CompTIA Network +

Chapter 2 Dissecting the OSI Model

Updated 8-20-16

C TemplatesWise.com

Objectives

- What is the purpose of a Network model?
- What are the layers of the OSI model?
- What are the characteristics of each layer of the OSI model?
- How does the TCP/IP stack compare to the OSI model?
- What are the well-known TCP and/or UDP port numbers for a given collection of common applications

The Purpose of Reference Models

- It breaks network communication into smaller, simpler parts that are easier to develop.
- It facilitates standardization of network components to allow multiple-vendor development and support.
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting the other layers so that they can develop more quickly.
- It breaks network communication into smaller parts to make learning it easier to understand.

Warriors of the Net



• Link "Net 4"

The OSI seven-layer model

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Mnemonics for the OSI Model

Away Pizza Sausage Throw Not Do Please All People Seem To Need Data Processing

Protocol Data Unit (PDU)

7	Application	
6	Presentation	
5	Session	
4	Transport	Segments
3	Network	Packets
2	Data Link	Frames
1	Physical	Bits

Figure 2-3 PDU Names

Quick Summary of Layers 1-4

4	Transport
3	Network
2	Data Link
1	Physical

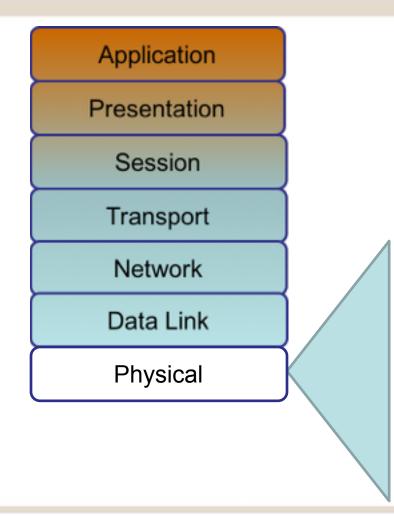
TCP & UDP Ports	Service
Routers, IP Address	WAN
Switches, MAC Address	LAN
Cables	

OSI Layers in Wireshark

- 1 2 3 4 7
- ▷ Frame 1216: 467 bytes on wire (3736 bits)
- Ethernet II, Src: Apple_4f:2b:55 (28:cf:e9:4f:2b:55)
- Internet Protocol Version 4, Src: 192.168.1.141
- Transmission Control Protocol, Src Port: 58163
- Hypertext Transfer Protocol

Physical Layer



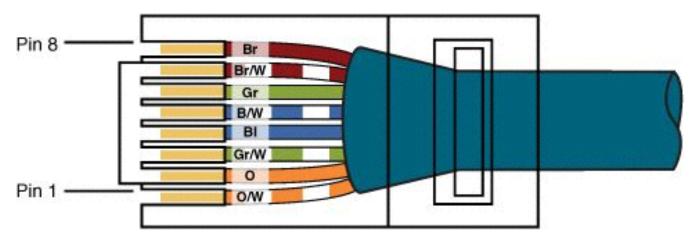


- How Bits are represented on the medium
- Wring standards for connectors and jacks
- Physical topology
- Synchronizing bits
- Bandwidth usage
- Multiplexing strategy

Figure 2-4 Layer 1: Physical Layer

Wiring Standards

Figure 2-7 TIA/EIA-568-B Wiring Standard for an RJ-45 Connector



Asynchronous and Synchronous Communications

- Synchronizing Bits
 - Two devices must agree on when one bit stops and another bit starts

Asynchronous

- Uses start and stop bits

Synchronous

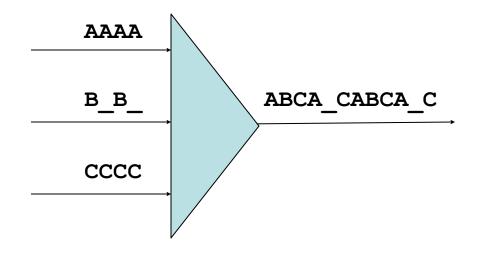
 Internal clocks are synchronized at each end of the cable

Bandwidth Usage

- Broadband
 - Multiple channels share the same medium
 - Ex: cable TV uses frequency division multiplexing (each channel uses a different frequency range)
- Baseband
 - The whole medium is used for one transmission
 - Example: Ethernet

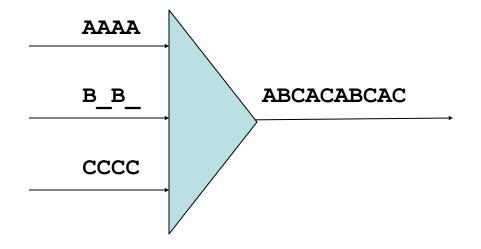
Time-Division Multiplexing (TDM)

• Each channel gets the same amount of time on the wire



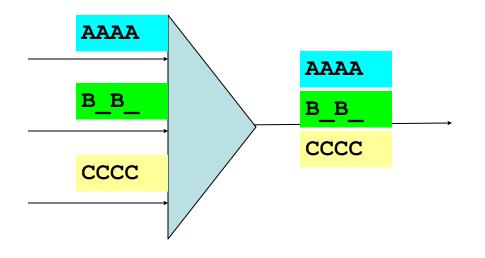
Statistical Time-Division Multiplexing (StatTDM)

• Busy channels get more time on the wire



Frequency Division Multiplexing (FDM)

• Example: signals sent with different colors through the same fiber optic cable



Layer 1 Devices

- Cables
- Wireless access points
- Hubs
 - Because they don't pay any attention to addresses, they just deliver signals to every connected device like a crossover cable

Data Link Layer



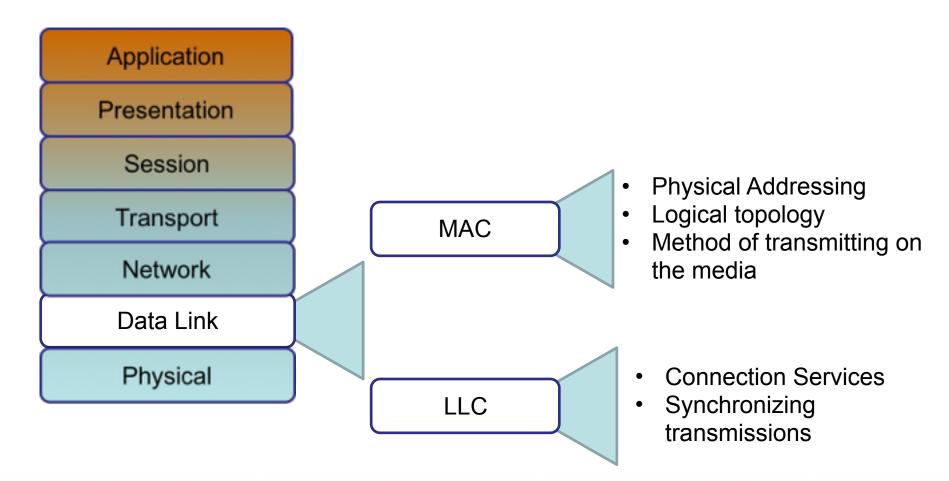


Figure 2-8 Layer 2: The Data Link Layer

MAC Addresses

- IPCONFIG /ALL
- Physical Address
- Built into the network interface

Ethernet adapter Local Area Connection:

Connection-specific DNS	Su	ff	i×		:	localdomain Intel(R) PR0/1000 MT Network Connection 00-0C-29-52-34-92
Description					:	Intel(R) PRO/1000 MT Network Connection
Physical Address					:	00-0C-29-52-34-92
DHCP Enabled. Autoconfiguration Enable						Yes
Autoconfiguration Enable	ed.				:	Yes
IPv6 Address					:	2::4(Preferred)
Link-local IPv6 Address					:	2::4(Preferred) fe80::5a7:33af:ed86:b39f%11(Preferred)
IPv4 Address					:	192.168.119.154(Preferred)
Subnet Mask					-	255.255.255.0
Lease Obtained					:	Tuesday, August 20, 2013 12:37:23 PM Tuesday, August 20, 2013 1:07:23 PM
Lease Expires					:	Tuesday, August 20, 2013 1:07:23 PM
Default Gateway						192.168.119.2
DHCP Server					:	192.168.119.254
DHCPV6 IAID					:	234884137
DHCPv6 Client DUID						234884137 00-01-00-01-15-0E-CB-08-00-0C-29-BB-32-CA
	•	•				00 01 00 01 10 02 00 00 00 00 27 DD 02 0A
DNS Servers						192, 168, 119, 2
Primary WINS Server						192 168 119 2
NetBIOS over Topip	•	•	•	•		Epabled
Herbitoo over Topip			•			LIIBIEO

Connection Services

- Flow control
 - Prevents sender from sending data faster than the client can accept it
- Error control
 - When a frame is received, a checksum is used to detect errors
 - Usually a Cyclic Redundancy Check (CRC)
 - If the receiver's checksum does not match the sender's checksum, the frame is discarded and resent

Layer 2 Devices

- Switches
- Bridges
- Network Interface Cards (NICs)

Network Layer



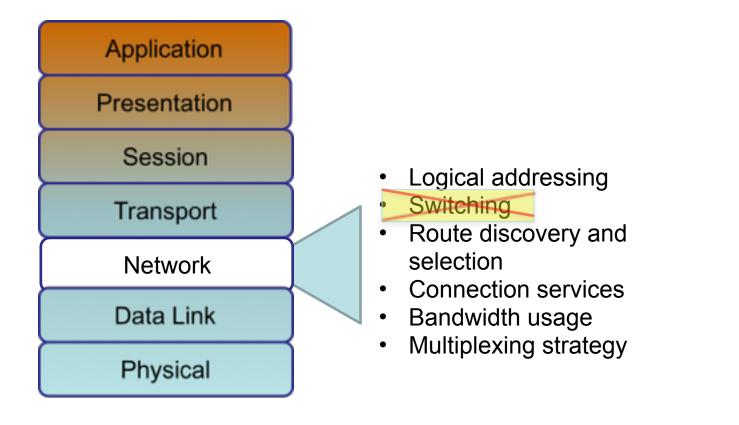


Figure 2-9 Layer 3: The Network Layer

IP Address

- Logical address
- · Changes when the device is moved

Ethernet adapter Local Area Connection:

Autoconfiguration Enabled IPv6 Address Link-local IPv6 Address IPv4 Address Subnet Mask Lease Obtained Lease Expires Default Gateway DHCP Server		Intel(R) PR0/1000 MT Network Connection 00-0C-29-52-34-92 (es 2::4(Preferred) 680::5a7:33af:ed86:b39f%11(Preferred) 192.168.119.154(Preferred) 255.255.255.0 [uesday, August 20, 2013 12:37:23 PM [uesday, August 20, 2013 1:07:23 PM [uesday, August 20, 2013 1:07:23 PM
DHCPv6 Client DUID	: 0	10-01-00-01-15-0E-CB-08-00-0C-29-BB-32-CA
DNS Servers	: 1	.92.168.119.2

Switching

- Packet switching
 - Data is broken into packets
 - Many packets travel along network connections like cars on a freeway
- Circuit switching
 - A physical line is dedicated to each connection
 - Ex: old copper landline phone systems
- Message switching
 - Store-and-forward, like email

Layer 3 Devices

- Routers
- Multilayer Switches

Transport Layer



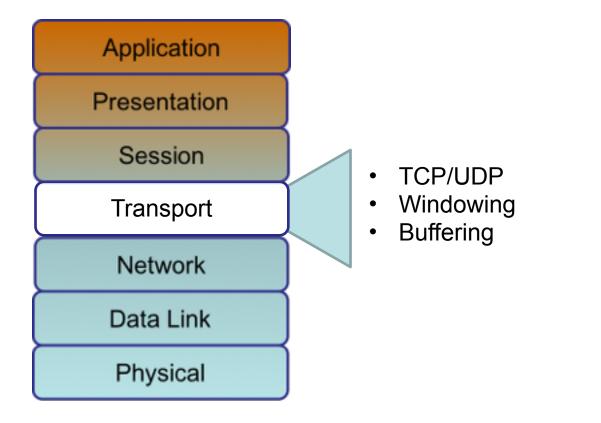


Figure 2-10 Layer 4: The Transport Layer

TCP and UDP

- Transmission Control Protocol (TCP)
 - Connection-oriented and reliable
 - Handshake makes sure both ends are ready
 - Segments are acknowledged and resent if necessary
- User Datagram Protocol (UDP)
 - Connectionless and unreliable
 - No handshake
 - Best-effort delivery, no acknowledgements

TCP Sliding Window

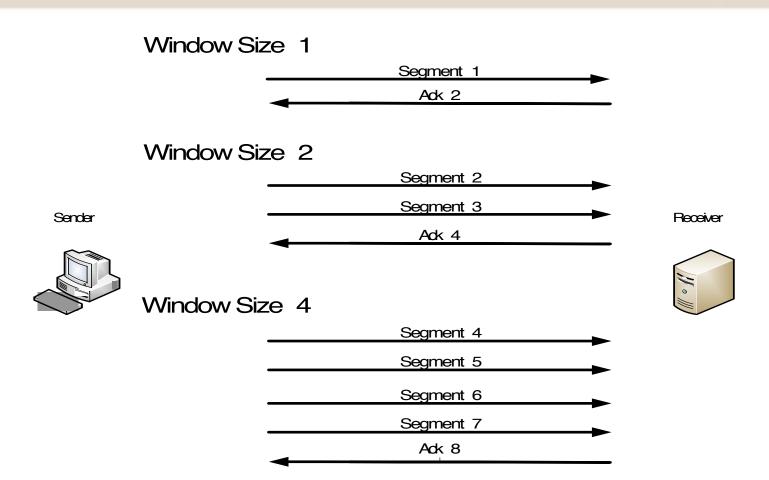


Figure 2-11 TCP Sliding Window

Demo: Downloading a Large File

1	88 1	2601:645:c000:8df0:c8	2001:67c:1560:80	HTTP	931	GET /ubuntu/dists/precise-updates/main/installer-amd64/current/image
13	39 1	192.168.1.107	224.0.0.251	MDNS	103	Standard query 0x0000 PTR _36061251subgooglecasttcp.local, "QM
14	0 1_	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	86	80 → 59236 [ACK] Seq=1 Ack=846 Win=30336 Len=0 TSval=977628964 TSecr
14	1 1_	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514	[TCP segment of a reassembled PDU]
1/	2 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514	[TCP segment of a reassembled PDU]
14	3 1	2601:645:c000:8df0:c8	2001:67c:1560:80	TCP	86	59236 → 80 [ACK] Seq=846 Ack=2857 Win=129632 Len=0 TSval=833604337 T.
14	4 1_	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514	[TCP segment of a reassembled PDU]
1/	15 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514	[TCP segment of a reassembled PDU]
1/	16 1	2601:645:c000:8df0:c8	2001:67c:1560:80	TCP	86	59236 → 80 [ACK] Seq=846 Ack=5713 Win=126784 Len=0 TSval=833604338 T
14	7 1_	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514	[TCP segment of a reassembled PDU]
1/	18 1_	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514	[TCP segment of a reassembled PDU]
1/	9 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514	[TCP segment of a reassembled PDU]
1	ið 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514	[TCP segment of a reassembled PDU]
1	51 1_	2601:645:c000:8df0:c8	2001:67c:1560:80	TCP	86	59236 → 80 [ACK] Seq=846 Ack=8569 Win=123904 Len=0 TSval=833604338 T
1	52 1_	2601:645:c000:8df0:c8	2001:67c:1560:80	TCP	86	59236 → 80 [ACK] Seq=846 Ack=11425 Win=121056 Len=0 TSval=833604338
15	i3 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514	[TCP segment of a reassembled PDU]
1	i4 1	2601:645:c000:8df0:c8	2001:67c:1560:80	TCP	86	[TCP Window Update] 59236 → 80 [ACK] Seq=846 Ack=11425 Win=131072 Le.
1	55 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514	[TCP segment of a reassembled PDU]
15	6 1	2601:645:c000:8df0:c8.	2001:67c:1560:80	TCP	86	59236 → 80 [ACK] Seq=846 Ack=14281 Win=129632 Len=0 TSval=833604339
15	i7 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514	[TCP segment of a reassembled PDU]

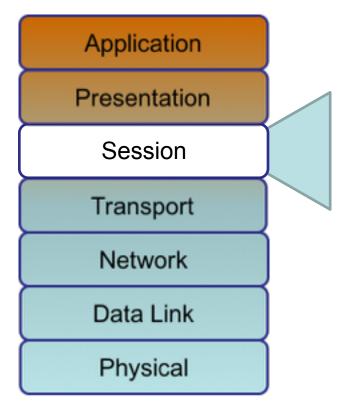
598 1	2601:645:c000:8df0:c8	2001:67c:1560:80	TCP	86 [TCP Window Update] 59236 → 80 [ACK] Seq=846 Ack=359857 Win=253856 L
599 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514 [TCP segment of a reassembled PDU]
600 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514 [TCP segment of a reassembled PDU]
601 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514 [TCP segment of a reassembled PDU]
602 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514 [TCP segment of a reassembled PDU]
603 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514 [TCP segment of a reassembled PDU]
604 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514 [TCP segment of a reassembled PDU]
605 1	2001:67c:1560:8001::11	2601:645:c000:8d	TCP	1514 [TCP segment of a reassembled PDU]
606 1	2601:645:c000:8df0:c8	2001:67c:1560:80	TCP	86 59236 → 80 [ACK] Seq=846 Ack=362713 Win=252448 Len=0 TSval=833605131

ICMP (Internet Control Message Protocol)

- At layer 4
- Used by ping and traceroute, and to indicate errors such as dropped packets

Session Layer





- Setting up a session
- Maintaining a session
- Tearing down a session

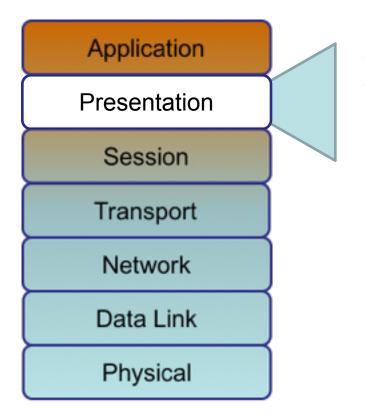
Figure 2-12 Layer 5: The Session Layer

Example of a Session

- User logs in with a username & password
- All data now has a special significance until that user logs off, or the session times out, or is terminated some other way
- Layer 6 Protocol

 H.323 (voice or video)
 NetBIOS (file sharing)

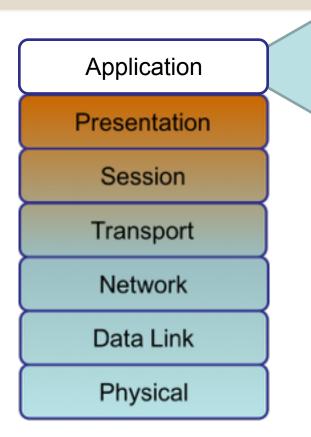
Presentation Layer



- Data formatting
- Encryption

Figure 2-13 Layer 6: The Presentation Layer

Application Layer

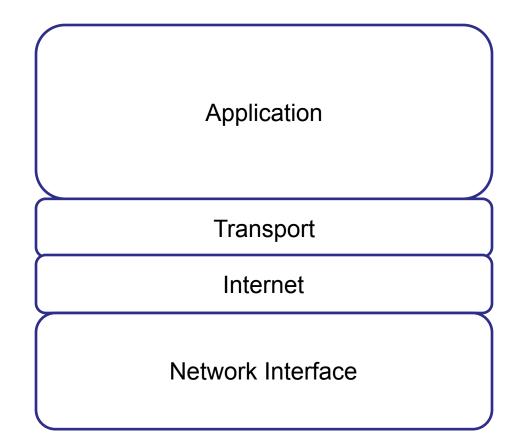


- Application services
- Service advertisement

Application Layer

- Closest to the user
- Hands data to an application in the format it expects, with no addresses or other transmission artifacts
- Examples: a downloaded file, an email message

The TCP/IP Stack



The TCP/IP and OSI Models Compared

OSI Stack

TCP/IP Stack

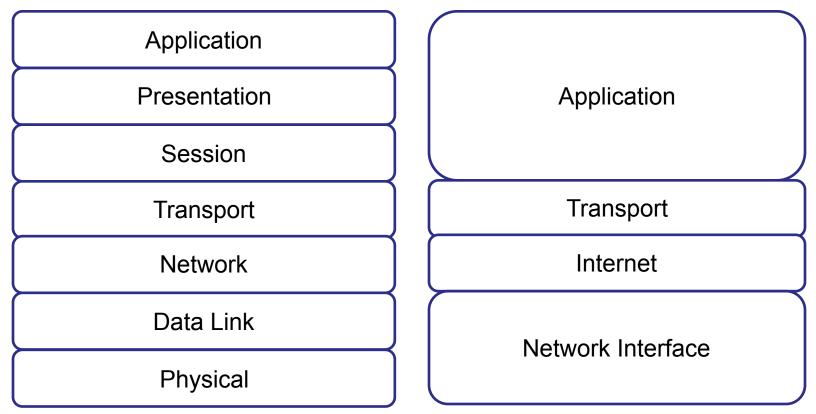


Figure 2-15 TCP/IP Stack

IP Ver4 Header



Version	Header Length	Type of Service	Total Length				
Identification			IP Flags	Fragment Offset			
TTL		Protocol	Header Checksum				
Source Address							
Destination Address							
IP Option (Variable Length)							

TTL (Time-to-Live)

- TTL decreases by one each time the packet is forwarded by a router
- If TTL reaches zero, the packet is discarded
- This eliminates packets trapped in routing loops

Demo: Routing Loop

```
X
Administrator: cmd - Shortcut (2)
                                                                                                        ۰
C:\>ping 2001:05c0:1000:000b:0000:0000:0000:10ef
                                                                                                        Ē
Pinging 2001:5c0:1000:b::10ef with 32 bytes of data:
Reply from 2001:5c0:1000:b::10ef: TTL expired in transit.
Ping statistics for 2001:5c0:1000:b::10ef:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
C:\>tracert 2001:05c0:1000:000b:0000:0000:0000:10ef
Tracing route to 2001:5c0:1000:b::10ef over a maximum of 30 hops
                                 2001:5c0:1000:b::10ec
  1
       99 ms
                97 ms
                         96 ms
 23456
                                 ix-5-0-1.6bb1.MTT-Montreal.ipv6.as6453.net [2001:5a0:300::5]
       96 ms
                98
                   ms
                        104 ns
                97 ms
       97 ms
                         96 ms
                                 2001:5c0:1000:b::10ec
                97 ms
      102 ms
                         96 ms
                                 ix-5-0-1.6bb1.MTT-Montreal.ipv6.as6453.net [2001:5a0:300::5]
                97 ms
                        108 ms
      101 ms
                                 2001:5c0:1000:b::10ec
                                 ix-5-0-1.6bb1.MTT-Montreal.ipv6.as6453.net [2001:5a0:300::5]
      100 ms
               101 ms
                        101 ns
^C
C:∖>
```

TCP Header

0	4	10	16	24	31				
	SOURCE PO	RT	DESTINATION PORT						
SEQUENCE NUMBER									
ACKNOWLEDGEMENT NUMBER									
HLEN	RESERVED	CODE BITS	WINDOW						
	CHECKSU	м	URGENT POINTER						
	OPTI	PAD	DING						
DATA									

Figure 2-17 TCP Segment Format

TCP Header Fields

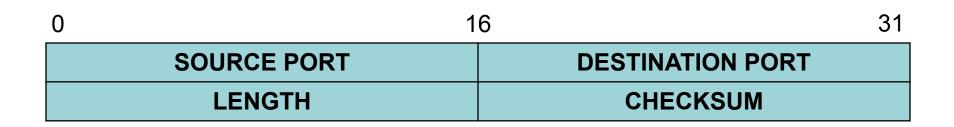
- Port numbers
 - Indicate which program on the end device should receive the data
 - Examples: Port 25 for email, 80 for HTTP
- Window size
 - Number of bytes that can be sent before waiting for an ACK

TCP Header Fields

- Sequence and Acknowledgement numbers

 Used to put packets in order to reassemble
 files and other large messages
- Flags like SYN and ACK are used for the TCP handshake and to acknowledge data received

UDP Header



 No handshake, acknowledgements, sequencing, or flow control

Common Ports

Link "Net 5" for flash cards

DNS (Domain Name System) TOP/UDP 53 HTTP (Hypertext Transfer Protocol) TCP 80 SMTP (Simple Mail Transfer Protocol) TCP 25 POP (Post Office Protocol) TCP 110 TOP 23Telnet DHCP (Dynamic Host Configuration Protocol) UDP 67(IPv4 client) and 68(IPv4 server); FTP (File Transfer Protocol) TOP 20(data) and 21(control) TFTP (Trivial File Transfer Protocol) UDP 69 NBNS(NetBIOSName Service) **UDP/TOP 137** IMAP4 (Internet Message Access Protocol) TOP 143 SNMP (Smple Network Management Protocol) TCP/UDP 161 HTTPS (Hypertext Transfer Protocol Secure) TCP 443 **UDP 123** NTP (Network Time Protocol) SSL (Secure Sockets Layer) TCP 443 TCP 22 SSH (Secure Shell)

Port Types



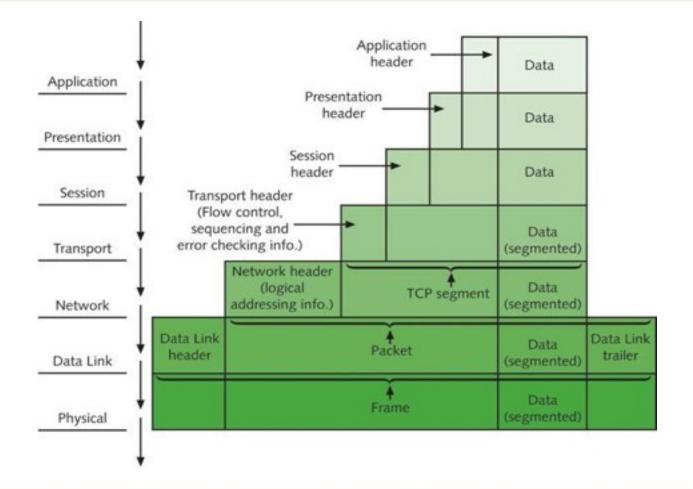
Port numbers are assigned in various ways, based on three ranges:

 System Ports (0-1023), System Ports are assigned by IETF process for standards-track protocols, as per RFC6335. Also known as <u>well-known-</u> <u>ports</u>

 User Ports (1024-49151), User Ports are assigned by IANA using the "Expert Review" process, as per RFC6335

 Dynamic and/or Private Ports (49152-65535), Dynamic Ports are not assigned, they are dynamically created as your computer need them. Also known as <u>ephemeral ports</u>.

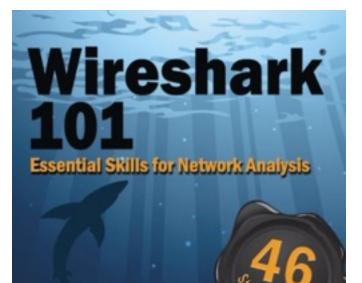
Communication Between Two Systems



Next Steps



- Excellent book
- Many hands-on projects
- Downloadable PCAP files
- Also a certification "WCNA"
- Links: "Net 1" & "Net 2"



Laura Chappell Foreword by Gerald Combs Creator of Wireshark

Master key Wireshark skills to quickly characterize network traffic rates, protocols, applications and hosts

A Wireshark Solutions Series Book

Next Steps



Excellent videos

Link: "Net 3"

Network Analysis O

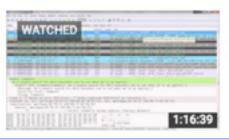
 Define Notacch Analysis
 Traubleshooting Tasks for the Notaco Security Tasks for the Notaco Security Tasks for the Network Analys Optimization Tasks for the Network A Application Analysis Tasks for the Net De Aware IT Legal Insuce O Lickening Optimization Tasks for the Net Tasks and Tasks and Clubering Optimization of Control (Control) Determined Network Tasks
 School (Control)



WCT02 Class: Introduction to Wireshark

Laura Chappell

WCT01-S0: Course Introduction [WCT1: Network Analysis Overview] 3:52 WCT01-S1: Define Network Analysis [WCT01 Network Analysis Overview Course] 4:08 View full playlist (13 videos)



Sharkfest 2013 - Wireshark Network Forensics (Laura Chappell)

Chris Greer

3 years ago + 65,575 views

This session was recorded at Sharkfest 2013, UC Berkeley, CA Join Laura Chappell in this session as she examines a slew of ...