Master Thesis - Security Aspects in Virtual Networks
SITREP 10

Laurent De Wilde
Master of Science in the Applied Computer Science
Vrije Universiteit Brussel

March 16, 2015

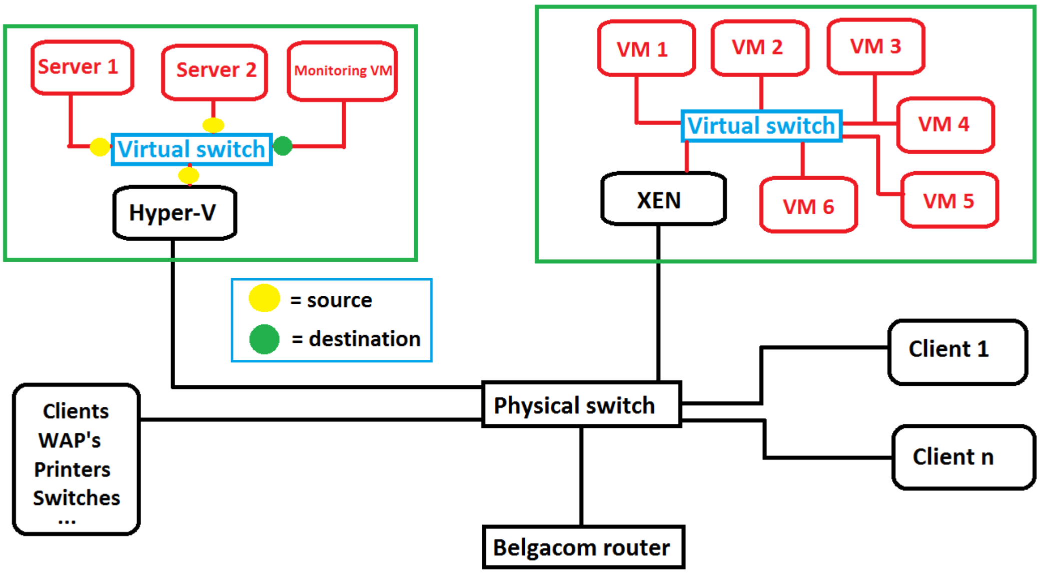
Work done

This is an overview of the work performed in the past week:

- Theoretical study is finished.
- Made an appointment with Prof to discuss the practical testing.
- Transported the pizzaserver from the VUB datacenter to my home by car.
- Integrated the server into the existing infrastructure.
- I installed the Hyper-V role on WS2012 R2, using two NIC's: one for the virtual switch and one for monitoring / remote desktop connection. Obviously, I make use of the so-called "external network" of Hyper-V.

  The reason I installed Hyper-V (besides XEN) is that, in contrast to XEN, I do not have much experience with Hyper-V and I would like to gain more experiece with it.

The figure below visualizes my current network setup.



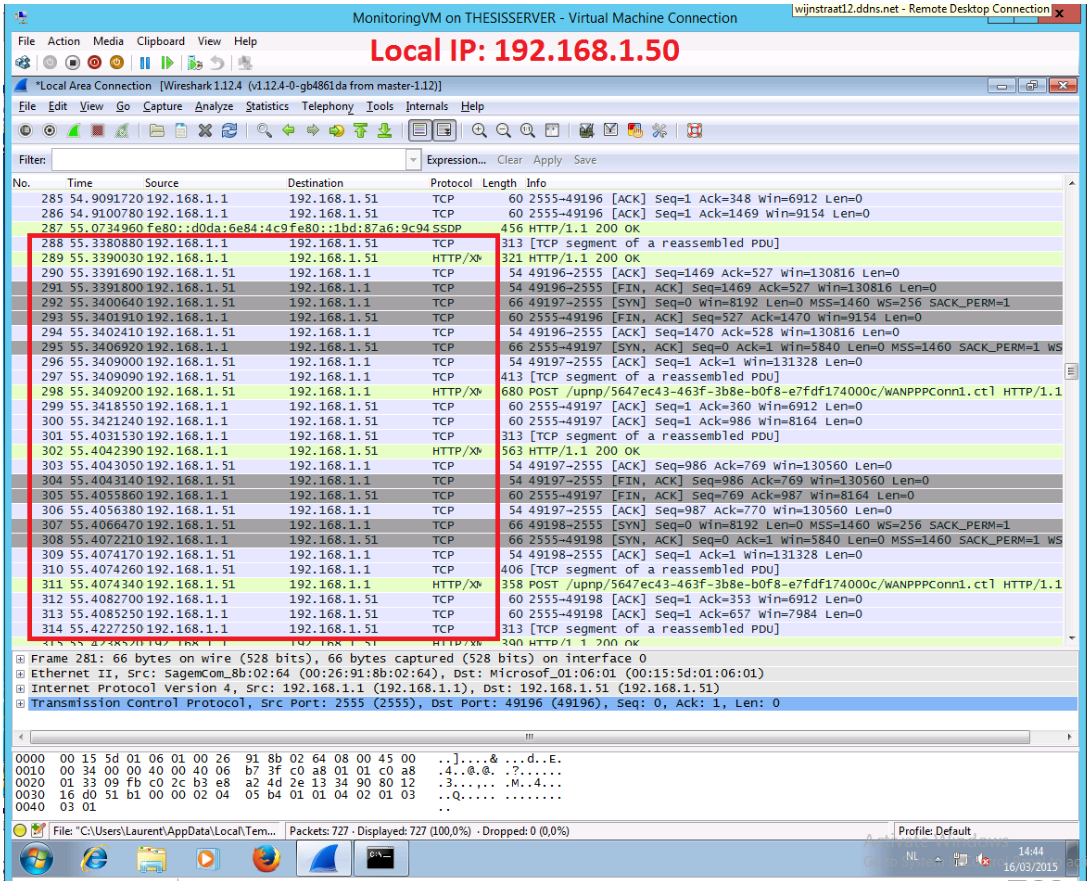
- After the hardware setup was completed, I started configuring Hyper-V: I have setup three VM's and each VM has its own vNIC and is connected to the virtual switch. One of those VM's is used to capture all traffic that passes on all the ports of the switch, hence the name "monitoring VM".

  As the Prof stated he was very pleased with the dynamic memory feature of Hyper-V, all VM's use dynamic memory.

  I was asked if a vNIC is able to capture traffic on the network to later reconstruct the protocols. After some research, it turns out one can use port mirroring for this purpose. So I configured the vPorts of Server 1 and Server 2 on the vSwitch to act as a source. Meaning they make a copy of the traffic to and from those ports and send it to the destination. This destination is Monitoring VM.

  After that, I tested the setup. I installed Wireshark on the "Monitoring VM" and pinged from "Server 1" to "Server 2" and watched how Wireshark captured all the ICMP Ping requests and replies - not destinated to the "Monitoring VM". So, **yes**, the vNIC on the "Monitoring VM" captured traffic between VM's (inter - VM) on the same physical host and thus act as a sniffer.

Below are some screenshots. One can observe that broadcast messages not originating from the Hyper-V VM's are captured as well as some traffic from a XEN VM (the primary DNS server of my domain to be precise).



MonitoringVM on THESISSERVER - Virtual Machine Connection
wijnstraat12.ddns.net - Remote Desktop Connection
File Action Media Clipboard View Help
*Local Area Connection [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default
NL
14:44
16/03/2015

Local IP: 192.168.1.50

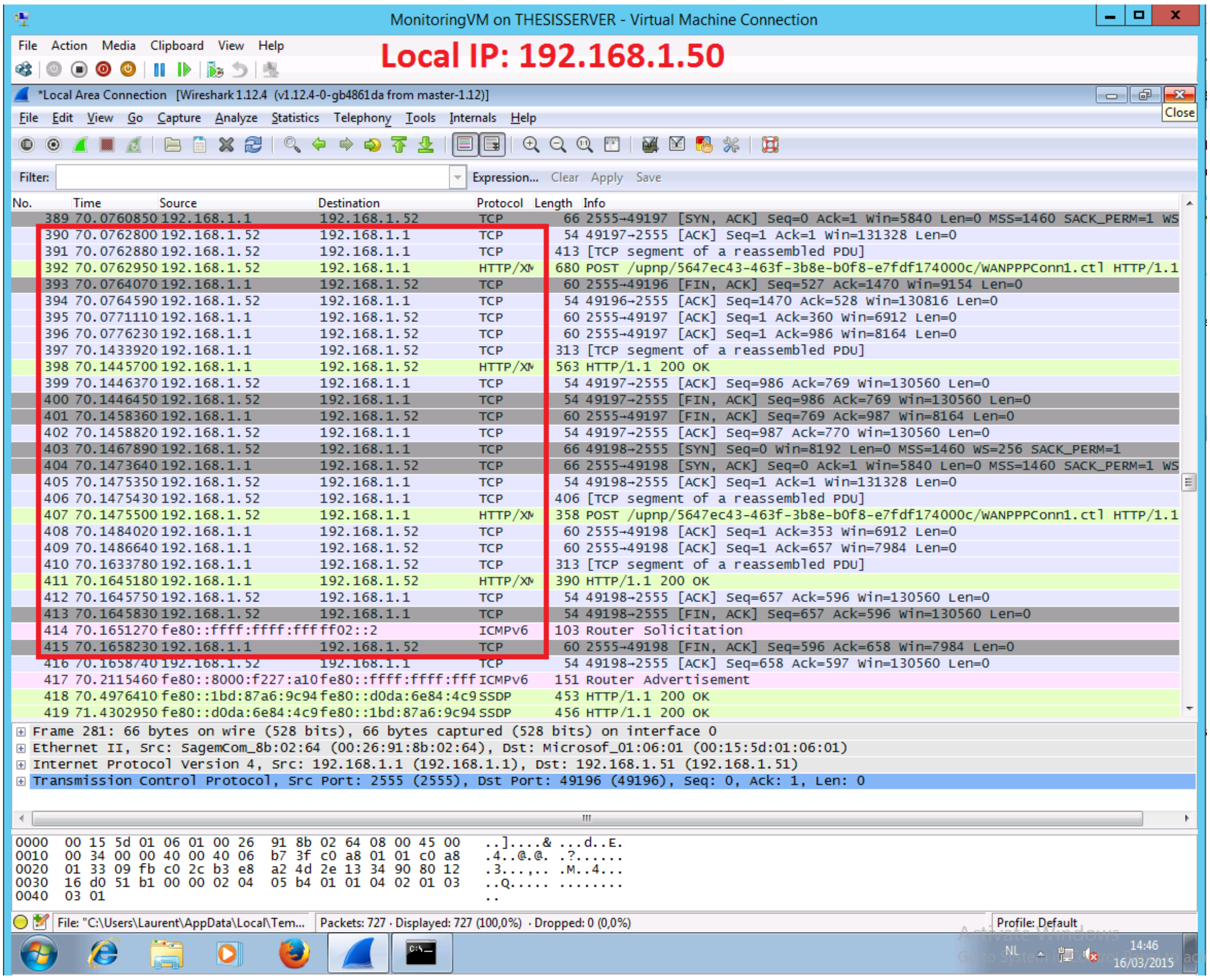
```
No.     Time       Source                  Destination             Protocol Length Info
    285 54.9091720 192.168.1.1             192.168.1.51            TCP        60 2555→49196 [ACK] Seq=1 Ack=348 Win=6912 Len=0
    286 54.9100780 192.168.1.1             192.168.1.51            TCP        60 2555→49196 [ACK] Seq=1 Ack=1469 Win=9154 Len=0
    287 55.0734960 fe80::d0da:6e84:4c9fe80::1bd:87a6:9c94 SSDP     456 HTTP/1.1 200 OK
    288 55.3380880 192.168.1.1             192.168.1.51            TCP       313 [TCP segment of a reassembled PDU]
    289 55.3390030 192.168.1.1             192.168.1.51            HTTP/XM   321 HTTP/1.1 200 OK
    290 55.3391690 192.168.1.51            192.168.1.1             TCP        54 49196→2555 [ACK] Seq=1469 Ack=527 Win=130816 Len=0
    291 55.3391800 192.168.1.51            192.168.1.1             TCP        54 49196→2555 [FIN, ACK] Seq=1469 Ack=527 Win=130816 Len=0
    292 55.3400640 192.168.1.51            192.168.1.1             TCP        66 49197→2555 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    293 55.3401910 192.168.1.1             192.168.1.51            TCP        60 2555→49196 [FIN, ACK] Seq=527 Ack=1470 Win=9154 Len=0
    294 55.3402410 192.168.1.51            192.168.1.1             TCP        54 49196→2555 [ACK] Seq=1470 Ack=528 Win=130816 Len=0
    295 55.3406920 192.168.1.1             192.168.1.51            TCP        66 2555→49197 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS
    296 55.3409000 192.168.1.51            192.168.1.1             TCP        54 49197→2555 [ACK] Seq=1 Ack=1 Win=131328 Len=0
    297 55.3409090 192.168.1.51            192.168.1.1             TCP       413 [TCP segment of a reassembled PDU]
    298 55.3409200 192.168.1.51            192.168.1.1             HTTP/XM   680 POST /upnp/5647ec43-463f-3b8e-b0f8-e7fdf174000c/WANPPPConn1.ctl HTTP/1.1
    299 55.3418550 192.168.1.1             192.168.1.51            TCP        60 2555→49197 [ACK] Seq=1 Ack=360 Win=6912 Len=0
    300 55.3421240 192.168.1.1             192.168.1.51            TCP        60 2555→49197 [ACK] Seq=1 Ack=986 Win=8164 Len=0
    301 55.4031530 192.168.1.1             192.168.1.51            TCP       313 [TCP segment of a reassembled PDU]
    302 55.4042390 192.168.1.1             192.168.1.51            HTTP/XM   563 HTTP/1.1 200 OK
    303 55.4043050 192.168.1.51            192.168.1.1             TCP        54 49197→2555 [ACK] Seq=986 Ack=769 Win=130560 Len=0
    304 55.4043140 192.168.1.51            192.168.1.1             TCP        54 49197→2555 [FIN, ACK] Seq=986 Ack=769 Win=130560 Len=0
    305 55.4055860 192.168.1.1             192.168.1.51            TCP        60 2555→49197 [FIN, ACK] Seq=769 Ack=987 Win=8164 Len=0
    306 55.4056380 192.168.1.51            192.168.1.1             TCP        54 49197→2555 [ACK] Seq=987 Ack=770 Win=130560 Len=0
    307 55.4066470 192.168.1.51            192.168.1.1             TCP        66 49198→2555 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    308 55.4072210 192.168.1.1             192.168.1.51            TCP        66 2555→49198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS
    309 55.4074170 192.168.1.51            192.168.1.1             TCP        54 49198→2555 [ACK] Seq=1 Ack=1 Win=131328 Len=0
    310 55.4074260 192.168.1.51            192.168.1.1             TCP       406 [TCP segment of a reassembled PDU]
    311 55.4074340 192.168.1.51            192.168.1.1             HTTP/XM   358 POST /upnp/5647ec43-463f-3b8e-b0f8-e7fdf174000c/WANPPPConn1.ctl HTTP/1.1
    312 55.4082700 192.168.1.1             192.168.1.51            TCP        60 2555→49198 [ACK] Seq=1 Ack=353 Win=6912 Len=0
    313 55.4085250 192.168.1.1             192.168.1.51            TCP        60 2555→49198 [ACK] Seq=1 Ack=657 Win=7984 Len=0
    314 55.4227250 192.168.1.1             192.168.1.51            TCP       313 [TCP segment of a reassembled PDU]
    315 55.4238520 192.168.1.1             192.168.1.51            HTTP/XM   390 HTTP/1.1 200 OK
```

```
⊞ Frame 281: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: SagemCom_8b:02:64 (00:26:91:8b:02:64), Dst: Microsof_01:06:01 (00:15:5d:01:06:01)
⊞ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.51 (192.168.1.51)
⊞ Transmission Control Protocol, Src Port: 2555 (2555), Dst Port: 49196 (49196), Seq: 0, Ack: 1, Len: 0
```

```
0000  00 15 5d 01 06 01 00 26  91 8b 02 64 08 00 45 00   ..]....& ...d..E.
0010  00 34 00 00 40 00 40 06  b7 3f c0 a8 01 01 c0 a8   .4..@.@. .?......
0020  01 33 09 fb c0 2c b3 e8  a2 4d 2e 13 34 90 80 12   .3...,.. .M..4...
0030  16 d0 51 b1 00 00 02 04  05 b4 01 01 04 02 01 03   ..Q..... ........
0040  03 01                                              ..
```

File: "C:\Users\Laurent\AppData\Local\Tem... Packets: 727 · Displayed: 727 (100,0%) · Dropped: 0 (0,0%)

Figure 1: Traffic between Server 1 (192.168.1.51) and the Belgacom router captured by the vNIC.


MonitoringVM on THESISSERVER - Virtual Machine Connection
File Action Media Clipboard View Help
*Local Area Connection [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Close
Filter:
Expression... Clear Apply Save
Profile: Default
NL
14:46
16/03/2015

Local IP: 192.168.1.50

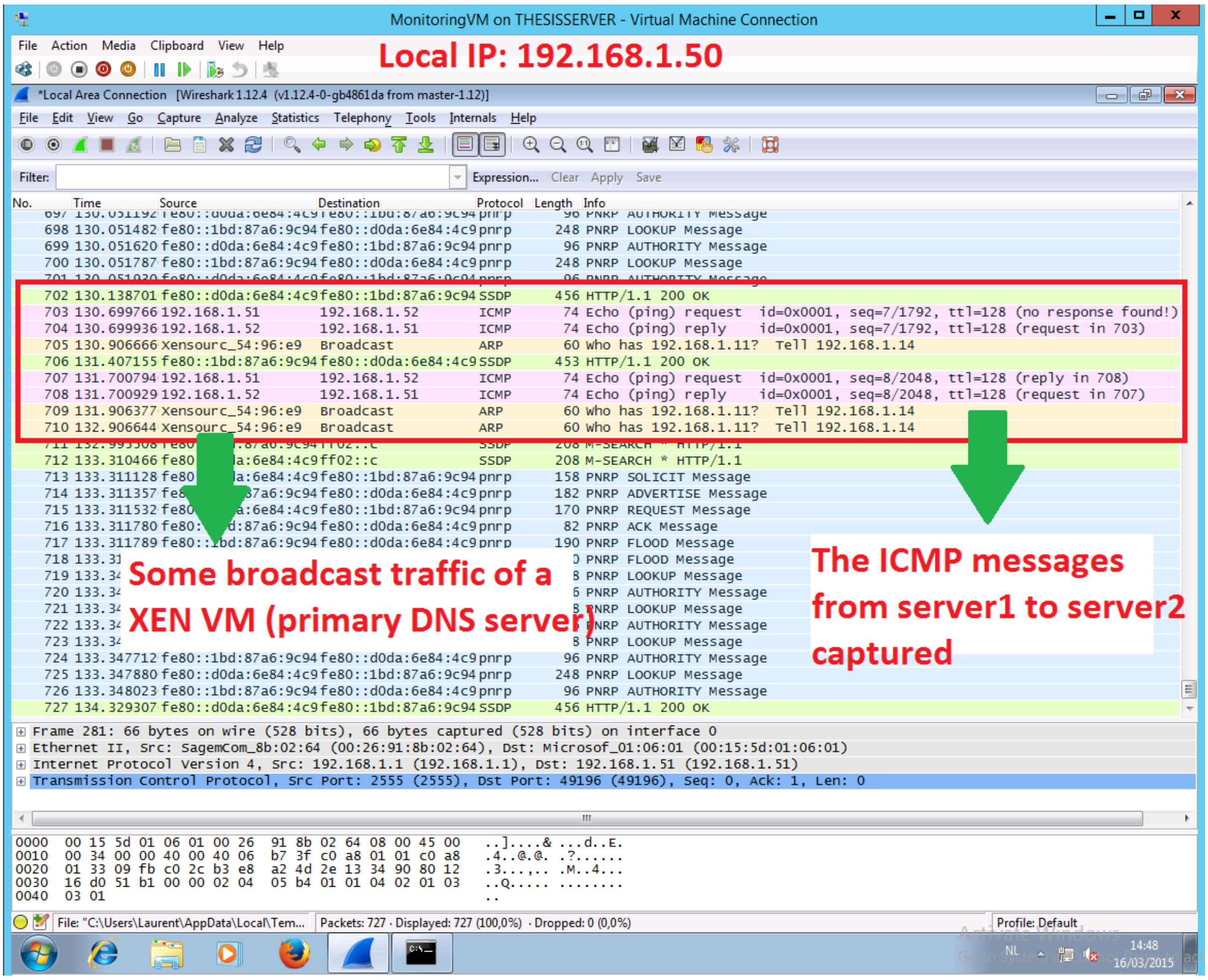
```
No.   Time       Source          Destination      Protocol Length Info
  389 70.0760850 192.168.1.1     192.168.1.52     TCP       66 2555→49197 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS
  390 70.0762800 192.168.1.52    192.168.1.1      TCP       54 49197→2555 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  391 70.0762880 192.168.1.52    192.168.1.1      TCP      413 [TCP segment of a reassembled PDU]
  392 70.0762950 192.168.1.52    192.168.1.1      HTTP/XM  680 POST /upnp/5647ec43-463f-3b8e-b0f8-e7fdf174000c/WANPPPConn1.ctl HTTP/1.1
  393 70.0764070 192.168.1.1     192.168.1.52     TCP       60 2555→49196 [FIN, ACK] Seq=527 Ack=1470 Win=9154 Len=0
  394 70.0764590 192.168.1.52    192.168.1.1      TCP       54 49196→2555 [ACK] Seq=1470 Ack=528 Win=130816 Len=0
  395 70.0771110 192.168.1.1     192.168.1.52     TCP       60 2555→49197 [ACK] Seq=1 Ack=360 Win=6912 Len=0
  396 70.0776230 192.168.1.1     192.168.1.52     TCP       60 2555→49197 [ACK] Seq=1 Ack=986 Win=8164 Len=0
  397 70.1433920 192.168.1.1     192.168.1.52     TCP      313 [TCP segment of a reassembled PDU]
  398 70.1445700 192.168.1.1     192.168.1.52     HTTP/XM  563 HTTP/1.1 200 OK
  399 70.1446370 192.168.1.52    192.168.1.1      TCP       54 49197→2555 [ACK] Seq=986 Ack=769 Win=130560 Len=0
  400 70.1446450 192.168.1.52    192.168.1.1      TCP       54 49197→2555 [FIN, ACK] Seq=986 Ack=769 Win=130560 Len=0
  401 70.1458360 192.168.1.1     192.168.1.52     TCP       60 2555→49197 [FIN, ACK] Seq=769 Ack=987 Win=8164 Len=0
  402 70.1458820 192.168.1.52    192.168.1.1      TCP       54 49197→2555 [ACK] Seq=987 Ack=770 Win=130560 Len=0
  403 70.1467890 192.168.1.52    192.168.1.1      TCP       66 49198→2555 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  404 70.1473640 192.168.1.1     192.168.1.52     TCP       66 2555→49198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS
  405 70.1475350 192.168.1.52    192.168.1.1      TCP       54 49198→2555 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  406 70.1475430 192.168.1.52    192.168.1.1      TCP      406 [TCP segment of a reassembled PDU]
  407 70.1475500 192.168.1.52    192.168.1.1      HTTP/XM  358 POST /upnp/5647ec43-463f-3b8e-b0f8-e7fdf174000c/WANPPPConn1.ctl HTTP/1.1
  408 70.1484020 192.168.1.1     192.168.1.52     TCP       60 2555→49198 [ACK] Seq=1 Ack=353 Win=6912 Len=0
  409 70.1486640 192.168.1.1     192.168.1.52     TCP       60 2555→49198 [ACK] Seq=1 Ack=657 Win=7984 Len=0
  410 70.1633780 192.168.1.1     192.168.1.52     TCP      313 [TCP segment of a reassembled PDU]
  411 70.1645180 192.168.1.1     192.168.1.52     HTTP/XM  390 HTTP/1.1 200 OK
  412 70.1645750 192.168.1.52    192.168.1.1      TCP       54 49198→2555 [ACK] Seq=657 Ack=596 Win=130560 Len=0
  413 70.1645830 192.168.1.52    192.168.1.1      TCP       54 49198→2555 [FIN, ACK] Seq=657 Ack=596 Win=130560 Len=0
  414 70.1651270 fe80::ffff:ffff:fff ff02::2      ICMPv6   103 Router Solicitation
  415 70.1658230 192.168.1.1     192.168.1.52     TCP       60 2555→49198 [FIN, ACK] Seq=596 Ack=658 Win=7984 Len=0
  416 70.1658740 192.168.1.52    192.168.1.1      TCP       54 49198→2555 [ACK] Seq=658 Ack=597 Win=130560 Len=0
  417 70.2115460 fe80::8000:f227:a10 fe80::ffff:ffff:fff ICMPv6 151 Router Advertisement
  418 70.4976410 fe80::1bd:87a6:9c94 fe80::d0da:6e84:4c9 SSDP 453 HTTP/1.1 200 OK
  419 71.4302950 fe80::d0da:6e84:4c9 fe80::1bd:87a6:9c94 SSDP 456 HTTP/1.1 200 OK
```

```
⊞ Frame 281: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: SagemCom_8b:02:64 (00:26:91:8b:02:64), Dst: Microsof_01:06:01 (00:15:5d:01:06:01)
⊞ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.51 (192.168.1.51)
⊞ Transmission Control Protocol, Src Port: 2555 (2555), Dst Port: 49196 (49196), Seq: 0, Ack: 1, Len: 0
```

```
0000  00 15 5d 01 06 01 00 26  91 8b 02 64 08 00 45 00   ..]....& ...d..E.
0010  00 34 00 00 40 00 40 06  b7 3f c0 a8 01 01 c0 a8   .4..@.@. .?......
0020  01 33 09 fb c0 2c b3 e8  a2 4d 2e 13 34 90 80 12   .3...,.. .M..4...
0030  16 d0 51 b1 00 00 02 04  05 b4 01 01 04 02 01 03   ..Q..... ........
0040  03 01                                              ..
```

File: "C:\Users\Laurent\AppData\Local\Tem... Packets: 727 · Displayed: 727 (100,0%) · Dropped: 0 (0,0%)

Figure 2: Traffic between Server 2 (192.168.1.52) and the Belgacom router captured by the vNIC.


MonitoringVM on THESISSERVER - Virtual Machine Connection
File Action Media Clipboard View Help
*Local Area Connection [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default
NL
14:48
16/03/2015

Local IP: 192.168.1.50

```
No.   Time       Source                 Destination            Protocol Length Info
697 130.051192 fe80::d0da:6e84:4c9 fe80::1bd:87a6:9c94 pnrp      96 PNRP AUTHORITY Message
698 130.051482 fe80::1bd:87a6:9c94 fe80::d0da:6e84:4c9 pnrp     248 PNRP LOOKUP Message
699 130.051620 fe80::d0da:6e84:4c9 fe80::1bd:87a6:9c94 pnrp      96 PNRP AUTHORITY Message
700 130.051787 fe80::1bd:87a6:9c94 fe80::d0da:6e84:4c9 pnrp     248 PNRP LOOKUP Message
701 130.051930 fe80::d0da:6e84:4c9 fe80::1bd:87a6:9c94 pnrp      96 PNRP AUTHORITY Message
702 130.138701 fe80::d0da:6e84:4c9 fe80::1bd:87a6:9c94 SSDP     456 HTTP/1.1 200 OK
703 130.699766 192.168.1.51        192.168.1.52        ICMP      74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (no response found!)
704 130.699936 192.168.1.52        192.168.1.51        ICMP      74 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=128 (request in 703)
705 130.906666 Xensourc_54:96:e9   Broadcast           ARP       60 Who has 192.168.1.11?  Tell 192.168.1.14
706 131.407155 fe80::1bd:87a6:9c94 fe80::d0da:6e84:4c9 SSDP     453 HTTP/1.1 200 OK
707 131.700794 192.168.1.51        192.168.1.52        ICMP      74 Echo (ping) request  id=0x0001, seq=8/2048, ttl=128 (reply in 708)
708 131.700929 192.168.1.52        192.168.1.51        ICMP      74 Echo (ping) reply    id=0x0001, seq=8/2048, ttl=128 (request in 707)
709 131.906377 Xensourc_54:96:e9   Broadcast           ARP       60 Who has 192.168.1.11?  Tell 192.168.1.14
710 132.906644 Xensourc_54:96:e9   Broadcast           ARP       60 Who has 192.168.1.11?  Tell 192.168.1.14
711 132.995508 fe80     :87a6:9c94 ff02::c             SSDP     208 M-SEARCH * HTTP/1.1
712 133.310466 fe80     a:6e84:4c9 ff02::c             SSDP     208 M-SEARCH * HTTP/1.1
713 133.311128 fe80     a:6e84:4c9 fe80::1bd:87a6:9c94 pnrp     158 PNRP SOLICIT Message
714 133.311357 fe8      7a6:9c94   fe80::d0da:6e84:4c9 pnrp     182 PNRP ADVERTISE Message
715 133.311532 fe80     a:6e84:4c9 fe80::1bd:87a6:9c94 pnrp     170 PNRP REQUEST Message
716 133.311780 fe80:     d:87a6:9c94 fe80::d0da:6e84:4c9 pnrp    82 PNRP ACK Message
717 133.311789 fe80::1bd:87a6:9c94 fe80::d0da:6e84:4c9 pnrp     190 PNRP FLOOD Message
718 133.31                                                       0 PNRP FLOOD Message
719 133.34                                                       8 PNRP LOOKUP Message
720 133.34                                                       6 PNRP AUTHORITY Message
721 133.34                                                       8 PNRP LOOKUP Message
722 133.34                                                         PNRP AUTHORITY Message
723 133.34                                                       8 PNRP LOOKUP Message
724 133.347712 fe80::1bd:87a6:9c94 fe80::d0da:6e84:4c9 pnrp      96 PNRP AUTHORITY Message
725 133.347880 fe80::d0da:6e84:4c9 fe80::1bd:87a6:9c94 pnrp     248 PNRP LOOKUP Message
726 133.348023 fe80::1bd:87a6:9c94 fe80::d0da:6e84:4c9 pnrp      96 PNRP AUTHORITY Message
727 134.329307 fe80::d0da:6e84:4c9 fe80::1bd:87a6:9c94 SSDP     456 HTTP/1.1 200 OK
```

Some broadcast traffic of a XEN VM (primary DNS server)

The ICMP messages from server1 to server2 captured

```
⊞ Frame 281: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: SagemCom_8b:02:64 (00:26:91:8b:02:64), Dst: Microsof_01:06:01 (00:15:5d:01:06:01)
⊞ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.51 (192.168.1.51)
⊞ Transmission Control Protocol, Src Port: 2555 (2555), Dst Port: 49196 (49196), Seq: 0, Ack: 1, Len: 0
```

```
0000  00 15 5d 01 06 01 00 26  91 8b 02 64 08 00 45 00   ..]....& ...d..E.
0010  00 34 00 00 40 00 40 06  b7 3f c0 a8 01 01 c0 a8   .4..@.@. .?......
0020  01 33 09 fb c0 2c b3 e8  a2 4d 2e 13 34 90 80 12   .3...,.. .M..4...
0030  16 d0 51 b1 00 00 02 04  05 b4 01 01 04 02 01 03   ..Q..... ........
0040  03 01                                              ..
```

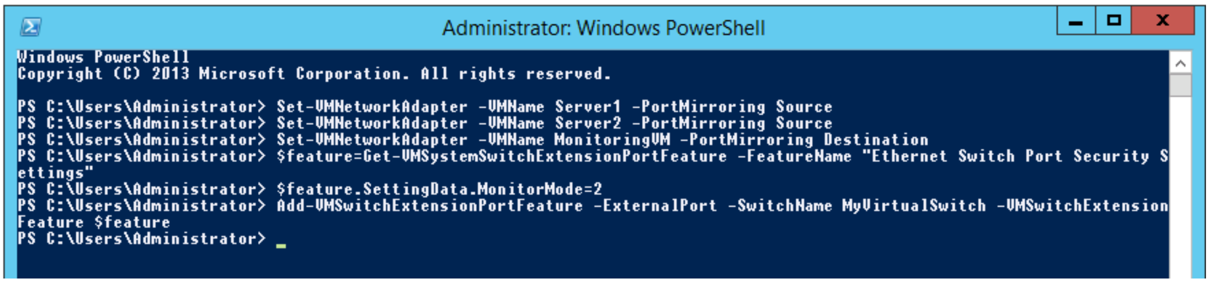
File: "C:\Users\Laurent\AppData\Local\Tem... Packets: 727 · Displayed: 727 (100,0%) · Dropped: 0 (0,0%)

Figure 3: ICMP Ping requests captured by the vNIC between server 1 and server 2.

But what about external traffic to and from external networks to the virtual switch?

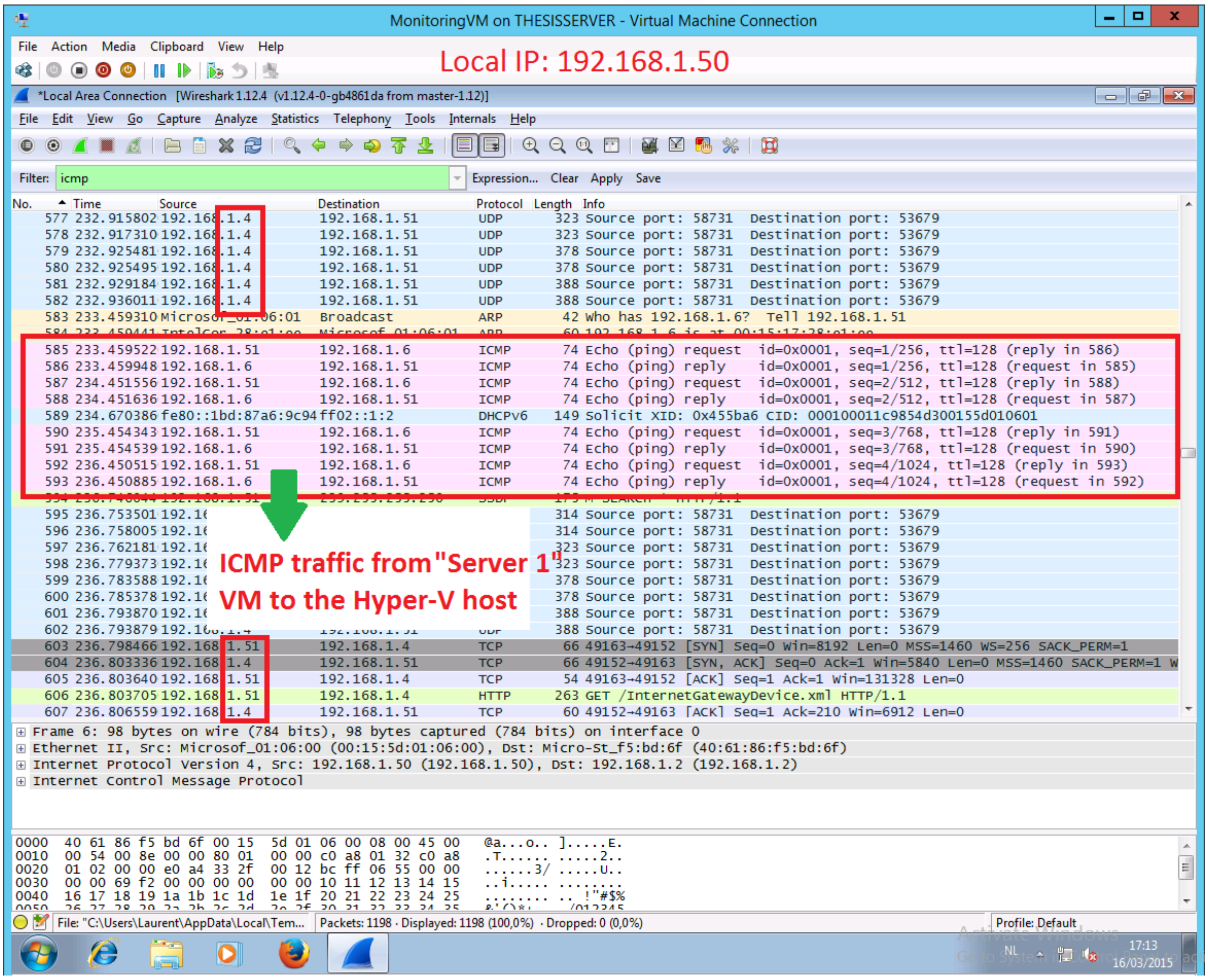
So far, I have only tested internal traffic between VM's. I also wanted to test if this "Monitoring VM" is able to capture traffic orginating from my XEN server or any other client on the network.
Therefore, additional settings must be configured on Hyper-V: the physical NIC bound to the vSwitch - that is, the external port of the vSwitch, must be set to "source" as well.

This is illustrated in the following figure: As it turned out, traffic from a XEN VM to a Hyper-V VM is captured by the "Monitoring VM". Also is traffic captured from a XEN VM to the Hyper-V host and traffic is also captured from a Hyper-V VM to the Hyper-V host. Notice that in the screenshots, other IP addresses not originating from the Hyper-V virtual switch appear in the list. This was not the case in the previous samples.



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Set-VMNetworkAdapter -VMName Server1 -PortMirroring Source
PS C:\Users\Administrator> Set-VMNetworkAdapter -VMName Server2 -PortMirroring Source
PS C:\Users\Administrator> Set-VMNetworkAdapter -VMName MonitoringVM -PortMirroring Destination
PS C:\Users\Administrator> $feature=Get-VMSystemSwitchExtensionPortFeature -FeatureName "Ethernet Switch Port Security S
ettings"
PS C:\Users\Administrator> $feature.SettingData.MonitorMode=2
PS C:\Users\Administrator> Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName MyVirtualSwitch -VMSwitchExtension
Feature $feature
PS C:\Users\Administrator> _
```



MonitoringVM on THESISSERVER - Virtual Machine Connection
File Action Media Clipboard View Help
Local IP: 192.168.1.50
*Local Area Connection [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
ICMP traffic from "Server 1"
VM to the Hyper-V host
Profile: Default

Filter: icmp

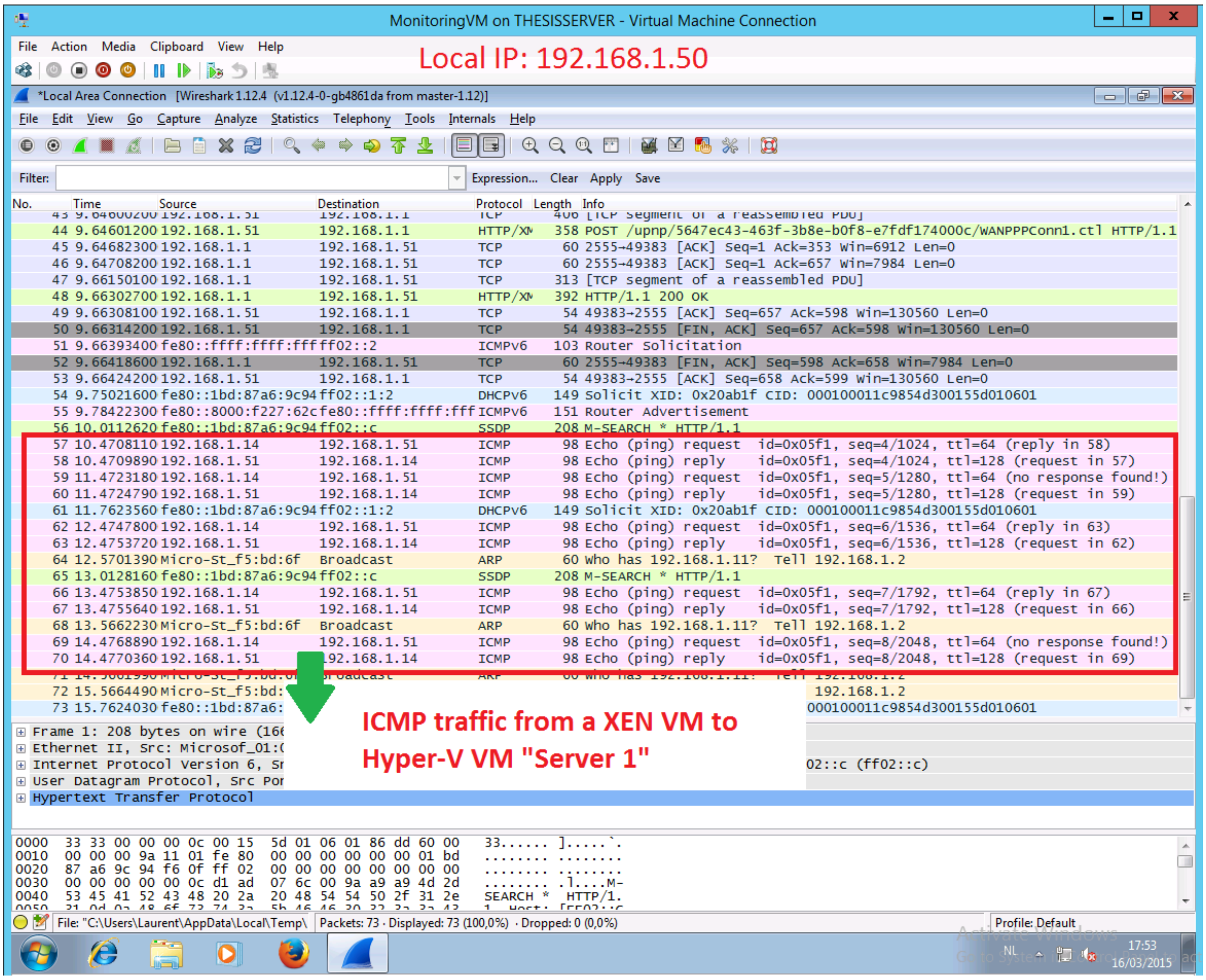
```
No.  Time       Source                 Destination        Protocol Length Info
 577 232.915802 192.168.1.4            192.168.1.51       UDP      323 Source port: 58731  Destination port: 53679
 578 232.917310 192.168.1.4            192.168.1.51       UDP      323 Source port: 58731  Destination port: 53679
 579 232.925481 192.168.1.4            192.168.1.51       UDP      378 Source port: 58731  Destination port: 53679
 580 232.925495 192.168.1.4            192.168.1.51       UDP      378 Source port: 58731  Destination port: 53679
 581 232.929184 192.168.1.4            192.168.1.51       UDP      388 Source port: 58731  Destination port: 53679
 582 232.936011 192.168.1.4            192.168.1.51       UDP      388 Source port: 58731  Destination port: 53679
 583 233.459310 Microsof_01:06:01      Broadcast          ARP       42 Who has 192.168.1.6?  Tell 192.168.1.51
 584 233.459441 IntelCor_28:e1:ee      Microsof_01:06:01  ARP       60 192.168.1.6 is at 00:15:17:28:e1:ee
 585 233.459522 192.168.1.51           192.168.1.6        ICMP      74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 586)
 586 233.459948 192.168.1.6            192.168.1.51       ICMP      74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=128 (request in 585)
 587 234.451556 192.168.1.51           192.168.1.6        ICMP      74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 588)
 588 234.451636 192.168.1.6            192.168.1.51       ICMP      74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=128 (request in 587)
 589 234.670386 fe80::1bd:87a6:9c94    ff02::1:2          DHCPv6   149 Solicit XID: 0x455ba6 CID: 000100011c9854d300155d010601
 590 235.454343 192.168.1.51           192.168.1.6        ICMP      74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 591)
 591 235.454539 192.168.1.6            192.168.1.51       ICMP      74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=128 (request in 590)
 592 236.450515 192.168.1.51           192.168.1.6        ICMP      74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 593)
 593 236.450885 192.168.1.6            192.168.1.51       ICMP      74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=128 (request in 592)
 594 236.748044 192.168.1.51           239.255.255.250    SSDP     175 M-SEARCH * HTTP/1.1
 595 236.753501 192.16                                             314 Source port: 58731  Destination port: 53679
 596 236.758005 192.16                                             314 Source port: 58731  Destination port: 53679
 597 236.762181 192.16                                             323 Source port: 58731  Destination port: 53679
 598 236.779373 192.16                                             323 Source port: 58731  Destination port: 53679
 599 236.783588 192.16                                             378 Source port: 58731  Destination port: 53679
 600 236.785378 192.16                                             378 Source port: 58731  Destination port: 53679
 601 236.793870 192.16                                             388 Source port: 58731  Destination port: 53679
 602 236.793879 192.168.1.4            192.168.1.51       UDP      388 Source port: 58731  Destination port: 53679
 603 236.798466 192.168.1.51           192.168.1.4        TCP       66 49163→49152 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 604 236.803336 192.168.1.4            192.168.1.51       TCP       66 49152→49163 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 W
 605 236.803640 192.168.1.51           192.168.1.4        TCP       54 49163→49152 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 606 236.803705 192.168.1.51           192.168.1.4        HTTP     263 GET /InternetGatewayDevice.xml HTTP/1.1
 607 236.806559 192.168.1.4            192.168.1.51       TCP       60 49152→49163 [ACK] Seq=1 Ack=210 Win=6912 Len=0
```

```
⊞ Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
⊞ Ethernet II, Src: Microsof_01:06:00 (00:15:5d:01:06:00), Dst: Micro-St_f5:bd:6f (40:61:86:f5:bd:6f)
⊞ Internet Protocol Version 4, Src: 192.168.1.50 (192.168.1.50), Dst: 192.168.1.2 (192.168.1.2)
⊞ Internet Control Message Protocol
```

```
0000  40 61 86 f5 bd 6f 00 15  5d 01 06 00 08 00 45 00   @a...o.. ].....E.
0010  00 54 00 8e 00 00 80 01  00 00 c0 a8 01 32 c0 a8   .T...... .....2..
0020  01 02 00 00 e0 a4 33 2f  00 12 bc ff 06 55 00 00   ......3/ .....U..
0030  00 00 69 f2 00 00 00 00  00 00 10 11 12 13 14 15   ..i..... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
```

File: "C:\Users\Laurent\AppData\Local\Tem... Packets: 1198 · Displayed: 1198 (100,0%) · Dropped: 0 (0,0%)

NL 17:13 16/03/2015


MonitoringVM on THESISSERVER - Virtual Machine Connection
File Action Media Clipboard View Help
*Local Area Connection [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

Local IP: 192.168.1.50

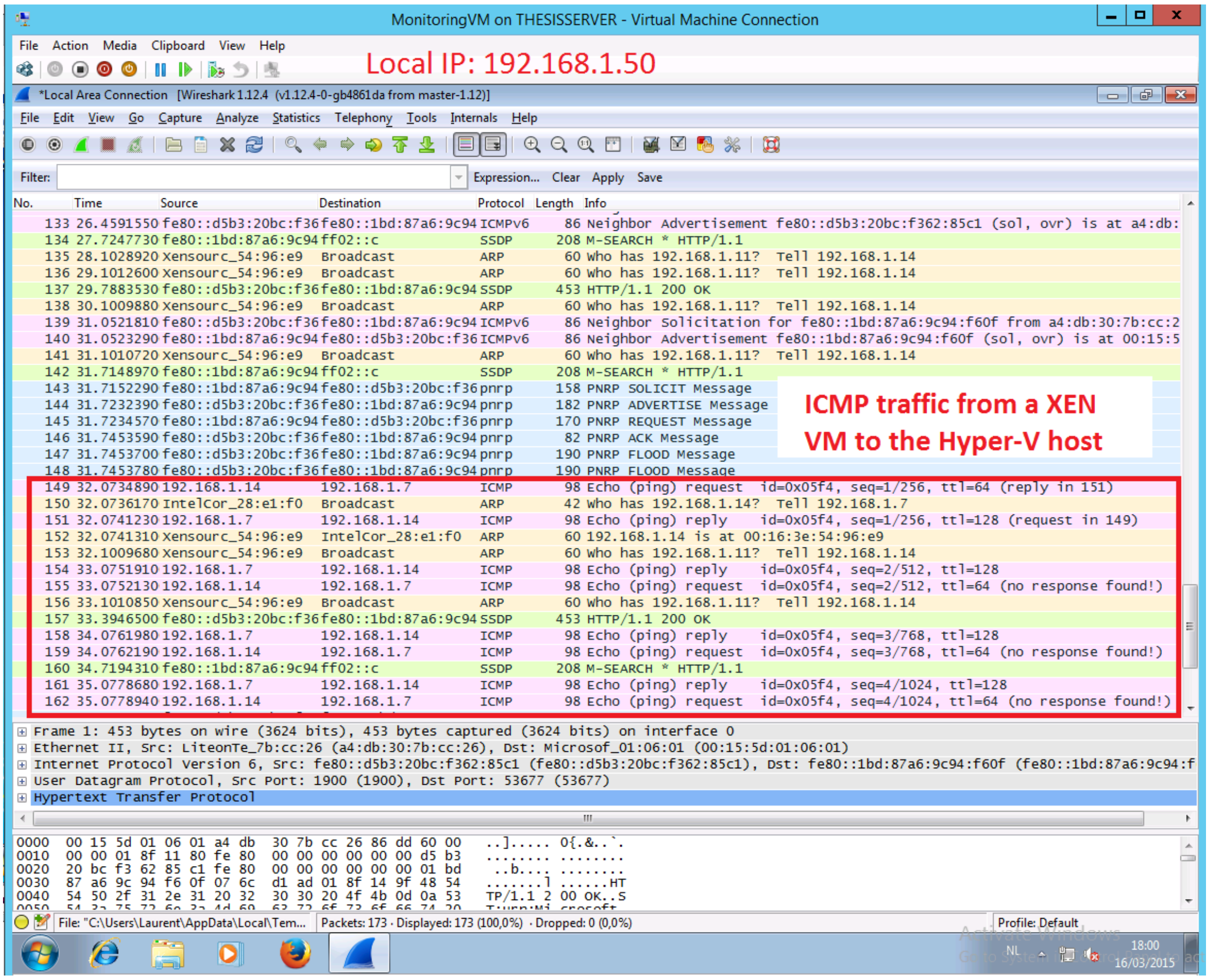
```
No.   Time       Source              Destination         Protocol  Length Info
   43 9.64600200 192.168.1.51        192.168.1.1         TCP       406 [TCP segment of a reassembled PDU]
   44 9.64601200 192.168.1.51        192.168.1.1         HTTP/XM   358 POST /upnp/5647ec43-463f-3b8e-b0f8-e7fdf174000c/WANPPPConn1.ctl HTTP/1.1
   45 9.64682300 192.168.1.1         192.168.1.51        TCP        60 2555→49383 [ACK] Seq=1 Ack=353 Win=6912 Len=0
   46 9.64708200 192.168.1.1         192.168.1.51        TCP        60 2555→49383 [ACK] Seq=1 Ack=657 Win=7984 Len=0
   47 9.66150100 192.168.1.1         192.168.1.51        TCP       313 [TCP segment of a reassembled PDU]
   48 9.66302700 192.168.1.1         192.168.1.51        HTTP/XM   392 HTTP/1.1 200 OK
   49 9.66308100 192.168.1.51        192.168.1.1         TCP        54 49383→2555 [ACK] Seq=657 Ack=598 Win=130560 Len=0
   50 9.66314200 192.168.1.51        192.168.1.1         TCP        54 49383→2555 [FIN, ACK] Seq=657 Ack=598 Win=130560 Len=0
   51 9.66393400 fe80::ffff:ffff:fff ff02::2             ICMPv6    103 Router Solicitation
   52 9.66418600 192.168.1.1         192.168.1.51        TCP        60 2555→49383 [FIN, ACK] Seq=598 Ack=658 Win=7984 Len=0
   53 9.66424200 192.168.1.51        192.168.1.1         TCP        54 49383→2555 [ACK] Seq=658 Ack=599 Win=130560 Len=0
   54 9.75021600 fe80::1bd:87a6:9c94 ff02::1:2           DHCPv6    149 Solicit XID: 0x20ab1f CID: 000100011c9854d300155d010601
   55 9.78422300 fe80::8000:f227:62c fe80::ffff:ffff:fff ICMPv6    151 Router Advertisement
   56 10.0112620 fe80::1bd:87a6:9c94 ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
   57 10.4708110 192.168.1.14        192.168.1.51        ICMP       98 Echo (ping) request  id=0x05f1, seq=4/1024, ttl=64 (reply in 58)
   58 10.4709890 192.168.1.51        192.168.1.14        ICMP       98 Echo (ping) reply    id=0x05f1, seq=4/1024, ttl=128 (request in 57)
   59 11.4723180 192.168.1.14        192.168.1.51        ICMP       98 Echo (ping) request  id=0x05f1, seq=5/1280, ttl=64 (no response found!)
   60 11.4724790 192.168.1.51        192.168.1.14        ICMP       98 Echo (ping) reply    id=0x05f1, seq=5/1280, ttl=128 (request in 59)
   61 11.7623560 fe80::1bd:87a6:9c94 ff02::1:2           DHCPv6    149 Solicit XID: 0x20ab1f CID: 000100011c9854d300155d010601
   62 12.4747800 192.168.1.14        192.168.1.51        ICMP       98 Echo (ping) request  id=0x05f1, seq=6/1536, ttl=64 (reply in 63)
   63 12.4753720 192.168.1.51        192.168.1.14        ICMP       98 Echo (ping) reply    id=0x05f1, seq=6/1536, ttl=128 (request in 62)
   64 12.5701390 Micro-St_f5:bd:6f   Broadcast           ARP        60 Who has 192.168.1.11?  Tell 192.168.1.2
   65 13.0128160 fe80::1bd:87a6:9c94 ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
   66 13.4753850 192.168.1.14        192.168.1.51        ICMP       98 Echo (ping) request  id=0x05f1, seq=7/1792, ttl=64 (reply in 67)
   67 13.4755640 192.168.1.51        192.168.1.14        ICMP       98 Echo (ping) reply    id=0x05f1, seq=7/1792, ttl=128 (request in 66)
   68 13.5662230 Micro-St_f5:bd:6f   Broadcast           ARP        60 Who has 192.168.1.11?  Tell 192.168.1.2
   69 14.4768890 192.168.1.14        192.168.1.51        ICMP       98 Echo (ping) request  id=0x05f1, seq=8/2048, ttl=64 (no response found!)
   70 14.4770360 192.168.1.51        192.168.1.14        ICMP       98 Echo (ping) reply    id=0x05f1, seq=8/2048, ttl=128 (request in 69)
   71 14.5661990 Micro-St_f5:bd:6f   Broadcast           ARP        60 Who has 192.168.1.11?  Tell 192.168.1.2
   72 15.5664490 Micro-St_f5:bd:                                                                   192.168.1.2
   73 15.7624030 fe80::1bd:87a6:                                                                  000100011c9854d300155d010601
```

```
⊞ Frame 1: 208 bytes on wire (16
⊞ Ethernet II, Src: Microsof_01:
⊞ Internet Protocol Version 6, Sr                                02::c (ff02::c)
⊞ User Datagram Protocol, Src Por
⊞ Hypertext Transfer Protocol
```

```
0000  33 33 00 00 00 0c 00 15  5d 01 06 01 86 dd 60 00   33...... ].....`.
0010  00 00 00 9a 11 01 fe 80  00 00 00 00 00 00 01 bd   ........ ........
0020  87 a6 9c 94 f6 0f ff 02  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 0c d1 ad  07 6c 00 9a a9 a9 4d 2d   ........ .l....M-
0040  53 45 41 52 43 48 20 2a  20 48 54 54 50 2f 31 2e   SEARCH *  HTTP/1.
```

File: "C:\Users\Laurent\AppData\Local\Temp\ Packets: 73 · Displayed: 73 (100,0%) · Dropped: 0 (0,0%) Profile: Default

ICMP traffic from a XEN VM to Hyper-V VM "Server 1"


MonitoringVM on THESISSERVER - Virtual Machine Connection
File Action Media Clipboard View Help
Local IP: 192.168.1.50
*Local Area Connection [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
ICMP traffic from a XEN VM to the Hyper-V host
NL
18:00
16/03/2015

```
No.    Time        Source                 Destination            Protocol Length Info
   133 26.4591550 fe80::d5b3:20bc:f36 fe80::1bd:87a6:9c94 ICMPv6    86 Neighbor Advertisement fe80::d5b3:20bc:f362:85c1 (sol, ovr) is at a4:db:
   134 27.7247730 fe80::1bd:87a6:9c94 ff02::c             SSDP     208 M-SEARCH * HTTP/1.1
   135 28.1028920 Xensourc_54:96:e9   Broadcast           ARP       60 Who has 192.168.1.11?  Tell 192.168.1.14
   136 29.1012600 Xensourc_54:96:e9   Broadcast           ARP       60 Who has 192.168.1.11?  Tell 192.168.1.14
   137 29.7883530 fe80::d5b3:20bc:f36 fe80::1bd:87a6:9c94 SSDP     453 HTTP/1.1 200 OK
   138 30.1009880 Xensourc_54:96:e9   Broadcast           ARP       60 Who has 192.168.1.11?  Tell 192.168.1.14
   139 31.0521810 fe80::d5b3:20bc:f36 fe80::1bd:87a6:9c94 ICMPv6    86 Neighbor Solicitation for fe80::1bd:87a6:9c94:f60f from a4:db:30:7b:cc:2
   140 31.0523290 fe80::1bd:87a6:9c94 fe80::d5b3:20bc:f36 ICMPv6    86 Neighbor Advertisement fe80::1bd:87a6:9c94:f60f (sol, ovr) is at 00:15:5
   141 31.1010720 Xensourc_54:96:e9   Broadcast           ARP       60 Who has 192.168.1.11?  Tell 192.168.1.14
   142 31.7148970 fe80::1bd:87a6:9c94 ff02::c             SSDP     208 M-SEARCH * HTTP/1.1
   143 31.7152290 fe80::1bd:87a6:9c94 fe80::d5b3:20bc:f36 pnrp     158 PNRP SOLICIT Message
   144 31.7232390 fe80::d5b3:20bc:f36 fe80::1bd:87a6:9c94 pnrp     182 PNRP ADVERTISE Message
   145 31.7234570 fe80::1bd:87a6:9c94 fe80::d5b3:20bc:f36 pnrp     170 PNRP REQUEST Message
   146 31.7453590 fe80::d5b3:20bc:f36 fe80::1bd:87a6:9c94 pnrp      82 PNRP ACK Message
   147 31.7453700 fe80::d5b3:20bc:f36 fe80::1bd:87a6:9c94 pnrp     190 PNRP FLOOD Message
   148 31.7453780 fe80::d5b3:20bc:f36 fe80::1bd:87a6:9c94 pnrp     190 PNRP FLOOD Message
   149 32.0734890 192.168.1.14        192.168.1.7         ICMP      98 Echo (ping) request  id=0x05f4, seq=1/256, ttl=64 (reply in 151)
   150 32.0736170 IntelCor_28:e1:f0   Broadcast           ARP       42 Who has 192.168.1.14?  Tell 192.168.1.7
   151 32.0741230 192.168.1.7         192.168.1.14        ICMP      98 Echo (ping) reply    id=0x05f4, seq=1/256, ttl=128 (request in 149)
   152 32.0741310 Xensourc_54:96:e9   IntelCor_28:e1:f0   ARP       60 192.168.1.14 is at 00:16:3e:54:96:e9
   153 32.1009680 Xensourc_54:96:e9   Broadcast           ARP       60 Who has 192.168.1.11?  Tell 192.168.1.14
   154 33.0751910 192.168.1.7         192.168.1.14        ICMP      98 Echo (ping) reply    id=0x05f4, seq=2/512, ttl=128
   155 33.0752130 192.168.1.14        192.168.1.7         ICMP      98 Echo (ping) request  id=0x05f4, seq=2/512, ttl=64 (no response found!)
   156 33.1010850 Xensourc_54:96:e9   Broadcast           ARP       60 Who has 192.168.1.11?  Tell 192.168.1.14
   157 33.3946500 fe80::d5b3:20bc:f36 fe80::1bd:87a6:9c94 SSDP     453 HTTP/1.1 200 OK
   158 34.0761980 192.168.1.7         192.168.1.14        ICMP      98 Echo (ping) reply    id=0x05f4, seq=3/768, ttl=128
   159 34.0762190 192.168.1.14        192.168.1.7         ICMP      98 Echo (ping) request  id=0x05f4, seq=3/768, ttl=64 (no response found!)
   160 34.7194310 fe80::1bd:87a6:9c94 ff02::c             SSDP     208 M-SEARCH * HTTP/1.1
   161 35.0778680 192.168.1.7         192.168.1.14        ICMP      98 Echo (ping) reply    id=0x05f4, seq=4/1024, ttl=128
   162 35.0778940 192.168.1.14        192.168.1.7         ICMP      98 Echo (ping) request  id=0x05f4, seq=4/1024, ttl=64 (no response found!)
```

```
⊞ Frame 1: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface 0
⊞ Ethernet II, Src: LiteonTe_7b:cc:26 (a4:db:30:7b:cc:26), Dst: Microsof_01:06:01 (00:15:5d:01:06:01)
⊞ Internet Protocol Version 6, Src: fe80::d5b3:20bc:f362:85c1 (fe80::d5b3:20bc:f362:85c1), Dst: fe80::1bd:87a6:9c94:f60f (fe80::1bd:87a6:9c94:f
⊞ User Datagram Protocol, Src Port: 1900 (1900), Dst Port: 53677 (53677)
⊞ Hypertext Transfer Protocol
```

```
0000  00 15 5d 01 06 01 a4 db  30 7b cc 26 86 dd 60 00   ..]..... 0{.&..`.
0010  00 00 01 8f 11 80 fe 80  00 00 00 00 00 00 d5 b3   ........ ........
0020  20 bc f3 62 85 c1 fe 80  00 00 00 00 00 00 01 bd    ..b.... ........
0030  87 a6 9c 94 f6 0f 07 6c  d1 ad 01 8f 14 9f 48 54   .......l ......HT
0040  54 50 2f 31 2e 31 20 32  30 30 20 4f 4b 0d 0a 53   TP/1.1 2 00 OK..S
```

File: "C:\Users\Laurent\AppData\Local\Tem... Packets: 173 · Displayed: 173 (100,0%) · Dropped: 0 (0,0%) Profile: Default

Figure 4: Traffic from any client to the Hyper-V host is also captured by the VM running on this Hyper-V host.

The tests show that it is possible, with some configuration, to snif a virtual switch. It is therefore possible to capture all ports on a vSwitch and forward (make a copy of) the packets to a VM that has a packet sniffer running.

Planning

This week, or otherwise next week, I plan to install Snort on the virtual network. But before I start with that, I would like to hear the Prof his opinion of the delivered work.

Problems

Issues

The tests were performed using Hyper-V. If requested, I can do the same with XEN.

Assistance

See planning.