Title: **Deliverable D4.3** **IPv6-IPv4 interoperability for eGoverment Cross-Border Services Scenarios**	**Document Version:** 1.0

Project Number: 297239	**Project Acronym:** GEN6	**Project Title:** Governments Enabled with IPv6

Contractual Delivery Date: 30/09/2014	**Actual Delivery Date:** 23/10/2014	**Deliverable Type* - Security**:** D – CO

* Type:	P - Prototype, R - Report, D - Demonstrator, O - Other
** Security Class:	PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible and Editor/Author: Antonio F. Gómez Skarmeta	**Organization:** UMU	**Contributing WP:** WP4

Authors (organisations):

Antonio Skarmeta (UMU), Pedro J. Fernández (UMU), Fernando Bernal Hidalgo (UMU), Gerold Gruber (Citkomm), Tassos Mavridis (Intelen), Carlos Gómez Muñoz (RedSARA), Steffen Konegen (FOKUS)

Abstract:

This deliverable performs a study of the behaviour of two different networks: GEANT and sTESTA. Also is tested the interoperability between IPv6 and IPv4 government networks.

Keywords:

IPv6, sTESTA, GEANT, tests, governments, IPsec, OpenVPN, Sensors

Revision History

The following table describes the main changes done in this document since its creation.

Revision	Date	Description	Author (Organization)
V0.1	30/09/2014	Document creation	Antonio F. Gómez Skarmeta (UMU)
V0.2	1/10/2014	UMU sections completed	Antonio F. Gómez Skarmeta (UMU)
V0.3	2/10/2014	UMU corrections	Antonio F. Gómez Skarmeta (UMU)
V0.4	8/10/2014	Citkomm add-ons	Gerold Gruber (Citkomm)
V0.5	8/10/2014	Intelen additions	Tassos Mavridis
V0.6	14/10/2014	Network configuration in Spanish side	Carlos Gómez Muñoz (RedSARA)
V0.7	17/10/2014	Some additions about German network side	Steffen Konegen
V1.0	20/10/2014	Document reviewed and closed	Antonio F. Gómez Skarmeta (UMU)

Disclaimer

The GEN6 project (number 261584) is co-funded by the European Commission under the ICT Policy Support Programme (PSP) as part of the Competitiveness and Innovation framework Programme (CIP). This document contains material that is the copyright of certain GEN6partners and the EC, and that may be shared, reproduced or copied "as is", following the Creative Commons "Attribution-NonCommercial-NoDerivs 3.0 Unported (CC BY-ND-NC 3.0) licence. Consequently, you're free to share (copy, distribute, transmit) this work, but you need to respect the attribution (respecting the project and authors names, organizations, logos and including the project web site URL "http://www.gen6-project.eu"), for non-commercial use only, and without any alteration, transformation or build upon this work.

The information herein does not necessarily express the opinion of the EC. The EC is not responsible for any use that might be made of data appearing herein. The GEN6 partners do not warrant that the information contained herein is capable of use, or that use of the information is free from risk, and so do not accept liability for loss or damage suffered by any person using this information.

Executive Summary

Governments of the EU have each one its own national network to deal with its daily duty to serve its citizens. But there are joint objectives that all the European countries need a better interconnection of their networks. This interconnection can be achieved in two ways: through public or otherwise accessible networks (see below), or through the secure and isolated government networks.

For the first case, the GEANT [Geant] network was designed for the purpose to interconnect European Institutions, Research Institutes and Universities. It is a high capacity network with enough resources to satisfy the Governments needs in addition to its primary purpose.

For the second case, the sTESTA [sTESTA] network was created to interconnect internally all the existing government networks. All these networks are isolated and not accessible via the Internet due to security reasons.

In this deliverable we will try to find the pros and cons of both cases and analyse which is the best option, taking into account security, reliability and throughput.

For this purpose, a batch of tests has been performed through both networks using IPv6 and protocols like TCP, UDP and ICMP. These tests will also show us the current state of them.

Also the services deployed in these networks are very important. This deliverable centres its focus on an authentication service that uses STORK, an identification service of the EU. Some tests have been performed over the web servers that host these services.

Table of contents

Table of figures

Table Index

1 INTRODUCTION

1.1 Purpose of the deliverable

The purpose of this deliverable is to show the performance of the GEANT and sTESTA networks, compare them and reach conclusions for future works.

GEANT and sTESTA is going to be the target of a batch of performance tests. The objective of these tests is to find out the pros and cons of each network and see, which is the best to fit the communication needs of different European Governments.

Also the services deployed in these networks are very important. This deliverable centres its focus on an authentication service that uses STORK, an identification service of the EU. Some tests have been performed over the web servers that host these services.

2 COMMUNICATION INFRASTRUCTURE

2.1 GÉANT and sTESTA

GÉANT and sTESTA are two very different networks. The first one, GÉANT is the pan-European data network for the research and education community. It interconnects national research and education networks (NRENs) across Europe, enabling collaboration on projects ranging from biological science to earth observation and arts & culture. The GÉANT project combines a high-bandwidth, high-capacity 50,000 km network with a growing range of services. These allow researchers to collaborate, working together wherever they are located. Services include identity and trust, multi-domain monitoring perfSONAR MDM, dynamic circuits and roaming via the Eduroam service. GÉANT supported native IPv6 since 2002 and multicast IPv6 since 2004.In 2013 a substantial network migration program was completed, meaning users could be offered multiple 100 Gbit/s links, with the core network supporting 500 Gbit/s and a network design that will support up to 8 Tbit/s.

The second one, sTESTA, is the European Community's own private, IP-based network. sTESTA offers a telecommunications interconnection platform that responds to the growing need for secure information exchange between European public administrations. It is a European IP network, similar to the Internet in its universal reach, but dedicated to inter-administrative requirements and providing guaranteed performance levels. sTESTA aims to provide telecommunication services for data exchanges required for the implementation of European policy. sTESTA is a network of networks, composed of the EuroDomain backbone and Local Domain networks. Local Domains can be national or regional networks, European Institutions or Agencies. The EuroDomain is a European backbone network for administrative data exchanges acting as a network communication platform between local administrations. This allows any site connected to EuroDomain to communicate with any other linked site. The EuroDomain is totally isolated from the public Internet. This guarantees restricted access as only administrations may access the EuroDomain. Security is also enhanced by the implementation of IPSEC technology to prevent eavesdropping and advanced encryption mechanisms. The sTESTA domain-based approach allows national administrations to connect to European information sources while maintaining national autonomy in network implementation. sTESTA supports native IPv4 since its creation, but does not support IPv6 currently.

2.2 Configuration details

2.2.1 Spanish side

In order to enable the UMU network to communicate with FOKUS network via sTESTA, some links between other networks like RedIRIS [Rediris](the Spanish academic and research network, which UMU is connected to) and RedSARA [Redsara](the Spanish administrations network with connection to sTESTA also) should be configured. In the Figure 1 a network schema of the Spanish side can be seen.

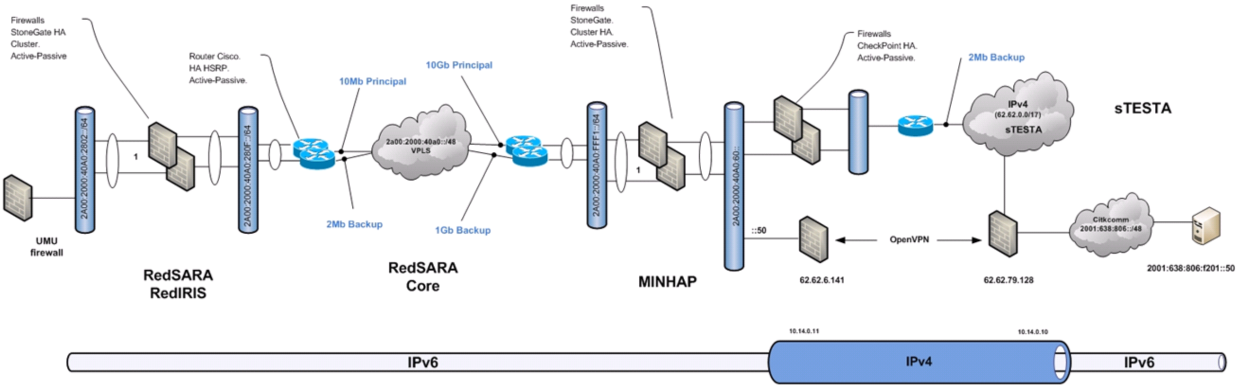
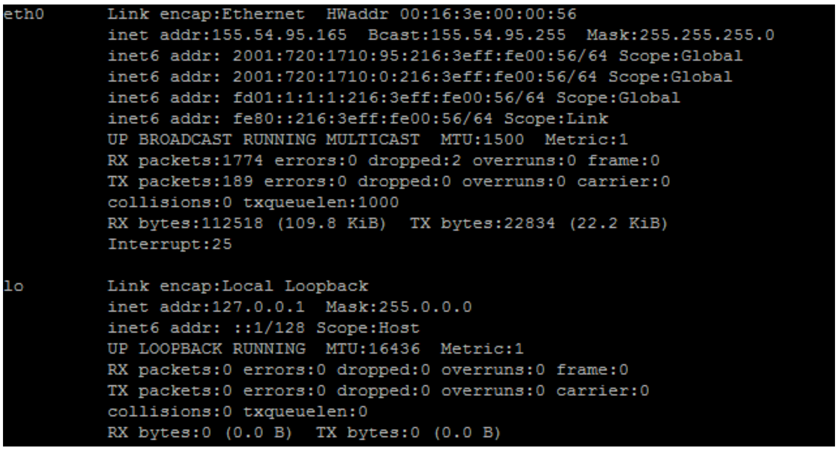


Figure 1 - Network schema to connect UMU with RedSARA

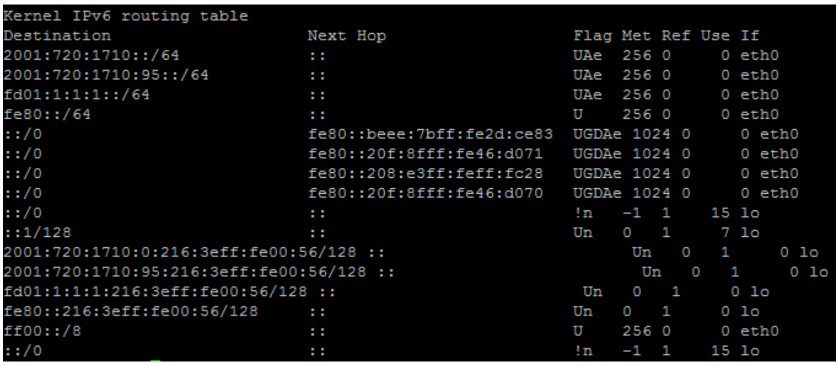
The UMU machine has two possible configurations. One connected to GEANT (Figure 2 and Figure 3), and another one connected to sTESTA (Figure 4 and Figure 5). It uses different interfaces to connect to each network. For the GEANT case, the computer auto-configures its IPv6 address when receives the router advertisement messages. There are several routers available, so it has more than one IPv6 address.



```
eth0      Link encap:Ethernet  HWaddr 00:16:3e:00:00:56
          inet addr:155.54.95.165  Bcast:155.54.95.255  Mask:255.255.255.0
          inet6 addr: 2001:720:1710:95:216:3eff:fe00:56/64 Scope:Global
          inet6 addr: 2001:720:1710:0:216:3eff:fe00:56/64 Scope:Global
          inet6 addr: fd01:1:1:1:216:3eff:fe00:56/64 Scope:Global
          inet6 addr: fe80::216:3eff:fe00:56/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1774 errors:0 dropped:2 overruns:0 frame:0
          TX packets:189 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:112518 (109.8 KiB)  TX bytes:22834 (22.2 KiB)
          Interrupt:25

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

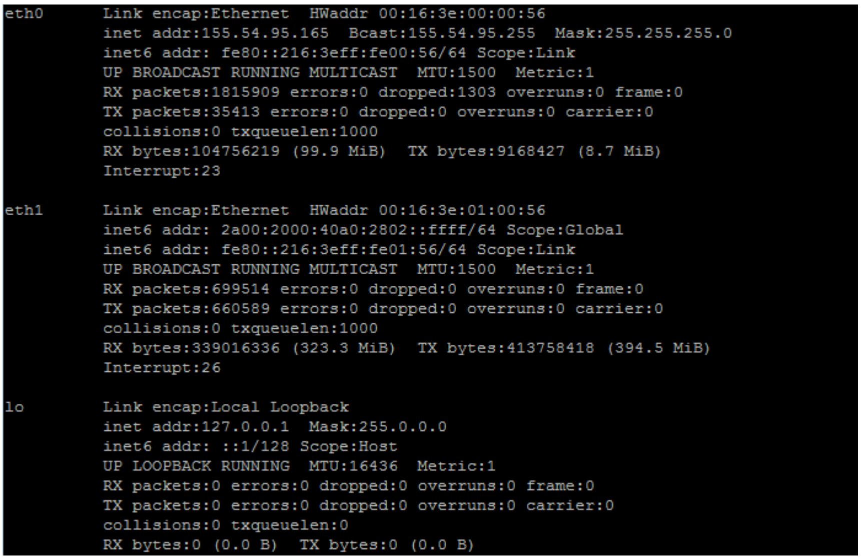
Figure 2 - IPv6 configuration in the UMU machine in GEANT mode



```
Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref Use If
2001:720:1710::/64             ::                         UAe  256 0      0 eth0
2001:720:1710:95::/64          ::                         UAe  256 0      0 eth0
fd01:1:1:1::/64                ::                         UAe  256 0      0 eth0
fe80::/64                      ::                         U    256 0      0 eth0
::/0                           fe80::beee:7bff:fe2d:ce83  UGDAe 1024 0      0 eth0
::/0                           fe80::20f:8fff:fe46:d071   UGDAe 1024 0      0 eth0
::/0                           fe80::208:e3ff:feff:fc28   UGDAe 1024 0      0 eth0
::/0                           fe80::20f:8fff:fe46:d070   UGDAe 1024 0      0 eth0
::/0                           ::                         !n   -1  1     15 lo
::1/128                        ::                         Un   0   1      7 lo
2001:720:1710:0:216:3eff:fe00:56/128 ::                         Un   0   1      0 lo
2001:720:1710:95:216:3eff:fe00:56/128 ::                         Un   0   1      0 lo
fd01:1:1:1:216:3eff:fe00:56/128 ::                          Un   0   1      0 lo
fe80::216:3eff:fe00:56/128     ::                         Un   0   1      0 lo
ff00::/8                       ::                         U    256 0      0 eth0
::/0                           ::                         !n   -1  1     15 lo
```

Figure 3- Routing configuration in the UMU machine in GEANT mode

In order to keep the sTESTA network isolated from the Internet, and of course from GEANT, the interface eth0 is only used for IPv4 communication that allow us to connect with it from the UMU network. It can be seen in Figure 4. The eth1 is only configured with an IPv6 address, so there is no possible communication with the Internet form sTESTA side. Indeed, the forwarding capabilities of the machine have been disabled.

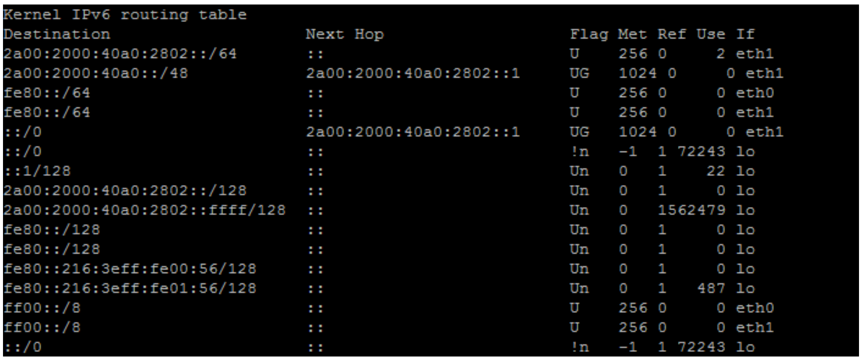


```
eth0      Link encap:Ethernet  HWaddr 00:16:3e:00:00:56
          inet addr:155.54.95.165  Bcast:155.54.95.255  Mask:255.255.255.0
          inet6 addr: fe80::216:3eff:fe00:56/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1815909 errors:0 dropped:1303 overruns:0 frame:0
          TX packets:35413 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:104756219 (99.9 MiB)  TX bytes:9168427 (8.7 MiB)
          Interrupt:23

eth1      Link encap:Ethernet  HWaddr 00:16:3e:01:00:56
          inet6 addr: 2a00:2000:40a0:2802::ffff/64 Scope:Global
          inet6 addr: fe80::216:3eff:fe01:56/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:699514 errors:0 dropped:0 overruns:0 frame:0
          TX packets:660589 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:339016336 (323.3 MiB)  TX bytes:413758418 (394.5 MiB)
          Interrupt:26

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Figure 4- IPv6 configuration in the UMU machine in sTESTA mode



```
Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref Use If
2a00:2000:40a0:2802::/64       ::                         U    256 0     2 eth1
2a00:2000:40a0::/48            2a00:2000:40a0:2802::1     UG   1024 0     0 eth1
fe80::/64                      ::                         U    256 0     0 eth0
fe80::/64                      ::                         U    256 0     0 eth1
::/0                           2a00:2000:40a0:2802::1     UG   1024 0     0 eth1
::/0                           ::                         !n   -1  1 72243 lo
::1/128                        ::                         Un   0   1    22 lo
2a00:2000:40a0:2802::/128      ::                         Un   0   1     0 lo
2a00:2000:40a0:2802::ffff/128  ::                         Un   0   1562479 lo
fe80::/128                     ::                         Un   0   1     0 lo
fe80::/128                     ::                         Un   0   1     0 lo
fe80::216:3eff:fe00:56/128     ::                         Un   0   1     0 lo
fe80::216:3eff:fe01:56/128     ::                         Un   0   1   487 lo
ff00::/8                       ::                         U    256 0     0 eth0
ff00::/8                       ::                         U    256 0     0 eth1
::/0                           ::                         !n   -1  1 72243 lo
```

Figure 5- Routing configuration in the UMU machine in sTESTA mode

2.2.1.1 Connectivity RedSARA – RedIRIS

RedSARA (SARA network) has communication equipment and network and security services in RedIRIS premises, which protect and provide connectivity to all the entities belonging to RedIRIS, among them the University of Murcia (UMU). All the elements that provide these services are located in a single rack, known as Connection Area.

Among the systems that provide connectivity and security services, there are two firewalls StoneGate 5.3.3 running on Intel platforms, configured in high availability. High availability is also configured in the rest of the elements of the Connection Area (switches, routers, servers and communication links).

Regarding the communication links, the throughput is 10 Mb for the main line, and 2Mb for the backup line.

Regarding the routers, they are Cisco routers, with:

- IOS Software, 2800 in the main router,
- Cisco IOS Software, C180X Software (C180X-ADVIPSERVICESK9-M), Version 12.4(24)T1, in the backup router, with ROM: System Bootstrap, Version 12.3(8r)YH9, RELEASE SOFTWARE (fc1)

All the communication and security elements in the Connection Area have native IPv6.

2.2.1.2 Connectivity MINHAP – sTESTA

This environment has two security levels. The Open VPN tunnel server is protected by two firewalls configured in high availability. One of the firewalls protects the VPN server from the Red SARA [Redsara] environment and the other from the sTESTA environment.

Red SARA environment is composed of three firewalls StoneGate version 5.3.3 in high availability, whereas sTESTA environment is composed of three firewalls CheckPoint R77.20 also in high availability. All the nodes in the high availability clusters have level 2 redundancy (switch level) by means of Cisco stacks.

sTESTA has its own Connection Area, known as TAP, where the communication and encryption elements are located. Regarding communications, the link has a throughput of 2Mb. All the elements of the TAP are configured in high availability: level 2, level 3 and power supply.

The elements that provide connectivity in the sTESTA TAP are:

Name / Function	TAP component (2Mbps)
TAP	**TAP-sTesta-2Mb-E1**
CE Routers	**2x Cisco 1841 + WIC-1T**
Layer 2 switches	**6x Cisco2940**
Encryption device	**2x SINA box 4L**
SLA probe	**1x Cisco 1841**
UPS	**2x Pulsar 1500**
Firewall	**2x Juniper SSG-5**

Table 1 - TAP Components for the sTESTA connectivity

The encryption devices are SECUNET SINA Boxes which specifications are:

Security standards

- RFC 2104 (HMAC)
- RFC 2367 (PFKey)
- RFC 2401-2412 (IPsec)
- RVD 2459 (X509v3)
- RVD 2510/2511 (CMP)
- ISO/IEC 15946-2 (EC-GDSA)

Internet protocol standards

- IP: v4, v6, v4/v6- and v6/v4-tunnelling
- Quality of Service (QoS): QoS DiffServ Code Points (DSCP), bandwidth management for each security relation

Software-based encryption performance

- data throughput depending on: packet size, processor clock rate, number of processors, crypto methods, key length
- Number of active tunnels: depending on memory size

Certificates

- Structure: X509v3 (IPsec/PKIX profile)
- Management protocol: CMP
- Attribute Certificate: X.501/RFC 3281; clearance / category

Approvals

- BSI (Germany): VS-NfD, VS-Vertraulich, Geheim, Streng Geheim
- NATO: NATO SECRET (NATO approval for national use), EU SECRET

2.2.1.3 OpenVPN server environment

The firewall that performs the functions of establishing the “IPv6 in IPv4” tunnel is a Linux CentOS 6.5 devoted exclusively to the OpenVPN [OpenVPN] service. The version is OpenVPN 2.3.2.

```
OpenVPN 2.3.2 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [eurephia] [MH]
[IPv6] built on Sep 12 2013
Originally developed by James Yonan
Copyright (C) 2002-2010 OpenVPN Technologies, Inc. <sales@openvpn.net>
Compile time defines: enable_crypto=yes enable_debug=yes enable_def_auth=yes
enable_dlopen=unknown enable_dlopen_self=unknown enable_dlopen_self_static=unknown
enable_eurephia=yes enable_fast_install=yes enable_fragment=yes enable_http_proxy=yes
enable_iproute2=yes enable_libtool_lock=yes enable_lzo=yes enable_lzo_stub=no
enable_management=yes enable_multi=yes enable_multihome=yes enable_pam_dlopen=no
enable_password_save=yes enable_pedantic=no enable_pf=yes enable_pkcs11=yes
enable_plugin_auth_pam=yes enable_plugin_down_root=yes enable_plugins=yes enable_port_share=yes
enable_pthread=yes enable_selinux=no enable_server=yes enable_shared=yes
enable_shared_with_static_runtimes=no enable_small=no enable_socks=yes enable_ssl=yes
enable_static=yes enable_strict=no enable_strict_options=no enable_systemd=no
enable_win32_dll=yes enable_x509_alt_username=yes with_crypto_library=openssl with_gnu_ld=yes
with_iproute_path=/sbin/ip with_mem_check=no with_plugindir='$(libdir)/openvpn/plugins'
with_sysroot=no
```

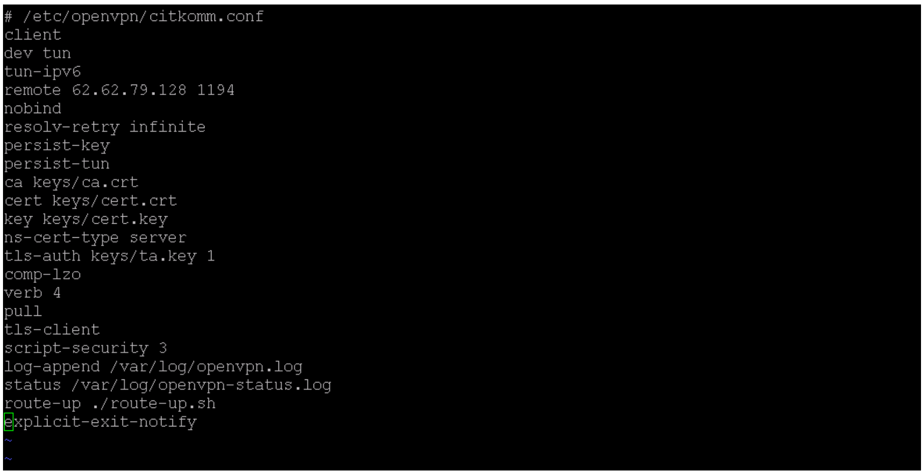
It has a Gigabit network interface:

```
1: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP>mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:50:56:bd:98:03 brd ff:ff:ff:ff:ff:ff
    inet 62.62.6.141/32 scope global eth0
    inet6 2a00:2000:40a0:60::50/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:febd:9803/64 scope link
       valid_lft forever preferred_lft forever
13: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP>mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 100
    link/[65534]
    inet 10.14.0.11 peer 10.14.0.10/32 scope global tun0
    inet6 fdb4:c127:dfb3::11/64 scope global
       valid_lft forever preferred_lft forever
```

During all the testing phase, the firewall has not reported any problem that can impact communication performance, neither at network interface level nor at OpenVPN application level.

```
Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500   0 44890985      0      0      0 43193617      0      0      0 BMRU
lo        16436   0      100      0      0      0      100      0      0      0 LRU
tun0       1500   0    42331      0      0      0    21249      0      0      0 MOPRU
```

The current configuration of the OpenVPN service is the following:



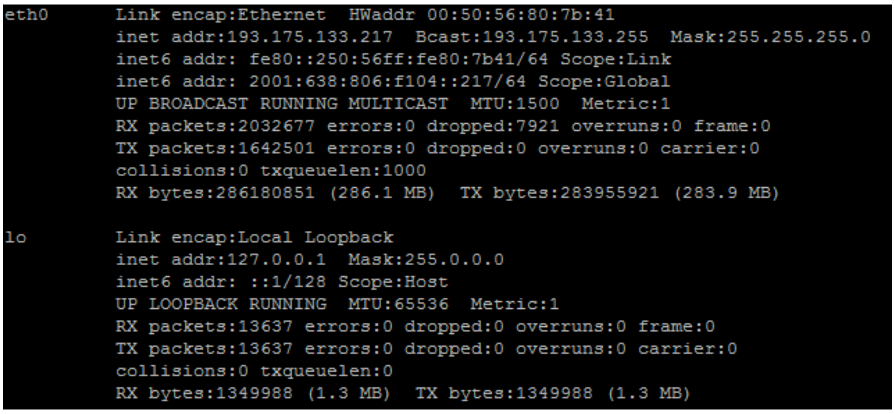
```
# /etc/openvpn/citkomm.conf
client
dev tun
tun-ipv6
remote 62.62.79.128 1194
nobind
resolv-retry infinite
persist-key
persist-tun
ca keys/ca.crt
cert keys/cert.crt
key keys/cert.key
ns-cert-type server
tls-auth keys/ta.key 1
comp-lzo
verb 4
pull
tls-client
script-security 3
log-append /var/log/openvpn.log
status /var/log/openvpn-status.log
route-up ./route-up.sh
explicit-exit-notify
~
~
```

Figure 6 - OpenVPN configuration in Spanish side

2.2.2 German side

On the German side two project partners take part in the tests, too. Citkomm as municipal data centre is connected to the national governmental network DOI. And it has already a tunnel based IPv6 connection to the FOKUS IPv6 testbed from the activities in WP3.

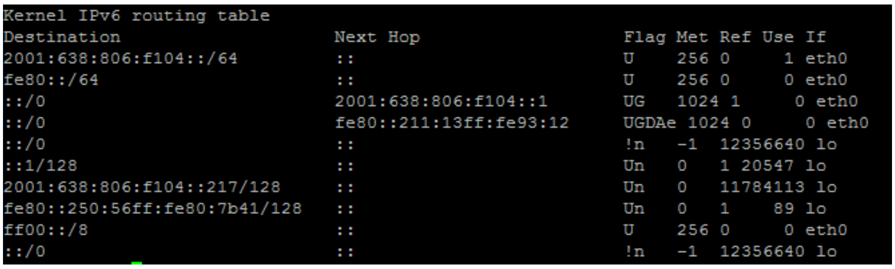
In FOKUS network, in Germany, there are two clones of the same machine, one connected to GEANT (Figure 7 and Figure 8), and the other one to sTESTA network (Figure 9 and Figure 10).



```
eth0      Link encap:Ethernet  HWaddr 00:50:56:80:7b:41
          inet addr:193.175.133.217  Bcast:193.175.133.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe80:7b41/64 Scope:Link
          inet6 addr: 2001:638:806:f104::217/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2032677 errors:0 dropped:7921 overruns:0 frame:0
          TX packets:1642501 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:286180851 (286.1 MB)  TX bytes:283955921 (283.9 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:13637 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13637 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1349988 (1.3 MB)  TX bytes:1349988 (1.3 MB)
```

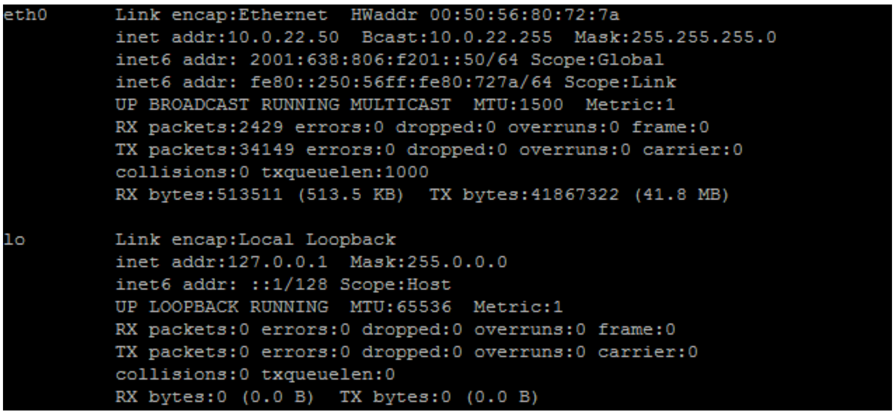
Figure 7 -IPv6 configuration in the FOKUS machine connected to GEANT network



```
Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref Use If
2001:638:806:f104::/64         ::                         U    256 0     1 eth0
fe80::/64                      ::                         U    256 0     0 eth0
::/0                           2001:638:806:f104::1       UG   1024 1     0 eth0
::/0                           fe80::211:13ff:fe93:12     UGDAe 1024 0     0 eth0
::/0                           ::                         !n   -1  12356640 lo
::1/128                        ::                         Un   0   1 20547 lo
2001:638:806:f104::217/128     ::                         Un   0   11784113 lo
fe80::250:56ff:fe80:7b41/128   ::                         Un   0   1    89 lo
ff00::/8                       ::                         U    256 0     0 eth0
::/0                           ::                         !n   -1  12356640 lo
```

Figure 8 -Routing configuration in the FOKUS machine connected to GEANTnetwork

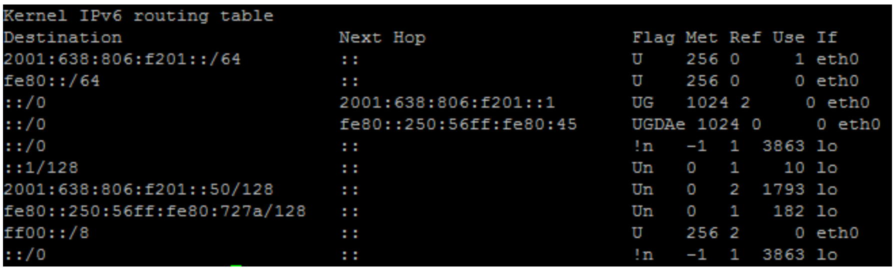
In this way we avoid the GEANT and sTESTA interconnection, due to sTESTA must be isolated. Between these machines no communication is possible.



```
eth0      Link encap:Ethernet  HWaddr 00:50:56:80:72:7a
          inet addr:10.0.22.50  Bcast:10.0.22.255  Mask:255.255.255.0
          inet6 addr: 2001:638:806:f201::50/64 Scope:Global
          inet6 addr: fe80::250:56ff:fe80:727a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2429 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34149 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:513511 (513.5 KB)  TX bytes:41867322 (41.8 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Figure 9 - IPv6 configuration in the FOKUS machine connected to sTESTA network



```
Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref Use If
2001:638:806:f201::/64         ::                         U    256 0     1 eth0
fe80::/64                      ::                         U    256 0     0 eth0
::/0                           2001:638:806:f201::1       UG   1024 2     0 eth0
::/0                           fe80::250:56ff:fe80:45     UGDAe 1024 0     0 eth0
::/0                           ::                         !n   -1  1  3863 lo
::1/128                        ::                         Un   0   1    10 lo
2001:638:806:f201::50/128      ::                         Un   0   2  1793 lo
fe80::250:56ff:fe80:727a/128   ::                         Un   0   1   182 lo
ff00::/8                       ::                         U    256 2     0 eth0
::/0                           ::                         !n   -1  1  3863 lo
```

Figure 10 - Routing configuration in the FOKUS machine connected to sTESTA network

The server is located in the testbed which was used for the WP3 pilot tests before. It uses the existing connection to Citkomm, which is then connected with the Spanish partners via a trans-sTESTA OpenVPN tunnel to Red SARA.

The first machine was directly connected to the internet and accessible from the GEANT network. The second machine is a clone from the first one and connected to the Fokus IPv6 testbed and only available from the sTESTA network. The machines are an Ubuntu 12.04 LTS server (32 Bit). It has 4GB memory, 2vCPUs and 25GB HDD. The virtual network card is a 1000 Gbit/s NIC, but the connection to the DFN Network is limited to 350 Mbit/s.

2.3 IPv6 support

GEANT network natively supports IPv6, but this is not the case of sTESTA network, which only supports IPv4. In order to overcome this lack and interconnect the IPv6 networks that are present in each country we can use OpenVPN [OpenVPN] tunnels. Here we can illustrate the Spanish-German example shown in the Figure 11. RedSARA is the internal national network to interconnect Spanish public administration services and European Institutions. In Germany is the DOI network in charge of all of these duties. Inside of these networks are two institutions: MINHAP (Ministerio de Hacienda y Administración Pública) in the Spanish side, and Citkomm [Citkomm] in the German side.

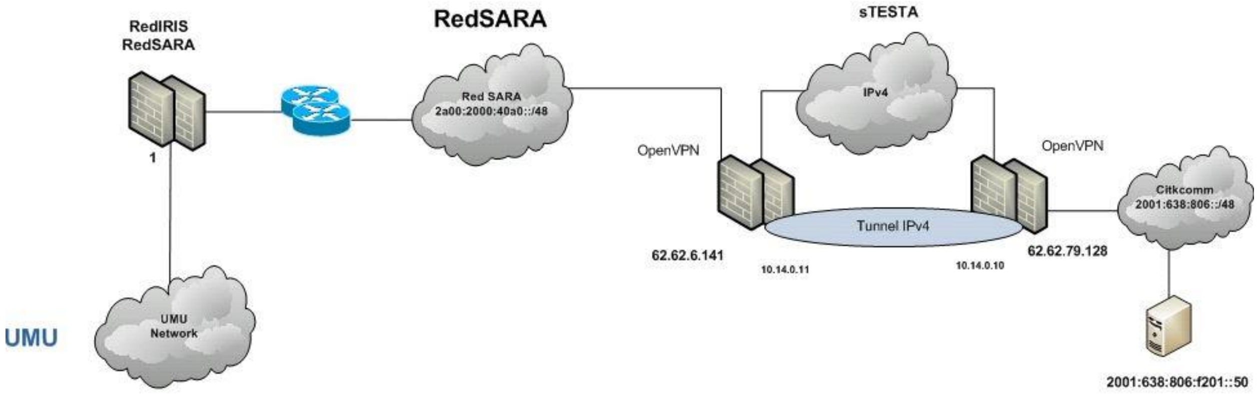


Figure 11- UMU and FOKUS interconnection scenario via sTESTA

The sTESTA network interconnects them using IPv4 based protocols. As IPv6 is not supported at this point, it is necessary the usage of OpenVPN tunnels to let the IPv6 traffic flow between those networks. In Figure 12 and Figure 13 is depicted the tunnel schema used in this case.

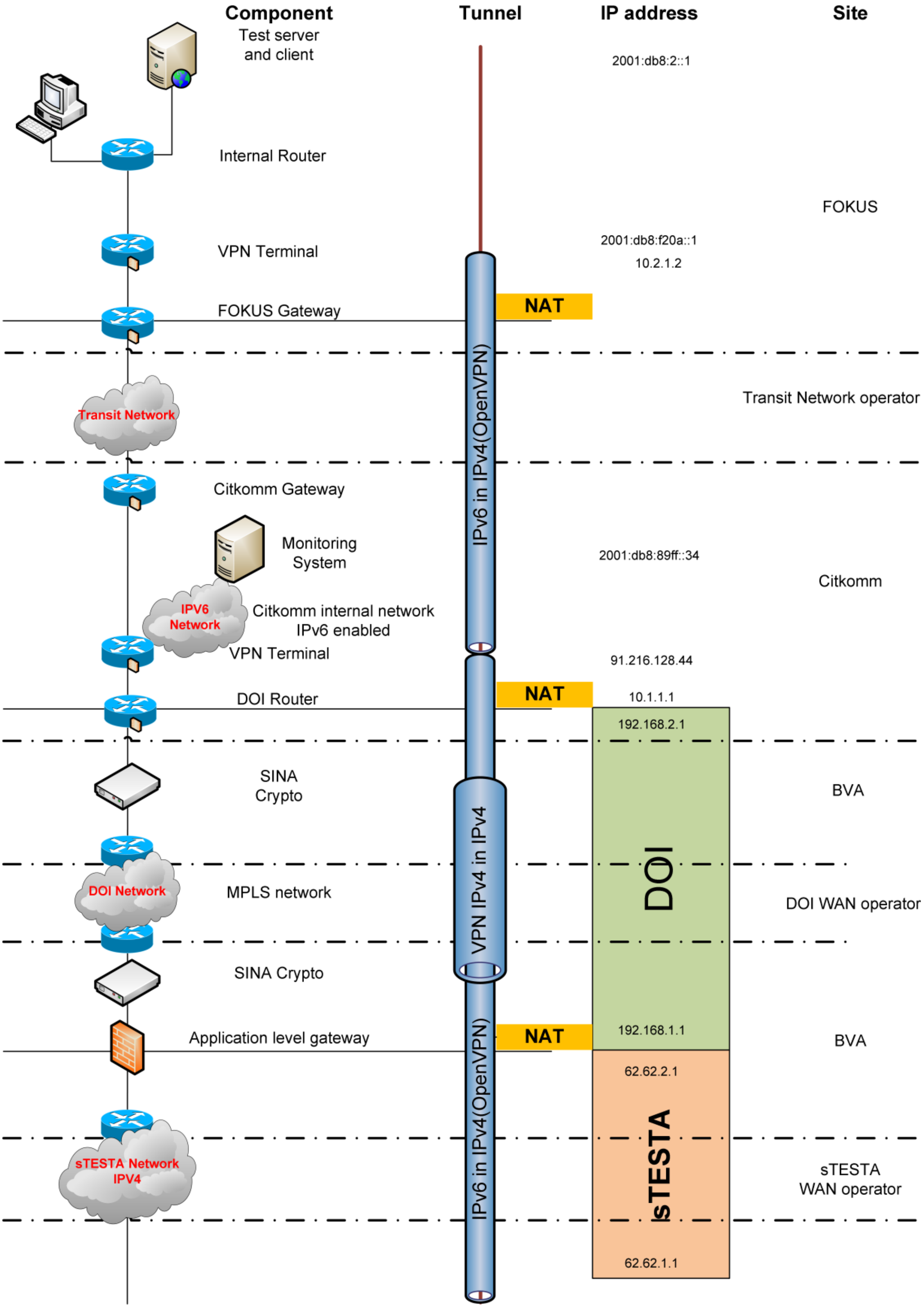


Figure 12- OpenVPN tunnel schema, German part

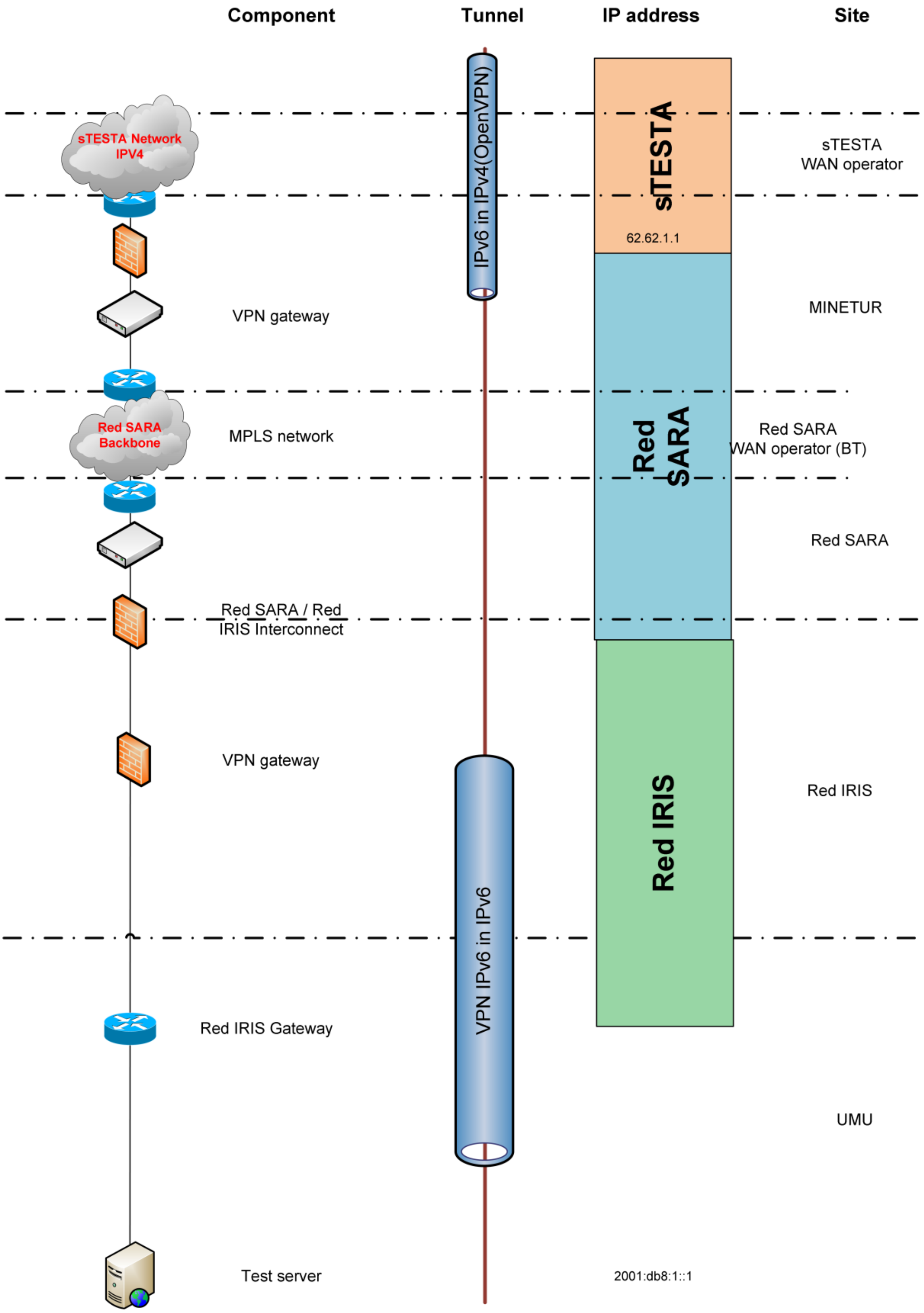


Figure 13 - OpenVPN tunnel schema, Spanish part

3 TESTING INFRASTRUCTURE

In order to test the performance of the networks under study, a set of tests have been developed in order to be executed sequentially and during a whole day. The test is repeated every hour during a day. The tests are performed between two machines, one in UMU network and the other one in the FOKUS network. The UMU machine is named as "A" machine, and "B" machine for the FOKUS one. The test is divided in the following parts, each one lasting 5 minutes:

- TCP traffic generated with "iperf" from A to B
- TCP traffic generated with "iperf" from B to A
- TCP traffic generated with "iperf" from A to B and form B to A simultaneously
- UDP traffic generated with "iperf" from A to B at 1 Mbps of bitrate
- UDP traffic generated with "iperf" from B to A at 1 Mbps of bitrate
- UDP traffic generated with "iperf" from A to B and form B to A simultaneously at 1 Mbps of bitrate
- Ping between A to B every second (300 pings)
- Ping between B to A every second (300 pings)

In this way we can see the behaviour of the network during a whole day and gather enough data to show accurate results.

3.1 GEANT tests

3.1.1 TCP results

The TCP test is divided in 3 parts. The first one is the test performed by "iperf" [Iperf] sending traffic from A to B and evaluates what is the maximum bandwidth that the link can support. First, in Figure 14 is shown the results of a single test, and we can appreciate that the value of maximum bandwidth is almost constant between 90 and 100 Mbps. In the Figure 15 are shown the same test but in a whole day, in order to see if the time could influence the results. But the results show that the time does not affect the values of maximum bandwidth using TCP protocol.

The second part is the opposite test, from B to A, shown in Figure 16 and Figure 17. The results are very similar. This and the previous test show that the network is not used as much as it could. There is no rush hour and no degradation of the performance is detected during a whole day.

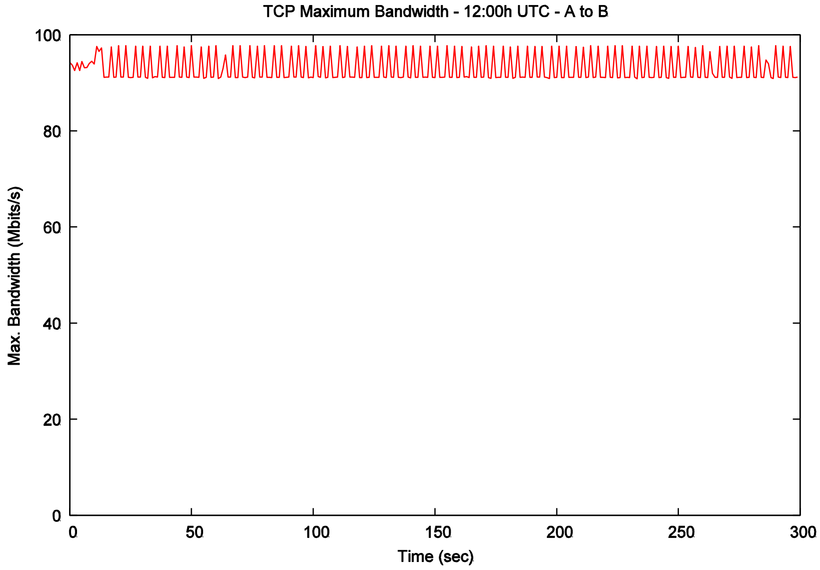


Figure 14 - TCP Maximum Bandwidth from A to B

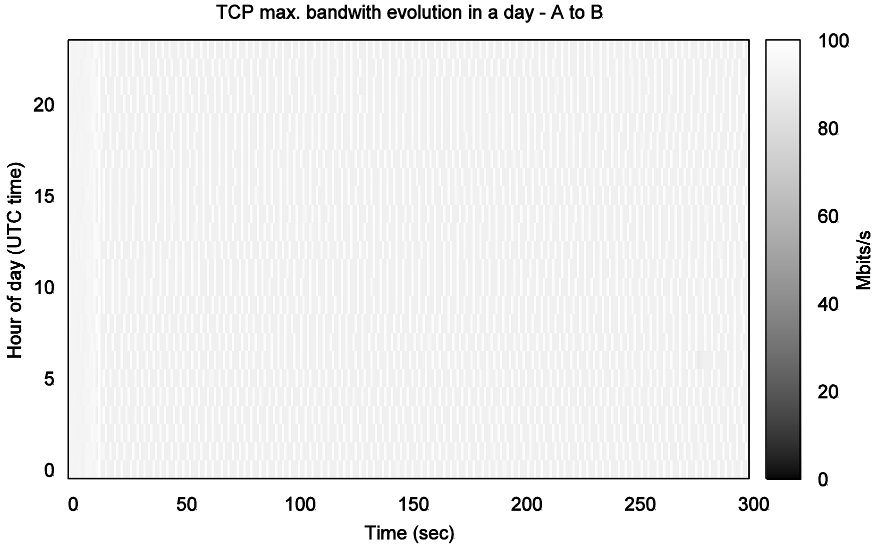


Figure 15 - TCP maximum bandwidth evolution in a day from A to B

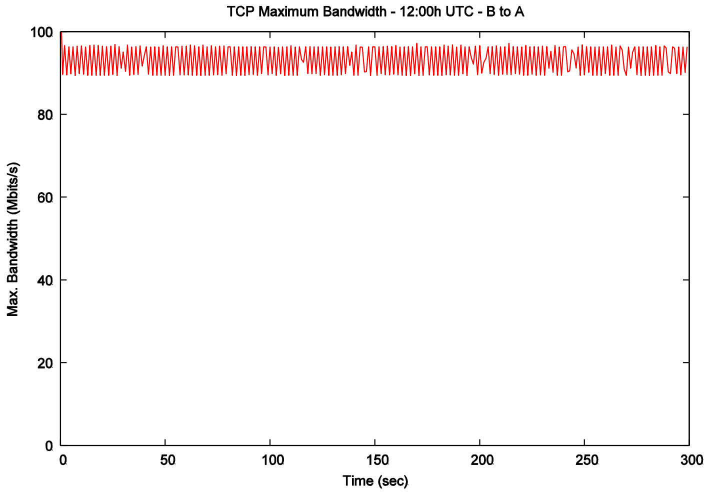


Figure 16 - TCP Maximum Bandwidth form B to A

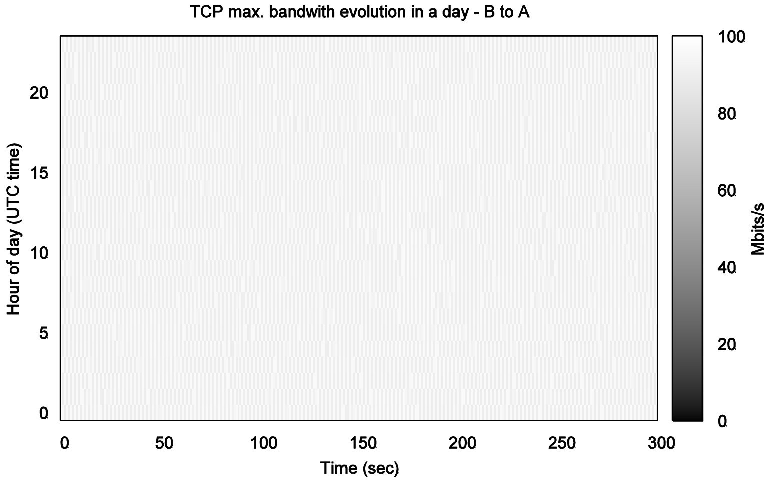


Figure 17 - TCP maximum bandwidth evolution in a day from B to A

The third part of the TCP test is to perform the previous two tests simultaneously to see if the network is or not full-duplex, and if the link performance in one direction is affected if the link in the other direction is being used at the same time. The Figure 18 shows a single test. We can appreciate a “slow-start” mechanism implemented by TCP protocol in the traffic that goes from A to B, but it does not appear in the B to A one. The only one conclusion that we can reach is that the link is of course full-duplex, but the way each endpoint manages the TCP protocol is different. The TCP maximum bandwidth values reached in this test is a bit lower, but with a wider oscillation from 70 to 95 Mbps. It is an expected result because the TCP ACK messages are always sent in the opposite direction, using part of the bandwidth that cannot be used to send data. In Figure 19 and Figure 20 we can appreciate the behaviour of the network during a day, and we can conclude that there are no important changes. Only the oscillation of the values is different at some hours of the day, but this has not the enough importance to be taken into account.

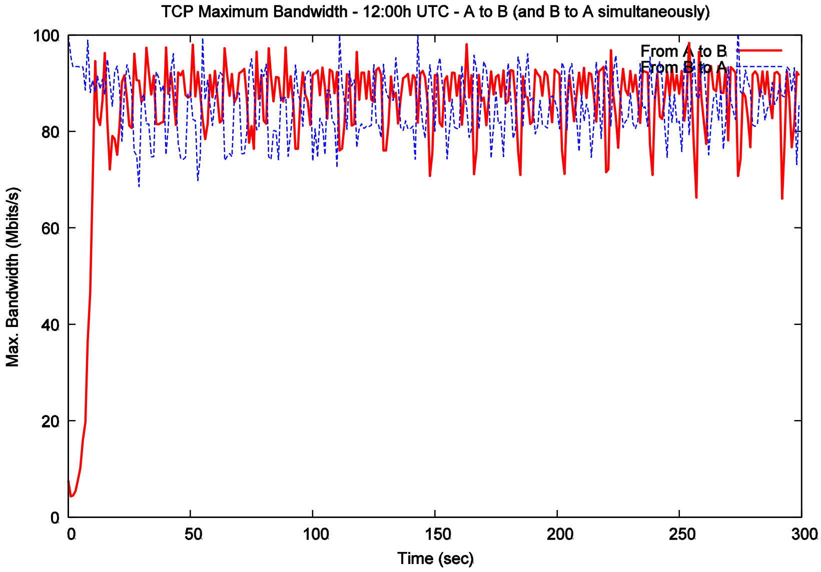


Figure 18 - TCP maximum bandwidth from A to B and B to A

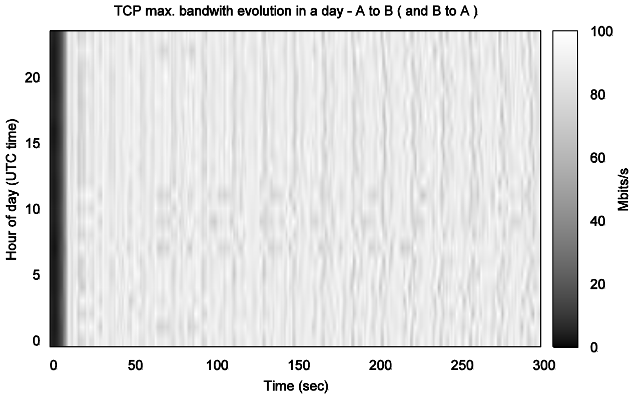


Figure 19 - TCP maximum bandwidth evolution in a day from A to B

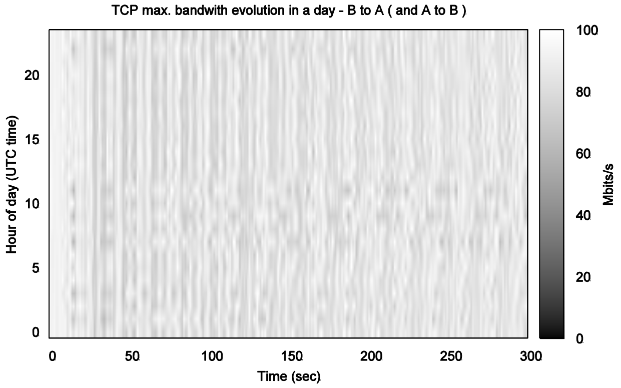


Figure 20 - TCP maximum bandwidth evolution in a day from B to A

As a summary of the tests, the Figure 21 and Figure 22 shows the mean values of the TCP maximum bandwidth during a whole day, that are almost the same in both directions.

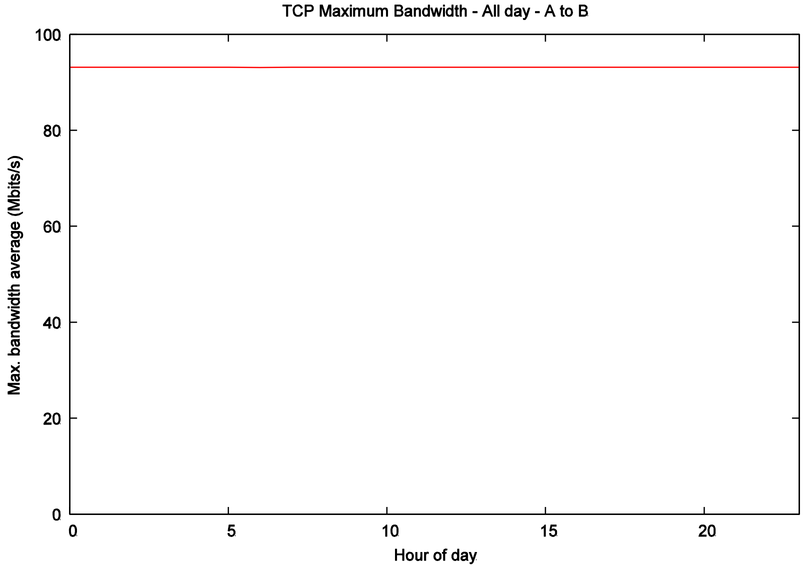


Figure 21 - Mean values of TCP maximum bandwidth from A to B during a day

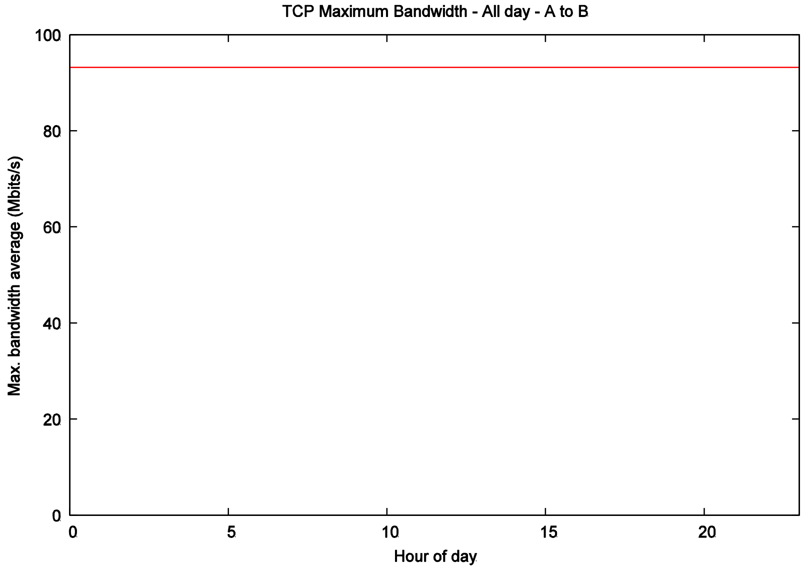


Figure 22 - Mean values of TCP maximum bandwidth from B to A during a day

3.1.2 UDP results

The UDP test is also divided in 3 parts. In the first part we use “iperf” tool to generate a 1 Mbps constant bit-rate flow from A to B. The second part the same but from B to A. And the last one both flows in both directions. This is a speed is far of the limit of the network. We are interested here in the Packet Delivery Ratio (PDR %), in other words, the percentage of packets that reach its destination. As can be seen Figure 23, the UDP transmission is performed perfectly, without packet loss, so the PDR is always 100%. Also if we perform the same test along a day we get the same result, as can be seen in Figure 24.

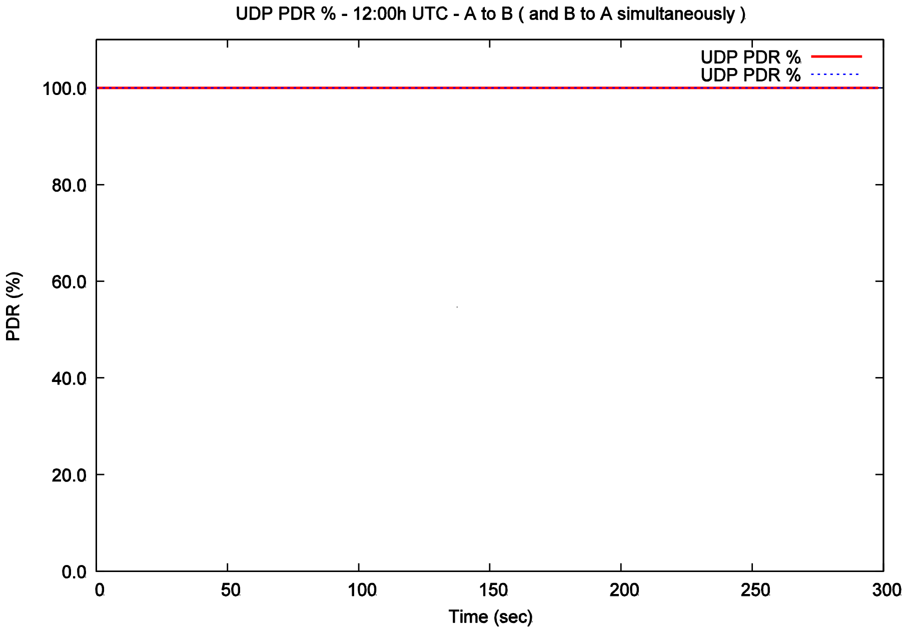


Figure 23 - Simple UDP test from A to B and B to A at 1 Mbps

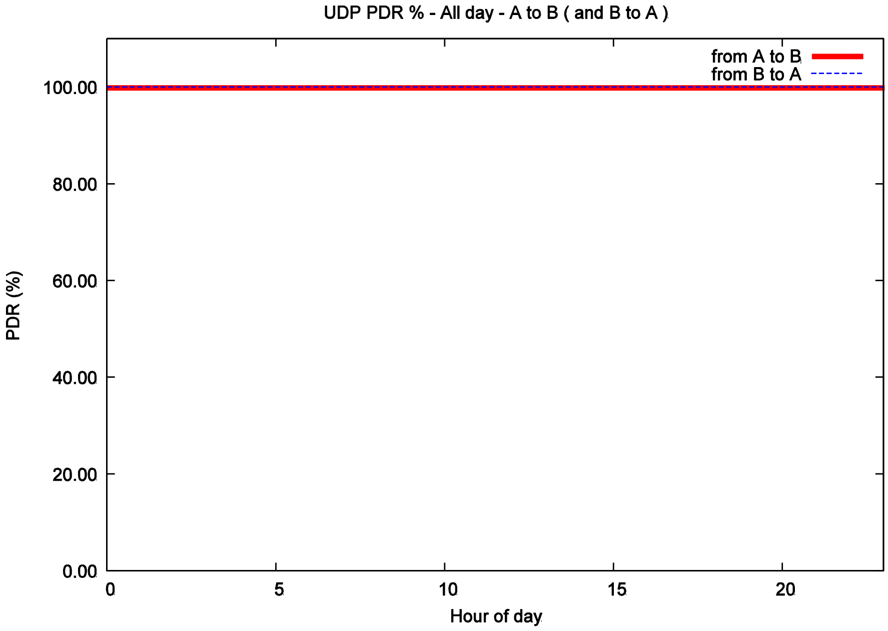


Figure 24 - PDR values in a whole day

Seeing that the transmission is perfect at low rates of data, we are interested in finding out the rate in which the PDR get worse. We have performed different tests increasing the bit-rate in small amounts. We observed that at rates higher than 88 Mbps the PDR % changes, but in a different way on each direction. From A to B, the traffic that reach it destination is reduced sharply from 100% to 5%, as can be seen in Figure 25. So it seems that there is a limiter mechanism that blocks the flows that use more than 88 Mbps of the bandwidth and punish them with only the 5%. From B to A, the traffic seems to be limited to 88 Mbps, and the rest is discarded. No punishment is detected here. It can be easily concluded seeing the Figure 26. So again, the behaviour and policies of the networks are different in each end point.

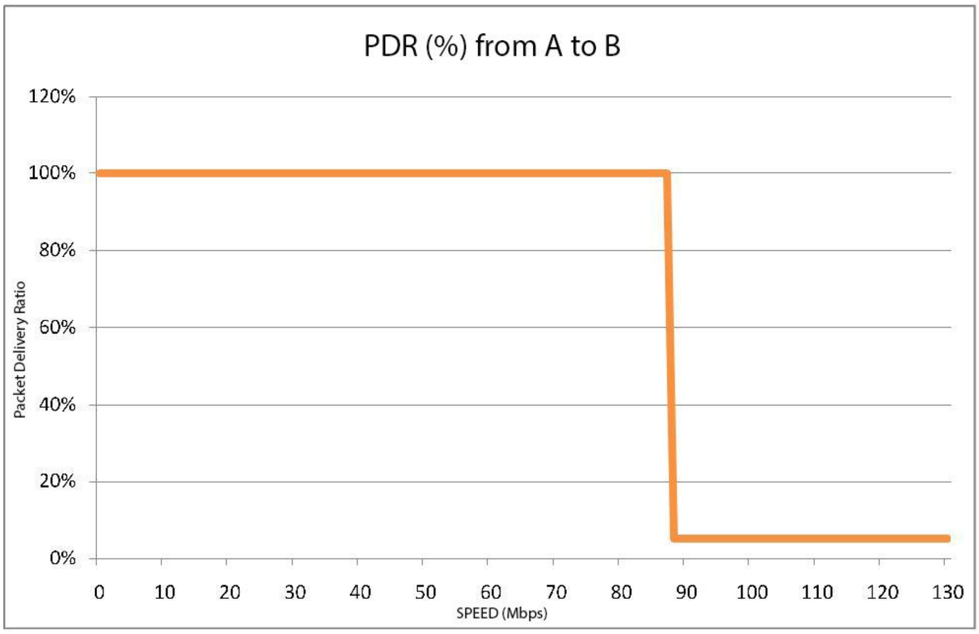


Figure 25 - PDR evolution at different bit-rates from A to B

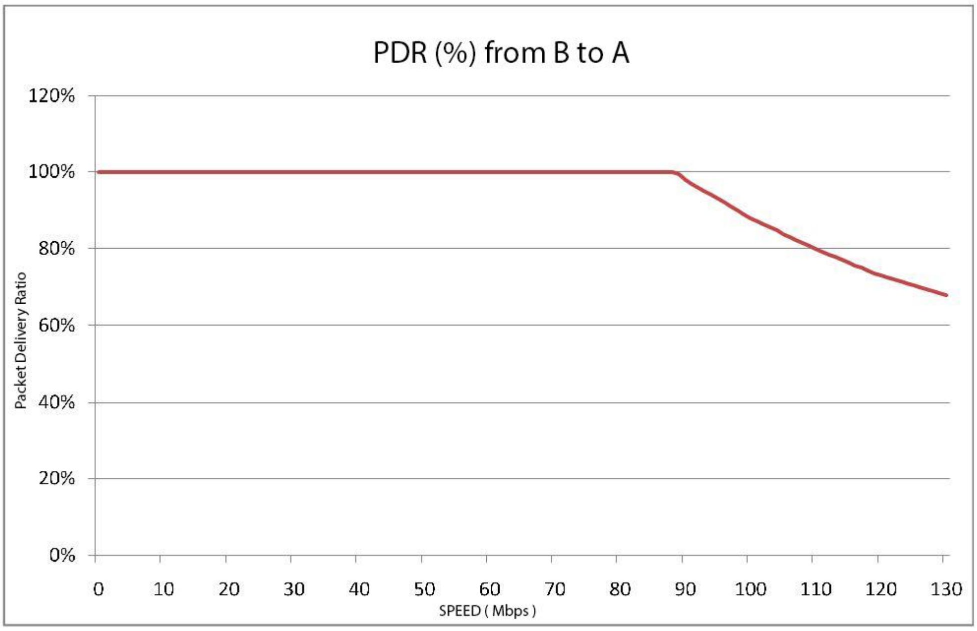


Figure 26 - PDR evolution at different bit-rates from B to A

3.1.3 ICMP tests

The ICMP test is divided in two parts. The first one we perform a ping every one second during 300 seconds from A to B. Then, we repeat the test from B to A. These tests are repeated every hour in a whole day. The results showed in Figure 27 and Figure 28 let us see that the average RTT in the test from A to B (0.12 sec) is lower than the test form B to A (0.15 sec). The rest of values are very similar.

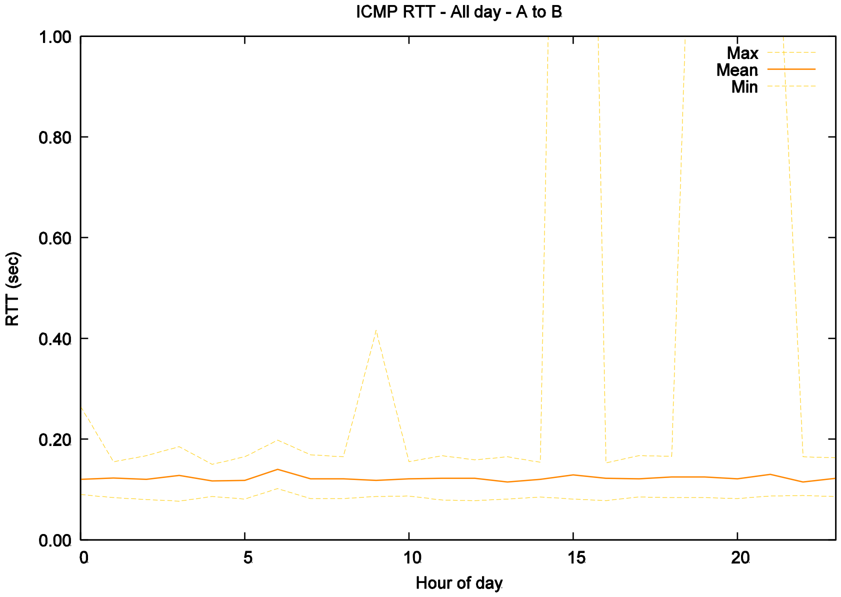


Figure 27 - ICMP results from A to B

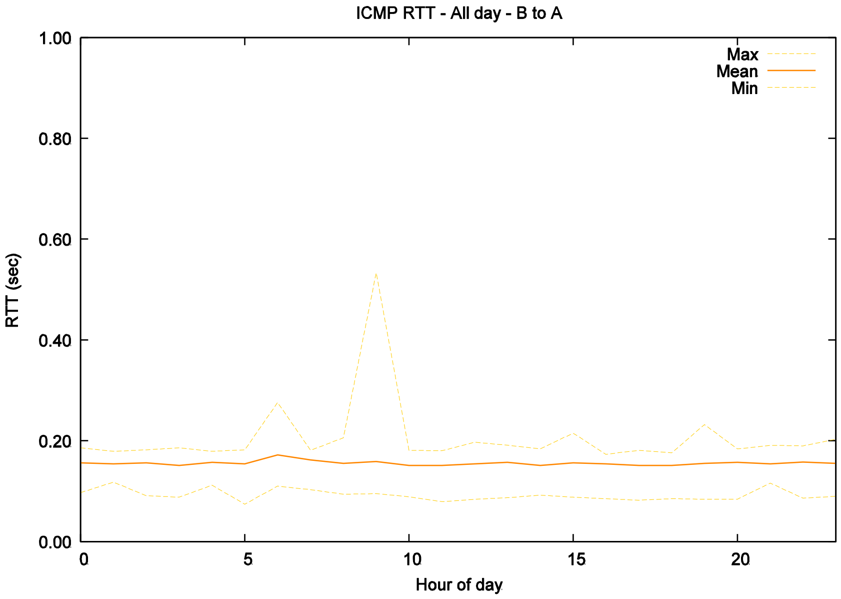


Figure 28 - ICMP results from B to A

3.2 sTESTA tests

3.2.1 TCP results

The TCP test is divided in 3 parts. The first one is the test performed by "iperf" sending traffic from A to B and evaluates what is the maximum bandwidth that the link can support. First, in Figure 29 is shown the results of a single test, and we can appreciate that the value of maximum bandwidth is almost constant about 7.1 Mbps, but sometimes this value is affected by other traffic flows that saturate the link. In the Figure 30 are shown the same test but in a whole day, in order to see if the time could influence the results. Indeed, we detected some service faults and link degradations in determined hours of the day. They can be identified with the darkest coloured zones of the figure.

The second part is the opposite test, from B to A, shown in Figure 31 and Figure 32. The results are very similar but the TCP maximum bandwidth values are close to 5.1 Mbps, 2 Mbps less than the other direction. This and the previous test show that the network is experiencing some congestion problems in short intervals of time. This is not a serious problem but the network is in the limit. It should be improved soon.

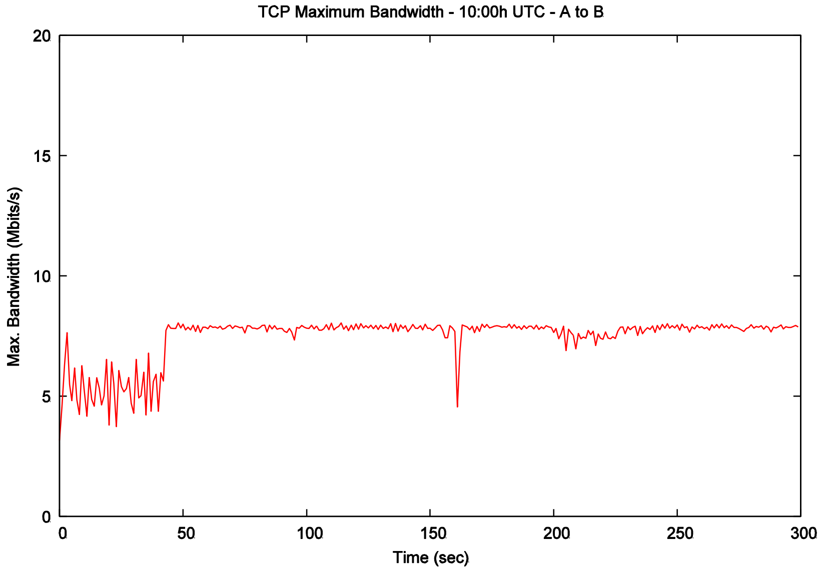


Figure 29 - TCP Maximum Bandwidth from A to B

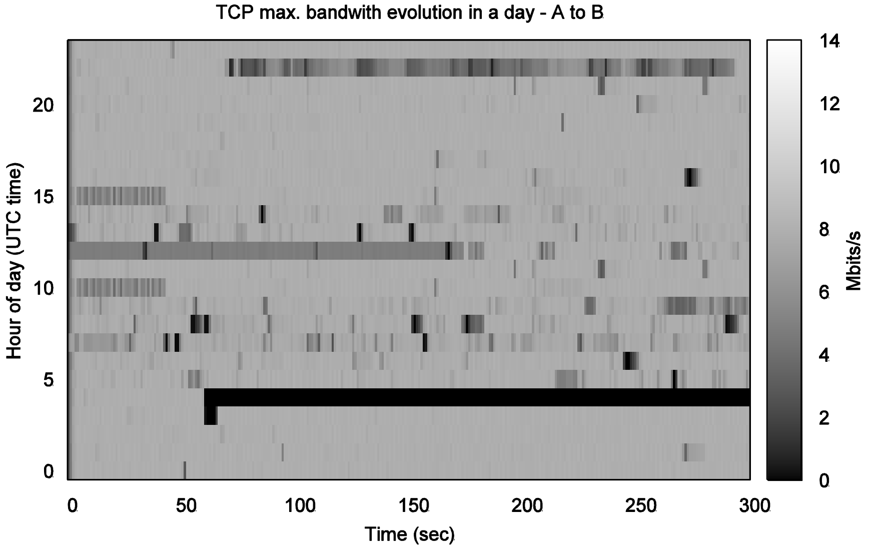


Figure 30 - TCP maximum bandwidth evolution in a day from A to B

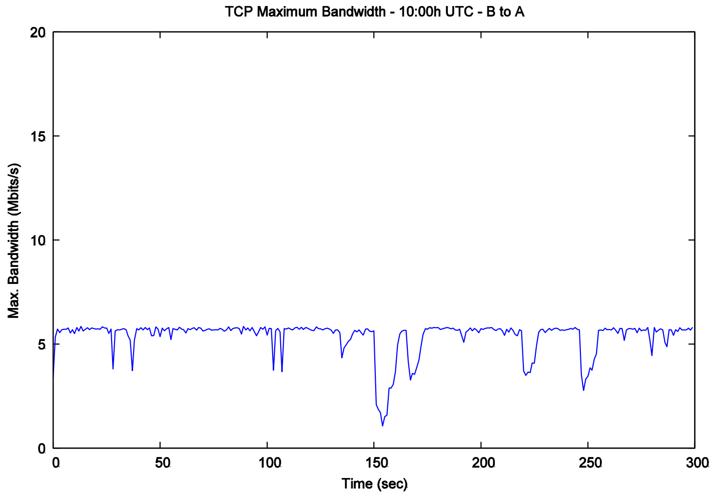


Figure 31 - TCP Maximum Bandwidth form B to A

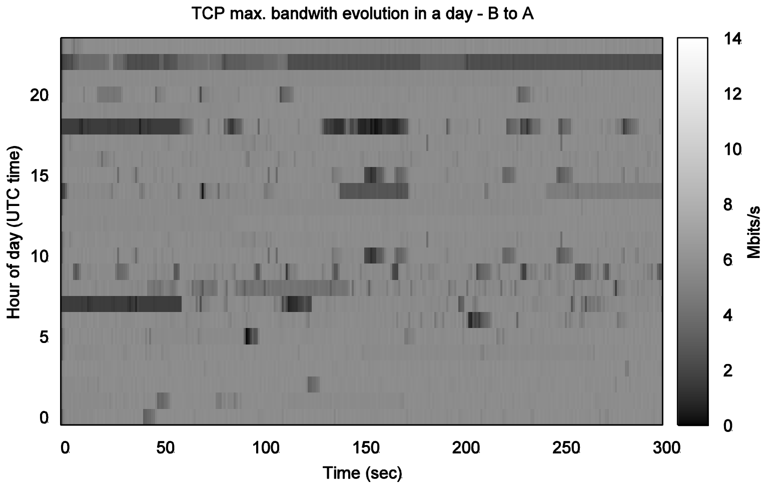


Figure 32 - TCP maximum bandwidth evolution in a day from B to A

The third part of the TCP test is to perform the previous two tests simultaneously to see if the network is or not full-duplex, and if the link performance in one direction is affected if the link in the other direction is being used at the same time. The Figure 33 shows a single test. We can appreciate a “slow-start” mechanism implemented by TCP protocol in the traffic that goes from A to B, but it does not appear in the B to A one. The only one conclusion that we can reach is that the link is of course full-duplex, but the way each endpoint manages the TCP protocol is different. The TCP maximum bandwidth values reached in this test are different in each direction, as we expected seeing the previous tests, but a bit lower. The A to B direction value has decreased to 6.2 Mbps, and in the B to A direction a more noticeable 3.4 Mbps. It is more than expected because the TCP ACK messages are not enough to reduce the bandwidth in such way, especially in the B to A case. In Figure 34 and Figure 35 we can appreciate the behaviour of the network during a day, and we can conclude that there is a significant degradation of the link in office time, form 7 a.m. to 12 p.m. and form 4 p.m. to 7 p.m.

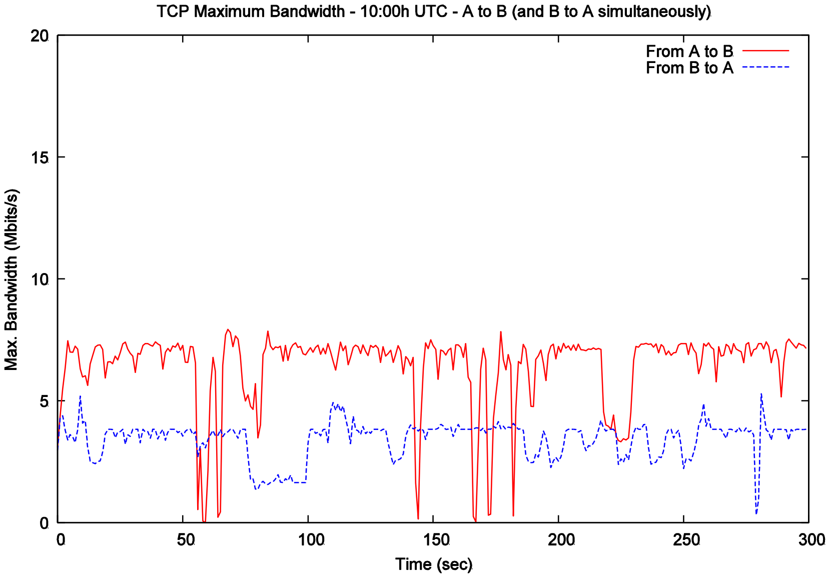


Figure 33 - TCP maximum bandwidth from A to B and B to A

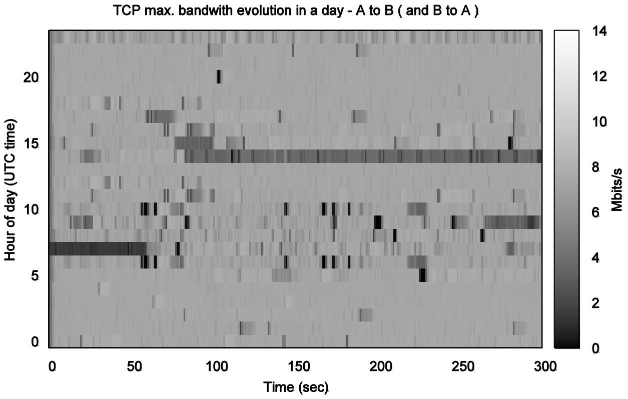


Figure 34 - TCP maximum bandwidth evolution in a day from A to B

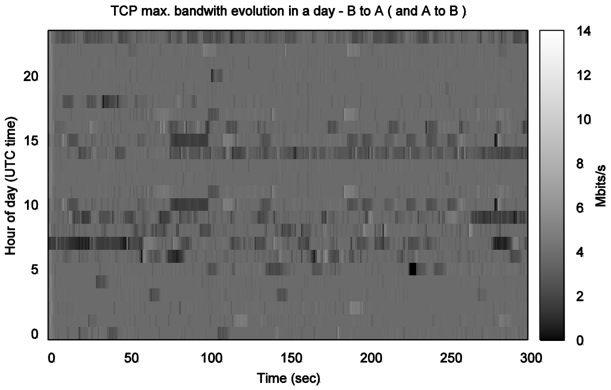


Figure 35 - TCP maximum bandwidth evolution in a day from B to A

As a summary of the tests, the Figure 36 and Figure 37 shows the mean values of the TCP maximum bandwidth during a whole day in both directions, that are quite different values.

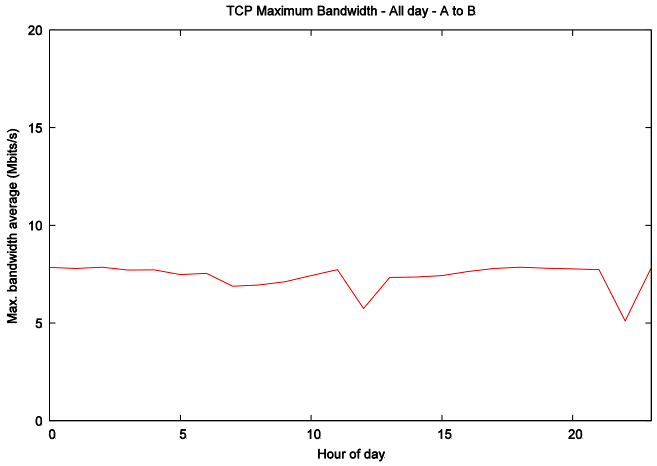


Figure 36 - Mean values of TCP maximum bandwidth from A to B during a day

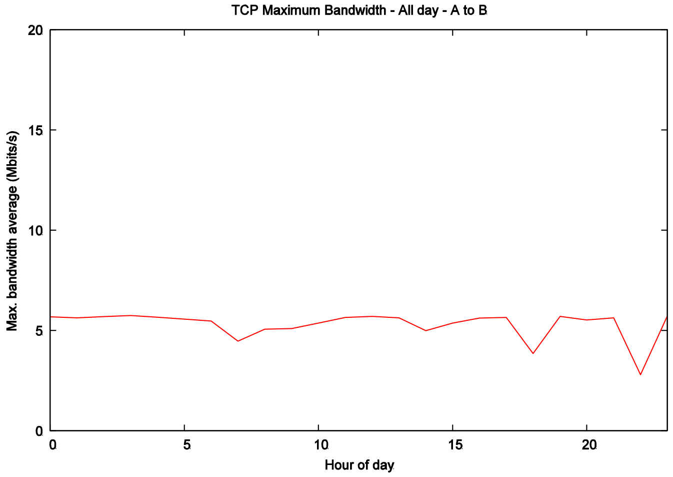


Figure 37 - Mean values of TCP maximum bandwidth from B to A during a day

Performing the previous test simultaneously, both mean values decrease, as can be seen in Figure 38.

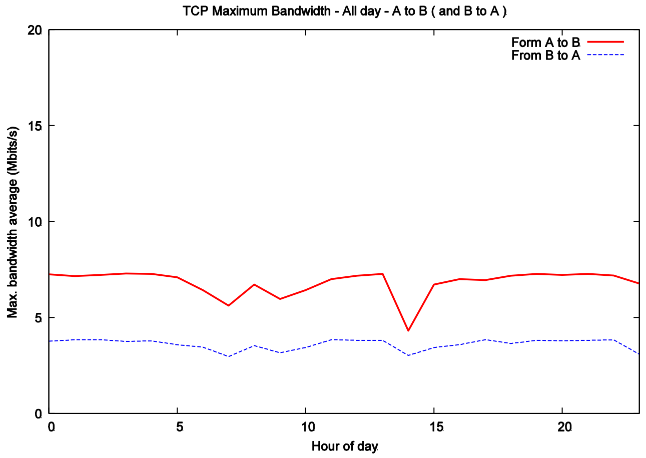


Figure 38 - Mean values of TCP maximum bandwidth from A to B and B to A simultaneously during a day

3.2.2 UDP results

The UDP test is also divided in 3 parts. In the first part we use “iperf” tool to generate a 1 Mbps constant bit-rate flow from A to B. The second part the same but from B to A. And the last one both flows in both directions. This is a speed is far of the limit of the network. We are interested here in the Packet Delivery Ratio (PDR %), in other words, the percentage of packets that reach its destination. As can be seen Figure 39, the UDP transmission is performed perfectly in the B to A direction, without packet loss, so the PDR is always 100%. But it is not the same in the A to B direction, where can be appreciated some moments of low PDR ratio. Also if we perform the same test every hour along a day, the PDR in the A to B case is less than 100% in some hours (office time), as can be seen in Figure 40.

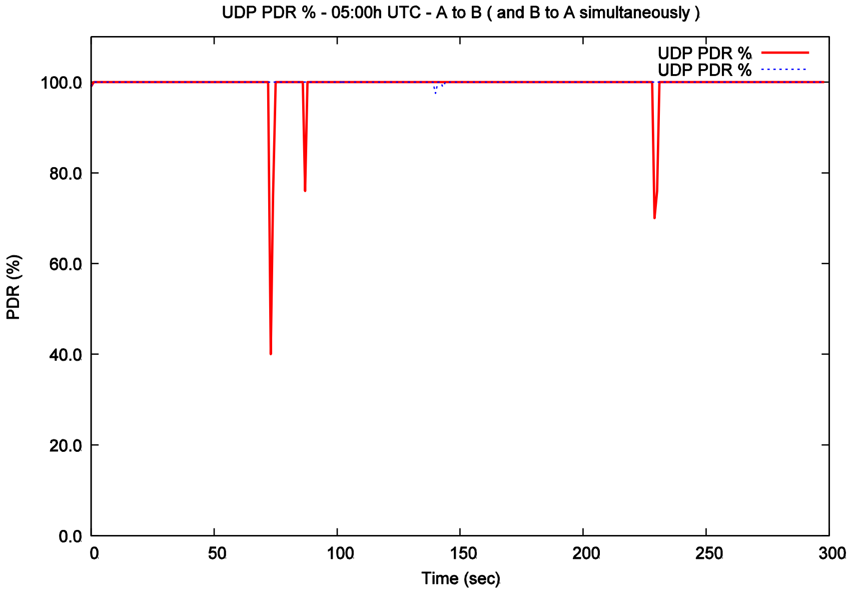


Figure 39 - Simple UDP test from A to B and B to A at 1 Mbps

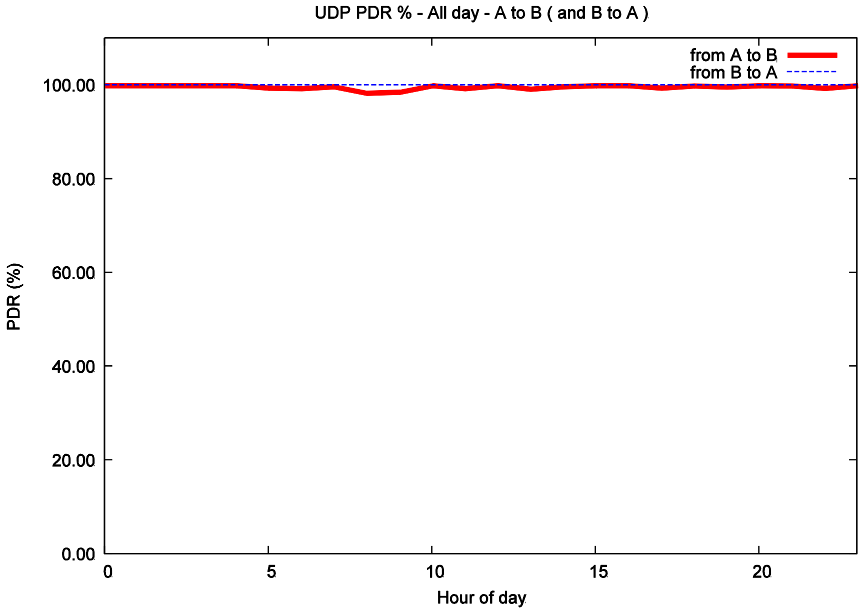


Figure 40 - PDR values in a whole day

Another way to see these small degradations of the link along the day is seeing the figures Figure 41 and Figure 42. In the first one in the A to B case, some dark dots can be appreciated. In the second one corresponding to the B to A case, there is no degradation of the DPR. It is always 100%.

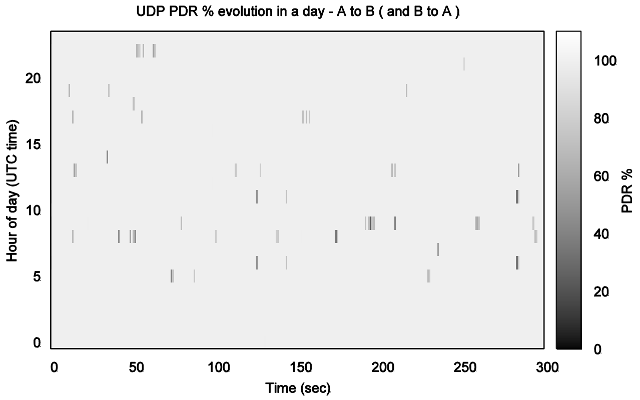


Figure 41–UDP PDR evaluation along a day from A to B

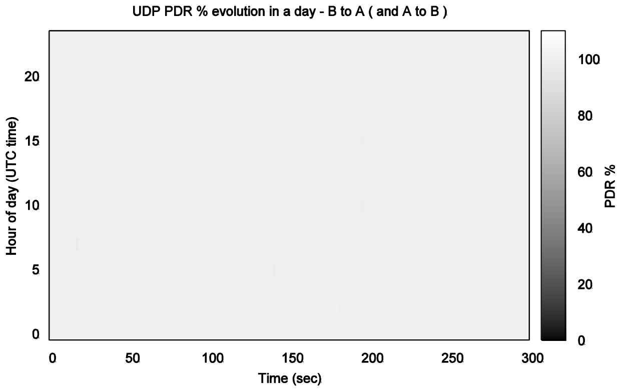


Figure 42 - UDP PDR evaluation along a day from B to A

Seeing that the transmission is almost perfect at low rates of data, we are interested in finding out the rate in which the PDR get worse. We have performed different tests increasing the bit-rate in small amounts. We observed that at rates higher than 9 Mbps the PDR % changes in the same way on each direction as can be seen in Figure 43 and Figure 44. The traffic seems to be limited to 9 Mbps, and the rest is discarded. No punishment is detected.

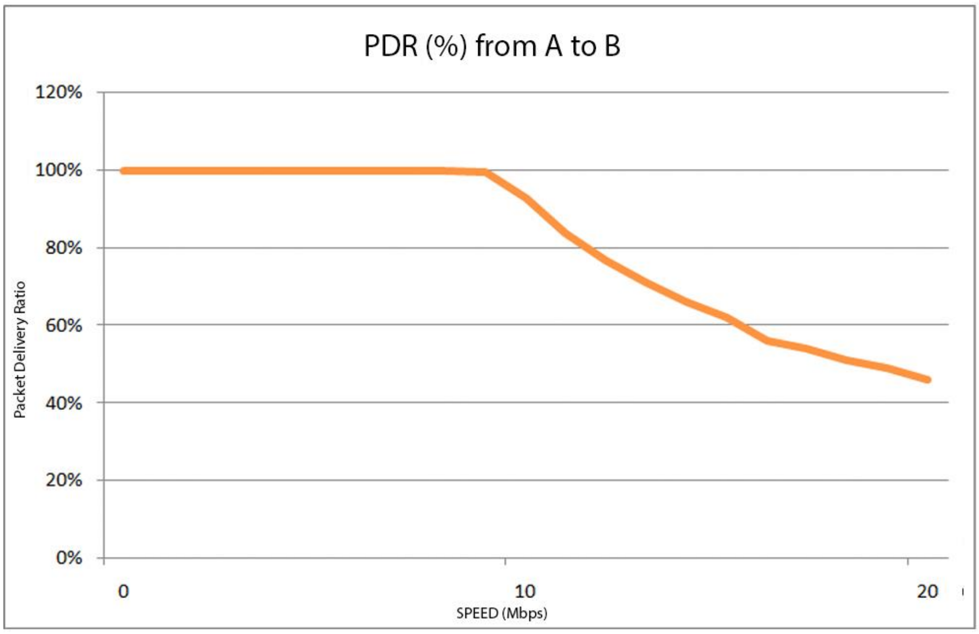


Figure 43 - PDR evolution at different bit-rates from A to B

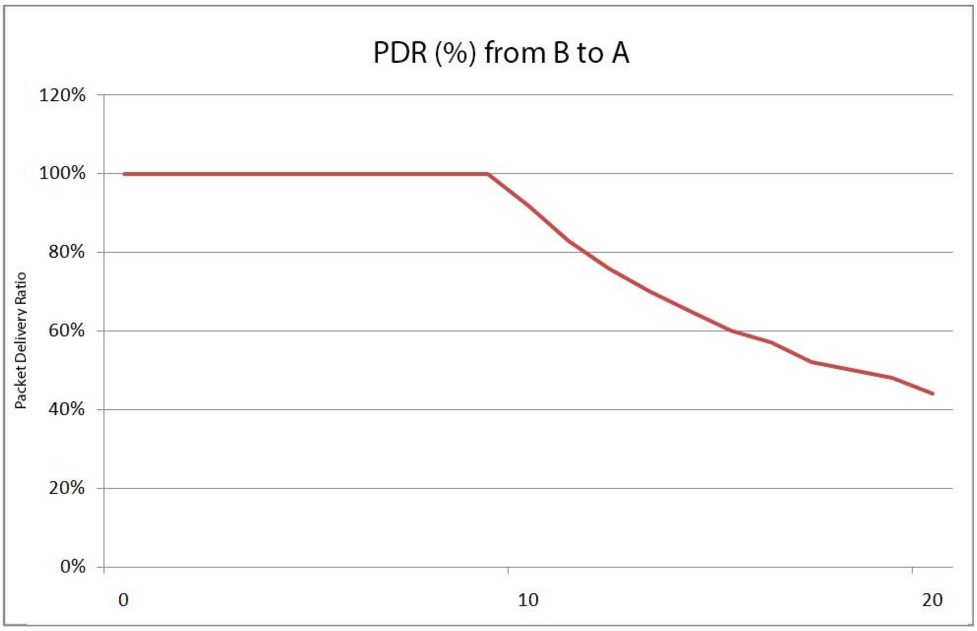


Figure 44 - PDR evolution at different bit-rates from B to A

3.2.3 ICMP tests

The ICMP test is divided in two parts. The first one we perform a ping every one second during 300 seconds from A to B. Then, we repeat the test from B to A. These tests are repeated every hour in a whole day. The results showed in Figure 45 and Figure 46 let us see that the average RTT in both tests is about 0.08 sec. It is worth to mention that both links decrease their quality at the same time.

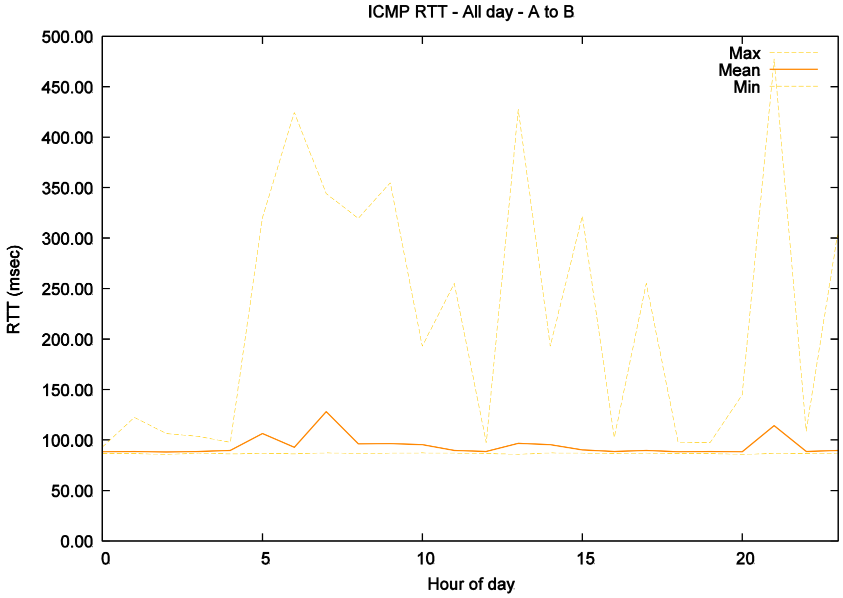


Figure 45 - ICMP results from A to B

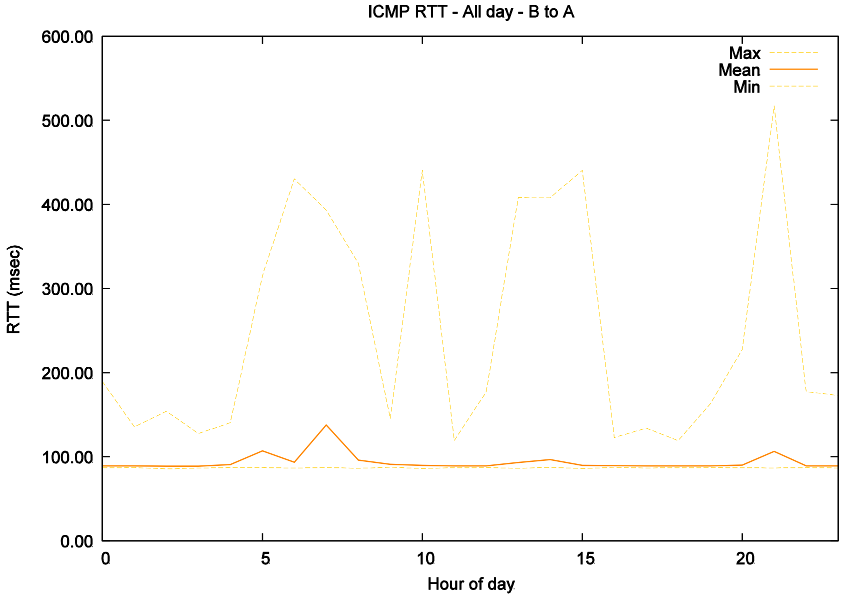


Figure 46 - ICMP results from B to A

3.3 GEANT vs sTESTA

It is important to establish a comparison between the results obtained from both networks. It can give us an idea of the possible behaviour of the applications and services deployed in them. In the Table 2 are compared the most significant values of the results.

Test parts	GEANT (mean)	sTESTA (corrected)	sTESTA (mean)
TCP Max. Bandwidth from A to B	93.141 Mbps	7.72 Mbps	7.11 Mbps
TCP Max. Bandwidth from B to A	93.182 Mbps	5.53 Mbps	5.10 Mbps
TCP Max. Bandwidth from A to B (and B to A)	84.677 Mbps	6.786 Mbps	6.249 Mbps
TCP Max. Bandwidth from B to A (and A to B)	84.676 Mbps	3.735 Mbps	3.440 Mbps
UDP Max. Bandwidth from A to B	~88 Mbps	~9.77 Mbps	~9 Mbps
UDP Max. Bandwidth from B to A	~88 Mbps	~9.77 Mbps	~9 Mbps
UDP PDR% from A to B at 1Mbps	100 %		99.76 %
UDP PDR% from B to A at 1Mbps	100 %		99.96 %
UDP PDR% from A to B (and B to A) at 1Mbps	100 %		99.68 %
UDP PDR% from B to A (and A to B) at 1Mbps	100 %		99.99 %
RTT from A to B	0.122333 sec		0.093963 sec
RTT from B to A	0.155458 sec		0.093710 sec

Table 2- Comparison between GEANT and sTESTA results

To make a fair comparison between these different networks we have to take into account that OpenVPN [OpenVPN] tunnels have been used in the case of the sTESTA network, so its performance is reduced due to the overhead produced by these tunnels. To get more comparable values, the results have to be corrected by a determined factor. This factor is calculated taking into account that the packet size is 1230 bytes without headers. If we perform a normal TCP communication, this value is increased by 40 bytes for the IPv6 header and 32 bytes for the TCP header, so in total 1302 bytes are sent without using OpenVPN. If we use OpenVPN to send the previous TCP communication, then the size increases to 1358 bytes, but in some parts of the network there are double tunnelling, so in total the size raises to 1414 bytes. The size has increased an 8.6%, so all the results have been corrected in an additional column using this correction factor.

As a conclusion we can say that the GEANT network is better than sTESTA network so far. The TCP maximum bandwidth in GEANT network is from 13 to 19 times bigger than sTESTA network. The UDP PDR is 100% in GEANT network, but in sTESTA there are small and random cuts that provoke packet loss. And finally, the only thing that is slightly better in sTESTA network is the RTT values, but this is not enough to compensate the rest of bad values.

3.4 Applying IPSEC

As an additional test, we want to know how much IPsec can deteriorate the link quality, so the tests have been repeated exactly the same but setting up an IPsec tunnel between the machines A and B. Now, an extension header called ESP has to be added in every packet, and the processing time should increase due to encryption/decryption tasks. So, it is not expected that the application of IPsec could improve the results. The idea is to see how much things get worse.

Test parts	sTESTA (with IPSEC)	sTESTA (without IPSEC)
TCP Max. Bandwidth from A to B	1.454 Mbps	7.11 Mbps
TCP Max. Bandwidth from B to A	1.506 Mbps	5.10 Mbps
TCP Max. Bandwidth from A to B (and B to A)	1.239 Mbps	6.249 Mbps
TCP Max. Bandwidth from B to A (and A to B)	1.302 Mbps	3.440 Mbps
UDP Max. Bandwidth from A to B	~1.7 Mbps	~9 Mbps
UDP Max. Bandwidth from B to A	~1.7 Mbps	~9 Mbps
UDP PDR% from A to B at 1Mbps	99.51 %	99.76 %
UDP PDR% from B to A at 1Mbps	98.70 %	99.96 %
UDP PDR% from A to B (and B to A) at 1Mbps	99.61 %	99.68 %
UDP PDR% from B to A (and A to B) at 1Mbps	99.26 %	99.99 %
RTT from A to B	0.097382 sec	0.093963 sec
RTT from B to A	0.091489 sec	0.093710 sec

Table 3- Comparison between sTESTA with and without IPsec

As can be seen in Table 3, every result has worsened with the application of IPsec. For the case of PDR and RTT values, they are practically the same, slightly worse in the IPsec case. But the TCP and UDP maximum bandwidth results have decreased dramatically, that is unexpected for us because this is impossible that the application of IPsec could produce such a degradation of the bandwidth. Seems that the network bandwidth is limited for this kind of traffic. This fact does not allow us to establish a good comparison of bandwidth values. The most probable is that there is a configuration problem in the firewalls that seems to be limiting this kind of traffic. At least this test has been useful to see that this problem exist and it has to be solved.

4 SERVICES: FINAL SETUP

4.1 STORK-IPV6 Support

Cross-border authentication is a traversal process that allows a Member State's service to verify other Member State's citizen's identity. This process is typically implemented following a series of HTTP redirections, where the citizen is re-directed from the target service in the visited MS to an identity provider (IdP) located in their origin MS. The IdP verifies the identity of the citizen, usually by means of an e-ID card previously distributed to their citizens. Finally, the IdP re-direct the citizen back to the target service, in the visited MS, including the result of the authentication and, optionally, some attributes (e.g. birth date, email address, postal address…).

In particular, two different cross-border authentication systems are used in this Pilot: Spanish citizens are authenticated via STORK, while German ones make use of the German e-ID system.

In order to make STORK ready to be used on IPv6, all the different entities involved in the authentication process need to be upgraded to support this protocol. This is required as STORK follows a user-centric model, that is, the end user participates on every interaction with the infrastructure, being redirected from one entity to the next one. This implies that if the end user is only able to communicate using IPv6, all the entities will be required to use that protocol.

In particular, it is mandatory to update all the national PEPS deployed by every Member State. This also applies to the Authentication Portals. Moreover, new records need to be added to national DNS servers in order to include the IPv6 addresses of their servers. Finally, firewalls and other network security elements, such as proxies or shapers, also need to be updated to allow traffic to these IPv6 addresses.

4.2 Testing Services

The services are web applications, so the performance of these applications depends directly on the web server. To find out the limits of the web server, a web server benchmark has been performed.

It has been implemented using PHP, and its main functionality resides on authenticating the public servant using STORK.

This web server has been configured as follows:

- **Operating system**: Ubuntu 12.04.3 LTS. This is a GNU/Linux operating system using Linux kernel 3.5. This OS has dual-stack support enabled by default, allowing using IPv6 connection with no further modifications or configurations.
- **Web server**: Apache 2.2.22. This is one of the most used web servers world-wide. It

provides IPv6 support out-of-the-box; hence it does not require any specific configuration for it.

- **PHP**: Version 5.3.10. It is the version included with the OS distribution. It is not relevant for the purposes of IPv6 support, as web links are generated based on host names, and not on host addresses.

- **Network configuration.** This web server has been configured with a global IPv6 address (2001:638:806:f104::217), which makes the host reachable from any point of the IPv6-enabled Internet. It has also been configured with a global IPv4 address (193.175.133.217), that can be used to access the host from an IPv4-only host.

- **DNS**: The web server hostname (gen6.fokus.fraunhofer.de) has been registered on FOKUS's DNS, including both addresses.

In next figures it is shown the results of a web benchmark performed to this web server. The conclusion, considering the results, up to 9000 requests can be done before the server starts to increase the response time. More than 10000 requests poses into a threat the server stability, because the response times increase exponentially.

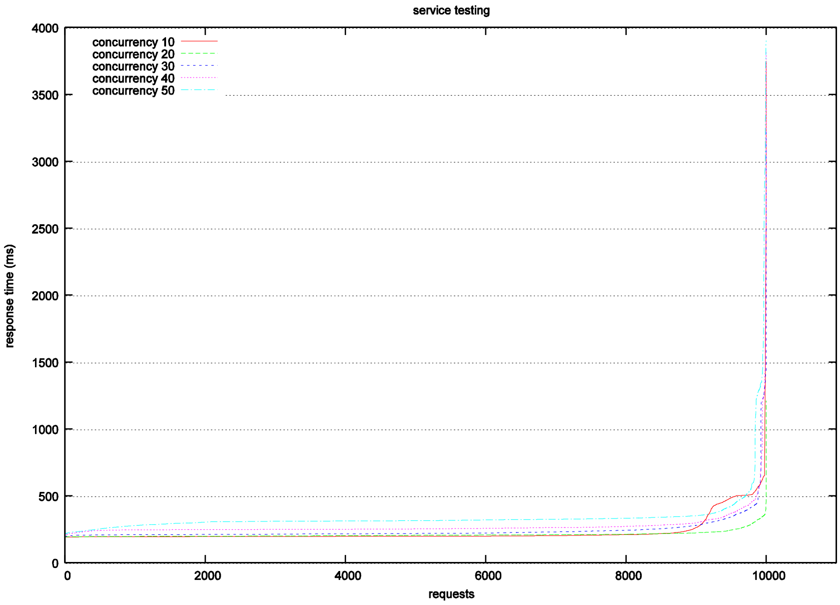


Figure 47 - Web server total time per request results

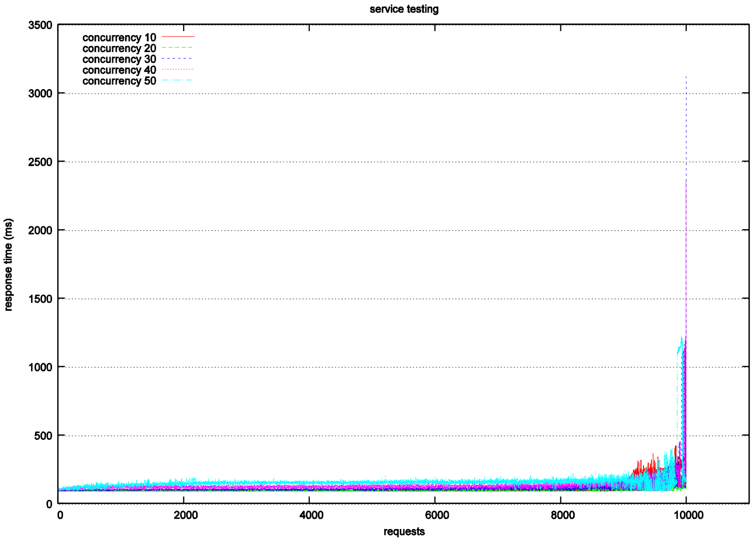


Figure 48 - Web server connection time results

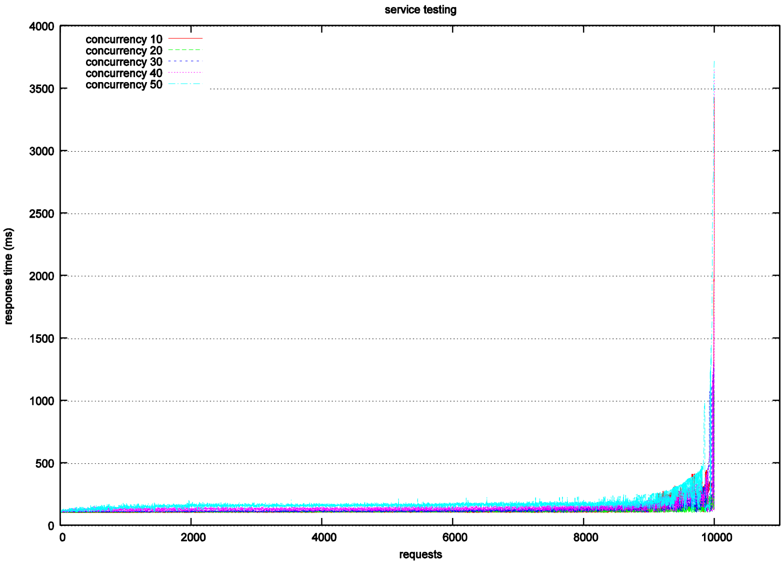


Figure 49 - Web server processing time results

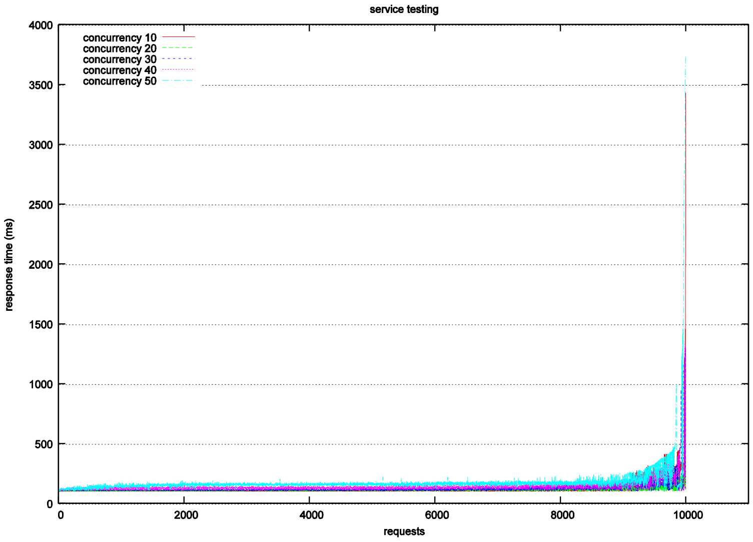


Figure 50 - Web server waiting time results

4.3 Sensors

Ultimeter 100 is a basic weather station that provides a serial IO interface. A BeagleBone Black embedded pc was used to enhance this interface and provide bidirectional end to end communication over ipv6. For the cross-border scenario humidity, luminosity and temperature sensors were connected to a 6LoWPAN enabled Mote, which communicates with an Ethernet bridge. A detailed description of both setups is provided in sections 4.3.1 and 4.3.2

4.3.1 Ultimeter

Ultimeter 100 is equipped with a wind and a temperature sensor, measuring wind speed, wind direction, outdoor temperature and wind chill. It can operate in 7 different modes, from which the "data logger" and "modem" modes are noteworthy for our purposes. In "data logger" mode Ultimeter can transmit up to 2 packets of records every second, while in "modem" mode user can request a data packet of current and average values of the last minute. Below is a sample of such a packet:

- Wind: Cur 8.0MPH 180Deg, 1mAvg 4.6MPH, 1mPeak 9.8MPH 176Deg
  - Hi 9.9MPH 188Deg
- WChill: Cur 75.7F, Lo 75.6F
- Temp Out: Cur 75.7F, Hi 75.7F, Lo 75.6F
- Temp In: Cur 76.4F, Hi 76.6F, Lo 76.3F *
- Hum Out: Cur 65.6%, Hi 65.9%, Lo 65.6% *
- Baro: Cur 29.93inHg, Hi 29.94inHg, Lo 29.93inHg, 3hr chg +0.0inHg*
- Dewpt: Cur 63.6F *
- Heatx: Cur 77.0F *
- Rain: Today 0.21in, Since 01/01/05: 2.57in*

According to the above information the following raw data are collected in BeagleBone:

1. 1 minute average wind speed
2. 1 minute peak wind speed and degrees of wind direction
3. Highest wind speed and degrees of wind direction
4. Highest and lowest outdoors temperature for the current day
5. Lowest wind chill for the current day

The following aggregate values are calculated in BeagleBone, in 15 minute intervals:

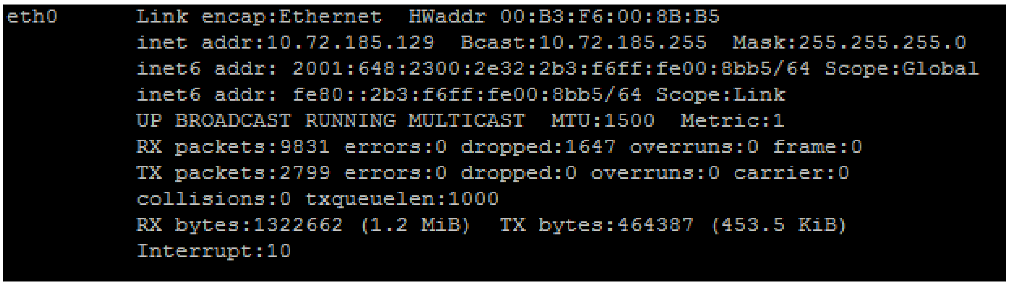
1. Average wind speed
2. Peak wind speed and degrees of direction
3. Highest wind speed and degrees of direction for the current day
4. Highest and lowest temperature for the current day
5. Average wind chill
6. Lowest wind chill for the current day
7. Average temperature
8. Highest and lowest temperature for the current day

Communication from BeagleBone to a backend server is used for data transfer at regular intervals, while communication from the backend server to BeagleBone can be used to send commands to Ultimeter through BeagleBone over IPv6. The following table summarizes available Ultimeter commands

Command	Description
A	Set date and time
B	Set wind direction correction factor
C	Set rain gauge increment
D	Set barometer correction factor
E	Set local sea level barometric pressure
F	Set leap year counter
G	Master reset
H	Request one complete packet
I	Set output mode to data logger mode (continuous output)
J	Set output mode to Packet Mode (output every 5 min)
K	Set output mode to Complete Record Mode (continuous output)
O	Set Outdoor Temperature Offset (sdd = -99 to +99 deg F)
P	Set Indoor Temperature Offset (sdd = -99 to +99 deg F)
Q	Set Outdoor Humidity Offset (sdd = -99 to +99%)
R	Set Indoor Humidity Offset (sdd = -99 to +99%)
T	Set output mode to Complete History Mode
U	Set year
V	Set output mode to Multiple Output Mode (continuous output)
W	Set output mode to WeatherText Output Mode
X	Set Wind Speed Correction Offset and Scale factors.
Y	Request one WeatherText data packet

Table 4: Available Ultimeter commands

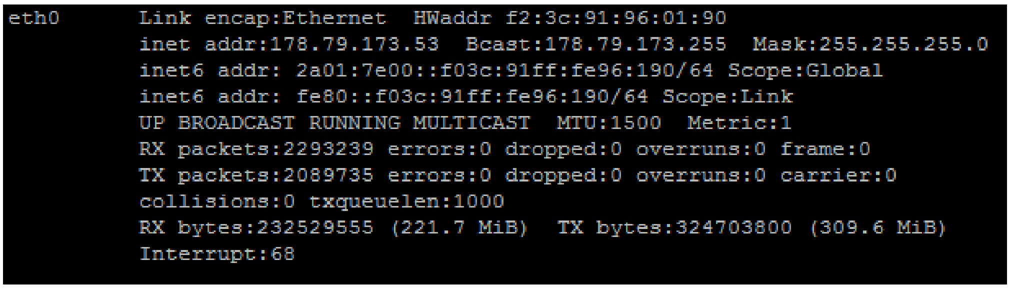
BeagleBone runs a Debian Linux. The following image displays the network interface configuration for IPv6 in BeagleBone.



```
eth0      Link encap:Ethernet  HWaddr 00:B3:F6:00:8B:B5
          inet addr:10.72.185.129  Bcast:10.72.185.255  Mask:255.255.255.0
          inet6 addr: 2001:648:2300:2e32:2b3:f6ff:fe00:8bb5/64 Scope:Global
          inet6 addr: fe80::2b3:f6ff:fe00:8bb5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9831 errors:0 dropped:1647 overruns:0 frame:0
          TX packets:2799 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1322662 (1.2 MiB)  TX bytes:464387 (453.5 KiB)
          Interrupt:10
```

Figure 51 - IPv6 configuration in BeagleBone Black

The BeagleBone and Ultimeter are installed in GRNET, the academic network for Greece. BeagleBone communicates with a backend application running in a VM server in Intelen’s cloud infrastructure. The following image displays the network interface configuration for IPv6 in that server



```
eth0      Link encap:Ethernet  HWaddr f2:3c:91:96:01:90
          inet addr:178.79.173.53  Bcast:178.79.173.255  Mask:255.255.255.0
          inet6 addr: 2a01:7e00::f03c:91ff:fe96:190/64 Scope:Global
          inet6 addr: fe80::f03c:91ff:fe96:190/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2293239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2089735 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:232529555 (221.7 MiB)  TX bytes:324703800 (309.6 MiB)
          Interrupt:68
```

Figure 52 - IPv6 configuration for Intelen backend server

Measurements are collected by an application build in php, stored in a MySQL database and exposed to other applications through an IPv6 enabled RESTful web API. The following configuration was applied in an Nginx server, in order to enable IPv6 support

listen [2a01:7e00::f03c:91ff:fe96:190]:80;

Measurements are exposed in JSON format, through a web API build in php. The following table summarises the API, which will be integrated in the Greek pilot platform.

API url	[2a01:7e00::f03c:91ff:fe96:190]:80/ultimeter/data
Parameters	**mac**: BeagleBone mac address **interval**: {day,month,year} **date**: a date in euro-date format e.g. 31-12-2014 **type**: {ws,pws,pwd,ht,lt,wc,lwc,temp,htemp,ltemp,hws,hwd} ws: Average wind speed pws: Peak wind speed pwd: peak wind degrees of direction hws: Highest wind speed for the current day hwd: Highest wind degrees of direction for the current day ht: Highest temperature for the current day ht: Lowest temperature for the current day wc: Average wind chill lwc: Lowest wind chill for the current day temp: Average temperature htemp: Highest temperature for the current day ltemp: Highest temperature for the current day
Request example	[2a01:7e00::f03c:91ff:fe96:190]:80/ultimeter/data/mac/123/interval/day/date/31-12-2014
Response Format	JSON

Response example	{
	"data": [
	{
	"00:00": 1.1
	},
	{
	"00:15": 1.2
	}
	]
	}

4.3.2 6LoWPAN Mote

A 6LoWPAN Mote is used to collect data from humidity, luminosity and temperature sensors. The Mote communicates with the sensors over CoAP/HTTP and with an EthBridge over 6LoWPAN. The EthBridge is responsible for converting 6LoWPAN packets generated by the motes to IPv6 packets and send them to an IPv6 enabled VM server in Intelen's cloud infrastructure, which is the same server that collects data from Ultimeter. The network interface configuration of the server can be seen in figure 49. The Mote has a jennic 5149 processor and runs Contiki OS, exposing a "request data sender" service, which is responsible to push sensor readings to a remote server over 6LoWPAN.

In Intelen's VM raw readings are stored in a MySQL database and exposed to other components or apps through an API, which is described in the following table.

API url	[2a01:7e00::f03c:91ff:fe96:190]:80/data/receiver
Parameters	**mac**: Mote mac address **interval**: {day,month,year} **date**: a date in euro-date format e.g. 31-12-2014
Request example	[2a01:7e00::f03c:91ff:fe96:190]:80/data/receiver /mac/123/interval/day/date/31-12-2014
Response Format	JSON

Response example	{
	  "success": "true",
	  "data": [
	    {
	      "24-09-2014 00: 15": {
	        "tem": 0,
	        "hum": 0,
	        "lum": 0
	      }
	    },
	    {
	      "24-09-201400: 30": {
	        "tem": 0,
	        "hum": 0,
	        "lum": 0
	      }
	    }
	  ]
	}

4.3.2.1 Jennic Mote

The smart object is enabled by an IEEE 802.15.4 device from the Jennic Company. The jennic device runs the Contiki Operating System. Contiki provides radio and 6LoWPAN layers to support the implementation of IPv6-based applications. Jennic mote performs the following main tasks:

- Registering its sensors as IoT services in the Digcovery system.
- Measuring the environment conditions using its integrated sensors.
- Transmitting its sensor values to the Smart Thing Information System (STIS).
- Responding queries about the available sensors.

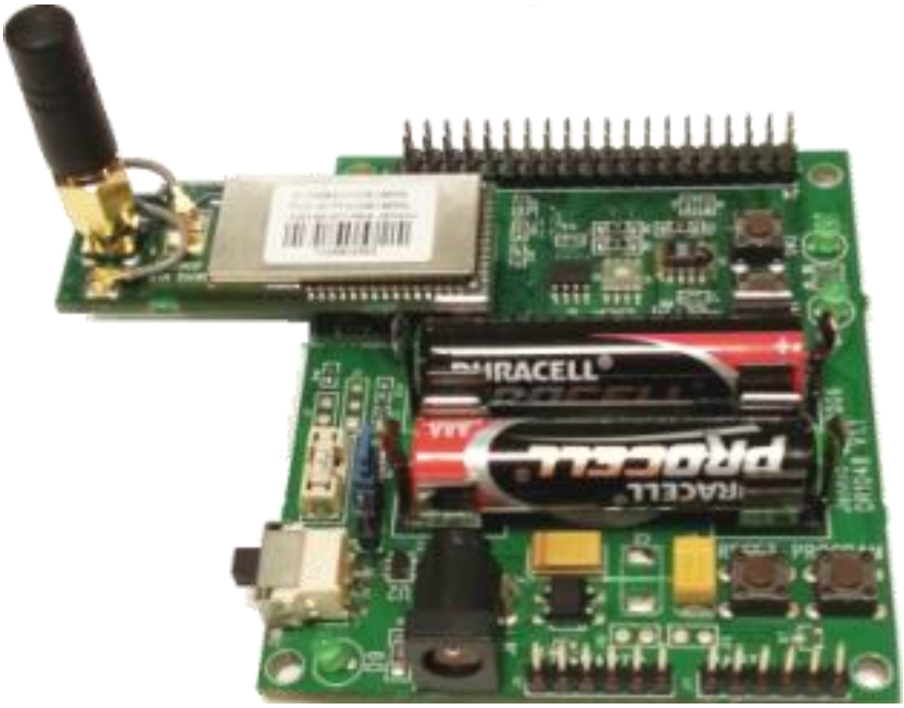


Figure 53 - Jennic development kit

Jennic mote is connected to Internet through an IoT6 Ethbridge. IoT6 Ethbridge offers the translation between 6LoWPAN and IPv6 to support the connectivity of wireless sensors networks (IEEE 802.15.4) to Internet.

4.3.2.2 Ethbridge

The ethbridge device was developed by WP3 to support the interoperability between two technologies: IEEE 802.15.4 wireless networks and IEEE 802.3 Ethernet networks. The ethbridge contains an IEEE 802.15.4 Jennic chip and a USB port connected to the IoT6 smart-board that generates a virtual Ethernet interface. The ethbridge acts as a gateway to enable the communication between 6LoWPAN constrained devices and IPv6 hosts. Ethbridge performs the following main tasks:

- Processing 6lowpan messages in order to translate to IPv6 header and resend them to the virtual Ethernet interface.
- Processing IPv6 messages in order to compress in 6lowpan header and resend them to wireless sensor network.

To do that, Ethbridge provides the following applications to support the translation IEEE 802.15.4 WSN and IEEE 802.3 Ethernet:

- 802.15.4 Network communication.
- USB Communication Device Class (USB-CDC).
- 6lowpan to IPv6 adaptation.
- IPv6 to 6lowpan adaptation.

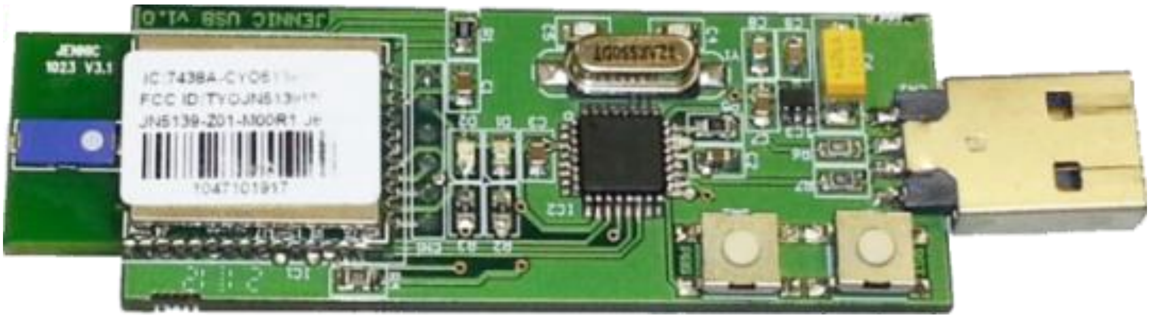


Figure 54 - Ethbridge

5 CONCLUDING REMARKS

In this deliverable has been carried out different tests in order to analyse the performance in GEANT and sTESTA networks. Moreover, a comparison between them has been performed in order to have a clear vision of how the security system provided by sTESTA affects the global network performance. GEANT network, which is not providing any security mechanism by default, is used to prove that sending unsecured traffic get better performance ratios, for example, in bandwidth measurements.

In the other side, over these networks have been deployed authentication services which imply the communication between several European institutions in order to authenticate its citizens when they are outside from their country. Therefore, check the performance of these servers where the services are deployed is important. In this deliverable, the authentication server has been stressed in order to check how many requests can be handled in a short period of time to find out where is the breakpoint where the server starts to be overloaded.

6 References

[Geant]	GÉANT is the pan-European research and education network that interconnects Europe’s National Research and Education Networks (NRENs). http://www.geant.net/
[sTesta]	STESTA: Secure Trans European Services for Telematics between Administrations http://ec.europa.eu/idabc/en/document/2097.html
[OpenVPN]	Open Virtual Private Network https://openvpn.net/
[Redsara]	The Red SARA (Sistemas de Aplicacions y Redes para las Administraciones) is a set of communications infrastructure and basic services that connects networks of the Spanish government and European institutions facilitating the exchange of information and access to services. http://administracionelectronica.gob.es/ctt/redsara
[Rediris]	RedIRIS is the Spanish academic and research network that provides advanced communication services to the scientific community and national universities. It is funded by the Ministry of Economy and Competitiveness and is included in the Ministry's map of Special Scientific and Technological Facilities (ICTS). http://www.rediris.es/rediris/
[Citkomm]	The Citkomm, with its 40-year history, is a great local IT service provider in North Rhine-Westphalia. Our clients include local authorities as well as public companies and non-profit organizations. http://www.citkomm.de/
[Iperf]	While tools to measure network performance. Iperf was originally developed by NLANR/DAST as a modern alternative for measuring TCP and UDP bandwidth performance. https://iperf.fr/