Exam Pattern

	Student
Network Management	**First Name:...** **Last name:..**
Assignment of tasks: Prof. Dr.-Ing. Alexandru Soceanu / Dipl.-Inform(FH). Kurt Spörl	**Semester:...** **Student ID.:..**
Exam date **………………………..** **Duration: 90 Min.**	**Alowed materials:** **All**

Total Number of Points: 100

Section	Points/Grade
I	
II	
III	
IV	
Total Number of Points/	
Grade	

I. Management Information Base

Consider the Configuration in Appendix 1

The network Manager needs to find out a series of information:

1.1 (6 Pts.) Indicate the necessary OID to find out the ***"Next Hop Address"*** used by the ***Router R7*** to send messages to Subnet_B
Explain your answer!

1.2 (5 Pts.) Indicate how does the manager find out the ***time interval in hours*** since Router R7 was in operation since last start.

1.3 (7 Pts.) Please consider the ***Traffic Listings Nr.2***
Indicate how a manager can establish - using SNMUTIL-Tool - which is the state of the connection between the ***Client Station*** with the IP-Address ***192.168.1.2*** and the ***Station*** with the ***IP-Address= 192.168.2.2 from the client point of view*** ?

II. Management Network Configuration

Consider the Network Configuration in Appendix 1.

2.1. Calculate the following Subnet-Addresses and Subnet-Masks

2.1.1. (3 Pts.) Sub_D = --;

2.1.2. (3 Pts.) Sub_B = --;

2.1.3. (4 Pts.) Sub_E = --;

2.1.4. (4 Pts.) Sub_F = --;

2.1.5. (6 Pts.) Sub_M = --;

SM_M=---

(Sub_M does contain max. 7 Stations)

(Sub_M enthält max. 7 Stationen)

2.2. (3 Pts.) Please assign the following IP-Addresses:

$IP_{Interf1/R6}$= --;

IP_{0-R0} = ---

IP_{1-R5} = ---

2.3. (8 Pts.) The manager substitutes the ***Router R*5** with a ***Switch Layer 2***.
Explain what setting of the configuration does the manger has to do after the substitution of the Router R5 with a Switch Layer2?

2.4. (6 Pts.) Station ***PC22*** from ***Sub_G*** sends an ***FTP Data Massage*** to the FTP Server from ***Sub_E.*** The Analyzers A, B, and C monitor this message.
Which Information will show you these analyzers?

Analyzer	***Dest-MAC-Addr.***	***Source MAC-Addr.***	***Dest.- IP Addr.***	***Source- IP Addr.***	***TCP-Ports*** ***Dest/Source***
A					
B					
C					

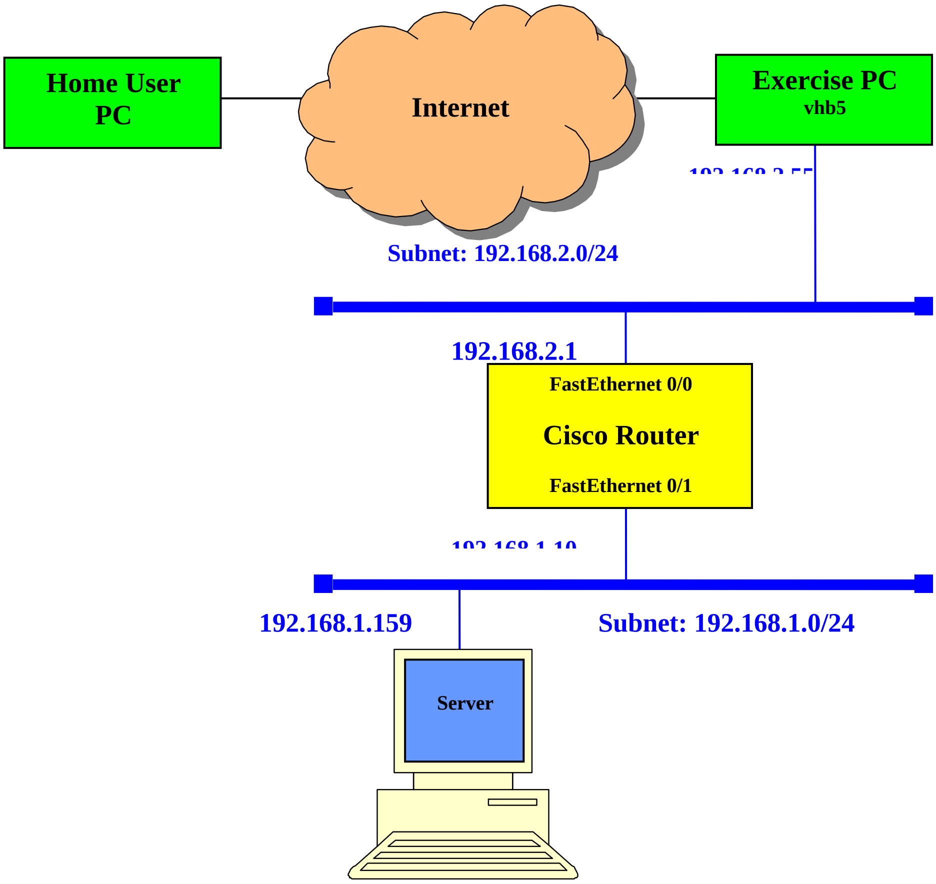
III. Routing

Please consider the configuration (see picture below) used during the exercise ***„Setup an Ethernet CISCO Router“***
Consider also the Routing Table set for the Exercise Host (see table below)

3.1. (5 Pts.) Identify the address of the Default Gateway. Justify your answer

3.2. (5 Pts.) Consider that the Exercise Host receives a message which has the destination: “**192.168.1.159**”
Indicate to which address will be forwarded this message?

3.3. (5 Pts.) Explain what happened if by mistake the Destination Network with address: “**194.95.109.48”** will be removed from the routing table?



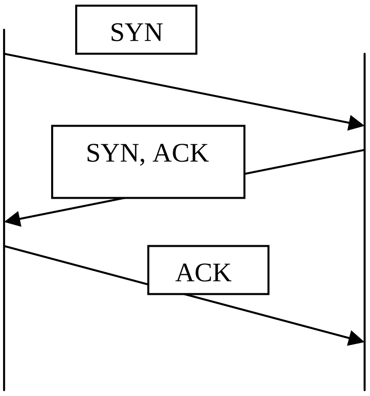
```
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 10 4b 63 c1 24 ...... 3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX)
- Packet Scheduler Miniport
0x3 ...00 0d 56 d2 9c b5 ...... Intel(R) PRO/1000 MT Network Connection - Packet
 Scheduler Miniport
0x4 ...00 10 4b 42 c8 da ...... 3Com 3C905TX-based Ethernet Adapter (Generic) #2
 - Packet Scheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    194.95.109.49   194.95.109.55     20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1      1
      192.168.1.0    255.255.255.0      192.168.2.1    192.168.2.55      1
      192.168.2.0    255.255.255.0     192.168.2.55    192.168.2.55     20
     192.168.2.55  255.255.255.255        127.0.0.1       127.0.0.1     20
    192.168.2.255  255.255.255.255     192.168.2.55    192.168.2.55     20
     192.168.10.0    255.255.255.0    192.168.10.55   192.168.10.55     20
    192.168.10.55  255.255.255.255        127.0.0.1       127.0.0.1     20
   192.168.10.255  255.255.255.255    192.168.10.55   192.168.10.55     20
    194.95.109.48  255.255.255.240    194.95.109.55   194.95.109.55     20
    194.95.109.55  255.255.255.255        127.0.0.1       127.0.0.1     20
   194.95.109.255  255.255.255.255    194.95.109.55   194.95.109.55     20
        224.0.0.0        240.0.0.0     192.168.2.55    192.168.2.55     20
        224.0.0.0        240.0.0.0    192.168.10.55   192.168.10.55     20
        224.0.0.0        240.0.0.0    194.95.109.55   194.95.109.55     20
  255.255.255.255  255.255.255.255     192.168.2.55    192.168.2.55      1
  255.255.255.255  255.255.255.255    192.168.10.55   192.168.10.55      1
  255.255.255.255  255.255.255.255    194.95.109.55   194.95.109.55      1
===========================================================================
```

IV. Network Security

4.1. (8 Pts.) Please consider ***Listing 1*** (see attachment) captured during a Network attack session.It is a sequence of frames necessary for a connection establishment at the level of TCP layer.
The station ***192.168.133.253*** used the Frames nr. 7, 9 and 163 to initiate a connection establishment with ***192.168.133.254***

Explain why the frames ***7, and 9*** are replied with ***RST, ACK*** flags set and the frame ***163*** is replied with ***SYN, ACK*** flags set ?

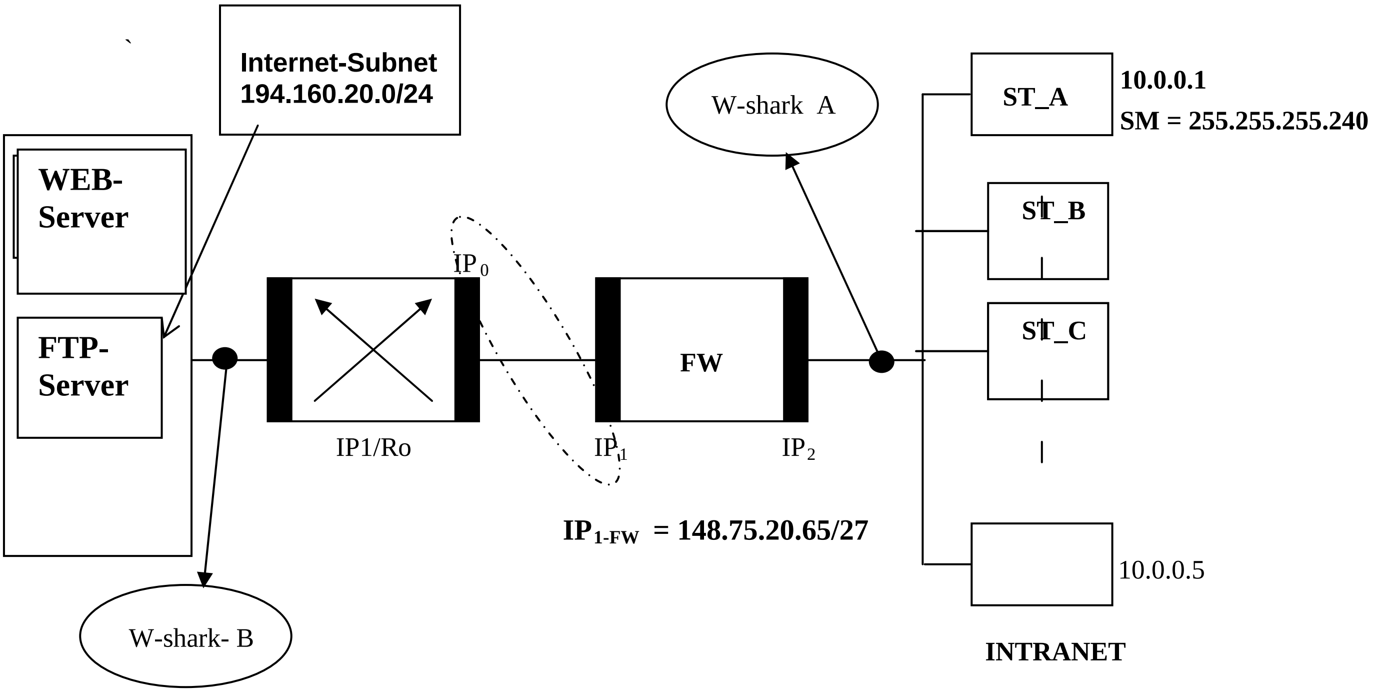
4.2. (8 Pts.) Please consider ***Listing Nr. 2*** (see attachment) captured during a Network attack session. It is again a sequence of frames necessary for a connection establishment at the level of TCP layer
A normal TCP connection establishment is a 3 way handshake process (see below):



Please explain why the station with the IP-Addr.= ***192.168.1.2*** which initiated the connection does respond with a msg. where the flag ***RST*** is set instead of answering with ***ACK*** flag set (see frame nr. 3)?

4.3 . ***Network Security with Firewall***

Consider the following FW configuration:



4.3.1. (4 Pts.) Please assign following IP-Addresses (s. figure above)

IP_2 – FW =>…………………………………

IP_0 – Ro =>……………………………………………

IP_1 – Ro =>……………………………………………

IP-WEB-Server =>..

IP-FTP-Server =>..

4.3.2. (10 Pts.) Consider following scenario:

- ST_A accesses via FW, Router and Internet the WEB server
- ST_B accesses at the same time with ST_A via FW, Router and Internet the FTP server
- A manager captures this frames with a Network Analyzer (Wireshark) at the location A and B of the above configuration.

Please fill out the following tables indicating the message headers captured by the analyzers : ***Wireshark_A*** and ***Wireshark_B***

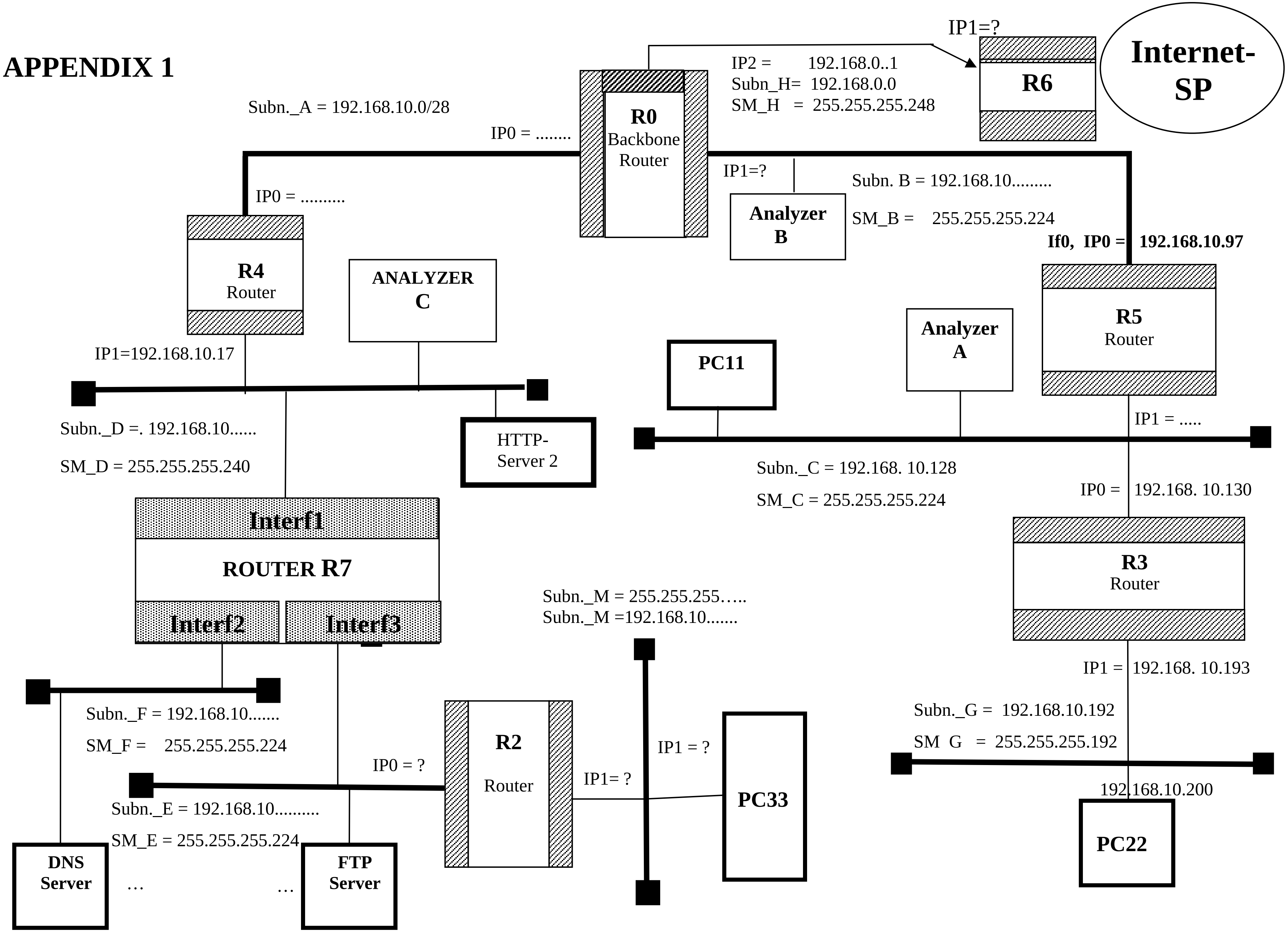
Wireshark A

Direction	**WS**	**Destination IP**	**Source IP**	**Dest.- Port**	**Source Port**
From ST_A	To WEB				
From ST_B	To FTP				
From WEB	To ST_A				

Wireshark B

Direction	**WS**	**Destination IP**	**Source IP**	**Dest.- Port**	**Source Port**
From ST_A	To WEB				
From ST_B	To FTP				
From WEB	To ST_A				
From FTP	To ST_B				

APPENDIX 1



IP1=?
Internet-SP
R6
IP2 = 192.168.0..1
Subn_H= 192.168.0.0
SM_H = 255.255.255.248
Subn._A = 192.168.10.0/28
IP0 = ...
R0
Backbone
Router
IP1=?
Analyzer
B
Subn. B = 192.168.10.........
SM_B = 255.255.255.224
If0, IP0 = 192.168.10.97
IP0 = ...
R4
Router
ANALYZER
C
IP1=192.168.10.17
R5
Router
Analyzer
A
PC11
HTTP-
Server 2
Subn._D =. 192.168.10......
SM_D = 255.255.255.240
IP1 = ...
Subn._C = 192.168. 10.128
SM_C = 255.255.255.224
IP0 = 192.168. 10.130
Interf1
ROUTER R7
Interf2
Interf3
R3
Router
Subn._M = 255.255.255…..
Subn._M =192.168.10.......
IP1 = 192.168. 10.193
Subn._G = 192.168.10.192
SM G = 255.255.255.192
Subn._F = 192.168.10.......
SM_F = 255.255.255.224
IP0 = ?
R2
Router
IP1 = ?
IP1= ?
PC33
192.168.10.200
PC22
Subn._E = 192.168.10..........
SM_E = 255.255.255.224
DNS
Server
…
…
FTP
Server

Listing 1: TCP Connection Establishment

```
…………………………………………………………………………………….
…………………………………………………………………………………..

No.     Time        Source              Destination         Protocol Info
6    0.007036    192.168.133.254      192.168.133.253     TCP  tcpmux > search-agent [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Transmission Control Protocol, Src Port: tcpmux (1), Dst Port: search-agent (1234), Seq: 1, Ack: 1, Len: 0

No.  Time         Source              Destination         Protocol Info
7   0.009065    192.168.133.253     192.168.133.254     TCP  search-agent > compressnet [SYN] Seq=0 Win=8192 Len=0

Transmission Control Protocol, Src Port: search-agent (1234), Dst Port: compressnet (2), Seq: 0, Len: 0

No.    Time        Source              Destination        Protocol Info
8   0.009186    192.168.133.254    192.168.133.253     TCP  compressnet > search-agent [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Transmission Control Protocol, Src Port: compressnet (2), Dst Port: search-agent (1234), Seq: 1, Ack: 1, Len: 0

No.    Time        Source              Destination        Protocol Info
9   0.011220    192.168.133.253    192.168.133.254     TCP  search-agent > compressnet [SYN] Seq=0 Win=8192 Len=0

Transmission Control Protocol, Src Port: search-agent (1234), Dst Port: compressnet (3), Seq: 0, Len: 0

No.    Time         Source             Destination         Protocol Info
10  0.011320    192.168.133.254    192.168.133.253     TCP  compressnet > search-agent [RST, ACK] Seq=1 Ack=1 Win=0
Len=0

Transmission Control Protocol, Src Port: compressnet (3), Dst Port: search-agent (1234), Seq: 1, Ack: 1, Len: 0
…………………………………………………………………………………….
…………………………………………………………………………………..
…………………………………………………………………………………….


No.     Time        Source             Destination         Protocol Info
163   0.174751    192.168.133.253    192.168.133.254     TCP  search-agent > http [SYN] Seq=4294967295 Win=8192 Len=0

Transmission Control Protocol, Src Port: search-agent (1234), Dst Port: http (80), Seq: 4294967295, Len: 0
```

```
No.     Time        Source                Destination           Protocol Info
164   0.174875   192.168.133.254      192.168.133.253      TCP  http > search-agent [SYN, ACK] Seq=0 Ack=0 Win=5840 Len=0
MSS=1460

Transmission Control Protocol, Src Port: http (80), Dst Port: search-agent (1234), Seq: 0, Ack: 0, Len: 0
```

Listing 2/1: SYN/SYN, ACK/RST

```
No.   Time       Source          Destination      Protocol Info_______________
1    0.000000    192.168.1.2     192.168.2.2      TCP  ftp-data > http [SYN] Seq=4294967295 Win=8192 Len=0

Frame 1 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: CadmusCo_82:92:27 (08:00:27:82:92:27), Dst: CadmusCo_9b:f3:9d (08:00:27:9b:f3:9d)
Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.2.2 (192.168.2.2)
Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: http (80), Seq: 4294967295, Len: 0
    Source port: ftp-data (20)
    Destination port: http (80)
    Sequence number: 4294967295    (relative sequence number)
    Header length: 20 bytes
    Flags: 0x02 (SYN)
        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
    Window size: 8192
    Checksum: 0x0b2a [correct]
    [SEQ/ACK analysis]
```

```
No.  Time       Source          Destination      Protocol Info__________________
2    0.000713   192.168.2.2     192.168.1.2      TCP  http > ftp-data [SYN, ACK] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460

Frame 2 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: CadmusCo_9b:f3:9d (08:00:27:9b:f3:9d), Dst: CadmusCo_82:92:27 (08:00:27:82:92:27)
Internet Protocol, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.1.2 (192.168.1.2)
Transmission Control Protocol, Src Port: http (80), Dst Port: ftp-data (20), Seq: 0, Ack: 0, Len: 0
    Source port: http (80)
    Destination port: ftp-data (20)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 0    (relative ack number)
    Header length: 24 bytes
    Flags: 0x12 (SYN, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 0... = Push: Not set
    .... .0.. = Reset: Not set
    .... ..1. = Syn: Set
    .... ...0 = Fin: Not set
Window size: 5840
Checksum: 0x95a7 [correct]
Options: (4 bytes)
[SEQ/ACK analysis]
```

Listing 2/2:   SYN/SYN, ACK/RST

```
No.  Time        Source           Destination      Protocol Info_____________
3    0.001024    192.168.1.2      192.168.2.2      TCP  ftp-data > http [RST] Seq=0 Win=0 Len=0

Frame 3 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: CadmusCo_82:92:27 (08:00:27:82:92:27), Dst: CadmusCo_9b:f3:9d (08:00:27:9b:f3:9d)
Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.2.2 (192.168.2.2)
Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: http (80), Seq: 0, Len: 0
    Source port: ftp-data (20)
    Destination port: http (80)
    Sequence number: 0    (relative sequence number)
    Header length: 20 bytes
    Flags: 0x04 (RST)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...0 .... = Acknowledgment: Not set
        .... 0... = Push: Not set
        .... .1.. = Reset: Set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 0
    Checksum: 0x2b27 [correct]
```