NATO STANDARD

AEP-76
VOLUME V

SPECIFICATIONS DEFINING THE JOINT DISMOUNTED SOLDIER SYSTEM INTEROPERABILITY NETWORK (JDSSIN) – NETWORK ACCESS

Edition A Version 3

MARCH 2023

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED ENGINEERING PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

20 March 2023

1. The enclosed Allied Engineering Publication AEP-76, Volume V, Edition A, Version 2, SPECIFICATIONS DEFINING THE JOINT DISMOUNTED SOLDIER SYSTEM INTEROPERABILITY NETWORK (JDSSIN) - NETWORK ACCESS which has been approved by the nations in the NATO ARMY ARMAMENTS GROUP, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 4677.

2. AEP-76, Volume V, Edition A, Version 3 is effective upon receipt and supersedes AEP-76, Volume V, Edition A, Version 2, which shall be destroyed in accordance with the local procedure for the destruction of documents.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (https://nso.nato.int/nso/) or through your national standardization authorities.

4. This publication shall be handled in accordance with C-M(2002)60.

Dimitrios SIGOULAKIS
Lieutenant General, GRC (A)
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATO LETTER OR PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Documents Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Documents Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.1 AIM

Standardization Agreement (STANAG) 4677 [1] on Dismounted Soldier Systems (DSS) Standards and **Protocols** for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability STANAG) aims at enabling interoperability through a standardised exchange of information between C4 systems used by dismounted soldiers across North Atlantic Treaty Organisation (NATO) or Partners for Peace (PFP) force boundaries. The DSS C4 Interoperability solution is depicted in Figure 1.

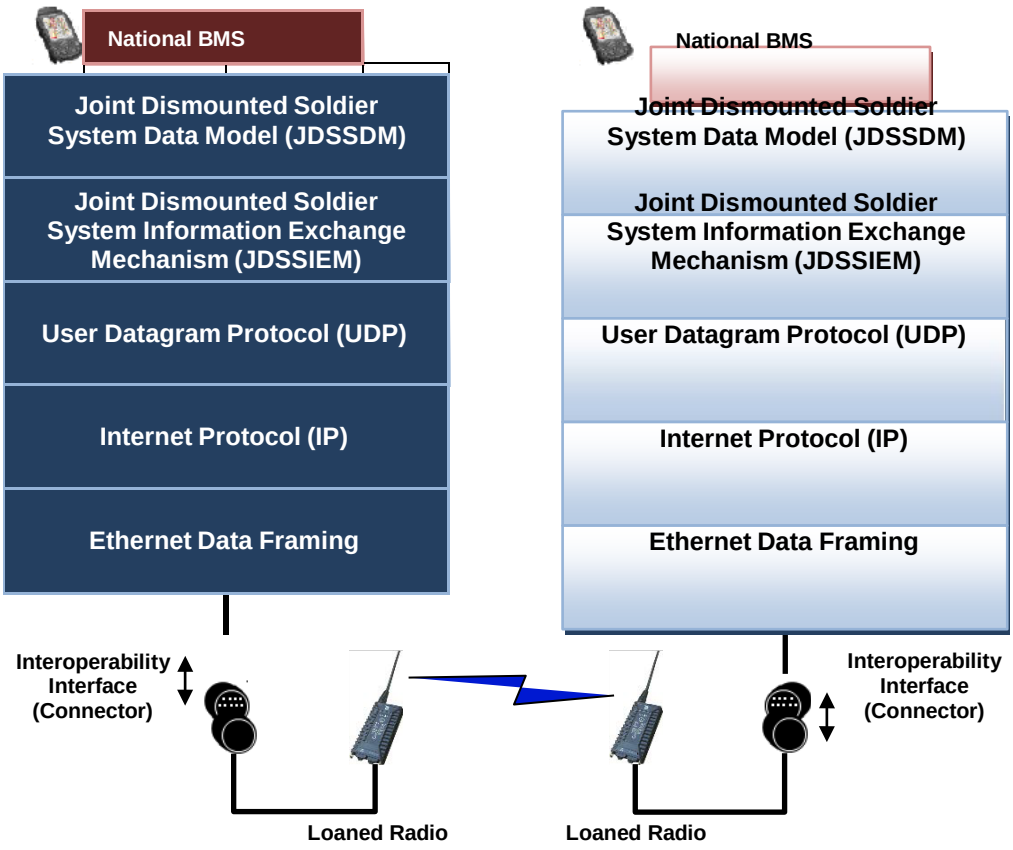

Figure 1 Dismounted Soldier System C4 Interoperability Solution

The DSS C4 Interoperability solution contains:

- A Joint Dismounted Soldier System (JDSS) Gateway, acting as a message translator, added to each C4 sub-system of a national DSS consisting of:
  - Joint Dismounted Soldier System Data Model (JDSSDM)
  - Joint Dismounted Soldier Information Exchange Mechanism (JDSSIEM)
  - User Datagram Protocol (UDP)
  - Internet Protocol (IP
  - Ethernet
- A physical connection between the JDSS Gateway and the Loaned Radio based on STANAG 4851 in conjunction with the use of Ethernet over USB.
- A Loaned Radio.

1.2 OBJECTIVE

The objective of this AEP is to define the Network Access and Addressing related to the Interoperability Network and the connected JDSS Gateways.

The Interoperability Network constituted by the JDSS Gateways and interconnected by the Loaned Radios is totally separated from the national wireless networks and is only connected to the national DSS through the Gateway Soldiers as shown in Figure 2. The JDSS Gateway is not a part of the Loaned Radio, but will reside in either the national C4 computer or a dedicated soldier computer.

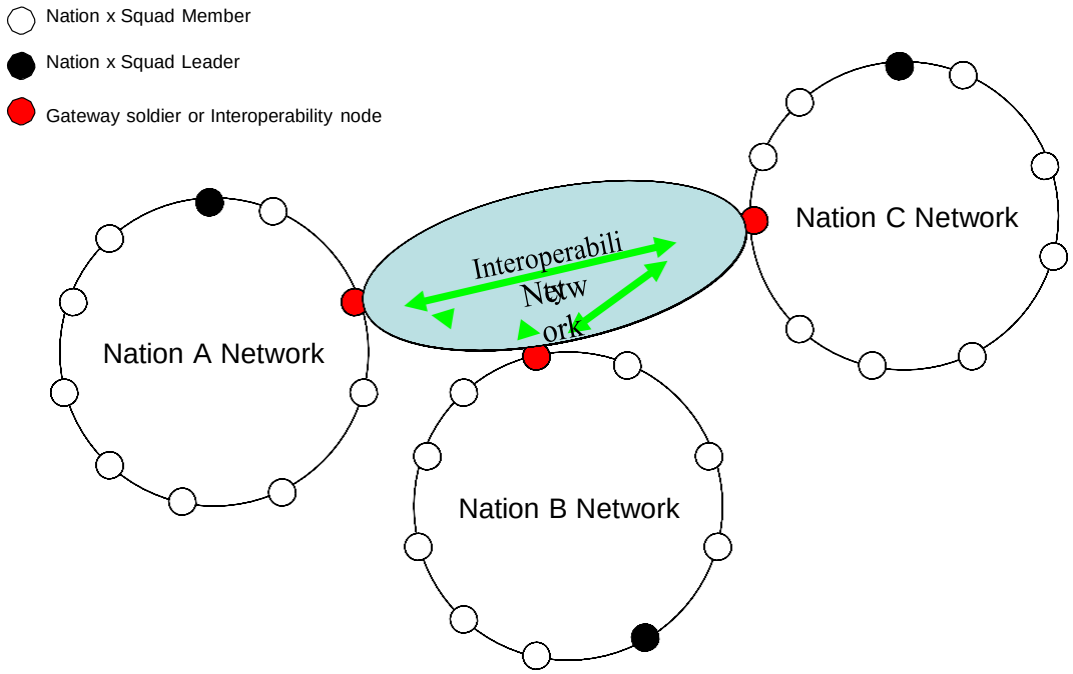

Figure 2 The Interoperability Network Approach

1.3 SCOPE

Both among the coalition nations and within each nation there must be a scheme to request, distribute and install IP addresses. The hosts that form the Interoperability Network and JDSS Gateways must be given unicast and multicast IP addresses. Routines and methods for installing and using the distributed addresses in the involved equipment must be defined. This AEP considers OSI Layer 2 and Layer 3 Loaned Radios.

This AEP describes the Unicast and Multicast IP address definition and distribution prior to a coalition mission. Before deployment, the coalition nations must agree on a Concept of Employment (CONEMP) to solve organisational, security and technical issues outside the scope of this AEP. Most likely the coordination of IP addresses takes place at the coalition Headquarters (HQ) before deployment.

This AEP assumes that the JDSS Interoperability Network operates within one security domain. The AEP on security protection for DSS interoperability [6] provides guidance and specifications for security protection of the JDSS interoperability network.

This AEP identifies areas that must be mutually negotiated to achieve IP network connectivity.

1.4 REFERENCED DOCUMENTS

LCG/1 Documentation

Ref	Document ID	Title	Revision
[1]	STANAG 4677 Edition A	Dismounted Soldier Systems Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability Standardisation Agreement (DSS C4 Interoperability STANAG)	Ed A
[2]	STANAG 4851	STANAG 4851 COMBINED POWER AND DATA ACCESSORY CONNECTOR FOR DISMOUNTED SOLDIER SYSTEMS (DSS)	Ed A
[3]	AEP-76, VOL. III	AEP-76, VOL.III Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – LOANED RADIO (STANAG 4677) Edition A	Ed A
[4]	AEP-76, VOL. IV	AEP-76, VOL.IV Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Information Exchange Mechanism (STANAG 4677) Edition A	Ed A
[5]	AEP-76, VOL. II	AEP-76, VOL.II Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) Data Model (STANAG 4677) Edition A	Ed A
[6]	AEP-76, VOL. I	AEP-76, VOL. I Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Security (STANAG 4677) Edition A	Ed A
[7]	RFC 768	User Datagram Protocol	
[8]	RFC 791	Internet Protocol Specification	
[9]	RFC 792	Internet Control Message Protocol	
[10]	RFC 826	Ethernet Address Resolution Protocol	

Ref	Document ID	Title	Revision
[11]	RFC 894	A Standard for the Transmission of IP Datagrams over Ethernet Networks	
[12]	RFC 950	Internet Standard Subnetting Procedure	
[13]	RFC 2236	Internet Group management Protocol, Version 2	
[14]	RFC 1191	Path Maximum Transmission Unit Discovery (PMTUD)	
[15]	RFC 1918	Address Allocation for Private Networks	
[16]	RFC 2474	Definition of the Differentiated Services Field	
[17]	RFC 4632	Classless Inter-Domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan	
[18]	RFC 5771	IANA Guidelines for IPv4 Multicast Address Assignments	

1.5 RELATED DOCUMENTS

Document ID	Title	Revision
NIAG Study SG103 Annex F	Radio Aspects	
NIAG Study SG103 Annex D	Overall Interoperability Architecture	
NIAG Study 123	Soldier Systems Communications Interoperability Validation Study	

1.6 GLOSSARY

Gateway Soldier	The designated soldier within a national squad interfacing the Loaned Radio with the national DSS.
Host	An IP addressable end-point.
Interoperability Network	The IP network formed by the JDSS Gateways interconnected by the Loaned Radios in order to exchange information between the national DSS.
JDSS Gateway	A message translator added to each C4 sub-system of a national DSS including the JDSSDM, JDSSIEM, UDP, IP and Ethernet.
JDSS Interoperability Interface	Defines the physical interface between the Loaned Radio and the JDSS Gateway.

Loaned Radio	The radio provided by one of the participating nations enabling the Interoperability Network.

CHAPTER 2 OVERVIEW

This AEP has been developed to formalise the manner and way in which national DSS networks are interconnected in the field and is organised as follows:

The first section specifies the general characteristics of the interconnection of national DSS networks and the Interoperability Network. STANAG 4677 [1] clearly mandates the use of UDP/IP protocols, therefore the interconnection must support Internet Protocol version 4 (IPv4). This AEP is limited to the interconnection between JDSS Gateways through Loaned Radios and specifies the rules, policies and constraints for the implementation of an IP unicast and multicast addressing plan for the DSS C4 Interoperability solution. Interior routing protocols, encryption, implementation of the hosts in the national domain and systems management are subject to agreement on a case-by-case basis and IPv6 may be considered in the future.

Finally, this AEP gives guidance to the network operators. Dissemination of management information is performed prior to deployment and by appropriate management procedures.

Throughout the requirements the words '*shall*', '*should*' and '*may*' are used to state the nature of the requirements. *Shall* is used to identify mandatory requirements, while *should* is used to identify guidelines that are desirable but not mandatory. *May* is used to indicate a freedom of choice to be implemented on a bilateral basis between the participating nations.

CHAPTER 3 NETWORK ACCESS REQUIREMENTS

3.1 INTERNET PROTOCOL

There are two versions of the IP that are in use, IPv4 and IPv6, each defining an IP address differently. At this time, the aim is to define the interface for the network interconnection based on IPv4. Internetworking between IPv4 and IPv6 is not an aim of this AEP.

Requirement 1. IPv4 interconnections shall be in conformance with Internet Standard (STD) 5, including:

- RFC 791 [8] ”Internet Protocol” updated by RFC 2474 [16] ”Definition of the Differentiated Services Field”
- RFC 950 [12] ”Internet Standard Subnetting Procedure”

Requirement 2. Interconnections supporting IPv4 over Ethernet shall be in conformance with Internet STD 0041 (RFC 894 [11]) and support the Address Resolution Protocol (ARP) in conformance with Internet STD 0037 (RFC 826 [10]).

IPv4 uses the Classless Inter Domain Routing (CIDR) concept and notation specified in RFC 4632 [17]. CIDR is based on variable length subnet masking (VLSM) to allow allocation and routing based on arbitrary length prefixes.

For this purpose, an IP address consists in two parts: the *network prefix* and the *host identifier*. The subnet mask or the CIDR prefix determines how the IP address is divided into network and host parts. In this, the IP address is followed by a slash and the number of bits used for the network part. For example the CIDR notation for the IPv4 address 192.168.1.2 and its subnet mask 255.255.255.0 is 192.168.1.2/24 where the first 24 bits of the IP address indicate the network and subnet.

3.2 IP ADDRESSING

For the JDSS Gateway, only unicast and multicast needs to be supported.

3.2.1 UNICAST

In unicast addressing the IP-packet header is set up with a unicast IP-address which will only be

addressed to the host with the given IP-address. It is a one to one transfer decided by the transmitter. Sending the same data to multiple unicast addresses requires the sender to send multiple copies of the packet to each recipient.

IPv4 reserves some addresses for private networks which may be used by any nation, since they are not expected to be routable on the global Internet. Three IPv4 ranges are reserved for private networks as defined in Table 1 and RFC 1918 [15].

Requirement 4. As the JDSS Interoperability network is a closed network, the network IP addressing scheme should use private network addresses as defined in RFC 1918 [15].

Prefix	IPv4 Range		# addresses
24-bit block (10/8)	10.0.0.0	10.255.255.255	16 777 216
20-bit block (172.16/12)	172.16.0.0	172.31.255.255	1 048 576
16-bit block (192.168/16)	192.168.0.0	192.168.255.255	65 536

Table 1: private IPv4 network range

3.2.2 MULTICAST

IP multicast is a bandwidth conserving technology that delivers data streams to multiple receivers without adding any additional burden on the source or receivers while using the least network bandwidth. In multicast addressing the IP-packet header is set up with a multicast IP-address which will only be received by the IP hosts preset to accept IP-packets with the given multicast IP-address, in other words this is a one-to-many nodes transfer.

For an OSI Layer 3 radio the IP stack may just forward any incoming IP multicast packet instead of filtering incoming IP multicast packets as required by the host gateway.

With multicast addressing it is possible to establish several multicast groups that can be joined by many IP hosts and can support the partitioning of application layer delivery confirmation through multiple groups: position reports in one multicast group and graphics in another multicast group.

Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive information sent to this group. The multicast address is only applicable to the group address or the destination address of an IP packet. The source address for multicast packets is always the unicast source address of the device originating the packet.

Requirement 5. The IPv4 multicast implementation in the Interoperability Network shall be in conformance with IGMPv2 RFC 2236 [13].

3.3 TRANSPORT PROTOCOL

Requirement 6. The Interoperability Network shall support UDP in conformance with Internet STD 0006 (RFC 768 [7]).

Rationale: UDP provides an unreliable transport layer protocol and datagrams may arrive out of order or get lost without notice. As wireless bandwidth in the interoperability network is likely to be limited, it is important to control how lost messages are retransmitted in the interoperability network. The JDSSIEM [4] is responsible for ensuring that messages are retransmitted successfully while accounting for the interoperability network's bandwidth, hence ensuring robust and efficient exchange of information over tactical radio networks.

The Maximum Transmission Unit (MTU) is the size in bytes of the largest UDP datagram that the JDSS Gateway can pass onwards, based on the most restricted device in the path, i.e. the Loaned Radio.

Requirement 7. The JDSS Gateway interface shall either support Path Maximum Transmission Unit Discovery (PMTUD) as described in RFC 1191 [14] or be

able to configure a static MTU that corresponds to the MTU of the device that has the lowest MTU in the network.

Requirement 8. A DSS shall set the Time To Live (TTL) of datagrams by default to 2. It shall provide the ability to configure an alternative value.

Rationale
With a layer 3 loaned radio, the TTL must be set to 2 hops by the sending DSS otherwise the datagrams will be discarded by the loaned radio forwarding function before they reach the other system.

CHAPTER 4 MANAGEMENT PROCEDURES

4.1 GENERAL PRINCIPLE

Dissemination of management information shall be performed prior to deployment and by the appropriate procedures. This section gives guidance to the network operators for the IP addressing plan specification of the Interoperability Network. The Interoperability Network formed by the JDSS Gateways and interconnected by the Loaned Radios is indicated by the dashed rectangle in Figure 3.

In general for Coalition and NATO operations a so called Supporting nation / Supported nation framework is applied. The Supporting nation is given the full responsibility to establish the Command and Control (C2) structures for its own forces, including the troops provided by other nations within its area of responsibility. Therefore, the Supporting nation is probably the nation providing the Loaned Radio and is responsible for the following planning tasks:

- Definition of the rules and policies for the implementation of an IP addressing plan.
- Definition of the rules, policies and constraints for the implementation of multicast addressing mechanisms for the JDSS Gateway interface.

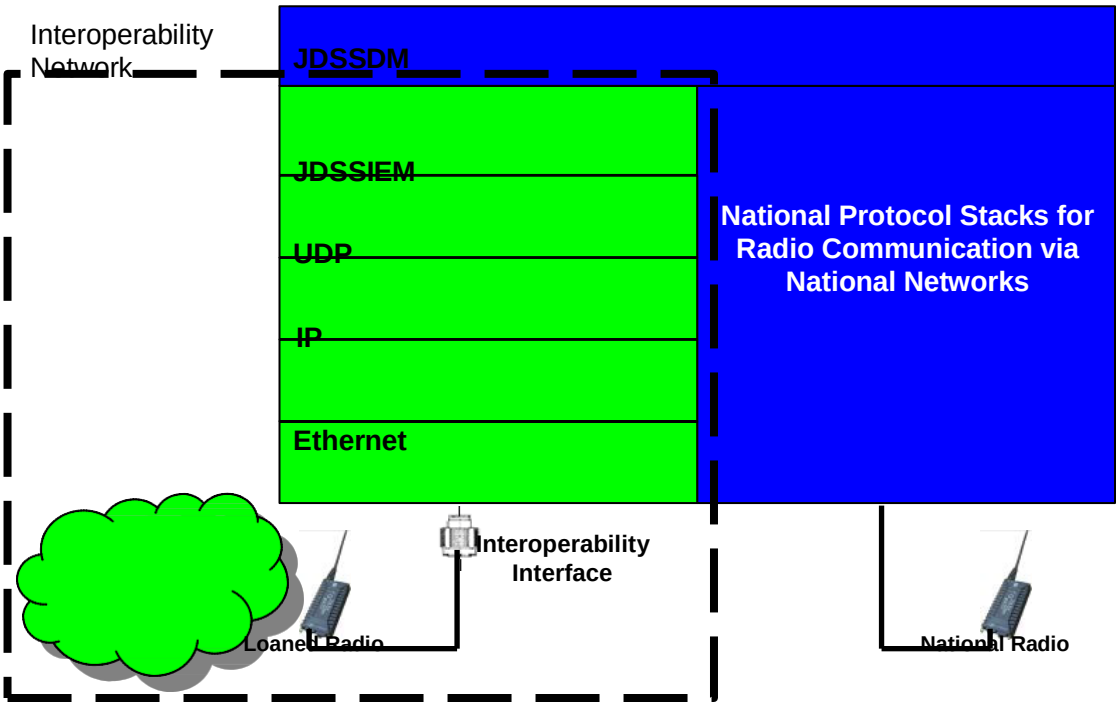

Figure 3 JDSS Gateway interface

4.2 IP ADDRESSING PLAN SPECIFICATION

4.2.1 Address Assignment Guidelines

The IP addressing plan specification is applicable to the Interoperability Network, which includes both the JDSS Gateways and the Loaned Radio network, i.e. the dashed rectangle depicted in Figure 3.

The IP addressing plan specification for the national networks remains a national responsibility.

Based on the Supporting nation / supported nation framework of the previous section, the national network operators in coordination with the Supporting nation must agree upon the IP addressing plan for the Interoperability Network, which follows the characteristics below:

- Agreement on the allocation of addressing blocks, documented prior to deployment
- Use of private IP addressing block based on RFC 1918 [15]

- Selection and use of IP multicast groups as per RFC 2236 [13]
- Implement CIDR and document IPv4 prefix / range before deployment
- Perform network tests before deployment

The Supporting nation providing the Loaned Radio is responsible for the configuration of the Loaned Radio including the IP addressing, radio frequency (RF) settings and key management.

4.2.2 OSI Layer 2 Radio

If an OSI Layer 2 radio is selected for the Interoperability Network, all IP hosts must be configured in one single subnet. An example of such a network IP configuration is illustrated in Figure 4.

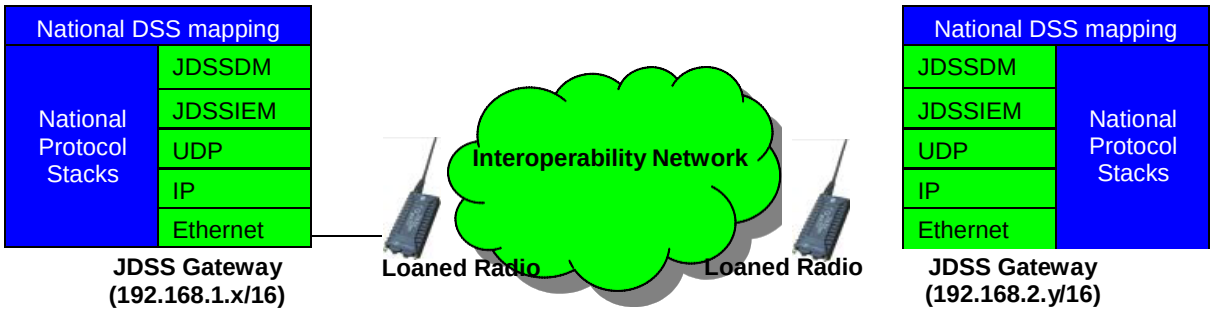

Figure 4: Layer 2 Radio IP Assignment

4.2.3 OSI Layer 3 Radio

When an OSI Layer 3 radio is selected for the Interoperability Network, IP hosts may be in different networks. An example of such a network IP configuration is illustrated in Figure 5.

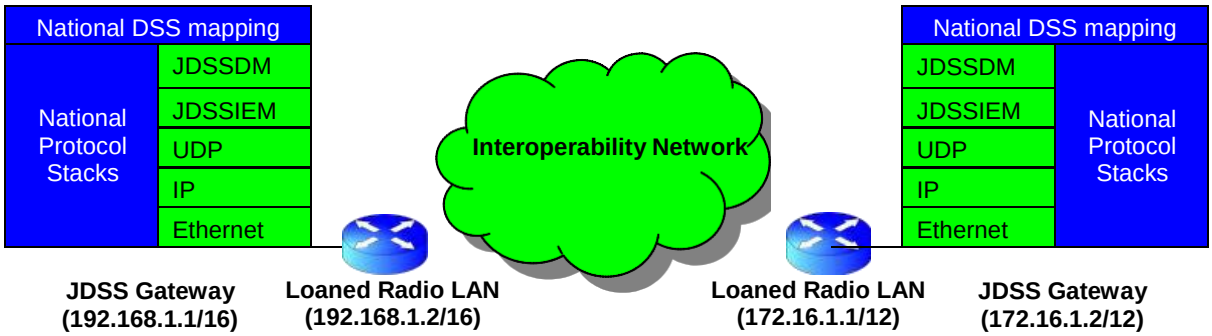

Figure 5: Layer 3 Radio IP Assignment

4.2.4 Multicast Address Assignment

In IPv4 all IP multicast addresses fall in the range from 224.0.0.0 to 239.255.255.255. Within this range the administratively scoped block (from 239.0.0.0 to 239.255.255.255) as defined in RFC 5771 [18] is constrained for local use inside private domains.

Two scopes are defined:

- Local scope (239.255.0.0/16) is the minimal enclosing scope and thus not further divisible.
- Organisational local scope (239.192.0.0/14) is the space from which an organisation should allocate subranges when defining scopes for private use.

Within the JDSS Interoperability Network, multicast addresses should be taken from the 239.192.0.0/14 range (organisational local scope).

CHAPTER 5 TEST AND VERIFICATION

5.1 Unicast / Multicast connectivity and throughput test

Prior to deployment a test confirming the UDP/IP Unicast and Multicast connectivity between all the JDSS Gateways across the Interoperability Network should be performed.

As an example the IPERF test is described for at least 30 seconds, with 500B packet length and 50k bandwidth:

5.1.1 Unicast Test set up description:

Set up all Loaned radios with connected JDSS Gateways at an agreed frequency. Use the JDSS Gateway Computer's Command console for IPERF test in sequence to each of the other connected JDSS Gateway Computer's LAN addresses.

Run the IPERF test as follows:

Client (Nation A): iperf –c 10.1.1.200 (chosen UDP/IP unicast server LAN address) –u (UDP/IP) –l 500 (chosen packet length, if none is set default 1470Bytes) –b 50k (bandwidth, if none is set iperf will push as fast as possible, but with a variable packet loss %) –i 1 (how often presented on the screen) –t 30 (how long you want to measure in seconds) –p 2010 (chosen port)

Server (Nation B): iperf –s –u (UDP/IP) -i 1 (how often measured) - p 2010 (chosen port)

5.1.2 Multicast test set up description

Set up all Loaned radios with connected JDSS Gateways at an agreed frequency. Use the JDSS Gateway Computer's Command consol for IPERF test in sequence to each of the other connected JDSS Gateway Computer's LAN addresses.

Run the IPERF test as follows:

Client (Nation A): iperf –c 239.239.239.1(chosen UDP/IP multicast address) –u (UDP/IP) –T 2 (number of allowed multicast hops, equal to time to live) –l 500 (chosen packet length, if none is set default 1470Bytes) –b 50k (bandwidth, if none is set iperf will push as fast as possible, but with a variable packet loss %) –i 1 (how often presented on the screen) –t 30 (how long you want to measure in seconds) –p 2010 (chosen port)

Server (Nation B): iperf –s –u (UDP/IP) –B 239.239.239.1 (chosen UDP/IP multicast address) -i 1 (how often measured) -p 2010 (chosen port)

ANNEX A ABBREVIATIONS

AEP	Allied Engineering Publication
ARP	Address Resolution Protocol
C2	Command and Control
C4	Command, Control, Computer, Communication
CIDR	Classless Inter Domain Routing
CONEMP	Concept of Employment
DSS	Dismounted Soldier System
HQ	Headquarters
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
JDSSDM	Joint DSS Data Model
JDSSIEM	Joint DSS Information Exchange Mechanism
JDSS	Joint Dismounted Soldier System
LAN	Local Area Network
LCG/1	Land Capability Group 1

MTU	Maximum Transmission Unit
NATO	North Atlantic Treaty Organisation
OSI	Open System Interconnection
PfP	Partners for Peace
PMTUD	Path Maximum Transmission Unit Discovery
RF	Radio Frequency
RFC	Request For Comments
STANAG	Standardization Agreement
STD	Standard
UDP	User Datagram Protocol

AEP-76 VOLV (A)(3)