Network Infrastructure Test Protocol Document

for

NATO Education and Training Network (NETN)

Developed by MSG-068 NETN – Infrastructure Working Group

Roel Wymenga (TNO)
Wim Huiskamp (TNO)
Per Philip Sollin (Pitch Technology)

1 Table of contents

1 Table of contents 2
2 Introduction 4
3 Test protocol Overview 5
3.1 Pre initiative test 5
3.2 Monitoring test 5
4 Test protocol 7
4.1 Security 7
4.2 Hardware needed 7
4.3 Network and test device initialization 7
4.3.1 Routers and switches 7
4.3.2 Computers and SERVERS 7
4.4 Network pre initiative test 7
4.4.1 Check router tables black routers 7
4.4.2 Check router tables red routers 7
4.4.3 Black site Connectivity and delay 8
4.4.4 Red site Connectivity and delay 8
4.4.5 Unclassified PC configuration 9
4.4.6 Classified PC configuration 9
4.4.7 Black site bandwidth test 10
4.4.8 Red site bandwidth test 13
4.5 Network monitoring during pre initiative test and initiative 15
4.5.1 Network devices 15
4.5.2 Server 1 LINUX 16
4.5.3 Server 2 Windows 16
5 Test Results and Conclusions from the NETN Experiment 20
5.1 Intro 20
5.1.1 Unclassified Network Infrastructure over Internet 20
5.1.2 Unclassified Network Infrastructure over CFBLNet 21
5.2 Pre initiative test 23
5.3 Monitoring test 23
6 Referenced publications 28

Appendix E.1 NETN Server Hardware
Appendix E.2 NETN Client Hardware
Appendix E.3 NETN Infrastructure Test Tool Specifications
Appendix E.4 Measured Average Delay between National PoPs over CFBLNet

2 Introduction

This document is a deliverable of the MSG-068 NETN Infrastructure Working group and provides a detailed infrastructure test protocol description and recommendations for its implementation. The document refers to the NETN Infrastructure Design that was proposed and discussed in [Annex D MSG-068 NETN Network Infrastructure Design Document].

Note that within the given constraints of time and resources, the NETN Infrastructure team has performed a subset of these tests during the preparation and the execution of the MSG-068 NETN experiments in Nov 2010. The test results as collected for the NETN infrastructure used in the experiment are included in the final paragraph of this document.

3 Test protocol Overview

There are two kinds of network tests foreseen. The first is before the initiative starts (pre initiative test) and the other is during the initiative (monitoring test).

The pre initiative test is to determine the default parameter values as available bandwidth protocols and services. The monitoring test is to detect problems. This monitoring information can then be used to solve (network or application) problems immediately if possible or the use this information to improve new initiatives.

It is difficult to describe a standard ('one size fits all') test protocol because initiatives are so different. In this document examples are presented to take care of most common issues in an initiative.

3.1 Pre initiative test

In the pre initiative test the following parameters are essential to predict the influence of the network on most applications. The requirements and implementation determine if all tests should be done.

- Maximum Bandwidth
    - For different protocols (TCP, UDP)
    - For different data classes
- Delay between all sites for different packet sizes
- Routing (unicast, multicast)
- Protocols (TCP, UDP, multicast, broadcast)
- Reachable services (NTP, DNS, x, x, x)
- Max MTU size / fragmentation

These tests should be carried out on the classified side of the network. If this is not possible due to accreditation issues an indication on the unclassified side can be used for the following parameters:

- Bandwidth
- Delay to all sites

3.2 Monitoring test

In the monitoring test the following information of the classified network is important to find problems:

- Used Bandwidth for the protocols used

- Delay between all sites
- Reachable services
- Fragmentation

4 Test protocol

4.1 Security

Be aware that no unclassified computer is connected to the classified network!
Be aware that no classified computer is connected to the unclassified network!

Do not use DHCP on computers. Different IP address ranges are the first line of defense for computers connected to the incorrect network!

4.2 Hardware needed

- Unclassified PC (any computer)
- Classified PC (any computer)
- Classified SERVER LINUX
- Classified SERVER WINDOWS SERVER 2008

For information about the server hardware see Appendix E.1.

4.3 Network and test device initialization

4.3.1 Routers and switches

Do NOT set router and switch Ethernet ports to auto. This often shows bad behavior when the network becomes “loaded”.

4.3.2 Computers and SERVERS

Do NOT set Computers and SERVERS Ethernet ports to auto. This often shows bad behavior when the network becomes “loaded”.

4.4 Network pre initiative test

4.4.1 Check router tables black routers

The command “ship route” should show all active routs to all connected routers.

4.4.2 Check router tables red routers

The command “ship route” should show all active routs to all connected routers.

4.4.3 Black site Connectivity and delay

The 'Ping' is a simple test and gives information about the connectivity and delay between two systems. The protocol used is ICMP and is based on UDP. The Ping command is available on each Windows and Linux PC. This test also shows if there is a problem with a crypto or Ethernet network port along the way.

PING all connected routers in the unclassified network to test if all sites can be reached.
The PING also provides "min", "average" and "maximum" round trip delay times. The PING length should be set to the following length:

PING		Remarks
Size	RTT	
100 bytes		
500 bytes		
1000 bytes		
2000 bytes		
3000 bytes		
5000 bytes		

If this test shows a loss of data then there is probably a network port set to "auto" in the path. If there is packet loss the problem should be solved before the other tests could be done.

4.4.4 Red site Connectivity and delay

PING all connected routers in the classified network to test if all sites can be reached. The PING also provides "min", "average" and "maximum" round trip delay times. The PING length should be set to the following length:

PING		Remarks
Size	RTT	
100 bytes		
500 bytes		
1000 bytes		
2000 bytes		
3000 bytes		
5000 bytes		

If this test shows a loss of data then there is probably a network port set to "auto" in the path. If there is packet loss the problem should be solved before the other tests could be done. Experience has shown that also a crypto could initiate packet loss at longer packets (Restart all crypto's involved).

4.4.5 Unclassified PC configuration

To optimize the network capacity, the maximum transmission unit (MTU) size is determined. This will be done with the program TCP optimizer.

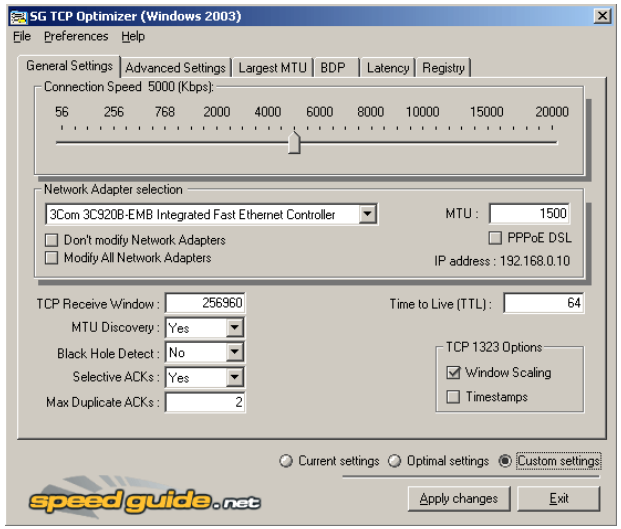

Figure 1 TCP optimizer

After the MTU size determination the connection speed is set to 20.000 and Optimized settings is set and fixed with Apply changes. This initialized the computer for best network performance.

4.4.6 Classified PC configuration

To optimize the network capacity, the maximum transmission unit (MTU) size is determined. This will be done with the program TCP optimizer.

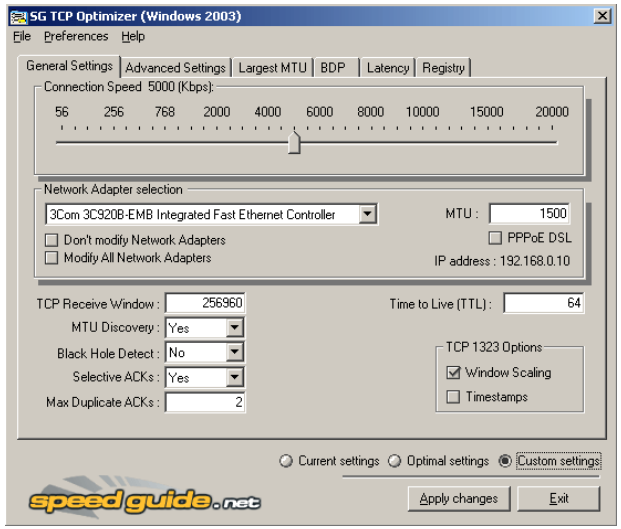

Figure 2 TCP optimizer

After the MTU size determination the connection speed is set to 20.000 and Optimized settings is set and fixed with Apply changes. This initialized the computer for best network performance.

4.4.7 Black site bandwidth test

The TCP and UDP network capacity is tested with JPerf. This will provide information in the peak and average capacity of the network.

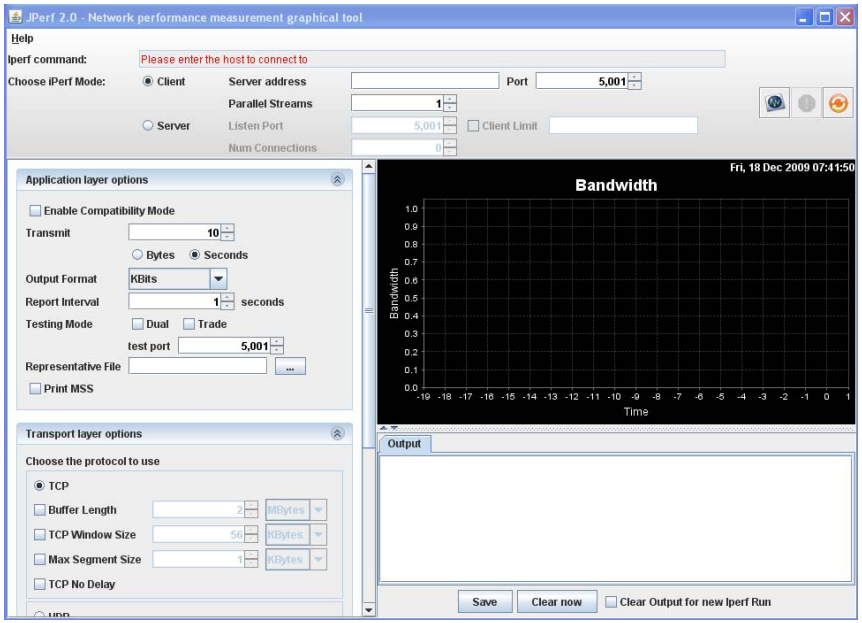

Figure 3 JPerf

4.4.7.1 JPERF Client unclassified Configuration

Server address **t.b.d.**
Port 5001
Parallel streams1

<u>Application layer options</u>

Transmit	10 seconds
Output	Kbit/s
Report interval	1 second
Test port	5001

Transport layer options

TCP	
Buffer length	**t.b.d.**
TCP window size	**t.b.d.**
Max segment size	**t.b.d.**
TCP no delay	(off)
UDP	
UDP bandwidth	**t.b.d.**
UDP buffer size	**t.b.d.**
UDP packet size	**t.b.d.**

IP layer options

TTL	1
Type of service	None
Bind to host	**t.b.d.**
IPv6	(off)

4.4.7.2 JPERF Server unclassified Configuration

Listen Port	5001
Client limit	**t.b.d.**
Number of connections	1

Application layer options

Transmit	10 seconds
Output	Kbit/s
Report interval	1 second
Test port	5001

Transport layer options

TCP	
Buffer length	**t.b.d.**
TCP window size	**t.b.d.**
Max segment size	**t.b.d.**
TCP no delay	(off)
UDP	
UDP bandwidth	**t.b.d.**

UDP buffer size	**t.b.d.**
UDP packet size	**t.b.d.**

IP layer options

TTL	1
Type of service	None
Bind to host	**t.b.d.**
IPv6	(off)

4.4.8 Red site bandwidth test

The TCP and UDP network capacity is tested with JPerf. This will provide information in the peak and average capacity of the network.

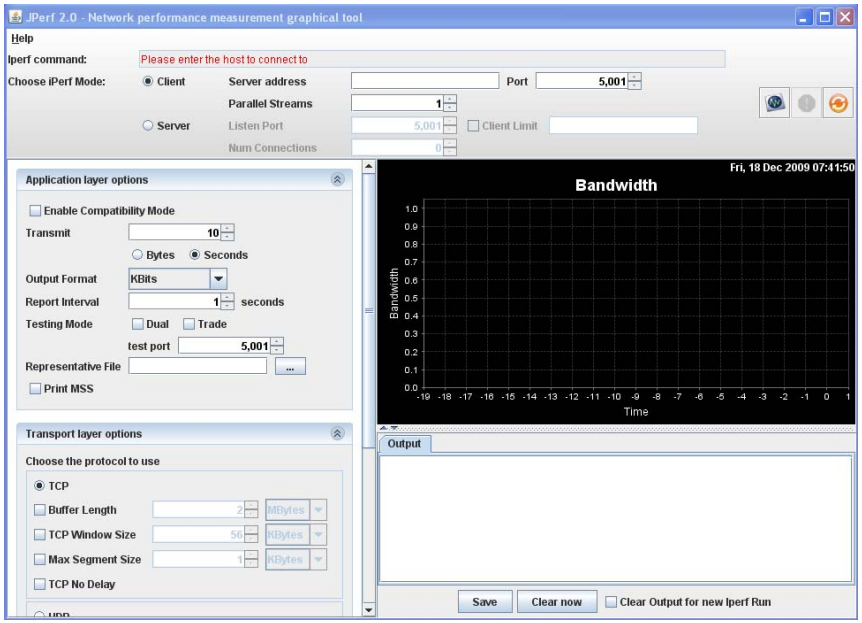

Figure 4 JPerf

4.4.8.1 JPERF Client classified Configuration

Server address	**t.b.d.**
Port	5001
Parallel streams1	

Application layer options

Transmit	10 seconds
Output	Kbit/s
Report interval	1 second
Test port	5001

Transport layer options

TCP	
Buffer length	**t.b.d.**
TCP window size	**t.b.d.**
Max segment size	**t.b.d.**
TCP no delay	(off)
UDP	
UDP bandwidth	**t.b.d.**
UDP buffer size	**t.b.d.**
UDP packet size	**t.b.d.**

IP layer options

TTL	1
Type of service	None
Bind to host	**t.b.d.**
IPv6	(off)

4.4.8.2 JPERF Server classified Configuration

Listen Port	5001
Client limit	**t.b.d.**
Number of connections	1

Application layer options

Transmit	10 seconds
Output	Kbit/s
Report interval	1 second
Test port	5001

Transport layer options

TCP	
Buffer length	**t.b.d.**
TCP window size	**t.b.d.**
Max segment size	**t.b.d.**
TCP no delay	(off)
UDP	
UDP bandwidth	**t.b.d.**
UDP buffer size	**t.b.d.**
UDP packet size	**t.b.d.**

IP layer options

TTL	1
Type of service	None
Bind to host	**t.b.d.**
IPv6	(off)

4.5 Network monitoring during pre initiative test and initiative

The network monitoring system consists of two centralized 19” servers. One server uses LINUX as operating system and the other server is using WINDOWS SERVER 2008 as operating system. These two servers monitor the network and provide all sites connect with the network status information on a web based interface.

4.5.1 Network devices

Network devices such as routers and switches need to provide access to the network tools. This means that Simple Network Management Protocol (SNMP) “READ” access is needed by the network management and monitoring tools.

4.5.1.1 Router and switch configuration

To provide read access for the network management and monitoring tools the following information should be added to CISCO network device configuration (example for TNO in The Hague):

!
snmp-server community !NETN@CFBL#$! RO
snmp-server location NLD, TNO, The Hague
snmp-server contact phone: +31651096151
!

4.5.2 Server 1 LINUX

For information about the server hardware see Appendix E.1.

4.5.2.1 MRTG

MRTG is using the Simple Network Management Protocol (SNMP) to get information from network devices.
X
X Diagram not available
X

4.5.2.1.1 MRTG Configuration

The MRTG configuration depends on the detailed implementation. Therefore it is not possible to describe that at this stage.

4.5.3 Server 2 Windows

For information about the server hardware see Appendix E.1.

4.5.3.1 WhatsUp Gold

WhatsUp Gold is network management software. PING and Simple Network Management Protocol (SNMP) protocols are used to test connectivity to devices and to request status information from these devices. The software provides delay information to all devices and if the devices are reachable by SNMP and is allowed to have access also bandwidth and error information for each port used on that device is available.

The tool also has a build in web-server. This makes it easy to access it with a standard web browser from different locations while it is on one site installed.

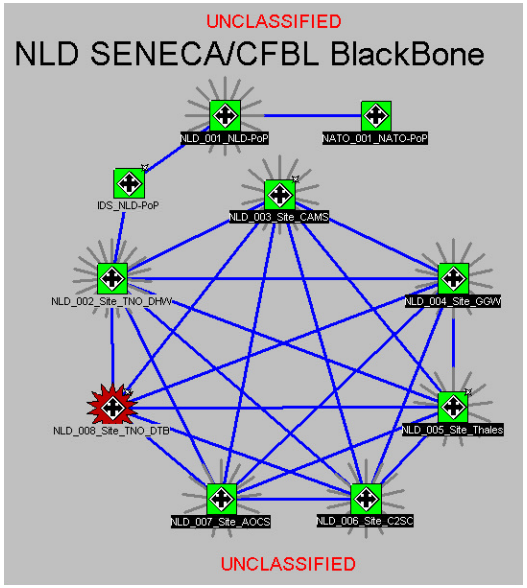

Figure 5 WhatsUp Gold Network example

4.5.3.1.1 Whats Up gold Configuration

The WhatsUp configuration depends on the detailed implementation. Therefore it is not possible to describe that at this stage.

4.5.3.2 MTRG

Multi Router Traffic Grapher (MTRG) is free software and available for windows and Linux. For live Traffic graphs of GEANT 2 network see: http://www.switch.ch/network/operation/statistics/geant2.html
MRTG shows live and history information about network devices (Used bandwidth, delay, errors). It is able to monitor all ports on all initiative switches and presents the results on a web server for easy user access on daily, weekly, monthly and yearly bases.

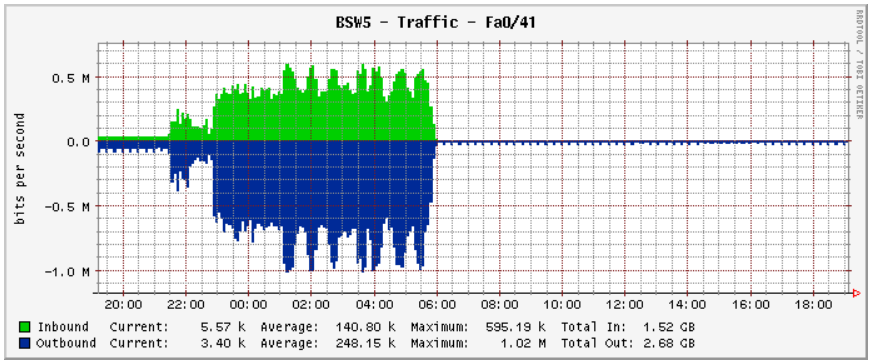

Figure 6 Network load NLD during CDEP initiative (NLD <>CFBL connection)

4.5.3.2.1 MTRG Configuration

The MTRG configuration depends on the detailed implementation. Therefore it is not possible to describe that at this stage.

4.5.3.3 Wireshark

Wireshark is a monitoring tool. The tool can look deep in the IP packet and show the interpretation of bits in the received packet header. This makes it possible to detect fragmentation, find problems in for instance multicast associations and so on. The problem is that it has to be installed on the site and remote management is not possible other then a remote desktop connection. Wireshark is a free tool.

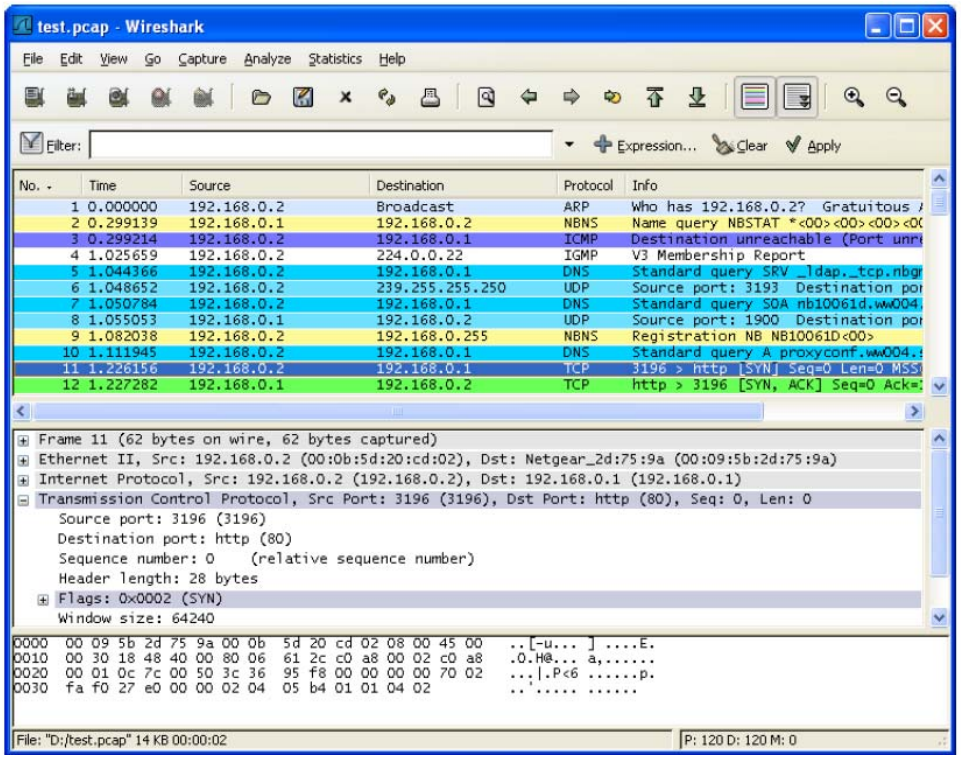

Figure 7 Wireshark window

4.5.3.3.1 Wireshark Configuration

The Wireshark configuration depends on the detailed implementation. Therefore it is not possible to describe that at this stage.

5 Test Results and Conclusions from the NETN Experiment

5.1 Intro

The MSG-068 Infrastructure Subgroup developed the initial network topology design for the Experiments. The Infrastructure consisted of three variants:

- Unclassified Network Infrastructure using Internet
- Unclassified Network Infrastructure using CFBLNet over Internet backbone
- Unclassified Network Infrastructure using CFBLNet over NATO NGCS backbone

The latter two options are closely related and will be discussed together.

5.1.1 Unclassified Network Infrastructure over Internet

The Internet was used during most of the preparation and testing for the Experiment. In order to simplify the network configuration of the assets (IP ranges, Firewall settings etc) a tool supplied by Sweden was used. This tool is named ‘Booster’. It provides a type of Virtual Private Network for HLA related traffic. The sites install a local client and a central server node is available to monitor the network and node activity, participating federates and other information. The Booster server was located in Linkoping Sweden during the preparation phase and in Bydgoszcz (Poland) during the experiment.

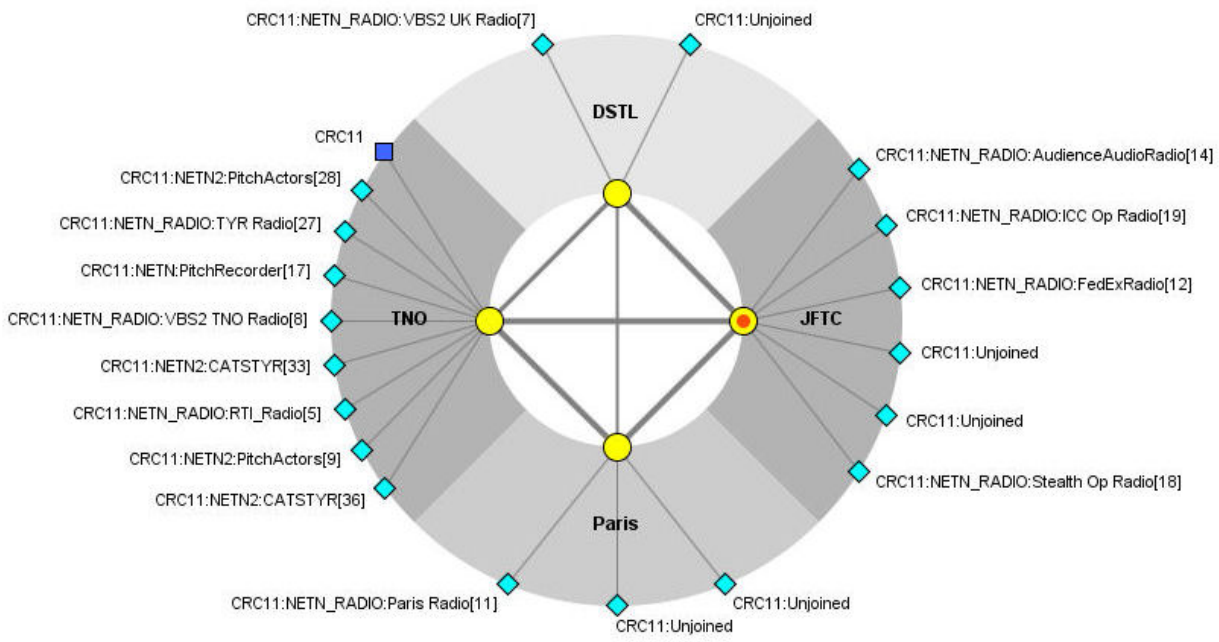

Figure 8 Booster Network Overview Diagram

5.1.2 Unclassified Network Infrastructure over CFBLNet

The MSG-068 Infrastructure Subgroup developed the initial network topology design for the Experiments. The Infrastructure was based on CFBLNet. Given the nature of the experiments (unclassified, technical feasibility demonstration) and the available resources, the decision was

taken to establish the NETN Infrastructure on an existing CFBLnet Unclass Enclave (CUE), also known as White Enclave ((future) Standing Class Enclave). The necessary paper work (CFBLNet Initiative Information Package CIIP) was produced in collaboration with the nations and the CFBLnet organization. The proposed topology with planned bandwidths is shown in the diagram below. Note that a permanent Infrastructure solution should establish a dedicated NETN Enclave under CFBLNet to simplify and streamline the process of setting up an exercise or experiment.

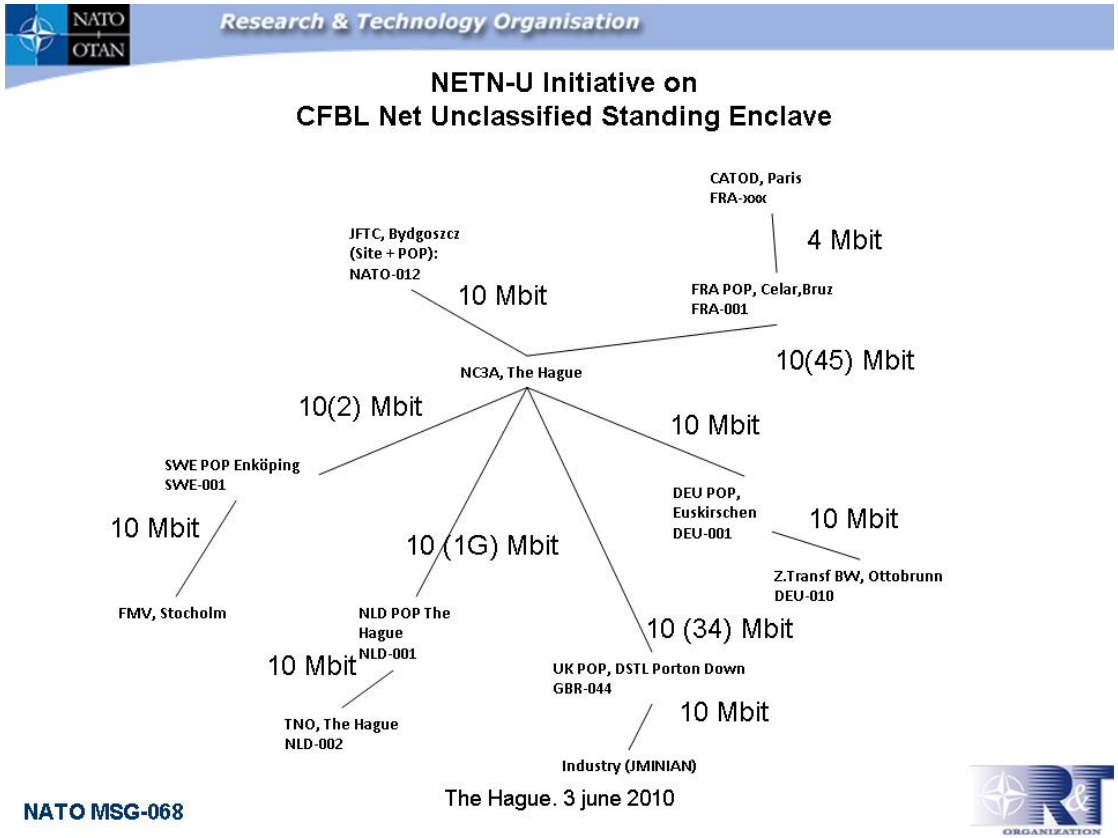

Figure 9 CFBLNet Topology as planned for MSG-068 NETN Experiment

Due to resource and scheduling issues the final topology that was used in the NETN Experiment differed from the proposal in two ways:

- Site Ottobrunn in Germany could not be connected and thus The German team did not participate in the CFBLnet based Experiments.
- Site Stockholm in Sweden could not be connected and the Swedish team moved to The Hague, Netherlands to participate in the CFBLnet based Experiments.
- The UK used the site Porton Down and did not bring Industry sites on-line.

The Spanish team moved to CATOD, Paris during the Experiment as was planned during the design phase. Note that, according to plan, several other Team members used the site in Bydgoszcz to connect their assets.

The CFBLNet was implemented under supervision of the CFBLnet national Technical POCs. Unfortunately several sites came on-line only shortly before the Experiment started. This was due to resource issues as well as to accreditation issues that needed more time to sort out than what was expected. This resulted in very limited opportunity for testing federates running over CFBLnet before the actual Experiment started.

The NETN Infrastructure was largely based on an existing CFBLnet Unclass Enclave (CUE). The new ‘legs’ (e.g. The Hague-Bydgoszcz) were initially planned to run on an NGCS backbone. Due to performance concerns an alternative was also tested that used (encrypted) Internet backbones. This Internet-based setup provided good performance, although no Quality of Service could be guaranteed.

5.2 Pre initiative test

In the pre initiative test information was collected based on available measured CFBLNet network parameters and based on specific Ping tests that provided connectivity and delay information. The tests were done on the unclassified side of the network (Appendix E.4). Testing opportunities were very limited due to late availability of the Infrastructure.

Setup wise there were two types of networks being used, namely ordinary Internet or CFBLNet. The CFBLNet type was also evaluated in two different flavors, standard CFBLNet over NGCS as well as CFBLNet over encrypted Internet. The ordinary Internet connection contained no encryption or other security measures beyond the booster encapsulation of data. Also, no traffic prioritization improvements were possible on the Internet connection. The CFBLNet over NGCS has QoS and Routing control since all traffic is routed through a separate internal network that is laid in parallel with the regular Internet connection. Due to ping/latency problems when using CFBLNet over NGCS between Bydgoszcz and The Hague a separate CFBLNet connection over encrypted Internet was tested. This encrypted Internet connection of course had the same shortcomings as the normal Internet connection since the same basic layer of connectivity was used.

5.3 Monitoring test

In the monitoring test the following information of the classified network is important to find problems:

- Used Bandwidth for the protocols used
- Delay between all sites
- Reachable services
- Fragmentation

In the Hourly Throughput below (Figure 11) a trend can be seen in that Bandwidth usage increased steadily over the course of the experiment. This is mainly due to an increased number of participants and increased radio traffic between actors. The experiment was conducted with NGCS over encrypted Internet. This caused perceived problems in that the training audience experienced failures in radio communication, mostly in the form of breakups in transmissions. A note about this is that there is no prioritization being performed during any of the stages now, neither on the network layers nor in the booster overlay. Following to this experiment a new network traffic ordering and prioritizing transport scheme is tested in the booster. The main difference is that not any one federate is allowed to send for more than a short period of time, i.e. a round-robin pattern. Latency wise the connection was very good though, the problems perceived were of the bandwidth and prioritization nature.

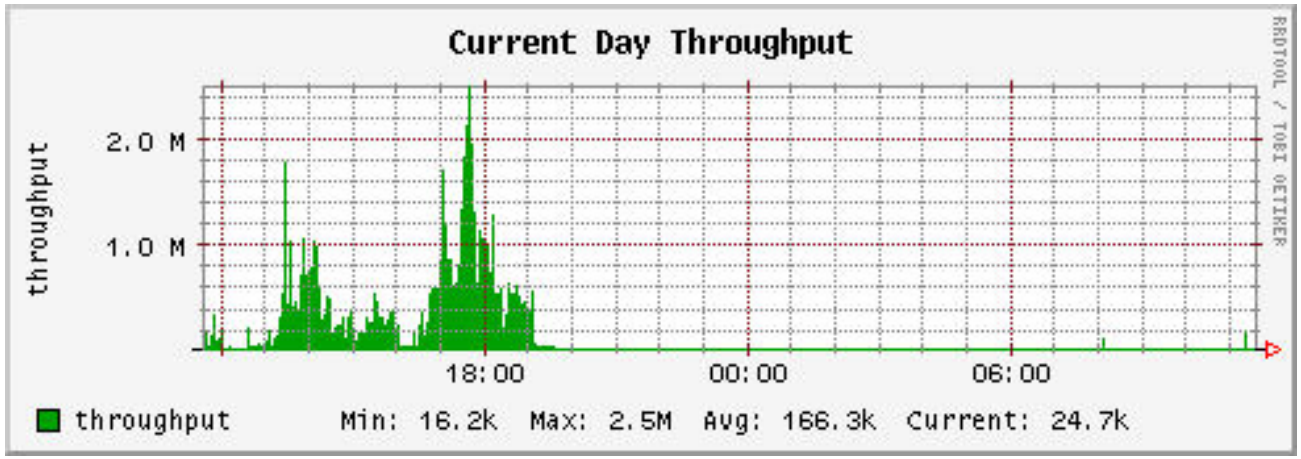

Figure 10 Daily Throughput (Afternoon 3 nov 2010 - Morning 4 nov 2010)

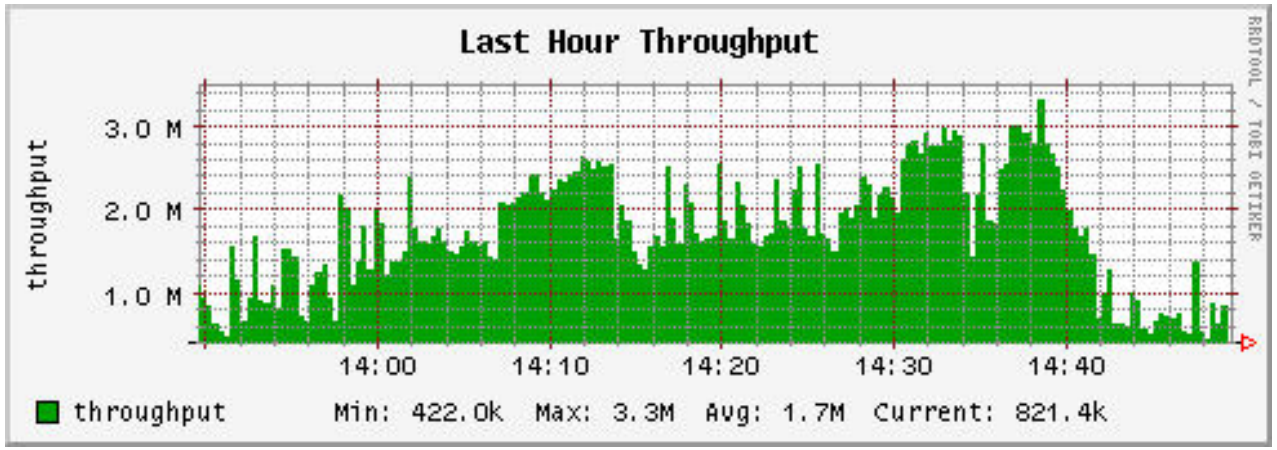

Figure 11 Hourly throughput during NLVC Experiment (Afternoon 4 nov 2010)

The Booster monitor visualizes the increased number of participants and connections during the experiment.

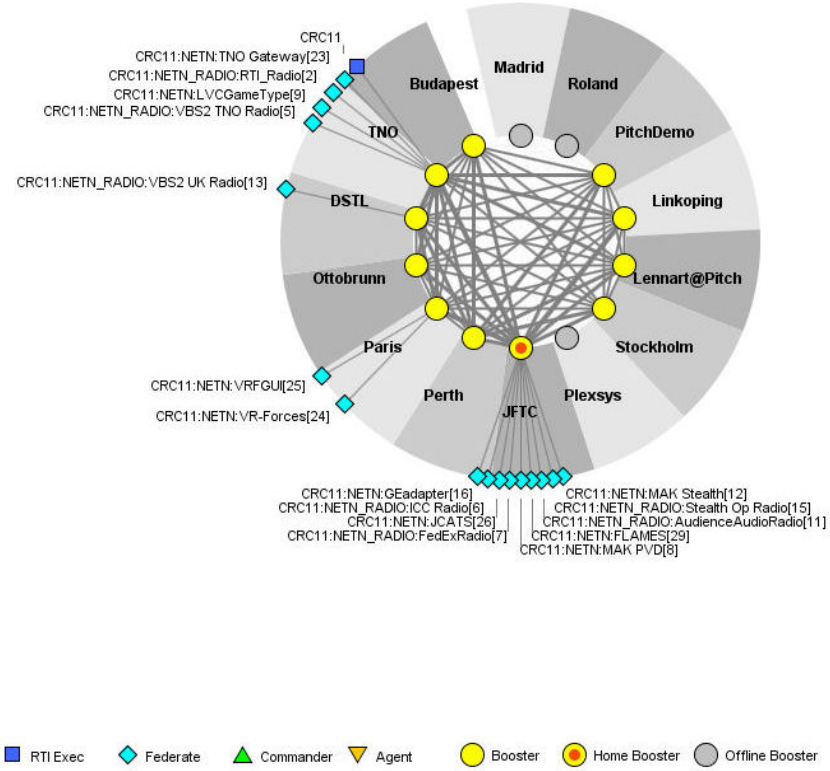

Figure 12 Booster Network Overview Diagram (Internet Experimentation)

On average the network bandwidth did not exceed 3 Mbit/s. However, this depends highly on the events (interactions) taking place during the exercise and in particular on the radio traffic which consumes much bandwidth. A problem remains that we (engineers) still don't have good way to specify what capabilities the network needs to have for a specific set of federates and a specific scenario. This includes

estimating the data rates that result from typical manoeuvring that operational pilots execute during missions and the impact of radio/voice transmissions on the required bandwidth.

The MSG-068 experience with CFBLNet showed that this infrastructure shows promise but has not yet achieved a good grip on providing a guaranteed service level wrt bandwidth, latency etc.

6 Referenced publications

1. CFBLNet-Pub1- Main-V6.0-U
2. CFBLNet-Pub1- Annex A-V6.0-U
3. CFBLNet-Pub1- Annex B-V6.0-U
4. CFBLNet-Pub1- Annex C-V6.0 Appendices-U
5. CFBLNet-Pub1- Annex C-V6.0-U
6. CFBLNet-Pub1- Annex D-V6.0 Appendices-UNRI
7. CFBLNet-Pub1- Annex D-V6.0-U
8. CFBLNet-Pub1- Annex E-V6.0
9. CFBLNet-Pub1- Annex F-V6.0
10. CFBLNet-Pub1- Annex G-V6.0-U
11. NATO STANAG 4603 – HLA
12. IEEE 1516 HLA
13. IEEE Std 1278.1a-1998
    IEEE Standard for Distributed Interactive Simulation – Application Protocols
    18 august 1998, New York
14. IEEE Std 1278.1-1995
    IEEE Standard for Distributed Interactive Simulation – Application Protocols
15. IST-CF-98-07
    Enumeration and Bit Encoded Values for Use with Protocols for Distributed Interactive Simulation Applications. This document accompanies IEEE Std. 1278.1-1995 and IEEE Std. 1278.1a-1998 June 20, 1998
16. MSG-068 NETN Network Infrastructure Design Document (Annex D of this report)

Appendix E.1 NETN SERVER Hardware

DELL™ PowerEdge™ R200 (SV4R200) € 730,00

Module	description
Base	Dual Core Intel® Xeon® E3120, 3.16GHz, 6MB Cache, 1333MHz FSB
Memory	4 GB Memory, DDR2, 800 MHz (2 x 2GB Dual Ranked DIMMs)
Optical drive stations	16 X DVD +/- RW Drive SATA
1 st hard drive	250 GB, SATA, 3.5-inch, 7.2K RPM Hard Drive (Cabled)
2 de hard drive	250 GB, SATA, 3.5-inch, 7.2K RPM Hard Drive (Cabled)
1 st RAID- or SCSI-controller card	SAS 6iR internal RAID Controller, PCI-Express
RAID-connectivity	C4 - Add-in SAS 6iR (SATA / SAS Controller) which supports 2 Hard Drives - RAID 1
Rails rack montage	Rack Rails Static Rapid
Extension card	Riser with PCI-E Support (1 x PCI-E x8 slot, 1x PCI-E x4 slot)
System management	Open Manage Software loaded and DVD Kit
Operating System	Not Included
Bezel	Power Edge R200 Bezel Assembly

Appendix E.2 NETN Client Hardware

Module	description
Base	
Memory	
Optical drive stations	
1 st hard drive	
2 de hard drive	
1 st RAID- or SCSI-controller card	
RAID-connectivity	
Rails rack montage	
Extension card	
System management	
Operating System	
Bezel	

Appendix E.3 NETN Infrastructure Test Tool Specifications

Tool Description	Operating system	Version	Date	Vendor	Website	Approx. Costs	Remarks
WhatsUp Gold	windows					E 2000,-	
MRTG	LINUX	latest			MRTG	free	Multi Router Traffic Grapher (MTRG) is free software and available for windows and Linux.

Appendix E.4 Measured Average Delay between National CFBLNet PoPs (January 2009)

CFBLNet BlackBone

	AUS	CAN	DEU	FRA	GRB	ITA	NATO	NLD	NZL	USA	SWE	
AUS												
CAN												
DEU												
FRA												
GRB												
ITA												
NATO	390	170	24	25	30	140		1	450	135		
NLD	390	170	24	25	30	140	1		450	135		
NZL												
USA												
SWE												

All times are in milliseconds

NETN enclave (Data removed due to declassification)

	AUS	CAN	DEU	FRA	GRB	ITA	NATO	NLD	NZL	USA	SWE	
AUS												
CAN												
DEU												
FRA												
GRB												
ITA												
NATO												
NLD												
NZL												
USA												
SWE												

All times are in milliseconds