Network Infrastructure Design Document

for

NATO Education and Training Network (NETN)

Developed by MSG-068 NETN – Infrastructure Working Group

Roel Wymenga (TNO)
Robbert Krijnen (TNO)
Wim Huiskamp (TNO)
Edgar Harmsen (NC3A)

1 Table of contents

1 Table of contents ... 2
2 Definitions and Abbreviations ... 4
2.1.1 NETN usage ... 5
2.1.2 NETN nations involved ... 5
2.2 Applications and information flow ... 5
2.2.1 Information flow between applications ... 6
2.2.2 Information flow between sites ... 7
2.2.3 Bandwidth ... 7
2.2.4 Delay (latency) and jitter ... 7
2.2.5 Availability and Reliability ... 7
2.2.6 Security ... 7
3 National Defense network infrastructure overview ... 8
3.1.1 National and Organisational Network Infrastructures ... 8
4 Selection of Network Infrastructure for NETN ... 10
4.1 International Network infrastructure overview ... 10
4.1.1 CFBLNet ... 10
4.1.2 NGCS ... 11
4.1.3 BICES ... 12
4.1.4 GEANT ... 12
4.1.5 Public Internet ... 13
4.1.6 Proprietary networks on leased lines ... 13
4.2 International Network infrastructure selection ... 14
5 Combined Federated Battle Laboratories Network (CFBLNet) ... 15
5.1 History ... 15
5.2 CFBLNet organisation ... 16
5.3 CFBLNet Architecture and Terminology ... 17
5.3.1 CFBLNet Levels ... 17
5.3.2 Enclaves ... 18
5.4 CFBLNet countries and sites involved ... 19
6 NETN Network design ... 20
6.1 Introduction ... 20
6.2 Network concept ... 20
6.2.1 Hardware ... 21
6.3 Security ... 22
6.3.1 Accreditation ... 22
6.3.2 Classification ... 23
6.3.3 Marking ... 23
6.3.4 Crypto ... 23
6.3.5 Key material ... 23
6.4 Protocols and Services ... 24
6.4.1 Protocol translation ... 24
6.4.2 Protocol support ... 24
6.4.3 Quality of Service (QoS) ... 25
6.4.4 Network Services ... 25
6.5 Data flow and capacity ... 25
6.5.1 MTU size enclave routers ... 26
6.5.2 MTU size enclave crypto ... 26
6.6 Network topology ... 26
6.6.1 Black Network (International network) ... 26
6.6.2 Crypto network ... 27
6.6.3 Enclave router network ... 28
7 NETN Network Management and Network Support Services ... 29

7.1 NETN Network Operation Centre (NOC) ... 29
7.2 NETN Network Services ... 29
7.2.1 Domain Name System (DNS) ... 29
7.2.2 Simple Network Management Protocol (SNMP) ... 29
7.2.3 File Transfer Protocol (FTP) ... 29
7.2.4 E-Mail ... 29
7.2.5 Voice over IP (VoIP) ... 29
7.2.6 Network Time Protocol (NTP) ... 29
7.2.7 VTC ... 30
7.2.8 Wiki Webserver ... 30
7.2.9 Quality of Service ... 31
7.2.10 Network Monitoring ... 31
8 NETN Simulation Interoperability and Simulation Support Services ... 33
8.1 Simulation Interoperability ... 33
8.1.1 HLA-RTI and Central RTI Component (CRC) ... 33
8.1.2 HLA-RTI and Local RTI Component (LRC) ... 33
8.1.3 HLA-RTI and Web Service Provider RTI (WSPRC) ... 33
8.2 Simulation Support Services ... 33
8.3 Execution Control ... 34
8.4 Database Services ... 34
8.5 Bridge or Gateway Services ... 34
9 NETN Infrastructure Budget Requirements ... 35
9.1 CFBLNet Business model ... 35
9.2 CFBLNet Subscription Costs ... 35
9.2.1 CFBLNetwork Cost Estimates ... 35
9.2.2 International network Costs ... 37
9.2.3 National network Costs ... 37
9.2.4 CFBLNet National PoP / Access node considerations ... 37
10 Referenced publications ... 39

2 Definitions and Abbreviations

ACT	Allied Command Transformation
ASTi	Advanced Simulation Technology, inc.
CFBLNet	Combined Federated Battle Laboratories Network
CLR	CFBLNet Lead Representative
CRC	Central RTI Component (HLA)
CWE	Collaborative Work Environment
DIS	Distributed Interactive Simulation
DNS	Domain Name System
DWG	Documentation Workgroup
FAD	Federation Agreements Document
FTP	File Transfer Protocol
Gbit/s	Giga bit per second
HLA	High Level Architecture
IP	Internet Protocol
IWG	Initiative Workgroup
JCATS	Joint Conflict and Tactical Simulation
JFTC	Joint Forces Training Command
JTLS	Joint Theatre Level Simulation
JWC	Joint Warfare Centre
LAN	Local Area Network
LVC	Live, Virtual, Constructive
Mbit/s	Mega bit per second
MSG	(NATO) Modelling & Simulation Group
MSAB	Multinational Security Accreditation Board
NATO	North Atlantic Treaty Organization
NC3A	NATO Command & Control and Consultation Agency
NETN	NATO Education and Training Network
NMSG	NATO Modelling & Simulation Group
NRF	NATO Response Force
NTP	Network Time Protocol
NWG	Network Workgroup
PoP	Point of Presence
POP3	Post Office Protocol version 3
QoS	Quality of Service
RTI	Run Time Interface (HLA)
SENECA	Simulation Environment for Network-Enabled Capability Assessment (Dutch national NEC network)
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
STANAG	Standard NATO Agreement
SWG	Security workgroup
TG	Task Group
VoIP	Voice over Internet Protocol
VTC	Video Tele Conference
WAN	Wide Area Network

This document is the deliverable of the MSG-068 NETN Infrastructure Working group and provides the infrastructure design and recommendations for implementation.

2.1.1 NETN usage

NETN connectivity should be flexible in the sense that nations and organisations that have access to the NETN infrastructure will be able to perform exercises or experiments in different configurations. In some cases all nations may want to join a specific event, in other cases, a (small) numbers of nations may use NETN for a particular training exercise or mission preparation event.
NETN is intended to become a permanent (persistent) NATO capability. The preparation time to set up a particular event should be minimised as a result of the permanent character of NETN. As NETN consists of four projects the initial and full operational capability will be implemented in phases according to the project plans. Testing and incremental implementation/upgrading is expected to take several years. Additional sites and new applications will be added during these years.

2.1.2 NETN nations involved

The following nations and organisations were initially involved in NETN when planning was started for the infrastructure design.

Table 1 nations and organisations originally involved

Country	NATO Country Code	Number of sites
Australia	AUS	?
Bulgaria	BGR	?
Czech Republic	CZE	?
France	FRA	3
Germany	DEU	3
Italy	ITA	?
NATO	NATO	1
Netherlands	NLD	1
Romania	ROU	?
Slovenia	SVN	?
Spain	SPA	1
Sweden	SWE	?
Turkey	TUR	?
United Kingdom	GBR	?
United States	USA	?

Note: in the final experiments of NETN (2010) several nations moved their assets to other sites and participated from that location.

2.2 Applications and information flow

The following applications are foreseen in NETN:

- Simulators (including simulated radio and data links), possibly with hardware in the loop for training purposes. Simulation interoperability will be based on the High Level Architecture (HLA) IEEE 1516 as agreed by STANAG 4603.
- C2 systems, mainly identical to the applications that are used operationally

- Video Tele Conferencing (VTC) for exercise mission briefings, mission planning and after action review.
- Video Tele Conferencing (VTC) for technical briefings, technical planning and technical after action review.
- VoIP for technical management and control (before, during and after the exercise)
- Network remote management, control and monitoring
- Network Time synchronisation (using Network Time Protocol NTP)

Also classified data storage and data exchange for planning, results, documentation etc should be accessible from all sites. This includes:

- E-mail
- Webservers, WIKI based collaborative workspaces
- FTP servers (e.g. to distribute scenario data)

All mandatory applications should be available at all sites.

Table 2 Applications

Application	Protocols	Remarks
VoIP	Mandatory	
Simulation	Mandatory	HLA IEEE 1516 (according to STANAG 4603) using a FOM based on the NETN reference FOM which is based on RPR-FOM 2d17. Note: legacy systems using DIS or HLA 1.3 need adapters/bridges/gateways.
C2, Datalinks	Mandatory	HLA IEEE 1516 (according to STANAG 4603) using a FOM based on the NETN reference FOM which is based on the HLA Link 16 BOM (SISO-STD-002-2006). Note: legacy systems using SIMPLE, MTDS, or NACT need adapters/bridges/gateways.
Radio Simulation	Mandatory	HLA IEEE 1516 (according to STANAG 4603) using a FOM based on the NETN reference FOM which is based on RPR-FOM 2d17. Notably ASTi systems
VTC	Mandatory	
Storage	Mandatory	

2.2.1 Information flow between applications

The proposed solution from a user perspective should be to provide a number of physically separated networks that are dedicated to a certain type of information flow. For example a network dedicated to (HLA based) simulation data, another network intended for C2 related data and networks reserved for VoIP, VTC etc. The functionally separated networks would in fact be logical channels that all share the same network infrastructure on the WAN between nations or sites. Network configuration control would allow a flexible allocation of WAN bandwidth to specific data channels. This method would provide maximum bandwidth to the simulation channel during an exercise, while

reallocating this WAN bandwidth to VTC channels during Briefings and Debriefing sessions.

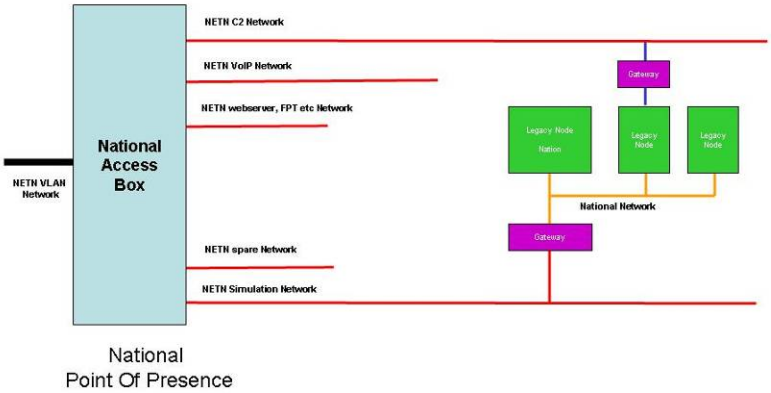


Figure 1 Assigning WAN bandwidth to logical channels

2.2.2 Information flow between sites

It should be possible that all mandatory applications can function on all sites involved in a particular NETN event. The network should be ‘fully meshed’ and suitable for classified data exchange among all sites.

2.2.3 Bandwidth

Several applications require significant bandwidth. However, the required bandwidth depends on the training scenarios and the applications that are in use for the scenario. In most cases, not all of the applications listed above will be operational at the same time (e.g. VTC and Simulations). The NETN infrastructure should allow a flexible allocation of the available WAN bandwidth to different applications depending on the needs. The WAN bandwidth capacity should be scalable and upgrades or downgrades should be relatively painless.

2.2.4 Delay (latency) and jitter

Several applications are time critical therefore the delay or latency and especially jitter should be kept at as low as possible. Typical maximum acceptable latency values for real-time (man-in-the-loop) simulations are 100ms between any two applications. The performance levels should be guaranteed to a defined minimum or maximum, thus providing a certain Quality of Service (QoS).

2.2.5 Availability and Reliability

The NETN is intended for training purposes. It should be available and reliable for continuous periods of several sequential days. The mean downtime should be minimal and downtime due to maintenance etc should be planned in advance and needs to be scheduled in agreement with the user community.

2.2.6 Security

NETN should be able to handle SECRET data. Nations or organisations that are not involved in a particular event taking place on the NETN infrastructure should not have access to the data related to that event.

3 National Defense network infrastructure overview

Nations and Organisations often use an isolated part of their national defense network infrastructure to form distributed education and training capability able to support training. The isolation is primarily required to avoid disruption of operational systems and capabilities and provide a controlled sandbox for the distributed education and training capability. This paragraph visualise the main characteristics[i] from the national and organisational network in support of Allied and Coalition Education, Training, and /or Research and Development within nations/organisation.

This chapter provides an overview of several national networks as identified by the national experts of the MSG-068 Network Infrastructure subgroup.

3.1.1 National and Organisational Network Infrastructures

3.1.1.1 Australia

Defence Wide Area Communications Network (DWACN). Externally the Combined Federated Battle Lab (CFBL) network has also been used for international DSTO networking exercises.

3.1.1.2 Bulgaria

3.1.1.3 Czech Republic

3.1.1.4 France

EXAC C3R Secure Network for Experiment and Referentiel d'Interoperabilite Technique (RIT). The Celar, Bruz element of EXAC C3R is also the France PoP in the Combined Federated Battle Laboratories Network (CFBLNet), enabling connection to this Multi-National Network.

3.1.1.5 Germany

German Experimental Network which is a VPN based network over the German Defense WANBw (WAN Bundeswehr) and/or Digitales Ubertragungs Net Bundeswehr. The German Experimental Network could also use public infrastructure with VPN technology. The main Point of Presence of the German Experimental Network Euskirchen, is also the German PoP in the Combined Federated Battle Laboratories Network (CFBLNet), enabling connection to this Multi-National Network.

3.1.1.6 NATO

3.1.1.6.1 NATO General Communications System (NGCS) is the basic communications infrastructure for all NATO communications. It addresses voice and data transmission requirements, circuit-switched and packet-switched, for both unclassified and classified (up to NATO SECRET) communications. NGCS connectivity ranges from Norway to Greece and from Norfolk, Virginia in the US to Kabul in Afghanistan including all NATO Commands and Primary facilities plus most of the NATO nations MOD. The operation and maintenance of NGCS is the responsibility of the NATO CIS Services Agency (NCSA). On request NGCS can support Exercises and Training capacity for and between NATO Commands and facilities.

3.1.1.6.2 NATO Combined Federated Battle Laboratories Network (CFBLNet) provides the NATO and European main Point of Presence for NATO organisations, NATO nations and mission partners. High speed Wide Area Network links are used to interconnect the CFBLNet participants.NATO Facilities typically utlises the NGCS network (prefered) or dedicated leased lines to connect to the NATO CFBLNet PoP located in NATO C3 Agency ,The Hague, Netherlands.

3.1.1.7 The Netherlands

The Netherlands uses a CFBLNet extension for all experiments to connect military sites inside the Netherlands with each other and also to other countries through

CFBLNet. This network is called SENECA/CFBLNet and is a 1Gbit/s Virtual Private Network (VPN) special created for this purpose on top of a 10 Gbit/s MOD network and is available on almost all MOD sites. At this time 8 sites are connected and this could become more in the near future. SENECA/CFBLNet is connected to the NATO CFBL PoP at NC3A in The Hague through the NLD-PoP. Several security enclaves are available on top of this SENECA/CFBLNet.

3.1.1.8 Romania

3.1.1.9 Slovania

3.1.1.10 Spain

There are several sites in Spain involved in coalition experimentation.

3.1.1.11 Sweden

The Point of Presence of the Sweden armed forces Enkoping, is also the Swedish PoP in the Combined Federated Battle Laboratories Network (CFBLNet), enabling connection to this Multi-National Network.

3.1.1.12 Turkey

3.1.1.13 United Kingdom

The UK Joint Multi-National Information Assurance Network (JMNIAN) is a project managed by the Integration Authority's (IA) Defence Test and Reference Co-ordination Office (DT&R CO). It provides a secure Asynchronous Transfer Mode (ATM) Wide Area Network (WAN) that will connect Test & Reference sites. Points of Presence (PoPs) at test sites provide connectivity to the WAN. The JCMB ARTD element of JMNIAN is also the UK PoP in the Combined Federated Battle Laboratories Network (CFBLNet), enabling connection to this Multi-National network. Key features of JMNIAN are: It has a high bandwidth, and can operate in near real-time; It supports a variety of standards/protocols, such as Serial, ISDN and IP; It will be accredited to SECRET.

3.1.1.14 United States

3.1.1.14.1 Defense Information Systems Network (DISN)

DISN as DOD's networking capability for the transfer of information in support of military operation in the context of the Global Information Grid (GIG). It further specifies that DISN shall be the means for wide-area and metropolitan-area networking.

3.1.1.14.2 Joint Training and Experimentation Network (JTEN)

JTEN is the communications network for the Joint National Training Capability (JNTC), U.S. Joint Forces Command (USJFCOM). This network will be interconnected with CFBLNet July2009 in support of Coalition JTEN Initiatives.

3.1.1.14.3 Combined Federated Battle Labs Network (CFBLNet) environment which utilizes a distributed Wide Area Network (WAN) as the vehicle to experiment with new capabilities by conducting Research and Development, Trials and Assessment including Training initiatives. The U.S. CFBLNet infrastructure is extensive and reaches to international demarcation points for the Southern Hemisphere and Europe.

4 Selection of Network Infrastructure for NETN

4.1 International Network infrastructure overview

This chapter looks into network solutions for the international infrastructure which were identified by the experts of the MSG-068 Network Infrastructure subgroup.

4.1.1 CFBLNet

Figure 2 CFBLNet logo

The Combined Federated Battle Laboratories Network (CFBLNet) is a network build, maintained and constantly improved by its members. The network is available for experiments and training with different classifications and markings. Several nations and NATO organizations have permanent connections to CFBLNet, while others establish a connection when needed. CFBLNet is more than a network, It features standard services like, Network management, Crypto management, DNS, Web, E-Mail, Voice, FTP, Network Time server and VTC(on request). CFBLNet has an efficient organisation, proven processes and documents and includes a CFBLNet secretariat to assist the users in its optimum use of the CFBLNet capabilities. It has extensive knowledge on coalition classified networks, security accreditation and rules, crypto technology and interactions between simulators and network protocols. The use of CFBLNet for NETN may at first glance look expensive, but the countries already connected to CFBLNet use the network and organisation for multiple initiatives. A new initiative like NETN should consider that the fixed costs are already paid for. CFBLNet allows using various WAN links, including leased lines, SatCom, NGCS, (and tunnelling using the internet (with special measures)). CFBLNet is a closed network. CFBLNet provides you an established, stable international network with proven information assurance measures, and the support of a robust environment. This results in a sustainable and accreditable architecture to effectively field equipment and services.

CFBLNet has been used to minimize risk in systems prior to deployment to the war fighter; reducing costs and countless hours of development. CFBLNet has an effective method for integrating and improving interoperability with allied and coalition partners. CFBLNet has hosted many multi-national C4ISR events and has a track record of success that speaks for itself:

- CWID
- Fleet Synthetic Training-Joint
- Multi-National Experiment
- Empire Challenge
- Blue Force Tracker
- NATO ALTBMD

The CFBLNet has supported several key warfighting Initiatives, including: multi-national connectivity for air picture; messaging services; collaboration; multi-level security Initiatives; homeland defense and crisis response tools; ship-to-ship command and control; unmanned aerial vehicle imagery; and situational awareness via enhanced tactical data link interoperability. Imagery and video systems proven on CFBLNet are currently supporting operations in Afghanistan and Iraq. The network also supported key second-tier warfighting objectives including on-line distributed war gaming and multinational training exercises. Some specific success stories include the following:

- Intelligence, Reconnaissance and Surveillance (ISR) lessons learned in live and unmanned aircraft and satellite surveillance in Empire Challenge 06 were applied immediately in support of International Security Assistance Force (ISAF) – Afghanistan.
- In Project Churchill, the US-UK bilateral trials led to enhanced communications capabilities for Unmanned Combat Air Systems.
- The United Kingdom International Support Team (UK-IST III) and the US conducted experiments that established real time wargaming for C2, consultation, and future consequence mitigation.
- NATO is very successfully using CFBLNet for the NATO ALTBMD program, where CFBLNet interconnect all involved ALTBMD sites and support HLA/DIS, link, voice, VTC and other traffic to the network distributed systems, including hardware in the loop (HWIL) within the involved nations.

4.1.2 NGCS

NATO General Communications System (NGCS) is the basic communications infrastructure for all NATO communications. It addresses voice and data transmission requirements, circuit-switched and packet-switched, for both unclassified and classified (up to NATO SECRET) communications. NGCS connectivity ranges from Norway to Greece and from Norfolk, Virginia in the US to Kabul in Afghanistan including all NATO Commands and Primary facilities plus most of the NATO nations MOD. The operation and maintenance of NGCS is the responsibility of the NATO CIS Services Agency (NCSA). On request NGCS can support Exercises and Training capacity for and between NATO Commands and facilities.

NGCS is evolving their capabilities to the NATO Network Enabled Capability Network and Network and Information Systems Infrastructure (NNEC-NII) which is based on the NCGS Protected Core Network (P-Core), an MPLS Transport backbone with Traffic Engineering extension. The evolving capability, expected to be fully available 2012/2013 will support the coloured cloud principle on top of the transport network. The main Coloured clouds will be NS, NU/NR and MS. In support of specific requirements or for training, exercises and events, VPN can be provisioned with the main clouds (equal classification/releasability) or separate Coloured clouds can be provisioned for other classification/releasability or specific requirements. For these separated Coloured clouds the management aspects needs to be taken into account.

The NGCS Transport and Coloured clouds fully support Quality of Service (QoS), are Service Level Managed with SLA's from a NGCS Services catalogue providing SLA templates.

The NGCS P-Core going to be coupled with the national defense networks with the use of Packet Network gateways capability. Initial on L2 level best effort (phase I: 2010), later also on Layer 3.

Topic of attention:

- Accreditation is required for applications.
- Restrictions and issues connecting simulations and operational systems
- Intended for use between NATO sites rather than national assets.

4.1.3 BICES

Figure 3 BICES logo

Battlefield Information Collection and Exploitation Systems (BICES) is an operational NATO network. The objective of BICES is to share and exchange information / intelligence among the participating Nations and with NATO in peace, crisis and war through the use of interoperable Automatic Data Processing (ADP) based national and NATO intelligence support systems. BICES is a network reserved for operations and not for experiments or training. This implies that applications and systems need accreditation before they can be used on BICES. BICES is not available on many sites that were listed for NETN.

4.1.4 GEANT

Figure 4 GEANT logo

GEANT provides low latency and high throughputs, which makes it suitable for distributed test beds with unclassified and near real-time requirements. GEANT is the interconnecting network to the national academic research networks like for instance SurfNET in the Netherlands. However, several issues have been identified in GEANT:

- There is not always a guaranteed bandwidth, latency or Quality of Service available.
- Many countries do not allow SECRET networks operating over open networks or networks connecting the internet. GEANT has interconnections to internet.
- GEANT and its national networks are an academic research network and is not available on military sites (only research institutes and universities)

4.1.5 Public Internet

The public Internet is readily available at almost any location on earth. The connection costs are in general very low. The issues regarding the use of the public Internet for NETN are:

- There is no guaranteed bandwidth, latency or Quality of Service available. Contracts with Internet Service Providers (ISPs) do not in general provide solid performance guarantees.
- Many countries do not allow SECRET networks operating over open networks or networks connecting to the internet.

Remarks: USA and UK have stated that classified simulation assets are not allowed to have connections to open internet. The Open Internet and VPNs have been used for several experiments (e.g. FMV SmartLab Sweden).

4.1.6 Proprietary networks on leased lines

Proprietary networks on leased telecom lines can be made available at almost any location on earth. The connection costs are in general significant. The issues regarding the use of proprietary networks for NETN are:

- Guaranteed bandwidth, latency and Quality of Service are in general available at a price.
- A management organisation needs to be in place to negotiate contracts with telecom operators and deal with technical issues and maintenance.

4.2 International Network infrastructure selection

The table below compares the international network solutions for NETN which were presented above.

Table 3 Network comparison

	CFBLNet	BICES	NGCS (current)	NGCS (NNEC-NII)	GEANT	Internet	Leased lines
Network physical available	YES	YES	YES	YES	YES	YES	YES
Network available to all NETN participants	YES	NO	YES[1]	YES	YES (through internet)	YES	YES
Allowed to carry SECRET information by national security rules	YES	YES	YES	YES	NO	NO	YES with additional security measure s
Organisation has knowledge of classified networks	YES	YES	YES	YES	NO	NO	NO
Ownership	All MODs connected	NATO	NATO	NATO+ MOD connected		ISPs	Telecom operator
Black Network management	Available	Available	Available	Available	Not available	Not available	Not available
Security organisation in place	YES	YES	YES	YES	NO	NO	NO
Security measures and procedures in place	YES	YES	YES	YES	NO	NO	NO

Given the NETN requirements and the comparison of the available infrastructure options, the MSG-068 Infrastructure Working group has decided to base the design of the network infrastructure on the Combined Federated Battle Laboratory (CFBL) Network. CFBLNet will be the black (unclassified) backbone between participating nations and NATO organisations. The next chapters will discuss the infrastructure design in more detail.

[1] Network available to all NATO nations. To non-NATO nations through specific separate domain build or using Information Exchange gateways.

5 Combined Federated Battle Laboratories Network (CFBLNet)

The Combined Federated Battle Laboratories Network (CFBLNet) is a network build, maintained and constantly improved by its members. The network is available for experiments and training with different classifications and markings. Several nations and NATO organizations have permanent connections to CFBLNet while others establish a connection when needed.

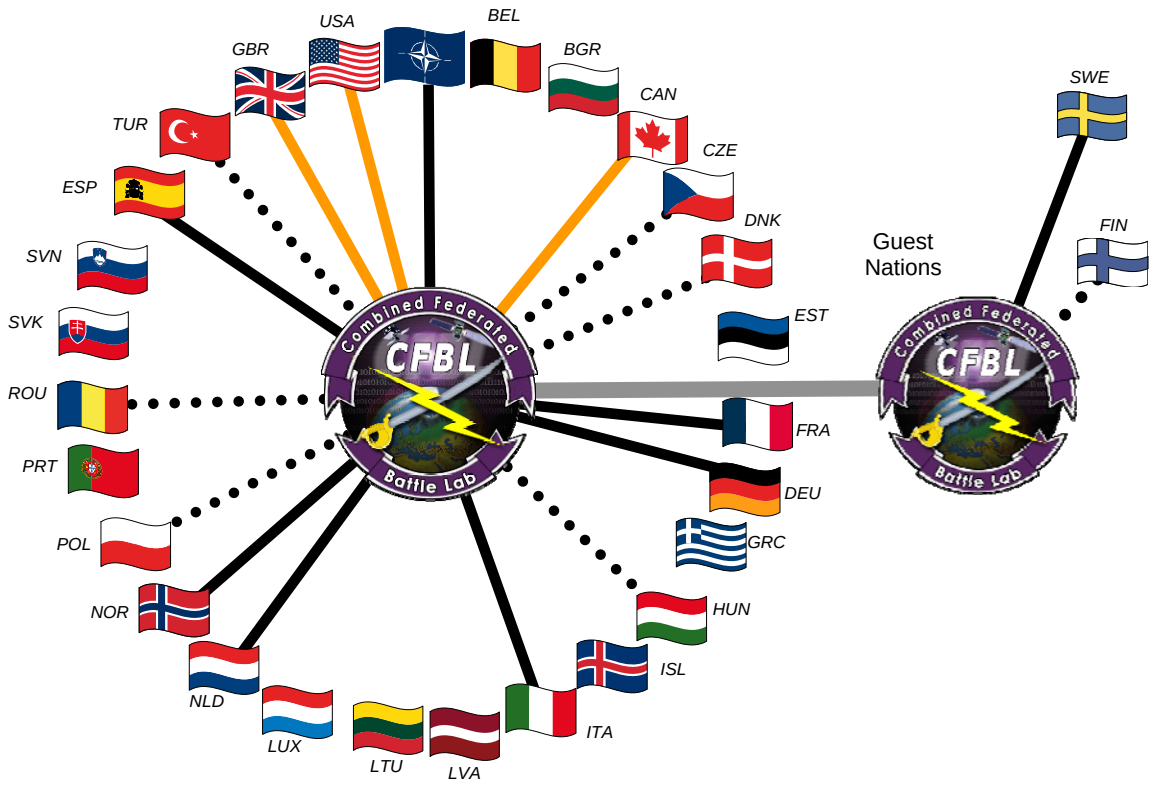


Figure 1 CFBLNet countries,
NATO nations and Partners perspective (January 2009)

5.1 History

In April 1999, the US made a proposal to the NATO C3 Board to establish a Combined Federated Battle Laboratories Network (CFBLNet). The Concept was to build on the Combined Wide Area Network (CWAN) that had been established each year for JWID, to establish a year-round network for research, development, trials, and assessment operating at a Combined Secret Releasable accreditation level.

The participants would include the US, the Combined Communications-Electronics Board (CCEB), and NATO. NATO in the CFBLNet context, are all individual NATO nations and NATO the organisation. The Network would be used to develop coalition interoperability, doctrine, procedures and protocols that can be transitioned to operational coalition networks in future contingencies.

The CFBLNet will leverage Coalition Warrior Interoperability Demonstration (CWID), formerly JWID, resources and existing NATO and national laboratories and test beds. It is not a US owned network. As a combined network, the participants will have equal say in its utilization and management, yet specific initiatives may be configured between any numbers of participants. The CFBLNet participants are to respect sovereign and intellectual property rights of activities conducted on the network.

5.2 CFBLNet organisation

The CFBLNet will fall under the oversight of a CFBLNet Senior Steering Group (C-SSG), comprised of three Flag level executives representing U.S., NATO, and CCEB. Control of the CFBLNet will be conducted by a CFBLNet Executive Group (C-EG) of 06 (or equivalent) level members also representing US, NATO and CCEB, working for the C-SSG members. The C-EG may stand up subordinate groups as required.

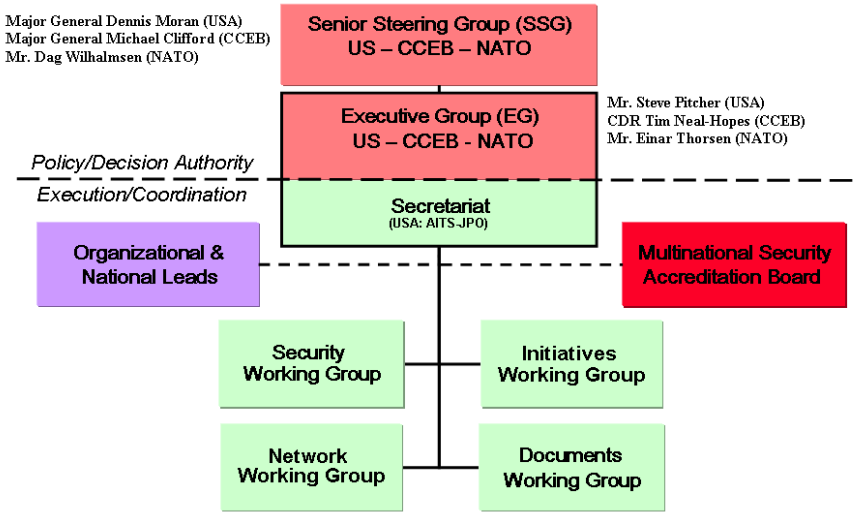


Figure 2 CFBLNet organisation (2008)

There are several roles in the CFBLNet organisation. These roles are:

- The CFBLNet Lead Representative (CLR) is responsible for coordination within the CN/O; Initiatives, work, equipment, crypto, accreditation, etc.
- The Networking Working Group (NWG) is responsible for building and maintenance the required network and enclaves.
- The Security Working Group (SWG) is responsible for the security on the network (PoP) and in the enclaves.
- The Document Working Group (DWG) is responsible for correct documentation
- The Initiative Working Group (IWG) is responsible coordination of initiatives
- The national Multinational Security Accreditation Board (MSAB) representative is responsible for accreditation of the national sites and initiatives.

One of the big advantages of this construction is that several national MSAB representatives taking part in the Security Working Group (SWG) and are at the CFBL Management Meetings each 6 month.

Multinational Security Accreditation Board

5.3 CFBLNet Architecture and Terminology

CFBLNet is a network build and maintained by its members. The network consists of sites, national *Point of Presence* (PoPs), infrastructure, services and knowledge management. The national / organisational PoP is the connection from the national / organisational *Wide Area network* (WAN) to the international part of the CFBL WAN.

Backbone Infrastructure
The *BLACKBONE* (= Black backbone) provides a common, closed, unclassified IP routed network layer implementation using a mixture of both ATM and IP bearer networks. Its primary purpose is to transport encrypted traffic throughout the network.

Enclaves are the cryptographic protected networks on top of the CFBLNet BlackBone. Each enclave has a *classification* and a *marking* indicating security level and the countries allowed connecting.

Initiatives use the Enclaves to exchange data.

5.3.1 CFBLNet Levels

5.3.1.1 CFBLNet Level 0 the international network

The CFBLNet level 0 network is the network between nations and/or NATO organisations. There are three regional PoPs (Europe, North America and Oceania) connecting the nations / organisation PoPs. The national / organisation PoPs connect the nations / organisation sites to the international.

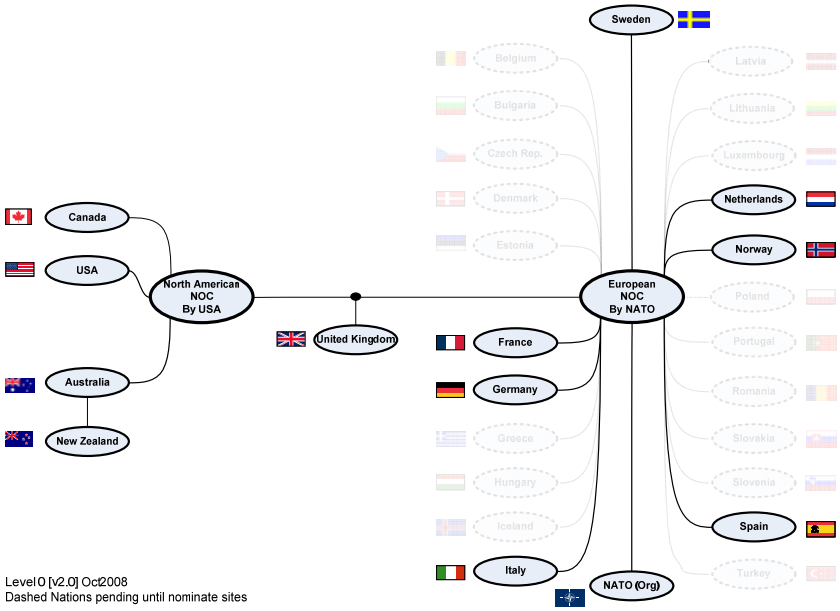


Figure 5 Level 0 connections (December 2008)

5.3.1.2 CFBLNet Level 1 the national network

The CFBLNet level 1 network is the network between national PoPs and the national sites. The national PoP's network and sites are maintained by national CFBLNet organisation.

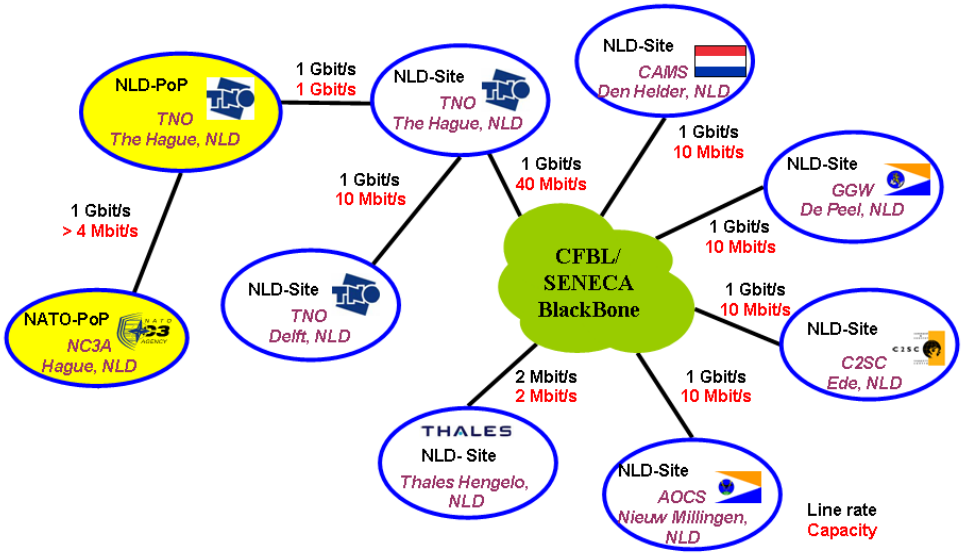


Figure 6 NLD example Level 1 connections (January 2009)

5.3.1.3 Level 2 is the site network

The CFBLNet level 2 network is the network at the national sites. The architecture differs for almost all sites but it consists at least of a black router, a crypto and a red router.

5.3.2 Enclaves

There are several security enclaves on CFBLNet.

- The CFBLNet BLUE enclave is a permanent classified IP routed logical network operating over the BLACKBONE. It will operate as a System High logical network at the SECRET level, releasable to AUSCANNZUKUS + NATO;
- The CFBLNet RED enclave is also a permanent classified IP routed logical network operating over the BLACKBONE. It will operate as a System High logical network at the NATO SECRET level.
- The CFBLNet Unclassified Enclave (CUE). The CUE is a permanent enclave operating over the BLACKBONE.
- Temporary enclaves are created for a finite period to support the execution of specific Initiatives and operating over the BLACKBONE. The level of classification and release caveats used within these enclaves will be determined by the Initiative requirements.

    - The CFBLNet GREEN enclave is a temporary classified IP routed logical network operating over the BLACKBONE. It will operate as a System High logical network at the SECRET level, releasable to AUSCANNZUKUS + NATO + Sweden;

5.4 CFBLNet countries and sites involved

Currently, there are already many sites connected to CFBLNet.

Nation/Organization	Number of Sites
Australia (AUS)	13
Canada (CAN)	29
United Kingdom (GBR)	37
New Zealand (NZL)	6
Germany (DEU)	17
Spain (ESP)	3
France (FRA)	3
Italy (ITA)	8
NATO	9
Netherlands (NLD)	8
Norway (NOR)	7
Poland (POL)	1
Sweden (SWE)	1
USA	22
Total	**164**

Figure 7 Connected sites to CFBLNet (October 2008)

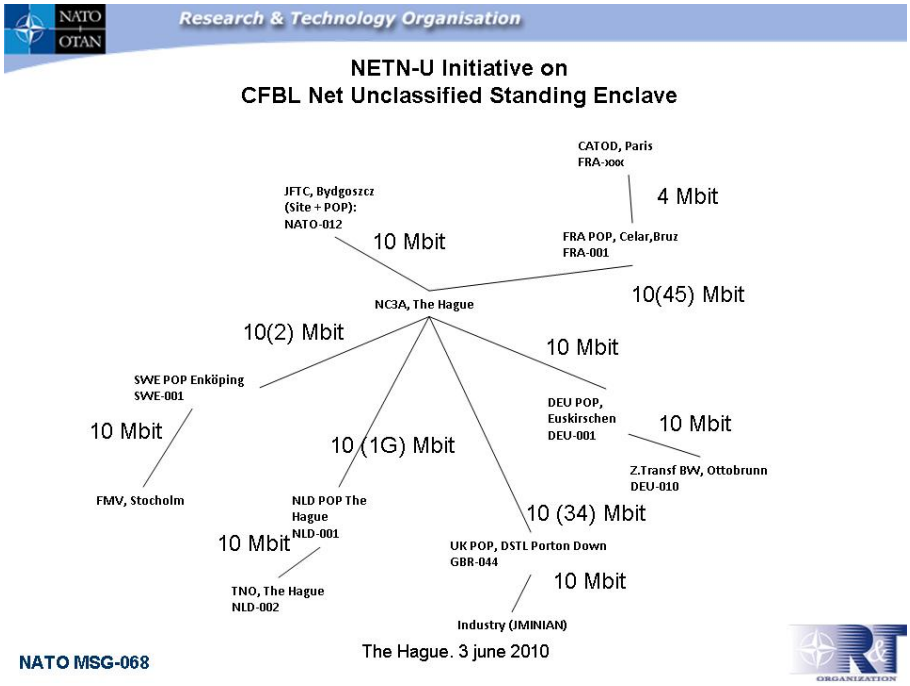
Detailed up-to-date information regarding the countries and sites connectivity to CFBLNet and Point of Contact data is available through the CFBLNet organisation.

6 NETN Network design

6.1 Introduction

The design of the NETN infrastructure is based on the assumption that the Combined Federated Battle Laboratory (CFBL) Network will be the black (unclassified) backbone between participating nations. Each participating nation will, or has already, acquired the necessary routers, switches, crypto devices and workstations to meet the respective national requirements for installation, connection and operation of the CFBL network at the nation's respective sites. The NETN network design will be used as the basis for future M&S applications as planned within ACTs NETN initiative.

The MSG-068 Infrastructure Subgroup developed the initial network topology design for the Experiments. 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.



6.2 Network concept

The idea is to create a new permanent enclave for coalition purposes. At this moment there are several enclaves on the CFBLNet BlackBone. The enclave suitable for this is the temporary enclave CFBLNet GREEN. The enclave CFBLNet GREEN ends in the red router. At the red router are several Virtual Private Networks (VPNs) available, all with the same releasability. One of the VPNs is NETN. Each initiative has its own end switch.

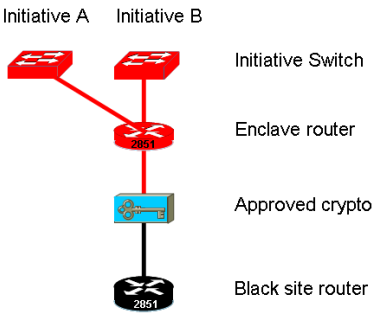


Figure 8 network level 2

The black router, crypto and enclave router are managed by CFBLNet. The initiative switch is managed by the initiative. This concept permits that a NETN network-manager is able to manage the NETN network within the agreed boundaries. An example is that the NETN network-manager stops all Conference calls and adds all bandwidth to the training simulators to prevent hiccups in the exercise. After the training session the VTC is allowed to access the NETN network for after action review. There are also possibilities to automate this process.

Another advantage of this concept is that hardware and software for services like “Voice over IP” (VoIP), the Video teleconference manager, Network time server, and so on can be used for multiple parallel initiatives while the data (with the same level and releasability) itself is not mixed. This will reduce costs for everybody.

6.2.1 Hardware

The proposed hardware for a new site is mentioned below.

Figure 9 Black site router examples

The Black site router is the CISCO 2851 or 3845 (for E3 connection) router. This router is power full enough to handle the high speed encrypted data streams. (IOS=enterprice)

Figure 10 Enclave Crypto

The enclave crypto is the TCE621B (or C) for Europe and the TACLANE E100 for the USA.

Figure 11 Enclave router

The enclave router is the CISCO 3845 or ASR 1002 router. This is a powerful router capable of handling multiple VPNs and tunnels.

The initiative switch has to be divined. The switch should have “power over Ethernet” to support IP phones.

Figure 12 Default enclave IP phone

6.3 Security

Each national site is responsible for the certification and accreditation of their respective sites in accordance with their national directives. Each nation is responsible for submitting the site national accreditation endorsement certificate (S-NAEC) and the initiative national accreditation endorsement certificate (I-NAEC) for each participating site. The S-NAEC is the authority to connect to the CFBL network, while the I-NAEC is the authority to operate and participate in an approved CFBL initiative.

Each nation will maintain a security posture in accordance with CFBL instructions and national policies.

The network design is based on a fully meshed red network between the crypto devices at all event sites to prevent a single point of failure causing connectivity issues. Dynamic routing protocols will be utilized vice static routes whenever possible.

Each nation is responsible for obtaining the proper crypto devices. Network separation is provided by the different key-mat authorized for the different initiatives.

6.3.1 Accreditation

Each country is responsible for accreditation of its national sites. If a site does not have a valid accreditation certificate the site should be disconnected from CFBLNet.

6.3.2 Classification

The classification of the NETN environment is “SECRET”

6.3.3 Marking

Because Sweden is not a NATO country the marking is “releasable to NATO and SWE”. The strong recommendation is to include all future CFBLNet nations in this enclave to avoid security and releasability issues in the future.

6.3.4 Crypto

Event sites are connected by a fully meshed, dynamic protocol routed network. This allows the exchange of routing information to prevent a single point of failure from preventing connectivity between all sites when a site(s) is not operating properly, due to accreditation or technical issues.
The network is protected by approved crypto and operates in a ‘’system high’’ concept. The preferred crypto is the TCE 621b for Europe. NC3A can bridge this to a TACLANE for the USA.

6.3.5 Key material

The key material for the TCE 621b will be supplied by NATO. The key material for the TACLANE will be supplied by the USA (MNIS-JPO).

The key material for the crypto devices is provided and authorized by the NATO C3 Agency or by the Multi National Information Sharing Joint Program Office (MNIS JPO) in the United States and distributed to all nations according to authorized memorandums of agreement/procedures, through secure crypto channels. A valid S-NAEC and I-NAEC are required in order to obtain crypto key material. The point of contact for CFBLNet key material distribution:

NATO C3 Agency:

Table 4 Crypto custodians

NATO CFBLNet Comsec PoC:	
Department/Group/Organization	NATO C3 Agency
Name including title:	Mr Edgar Harmsen
Commercial Phone Number:	+31 70 374 3488
Internet Email Address:	Edgar.Harmsen@nc3a.nato.int
Comsec Custodian PoC:	
Department/Group/Organization	NC3A Custodian
Name including title:	Mr Cor Westenberg– Comsec Custodian
Commercial Phone Number:	+31 70 374 3231
Internet Email Address:	Cor.Westenberg@nc3a.nato.int

USA:

Table 5 Crypto custodians

Comsec Custodian (MNIS-JPO):	
Department/Group/Organization	MNIS- JPO (US)
Name including title:	Ron Watkins - Primary Comsec Custodian
Commercial Phone Number:	+1 703 284 8772
Internet Email Address:	rwatkins@hai.com
Comsec Custodian (MNIS-JPO):	
Department/Group/Organization	MNIS- JPO (US)
Name including title:	Charles Plummer – Secondary Comsec Custodian
Commercial Phone Number:	+1 703 284 7004
Internet Email Address:	cplummer@hai.com

6.4 Protocols and Services

6.4.1 Protocol translation

The applications in the NETN environment use protocols that are routable (broadcast is not routable). This means that no protocol translation is needed when required.

6.4.2 Protocol support

The port-numbers of expected protocols to be used are listed below. The port-numbers can be used to filter data and segregate different data streams into separate VLANs and Ethernet ports in the initiative switch as required.

- NTP = 123
- FTP = 21
- DNS = 53
- SNMP = 161
- SMTP = 25
- POP3 = 110
- WEB = 80
- VoIP = ?
- VTC = ?

Simulation protocols used in previous projects on CFBLNet:

- DIS = 3005 (Not used in NETN)
- ASTI = 5001 (Not used in NETN)
- Link 11 = 1000 Link16 = 10000 (Not used in NETN)
- HLA pitch commander = 8070 (agent on each host running federate), 8071 (Commander)
- TNO RTI (HLA) = 3100 (RTI exec), 3101 and 3102 (RTI fedex), 3103 (for forwarding)
- Mäk RTI (HLA) = 4000

Especially for the simulation protocols the port numbers to be used in a NETN experiment have to be documented in the Federation Agreements Document (FAD) corresponding to that specific experiment.

6.4.3 Quality of Service (QoS)

It is proposed to place applications in different classes to prioritize network access and services for there applications. This is used to automate the bandwidth assignment.

Table 6 Access classes (example)

Class	Application	Remarks
High	VTC, VoIP, Radio Simulation (HLA, ASTi)	Low latency
Medium	Simulation (HLA)	
Best Effort	E-mail	

6.4.4 Network Services

The network services available at this time on CFBLNet are:

- VoIP
- NTP
- VTC
- HTTP
- Mail
- FTP

All Network Services to be provided by the NETN network infrastructure are listed in 7.2.

6.5 Data flow and capacity

To make a total design the required services and their use (number of terminals connected / used at the same time / the location) are needed. This gives a better perception of the data flow between sites and the capacity needed to support the services, training and education systems. This information should be documented in tables like shown below. Actual data are not provided here for classification reasons.

Table 7 Capacity between countries (Level 0)

Country	NATO Country Code	Capacity Mbit/s to CFBLNet
Australia	AUS	(data removed)
Bulgaria	BGR	(data removed)
Czech Republic	CZE	(data removed)
France	FRA	(data removed)
Germany	DEU	(data removed)
Italy	ITA	(data removed)
NATO	NATO	(data removed)
Netherlands	NLD	(data removed)
Romania	ROU	(data removed)
Slovenia	SVN	(data removed)
Spain	SPA	(data removed)
Sweden	SWE	(data removed)
Turkey	TUR	(data removed)
United Kingdom	GBR	(data removed)
United States	USA	(data removed)

6.5.1 MTU size enclave routers

The MTU size for the enclave routers will be 1368 bytes. (Explanation removed due to declassification)

6.5.2 MTU size enclave crypto

The MTU size for the enclave crypto will be 1476 bytes. (Explanation removed due to declassification)

6.6 Network topology

6.6.1 Black Network (International network)

The diagram below shows the top-level design of the NETN VPN on top of the CFBLNet GREEN enclave on top of the CFBLNet BlackBone. Each nation will be connected to the NETN CFBLNet through its national access point or Point-of-Presence (PoP). The PoP will either connect to a national asset located at that site or will provide the interface to the national network infrastructure which connects national assets.

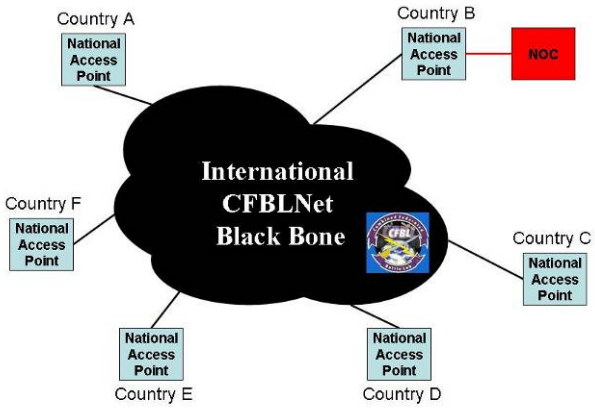


Figure 13 Top level diagram of WAN

The diagram below shows a more detailed representation of the CFBLNet BlackBone infrastructure that provides the NETN Enclave.

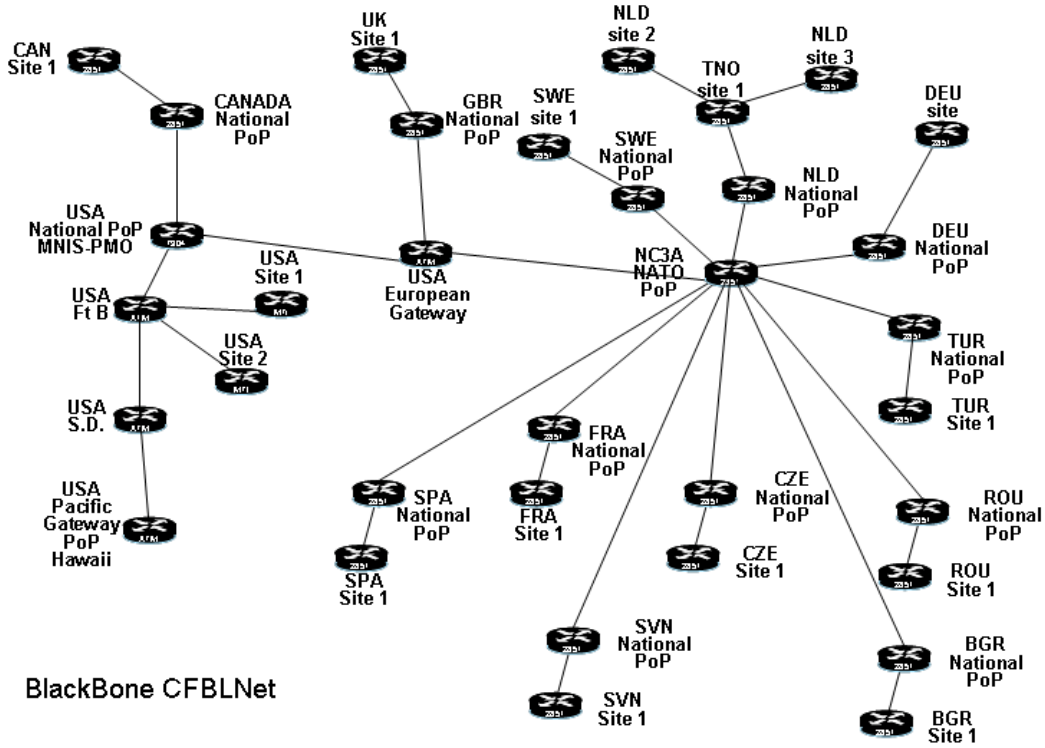


Figure 14 CFBLNet BlackBone infrastructure for NETN (not completed)

6.6.2 Crypto network

The crypto network topology is the way the crypto's are connect to each other. There are two options based on the national security policy.

6.6.2.1 Direct connections

The first option is to make direct connections between all sites (international). Each site has a crypto and is connected to all other sites. The national PoP can have a crypto as well, but the data can go directly from site “1” in country “A” to site “1” in country “B”.

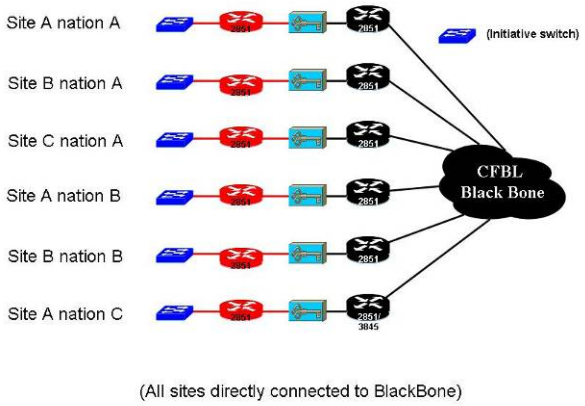


Figure 15 Crypto Direct Connection

6.6.2.2 Connections through the national PoP

The second option is the make a connection through the national PoP and then to the national sites. Each site has a crypto and is connected to the crypto in the national PoP. Another crypto in the national PoP has connection to the crypto’s in the PoP or sites in other countries. This means that data from site “1” in country “A” first goes to the national PoP and is the send to the other country. Nations may use a national crypto system on the national network. Nations can also include specific data filters or other types of data protection or data translation devices at the PoP.

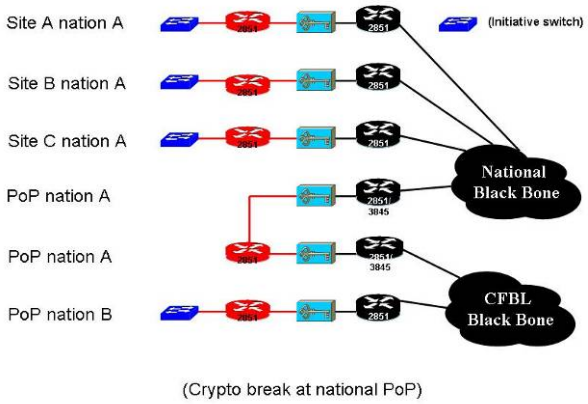


Figure 16 Crypto Indirect Connection (Crypto Break)

6.6.3 Enclave router network

Each enclave router has tunnels to all other enclave routers to provide services needed in the enclave. The enclave router also separates the different VPN using the enclave.

7 NETN Network Management and Network Support Services

7.1 NETN Network Operation Centre (NOC)

The NETN Network Operation Centre (NOC) is a PC connected somewhere in the NETN network managing the NETN initiative switch and services.

7.2 NETN Network Services

The following network services are managed by NETN. Some of them are already part of the standard services provided by CFBLNet.

The Network Services used in an experiment have to be clearly documented in the federation specific FAD.

7.2.1 Domain Name System (DNS)

Used for the translation from host names to IP addresses.

7.2.2 Simple Network Management Protocol (SNMP)

Used for monitoring network-attached devices for conditions that warrant administrative attention.

7.2.3 File Transfer Protocol (FTP)

An FTP server has to be available on the NETN network to which FTP clients can connect for downloading and uploading files.

7.2.4 E-Mail

A mail server (POP3 and SMTP) has to be available on the NETN network.

7.2.5 Voice over IP (VoIP)

Service for maintenance, tech. support and exercise management.

Figure 17 Default enclave IP phone

A Central Call manager facility should be provided. The NOC site would be most logical location.

7.2.6 Network Time Protocol (NTP)

NTP time is available through the network and provided by CFBLNet. In time critical applications an extra local time source is needed (e.g. a GPS synchronised local clock). An example is the Meinberg M300 NTP server using GPS to synchronise.

Figure 18 Meinberg M300 GPS NTP server

The need for such a local service depends on the NETN requirements

7.2.7 VTC

For briefing & debriefing in a distributed environment it is important that participants are presented with presentation slides (e.g. package lead briefing) and an overall tactical display. Video teleconferencing (VTC) is necessary for interactive discussions concerning the mission plan and after action review (AAR). Obviously, all of these interactions fall under the same security requirements as the mission itself. For this reason, the secure network is also used for the VTC and briefing distribution. Besides communication of the mission plan and evaluation of the executed mission, VTC is also important as part of Exercise Control and for managing technical issues.

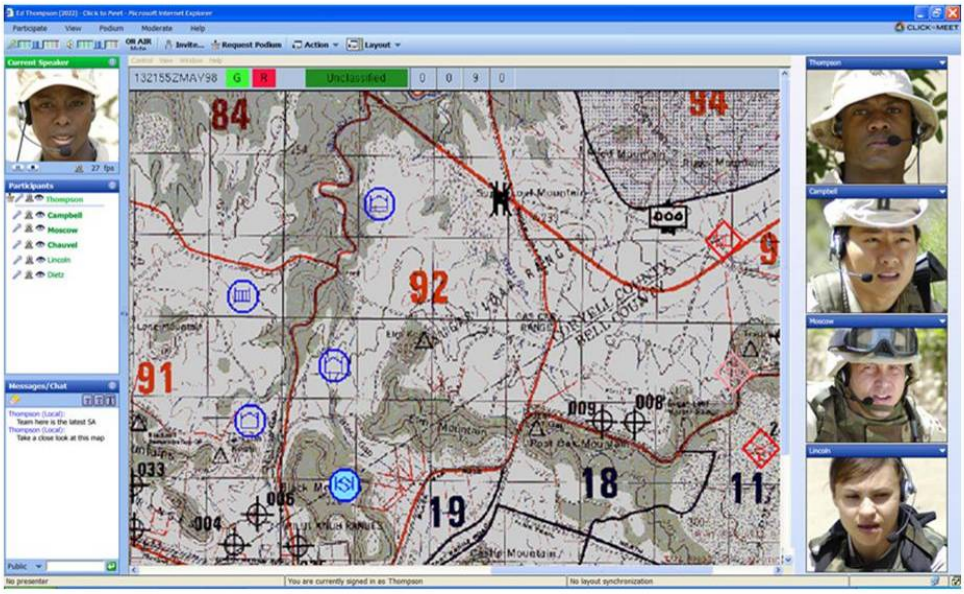


Figure 19 Example VTC Application "Click to Meet"

7.2.8 Wiki Webserver

A wiki webserver providing a Collaborative Work Environment (CWE) has to be available on the NETN network. The CWE can have a general part for looking up all kind of useful information for example about the FOM and each experiment can have its specific part on the CWE to share for example simulation results. The current MSG-052 and MSG-068 CWEs could be the basis of such a CWE.

7.2.9 Quality of Service

Network management refers to the activities, methods, procedures and tools that pertain to the operation, administration, maintenance and provisioning of networked systems.

Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible.

Administration deals with keeping track of resources in the network and how they are assigned. It includes all the “housekeeping” that is required to keep the network under control.

Maintenance is concerned with performing repairs and upgrades. For example, if equipment must be replaced or patches applied to operating systems or router/switch IOS’s. Maintenance also includes corrective actions and preventive measures to make the managed network run better.

Provisioning is concerned with configuring resources in the network to support a given service.

This network document, while not all inclusive, is meant to provide the basics of network operations and governance of the networks while conducting NETN events.

7.2.10 Network Monitoring

Each nation will be responsible for monitoring and maintaining network operations within their national boundaries. MNIS JPO is responsible for monitoring and maintaining the black (unclassified) network backbone connectivity. The national CFBLNet engineer will provide the black side IP address schema and coordinate with the various national sites involved in NETN events to ensure proper blackside router configurations to properly pass encrypted data traffic and routing information.

The NETN NOC will monitor the initiative (classified) network.

Figure 20 MRTG logo

Software to monitor the initiative switch is for instance MRTG. This is free software. It is able to monitor all port on all initiative switches and presents the results on a web server for easy user access on daily, weekly, monthly and yearly bases.

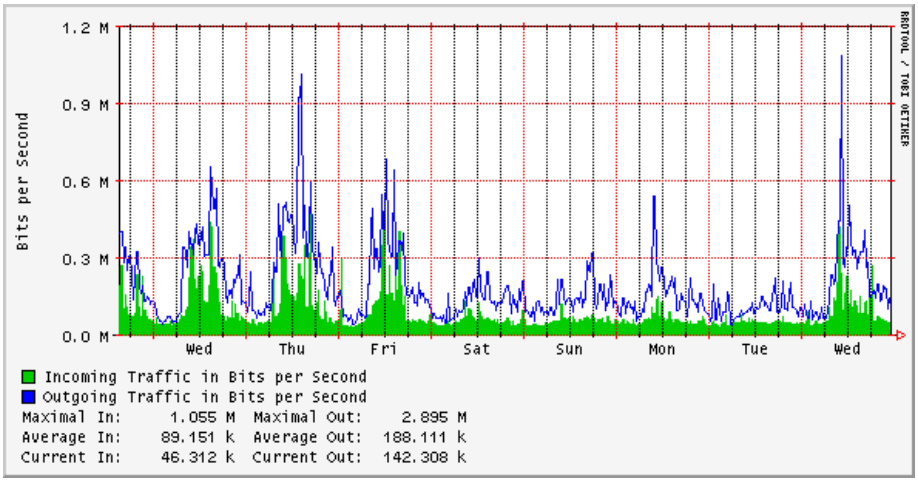


Figure 21 MRTG example weekly bases

Figure 22 WhatsUp logo

Other available monitor software is “WhatsUp”. This is not free software. It is able to show the network configuration and services. It also has a web server for easy user access.

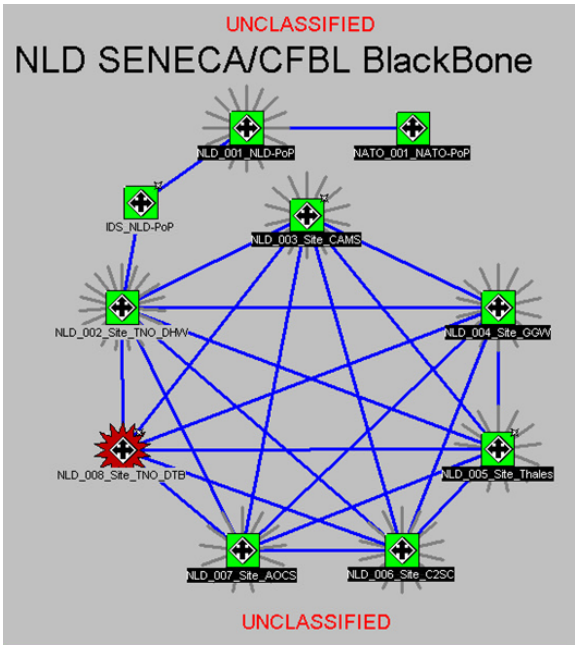


Figure 23 WhatsUp example for NLD black network

8 NETN Simulation Interoperability and Simulation Support Services

8.1 Simulation Interoperability

NETN federations are based on NATO STANAG 4603 which states that High-Level Architecture IEEE 1516 shall be used as the standard for developing and federating simulation systems.

Non-HLA or legacy HLA (i.e. HLA 1.3) federates can participate in the simulation using appropriate bridging and/or adapter technologies on the national network. Any bridging required in order to adapt federates to IEEE 1516 shall be the responsibility of the integrating federate.

8.1.1 HLA-RTI and Central RTI Component (CRC)

NATO STANAG 4603 implies that a certified Run Time Infrastructure (RTI) will be used to provide HLA IEEE 1516 interoperability. For each NETN experiment the RTI to be used has to be agreed on and this choice is part of the Federation Agreements. Any bridging or adaptations of federates to the selected RTI shall be the responsibility of the integrating federate.

Most HLA implementations include a Central RTI Component (CRC) to provide HLA services like Time management. Unless running a connectionless RTI mode this component represents the RTI Executive and is the initial point of access to a federation. If required the CRC will be running at the NOC.

8.1.2 HLA-RTI and Local RTI Component (LRC)

The Local RTI Component (LRC) is an integral part of the Federate Application and is usually started in the same process space as the federate itself. Usually this service is not documented explicitly in the FAD unless the LRC does more than expected like loading a plugin for SOM to FOM translation.

8.1.3 HLA-RTI and Web Service Provider RTI (WSPRC)

Web Service Provider RTI Component (WSPRC) is an RTI component used when offering the RTI services using the standard IEEE 1516 Web-Service API.

8.2 Simulation Support Services

Simulation Support Services are processes (software) which must be executed in parallel to the federate processes to enable a federation execution or which are required to support individual simulations in the federation to enable them to participate in a federation according to the agreements.
The NETN infrastructure will not provide any Simulation Support Service by itself and it is up to each NETN experiment which Simulation Support Services are used and made available as long as HLA IEEE 1516 is used as the simulation standard. Below some typical Simulation Support Services are mentioned, but it is the responsibility of the participants and not of the NETN network to provide these services.

The Simulation Support Services used in an experiment have to be clearly documented in the federation specific FAD.

8.3 Execution Control

Execution Control software provides a facility to remotely startup, monitor, and shutdown federates. Participant nations can be required to install ‘daemon software’ on each machine that would be running a federate. It is up to each NETN experiment whether execution control is needed. An example of such a product is ‘Pitch Commander’.

8.4 Database Services

Specific database services may be needed for providing initialization data (e.g. scenarios, terrain databases, weather data, weapon system parameters, etc.) or logging purposes. Access to the database services may given be through different means (e.g. SQL, webservices, etc.). An example is the Logger tool ’Pitch Recorder’ that uses a MySQL database for storage.

8.5 Bridge or Gateway Services

Bridging/gateway/adapter services (either as a bi-directional transfer or as a data diode) may be required at federation start-up. Examples are:

° HLA 1.3 <=> HLA IEEE 1516
° FOM X <=> FOM Y
° DIS <=> HLA
° TENA <=> HLA
° RTI X <=> RTI Y
° SIMPLE <=> HLA LINK 16 BOM

9 NETN Infrastructure Budget Requirements

9.1 CFBLNet Business model

The business model for NETN is that all participants carry their own cost to establish the connectivity. CFBLNet is build with a cost sharing philosophy with pay as you go: every participant (NATO nation, NATO organisation and Guest Nations fulfil their own cost to connect and together they share the common cost (total shared cost/numbers users). The National/Organisation cost is internally handled.

National Cost:

- Non-recurring:
  - National Infrastructure
  - Initial installation
- Recurring:
  - Link cost to nearest PoP.
  - Monthly subscription cost (shared element).

9.2 CFBLNet Subscription Costs

9.2.1 CFBLNetwork Cost Estimates

The cost estimate is made under the condition that a 10 Mbit/s capacity is needed for NETN.

The subscription costs for CFBLNet (2009) are:

- One time Installation cost: EURO 4k (E3 connection)
- Monthly fee
  - 4 Mbit/s (default): EURO 7k
  - 10 Mbit/s (during training) EURO 9k

These Subscription costs are covering the shared Infrastructure hardware/software, CFBLNet Management and Coordination, helpdesk, standard services including Network Management, encryption, routing, DNS, mail, voice (over IP (VoIP)), Web and FTP services, Network time protocol (NTP) and full transparent access to the CFBLNet core network including transatlantic connections. On request VTC can be added as a service. The Installation cost include extensive coordination and installation efforts to get the links and blackbone routers interconnected and configured between the national PoP and the CFBLNet PoP facilities.

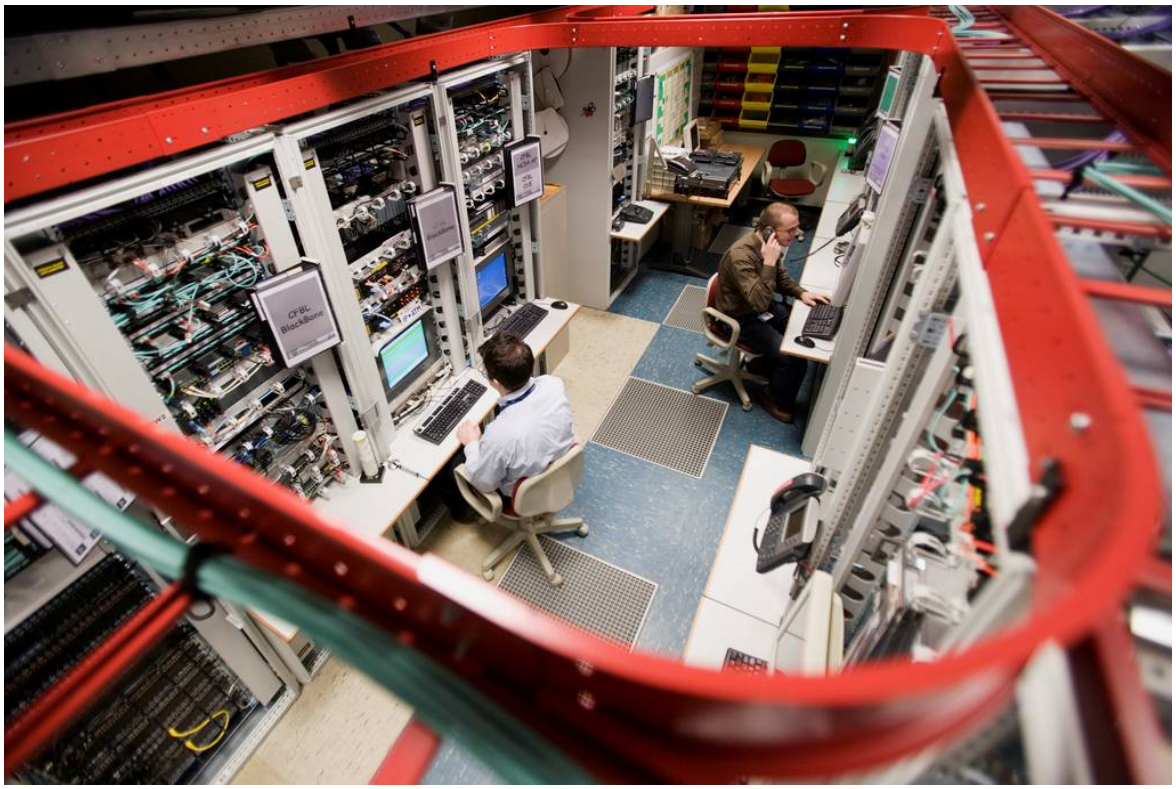


Figure 24 NATO and European CFBLNet Point of Presence.

A permanent subscription provides standard access to the:

- CFBLNet Blackbone (IPv4 (IPv6) transport network)
- CFBLNet CUE (Unclassified Enclave all participants)
- CFBLNet BLUE * (Coalition Secret Rel. ASCANZUKUS+NATO (nations and organisation)
- CFBLNet RED * (NATO Secret Rel. NATO (nations and organisation)

* Access when applicable

However, a permanent subscription on CFBLNet is already in place for most of the NETN countries. This means that these CFBLNet costs can be shared with other initiatives in that country (e.g. CWID). Maybe additional CFBLNet cost for extra bandwidth is needed during execution. As an example for these nations with a permanent CFBLNet subscription the NETN cost would only be EURO 9k / Month per 10Mbit/s during training. This depends from country to country. Contact you national CFBL representative for more information.

Table 8 CFBLNet subscription

Country	NATO Country Code	Permanent CFBLNet subscription in place
Australia	AUS	YES
Bulgaria	BGR	NO
Czech Republic	CZE	NO
France	FRA	YES
Germany	DEU	YES
Italy	ITA	YES ?
NATO	NATO	YES
Netherlands	NLD	YES
Romania	ROU	NO
Slovenia	SVN	NO
Spain	SPA	Not permanent
Sweden	SWE	Not permanent
Turkey	TUR	NO
United Kingdom	GBR	YES
United States	USA	YES

9.2.2 International network Costs

The cost for the international connection between the nation and the CFBLNet hub at NC3A (The Hague, The Netherlands) is often already paid for by the national part of the CFBLNet organisation. This means that these CFBLNet costs can be shared with other initiatives in that country. The connection costs for each country are for that country.
As an example, the network cost for a connection between NC3A and Istanbul for an E3 (34 Mbit/s) leased line will amount to about EURO 4k / month with a contract for at least one year. Note that the available capacities of lease lines is 2, 8, 10 (different technology) or 34 Mbit/s. In general, the 34Mbit/s line has the best price-performance.
On request, CFBLNet could provide the link between your National PoP/Site and the NATO and European CFBLNet PoP. However, experience learned that national service providers, through National MOD's, provide better arrangements.

9.2.3 National network Costs

The cost for the national connection is often already paid by the national part of the CFBLNet organisation. This means that these CFBLNet costs can be shared with other initiatives in that country. The site connection costs are for the country. No additional fee is required for that national connection to NC3A.

9.2.4 CFBLNet National PoP / Access node considerations

Depending on the national organisational arrangements a nation can decide to initially connect only one national site to CFBLNet. If more national sites would like to participate it is recommended to establish a National PoP.

9.2.4.1 National CFBLNet PoP setup cost

Cost of equipment for PoP differs from country to country and the national security rules. To setup a CFBL PoP starts with about 30K EURO for hardware and software

9.2.4.2 Natonal CFBLNet Site setup cost

Cost of equipment for a new site is around 30K EURO for hardware and software

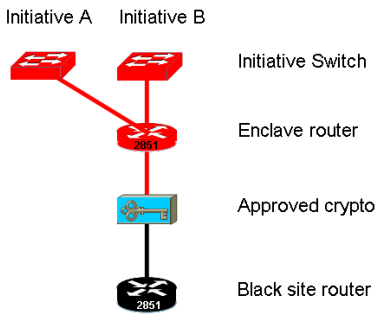


Figure 25 Site network equipment

10 Referenced publications

1. CFBLNet-Pub1-Main-V5.0-U
2. CFBLNet-Pub1-AnnexA-V5.0-U
3. CFBLNet-Pub1-AnnexB-V5.0-U
4. CFBLNet-Pub1-AnnexC-V5.0 Appendices-U
5. CFBLNet-Pub1-AnnexC-V5.0-U
6. CFBLNet-Pub1-AnnexD-V5.0 Appendices-UNRI
7. CFBLNet-Pub1-AnnexD-V5.0-U
8. CFBLNet-Pub1-AnnexE-V 5.0
9. CFBLNet-Pub1-AnnexF-V5.0
10. CFBLNet-Pub1-AnnexG-V5.0-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