# LINGI2141 - Individual Project Analysis of APT-GET

Benoît Baufays

Université Catholique de Louvain

**Abstract**

*This paper will deal with analysing the managing software apt-get wich are deployed on several linux distributions*

## I. Introduction

Apt-get is a software develloped for linux OS to centralize the management of your software. Apt-get install packages containing precompiled code, configuration files, and meta-information about the package. Because it is not very usefull to manage manually all your packages, apt-get was created. With him, you can update your system and yours packages but you can also install or remove packages. The utility of apt-get is the management of the dependencies and, with one program, you can maintain your system up to date.

## II. Apt-get

Apt-get have several commands, depending on what you want to do.

- update : with this command, apt-get search, on remotes servers, the last version for all packets. It get also the entire list of packets you can install via apt-get;

- upgrade or dist-upgrade : with this command, apt-get downloads packets installed on your system wich are to be updated. The difference between the command "upgrade" and "dist-upgrade" is that, whit hthe first, apt-get doesn't install new packages. For example, some packages must requires new dependencies. If you update with the first command, apt-get doesn't install new dependencies and, of course, doesn't update the packet. In other hand, with the second command, apt-get install all dependencies and update all packages;

- install : with this command, you can install new package. Apt-get search for dependencies and install the package and the required packages;

- remove : with this command, apt-get remove the package mentionned. It can also remove packages wich are not still required on your system. For example, if a package is only installed because it is a dependency for an other package and you remove this package, it is not require to have the dependency's package on your system.

Apt-get have several others command but the main has be presented below. To analyse how apt-get works and deal with network, we will use the same order presented in the list below. But, before, we discuss about the IPv 6 and apt-get.

## III. Apt-get and IPv6

To know where it must searching informations about packages, apt-get have one file "/etc/apt/sources.list" which contains addresses of servers. According to several bloggers, apt-get have some troubles with IPv6 because some servers have no Ipv6 address or the ISP doesn't support it.
To verify this information, we have used dig to send a DNS request to archive.ubuntu.com, the main server for every sources.

```
;; QUESTION SECTION:
;archive.ubuntu.com.            IN      AAAA

;; ANSWER SECTION:
archive.ubuntu.com.     425     IN      AAAA    2001:67c:1360:8c01::19
archive.ubuntu.com.     425     IN      AAAA    2001:67c:1360:8c01::1a
archive.ubuntu.com.     425     IN      AAAA    2001:67c:1360:8c01::22
archive.ubuntu.com.     425     IN      AAAA    2001:67c:1360:8c01::23
archive.ubuntu.com.     425     IN      AAAA    2001:67c:1360:8c01::15
archive.ubuntu.com.     425     IN      AAAA    2001:67c:1360:8c01::18
```

As we can see, archive.ubuntu.com have several IPv6 address, the problem do not come form that. When we go deeper in the code of apt-get, we see that some functionnalities are still using IPv4 libraries.

## IV. Apt-get analysis

# I. Update

### I.1 DNS Request

With this command, apt-get read first the file containing all server's name. With this information, it sends DNS request to know IP address of each server.

| | | |
|---|---|---|
| DNS | 79 | Standard query A security.ubuntu.com |
| DNS | 79 | Standard query A security.ubuntu.com |
| DNS | 73 | Standard query A dl.google.com |
| DNS | 77 | Standard query A ppa.launchpad.net |
| DNS | 77 | Standard query A extras.ubuntu.com |
| DNS | 79 | Standard query A toolbelt.heroku.com |
| DNS | 81 | Standard query A be.archive.ubuntu.com |
| DNS | 223 | Standard query response A 91.189.92.201 A 91.189.92.202 A 91.189.91.13 |
| DNS | 79 | Standard query A security.ubuntu.com |
| DNS | 223 | Standard query response A 91.189.92.190 A 91.189.92.200 A 91.189.92.201 |
| ICMP | 251 | Destination unreachable (Port unreachable) |
| DNS | 268 | Standard query response CNAME dl.l.google.com A 173.194.112.6 A 173.194 |
| DNS | 73 | Standard query A dl.google.com |
| DNS | 93 | Standard query response A 91.189.95.83 |

As we can see, Apt-get send first all his DNS requests before contacting servers. We see also that dl.google.com, an entry that we have added manually to access to packages from Google (GoogleTalk, ...) is, in reality, reachable via dl.l.google.com. Finally, we can see that apt-get send twice the DNS request about dl.google.com. It's not beacause it doesn't receive the response but because we have added twice this entry in the config file.
To test the DNS system, we have put manually a arbitrary IP address for the second DNS server. This test is visible in the schema below with the "Destination unreachable" message. After that, apt-get doesn't reuse this IP adress to send DNS query.
When we analysing packets receive by apt-get, we see that the time life of the information is 3 minutes 30. Also, we see that it receive more than one IP address for every server name. With this solution, apt-get doesn't want to resend a DNS query if a IP adress down. With multiple IP adresses, it can also use multi threading and request informations on multiple servers.

### I.2 Getting information

With the IP address, apt-get can now getting informations about packages. These informations are getting in two step.

| | | |
|---|---|---|
| HTTP | 574 | GET /skunk/pepper-flash/ubuntu/dists/precise/Release.gpg HTTP/1.1 GET /webupd8team/unstable/ubuntu/dists/precis |
| DNS | 79 | Standard query A toolbelt.heroku.com |
| DNS | 268 | Standard query response CNAME dl.l.google.com A 173.194.112.3 A 173.194.112.7 A 173.194.112.4 A 173.194.112.0 A |
| TCP | 74 | 33495 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=4294907300 TSecr=0 WS=128 |
| TCP | 74 | http > 37522 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1452 SACK_PERM=1 TSval=529080805 TSecr=4294907294 WS=25 |
| TCP | 66 | 37522 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=4294907301 TSecr=529080805 |
| HTTP | 300 | GET /ubuntu/dists/precise/Release.gpg HTTP/1.1 |
| DNS | 225 | Standard query response A 91.189.92.201 A 91.189.92.202 A 91.189.91.13 A 91.189.91.14 A 91.189.91.15 A 91.189.9 |
| TCP | 74 | 58406 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=4294907302 TSecr=0 WS=128 |
| TCP | 74 | http > 58404 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1452 SACK_PERM=1 TSval=515324992 TSecr=4294907298 WS=25 |
| TCP | 66 | 58404 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=4294907304 TSecr=515324992 |
| HTTP | 311 | GET /ubuntu/dists/precise-security/Release.gpg HTTP/1.1 |
| TCP | 66 | http > 39054 [ACK] Seq=1 Ack=509 Win=6912 Len=0 TSval=307927781 TSecr=4294907300 |
| HTTP | 353 | [TCP Previous segment lost] HTTP/1.1 304 Not Modified |
| TCP | 78 | [TCP Dup ACK 39#1] 39054 > http [ACK] Seq=509 Ack=1 Win=14720 Len=0 TSval=4294907309 TSecr=307927781 SLE=289 SR |
| HTTP | 354 | [TCP Out-Of-Order] HTTP/1.1 304 Not Modified |
| TCP | 66 | 39054 > http [ACK] Seq=509 Ack=576 Win=15744 Len=0 TSval=4294907309 TSecr=307927781 |
| HTTP | 331 | GET /skunk/pepper-flash/ubuntu/dists/precise/Release HTTP/1.1 |