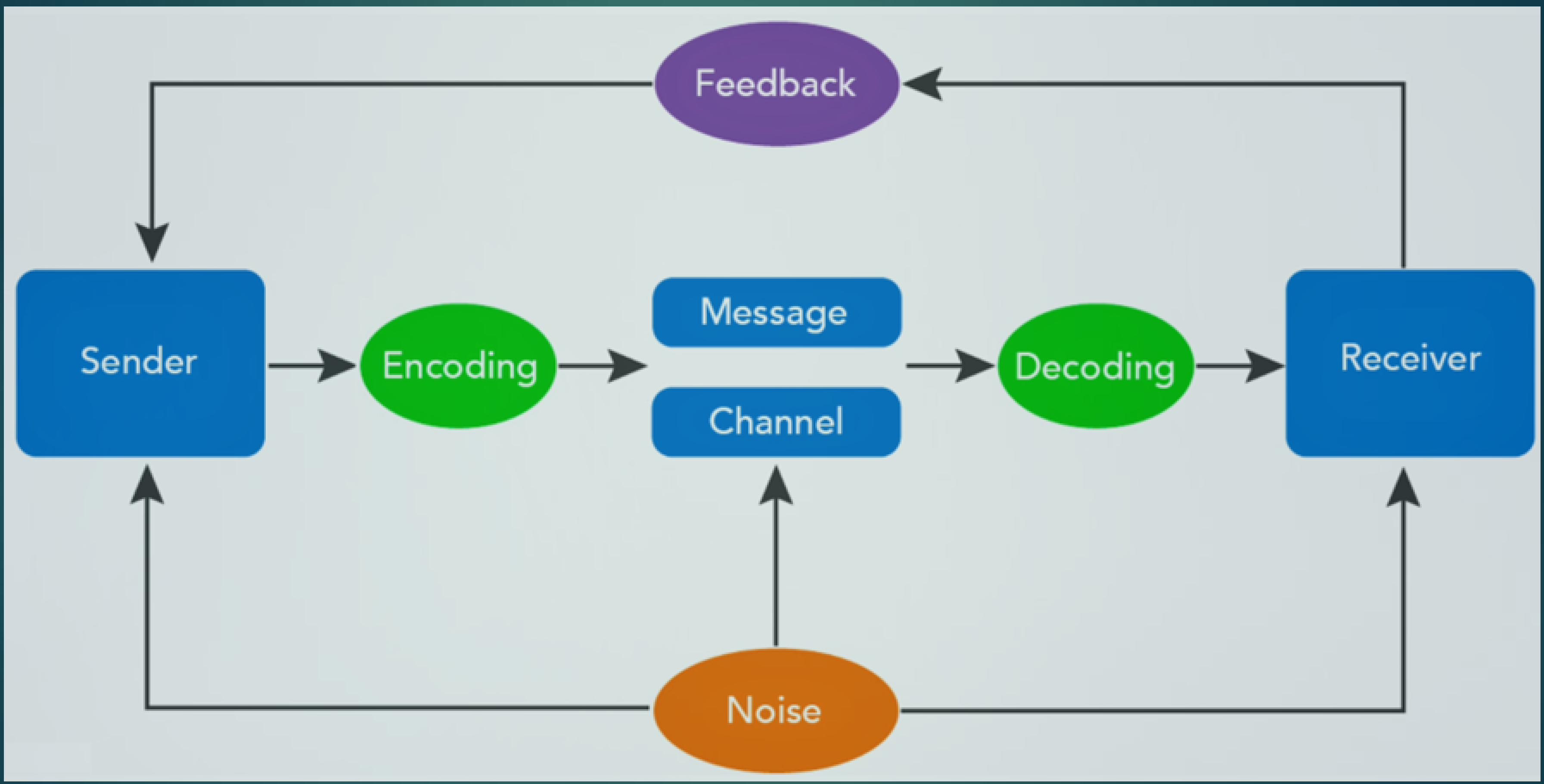
Why am I here?

- I saw a need for fundamentals after some of last years presentations here at DefCon
- I am a network routing and connectivity guy!
  - I thrive on BGP, EIGRP, and OSPF
- From a network standpoint, you have nothing to secure if you have no connectivity.

From Experience:

- Most communication problems are physical problems
- When the problem is not a physical problem, it is usually a simple & fundamental problem. This is the main reason I am here.
- All of these other experts here deal with the difficult problems. They may be fewer in number, but when they occur, they are serious problems.

Communication Process



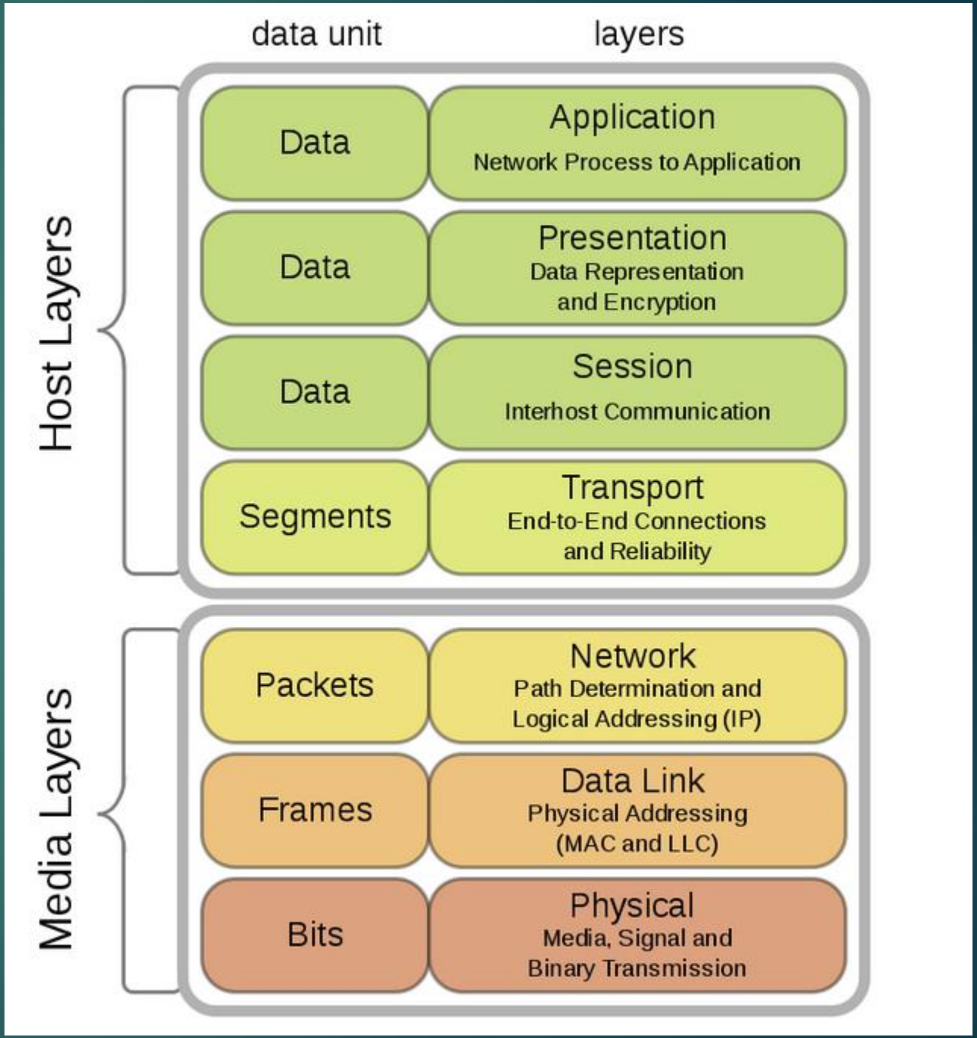
The Layered Model

- Benefits of a layered model
  - Reduce complexity
  - Standardize interfaces
  - Facilitate modular engineering
  - Ensure interoperable technologies
  - Accelerate evolution
  - Simplify teaching and learning

Overview of the OSI Model

- The International Standards Organizations developed the Open Systems Interconnect Model. (1984)
  - Seven layers
  - Each layer is independent of the other

Our focus will be the Media Layers



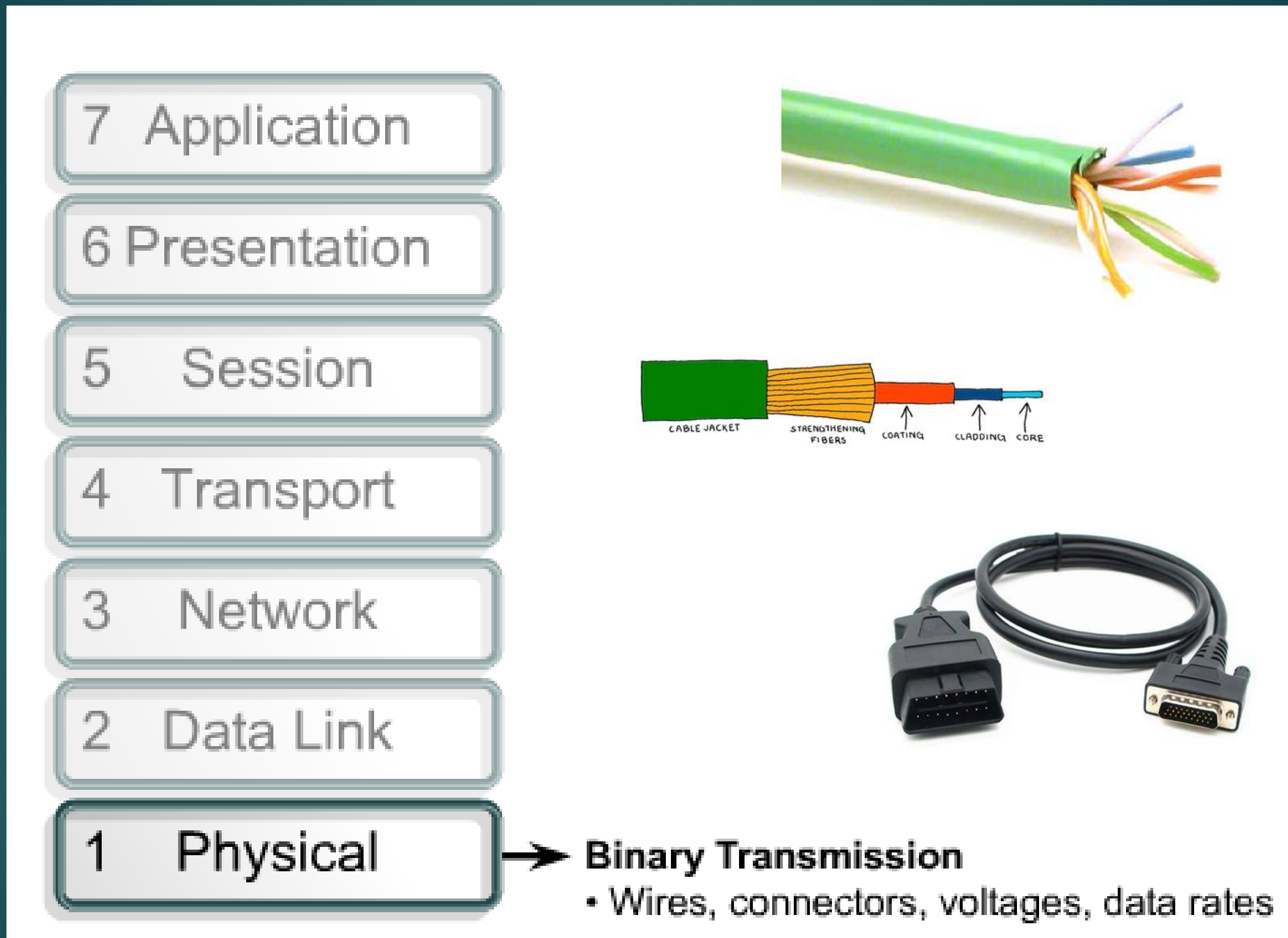
Standards Organizations

- The rules of the "road" are governed by many organizations:
  - EIA/TIA – Telecommunications Industry Assoc.
  - IETF –Internet Engineering Task Force
  - IEEE -Institute of Electrical and Electronics Engineers, Inc.
  - ITU - International Telecom. Union
  - ISO – International Organization for Standards
  - NIST – National Institute of Standards and Technology
  - IEC – International Electrotechnical Commission

OSI Layer 1
The Physical Network

- The previous mentioned organizations set standards for:
  - Cable pin-outs
  - Cable lengths
  - Cable support
  - Cable connector ends
  - Wiring closet sizes
  - Attenuation and noise tolerances
  - Signaling and encoding
  - Framing and encapsulation
  - And many other things.

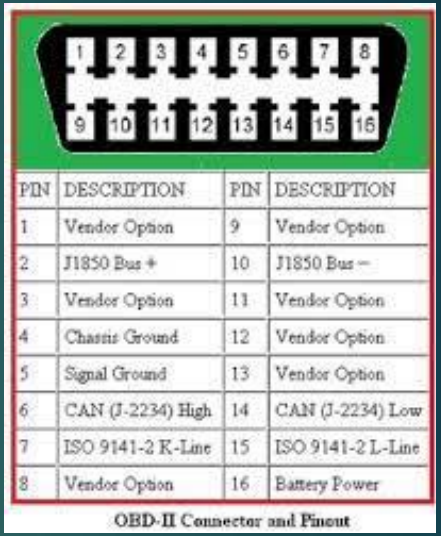
OSI Layer 1



7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
CABLE JACKET
STRENGTHENING FIBERS
COATING
CLADDING
CORE
Binary Transmission
• Wires, connectors, voltages, data rates

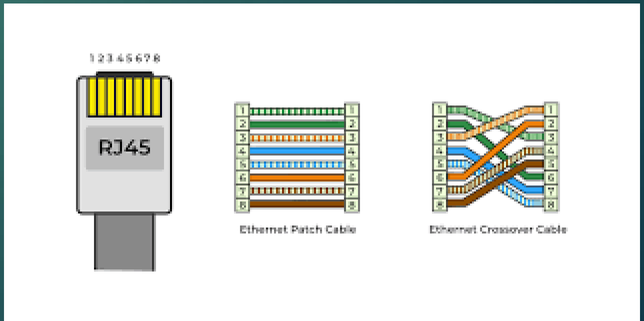
OSI Layer 1

- Physical Layer (L1 or Layer 1)
  - Connections and connector types
  - RTUs (sensors, valves, relays) for PLCs & DCS
  - Cables (Cat6, OBDII, etc)
  - Wireless
  - Fiber
  - Signaling standards
  - Voltages, attenuation, noise, etc



PIN	DESCRIPTION	PIN	DESCRIPTION
1	Vendor Option	9	Vendor Option
2	J1850 Bus +	10	J1850 Bus –
3	Vendor Option	11	Vendor Option
4	Chassis Ground	12	Vendor Option
5	Signal Ground	13	Vendor Option
6	CAN (J-2234) High	14	CAN (J-2234) Low
7	ISO 9141-2 K-Line	15	ISO 9141-2 L-Line
8	Vendor Option	16	Battery Power

OBD-II Connector and Pinout



OSI Layer 1
Network Analogy

Roads (are the cables)

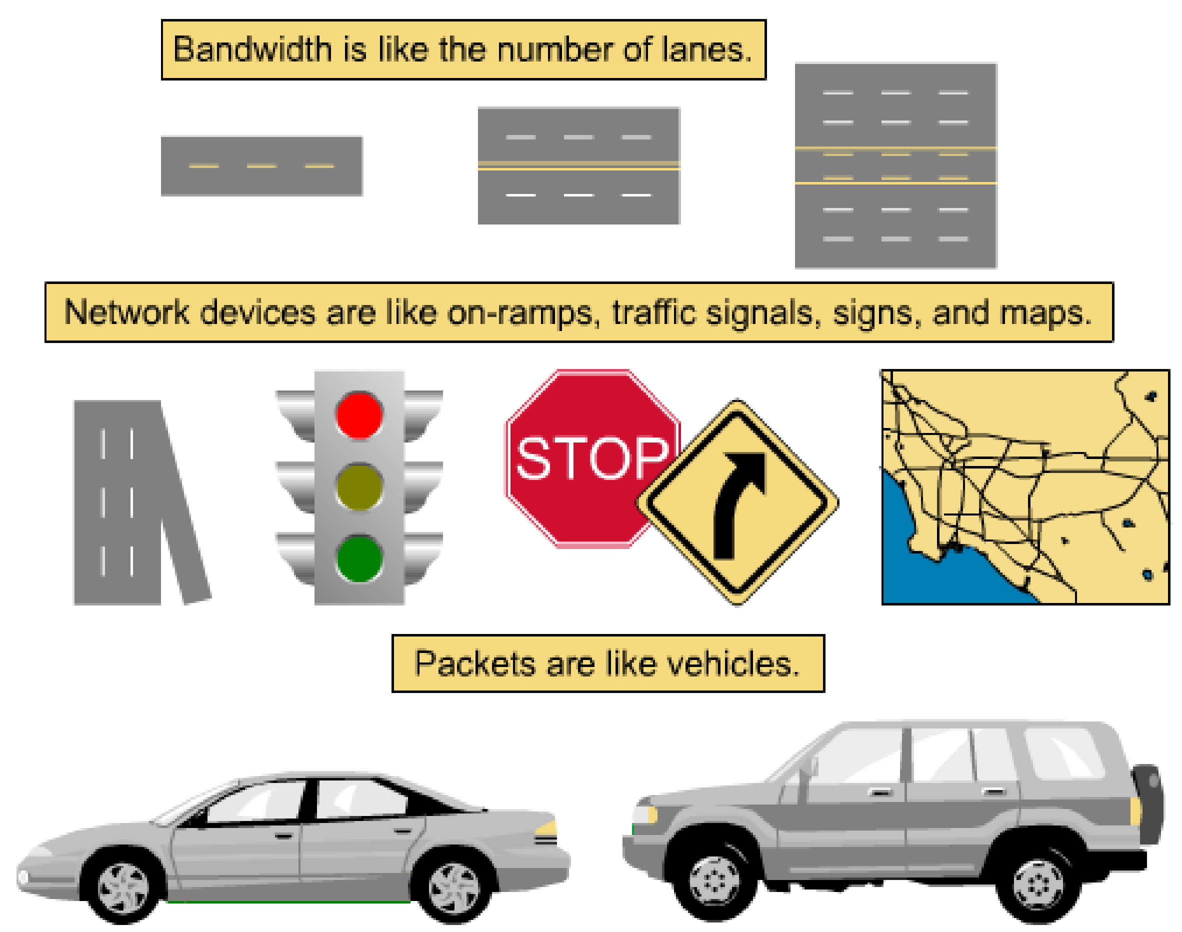
Superhighways (lots of bandwidth)

Local streets,
Alleys and side streets
(single lane/one way?)

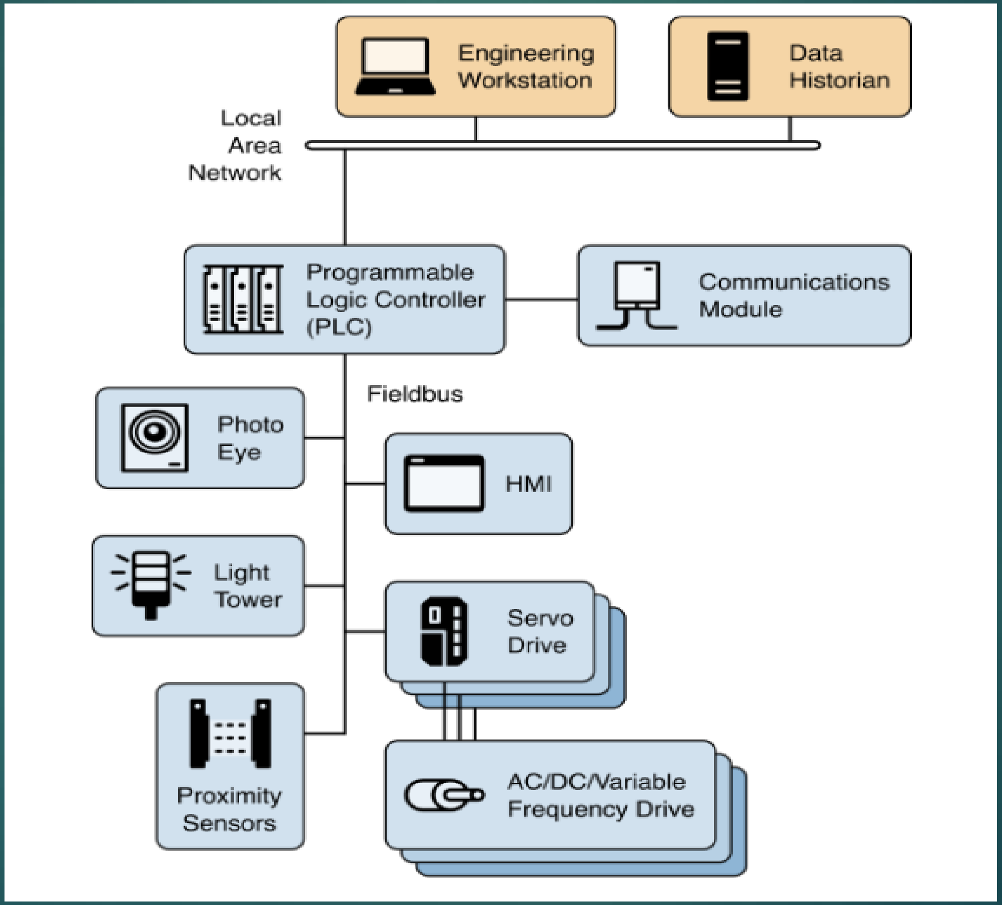
Traffic Laws (are the protocols)

Traffic signs and signals (routers and switches)

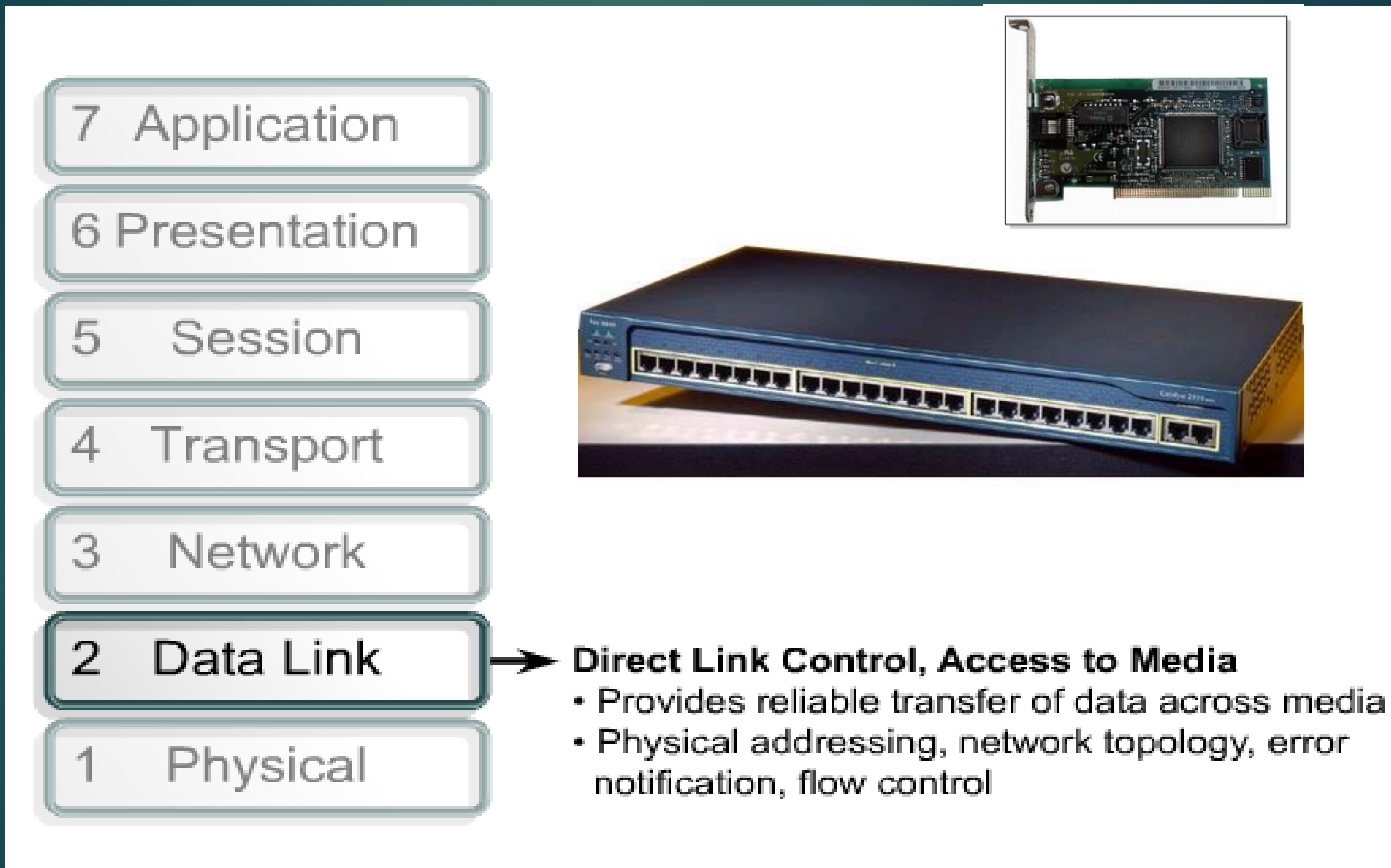
Bandwidth is not unlimited!
Bandwidth is NOT throughput.



OSI Layer 1
PLC Physical Example



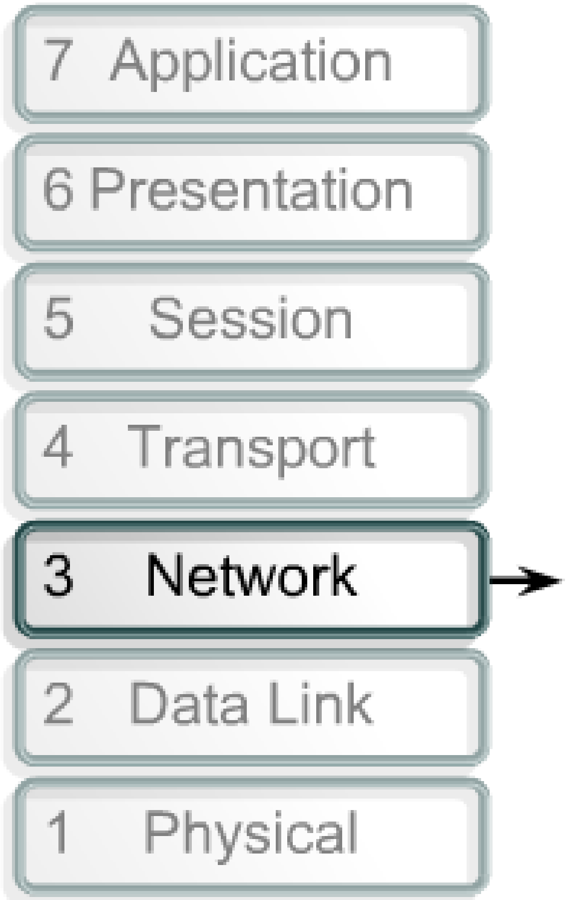
OSI Layer 2


7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Direct Link Control, Access to Media
• Provides reliable transfer of data across media
• Physical addressing, network topology, error notification, flow control

OSI Layer 2

- Data Link Layer (L2 or Layer 2)
  - Physical addressing – MAC for Ethernet
  - Framing
  - Network topology
  - Error detection
  - Access to media
  - Sub-Layers MAC and LLC
  - Ethernet
  - LAN Switches are L2 devices
  - CAN, FLEXRAY, Ethernet,

OSI Layer 3



Network Address and Best Path Determination

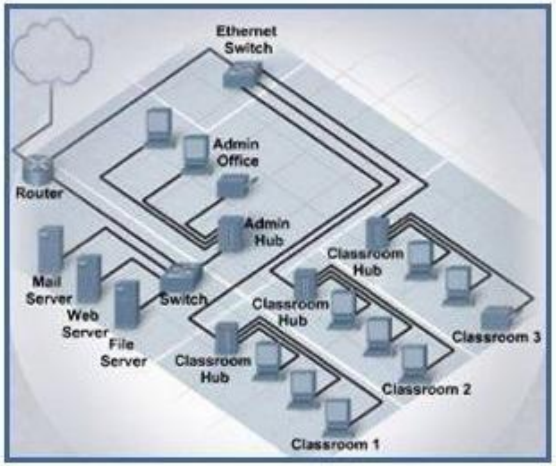
- Provides connectivity and path selection between two host
- Provides Logical address
- No error correction, best effort delivery.

OSI Layer 3

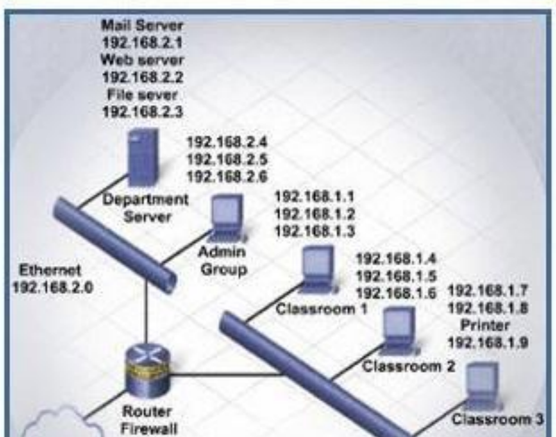
- Network Layer (L3 or Layer 3)
  - Logical addressing – IP address
  - Packets
  - Connection-less, best effort
  - Best path selection
  - Routers are Layer 3 devices

  - Post Office analogy

Documentation of Topo

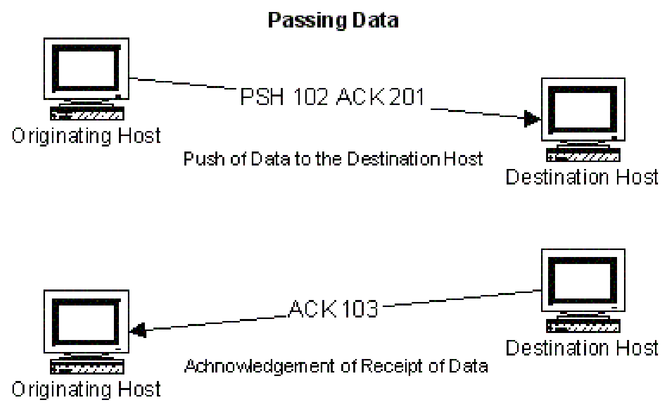


Physical topology is the physical layout of the components on the network.



Logical topology determines how the hosts access the medium to communicate across the network.

OSI Layer 4



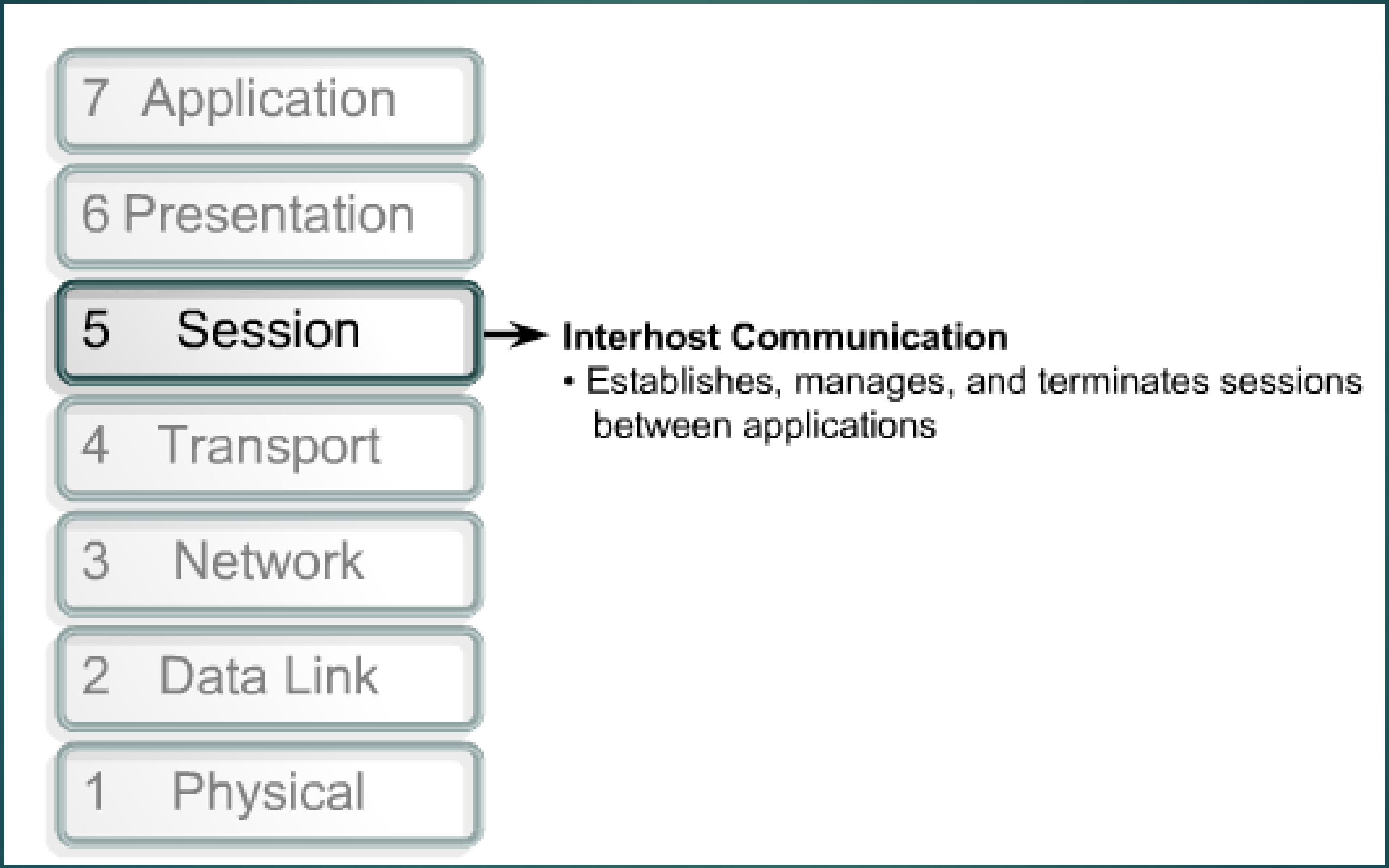
End-to-end Connections

- Concerned with transportation issues between hosts
- Data transport reliability
- Establish, maintain, terminate virtual circuits
- Fault detection and recovery information flow control

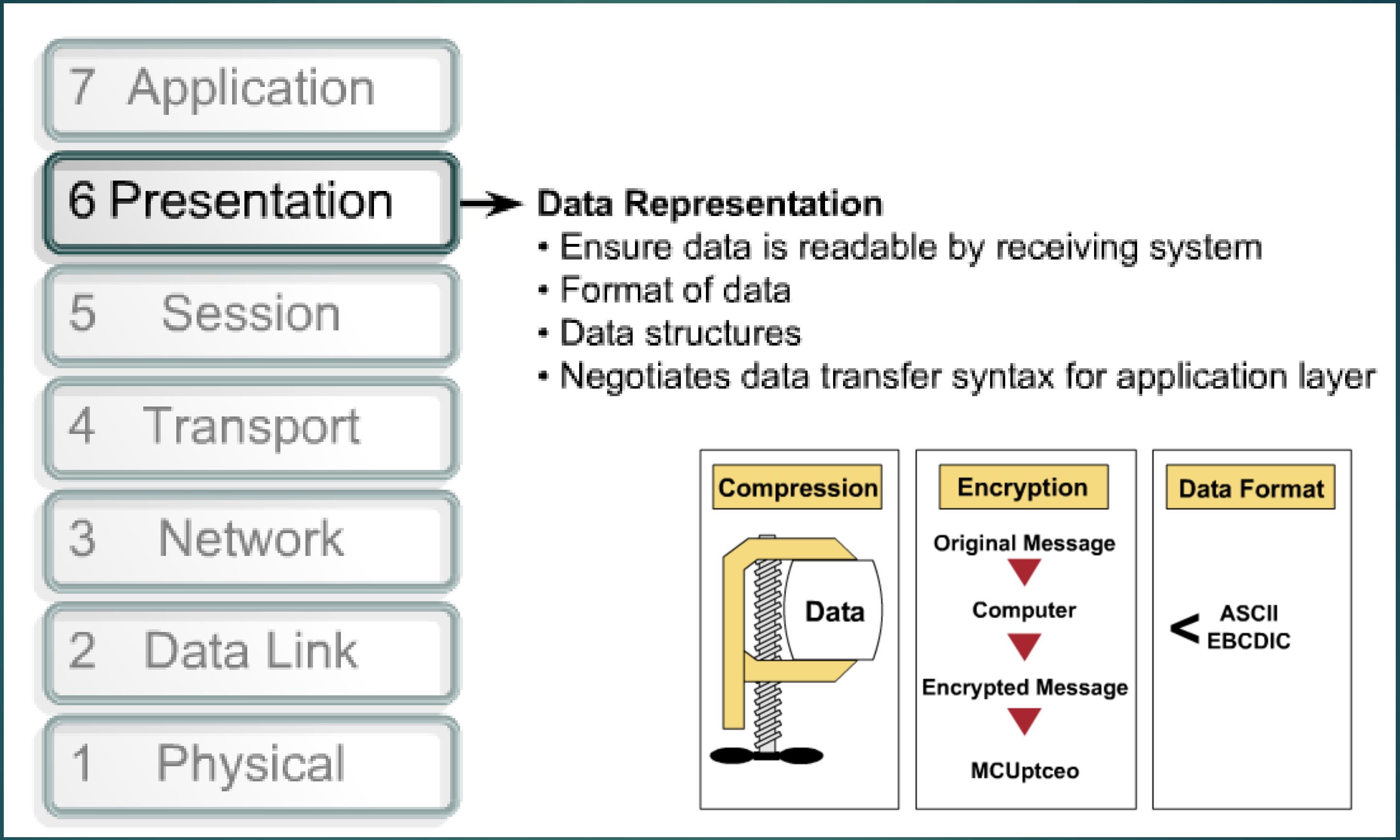
OSI Layer 4

- Transport Layer (L4 or Layer 4)
  - Segmentation of Data
  - Error correction
  - Reliability
  - End-to-end communication
  - Windowing
  - TCP and UDP
  - Use of Port numbers

OSI Layers 5


7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Interhost Communication
• Establishes, manages, and terminates sessions between applications

OSI Layer 6



7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Data Representation
• Ensure data is readable by receiving system
• Format of data
• Data structures
• Negotiates data transfer syntax for application layer
Compression
Data
Encryption
Original Message
Computer
Encrypted Message
MCUptceo
Data Format
<
ASCII
EBCDIC

OSI Layer 7

Network Processes to Applications

- Provides network services to application processes (such as electronic mail, file transfer, and terminal emulation)

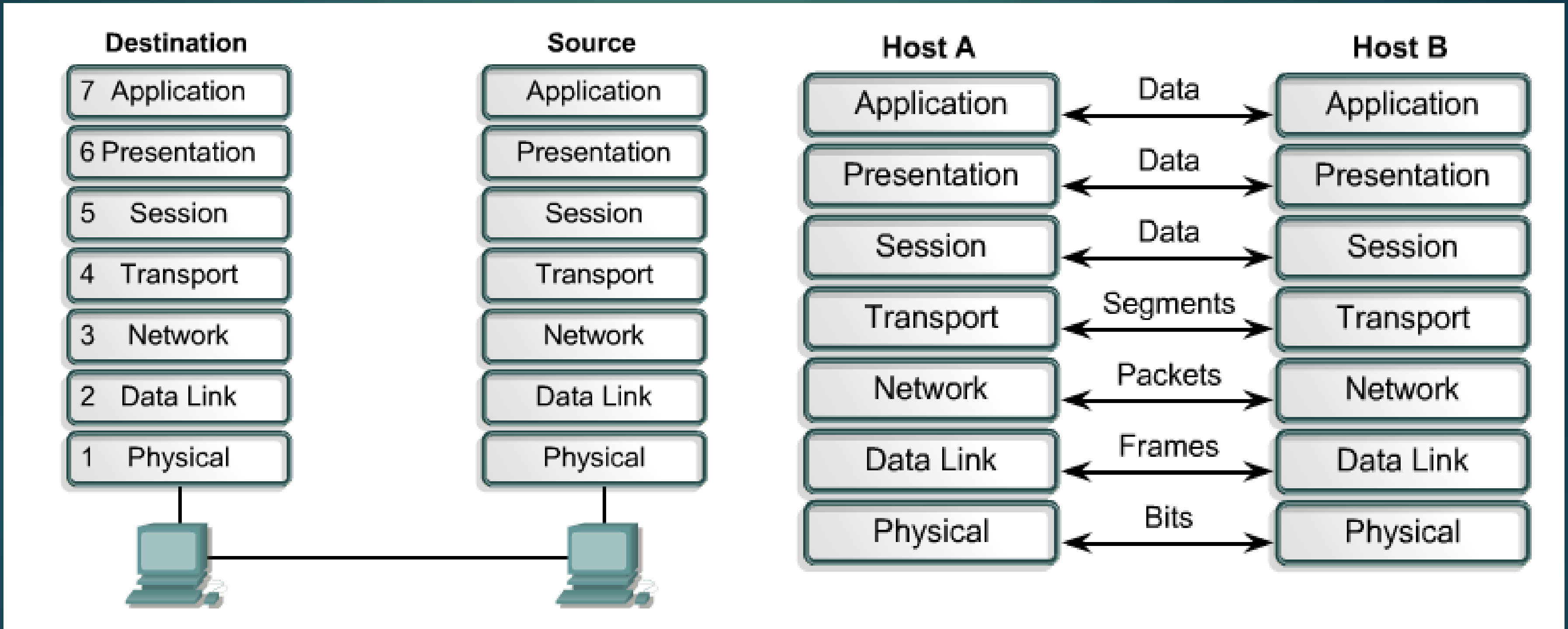
Common Application layer protocols
HTTP
Telnet
FTP
SNMP
DNS
FTP and TFTP
SMTP

OSI Layer 7

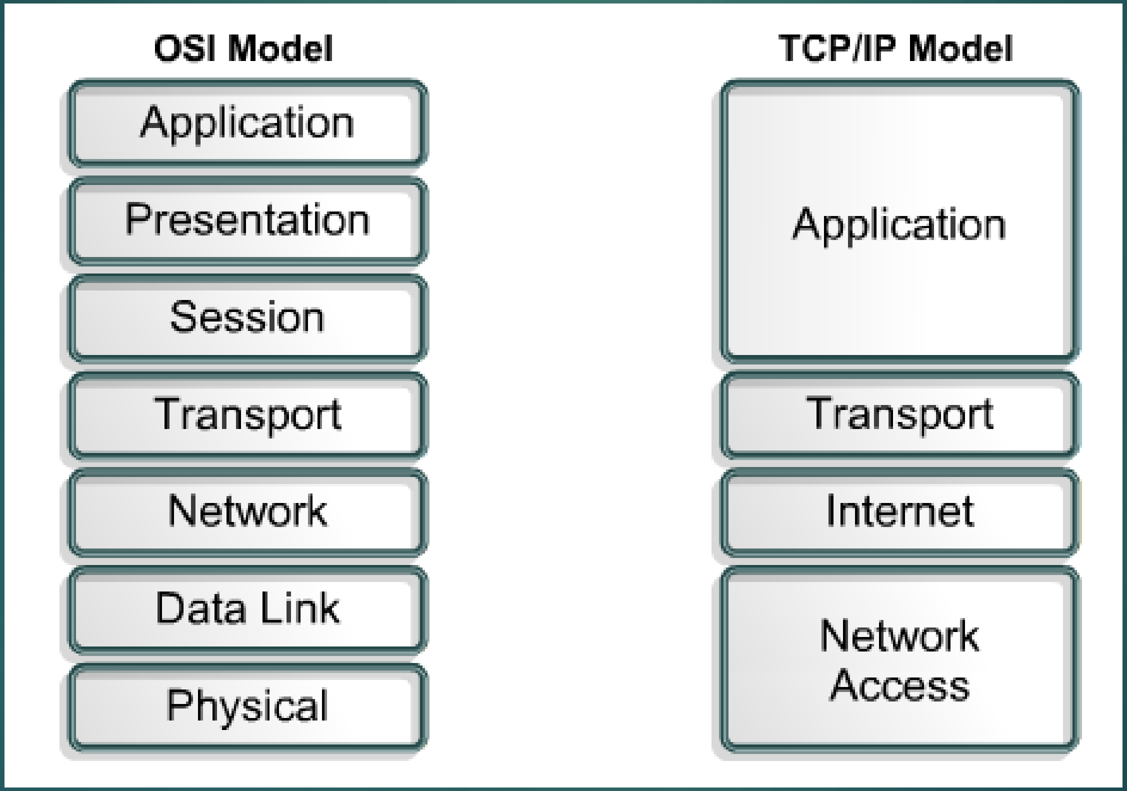
Application Layer (L7 or Layer 7)

- Identifying and establishing the availability of intended communication partners
- Synchronizing cooperating applications
- Establishing agreement on procedures for error recovery
- Controlling data integrity
    - Closest to the user
    - This is NOT the application you interact with
    - This is the underlying protocol of the application
        - HTML for web browsers
        - SMTP and POP3 for email

Peer-to-Peer Communication

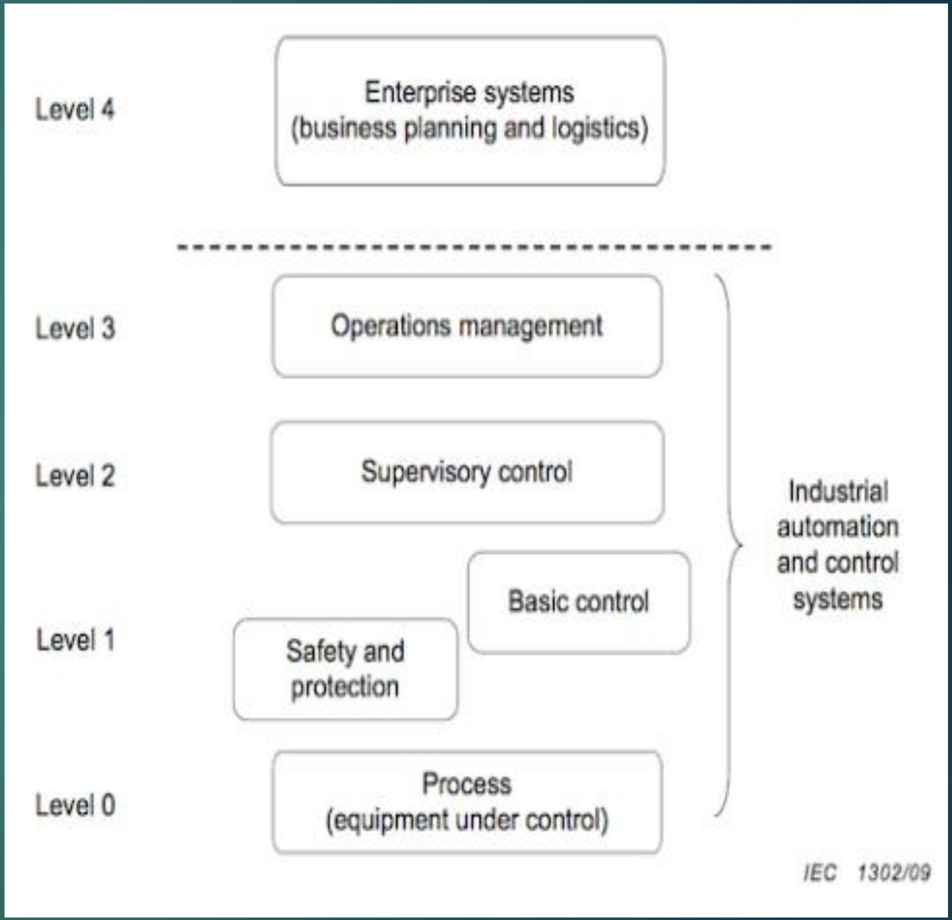


Compare:
OSI and TCP/IP models

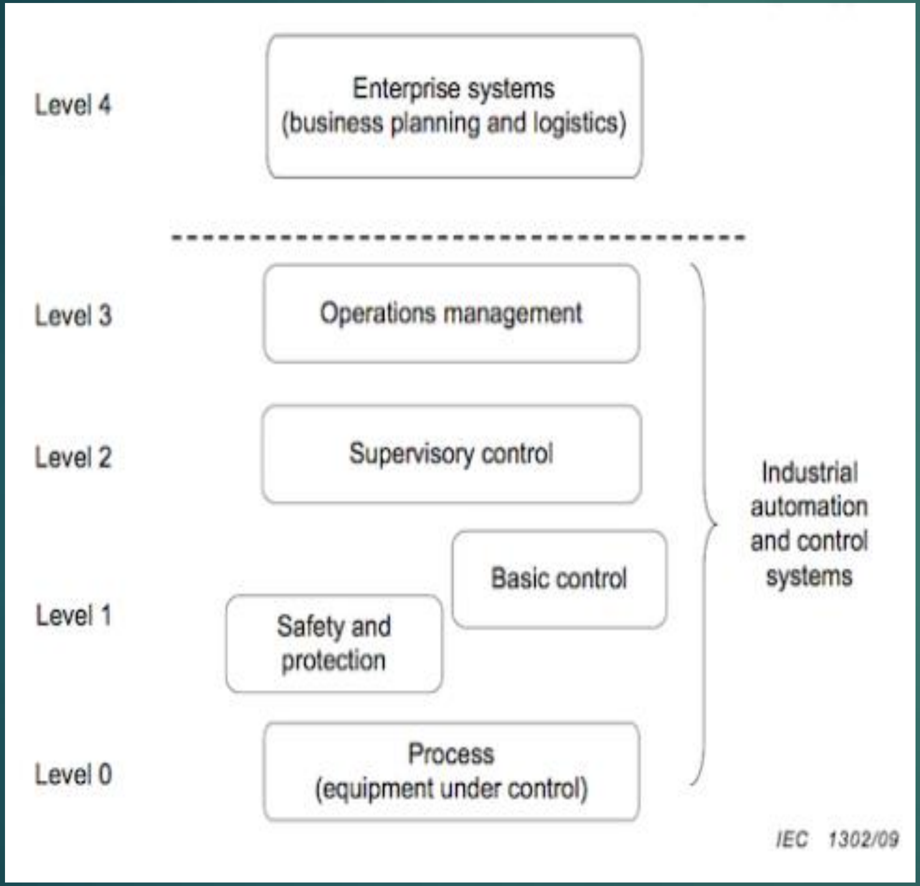


ICS Model

- From the Industrial Control System (ICS) point of view, a reference model describes a generic view of an integrated manufacturing or production system, expressed as a series of logical levels.
- IEC 62443 reference model adopting the segregation layers principle, with 5 layers in total that describe the fundamental categorization based on the functionality, interconnectivity, nature of operations and integrative approach.



ICS Model continued



<< Business Network

<< SCADA, Apps Server

<< DCS Control Server

<< PLC, DCS Controllers, RTU etc

<< Process I/O Devices

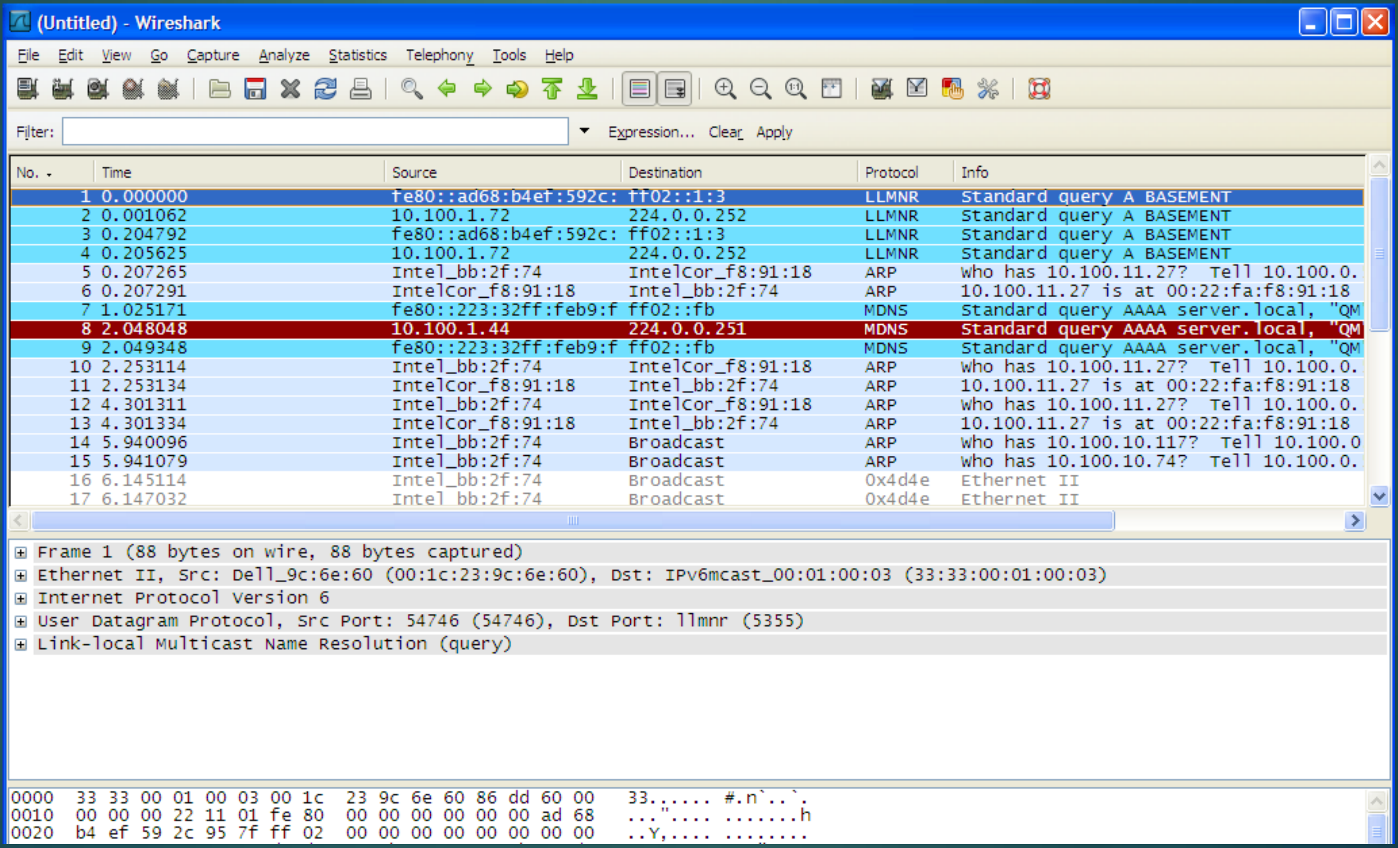
Compare: OSI & WWH OBD for Auto-Tech folks

<table>
<tr><th>OSI 7 layers</th><th colspan="5">OBDII</th><th colspan="3">WWH-OBD</th></tr>
<tr><td>Application (layer 7)</td><td colspan="5">ISO 15031-5/SAE J1979</td><td colspan="3">ISO 27145-3/ ISO 14229-2</td></tr>
<tr><td rowspan="2">Presentation (layer 6)</td><td colspan="5">ISO 15031-2, ISO 15031-5, ISO 15031-6</td><td colspan="3">ISO 27145-2</td></tr>
<tr><td colspan="5">SAE J1930-DA, SAE J1979-DA, SAE J2012-DA</td><td colspan="3">SAE J1930-DA, SAE J1979-DA, SAE J2012-DA</td></tr>
<tr><td>Session (layer 5)</td><td colspan="2">Not applicable</td><td colspan="6">ISO 14229-2</td></tr>
<tr><td>Transport (layer 4)</td><td colspan="2" rowspan="2">ISO 15031-5</td><td rowspan="2">ISO 14230-4</td><td rowspan="2">ISO 15765-2</td><td rowspan="4">ISO 15765-4</td><td rowspan="2">ISO 15765-2</td><td rowspan="4">ISO 15765-4</td><td rowspan="2">ISO 13400-2</td></tr>
<tr><td>Network (layer 3)</td></tr>
<tr><td>Data link (layer 2)</td><td rowspan="2">SAE J1850</td><td rowspan="2">ISO 9141-2</td><td>ISO 14230-2</td><td rowspan="2">ISO 11898-1, ISO 11898-2</td><td rowspan="2">ISO 11898-1, ISO 11898-2</td><td rowspan="2">ISO 13400-3 (DoIP- Wired Interface Based on IEEE 802.3)</td></tr>
<tr><td>Physical (layer 1)</td><td>ISO 14230-1</td></tr>
</table>

https://www.embitel.com/blog/embedded-blog/how-wwh-obd-is-steering-on-board-diagnostics-towards-

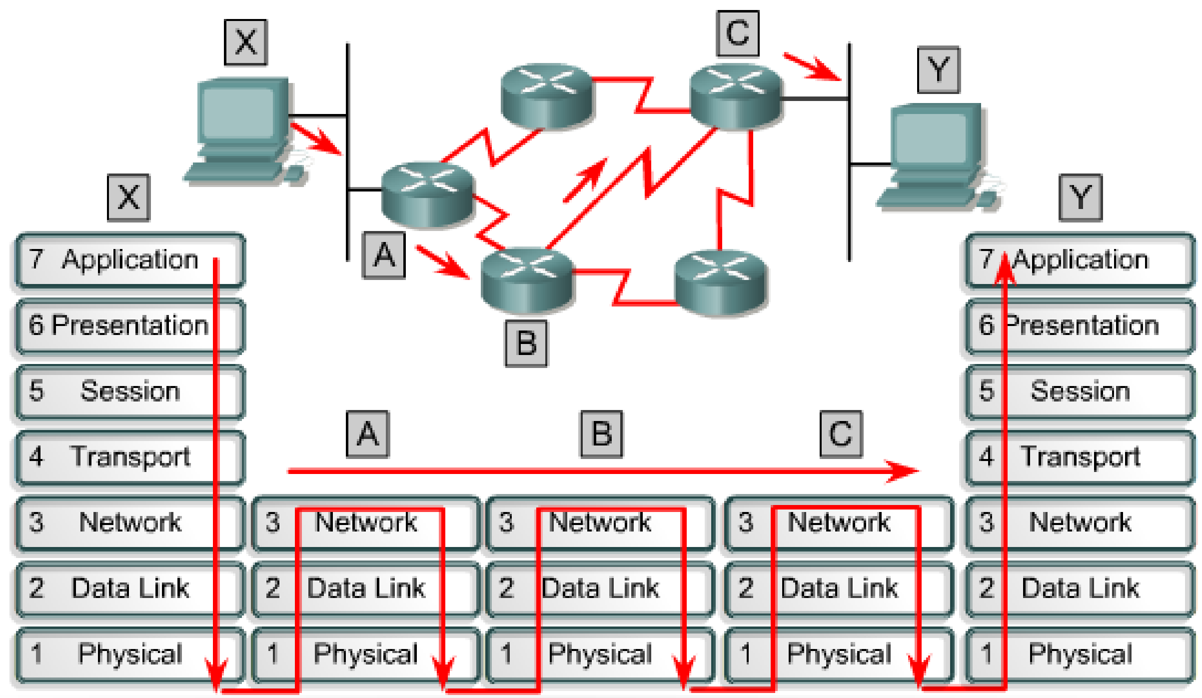
You can't be for real?

- Example-Wireshark (if time is short, skip to 55)



Putting it together

- Data flow example



Each router provides its services to support upper-layer functions.

Wireshark demonstration

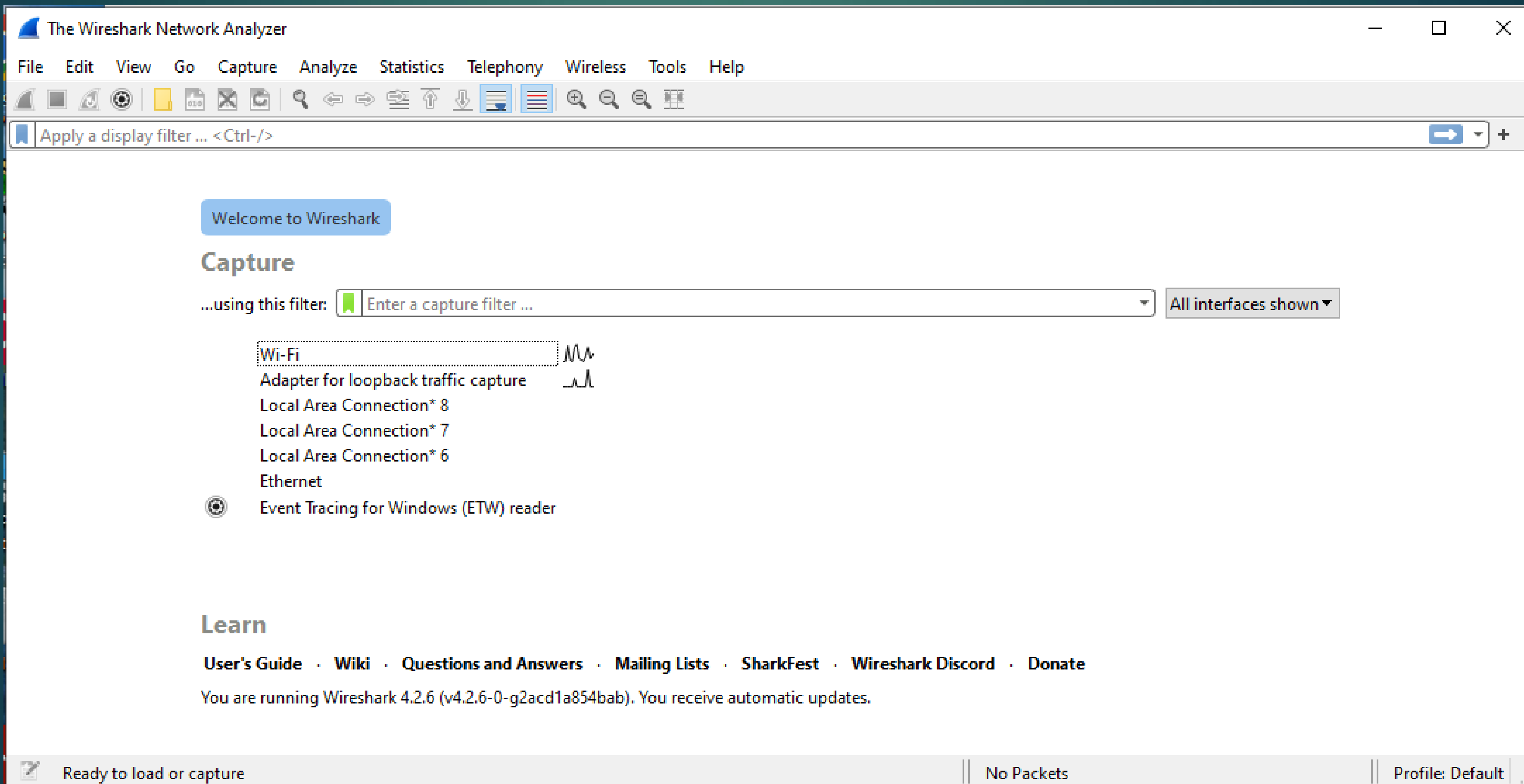
- Our Wireshark capture will prove what we have learned today. Free at Wireshark.org

<<<< Demonstration >>>>

Steps:

1. Run Wireshark Application and begin capture
2. Open Command Prompt and Ping aol.com
3. Stop packet capture
4. Analyze captured data

Opening Wireshark App

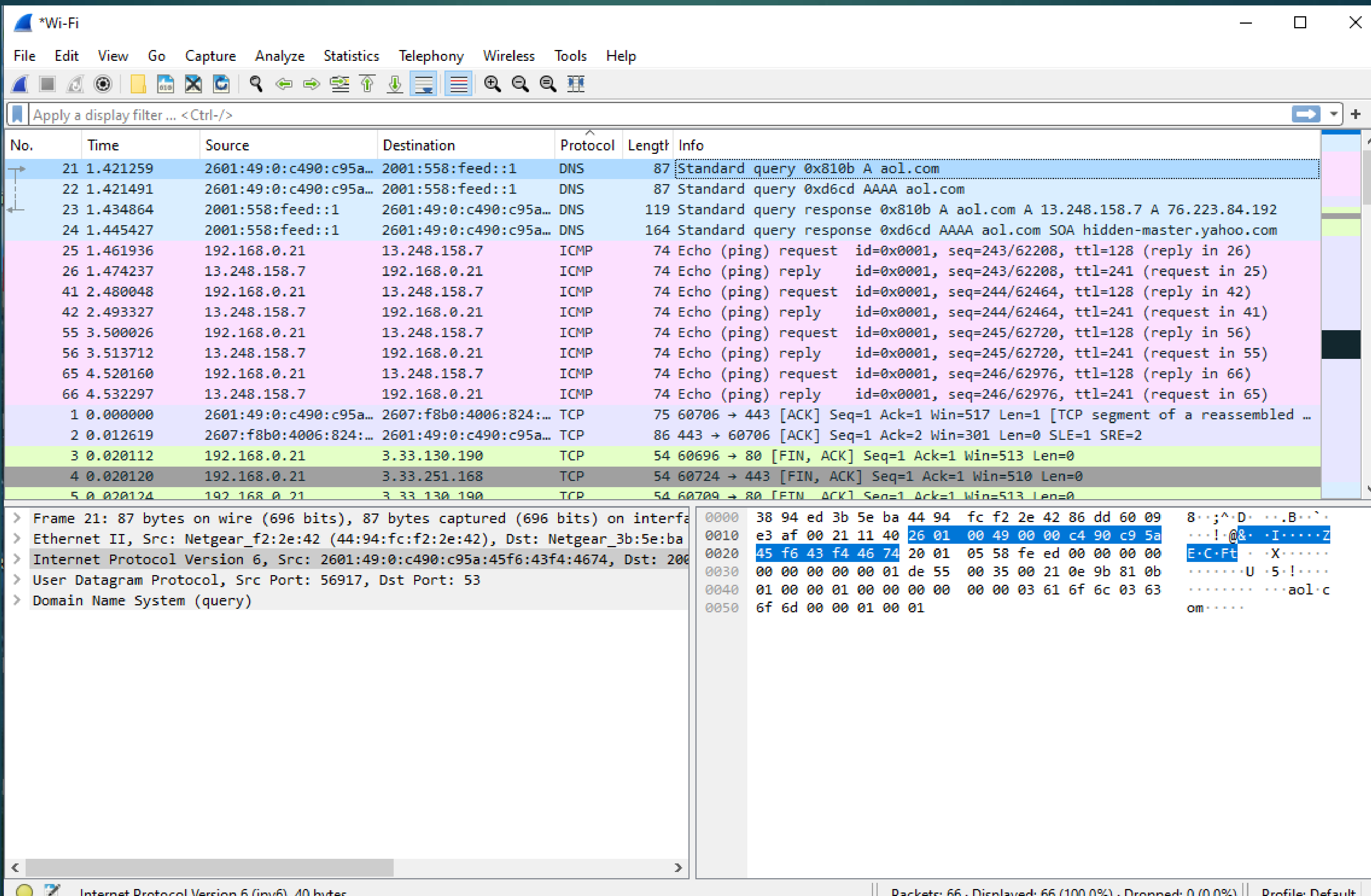


Ping

Select Command Prompt

```
Microsoft Windows [Version 10.0.19045.4651]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping aol.com

Pinging aol.com [13.248.158.7] with 32 bytes of data:
Reply from 13.248.158.7: bytes=32 time=12ms TTL=241
Reply from 13.248.158.7: bytes=32 time=13ms TTL=241
Reply from 13.248.158.7: bytes=32 time=13ms TTL=241
Reply from 13.248.158.7: bytes=32 time=12ms TTL=241

Ping statistics for 13.248.158.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 13ms, Average = 12ms

C:\Users\Administrator>
```

Analysis - Capture



Analysis: The Layers

```
> Frame 21: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{FE2C7701-3C29-4809-B692-BBCE0AC54D85}, id 0
v Ethernet II, Src: Netgear_f2:2e:42 (44:94:fc:f2:2e:42), Dst: Netgear_3b:5e:ba (38:94:ed:3b:5e:ba)
  > Destination: Netgear_3b:5e:ba (38:94:ed:3b:5e:ba)
  > Source: Netgear_f2:2e:42 (44:94:fc:f2:2e:42)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2601:49:0:c490:c95a:45f6:43f4:4674, Dst: 2001:558:feed::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1001 1110 0011 1010 1111 = Flow Label: 0x9e3af
    Payload Length: 33
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2601:49:0:c490:c95a:45f6:43f4:4674
    Destination Address: 2001:558:feed::1
v User Datagram Protocol, Src Port: 56917, Dst Port: 53
    Source Port: 56917
    Destination Port: 53
    Length: 33
    Checksum: 0x0e9b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (25 bytes)
> Domain Name System (query)
```

Analysis: The Application

```
> Frame 21: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_{FE2C7701-3C29-4809-B692-BBCE0AC54D85}, id 0
> Ethernet II, Src: Netgear_f2:2e:42 (44:94:fc:f2:2e:42), Dst: Netgear_3b:5e:ba (38:94:ed:3b:5e:ba)
> Internet Protocol Version 6, Src: 2601:49:0:c490:c95a:45f6:43f4:4674, Dst: 2001:558:feed::1
> User Datagram Protocol, Src Port: 56917, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x810b
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v aol.com: type A, class IN
        Name: aol.com
        [Name Length: 7]
        [Label Count: 2]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
    [Response In: 23]
```

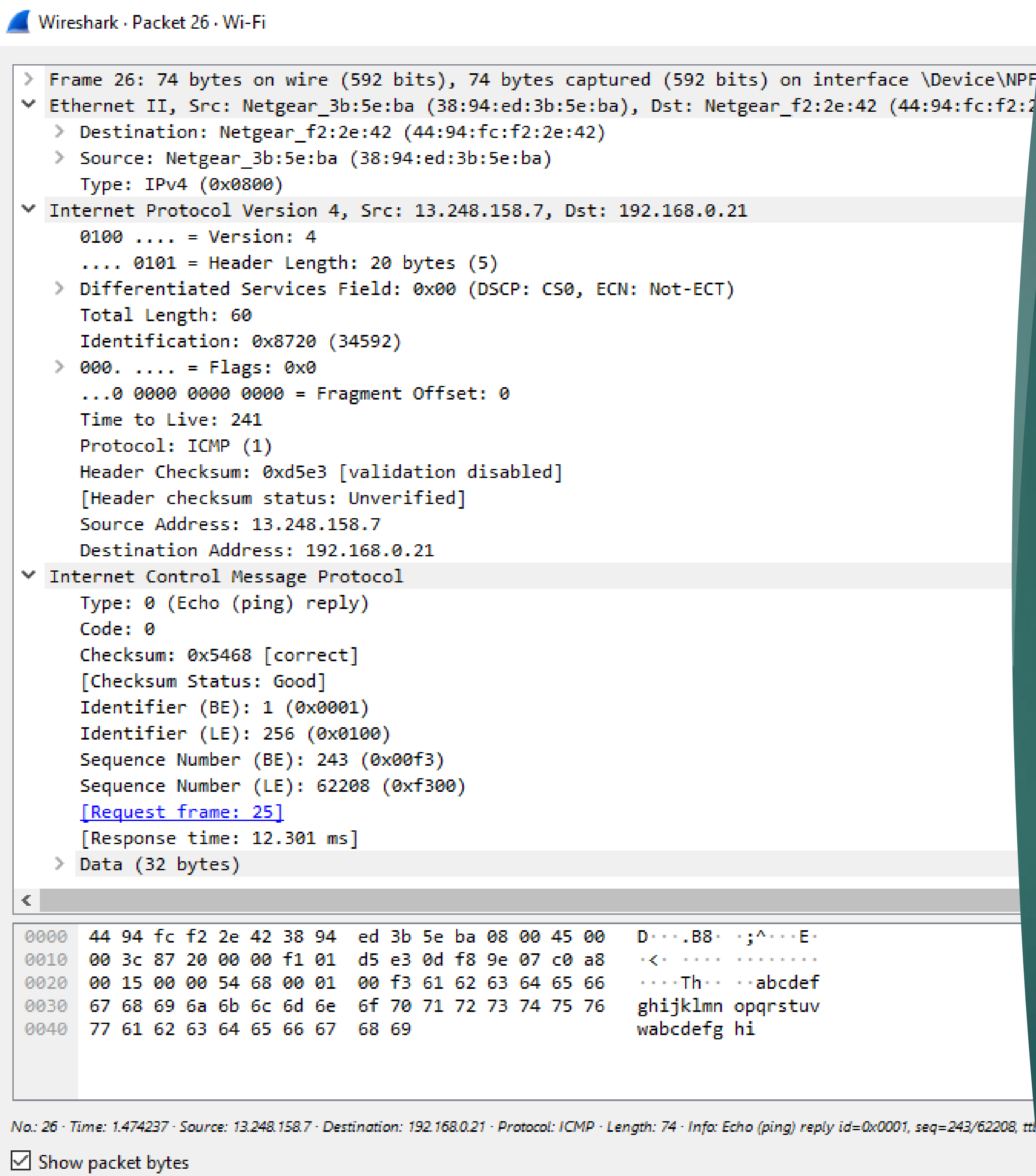
Analysis: The Application

```
> Frame 23: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface \Device\NPF_{FE2C7701-3C29-4809-B692-BBCE0AC54D85}, ic
> Ethernet II, Src: Netgear_3b:5e:ba (38:94:ed:3b:5e:ba), Dst: Netgear_f2:2e:42 (44:94:fc:f2:2e:42)
> Internet Protocol Version 6, Src: 2001:558:feed::1, Dst: 2601:49:0:c490:c95a:45f6:43f4:4674
> User Datagram Protocol, Src Port: 53, Dst Port: 56917
v Domain Name System (response)
    Transaction ID: 0x810b
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v aol.com: type A, class IN
        Name: aol.com
        [Name Length: 7]
        [Label Count: 2]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  v Answers
    v aol.com: type A, class IN, addr 13.248.158.7
        Name: aol.com
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 1239 (20 minutes, 39 seconds)
        Data length: 4
        Address: 13.248.158.7
```

Analysis: The Ping

```
Wireshark · Packet 25 · Wi-Fi

> Frame 25: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interfa
v Ethernet II, Src: Netgear_f2:2e:42 (44:94:fc:f2:2e:42), Dst: Netgear_3b:5e:ba
    > Destination: Netgear_3b:5e:ba (38:94:ed:3b:5e:ba)
    > Source: Netgear_f2:2e:42 (44:94:fc:f2:2e:42)
      Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.0.21, Dst: 13.248.158.7
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 60
      Identification: 0x8720 (34592)
    > 000. .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 128
      Protocol: ICMP (1)
      Header Checksum: 0x46e4 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.0.21
      Destination Address: 13.248.158.7
v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x4c68 [correct]
      [Checksum Status: Good]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 243 (0x00f3)
      Sequence Number (LE): 62208 (0xf300)
      [Response frame: 26]
    > Data (32 bytes)

0000  38 94 ed 3b 5e ba 44 94  fc f2 2e 42 08 00 45 00   8··;^·D· ··.B··E·
0010  00 3c 87 20 00 00 80 01  46 e4 c0 a8 00 15 0d f8   ·<· ···· F·······
0020  9e 07 08 00 4c 68 00 01  00 f3 61 62 63 64 65 66   ····Lh·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Analysis: The Ping Reply



Alt Analysis: A Look at TCP

Wireshark · Packet 1 · Wi-Fi

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{24C61B79-D675-45AD-85CC-4CB1D9F84671}, id 0
> Ethernet II, Src: IntelCor_cb:fb:3d (b4:6b:fc:cb:fb:3d), Dst: 4a:92:8c:2d:f8:27 (4a:92:8c:2d:f8:27)
> Internet Protocol Version 4, Src: 192.168.66.30, Dst: 208.73.176.100
v Transmission Control Protocol, Src Port: 28533, Dst Port: 80, Seq: 0, Len: 0
     Source Port: 28533
     Destination Port: 80
     [Stream index: 0]
     [Conversation completeness: Incomplete, SYN_SENT (1)]
     [TCP Segment Len: 0]
     Sequence Number: 0    (relative sequence number)
     Sequence Number (raw): 4278622271
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 0
     Acknowledgment number (raw): 0
     1000 .... = Header Length: 32 bytes (8)
   v Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Accurate ECN: Not set
        .... 0... .... = Congestion Window Reduced: Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
      > .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ··········S·]
     Window: 64240
     [Calculated window size: 64240]
     Checksum: 0xe99e [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
   > [Timestamps]
```

Alt Analysis: A look at ftp

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

No.	Time	Source	Destination	Protocol	Length	Info
85	6.877479	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	80	Response: 220-
86	6.877479	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	155	Response: 220--
87	6.877479	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	133	Response: 220- R S Y N C . O S U O S L . O R G
88	6.877479	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	129	Response: 220- Oregon State University
89	6.877479	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	125	Response: 220- Open Source Lab
90	6.877479	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	80	Response: 220-
91	6.877479	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	148	Response: 220- Unauthorized use is prohibited - violators will be prosecuted
92	6.877479	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	155	Response: 220--
93	6.877479	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	80	Response: 220-
94	6.877479	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	137	Response: 220- For more information about the OSL visit:
97	7.085937	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	442	Response: 220- http://osuosl.org/services/hosting
99	7.133650	2600:1011:b023:1664…	2600:3404:200:237::2	FTP	88	Request: OPTS UTF8 ON
102	7.331048	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	100	Response: 200 Always in UTF8 mode.
123	12.210989	2600:1011:b023:1664…	2600:3404:200:237::2	FTP	90	Request: USER anonymous
132	17.662857	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	108	Response: 331 Please specify the password.
211	33.678761	2600:1011:b023:1664…	2600:3404:200:237::2	FTP	98	Request: PASS KevinAtICSVillage
214	34.188997	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	97	Response: 230 Login successful.
237	37.075737	2600:1011:b023:1664…	2600:3404:200:237::2	FTP	130	Request: EPRT |2|2600:1011:b023:1664:24d2:65ab:e9c0:d03a|29758|
253	37.766753	2600:3404:200:237::2	2600:1011:b023:1664…	FTP	125	Response: 200 EPRT command successful. Consider using EPSV.
269	37.807583	2600:1011:b023:1664…	2600:3404:200:237::2	FTP	80	Request: LIST

Alt Analysis: A look at ftp

Wireshark · Follow TCP Stream (tcp.stream eq 1) · Wi-Fi

```
220-
220-----------------------------------------------------------------------------
220-                      R S Y N C . O S U O S L . O R G
220-                          Oregon State University
220-                              Open Source Lab
220-
220-       Unauthorized use is prohibited - violators will be prosecuted
220-----------------------------------------------------------------------------
220-
220-                For more information about the OSL visit:
220-                    http://osuosl.org/services/hosting
220-
220-          This host is the home to the primary archives of several
220-           projects.  We would prefer that only primary/secondary
220-                    mirrors use this service.  Thanks!
220-
220-----------------------------------------------------------------------------
220-
220
OPTS UTF8 ON
200 Always in UTF8 mode.
USER anonymous
331 Please specify the password.
PASS KevinAtICSVillage
230 Login successful.
EPRT |2|2600:1011:b023:1664:24d2:65ab:e9c0:d03a|29758|
200 EPRT command successful. Consider using EPSV.
LIST
```

Alt Analysis: A look at ftp

```
File Transfer Protocol (FTP)
  USER anonymous\r\n
      Request command: USER
      Request arg: anonymous
  [Current working directory: ]
```

Alt Analysis: A look at ftp

```
v File Transfer Protocol (FTP)
  v PASS KevinAtICSVillage\r\n
      Request command: PASS
      Request arg: KevinAtICSVillage
  [Current working directory: ]
```

Take-aways from today:

- Documentation!
- Encapsulation Process
- DON'T use FTP
- Troubleshooting: bottom up approach

Thank you.

Kevin Manna, Professor Emeritus

Northampton Community College

Bethlehem, PA, USA

kmanna@northampton.edu