

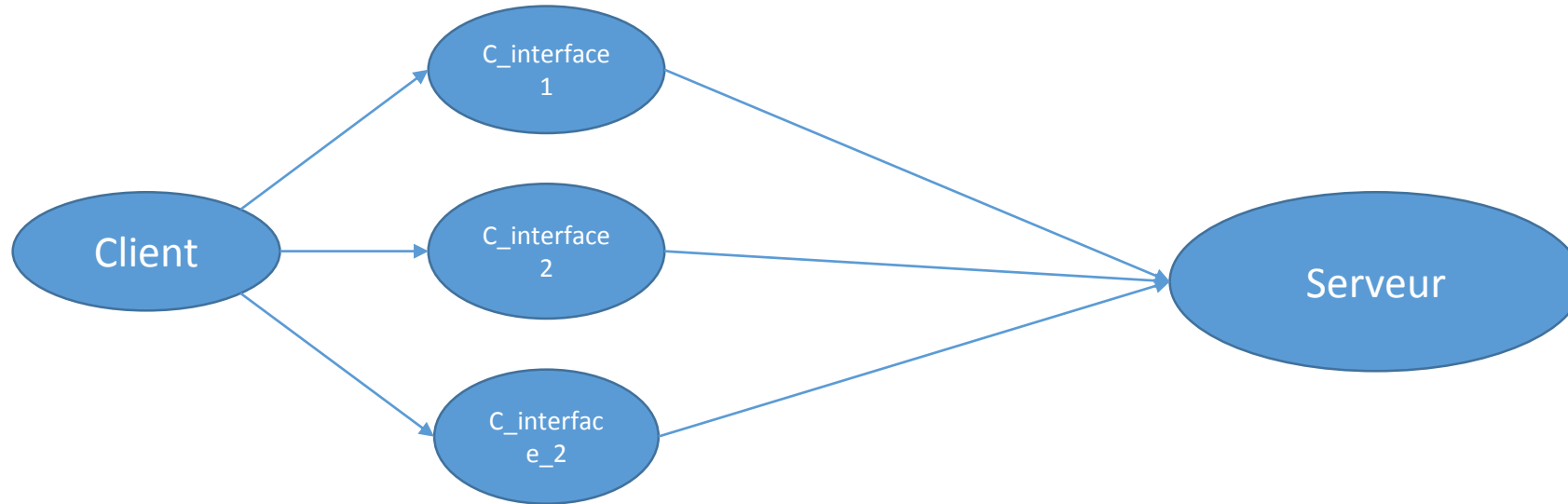
nc: *MPTCP mode on*

Charles-Henry Bertrand

Sylvain Dassier

Le concept

Se connecter via différentes interfaces à une interface d'un serveur



Premier Syn

client_20161113_123427.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)] (on mininet-vm)

Filter: ip.addr == 10.0.0.2

No.	Time	Source	Destination	Protocol	Length	Info
984	69.656569	10.0.0.1	10.0.0.2	TCP	88	56162 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3103652 TSecr=0 WS=512
985	69.675731	10.0.0.2	10.0.0.1	TCP	88	64000 > 56162 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3103655 TSecr=3103652 WS=512
986	69.675903	10.0.0.1	10.0.0.2	TCP	96	56162 > 64000 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=3103657 TSecr=3103655
987	69.675918	10.0.0.1	10.0.0.2	TCP	84	[TCP Dup ACK 986#1] 56162 > 64000 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=3103657 TSecr=3103655
988	69.675924	10.0.0.1	10.0.0.2	TCP	84	[TCP Dup ACK 986#2] 56162 > 64000 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=3103657 TSecr=3103655
1003	69.695442	10.0.0.2	10.0.0.1	TCP	84	[TCP Window Update] 64000 > 56162 [ACK] Seq=1 Ack=1 Win=28672 Len=0 TSval=3103661 TSecr=3103657
1004	69.695474	10.0.0.2	10.0.0.1	TCP	84	[TCP Dup ACK 1003#1] 64000 > 56162 [ACK] Seq=1 Ack=1 Win=28672 Len=0 TSval=3103661 TSecr=3103657
1065	79.712114	10.0.0.1	10.0.0.2	TCP	99	56162 > 64000 [PSH, ACK] Seq=1 Ack=1 Win=58880 Len=11 TSval=3106166 TSecr=3103661
1067	79.722967	10.0.0.2	10.0.0.1	TCP	76	64000 > 56162 [ACK] Seq=1 Ack=12 Win=57344 Len=0 TSval=3106168 TSecr=3106166
1079	79.740096	10.2.0.1	10.0.0.2	TCP	88	44917 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3106169 TSecr=0 WS=512
1085	79.740368	10.1.0.1	10.0.0.2	TCP	88	40313 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3106169 TSecr=0 WS=512
1095	79.756019	10.0.0.2	10.2.0.1	TCP	92	64000 > 44917 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106175 TSecr=3106169 WS=512
1098	79.756086	10.0.0.2	10.1.0.1	TCP	92	64000 > 40313 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106175 TSecr=3106169 WS=512
1136	80.721650	10.1.0.1	10.0.0.2	TCP	88	[TCP Retransmission] 40313 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3106419 TSecr=0 WS=512
1137	80.721684	10.2.0.1	10.0.0.2	TCP	88	[TCP Retransmission] 44917 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3106419 TSecr=0 WS=512
1144	80.734245	10.0.0.2	10.2.0.1	TCP	92	[TCP Retransmission] 64000 > 44917 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106420 TSecr=3106169 WS=512
1147	80.734273	10.0.0.2	10.1.0.1	TCP	92	[TCP Retransmission] 64000 > 40313 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106420 TSecr=3106169 WS=512
1156	81.370005	10.0.0.2	10.0.0.1	TCP	92	[TCP Retransmission] 64000 > 44917 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106670 TSecr=3106169 WS=512

Window size value: 29200
[Calculated window size: 29200]
Checksum: 0x143d [validation disabled]
Options: (32 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale, Multipath TCP
Maximum segment size: 1460 bytes
TCP SACK Permitted Option: True
Timestamps: TSval 3103652, TSecr 0
No-Operation (NOP)
Window scale: 9 (multiply by 512)
Multipath TCP: Multipath Capable
Kind: Multipath TCP (30)
Length: 12
0000 = Multipath TCP subtype: Multipath Capable (0)
.... 0000 = Multipath TCP version: 0
Multipath TCP flags: 0x81
1... = Checksum required: 1
.... 1 = Use HMAC-SHA1: 1
Multipath TCP Sender's Key: 7076236588249283789

0000 00 04 00 01 00 06 2a db c0 40 98 3e 4a 00 08 00*. .@.>...
0010 45 00 00 48 a6 a8 40 00 40 06 80 05 0a 00 00 01 E..H..@. @.....
0020 0a 00 00 02 db 62 fa 00 c2 23 fd 0c 00 00 00 00b..#.....

Second Syn

The image shows a Wireshark capture of network traffic. The filter is set to `ip.addr == 10.0.0.2`. The packet list shows a sequence of events: a successful SYN-ACK (No. 1067), followed by a SYN packet (No. 1079), and then a series of retransmissions (Nos. 1085, 1095, 1098, 1136, 1137, 1144, 1147, 1166, 1167, 1207, 1208, 1213, 1215). The retransmissions are marked as such in red text. The final packet in the list (No. 1226) is a RST, ACK, indicating a connection reset. The details pane for the selected packet (No. 1226) shows the following information:

- Window size value: 29200
[Calculated window size: 29200]
- Checksum: 0x143f [validation disabled]
- Options: (32 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale, Multipath TCP
 - Maximum segment size: 1460 bytes
 - TCP SACK Permitted Option: True
 - Timestamps: TSval 3106169, TSecr 0
 - No-Operation (NOP)
 - Window scale: 9 (multiply by 512)
 - Multipath TCP: Join Connection
 - Kind: Multipath TCP (30)
 - Length: 12
 - 0001 ... = Multipath TCP subtype: Join Connection (1)
 - Multipath TCP flags: 0x00
 -0 = Backup flag: 0
 - Multipath TCP Address ID: 4
 - Multipath TCP Receiver's Token: 3032705926
 - Multipath TCP Sender's Random Number: 4008407740

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```
0000 00 04 00 01 00 06 36 0c f9 0b 7b fa 00 00 08 00 .....6. ...{.....
0010 45 00 00 48 61 ca 40 00 40 06 c4 e1 0a 02 00 01 E..Ha.@. @.....
0020 0a 00 00 02 af 75 fa 00 9e 7b 04 b3 00 00 00 00 .....U. ...{.....
```

Troisième SYN

client_20161113_123427.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)] (on mininet-vm)

Filter: ip.addr == 10.0.0.2

No.	Time	Source	Destination	Protocol	Length	Info
1067	79.722967	10.0.0.2	10.0.0.1	TCP	76	64000 > 56162 [ACK] Seq=1 Ack=12 Win=57344 Len=0 TSval=3106168 TSecr=3106166
1079	79.748096	10.2.0.1	10.0.0.2	TCP	88	44917 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3106169 TSecr=0 WS=512
1085	79.748368	10.1.0.1	10.0.0.2	TCP	88	40313 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3106169 TSecr=0 WS=512
1095	79.756019	10.0.0.2	10.2.0.1	TCP	92	64000 > 44917 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106175 TSecr=3106169 WS=512
1098	79.756086	10.0.0.2	10.1.0.1	TCP	92	64000 > 40313 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106175 TSecr=3106169 WS=512
1136	80.721650	10.1.0.1	10.0.0.2	TCP	88	[TCP Retransmission] 40313 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3106419 TSecr=0 WS=512
1137	80.721684	10.2.0.1	10.0.0.2	TCP	88	[TCP Retransmission] 44917 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3106419 TSecr=0 WS=512
1144	80.734245	10.0.0.2	10.2.0.1	TCP	92	[TCP Retransmission] 64000 > 44917 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106420 TSecr=3106169 WS=512
1147	80.734273	10.0.0.2	10.1.0.1	TCP	92	[TCP Retransmission] 64000 > 40313 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106420 TSecr=3106169 WS=512
1166	81.730995	10.0.0.2	10.2.0.1	TCP	92	[TCP Retransmission] 64000 > 44917 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106670 TSecr=3106169 WS=512
1167	81.731000	10.0.0.2	10.1.0.1	TCP	92	[TCP Retransmission] 64000 > 40313 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106670 TSecr=3106169 WS=512
1207	82.725688	10.1.0.1	10.0.0.2	TCP	88	[TCP Retransmission] 40313 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3106920 TSecr=0 WS=512
1208	82.725722	10.2.0.1	10.0.0.2	TCP	88	[TCP Retransmission] 44917 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3106920 TSecr=0 WS=512
1213	82.736747	10.0.0.2	10.1.0.1	TCP	92	[TCP Retransmission] 64000 > 40313 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106921 TSecr=3106169 WS=512
1215	82.736758	10.0.0.2	10.2.0.1	TCP	92	[TCP Retransmission] 64000 > 44917 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1460 SACK_PERM=1 TSval=3106921 TSecr=3106169 WS=512
1226	83.827279	10.0.0.1	10.0.0.2	TCP	76	56162 > 64000 [RST, ACK] Seq=12 Ack=1 Win=88064 Len=0 TSval=3107195 TSecr=3106168
1238	83.837513	10.0.0.2	10.0.0.1	TCP	76	64000 > 56162 [RST, ACK] Seq=1 Ack=12 Win=86016 Len=0 TSval=3107196 TSecr=3106166
2147	2899.550430	10.0.0.1	10.0.0.2	TCP	88	56169 > 64000 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3811126 TSecr=0 WS=512

Window size value: 29200
[Calculated window size: 29200]
Checksum: 0x143e [validation disabled]
Options: (32 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale, Multipath TCP
Maximum segment size: 1460 bytes
TCP SACK Permitted Option: True
Timestamps: TSval 3106169, TSecr 0
No-Operation (NOP)
Window scale: 9 (multiply by 512)
Multipath TCP: Join Connection
Kind: Multipath TCP (30)
Length: 12
0001 = Multipath TCP subtype: Join Connection (1)
Multipath TCP flags: 0x00
.... .. = Backup flag: 0
Multipath TCP Address ID: 3
Multipath TCP Receiver's Token: 3032705926
Multipath TCP Sender's Random Number: 3309273748

```
0000 00 04 00 01 00 06 2e ae 38 f3 ad fc 00 00 08 00 ..... 8.....
0010 45 00 00 48 6c 1f 40 00 40 06 ba 8d 0a 01 00 01 E..H.L.@.....
0020 0a 00 00 02 9d 79 fa 00 c5 98 09 66 00 00 00 00 .....y...f....
0030 d0 03 73 10 14 7c 00 00 03 04 05 b4 04 03 08 0c ...
```