TTM 4150 PRACTICAL

EXERCISE 2

NETWORK ANALYZERS

Group 20

Maria Fernandez Rodriguez

David Rozas Domingo

Youzhang Liu

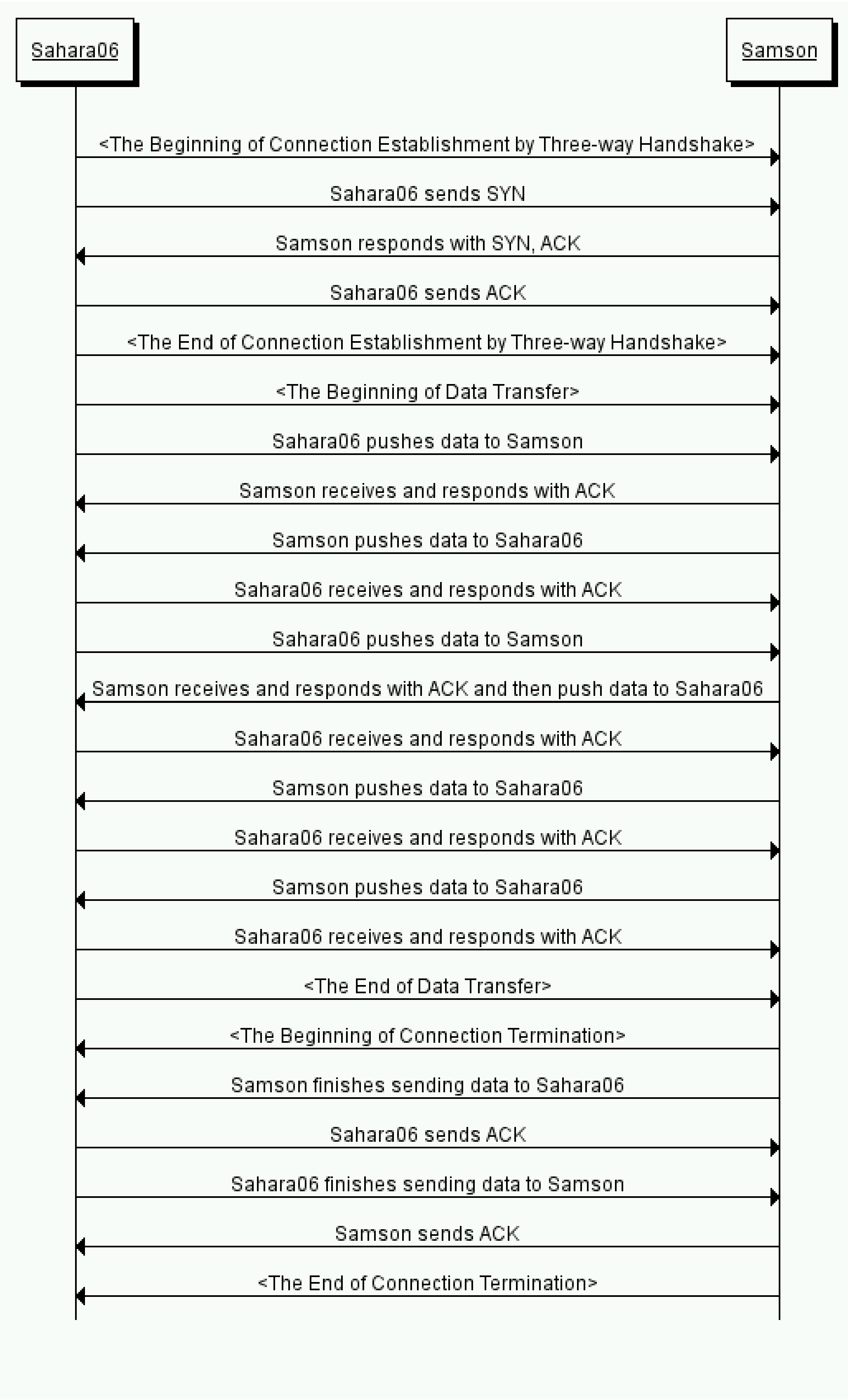
Part 1

The log file is as follows:

```
/*Connection Establishment by Three-way Handshake*/

09:13:37.514218 IP sahara06.item.ntnu.no.53588 >
samson.item.ntnu.no.www: S 215175111:215175111(0) win 5840 <mss
1460,sackOK,timestamp 65738354 0,nop,wscale 5>
09:13:37.514371 IP samson.item.ntnu.no.www >
sahara06.item.ntnu.no.53588: S 3198126294:3198126294(0) ack 215175112
win 5792 <mss 1460,sackOK,timestamp 194280270 65738354,nop,wscale
7>
09:13:37.514394 IP sahara06.item.ntnu.no.53588 >
samson.item.ntnu.no.www: . ack 1 win 183 <nop,nop,timestamp 65738354
194280270>

/*Data Transfer*/
09:13:37.514415 IP sahara06.item.ntnu.no.53588 >
samson.item.ntnu.no.www: P 1:423(422) ack 1 win 183 <nop,nop,timestamp
65738354 194280270>
09:13:37.514648 IP samson.item.ntnu.no.www >
sahara06.item.ntnu.no.53588: . ack 423 win 54 <nop,nop,timestamp
194280270 65738354>
09:13:37.516047 IP samson.item.ntnu.no.www >
sahara06.item.ntnu.no.53588: P 1:426(425) ack 423 win 54
<nop,nop,timestamp 194280271 65738354>
09:13:37.516058 IP sahara06.item.ntnu.no.53588 >
samson.item.ntnu.no.www: . ack 426 win 216 <nop,nop,timestamp 65738354
194280271>
09:13:37.615412 IP sahara06.item.ntnu.no.53588 >
samson.item.ntnu.no.www: P 423:770(347) ack 426 win 216
<nop,nop,timestamp 65738379 194280271>
09:13:37.616285 IP samson.item.ntnu.no.www >
sahara06.item.ntnu.no.53588: . 426:1874(1448) ack 770 win 62
<nop,nop,timestamp 194280296 65738379>
09:13:37.616314 IP sahara06.item.ntnu.no.53588 >
samson.item.ntnu.no.www: . ack 1874 win 307 <nop,nop,timestamp
65738379 194280296>
09:13:37.616402 IP samson.item.ntnu.no.www >
sahara06.item.ntnu.no.53588: . 1874:3322(1448) ack 770 win 62
<nop,nop,timestamp 194280296 65738379>
```

```
09:13:37.616410 IP sahara06.item.ntnu.no.53588 >
samson.item.ntnu.no.www: . ack 3322 win 397 <nop,nop,timestamp
65738379 194280296>
09:13:37.616465 IP samson.item.ntnu.no.www >
sahara06.item.ntnu.no.53588: P 3322:4063(741) ack 770 win 62
<nop,nop,timestamp 194280296 65738379>
09:13:37.616471 IP sahara06.item.ntnu.no.53588 >
samson.item.ntnu.no.www: . ack 4063 win 488 <nop,nop,timestamp
65738379 194280296>


/*Connection Termination*/
09:13:52.618198 IP samson.item.ntnu.no.www >
sahara06.item.ntnu.no.53588: F 4063:4063(0) ack 770 win 62
<nop,nop,timestamp 194284046 65738379>
09:13:52.658919 IP sahara06.item.ntnu.no.53588 >
samson.item.ntnu.no.www: . ack 4064 win 488 <nop,nop,timestamp
65742140 194284046>
09:14:03.028065 IP sahara06.item.ntnu.no.53588 >
samson.item.ntnu.no.www: F 770:770(0) ack 4064 win 488
<nop,nop,timestamp 65744733 194284046>
09:14:03.028233 IP samson.item.ntnu.no.www >
sahara06.item.ntnu.no.53588: . ack 771 win 62 <nop,nop,timestamp
1942866 65744733>
```

The interpretation of each message and MSD (message sequence diagram) is as follows: (Note that the words in the <> are not the interpretations but additional words for understanding of the log)


Sahara06
Samson
<The Beginning of Connection Establishment by Three-way Handshake>
Sahara06 sends SYN
Samson responds with SYN, ACK
Sahara06 sends ACK
<The End of Connection Establishment by Three-way Handshake>
<The Beginning of Data Transfer>
Sahara06 pushes data to Samson
Samson receives and responds with ACK
Samson pushes data to Sahara06
Sahara06 receives and responds with ACK
Sahara06 pushes data to Samson
Samson receives and responds with ACK and then push data to Sahara06
Sahara06 receives and responds with ACK
Samson pushes data to Sahara06
Sahara06 receives and responds with ACK
Samson pushes data to Sahara06
Sahara06 receives and responds with ACK
<The End of Data Transfer>
<The Beginning of Connection Termination>
Samson finishes sending data to Sahara06
Sahara06 sends ACK
Sahara06 finishes sending data to Samson
Samson sends ACK
<The End of Connection Termination>

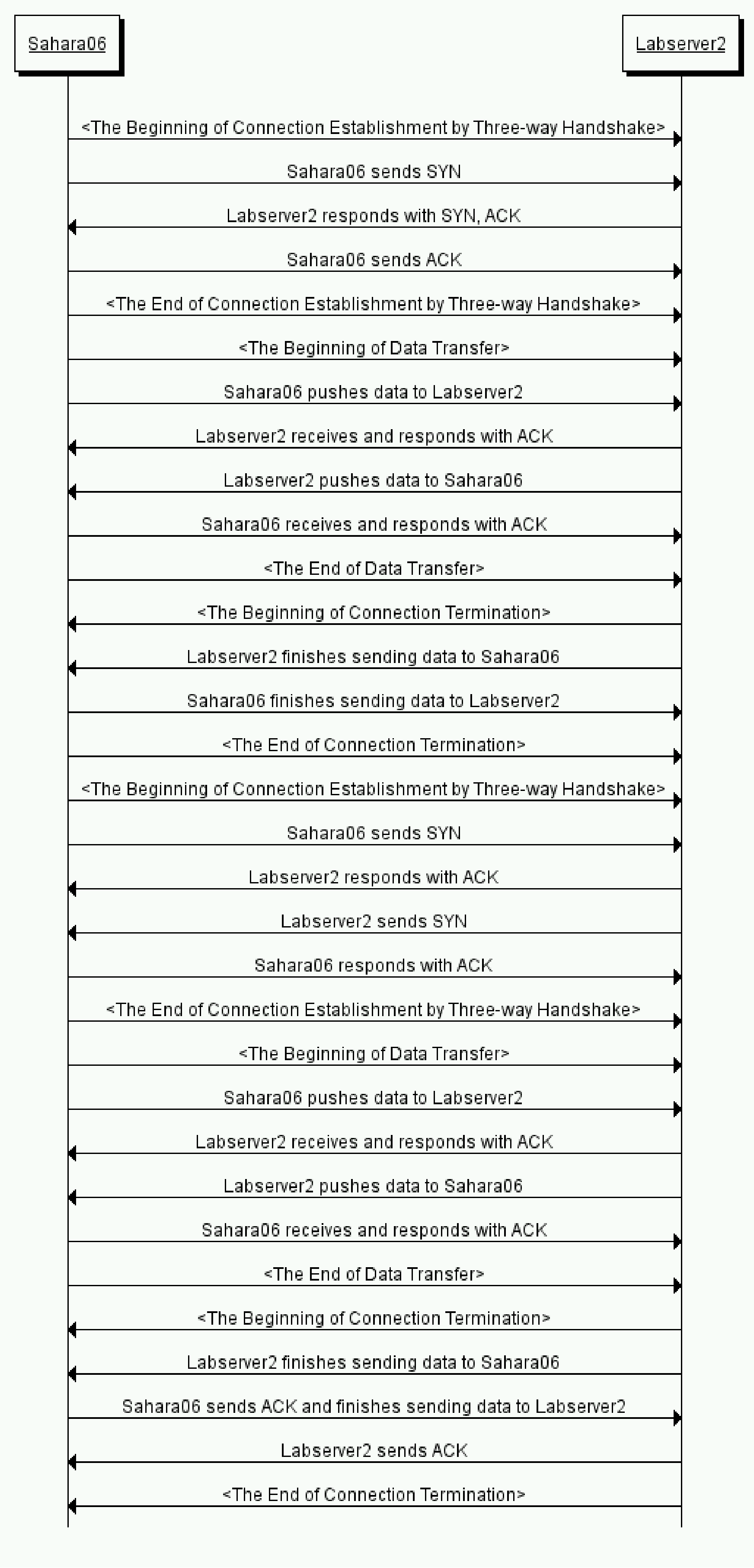
Part 2

The log file is as follows:

```
/*Connection Establishment 1*/
09:31:58.864452 IP sahara06.item.ntnu.no.51491 >
labserver2.item.ntnu.no.www: S 1379762317:1379762317(0) win 5840 <mss
1460,sackOK,timestamp 66013699 0,nop,wscale 5>
09:31:58.965176 IP labserver2.item.ntnu.no.www >
sahara06.item.ntnu.no.51491: S 3176691029:3176691029(0) ack
1379762318 win 5792 <mss 1460,sackOK,timestamp 6588901
66013699,nop,wscale 2>
09:31:58.965207 IP sahara06.item.ntnu.no.51491 >
labserver2.item.ntnu.no.www: . ack 1 win 183 <nop,nop,timestamp
66013724 6588901>

/*Data Transfer 1*/
09:31:58.965269 IP sahara06.item.ntnu.no.51491 >
labserver2.item.ntnu.no.www: P 1:432(431) ack 1 win 183
<nop,nop,timestamp 66013724 6588901>
09:31:59.066161 IP labserver2.item.ntnu.no.www >
sahara06.item.ntnu.no.51491: . ack 432 win 1716 <nop,nop,timestamp
6588911 66013724>
09:31:59.067017 IP labserver2.item.ntnu.no.www >
sahara06.item.ntnu.no.51491: P 1:400(399) ack 432 win 1716
<nop,nop,timestamp 6588911 66013724>
09:31:59.067028 IP sahara06.item.ntnu.no.51491 >
labserver2.item.ntnu.no.www: . ack 400 win 216 <nop,nop,timestamp
66013749 6588911>

/*Connection Termination 1*/
09:31:59.067041 IP labserver2.item.ntnu.no.www >
sahara06.item.ntnu.no.51491: F 400:400(0) ack 432 win 1716
<nop,nop,timestamp 6588911 66013724>
09:31:59.067224 IP sahara06.item.ntnu.no.51491 >
labserver2.item.ntnu.no.www: F 432:432(0) ack 401 win 216
<nop,nop,timestamp 66013749 6588911>

/*Connection Establishment 2*/
09:31:59.114941 IP sahara06.item.ntnu.no.51492 >
labserver2.item.ntnu.no.www: S 1384745561:1384745561(0) win 5840 <mss
1460,sackOK,timestamp 66013761 0,nop,wscale 5>
```

```
09:31:59.168038 IP labserver2.item.ntnu.no.www >
sahara06.item.ntnu.no.51491: . ack 433 win 1716 <nop,nop,timestamp
6588921 66013749>
09:31:59.215779 IP labserver2.item.ntnu.no.www >
sahara06.item.ntnu.no.51492: S 3181308070:3181308070(0) ack
1384745562 win 5792 <mss 1460,sackOK,timestamp 6588926
66013761,nop,wscale 2>
09:31:59.215811 IP sahara06.item.ntnu.no.51492 >
labserver2.item.ntnu.no.www: . ack 1 win 183 <nop,nop,timestamp
66013786 6588926>



/*Data Transfer 2*/
09:31:59.215889 IP sahara06.item.ntnu.no.51492 >
labserver2.item.ntnu.no.www: P 1:355(354) ack 1 win 183
<nop,nop,timestamp 66013786 6588926>
09:31:59.316768 IP labserver2.item.ntnu.no.www >
sahara06.item.ntnu.no.51492: . ack 355 win 1716 <nop,nop,timestamp
6588936 66013786>
09:31:59.317773 IP labserver2.item.ntnu.no.www >
sahara06.item.ntnu.no.51492: P 1:479(478) ack 355 win 1716
<nop,nop,timestamp 6588936 66013786>
09:31:59.317785 IP sahara06.item.ntnu.no.51492 >
labserver2.item.ntnu.no.www: . ack 479 win 216 <nop,nop,timestamp
66013812 6588936>

/*Connection Termination 2*/
09:31:59.317791 IP labserver2.item.ntnu.no.www >
sahara06.item.ntnu.no.51492: F 479:479(0) ack 355 win 1716
<nop,nop,timestamp 6588936 66013786>
09:31:59.317928 IP sahara06.item.ntnu.no.51492 >
labserver2.item.ntnu.no.www: F 355:355(0) ack 480 win 216
<nop,nop,timestamp 66013812 6588936>
09:31:59.418759 IP labserver2.item.ntnu.no.www >
sahara06.item.ntnu.no.51492: . ack 356 win 1716 <nop,nop,timestamp
6588946 66013812>
```

The interpretation of each message and MSD (message sequence diagram) is as follows: (Note that the words in the <> are not the interpretations but additional words for understanding of the log)



Sahara06
Labserver2
<The Beginning of Connection Establishment by Three-way Handshake>
Sahara06 sends SYN
Labserver2 responds with SYN, ACK
Sahara06 sends ACK
<The End of Connection Establishment by Three-way Handshake>
<The Beginning of Data Transfer>
Sahara06 pushes data to Labserver2
Labserver2 receives and responds with ACK
Labserver2 pushes data to Sahara06
Sahara06 receives and responds with ACK
<The End of Data Transfer>
<The Beginning of Connection Termination>
Labserver2 finishes sending data to Sahara06
Sahara06 finishes sending data to Labserver2
<The End of Connection Termination>
<The Beginning of Connection Establishment by Three-way Handshake>
Sahara06 sends SYN
Labserver2 responds with ACK
Labserver2 sends SYN
Sahara06 responds with ACK
<The End of Connection Establishment by Three-way Handshake>
<The Beginning of Data Transfer>
Sahara06 pushes data to Labserver2
Labserver2 receives and responds with ACK
Labserver2 pushes data to Sahara06
Sahara06 receives and responds with ACK
<The End of Data Transfer>
<The Beginning of Connection Termination>
Labserver2 finishes sending data to Sahara06
Sahara06 sends ACK and finishes sending data to Labserver2
Labserver2 sends ACK
<The End of Connection Termination>

The explanation that why Labserver2 behaves differently from web server in Samson is as follows:

Because Labserver2 uses http 1.0 and does not keep the connection open.

PART 3:

Slow Start:

The receiver starts with a window size = 183 and it's linearly incremented (+90/91) while it the acks are properly delivered.

The window stops increasing when the acks are received duplicated (see ACK 2897 and ACK 18825). This can be seen in Figure 1.

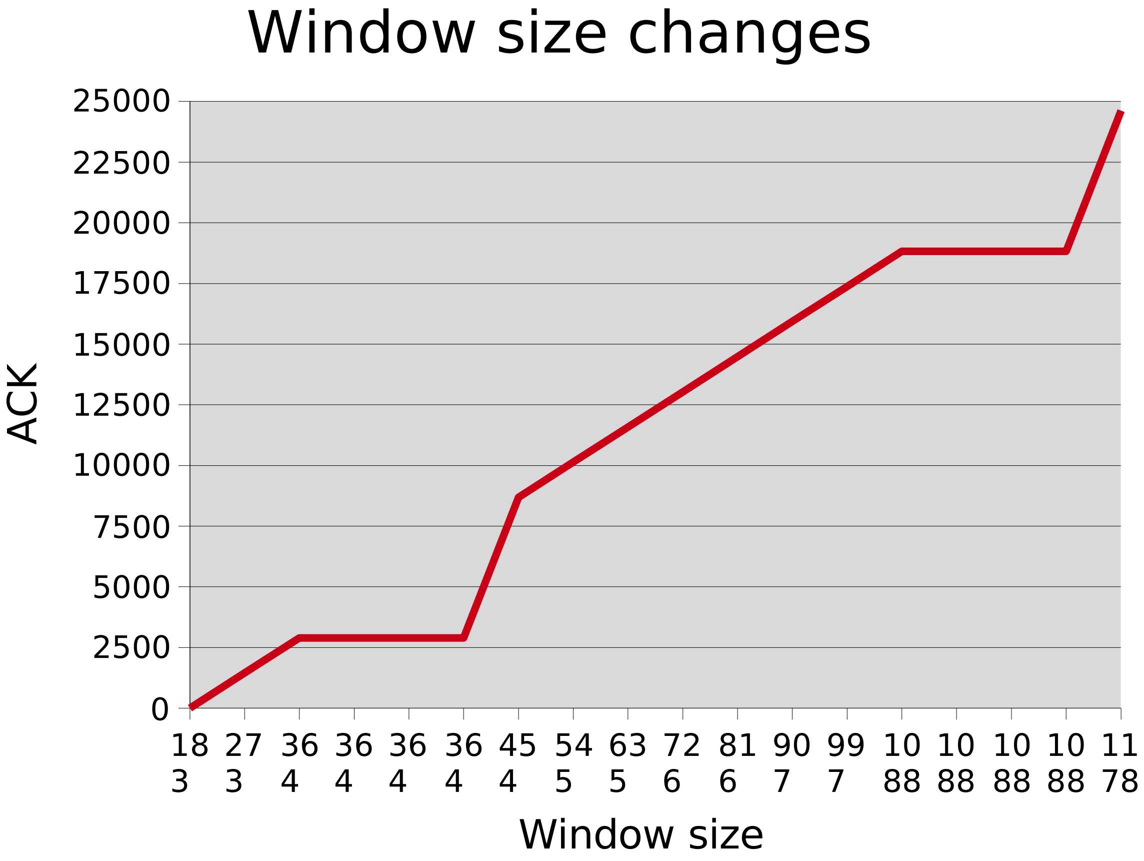


Figure 1: Window size changes

FAST RETRANSMIT:

Labserver2 receives three duplicate acknowledgements with the same acknowledge number (for instance ACK 2987 and ACK 18825), labserver2 can figure out that the segment was dropped. labserver2 then retransmit the packet that was supposed to be dropped before waiting for its timeout.

CONGESTION WINDOW:

If we look at the timestamp values, we can see different delays that can help us to calculate the congestion window. They can be seen in Figure 2.

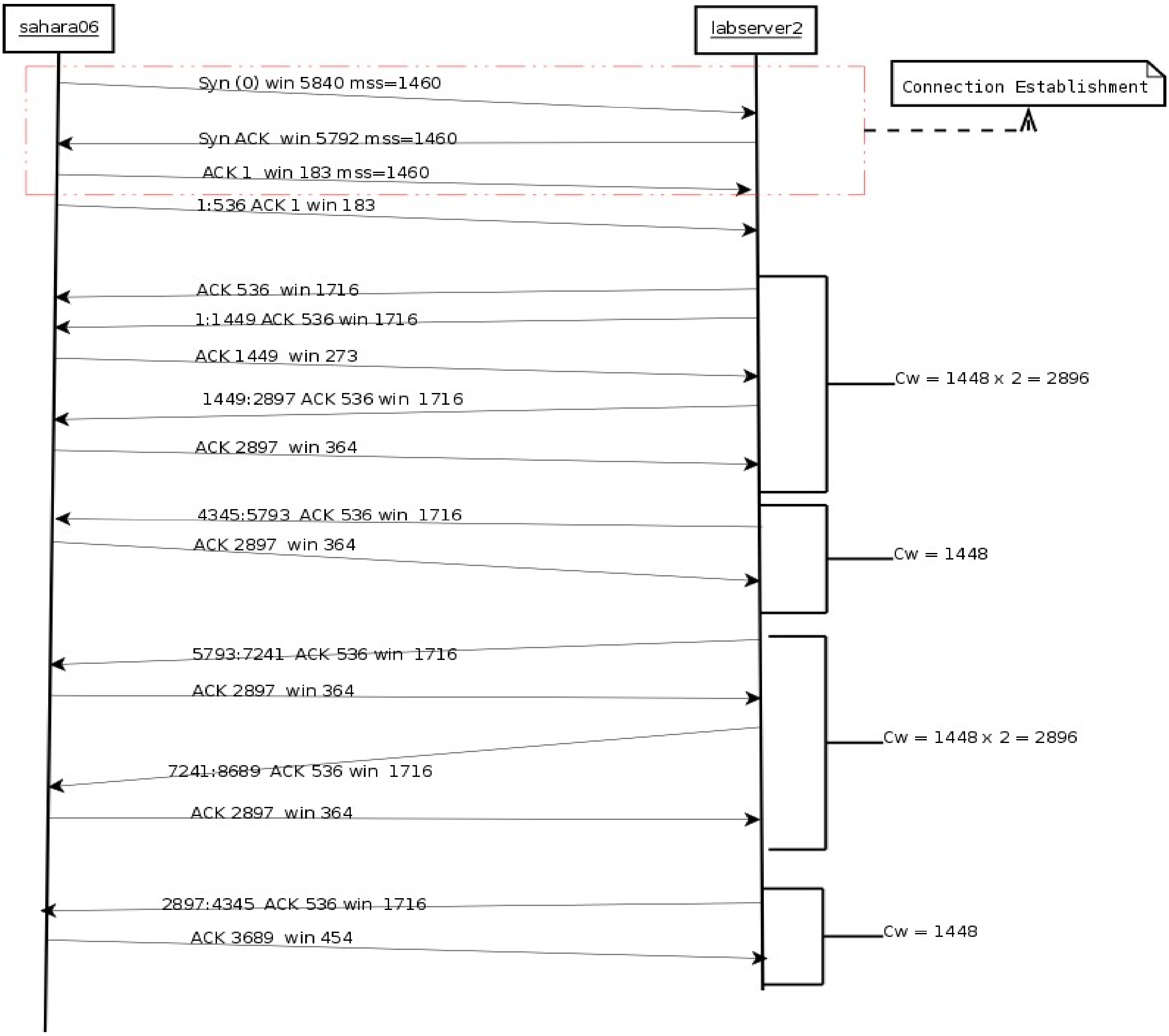

sahara06
labserver2
Connection Establishment
Syn (0) win 5840 mss=1460
Syn ACK win 5792 mss=1460
ACK 1 win 183 mss=1460
1:536 ACK 1 win 183
ACK 536 win 1716
1:1449 ACK 536 win 1716
ACK 1449 win 273
1449:2897 ACK 536 win 1716
ACK 2897 win 364
Cw = 1448 x 2 = 2896
4345:5793 ACK 536 win 1716
ACK 2897 win 364
Cw = 1448
5793:7241 ACK 536 win 1716
ACK 2897 win 364
7241:8689 ACK 536 win 1716
ACK 2897 win 364
Cw = 1448 x 2 = 2896
2897:4345 ACK 536 win 1716
ACK 3689 win 454
Cw = 1448

Figure 2: MSD

Part 4

A. Without Port Mirroring

What does this analyzer offer in addition to the TCPdump features?. Why do we need to pay for it?

It offers more features than TCPdump: nodes discovery, better statistics, graphical interface, etc.

So we should pay for it if we were looking for a more complex tool, but there may be some equivalent free software tools.

Why do we use a normal Ethernet cable, not a crossed one here?

It is usually necessary to use a crossed one when we connect two entities of the same kind (for instance two computers) to detect who is the sender and who is the receiver.

But in the case of these two switches, they have an internal auto-detect signal which allows to connect them with a normal cable.

Can you observe traffic initiated by both machines?. If so, justify your answer. If not, which machines own the observed traffic?.

No, we cannot see the traffic because we are connected trough a switch. A switch does not repeat the packet to all of its ports as a HUB does, rather it reads the destination address and send the package only to the suitable host.

The machine which owns the observed traffic is the machine which we are using to execute Network Analyzer.

How many computers are show here?. Does this result contradict the answer in the previous step?. Why?.

We can see more than 400 machines. This does not contradict the previous answer because we can see the broadcast traffic, and the tool use this kind of traffic to show the number of nodes. The switch does not send the specific packages if we are not that specific host, but the switch sends the broadcast traffic to all the ports.

B. With Port Mirroring

Observed the generated HTTP traffic. What is different now?.

Now we can see the HTTP traffic of the other nodes because the switch is mirroring the ports.

Discuss about the equipment, connectivity and applications sharing an internet connection.

It is very important to use security and encryption methods when we are working with sensible data. For instance, if we are going to make a connection with a bank and we are going to type our credit card number and code, we should be sure that the sever provides us any kind of security protocol as SSL.

This is critical because our packages can be captured. We are going to discuss on the basis of this critical example.

HUB vs SWITCH

In the case of the HUB our HTTP traffic could be captured by the people who are sharing our connection (and by everybody in the path), so if the website does not provide an encryption service, our code could be captured in the HTTP package. For instance if we write it through a form, and the data is send to the server in a POST request.

In the case of the SWITCH the people who are sharing our connection will not see the traffic which is not broadcast; but anyway a security method would be needed in this case because we do not know how is going the package to be transport and who can be capturing in the middle.

WIRED vs WIRELESS

As we can see a security method is needed when we are working with sensible data in any case. But is more critical when we are connected through a wireless network, because our traffic can be sniffed by somebody who is enough close to the access point. There are many tools for doing that like: Kismet, Airsnort, Network Stumbler, etc.

So in this case we should following some measures like: encrypt all our traffic with WPA or WEP, do not broadcast our SSID, enable MAC filtering (although this is not enough by itself, because the MAC address could be duplicated), etc.