Investigating TCP Internals

Anthony E. Nocentino
ENTERPRISE ARCHITECT @ CENTINO SYSTEMS
@nocentino www.centinosystems.com

Course Overview

Network Topologies and the OSI Model

Internet Protocol –
Addressing and Subnetting Fundamentals

Internet Protocol –
ARP and DNS Fundamentals

Internet Protocol - Routing Packets

Routing Packets with Linux

Investigating TCP Internals

Troubleshooting Network Issues

Module Overview

Transmission Control Protocol

Connection Establishment/Termination

Data Transfer

Ports

Flow and Congestion Control

Error Detection and Retransmission

UDP

Transmission Control Protocol

Connection oriented

Reliable Delivery

Maintains Order

Error Checking

Transmission Control Protocol

OSI Layer 4

Segments

Provides reliability by requiring positive acknowledgements of delivery

Guarantees order with sequence numbers

Provides error checking with checksums

TCP Header

- Source port
- Destination Port
- Sequence Number
- Acknowledgement Number
- Flags
- Window Size
- Checksum
- Options

Data Transfer in TCP

Application data is divided into segments, a header is added

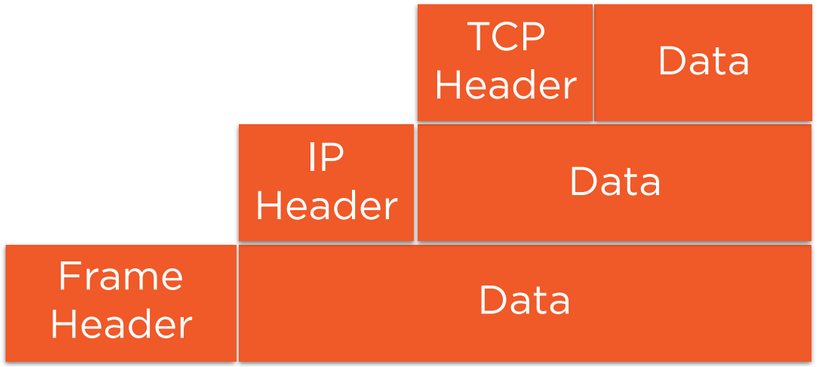
The TCP segment is placed into an IP packet then send to the destination

If a segment is not acknowledged in a period of time it's retransmitted

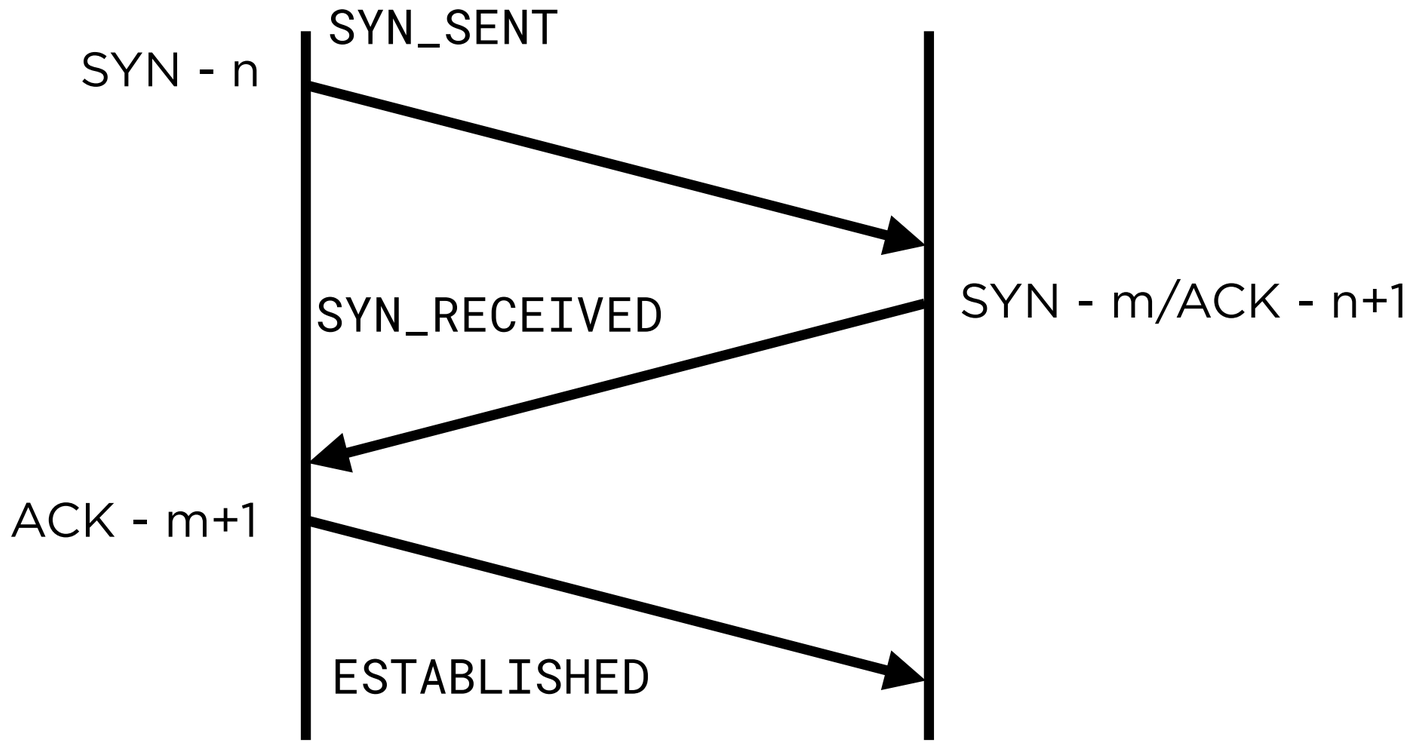
If a segment is received out of order, it's buffered on the receiver then ordered

Full Duplex - two independent streams

TCP Segment Encapsulation

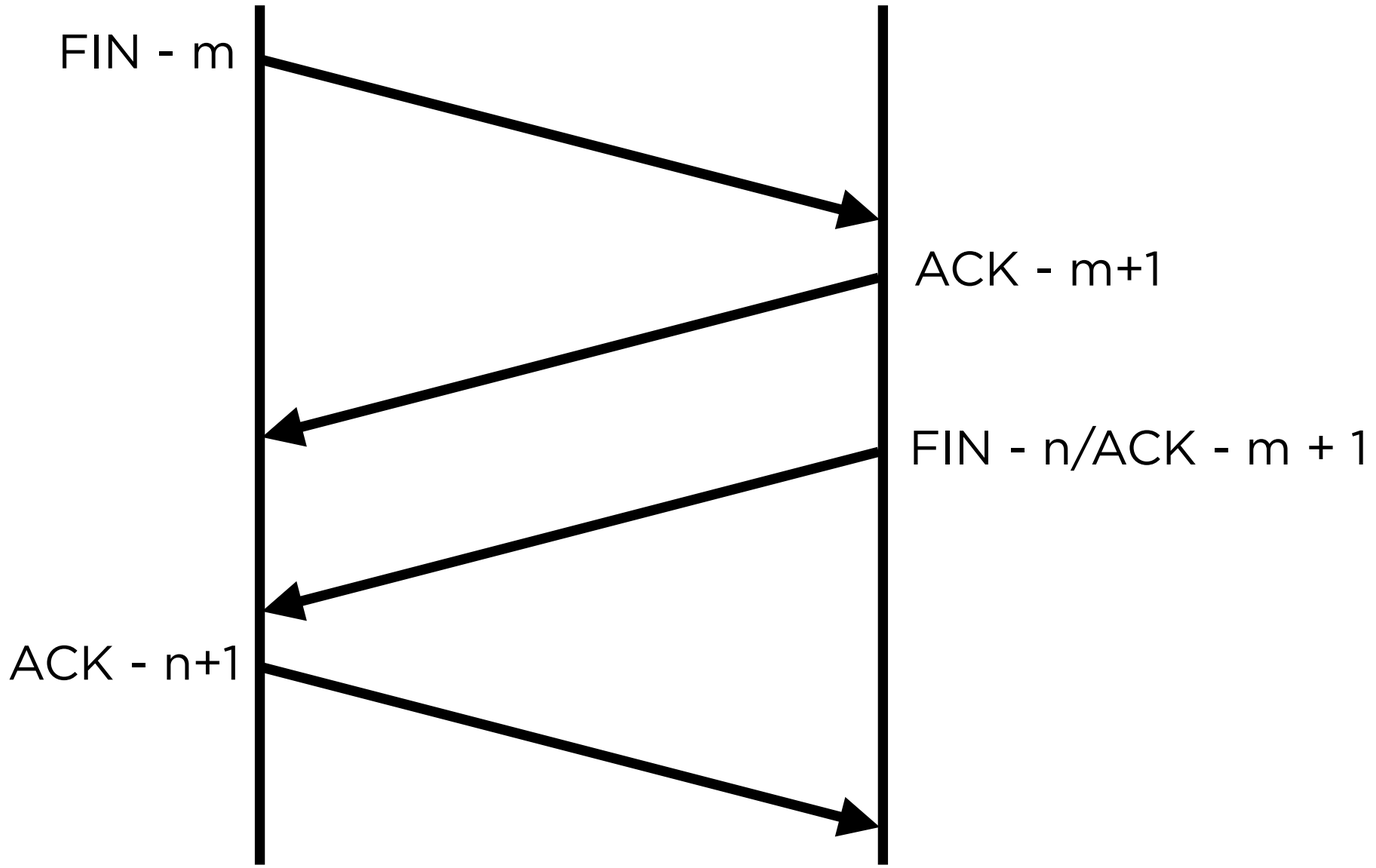


Connection Establishment - Three Way Handshake



Establishes Initial Sequence Numbers
Critical to ordered delivery in both directions

Connection Termination



Ports

Used to identify who is talking to whom

Allocated by an internal data structure

Only one process can one a port on an IP

Port Conflict

For an open connection there are two ports, one on the sender and one on the receiver

A connection consists of:

Sender IP+Port : Receiver IP+Port

Ports

16 bit value

0 - 65,535

Well Know Ports

0 - 1024

root only

Ephemeral Ports

32,768 - 61,000

Demo

- Examine a connection establishment in `wireshark`
- Examine a connection termination in `wireshark`
- Reserved and Ephemeral Ports
- Examining TCP state

Flow Control

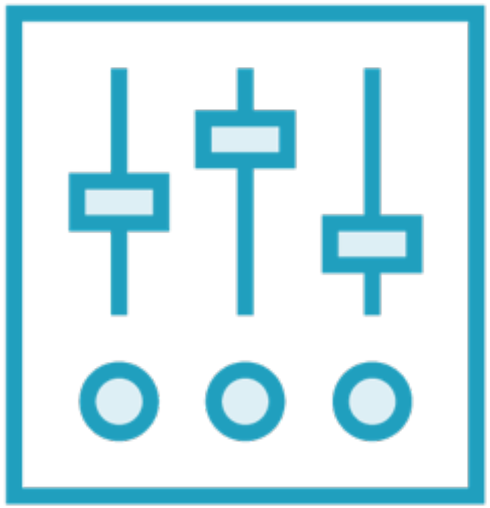
Sending one ACK for every segment is slow

Sliding Window - ability to have more than one segment in transport at a point in time

Maintained by the receiver

Fully realize the bandwidth of the link

Congestion Control



In response to network conditions

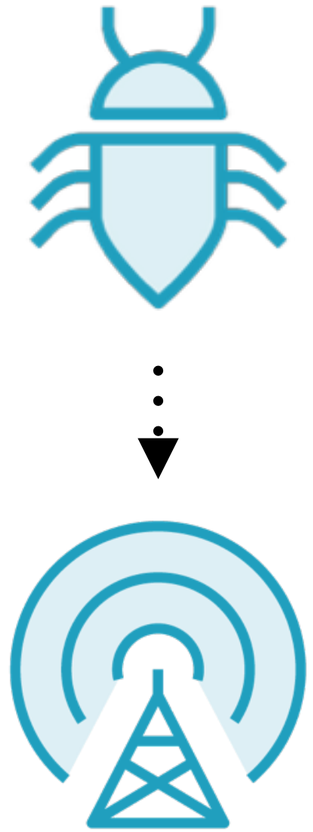
Reduce congestion window size

- The **sender** slows down

Various techniques exist

- Back off, then add load

Error Detection and Retransmission



Unacknowledged transmission

Based on a sample of RTT (how long)

Result in retransmission of the segment

Reduction in congestion window size

User Datagram Protocol (UDP)

Send it and forget it...

Application handles reliable transmission

High performance networking

DNS

VoIP

Demo

- Sliding Window
- Congestion Control
- User Datagram Protocol

Module Overview

Transmission Control Protocol

TCP Header

Connection Establishment/Termination

Data Transfer

Ports

Flow and Congestion Control

Error Detection and Retransmission

UDP

What's Next!

Troubleshooting Network Issues

References

& Further Reading

- **Internetworking with TCP/IP Vol. 1** by Douglas Comer - http://amzn.to/29X7dyT
- **UNIX Network Programming** by W. Richard Stevens- http://amzn.to/2atUjsx
- **TCP State Diagram** - http://bit.ly/28Lgq2u