الجامعة التكنولوجية
قسم هندسة الحاسوب
Department of Computer Engineering

LECTURE #8 (ROUTING PACKETS)

INSTRUCTOR: AMEER MOSA AL-SADI
DEPT OF COMPUTER ENGINEERING
UNIVERSITY OF TECHNOLOGY IN BAGHDAD

Brief Review

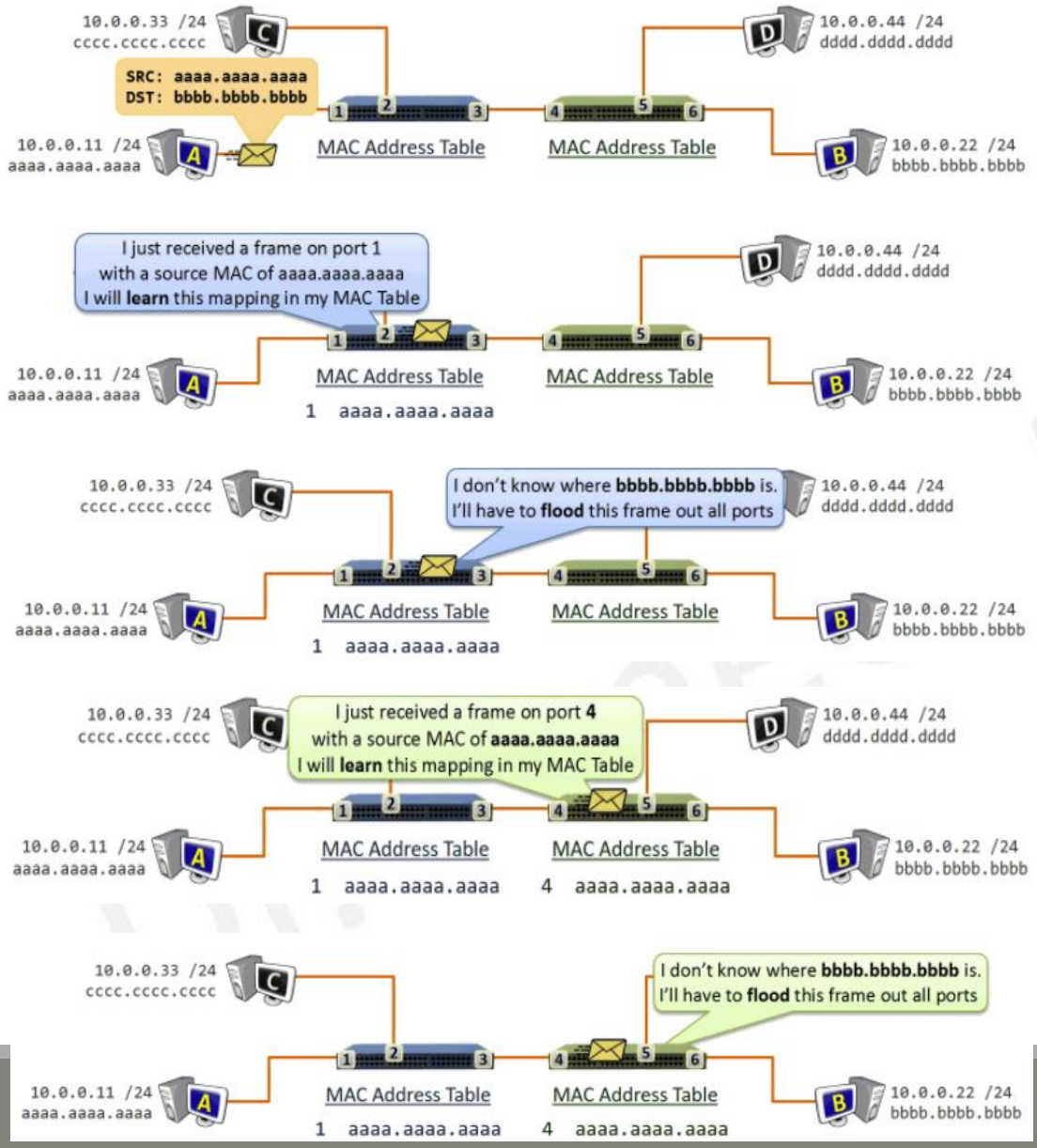
- **Lec1. Network Elements :**
  - Data, Devices, Links.
- **Lec2. Network terminology and concepts:**
  - Network Flow, Domains, challenges, measuring Parameters.
  - Network Design (Devices, Architecture, Topology, Size, Usage, Protocols, Addressing schemes , Transmission media/Links, Used Technology and QoS polices).
- **Lec3. Network Design:**
  - Architecture, Topology, Size, Usage.
- **Lec4. NOS:** Protocols, OSI model, Encapsulation and communication between layers.
- **Lec5. NOS:** TCP/IP Model, (Ethernet, IP, TCP and UDP) header, connection oriented Vs Connection less.
- **Lect6. IP Addressing: (**its classes), (private vs Public IP)and (host and network ranges)
- **Lect7. Subnetting**

What is this Lecture

- **Communication through two Switches**
- Routing Packets
- **Example for Routing.**
- Session establishment and Termination.
- **Example 2: TCP series between Client and HTTP server .**

Communication through two Switches (Layer 2)

Host A to Host B



1) It starts with Host A having a frame to deliver to Host B.

- The contents of the frame are irrelevant, it could be an ICMP (ping) packet, it could be an ARP packet, or it could be other data.
- The Layer3 header would include a Source IP address of 10.0.0.11 (Host A) and a Destination IP address of 10.0.0.22 (Host B).
- The Layer2 header would include a Source MAC address of aaaa.aaaa.aaaa and a Destination MAC address of bbbb.bbbb.bbbb. The switches will use the information in the Layer2 header to move the frame between the two hosts.
- To begin, the MAC address tables for *both* switches will be empty.
- They will populate as the switches learn of each device connected to each port by reading the Source MAC address field of each received frame.

2) When the frame arrives on the blue switch, the first thing that happens is the blue switch learns the MAC address aaaa.aaaa.aaaa exists on port 1.

3) Then, since the blue switch does not yet have an entry in tis MAC address table for bbbb.bbbb.bbbb, the frame is duplicated and flooded out every port.

The frame arrives on Host C, who will inspect the frame and realize it is not the intended recipient. Host C will silently discard the frame.

4) The frame will also arrive on the green switch. Just like the other switch, the first thing the green switch will do is learn that it received a frame on port 4 with a source MAC address of aaaa.aaaa.aaaa.

5) And again, just like the other switch, the green switch does not know where the MAC address bbbb.bbbb.bbbb exists, so the frame will again be duplicated and flooded out each switch port.

Notice in both cases, the frame was flooded out each port, *except the port it was received on*. This is an example of a switch's filtering behavior. This behavior prevents a switch from sending a frame out the same port it was received.

Host D will receive the frame, and silently discard it since the frame was not addressed to Host D.

Host B will receive the frame and accept it for processing, since Host B was the intended destination.

Communication through two Switches (Layer 2)

Host B to Host A

On the way back things will go a little simpler. The switches have already learned about some of the connected devices, and that should alleviate some of the additional flooding that was required for the initial communication in the previous section.
Specifically, both switches know the location of the MAC address aaaa.aaaa.aaaa – port 1 on the blue switch and port 4 on the green switch. Each switch learned the location independent of the other; there was no communication between the switches or sharing of MAC address tables.

1) In the response frame sent by Host B to Host A, the Layer2 header will have a Source MAC address of bbbb.bbbb.bbbb and a Destination MAC address of aaaa.aaaa.aaaa.

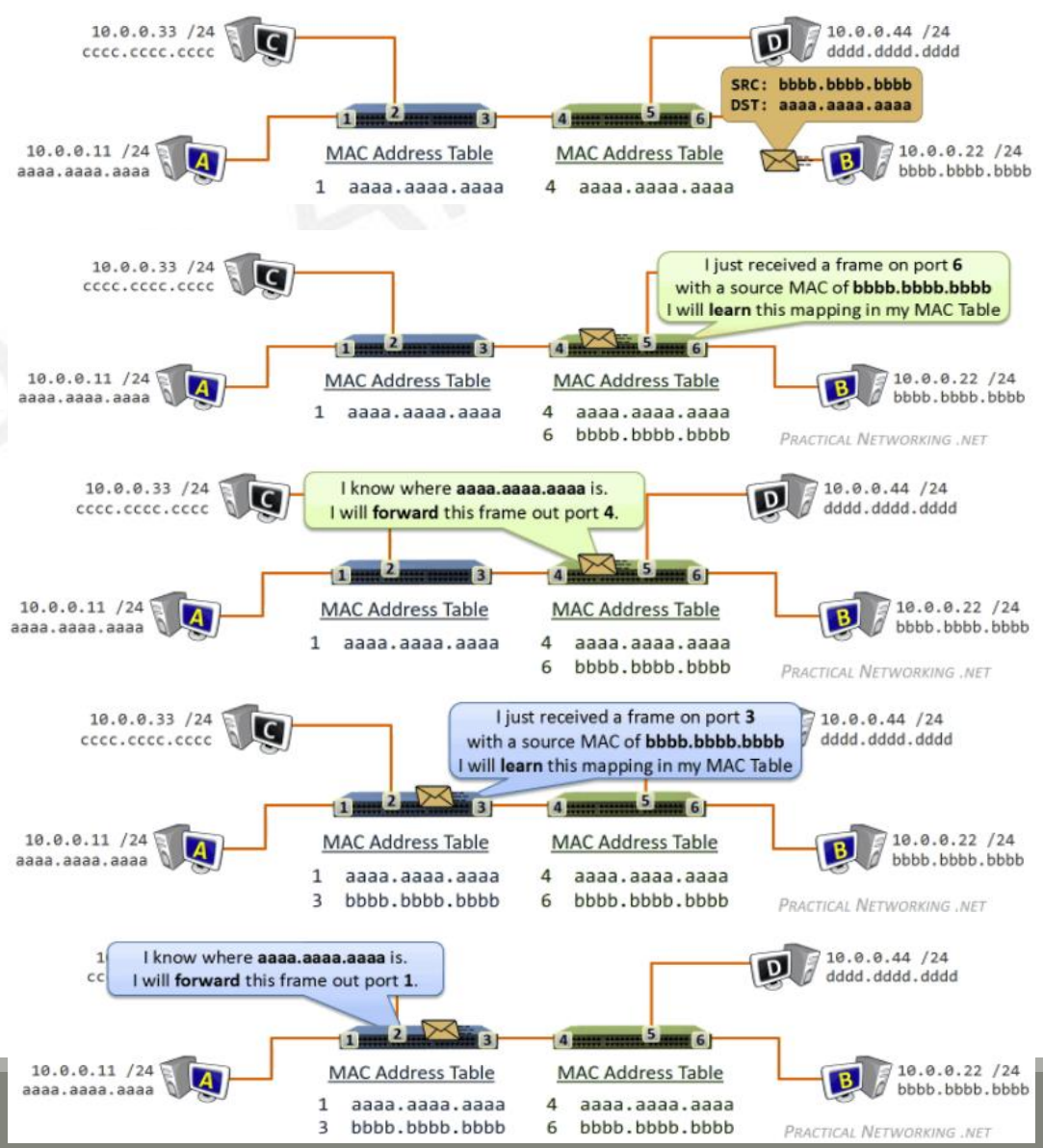
2) The response frame will first arrive on the green switch on port 6. Therefore, the green switch will learn that the MAC address bbbb.bbbb.bbbb exists out port 6.

3) The green switch then consults its MAC address table to determine that the frame destined to aaaa.aaaa.aaaa should be forwarded out port 4.

4) The response frame then arrives on the blue switch on port 3. Therefore, the blue switch will learn the MAC address bbbb.bbbb.bbbb exists out port 3.

5) The blue switch then consults its MAC address table to determine that the frame destined to aaaa.aaa.aaaa should be forwarded out port 1.

Which will finally get the response frame back to Host A. Notice on the way back no flooding was required. Both switches knew the location of the destination MAC address of the frame.



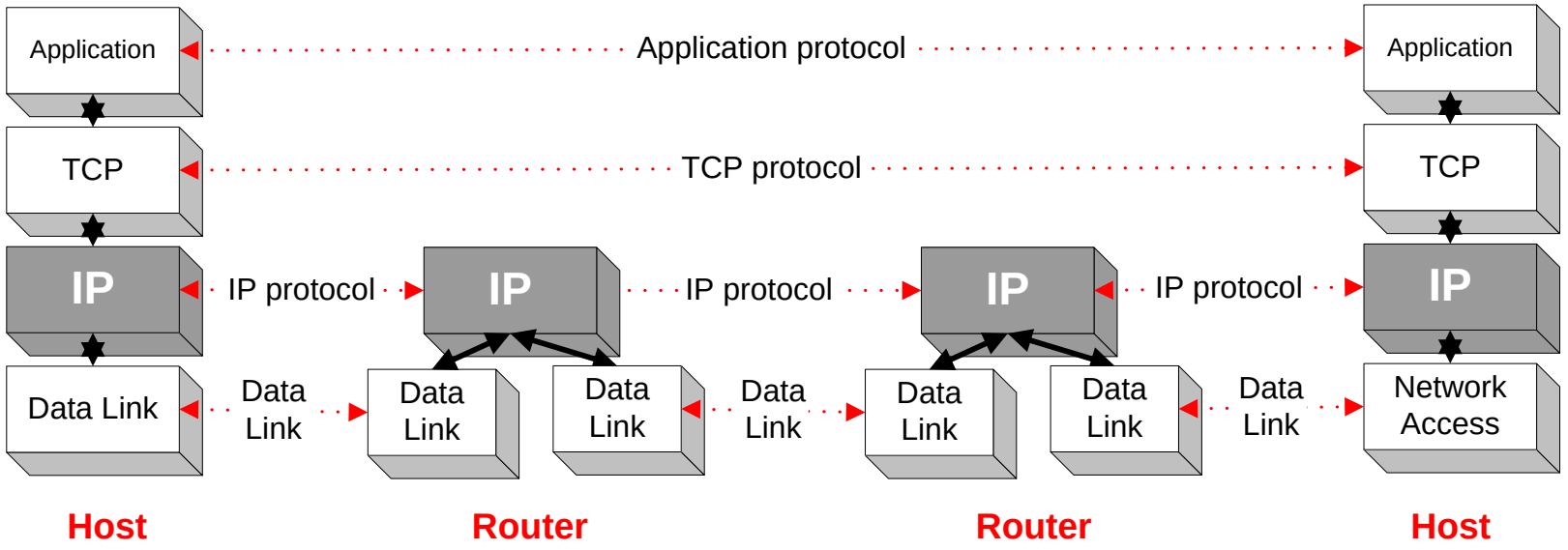
Routing Packets

- IP is the highest layer protocol which is implemented at both routers and hosts

6

Routing Packets

- IP is the highest layer protocol which is implemented at both routers and hosts



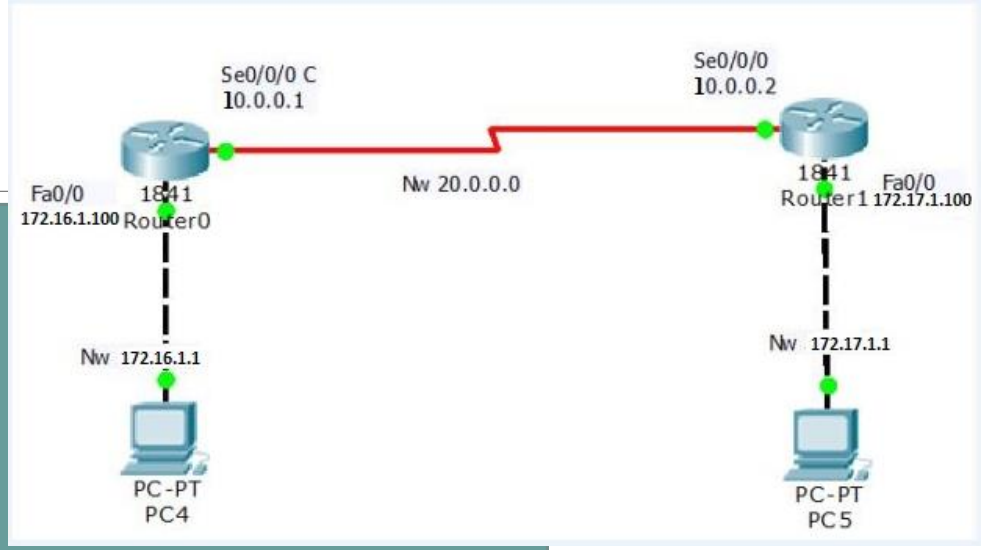
7

A routing is used to route data packets between two networks. As shown below:

1. Router reads the information in each packet to tell where it is going. If it is destined for an immediate network it has access to, it will strip the outer packet, re-address the packet to the proper Ethernet address, and transmit it on that network.

2. If it is destined for another network and must be sent to another router, it will re-package the outer packet to be received by the next router and send it to the next router.

Example for Routing:



(10.0.0.1) (10.0.0.2)

S0 S0

(R1)----------(R2)

!Fa0/0 (0ACF:AAA1:000A) ! Fa0/1 (1ACF:BBA1:010A)

!IP - 172.16.1.100 ! IP - 172.17.1.100

!

!

!

!

!

(Host A) **(Host B)**

E0 (ABC0:ABB1:00A0) E0 (CAA0:ABE1:110A)

IP - 172.16.1.1 IP - 172.17.1.1

Just assume this is a network & all interfaces having their

Layer 2 (physical address)& Layer 3 (IP address).

Host A want to send some data to Host B.

Now what would be the Layer 2 & 3 source & Destination address in the following sequence :

a) Packet leaving Host A.

Layer 3 Source add - 172.16.1.1

Layer 3 Destination add - 172.17.1.1

Layer 2 Source add - ABC0:ABB1:00A0 (E0 of Host A)

Layer 2 Destination add - 0ACF:AAA1:000A (E0/1 of R1)

b) Packet leaving Router R1 -

Layer 3 Source add - 172.16.1.1

Layer 3 Destination add - 172.17.1.1

Layer 2 Source add - 0ACF:AAA1:000A (E0/1 of R1)

Layer 2 Destination add - 1ACF:BBA1:010A (E0/1 of R2)

c) Packet leaving Router R2 -

Layer 3 Source add - 172.16.1.1

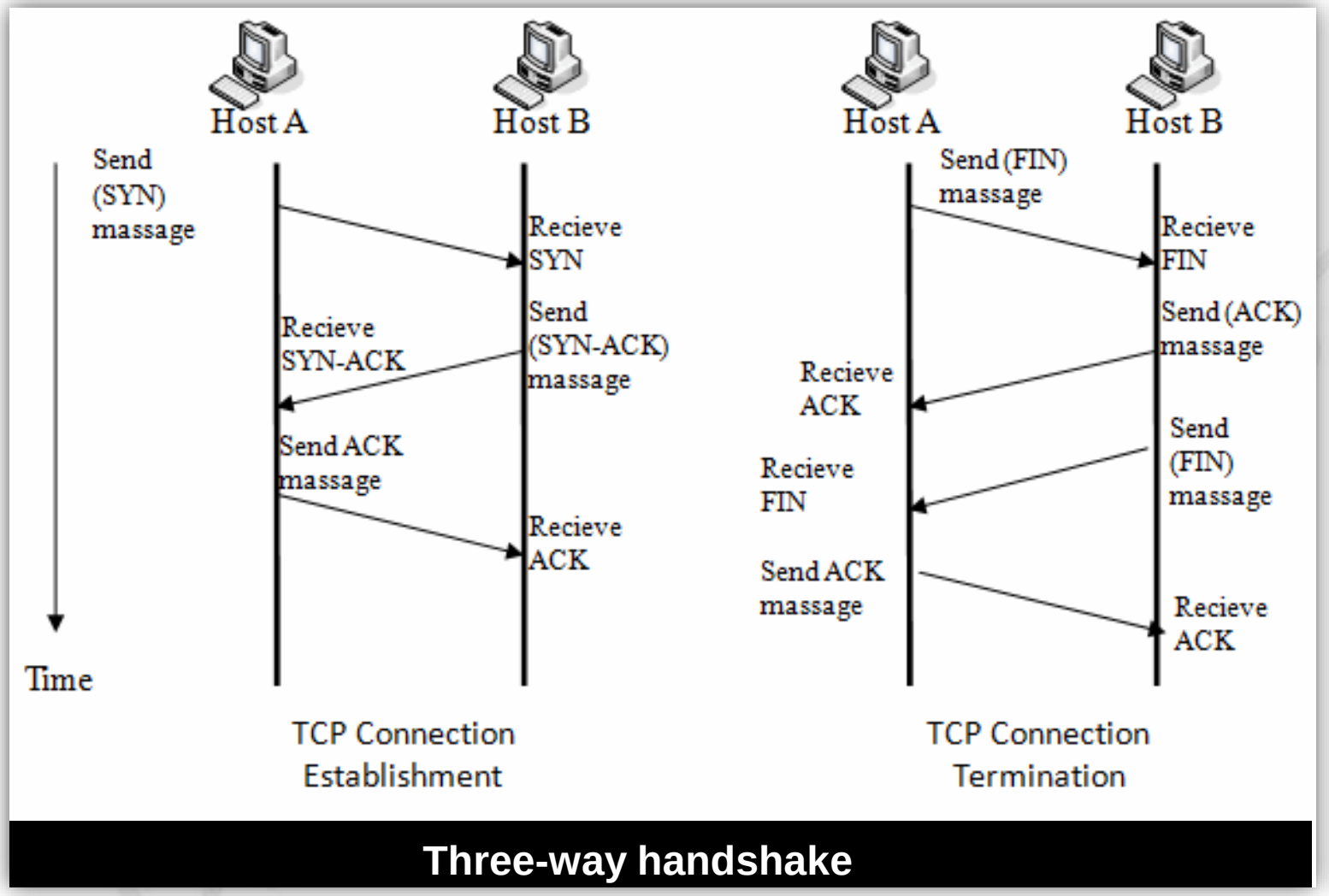
Layer 3 Destination add - 172.17.1.1

Layer 2 Source add - 1ACF:BBA1:010A (E0/1 of R2)

Layer 2 Destination add - CAA0:ABE1:110A (E0/1 of R2)

So every time ***destination physical address*** is changed.

Session establishment and Termination



Three-way handshake

Figure 1: TCP Connection Establishment and Termination, and *focus on basic flags of packets*.

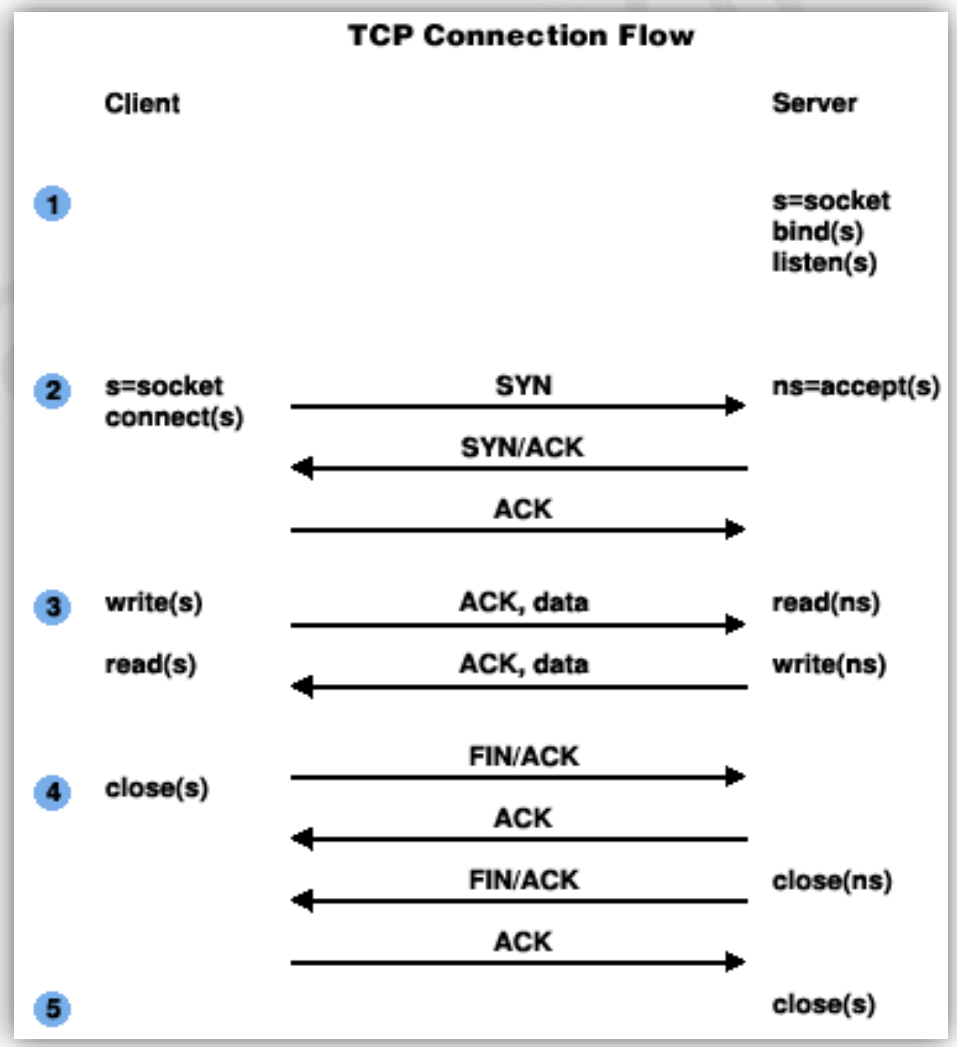


Figure 2: Establish, Transfer and Terminate TCP connection with focusing on socket concept.

More details for Session establishment and Termination

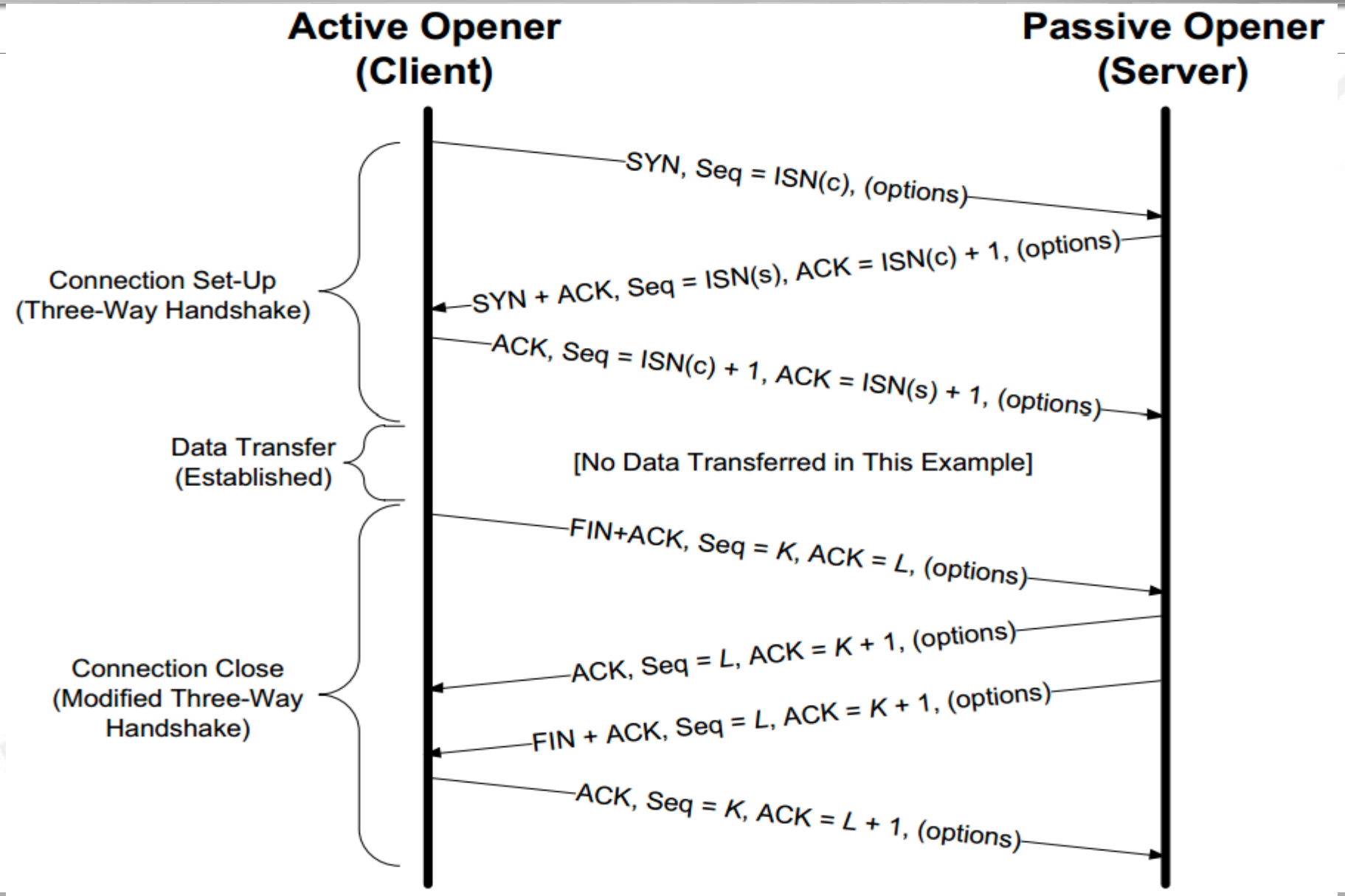


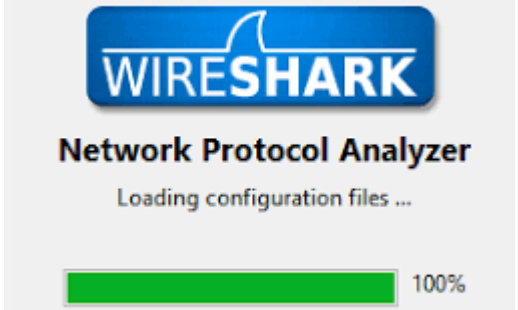
Figure 3: Establish, Transfer and Terminate TCP connection with focusing on Sequence and Acknowledgement Numbers

Practical TCP Series - Sequence and Acknowledgment Numbers

Wireshark Network Capturing Tools

Example 2: TCP series between Client and HTTP server .

Wireshark Network Capturing Tools



Time	192.168.1.2 (54841)	174.143.213.18 (80)	Comment
0.000	SYN		Seq = 0 Ack = 94856056
0.047	SYN, ACK		Seq = 0 Ack = 1
0.047	ACK		Seq = 1 Ack = 1
0.047	PSH, ACK - Len: 725		Seq = 1 Ack = 1
0.097	ACK		Seq = 1 Ack = 726
0.100	ACK - Len: 1448		Seq = 1 Ack = 726
0.100	ACK		Seq = 726 Ack = 1449
0.100	ACK - Len: 1448		Seq = 1449 Ack = 726
0.100	ACK		Seq = 726 Ack = 2897
0.100	ACK - Len: 1448		Seq = 2897 Ack = 726
0.100	ACK		Seq = 726 Ack = 4345
0.150	ACK - Len: 1448		Seq = 4345 Ack = 726
0.150	ACK		Seq = 726 Ack = 5793
0.152	ACK - Len: 1448		Seq = 5793 Ack = 726
0.152	ACK		Seq = 726 Ack = 7241
0.152	ACK - Len: 1448		Seq = 7241 Ack = 726
0.152	ACK		Seq = 726 Ack = 8689

Save As Close

https://packetlife.net/blog/2010/jun/7/understanding-tcp-sequence-acknowledgment-numbers/

Thank You