TCP and UDP Theory of Operation

Aaron Staines
NETWORK/SYSTEM ENGINEER | CCISO

Module Overview

TCP

- Datagram decomposition aka DNA
- How sessions are formed
- Data segmentation and reassembly
- Retransmitting lost data

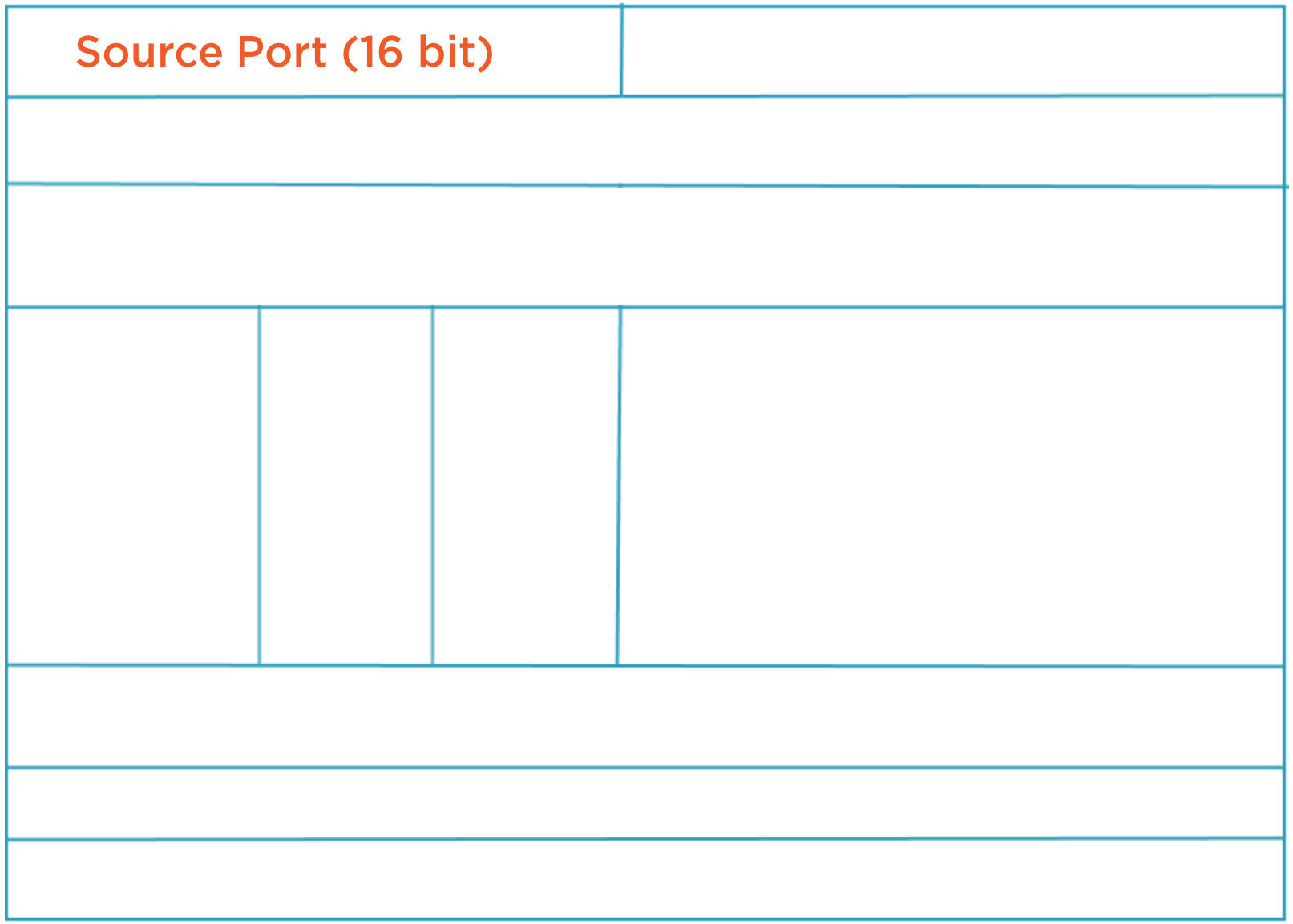
Module Overview

UDP

- Datagram decomposition
- Wireshark view of datagram
- UDP data transmission

TCP Breakdown

TCP Breakdown

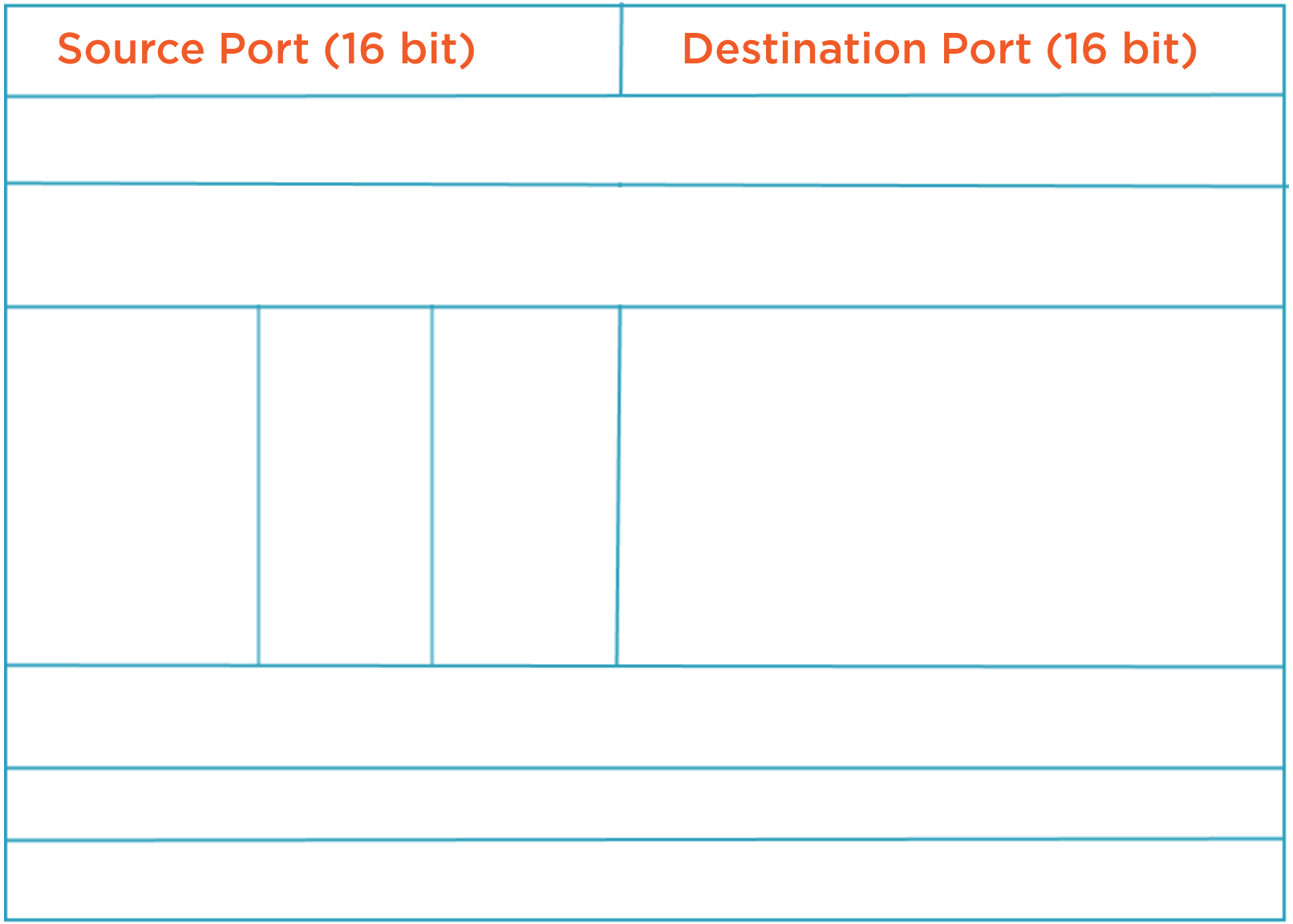


TCP Breakdown

Source port

- Connection tracking
- 16 bit

TCP Breakdown

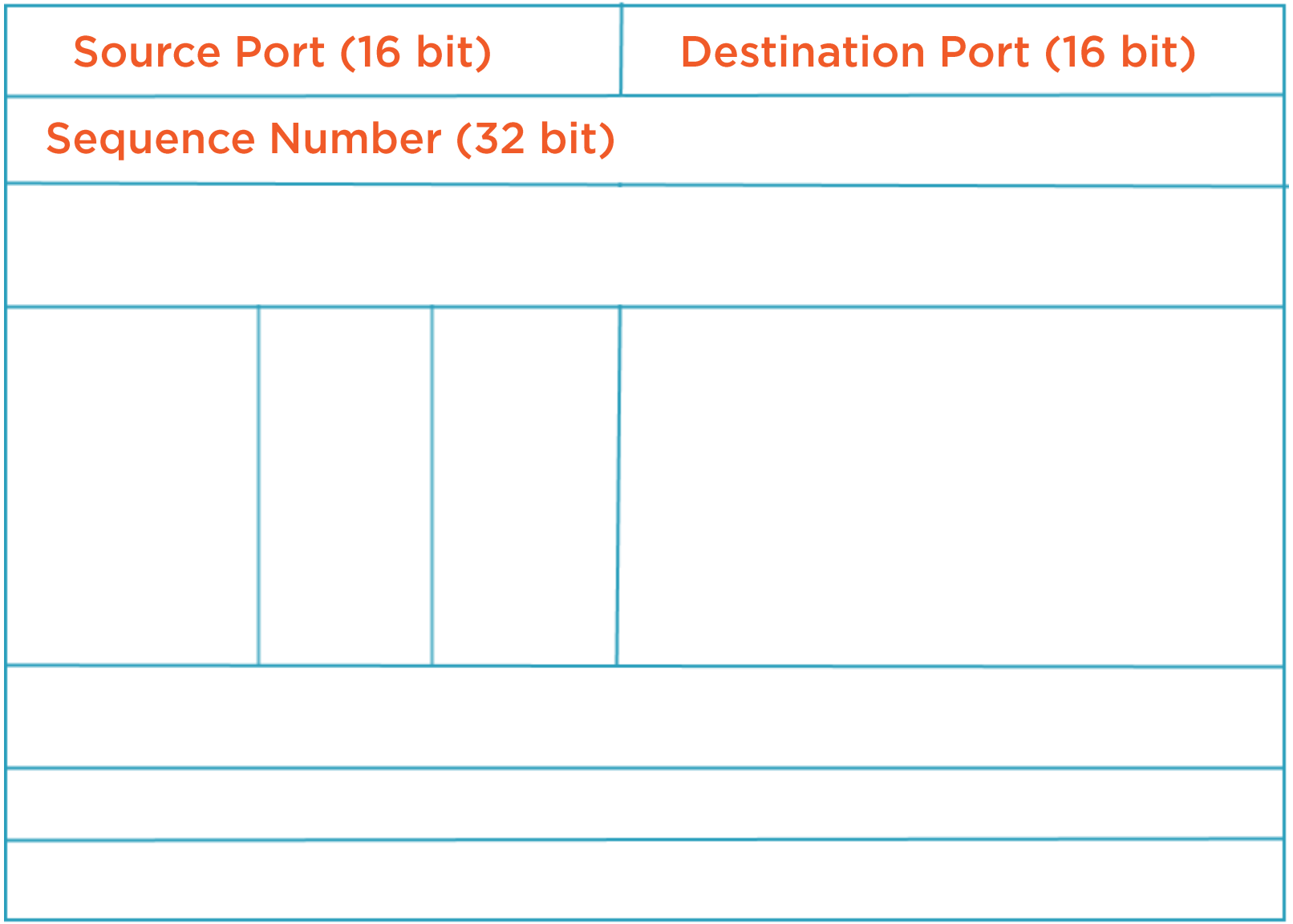


TCP Breakdown

Destination port

- Destination service
- Most common web server
  - Port 80 and 443
- 16 bit

TCP Breakdown

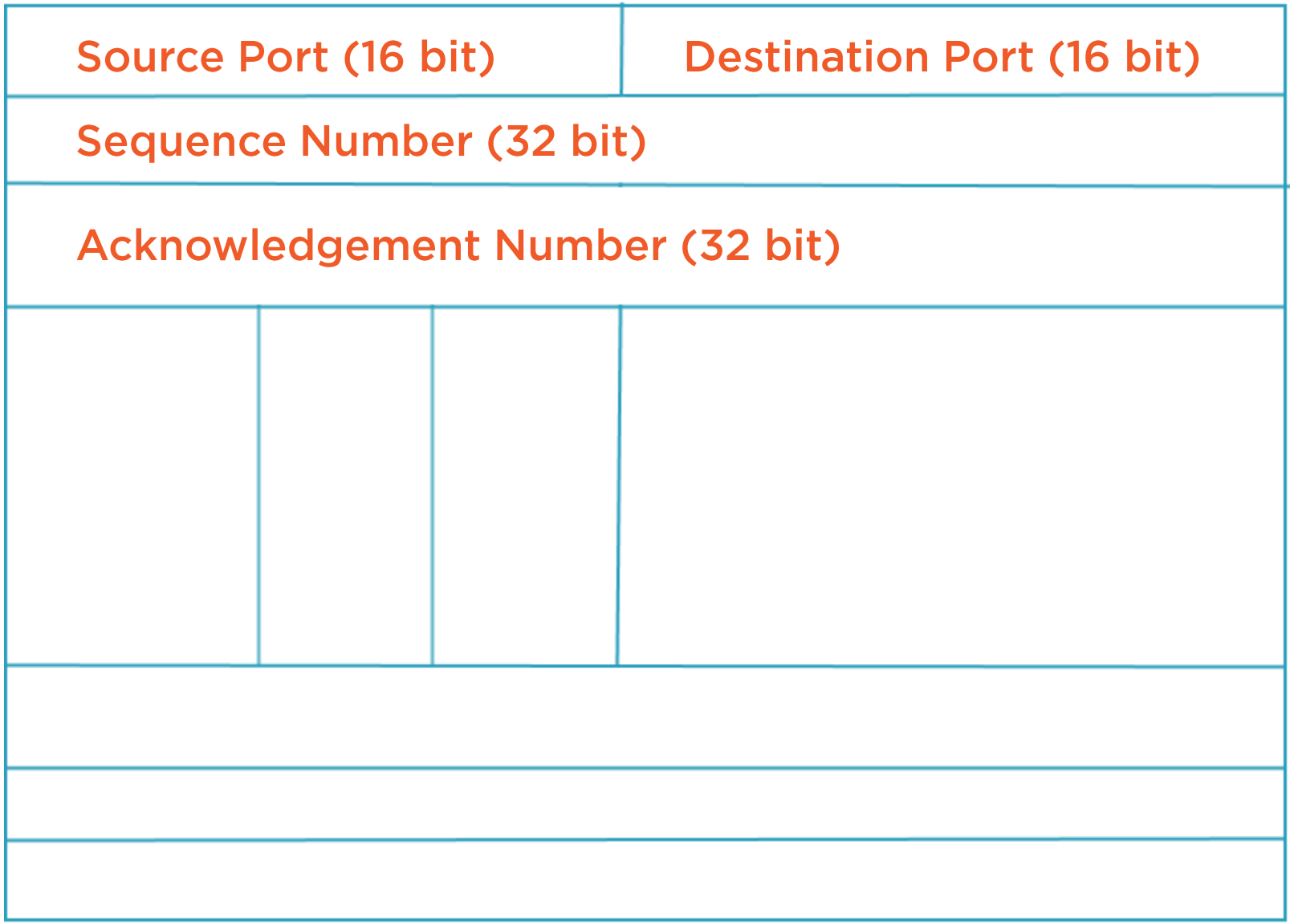


TCP Breakdown

Sequence number

- Separates TCP from UDP
- Each piece gets a number
- 32 bit

TCP Breakdown

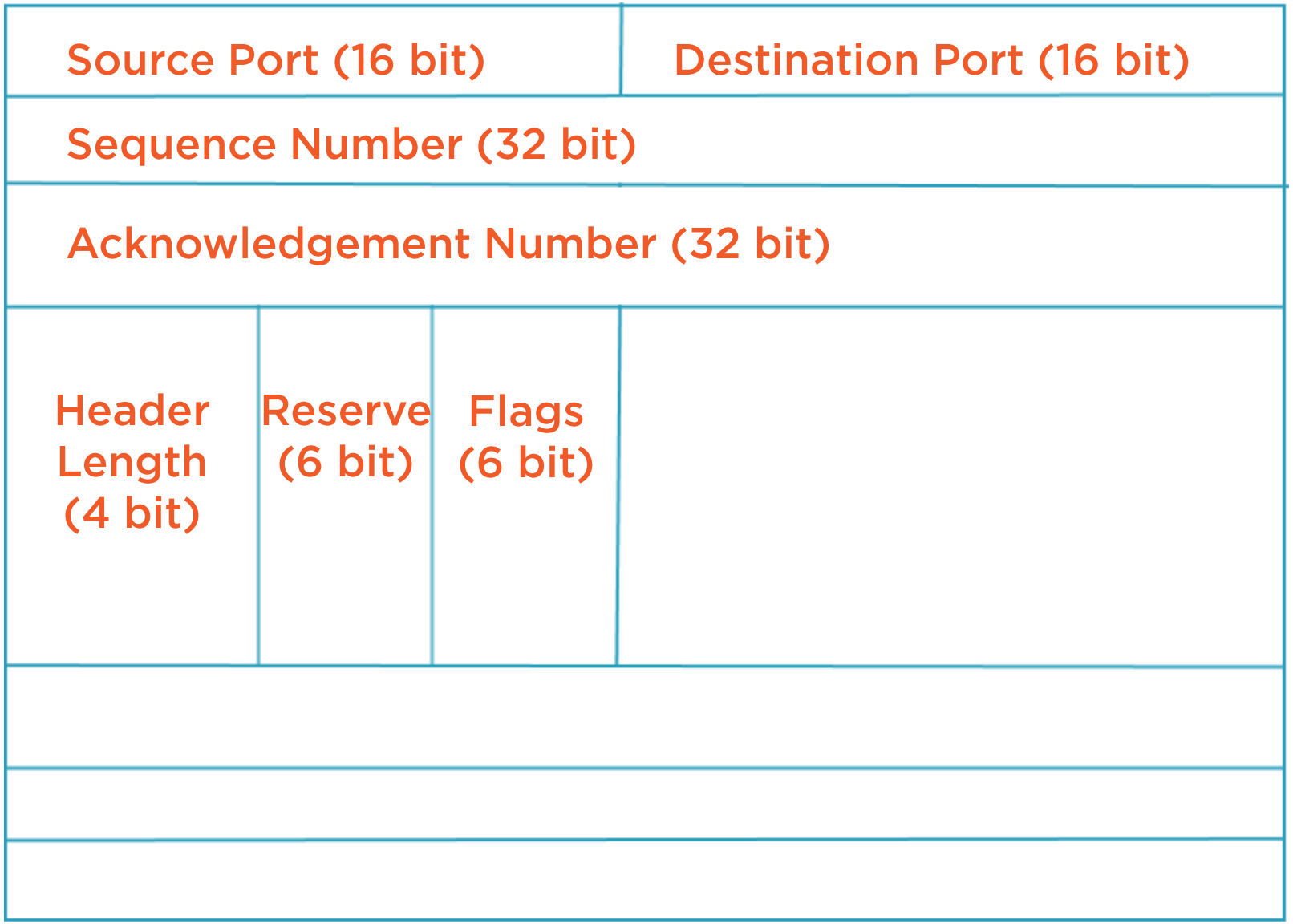


TCP Breakdown

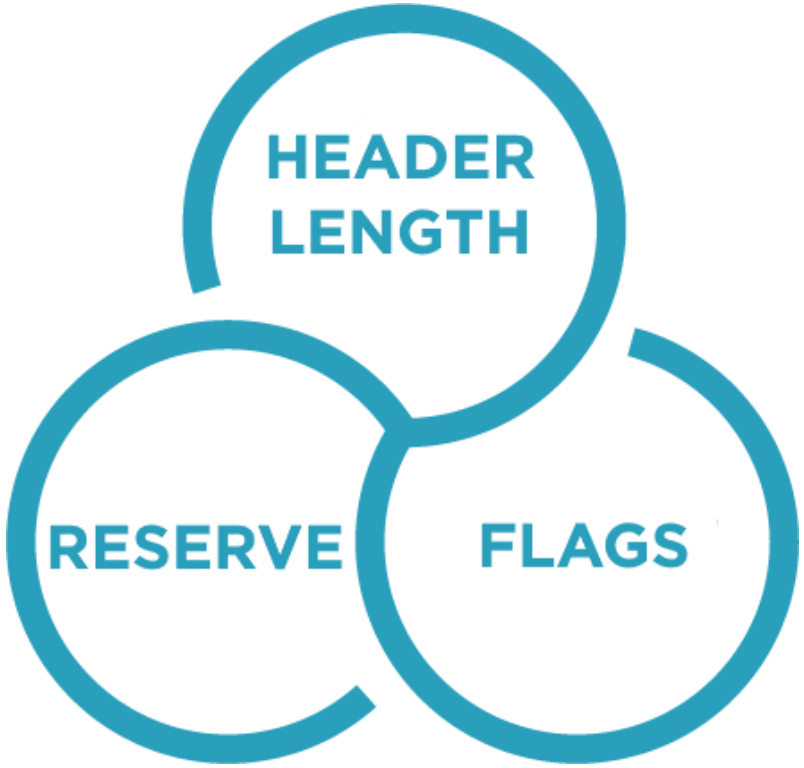
Acknowledgement number

- Works with Sequence number
  - Parity between both numbers
- 32 bit

TCP Breakdown



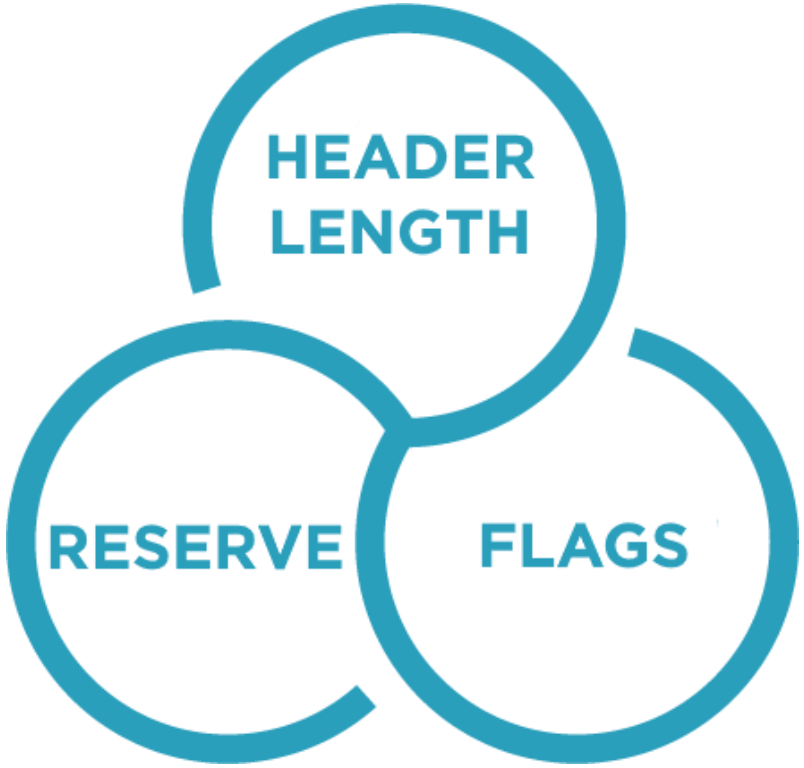
TCP Breakdown



Reserved

- Nothing, held for future use
- 6 bit

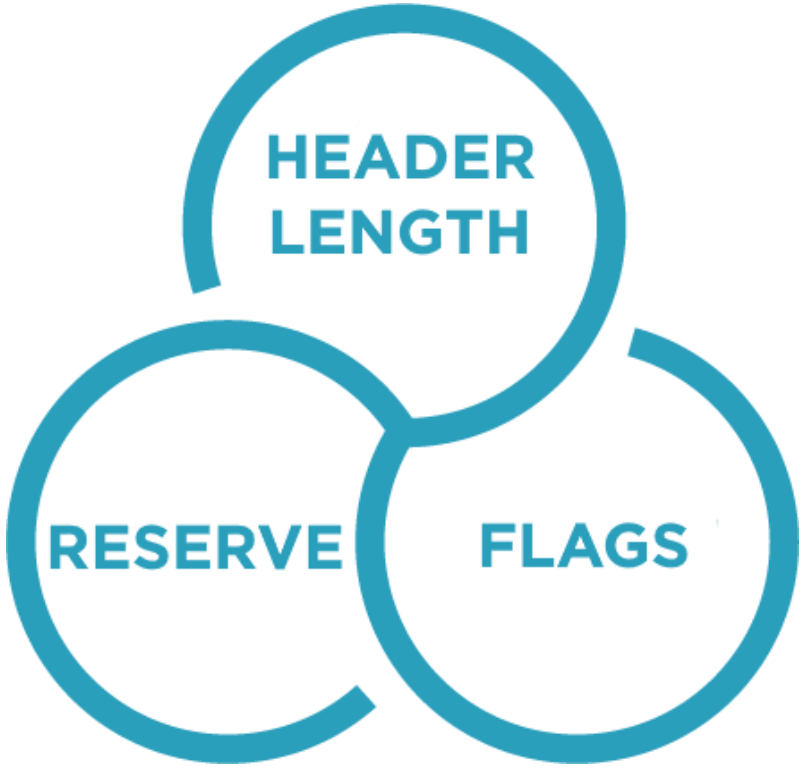
TCP Breakdown



Header length

- Where data begins
- Composed of all header bits
- 4 bit by default

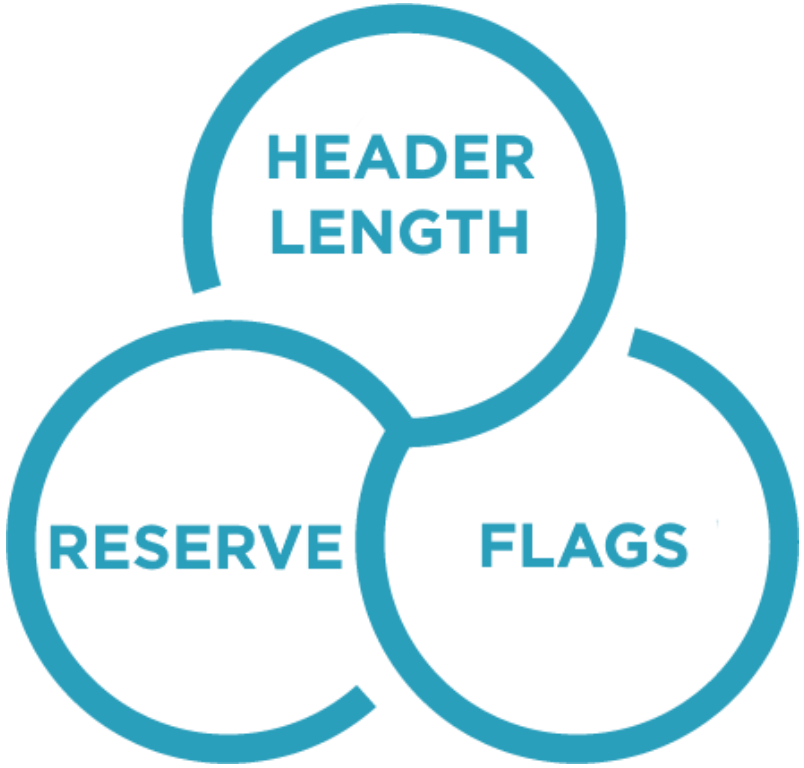
TCP Breakdown



Flags

- 6 primary Flags
- 6 bit
- 4 extra Flags

TCP Breakdown



Primary flags

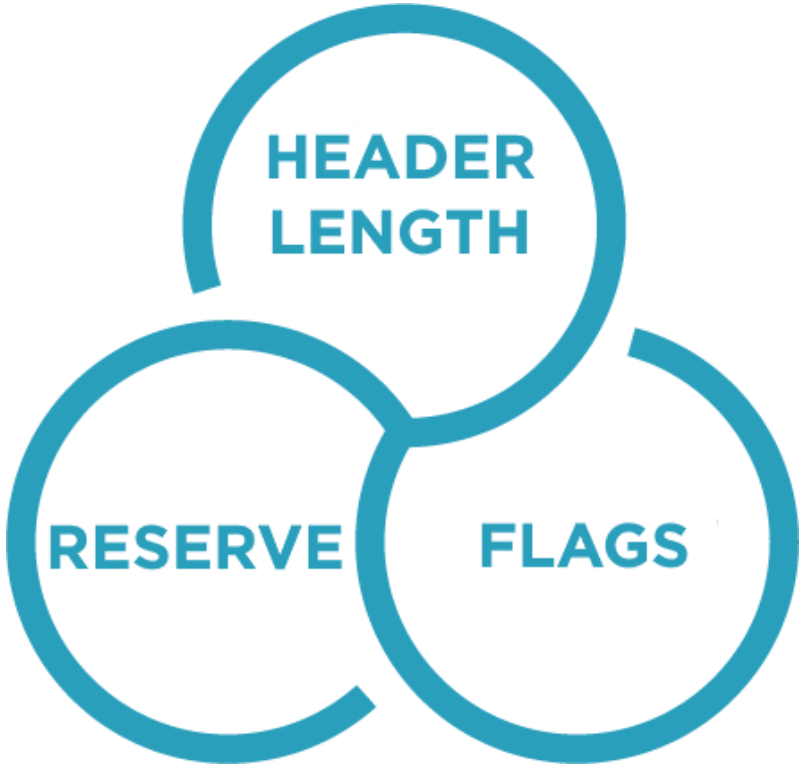
Urgent - Seen as URG

- Flags data as urgent
  - IETF – Don't use

Acknowledgement – Seen as ACK

- Acknowledges receipt of data

TCP Breakdown



Primary flags

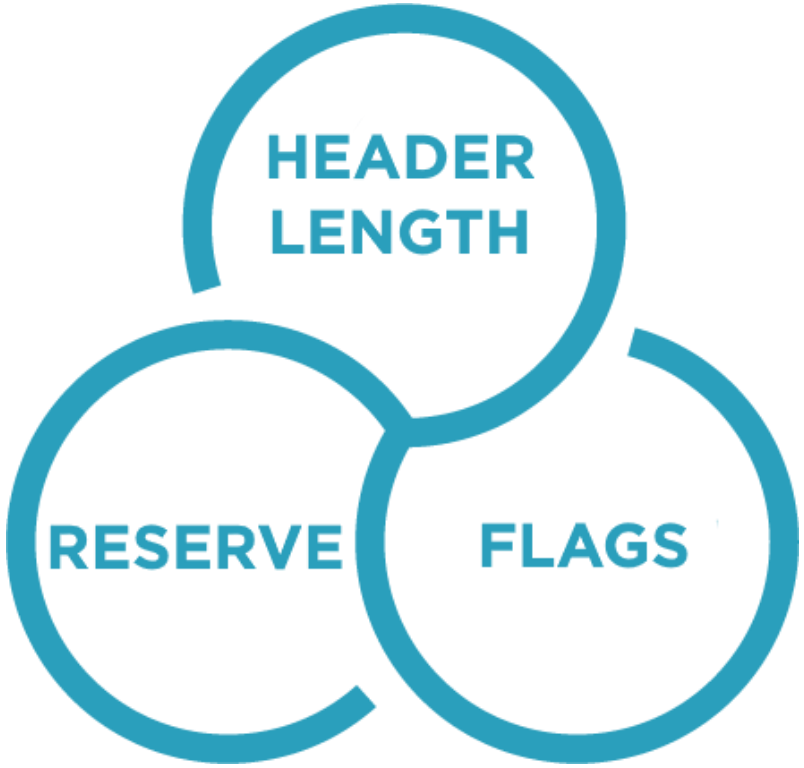
Push - Seen as PSH

- Get to the chopper
  - Do not buffer

Reset – Seen as RST

- Connection Reset
- Multiple causes
  - Firewall is primary

TCP Breakdown



Primary flags

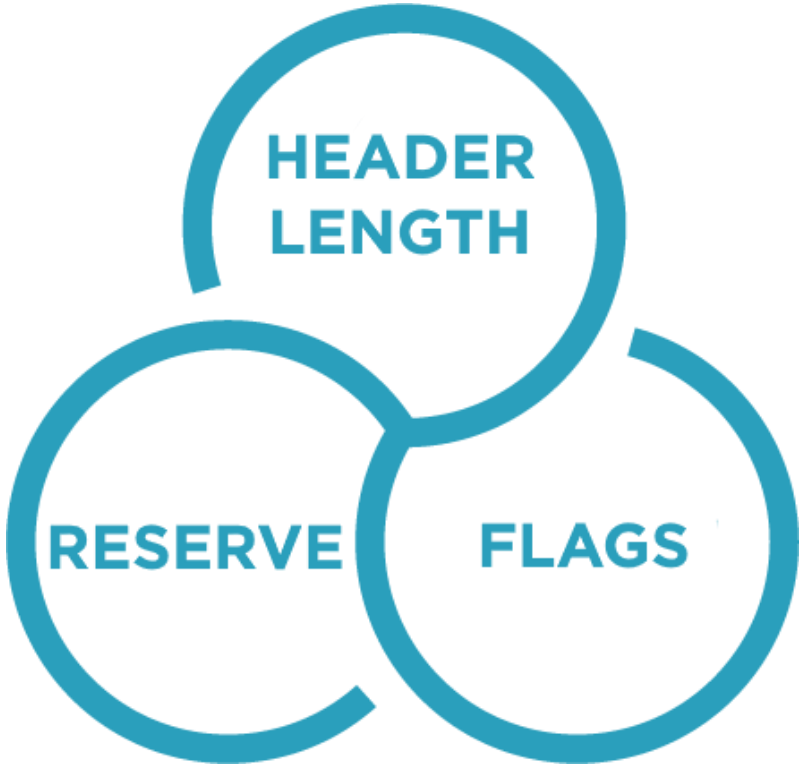
Synchronize - Seen as SYN

- Initiates a connection
- 3-way handshake

Finish – Seen as FIN

- Graceful end
- Should be last thing seen

TCP Breakdown



Extra flags

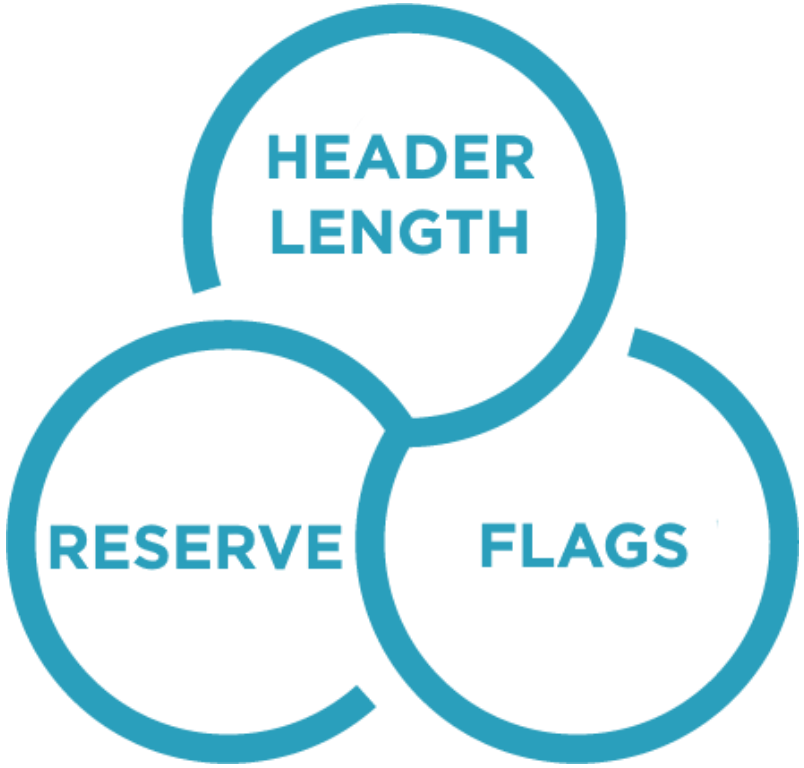
Reserved – Future use

- Per IETF must remain 0

Nonce – Experimental

- Goal to protect against malicious traffic

TCP Breakdown



Extra flags

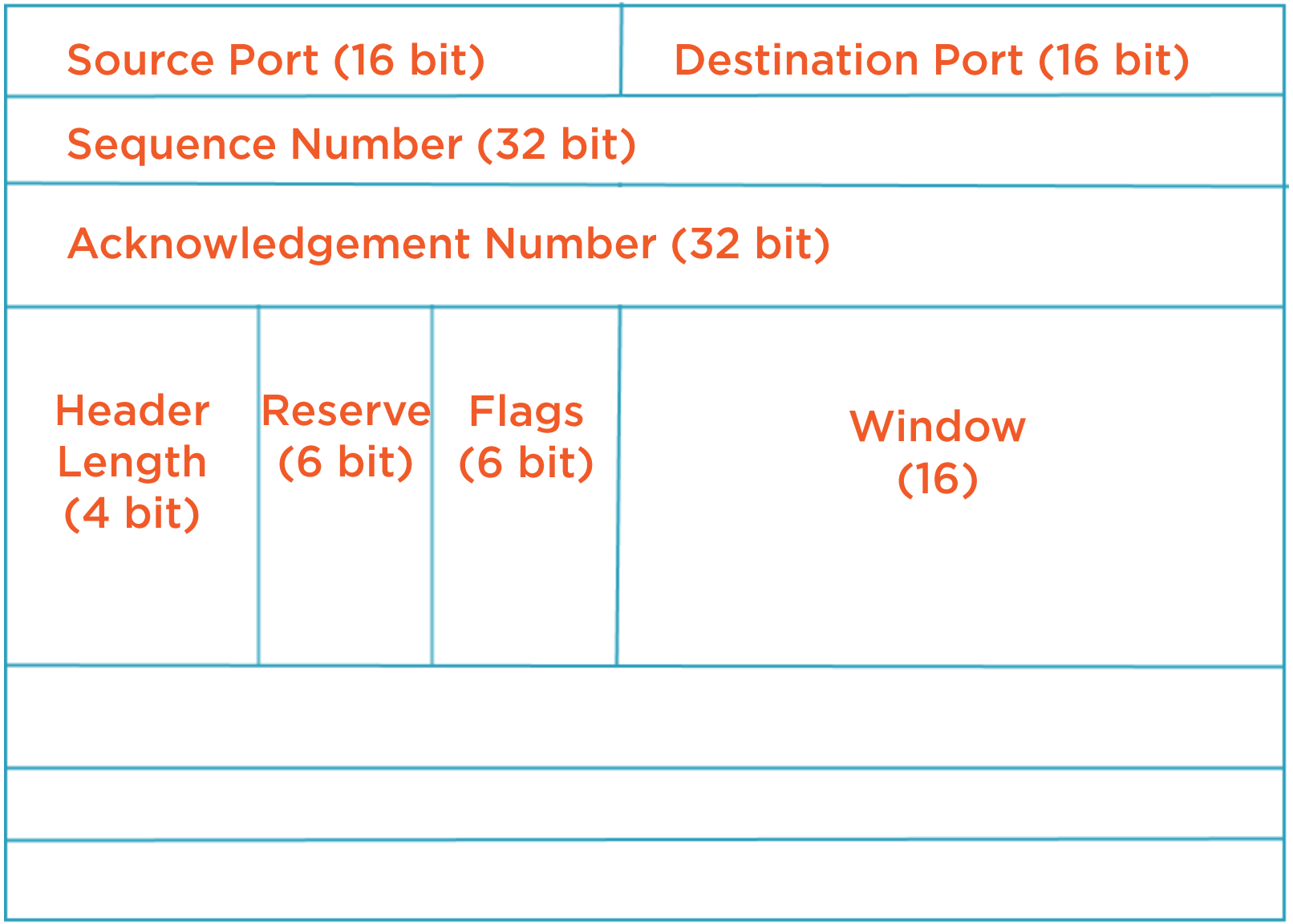
Congestion Window Reduced – AKA CWR

- Notifies about traffic congestion

ECN-Echo – Link to CWR

- Acknowledge traffic congestion

TCP Breakdown

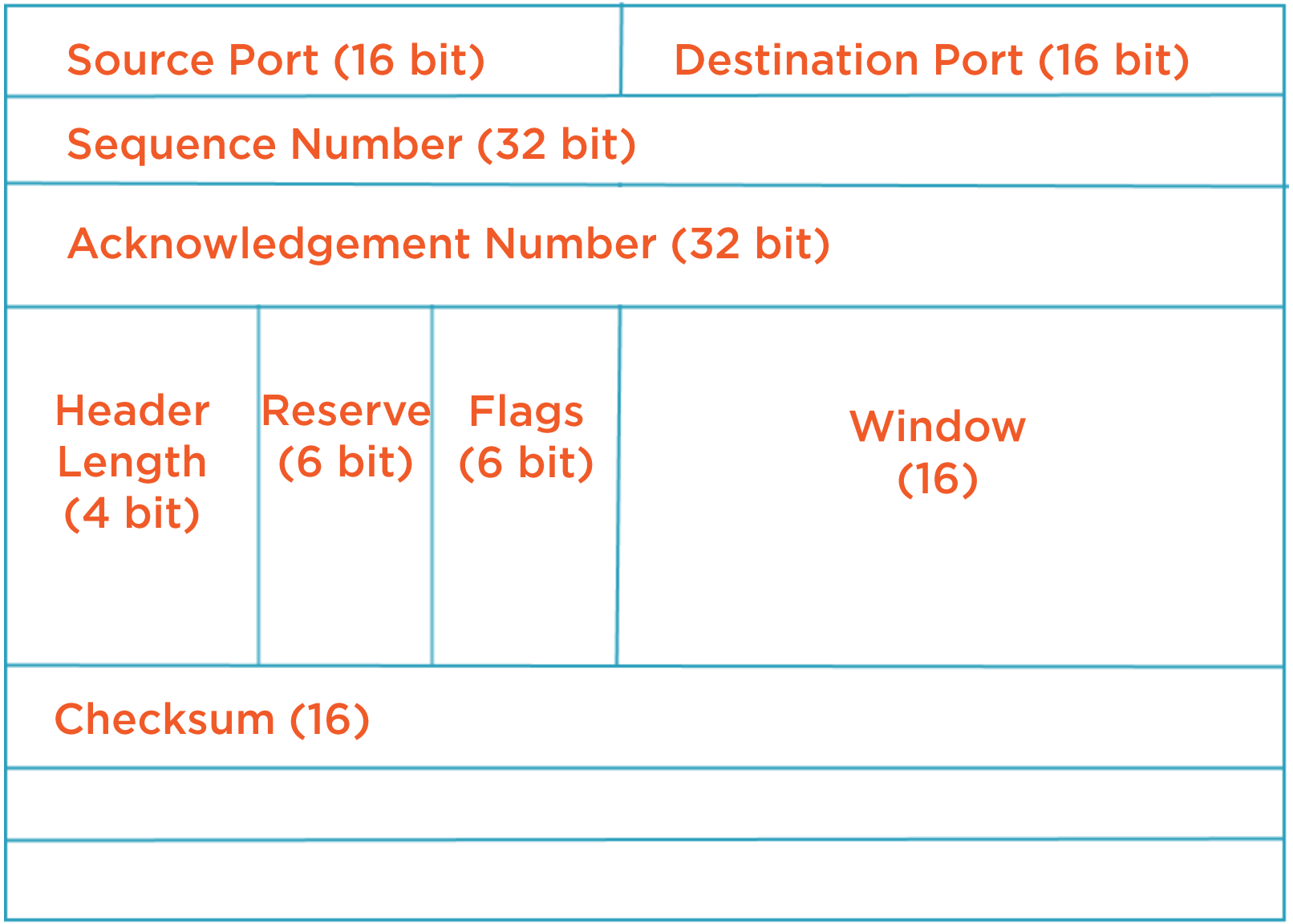


TCP Breakdown

Window – Flow control

- Can adjust rate
- Default bit size of 16

TCP Breakdown

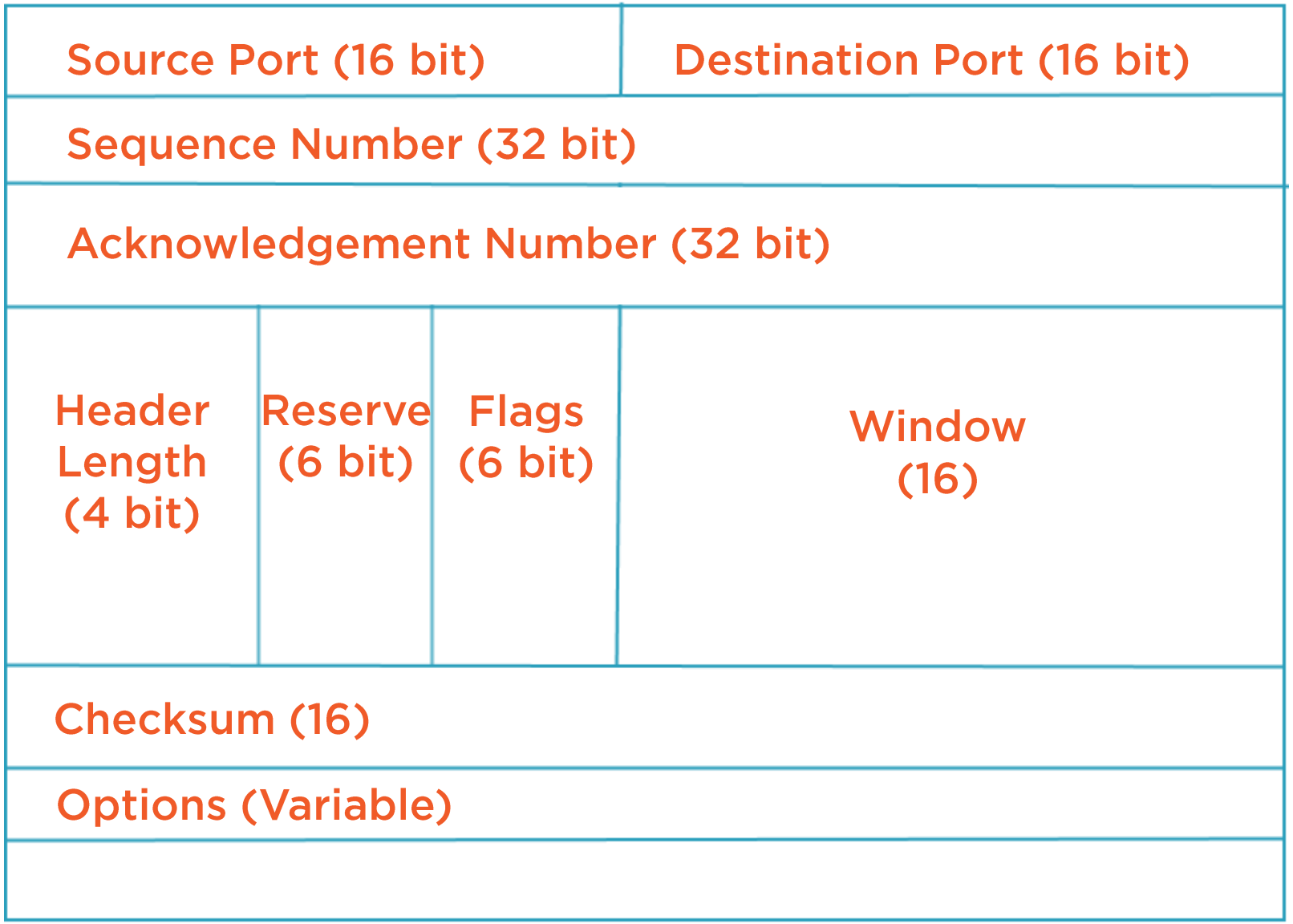


TCP Breakdown

Checksum – Check integrity

- 16 bit

TCP Breakdown

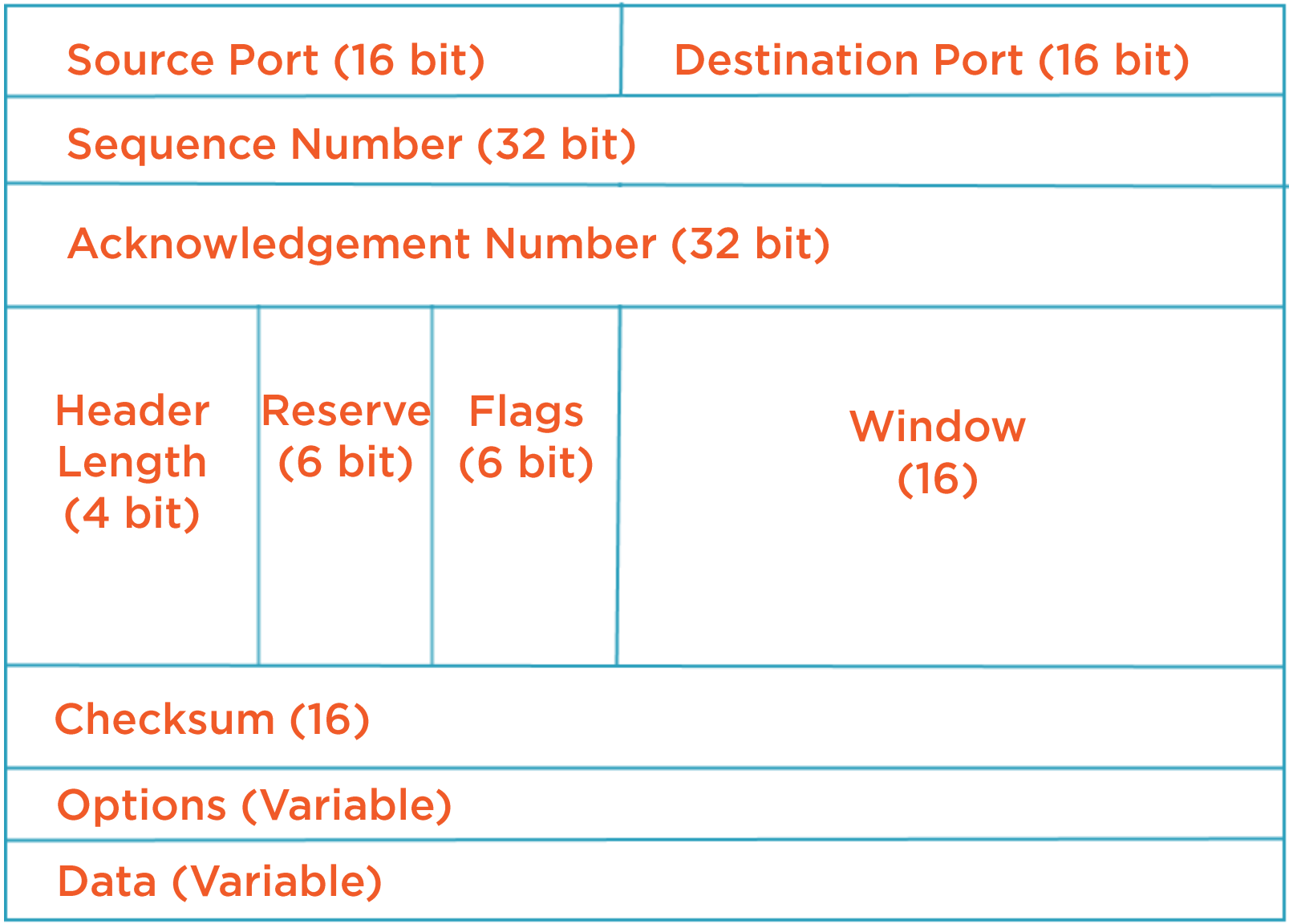


TCP Breakdown

Options – Multiple options

- NOP – No option
- MSS – Largest size of data allowed
- Window Scaling – Increase window size
- SACK – Acknowledge out of order data

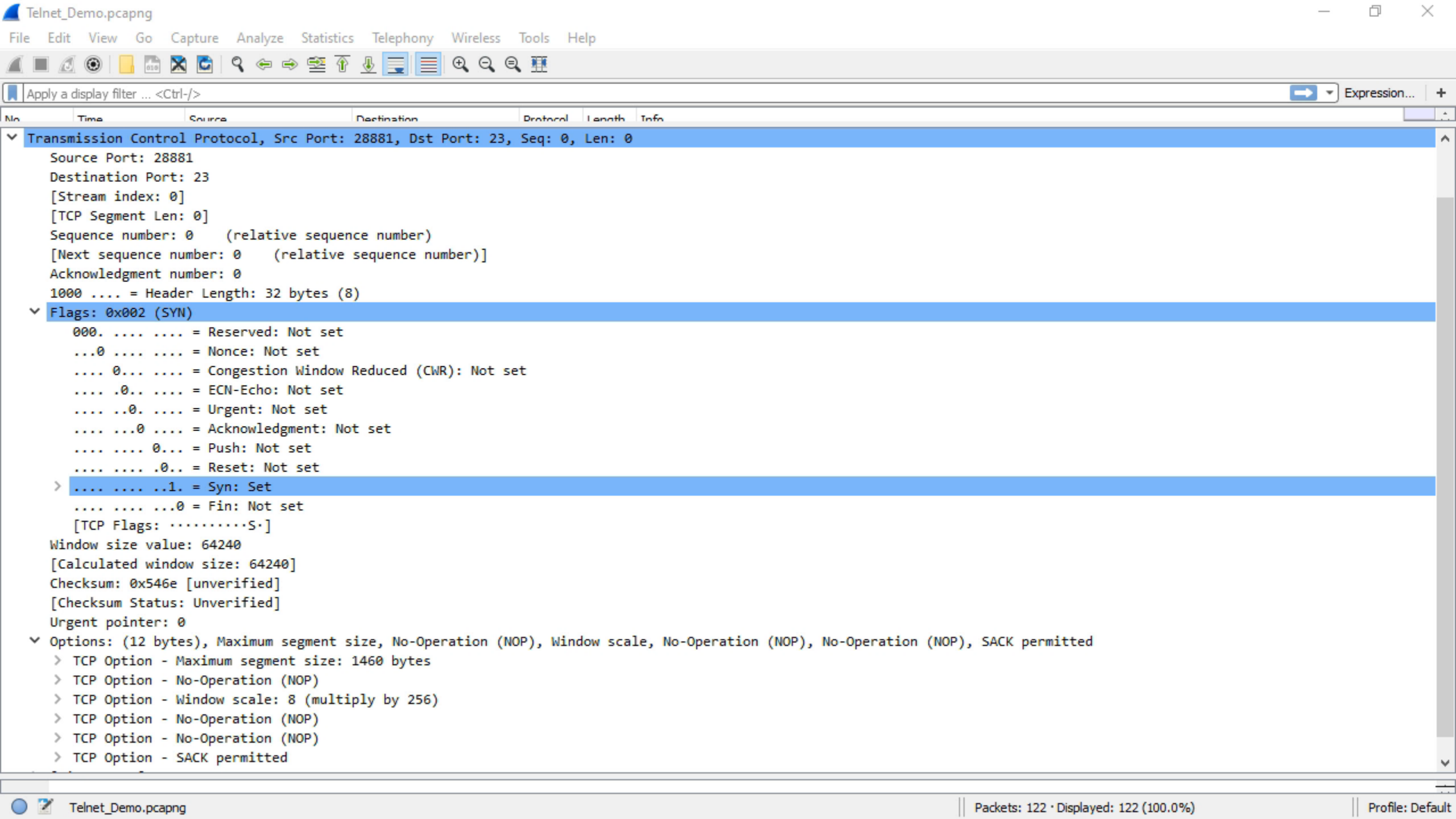
TCP Breakdown



TCP Breakdown

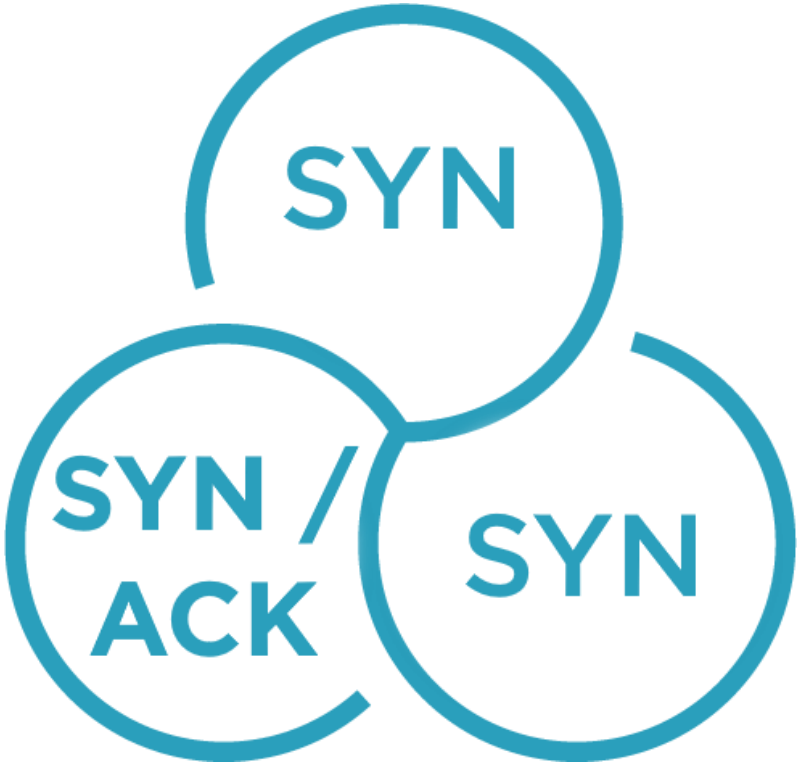
Data – information being transported

- Pictures
- Videos
- Database queries


Telnet_Demo.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
Transmission Control Protocol, Src Port: 28881, Dst Port: 23, Seq: 0, Len: 0
Source Port: 28881
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): 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 size value: 64240
[Calculated window size: 64240]
Checksum: 0x546e [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
TCP Option - Maximum segment size: 1460 bytes
TCP Option - No-Operation (NOP)
TCP Option - Window scale: 8 (multiply by 256)
TCP Option - No-Operation (NOP)
TCP Option - No-Operation (NOP)
TCP Option - SACK permitted
Telnet_Demo.pcapng
Packets: 122 · Displayed: 122 (100.0%)
Profile: Default

TCP Session Formation

TCP Session Formation



3-way handshake

- SYN – Start the conversation
- SYN/ACK – Acknowledges SYN
- 2nd SYN – Acknowledges the SYN/ACK

TCP Session Formation

192.168.1.1

192.168.1.100

TCP Data Segmentation

TCP Data Segmentation

Sequence – Numbers data + payload

Acknowledgement – Acks prior data

TCP Data Segmentation

192.168.1.1

192.168.1.100

TCP Data Reassembly

TCP Data Reassembly

Reassembly

- Order of operations
- Uses Sequence number

TCP Data Reassembly

192.168.1.1

192.168.1.100

TCP Data Retransmission

TCP Data Retransmission

Retransmission

- Relies on Sequence numbers
- Relies on Acknowledgement numbers

TCP Data Retransmission

192.168.1.1

192.168.1.100

TCP Session Termination

TCP Session Termination

Session termination

- Conservation
- Ungraceful termination happens
- Similar to 3-way handshake
  - Works through – ACK FIN flags

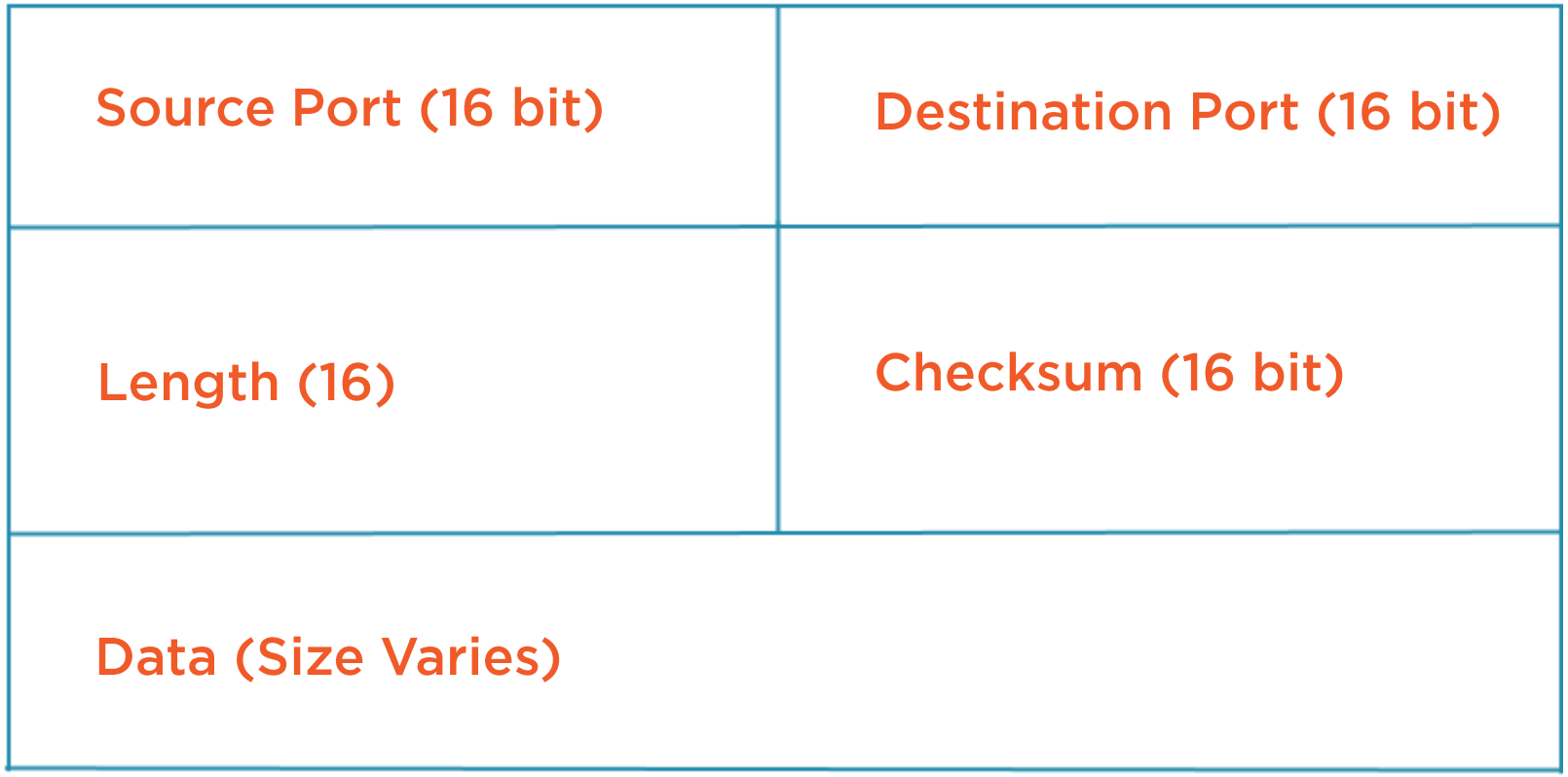
TCP Session Termination

192.168.1.1

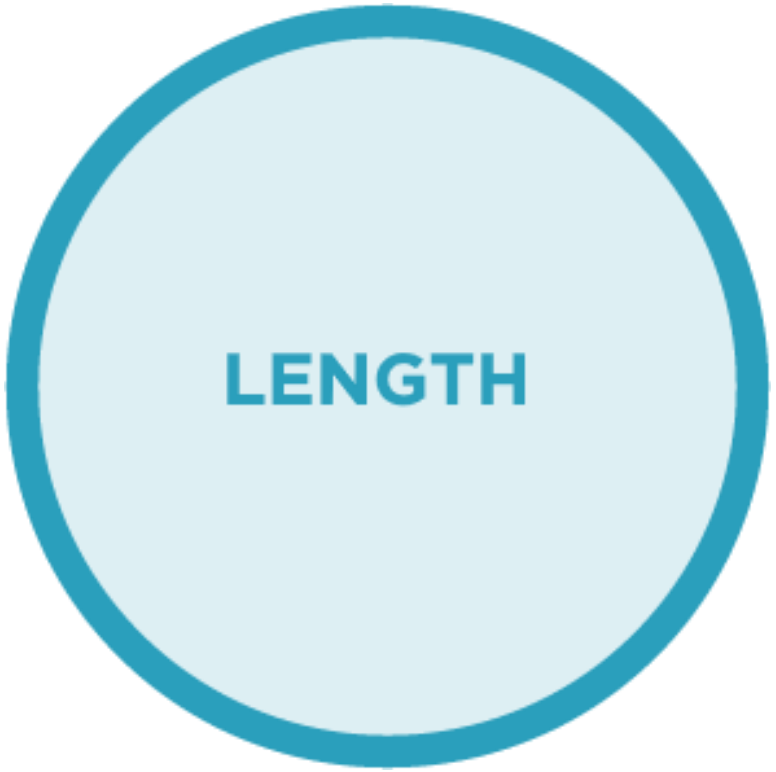
192.168.1.100

UDP Breakdown

UDP Breakdown



TCP Session Termination



Length

- 16 bit default
- Header + data = Value

Slide49_DHCP.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
17	5.023144	0.0.0.0	255.255.255.255	DHCP	308	DHCP Discover - Transaction ID 0x67f4cbc7
69	9.964811	0.0.0.0	255.255.255.255	DHCP	308	DHCP Discover - Transaction ID 0x67f4cbc7
93	13.925548	0.0.0.0	255.255.255.255	DHCP	308	DHCP Discover - Transaction ID 0x67f4cbc7
108	21.857314	0.0.0.0	255.255.255.255	DHCP	308	DHCP Discover - Transaction ID 0x67f4cbc7
112	37.363735	0.0.0.0	255.255.255.255	DHCP	308	DHCP Discover - Transaction ID 0x67f4cbc7
113	57.269083	0.0.0.0	255.255.255.255	DHCP	308	DHCP Discover - Transaction ID 0xc4f347a9
184	62.102177	0.0.0.0	255.255.255.255	DHCP	308	DHCP Discover - Transaction ID 0xc4f347a9
205	65.850463	0.0.0.0	255.255.255.255	DHCP	308	DHCP Discover - Transaction ID 0xc4f347a9
222	74.845706	0.0.0.0	255.255.255.255	DHCP	308	DHCP Discover - Transaction ID 0xc4f347a9
224	90.743174	0.0.0.0	255.255.255.255	DHCP	308	DHCP Discover - Transaction ID 0xc4f347a9
226	122.029000	0.0.0.0	255.255.255.255	DHCP	308	DHCP Discover - Transaction ID 0x7f03733a
228	123.030777	192.168.1.254	255.255.255.255	DHCP	308	DHCP Offer - Transaction ID 0x7f03733a
229	123.031315	0.0.0.0	255.255.255.255	DHCP	336	DHCP Request - Transaction ID 0x7f03733a
230	123.032770	192.168.1.254	255.255.255.255	DHCP	308	DHCP ACK - Transaction ID 0x7f03733a

```
> Frame 17: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: WistronI_6a:c6:75 (98:ee:cb:6a:c6:75), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 308
    Checksum: 0xfb60 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
  > [Timestamps]
> Dynamic Host Configuration Protocol (Discover)
```

Ready to load or capture

Packets: 313 · Displayed: 14 (4.5%)

Profile: Default

Module Review

TCP

- Datagram breakdown
- Wireshark analysis
- Session establishment
- Data segmentation

Module Review

TCP

- Data reassembly
- Loss recovery
- Graceful termination

Module Review

UDP datagram breakdown

- Datagram breakdown
- Wireshark analysis
- How UDP sessions are formed