Introduction to Network Troubleshooting with Wireshark

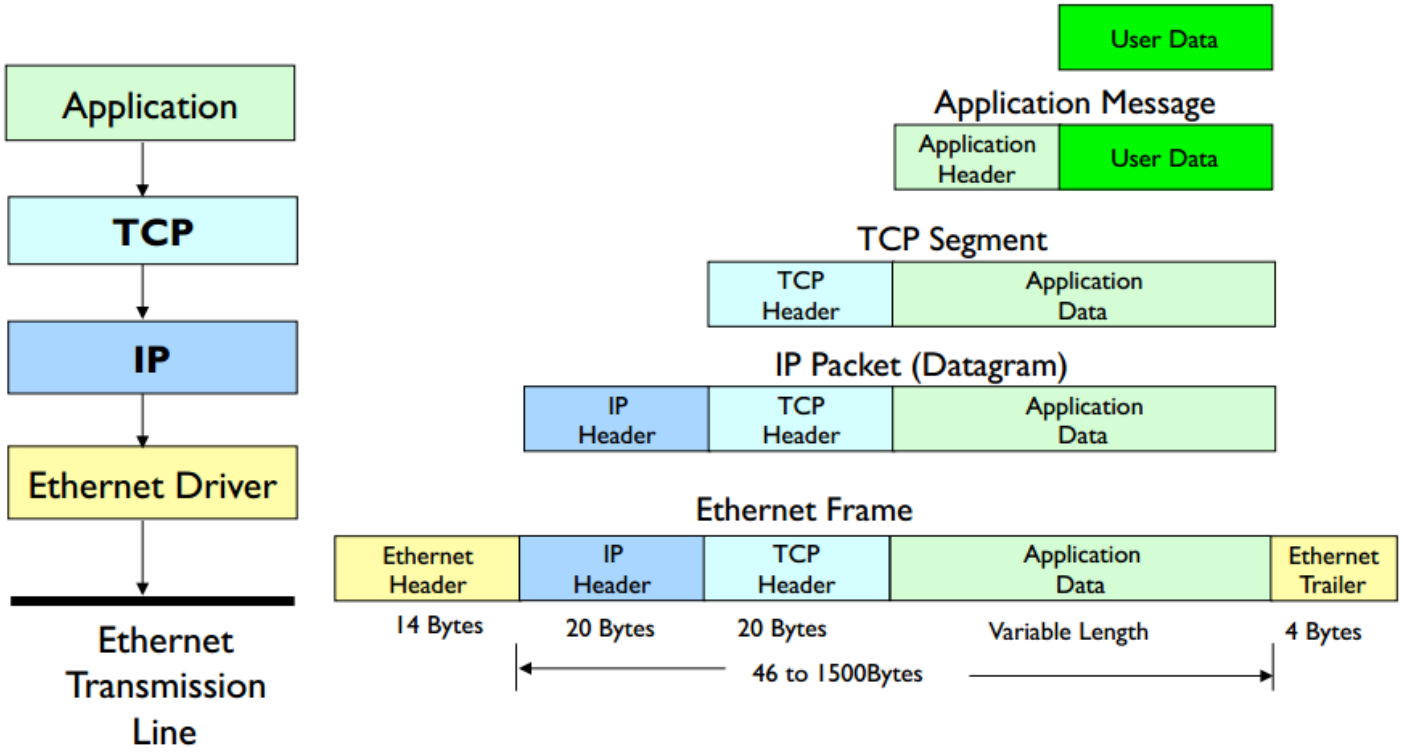
Introduction

In this class we'll look at the basics of using Wireshark to troubleshoot common network problems. We'll start with a basic Ethernet introduction and move on to using Wireshark to display data. Finally we'll look at real-world Ethernet data from a flight test scenario.

OSI 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		GATEWAY	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	PACKET FILTERING	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		Can be used on all layers	Internet
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	Land Based 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**			

Data in Layers



Layer 1 – Physical

- Standards define:
  - Signaling
  - Cabling
  - Connectors
- IEEE 802 is a family of standards covering the Data Link and Physical layer of the OSI networking reference model
- IEEE 802.3 defines Ethernet
- IEEE 802.11 defines Wireless LAN

Layer 2 – Data Link

- The Data Link layer is split into two sub layers
  - Logical Link Control (LLC)
  - Media Access Control (MAC)
- Addressing at this level is hardware unique – MAC address
- Channel access control mechanism
  - Most common is Carrier Sense Multiple Access / Carrier Detect (CSMA/CD) (802.3 standard)
  - Wireless uses CSMA/CA, ALOHA, TDMA, OFDMA
- Layer 2 Protocols
  - L2DP, LLDP, PPP, PPTP
- Layer 2 + 3 Protocols
  - ARP, RARP, SPB, X.25

MAC Addresses

- Six bytes of information
  - 00-1D-92-98-36-8A
- Globally Unique
  - Conflicts not allowed
- First three bytes = OUI = Vendor ID
  - Organizationally Unique Identifier – assigned by IEEE
  - 00:1D:92 = Micro-star International
  - http://aruljohn.com/mac/001D92

Layer 3 – Network

- IP lives here
- Protocols
  - ICMP – Internet Control Message Protocol (PING)
  - IGMP – Internet Group Management Protocol
  - IGRP – Interior Gateway Routing Protocol
  - IPv4 / IPv6 – Internet Protocol version 4 / 6
  - IPSec – Internet Protocol Security
  - IPX – Internetwork Packet Exchange
  - NDP – Neighbor Discovery Protocol
  - RIP – Routing Information Protocol

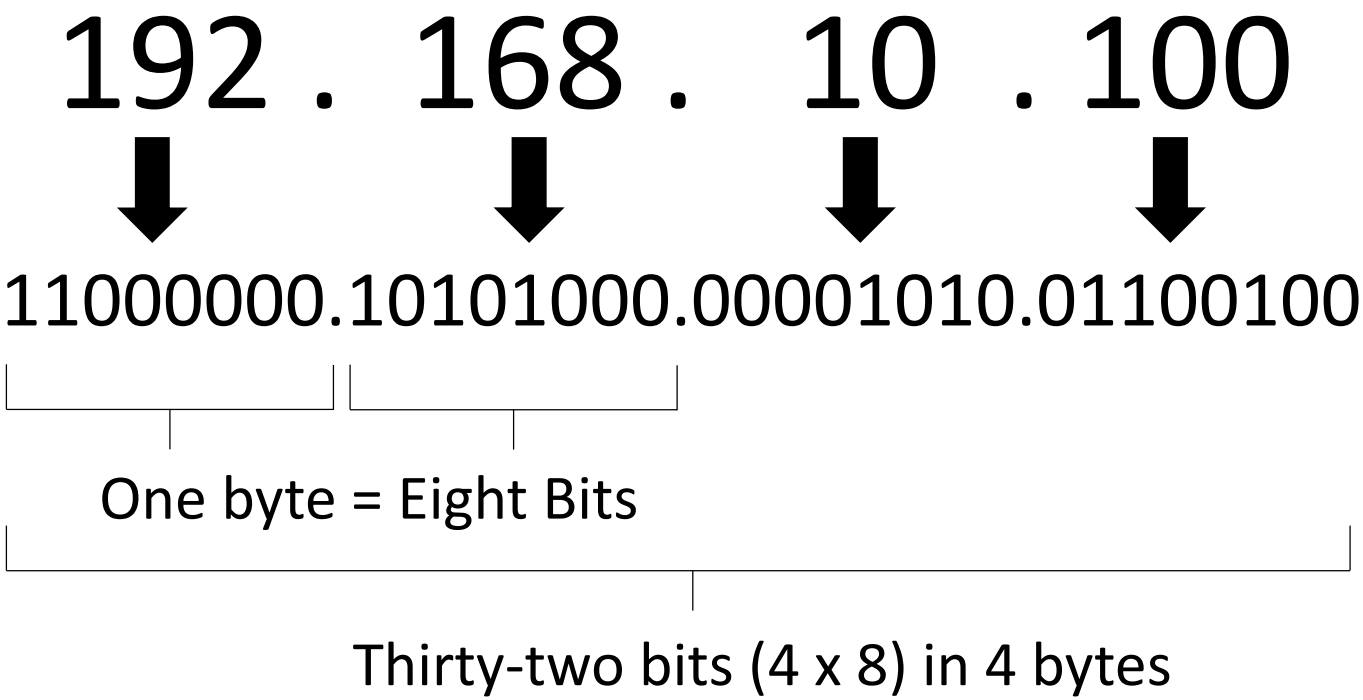
Packet Fundamentals

- IP Header = 24 Bytes
- TCP Header = minimum of 24 Bytes
- UDP Header = 8 Bytes exactly
- Maximum Transmission Unit (MTU) = 1500 bytes
  - Windows defaults to 1480 bytes
- Jumbo Frames
  - 9000-bytes long
  - Goal is to reduce packet overhead
  - CRC-based checksum

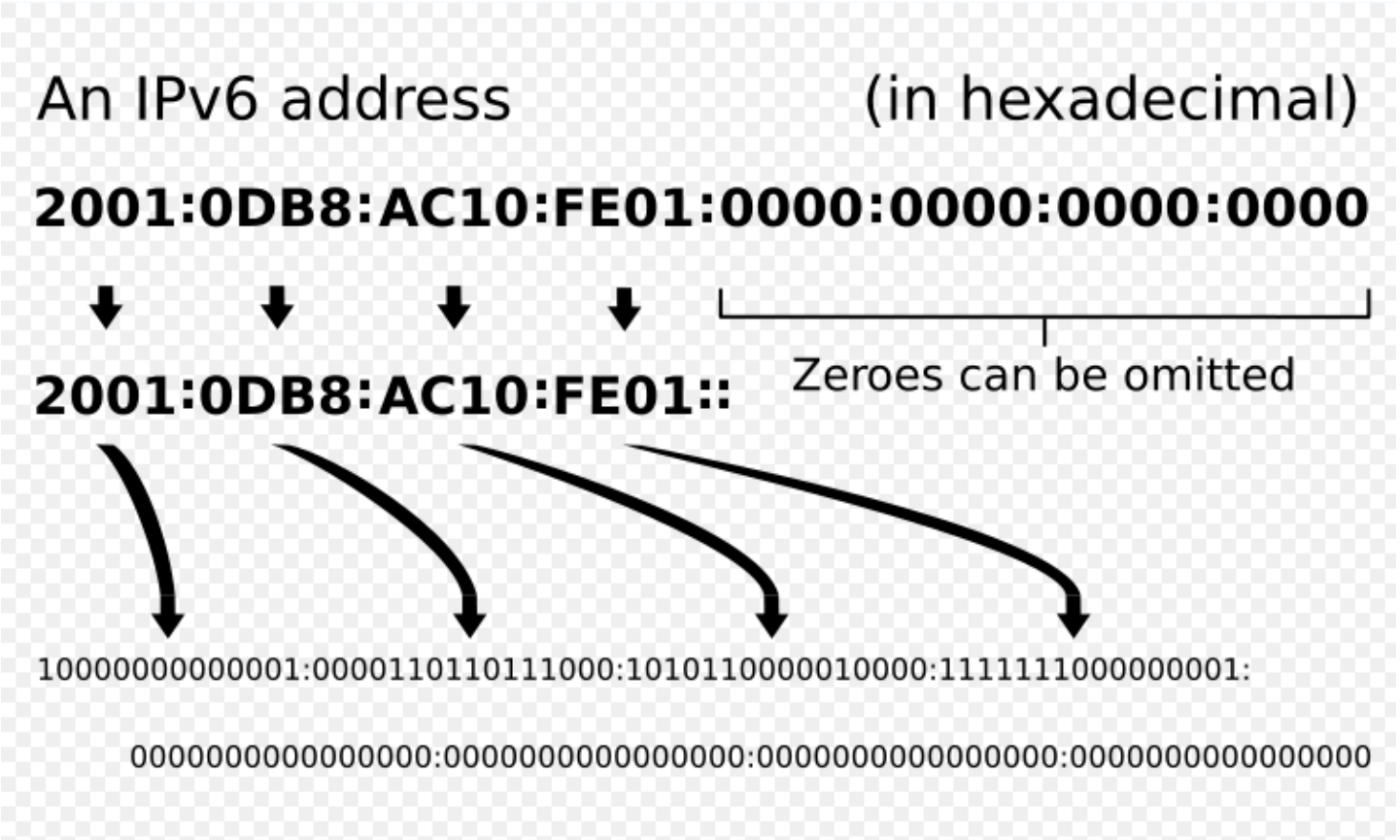
IP Addressing Basics

- IPv4 uses 32-bit addresses
- Class A (24-bit), B (20-bit) and C (16-bit)
- IPv4 addresses reserved in RFC 1918
- Dotted-decimal notation 192.168.1.1
- IPv6 uses 128-bit addresses
- IPv6 addresses reserved in RFC 4193
- Last octet may not be 0 or 255
  - 0 used for network identifier
  - 255 = broadcast address

IPv4 Addressing Details



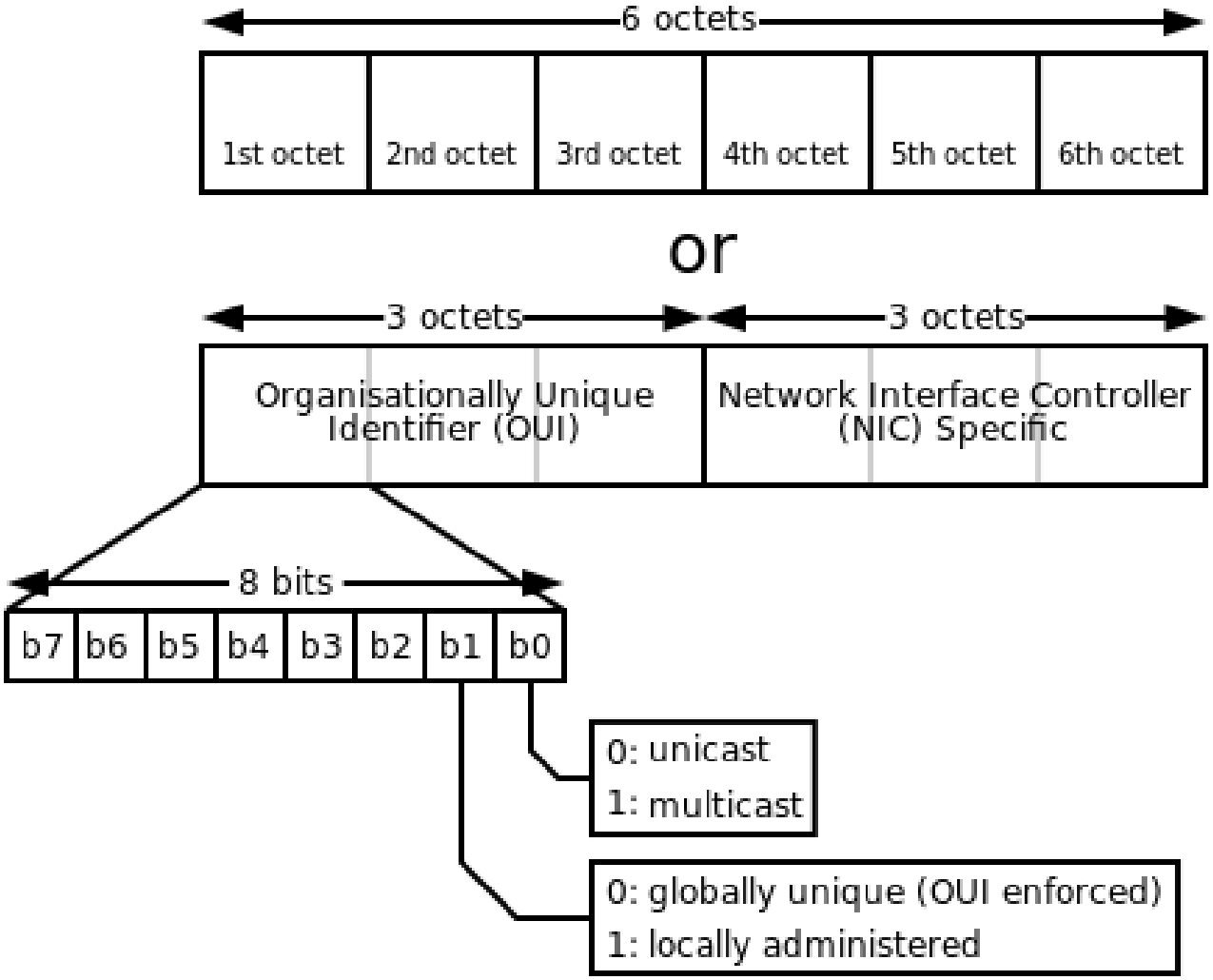
IPv6 Addressing Details



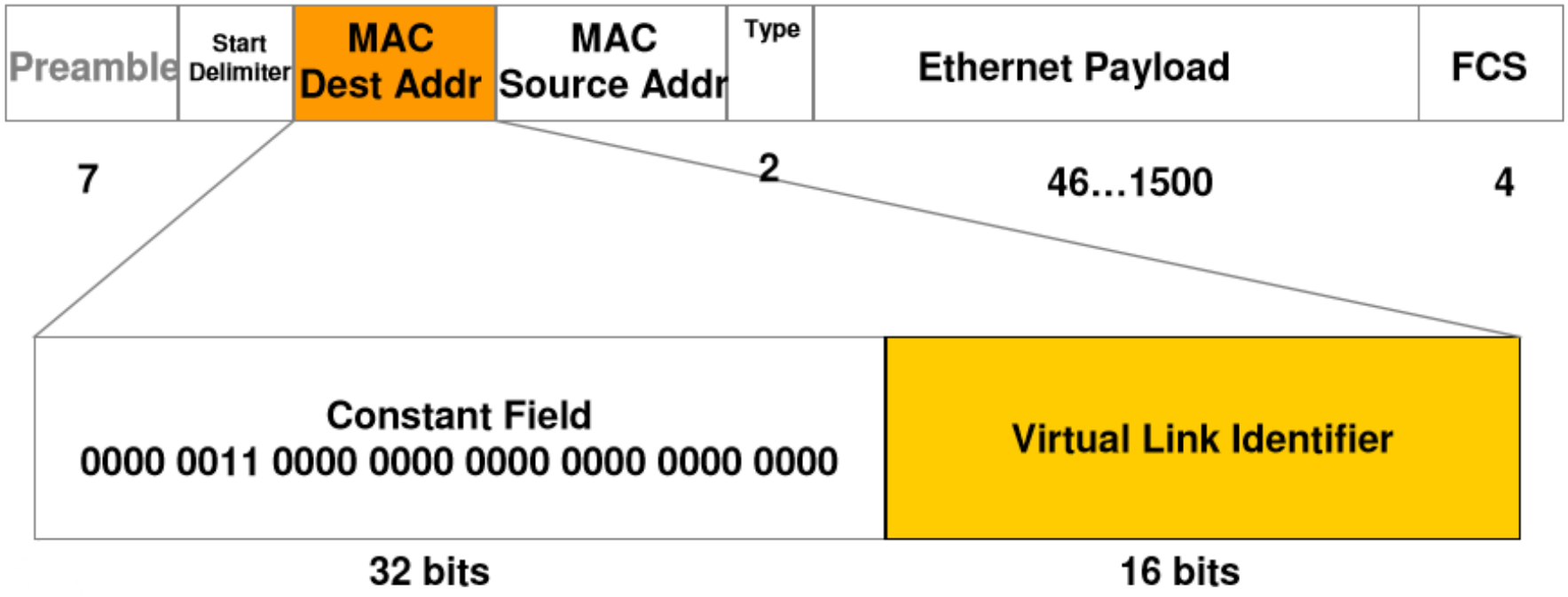
IP – Internet Protocol

- Datagram
  - Send it let it rattle around to its destination
  - If it takes too long throw it away
  - Address Format (V4)
    - 192.168.0.188 4 Octets (bytes)
- Sits on top of a Data Link Protocol
  - Ethernet
    - MAC Address Allocated by Card Manufacturer
      - http://aruljohn.com/mac.pl
  - But could be any of these
      - IEEE 802-2, Token Ring, FDDI, SMDS,SDLC, LAPB, etc.

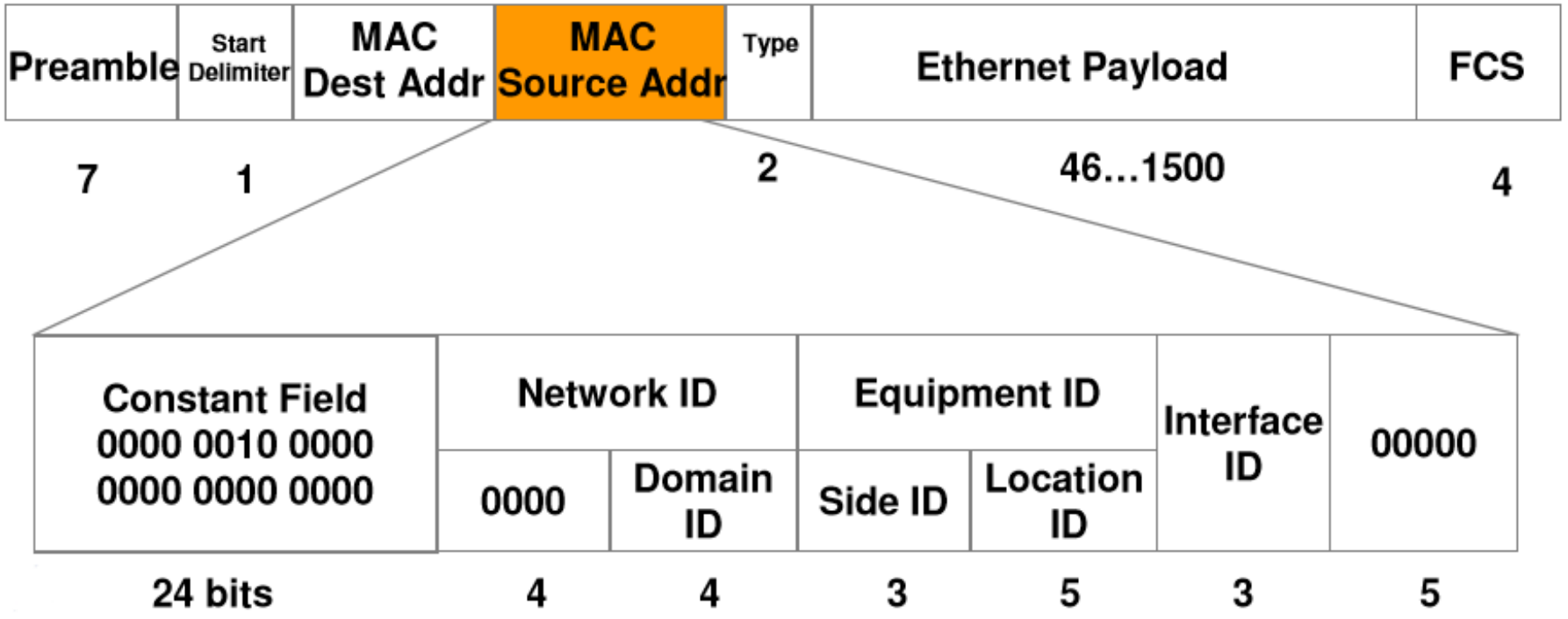
Hardware (MAC) Address



ARINC-664 MAC Destination Address



ARINC-664 MAC Source Address



IP V4 Packet Format

<table>
<tr><td>Version</td><td>Header Length</td><td>Differentiated Services</td><td>Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Fragment Info</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td>Header Checksum</td></tr>
<tr><td colspan="4">Source Address</td></tr>
<tr><td colspan="4">Destination Address</td></tr>
<tr><td colspan="4">Multiple 32 bit words of “Options”</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

IP Packet Header Details

- Version = 4 for IPv4
- Header length = number of 32-bit words in header
  - Min length = 5 words or 20 bytes
  - Max length = 15 words if all options present
- Header length can be used as an offset from the start of the header to the beginning of data
- Time to Live actually a hop count which is decremented by each gateway
- Identification – unique number for entire datagram – used to reassemble fragments

IP Packet Header Details (cont)

- Protocol
  - ICMP = 1
  - IGMP = 2
  - TCP = 6
  - UDP = 17
- Address
  - 32-bits with each octet (byte) representing one of four digits in address

IP Address Aspects

- The IP Address applies to a connection not a host
- "Networks" and Subnets
  - Conceptual Class A, B, C
  - Actual implementation is Subnets
    - Defined by Subnet Mask 255.255.255.0
    - Works with IP Address
- Network Address Translation (NAT)
  - Routable address for public IP
  - Non-routable address behind firewall
  - http://en.Wikipedia.org/wiki/Private_network

Private IP Address

- Private IP Address Ranges (non-routable)
  - 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 to 192.168.255.255
- Gateway provides Address Translation (and other fire wall services)
  - Typically home router or Gateway Computer at .1 or .254 address
  - ISP provides global (WAN) IP address
  - For outgoing traffic NAT maintains a cross reference table
  - Incoming traffic must have handling rules (Port forwarding)

Automatic Private IP Addressing

- Defined in RFC 3927
  - Dynamic Configuration of IPv4 Link-Local Addresses

    "This document describes how a host may automatically configure an interface with an IPv4 address within the 169.254/16 prefix that is valid for communication with other devices connected to the same physical (or logical) link."
  - In the absence of a DHCP service an address in the 169.254/16 range may be assigned.
  - Bonjour is Apple's implementation of RFC 3927
  - Linux uses Avahi which implements the Apple Zeroconf specification

Multicast IP Address

- Reserved range 224.0.0.0 to 239.255.255.255
- Well know addresses use 224.0 prefix
  - IGMP uses 224.0.0.22
  - PTP uses 224.0.0.107
  - NTP clients listen on 224.0.1.1
  - Zeroconf mDNS uses 224.0.0.251
- Ethernet multicast MAC addresses
  - FF:FF:FF:FF:FF:FF for broadcast
  - 01:80:C2:00:00:00, :03, :0E for Link Layer Discovery Protocol (LLDP)

Layer 4 - Transport

- TCP and UDP live here
- Also where encapsulation happens
  - GRE – Generic Routing Encapsulation for tunneling
- At this layer the data can be either connection oriented (TCP) or connectionless (UDP)
- A host operating system typically provides all services related to this layer
  - For a TCP connection the OS would handle all retransmit requests and return error status to the calling routine

TCP and UDP Port Numbers

- Destination Port # is the "application" or "service" host address
  - Applications/services register to listen for incoming data on the defined port
  - IANA port numbers: http://www.iana.org/assignments/port-numbers
  - 0 to 1023 Well Known ports managed by IANA
  - 1024 to 49151 Registered by IANA as a convenience
  - 49152 to 65535 Dynamic (used for source address)
  - C:\WINDOWS\system32\drivers\etc\services
  - Source Port number used with IP addresses and destination port number to create a unique identifier for the connection
  - Source port number incremented at each use in dynamic case

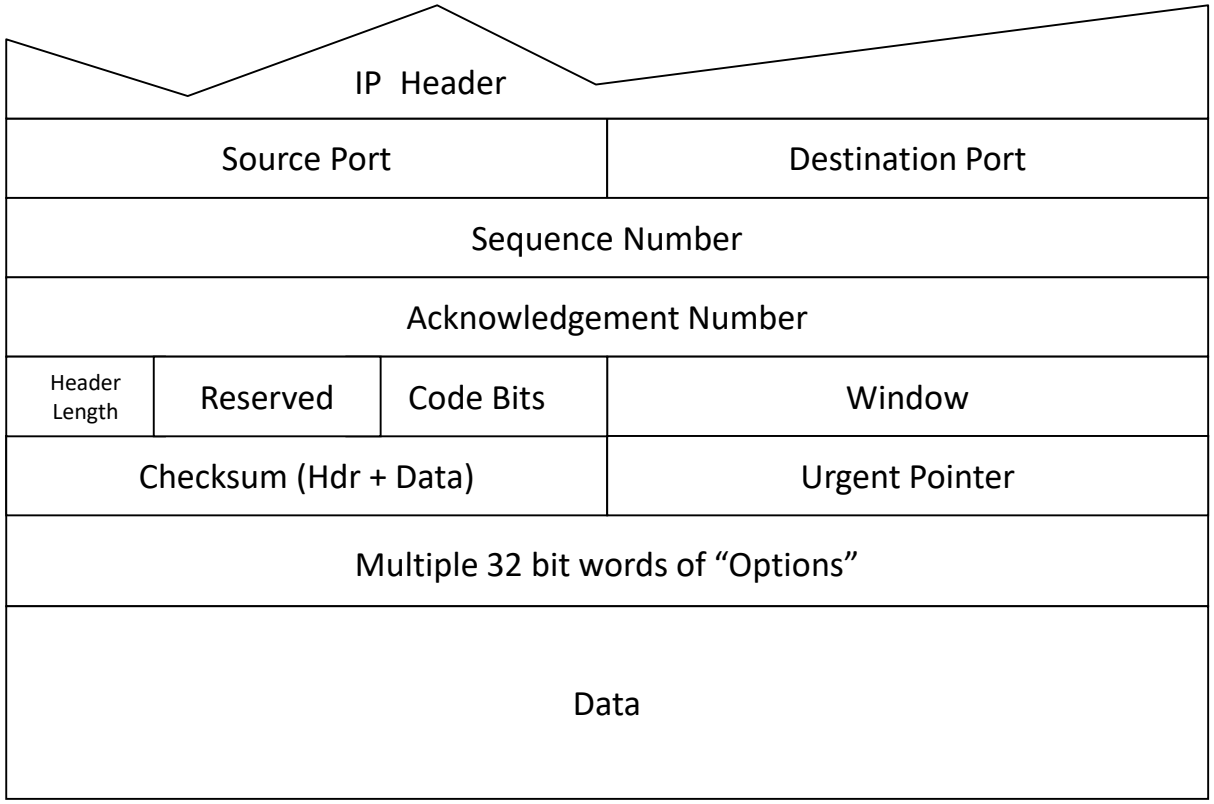
TCP

- Transmission Control Protocol
- Described in RFC 793
- Highly reliable
- Connection oriented
- Error detection through checksum
- ACK / NAK

TCP Distinctions

- Ordered data transfer – sequence number used to reassemble packets
- Retransmission of lost packets – not acknowledged packets resent
- Error-free data transfer – checksum used to ensure reliable transfer
- Flow control – limits transfer rate to ensure reliable delivery
- Congestion control
- PDU = Protocol Data Unit which for layer 4 is either a segment for TCP or datagram for UDP

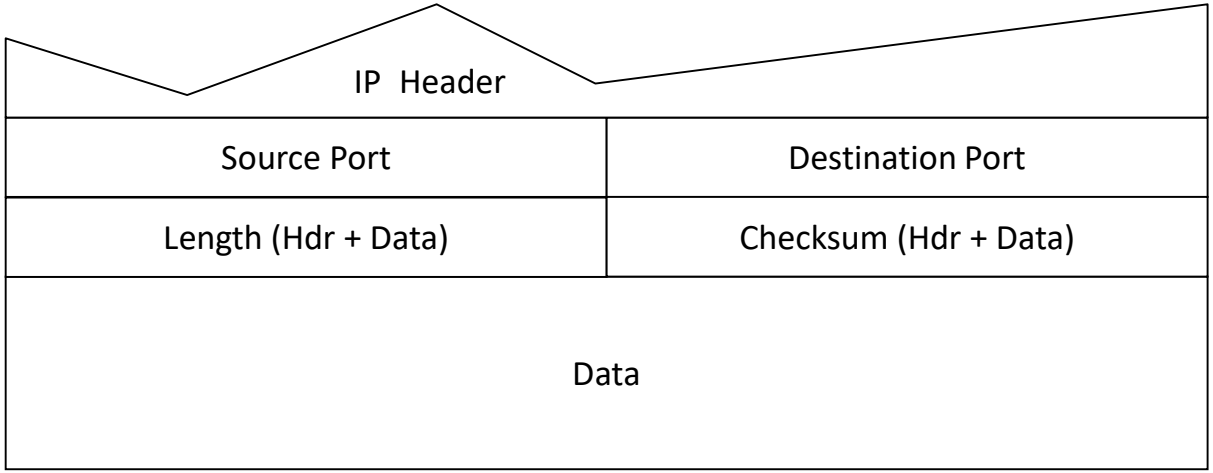
TCP PDU Format



UDP

- User Datagram Protocol
- Described in RFC 768
- Minimal overhead
- Transaction oriented
- Delivery and duplicate protection not guaranteed

UPD PDU Format



Routing

- Routing is the act of moving information across an internetwork from source to destination. Along the way, at least one intermediate node typically is encountered. Routing occurs at Layer 3 (the network layer) of the OSI reference model.
- Routing algorithms
  - OSPF is the most common interior gateway protocol (IGP)
  - OSPF V2 defined in RFC 2328 for IPv4
  - OSPF V3 defined in RFC 5340 updated for IPv6
- Routing Information Protocol (RIP)
  - RFCs 1058, 1388, 1723

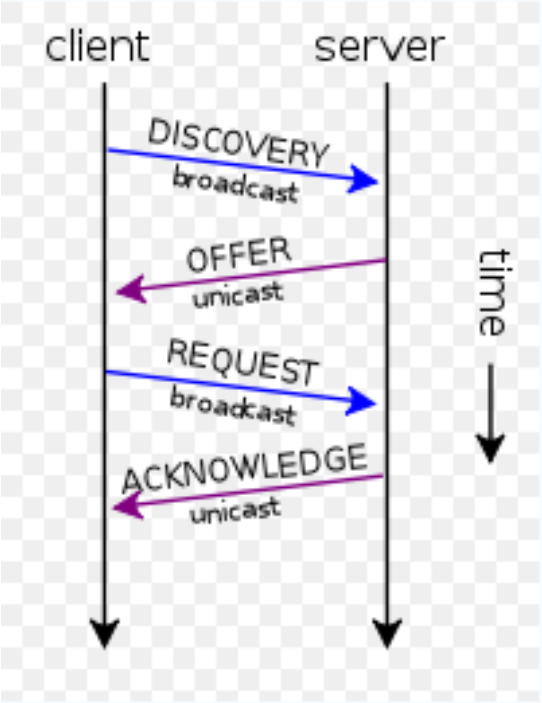
Domain Name System (DNS)

- Essentially a global phone book for the Internet
- Translates friendly names into IP addresses
- Original RFCs published in 1983 (882, 883)
- RFCs 1034, 1035 published in 1987 superseded previous versions
- Naming rules in RFCs 1035, 1123 and 2181
- Queries use UDP over port 53 using format specified in RFC 1035

DHCP

- Dynamic Host Control Protocol
- Described in RFC 1531 and RFC 2131
- IPv6 extensions in RFC 3315
- DHCP uses the same two IANA assigned ports as BOOTP: 67/udp for the server side, and 68/udp for the client side.
- Four basic phases: IP discovery, IP lease offer, IP request, and IP lease acknowledgement.

DHCP Sequence



The Basics

- Addressing
  - Physical (MAC)
  - Numerical (IPV4 192.168.1.1)
- Services
  - DHCP (give me an address)
  - DNS (find an address)
- Protocols
  - TCP (connection oriented, guaranteed delivery)
  - UDP (think streams)

MAC Addresses

- Six bytes of information
  - 00-1D-92-98-36-8A
- Globally Unique
  - Conflicts not allowed
- First three bytes = OUI = Vendor ID
  - Organizationally Unique Identifier – assigned by IEEE
  - 00:1D:92 = Micro-star International
  - http://aruljohn.com/mac/001D92

UDP Traffic

- DNS
- SNMP – Simple Network Management Protocol
- Video / Audio streaming

Common Problems

- Router
  - Ping outside IP address
- Broken DNS
- Firewall issues
- Addressing problems
  - Netmask – defaults on new gear

Expert Information

- Identifies potential problems
- Warnings Tab
  - Connection reset
  - Duplicate IP address
- Click on entry and jump to packet display

Bad Behavior

- Statistics -> Resolved Addresses
- Statistics -> Protocol Hierarchy
- Statistics -> Conversations
- Statistics -> Endpoints
- Statistics -> DNS
- Statistics -> Flow Graph

Wireshark IO Graphs

- Click in graph jumps to packet in main display
- Use Filter to show specifics
  - tcp shows just TCP traffic
- Click on Graph 1 button to show / hide
- Y-axis units
  - Packets / tick as default
  - Bytes, bits / tick available

Wireshark Config

- Turn extra panes off
  - View / highlight and press space bar
- Turn colors off
- Set appropriate time
  - Delta time
  - Time of day

Links

- http://wireshark.org
- http://wiki.wireshark.org
- http://www.riverbed.com/products/performance-management-control/network-performance-management/wireless-packet-capture.html
- https://www.youtube.com/channel/UCHBY7sUVdWK4bOSe7khG0UA
- https://www.youtube.com/
  - Tony Fortunato – LMTV
  - Chris Greer
  - The Technology Firm

QUESTIONS?