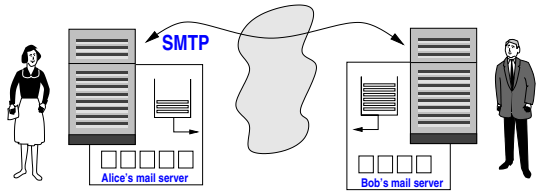
ComNet - Lab n°3

Application Layer (2): Mail, DNS and SNMP

Following on Lab n°2, this lab continues our exploration of the application layer, looking at the SMTP, POP, IMAP, DNS, and SNMP protocols. It includes exercises to be tackled without computer assistance, as well as trace capture and analysis using `wireshark/tshark`.



1 Mail

We look at the various mechanisms and protocols associated with sending and receiving e-mail. More specifically, we study approaches based on SMTP/POP/IMAP (local client), and eventually the other based on HTTP (web-mail).

1.1 Some exercises (without computer assistance)

1. Bob accesses his messages via the web. He sends a message to Alice. She retrieves her messages on her office computer when it is turned on. Describe all the information exchanges and protocols used.

2. Describe the structure of the message that are exchanged between mail servers.

3. Can you decode this header field?

```
Subject: =?iso-8859-1?B?Qydlc3QgcGFzIGZhY2lsZSAhCg==?=
```

4. You send a mail with a textual message encoded both in plain text and HTML, and including several attachements: a PNG image, an MP3 encoded sound, and a WAD file for Doom. What header lines will appear in the message?

1.2 Mail services on the networking testbed

The platform can deliver mail via the SMTP, POP and IMAP services.

We assume that you use the PPTI host **N**. Sending e-mail is done through the SMTP protocol that contacts the MTA located on the "server" VM. This is identified by its name (`mail.etu`**N**`.plateforme.lan`) or its IPv4 address (`10.`**N**`.1.`**N**3). You can use the `etudiant` mail box on the MTA in order to receive messages[1].

You can then send messages, if you use de GUI client `evolution`, from a dedicated local account on the client (e.g., "`Test SMTP`") simply by configuring your mail agent. If you use the text client `mutt`, you must edit the local ressource file (see `man mutt` and `man muttrc`). This configuration should include `mail.etu`**N**`.plateforme.lan` (or `10.`**N**`.1.`**N**3) as the mail server and SMTP (or ESMTP) as the protocol for sending mail.

Concerning message receipt, you can access the `etudaint@etu`**N**`.plateforme.lan` mailbox with the two following protocols: POP or IMAP. To do this, if you use de GUI client `evolution`, a second local account, "`Test POP`", is to be configured to access and retrieve messages via POP, and a third local account, "`Test IMAP`", is also to be configured for an access via IMAP to the messages on the server. If you use the text client `mutt`, you must edit the local ressource file.

1.2.1 Server configuration

The following are the 2 servers that we need for the lab:

- `smtpd`: We use **Postfix**[2], an alternative MTA to Sendmail. To avoid any server configuration, you need to use the box associated with the `etudiant` UNIX account.
- `imapd`: The **Courier-IMAP**[3] server provides POP and IMAP services.

1.2.2 `evolution` GUI client configuration (only if use of the network testbed from the PPTI room with X11)

Beware, if you use this application, do not use the proxy : Edition -> Préférences -> Préférences réseau -> in "Méthode" select: "Aucun serveur mandataire"

On your client machine, using the `evolution` UA requires some configuration in order to add local email accounts ("`Test SMTP`", "`Test POP`" and "`Test IMAP`"). After having started the application, from the Edition menu, select Preférence then use the + Ajouter button to add a new account. **Warning, the accounts are perhaps already configured**, in this case delete the mail that is in the system and recheck any parameters that might have been changed.

"Test SMTP" The steps to add the local account "`Test SMTP`" to `evolution`, in order to be able to send messages via SMTP, are the following:

- Don't restore the previous session, if asked
- Configure the name "`etudiant on VM3`" and the e-mail address `etudiant@etu`**N**`.plateforme.lan` (you can specify it as the default account)

[1] Basic UNIX server configuration associates local UNIX user accounts to mail accounts.
[2] `http://www.postfix.org/`
[3] `http://www.courier-mta.org/imap/`

- Do not configure any receiving server (choose "Aucun")
- Configure the SMTP server (select SMTP protocol, type the server name "`mail.etu`**N**`.plateforme.lan`" or address `10.`**N**`.1.`**N**`3` and don't select any authentication)
- Beware, when creating the SMTP account, it is never proposed to use this default account. After creating the SMTP account, go to Editions -> Préférences -> Click on SMTP Test and right-click "Par défault".
- Finish by configuring the name "`Test SMTP`"

"Test POP" The steps to add the local account "`Test POP`" to `evolution`, in order to be able to retrieve messages via POP from the server's `etudiant` mailbox are the following:

- Again, configure the name "`etudiant on VM3`" and the e-mail address `etudiant@etu`**N**`.plateforme.lan`
- Configure the POP server (select POP protocol, specify the server name "`mail.etu`**N**`.plateforme.lan`" or address `10.`**N**`.1.`**N**`3`, the username "`etudiant`", and don't change any security or authentication mechanisms)
- opt to keep the messages on the server ("Conserver les messages sue le serveur") and leave the other reception options at their default values
- Do not configure the SMTP server (select "`Sendmail`")
- Finish by configuring the name "`Test POP`"

"Test IMAP" The steps to add the local account "`Test IMAP`" to `evolution`, in order to be able to access via IMAP the messages of the `etudiant` mailbox on the server are the following:

- Again, configure the name "`etudiant on VM3`" and the e-mail address `etudiant@etu`**N**`.plateforme.lan`
- Configure the IMAP server (select the IMAP protocol, specify the server name "`mail.etu`**N**`.plateforme.lan`" or address `10.`**N**`.1.`**N**`3`, the username "`etudiant`", and don't change any security or authentication mechanisms)
- Leave the other reception options at their default values
- Do not configure the SMTP server (select "`Sendmail`")
- Finish by configuring the name "`Test IMAP`"

1.2.3 Preparing to capture the traffic

The aim of capturing the traces in the next section is to collect e-mail traffic and to understand its characteristics. On the networking testbed, the topology has been configured (client and server on the same LAN). You will perform these traffic captures using `wireshark/tshark`:

- From PPTI PC **N**, connect to the three corresponding testbed VMs with the help of three terminal windows
  - access in the "client" vm**N**1 (window 1) with SSH to `etudiant@10.0.7.`**N**`1` (use `-Y` if you want to run `evolution`)
  - access in the "monitor" vm**N**2 (window 2) with SSH to `etudiant@10.0.7.`**N**`2` (use `-Y` if you want to run `wireshark`)
  - access in the "server" vm**N**3 (window 3) with SSH to `etudiant@10.0.7.`**N**`3`
- Verify that the Postfix and Courier-IMAPservers are running on `10.0.7.`**N**`3` (window 3)
  - look for the servers processes by typing: `ps aux | grep postfix`, or `imapd`
  - look at the interfaces and especially the one of the experimental LAN (`/sbin/ifconfig eth1`) and verify that the IPv4 server address for the client connection is correct (it should be `10.`**N**`.1.`**N**`3`)
- Start the capture by running the sniffer on `10.0.7.`**N**`2` (window 2)
  - run the sniffer by typing: `wireshark/tshark`
  - indicate the capture on interface `eth1`, as previously described
- Start `evolution`, `mutt` or `telnet`, on `10.0.7.`**N**`1` (window 1)
  - either type `evolution` or `mutt` and use it to generate either SMTP, POP, or IMAP traffic, depending upon the type of trace desired
  - or type `telnet mail.etu`**N**`.plateforme.lan 25`
- Observe the trace in the `wireshark/tshark` window
- **Filter the traffic to keep only SMTP, POP, IMAP** (filter = `smtp`, `pop` or `imap`). Save the filtered traces in order to reuse them later.

1.3 Sending messages

1.3.1 Sending e-mail with the SMTP protocol

Capture a trace in which you use `evolution` (from the default local account "`Test SMTP`") or `mutt` to send an e-mail to the server mailbox (`etudiant`).

1. Which SMTP commands do you observe that are associated with the sending of an e-mail? Can you describe what they are used for and the type of response that they produce?

2. What constraints apply to the message format? Explain the structure of the message and describe the fields that compose its header.

3. What do you think of SMTP's authentication mechanisms?

Without the testbed... If you have difficulty accessing the network testbed, or you would like to practice from another machine, you can download the trace `tme3-smt.dmp` (similar to the one previously captured) either from the directory `/Infos/lmd/2022/master/ue/MU4IN001-2022oct`, or from the web page `http://www-npa.lip6.fr/~fourmaux/Traces/labV8.html`, and then analyze it using `wireshark` software (without the need for administrator's rights).

1.3.2 Sending e-mail with the TELNET protocol

An alternative, less attractive but nonetheless effective, is to access the SMTP server via a `telnet` client. Just type the command: `telnet mail.etu`**N**`.plateforme.lan 25`.

1. Verify that you can send an e-mail in this manner.
2. If you capture a trace, which filters do you use?

1.3.3 Sending e-mail with the HTTP protocol

You can download and analyze the trace `tme3-wm1.dmp` from the usual locations (see part 1.3.1).

1. Can you find the original message in the server's response?
2. What do you think of the level of confidentiality associated with checking your e-mail in this manner?

1.4 Receiving messages

1.4.1 Receiving e-mail with the POP protocol

Capture a trace in which you use `evolution` (from the "`Test POP`" local account) or `mutt` to retrieve an e-mail (make sure that this account has indeed received an e-mail).

1. Which commands does POP use to retrieve an e-mail? Can you describe what these commands do and what type of response they produce?

2. In your opinion, how would the POP server respond if there were several messages waiting?

3. What are the differences between the message sent previously and the one received here?

Without the testbed... If you need, you can download and analyze the trace `tme3-pop.dmp` (similar to the one previously captured) from the usual locations (see part 1.3.1).

1.4.2 Receiving e-mail with the IMAP protocol

Capture a trace in which you use the `evolution` (from the "`Test IMAP`" local account) or `mutt` to retrieve an e-mail (make sure that this account had indeed received an e-mail).

1. Characterize the types of messages exchanged between the client and the IMAP server

2. What protocol differences do you observe between POP and IMAP?

3. What are the differences between the message sent and the one previously received here?

4. Do you think that authentication is more secure with IMAP?

Without the testbed... If you need, you can download and analyze the trace `tme3-ima.dmp` (similar to the one previously captured) from the usual locations (see part 1.3.1).

1.4.3 Receiving e-mail with the TELNET protocol

Since POP and IMAP are textual protocols, the `telnet` client can be used to connect to the POP or IMAP servers. Just type the command: `telnet mail.etu`**N**`.plateforme.lan <portnum>`, where `<portnum>` is the port number used by the server protocol (110 for POP, and 143 for IMAP).

1. Check which actions you can take in this way with POP.
2. Check which actions you can take in this way with IMAP.
3. If you capture a trace, which filters do you use?

1.4.4 Receiving e-mail with the HTTP protocol

You can download and analyze the trace `tme3-wm2.dmp` from the usual locations (see part 1.3.1).

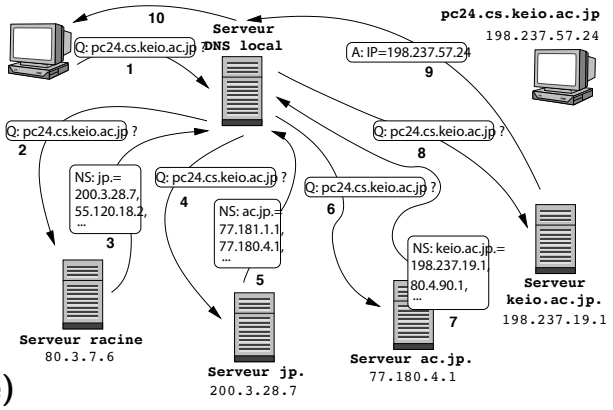
1. Can you find the original message in the server's response?
2. Viewing the message generates a lot of HTTP traffic. Discuss how well checking one's e-mail through the web performs.

1.5 Wide area trace (optional... you can tackle this by yourself if you are well ahead of the other students)

From a record containing one hour of wide area traffic between the *Lawrence Berkeley Laboratory* and the rest of the world in January 1994, find examples of SMTP, POP, and IMAP communications.

Load the trace `tme2-lbl.txt.gz`, either from the directory `/Infos/lmd/2022/master/ue/MU4IN001-2022oct`, or from the web page `http://www-npa.lip6.fr/~fourmaux/Traces/labV8.html`, to a **local** directory (eg. `/tmp`)[4]. Then using standard UNIX tools (`awk`, `perl`, `sed`,...), isolate interesting streams (SMTP, POP, and IMAP) and identify their typical characteristics. **Your tutor is present to answer questions related to the network, but will not be able to advise you on the use of these tools.**

[4] The size of the trace is quite large, if you work on your personal account, which is mounted via NFS, you will get very poor response time.



2 Directory Service

2.1 The DNS system (without computer assistance)

1. Each host on the Internet is generally associated with a local name server and an authoritative name server. What is the role played by each of these within the DNS system?

2. From a user's machine that has a browser (web client) and an MUA (e-mail client), you want to surf the website of an institution (e.g., your university), then send an e-mail to this institution's mail server. Which entities need to use the DNS system, and, in particular, which ones have to launch queries that involve the authoritative server of the institution? Can the web server and the mail server of this institution share the same name (e.g., server.upmc.org)?

3. While surfing the Web, you click a link to a page that interests you. Your machine does not know the IP address corresponding to the URL of the page requested and it is not in the cache of your browser. If n DNS servers are visited **iteratively** before obtaining the desired IP address, how long can we expect it to take before the page appears (assuming the transmission time for the object is negligible)? Draw a chronogram to illustrate your answer.

2.2 Examining a DNS exchange (without computer assistance)

In the DNS system, messages are exchanged in a connectionless fashion. Here is an example consisting of two frames that you will study by hand (without Wireshark). Sketch directly on the printout, to surround the various fields of the trace. Make sure that you understand the way in which names are coded by reference (a byte containing the code `0xC0`$+n$ is a pointer to a location n bytes from the beginning of the DNS message).

2.2.1 DNS Query

Here is a frame observed on the network:

```
0000  00 07 e9 0c 90 62 00 20  ed 87 fd e6 08 00 45 00   .....b.  ......E.
0010  00 39 00 00 40 00 40 11  a9 71 84 e3 3d 7a 84 e3   .9..@.@. .q..=z..
0020  4a 02 85 05 00 35 00 25  c0 74 a0 71 01 00 00 01   J....5.% .t.q....
0030  00 00 00 00 00 00 03 77  77 77 04 6c 69 70 36 02   .......w ww.lip6.
0040  66 72 00 00 01 00 01                              fr.....
```

1. Manually analyze the frame above, with the help of information in the slides for this course.
2. What is the purpose of the message contained in this frame? What action the user could this request trigger?

2.2.2 DNS Response

Shortly after the frame above, one can observe the following frame on the network:

```
0000  00 20 ed 87 fd e6 00 07  e9 0c 90 62 08 00 45 00   . ...... ...b..E.
0010  00 cf 2a 2d 00 00 3f 11  bf ae 84 e3 4a 02 84 e3   ..*-..?. ....J...
0020  3d 7a 00 35 85 05 00 bb  a1 3b a0 71 85 80 00 01   =z.5.... .;.q....
0030  00 02 00 03 00 03 03 77  77 77 04 6c 69 70 36 02   .......w ww.lip6.
0040  66 72 00 00 01 00 01 c0  0c 00 05 00 01 00 00 54   fr...... .......T
0050  60 00 08 05 68 6f 72 75  73 c0 10 c0 29 00 01 00   `...horu s...)...
0060  01 00 00 54 60 00 04 84  e3 3c 0d c0 10 00 02 00   ...T`... .<......
0070  01 00 00 54 60 00 07 04  69 73 69 73 c0 10 c0 10   ...T`... isis....
0080  00 02 00 01 00 00 54 60  00 09 06 6f 73 69 72 69   ......T` ...osiri
0090  73 c0 10 c0 10 00 02 00  01 00 00 54 60 00 0e 06   s....... ...T`...
00a0  73 6f 6c 65 69 6c 04 75  76 73 71 c0 15 c0 4d 00   soleil.u vsq...M.
```

```
00b0  01 00 01 00 00 54 60 00  04 84 e3 3c 02 c0 60 00   .....T‘. ...<..‘.

00c0  01 00 01 00 00 54 60 00  04 84 e3 3c 1e c0 75 00   .....T‘. ...<..u.

00d0  01 00 01 00 01 16 cb 00  04 c1 33 18 01            ........ ..3..
```

1. Analyze this frame by hand.
2. What information is being returned by the local DNS server? Is it what the client expected to receive?

2.2.3 Verification of the “manual” analysis

Only after having completed both manual analyses above, check your results using `wireshark`. Load the `tme3-dn1.dmp` trace either from the directory `/Infos/lmd/2022/master/ue/MU4IN001-2022oct`, or from the web page `http://www-npa.lip6.fr/~fourmaux/Traces/labV8.html`.

2.3 DNS on the networking testbed

For the purposes of the networking testbed, we have installed a DNS server on each “server” VM. It plays the role of local and authoritative server, and of relay. On it, you will find information relating to the `etu`**N**`.plateforme.lan` zone (if you are on the PPTI **N** host), as well as reverse resolution.

2.3.1 DNS client and server configuration

1. How does a host access the DNS system? Does one need a client program? Which parameters need to be configured? Examine the file `/etc/resolv.conf` on the client machine (`10.0.7.`**N**1) and explain the parameters.

2. The **BIND**[5] server configuration on the “server” VM (`10.0.7.`**N**3) can be found in the file `/etc/bind/named.conf.local`. This indicates the two locally-controlled zones:
   - **etuN.plateforme.lan**, described in the file `/etc/bind/db.etu`**N**`.plateforme.lan`
   - **N.10.in-addr.arpa**, for the reverse resolution, also in the file `/etc/bind/db.etu`**N**`.plateforme.lan`

   Analyze the contents of these files and explain how they are used. Specify what we must change if we wish to declare a new machine on the server.

3. How can we generate DNS traffic? Describe at least four possibile ways, which you will test in the following trace capture.

[5] BIND *(Berkeley Internet Name Daemon)*: http://www.isc.org/software/bind

2.3.2 Capturing local DNS traffic

The aim of this third trace capture is to collect DNS traffic and understand its characteristics. On the networking testbed, still using Topology 1 (client and server stations on the same LAN), capture the DNS traffic using `wireshark` or `tshark`:

- From PPTI PC **N**, connect to the three corresponding testbed VMs with the help of three terminal windows.
- Verify that the BIND server (`named`) is running on `10.0.7.`**N**3 (window 3).
- Start capturing traffic by running the sniffer on interface `eth1` of host `10.0.7.`**N**2 (window 2).
- From the "client" VM, verify the local DNS configuration and carry out the actions necessary to generate the DNS queries previously discussed (window 1).
- Observe the trace in the `wireshark` window as it is captured.
- **Filter the traffic to keep only DNS** (filter = `dns`). Save the filtered trace in order to reuse it later. Keep the application open in order to conduct the following analyses.

2.3.3 Analyzing local DNS traffic

1. Analyze the frames that are exchanged in the trace.
2. Does the local resolution have any impact on the DNS exchange?

2.4 DNS in the Internet

The DNS server for each testbed server plays the role of local server for areas other than **etuN.plateforme.lan**. Since this server does not have access to the rest of the Internet, requests regarding other zones of the Internet are relayed to the rack DNS server (which does have access to the global Internet DNS.)

2.4.1 Capturing external DNS traffic

The aim of this third trace capture is to collect additional DNS traffic and understand its characteristics. On the networking testbed, again using Topology 1 (client and server stations on the same LAN), capture the DNS traffic using `wireshark` or `tshark`:

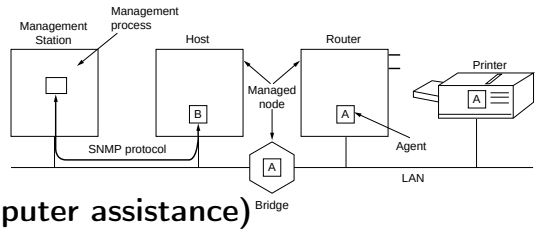
- From PPTI PC **N**, connect to the three corresponding testbed VMs with the help of three terminal windows.
- Verify that the BIND server (`named`) is running on `10.0.7.`**N**3 (window 3)
- Start the capture by running the sniffer on interface `eth1` of host `10.0.7.`**N**2 (window 2)
- With the "client" VM, verify the local DNS configuration, then type `dig www.apple.com` (window 1)
- Watch the captured traffic in the `wireshark`/`tshark` window
- **Filter traffic to keep only DNS** (filter = `dns`). Save the filtered trace in order to reuse it later. Keep the application running in order to conduct the following analysis.

2.4.2 Analysis of the external DNS exchange

1. Quickly analyze the two frames in the trace.
2. Explain the purpose of this exchange
3. In your opinion, why does the name resolution for `www.apple.com` refer to servers in the domain `aka*.net`?

2.4.3 Without the testbed...

If you need, you can download and analyze the trace `tme3-dn2.dmp` (similar to the one previously captured) from the usual locations (see part 1.3.1).



3 Network management

3.1 Exercices about network management (without computer assistance)

1. For a network administrator, what is the interest of using network management tools? Cite several examples.

2. Draw a diagram showing the different elements involved in network management and their interactions (application elements, exchanged messages, ...).

3. Define the following terms: *managing entity*, *managed device*, *management agent*, *Management Information Base (MIB)*, *Structure of Management Information (SMI)*, and *network management protocol*.

4. What are the PDUs used by SNMP? Which messages are used for query/response or one-way messages? What is the difference between these two kind of exchanges? What are the advantages and disadvantages?

5. In your opinion, why do we use UDP rather than TCP for the transport of SNMP PDUs?

6. (a) Propose a mechanism to discover the different machines on the management station LAN.

(b) Explain how to verify that a machine is a router (the standard MIB-II defines a simple object `ipForwarding`).

(c) How to obtain the names of these routers (MIB-II standard defines the object `system.sysName` with a character string type...)?

(d) Knowing that the MIB-II provides the table object `ipAddrTable` that reference all interfaces on a machine with their IP parameters (IP address, network mask, broadcast address ...), please specify how to obtain all IP addresses (ipAdEntAddr field) of a router.

(e) Specify how to change the network mask value (field ipAdEntNetMask) associated with the interface 3 of a router (the entries of the table object `ipAddrTable` are indexed by the number of this interface).

(f) Having the information just mentioned available in the MIB-II, suggest a general mechanism to discover all routers in the network of a company. Indicate the limitations of your approach.

3.2 The SNMP protocol

3.2.1 Capturing SNMP traffic

The aim of this last traffic capture is to collect an SNMP trace and understand its characteristics. On the networking testbed, again using Topology 1 (client and server stations on the same LAN), capture the SNMP traffic using `wireshark` or `tshark`:

- From PPTI PC **N**, connect to the three corresponding VMs of the testbed with the help of three terminal windows.
- Verify that the SNMP server (`snmpd`) is running on `10.0.7.`**N**3 (window 3)
- Start capturing the trace by running the sniffer on interface `eth1` of host `10.0.7.`**N**2 (window 2)
- Use the Net-SNMP commands (`snmpget`, `snmpgetnext`, `snmpwalk`...) on `10.0.7.`**N**1 (window 1)
  - type `snmpget -v 1 -c public 10.`**N**`.1.`**N**`3 .1.3.6.1.2.1.1.1.0`
  - then type `snmpgetnext -v 1 -c public 10.`**N**`.1.`**N**`3 .1.3.6.1.2.1.1.9.1.3.1`
  - then type `snmpwalk -v 1 -c public 10.`**N**`.1.`**N**`3 .1.3.6.1.2.1.1.9.1.3`
  - then type `snmpset -v 1 -c private 10.`**N**`.1.`**N**`3 .1.3.6.1.2.1.1.4.0 s toto@upmc.fr`
- Observe the trace as it appears in the `wireshark`/`tshark` window
- **Filter traffic to keep only SNMP** (filter = `snmp`). Save the filtered trace in order to reuse it later. Keep the application running in order to conduct the following analysis.

3.2.2 Analysis of the first SNMP request

1. Analyze the first frame by describing details of the encoding mechanism at the application layer.
2. What is the purpose of this request?
3. Who generated this message?

3.2.3 Analysis of the SNMP answer

1. Subsequent to this first frame, a second frame is transmitted. Analyze it.
2. What kind of equipment was involved?
3. Considering this exchange, what do you think of SNMP's security?

3.2.4 Analysis of the second SNMP exchange

1. Having looked at the first exchange, now analyze the next frames that are exchanged.
2. Which new operation is carried out by this exchange? What does this type of request allow one to do?

3.2.5 Analysis of the following SNMP exchanges

1. Having looked at these two first exchanges, analyze the following exchanges.
2. Which mechanism has generated these exchanges?

3.2.6 Analysis of the last SNMP exchange

1. Analyse then the last frame sent by the client
2. Which new operation does this frame initiate? What does this kind of message enable?

3.2.7 Without the testbed...

If you need, you can download and analyze the trace `tme3-snm.dmp` (from the usual locations, see part 1.3.1) in order to answer the questions of Part 3.2.

4 Before leaving the room

- If you have saved some traces on the monitor VM, do not forget to transfer them back to your PPTI user account. Type the following command on a local terminal of the PPTI host: `scp etudiant@10.0.7.N2:<trace> <dest>`
- Before closing your connections to the virtual machines, be sure to restore them to the state in which you found them, removing any modifications you might have made.