MARITIME TACTICAL WIDE AREA NETWORKING (MTWAN)

Technical Instructions

Uncontrolled copy when printed

ACP 200(C) Volume 2

March 2010

FOREWORD

1. The Combined Communications-Electronics Board (CCEB) is comprised of the five member nations, Australia, Canada, New Zealand, United Kingdom and United States and is the Sponsoring Authority for all Allied Communications Publications (ACPs). ACPs are raised and issued under common agreement between the member nations.

2. ACP 200(C) Volume 2, MARITIME WIDE AREA TACTICAL NETWORKING (MTWAN) Technical Instructions, is an UNCLASSIFIED CCEB publication.

3. This publication contains Allied military information for official purposes only.

4. This ACP is to be maintained and amended in accordance with the provisions of the current version of ACP 198.

Uncontrolled copy when printed

THE COMBINED COMMUNICATIONS-ELECTRONICS BOARD LETTER OF PROMULGATION

FOR ACP 200(C) Volume 2

1. The purpose of this Combined Communications-Electronics Board (CCEB) Letter of Promulgation is to implement ACP 200(C) Vol 2 within the Armed Forces of the CCEB Nations. ACP 200(C) Vol 2, MARITIME WIDE AREA NETWORKING (MTWAN) Technical Instructions, is an UNCLASSIFIED publication developed for Allied use under the direction of the CCEB Principals

2. ACP 200(C) Volume 2 is effective upon receipt for CCEB Nations and when directed by the NATO Military Committee (NAMILCOM) for NATO nations. ACP 200(C) Volume 1 and 2 will supersede ACP 200(C), which shall be destroyed in accordance with national regulations.

EFFECTIVE STATUS

Publication	Effective for	Date	Authority
ACP 200(C) Vol 2	CCEB	On Receipt	LOP

3. All proposed amendments to the publication are to be forwarded to the national coordinating authorities of the CCEB or NAMILCOM.

For the CCEB Principals

Paul Foster

P. FOSTER
Major, CF
CCEB Permanent Secretary

Uncontrolled copy when printed

RECORD OF MESSAGE CORRECTIONS

Identification of Message Correction And Date Time Group		Date Entered	Entered by (Signature, Name, rank)
DTG	**Correction**		

Uncontrolled copy when printed

TABLE OF CONTENTS

FOREWORD ii
LETTER OF PROMULGATION iii
RECORD OF MESSAGE CORRECTIONS iv
TABLE OF CONTENTS v
LIST OF FIGURES viii
LIST OF TABLES ix

CHAPTER 1 1-1
NETWORK ARCHITECTURE 1-1
INTRODUCTION 1-1
AIM 1-1
OVERVIEW 1-1
DESCRIPTION 1-1
ROUTING ARCHITECTURE (RA) 1-2
AUTONOMOUS SYSTEMS (AS) 1-2
TOPOLOGY 1-3
SINGLE AS TGAN TOPOLOGY 1-3
MULTIPLE AS TGAN TOPOLOGY 1-3
ROUTING PROTOCOLS 1-5
COMMUNICATIONS ARCHITECTURE (CA) 1-5
POINT-TO-POINT 1-5
MULTI-MEMBER 1-7
SECURITY ARCHITECTURE (SA) 1-8
NODE DESCRIPTIONS 1-8
GENERIC MOBILE NODE 1-8
CONCLUSION 1-8

CHAPTER 2 2-1
QUALITY OF SERVICE 2-1
INTRODUCTION 2-1
AIM 2-1
OVERVIEW 2-1
DEFINITION 2-1
LINK THROUGHPUT / BOTTLENECK 2-2
MAXIMIZING LINK THROUGHPUT 2-2
LATENCY 2-2
TCP CONGESTION CONTROL 2-3
CONTROLLING LESS URGENT TRAFFIC 2-3
OBJECTIVE 2-3
VISIBILITY 2-4
TYPES OF APPLICATIONS 2-4
PERFORMANCE MEASURES 2-4
TRAFFIC CLASSIFICATION 2-5
CONTROL 2-5
SERVICE LEVELS 2-5
PRIORITY MARKING OF MTWAN TRAFFIC 2-7
SERVICE CLASSES 2-7
ASSURED FORWARDING SERVICES CLASSES 2-9
COMPRESSION 2-10
TYPES OF COMPRESSION 2-10
PAIR WISE CONFIGURATION 2-10
QOS SOLUTIONS 2-11
INTEROPERABILITY 2-11

Uncontrolled copy when printed

PASS THROUGH FAILOVER 2-11
NETWORK TOPOLOGY 2-11
FUTURE WORK 2-11
MAPPING IER TO QOS 2-12
IPV6 2-12
CONCLUSION 2-12

CHAPTER 3 3-1
NETWORK MANAGEMENT 3-1
INTRODUCTION 3-1
AIM 3-1
OVERVIEW 3-1
NETWORK MANAGEMENT ARCHITECTURE (HIERARCHY) 3-1
PRIMARY NOC 3-1
NATIONAL NOC 3-1
NODE LEVEL 3-1
NETWORK MANAGEMENT ELEMENTS 3-2
PERFORMANCE MANAGEMENT 3-2
SECURITY MANAGEMENT 3-2
REMOTE OR LOCAL MANAGEMENT 3-3
GENERATION OF REPORTS 3-4
SECURITY RESPONSIBILITY 3-4
TOOLS 3-4
ANNEX A TO 1
ANNEX B TO 1
APPENDIX 1 TO 1

CHAPTER 4 4-1
TRANSPORT SERVICES 4-1
INTRODUCTION 4-1
AIM 4-1
OVERVIEW 4-1
TCP OVER HIGH LATENCY LINKS 4-2
IP FRAGMENTATION 4-3
PERFORMANCE ENHANCING TECHNIQUES 4-3

CHAPTER 5 5-1
NETWORK NAMING AND ADDRESSING 5-1
INTRODUCTION 5-1
AIM 5-1
OVERVIEW 5-1
HOST NAMING CONVENTION 5-1
DOMAIN NAMING CONVENTION 5-5
IP SUBNETTING AND MULTICAST ADDRESSING 5-7
CLASS D MULTICAST ADDRESSING 5-7
UNICAST CLASS C IP SUBNETTING 5-8
MULITCAST SUBNETTING 5-8
IP ADDRESSING CONVENTION 5-8
IP ADDRESS AUTHORITY TASKS 5-9
UNIT ASSIGNMENT OF HOSTS 5-9

CHAPTER 6 6-1
ROUTING 6-1
INTRODUCTION 6-1
AIM 6-1
OVERVIEW 6-1
ROUTING ARCHITECTURES 6-2

Uncontrolled copy when printed

INTERIOR TGAN ROUTING 6-6
EXTERIOR TGAN ROUTING 6-7
REDUCING ROUTING PROTOCOL TRAFFIC TO THE ALLIED WAN 6-9
CONCLUSION 6-9

CHAPTER 7 7-1
COMMUNICATION SUBNETS 7-1
INTRODUCTION 7-1
AIM 7-1
OVERVIEW 7-1
DEFINITIONS 7-1
COMMUNICATIONS ARCHITECTURE (CA) 7-3
COMMUNICATION SUBNETS / COMMUNICATION BEARERS 7-4
COMMUNICATION BEARERS/SERVICES 7-5
INTEGRATED SERVICES DIGITAL NETWORK (ISDN) 7-5
INMARSAT B 7-5
HIGH FREQUENCY BEYOND LINE-OF-SIGHT (HF BLOS) 7-6
HIGH FREQUENCY EXTENDED LINE-OF-SIGHT (HF ELOS) 7-6
SUBNET TECHNOLOGIES 7-6
SUBNET RELAY (SNR) 7-6
HF IP 7-6
MEDIUM-RATE CHANNEL ACCESS PROCESSOR (MCAP) 7-7
STANDARD NATO AGREEMENT (STANAG) 5066 EDITIONS 1 AND 2 7-7
CONCLUSION 7-7
GLOSSARY OF TERMS 1
LIST OF EFFECTIVE PAGES 1

Uncontrolled copy when printed

LIST OF FIGURES

Figure 1-1: Notional MTWAN Architecture 1-2
Figure 1-2: Single-AS TGAN 1-3
Figure 1-3: Multiple-AS TGAN 1-4
Figure 1-4: MTWAN Routing 1-6
Figure 1-5: Subnet Combinations 1-7
Figure 1-A-1: MTWAN Transit Network Connectivity 1A-1
Figure 1-A-2: MMF Node Configuration in Transit Phase 1A-2
Figure 1-A-3: MTWAN Connection in Assault Phase 1A-3
Figure 1-A-4: MMF Shore Node Configurations – Assault Phase 1A-3
Figure 1-A-5: Ship Node in Assault Phase 1A-4
Figure 1-A-6: MTWAN Network Connection in Lodgment Phase 1A-4
Figure 1-A-7: MMF Network Nodes in Lodgment Phase 1A-5
Figure 1-A-8: MTWAN Network in Sustainment Phase 1A-6
Figure 1-A-9: MMF Unit 2 Node Configuration in Sustainment Phase 1A-6
Figure 2-1: Grades of Service 2-6
Figure 4-1: Multicasting and Multicast Gateways 4-4
Figure 4-2: WAN Optimizers 4-6
Figure 5-A-1: IP Address 5A-2
Figure 5-B-1: Domain Name Schema 5B-2
Figure 5-B-2: DNS Servers 5B-3
Figure 6-1: Router Protocol Stacks 6-2
Figure 6-2: Interior and Exterior TGAN Routing 6-3
Figure 6-3: An Example of a Multi-AS TGAN 6-4
Figure 6-4: Private Routing 6-5
Figure 6-A-1: Sample BGP Configuration 6A-2
Figure 6-B-1: Example of Coalition and National Subnets Bandwidth 6B-2
Figure 6-B-2: Link Metric Values (Notional) 6B-3
Figure 7-1: Communication Subnet(s) 7-2
Figure 7-2: Communications Architecture 7-3
Figure 7-A-1: Operational View 7A-3
Figure 7-A-2: Relaying Concept 7A-3
Figure 7-A-3: Ship Moving from one Battle Group to Another 7A-4
Figure 7-A-4: Multiple, Dynamic Relays 7A-4
Figure 7-A-5: Relaying only when needed 7A-5
Figure 7-A-6: Subnetwork Splitting 7A-5
Figure 7-A-7: Subnetwork Mapping 7A-6
Figure 7-A-8: Multiple Relays to Destination 7A-6
Figure 7-B-1: Typical Network Node Configuration 7B-2

Uncontrolled copy when printed

LIST OF TABLES

Table 2-1: AF Service Classes 2-9
Table 2-2: Recommended QoS packet markings for a MTWAN 2-10
Table 5-1: Abbreviations for 'Use' Field 5-3
Table 5-2: Abbreviations for 'Type' Field 5-4
Table 5-A-1: IP Address Classes 5A-1
Table 6-B-1: Recommended Metric Values 6B-1
Table 7-1: Communication Subnet Matrix 7-5

Uncontrolled copy when printed

CHAPTER 1

NETWORK ARCHITECTURE

INTRODUCTION

101. Network architecture describes the logical structure and operating principles that govern a network. An MTWAN architecture, by necessity, has a flexible logical network structure capable of supporting heterogeneous computing in a Radio Frequency (RF) environment. This chapter expands upon the systems and technical concepts introduced in Chapter 2.

AIM

102. This chapter describes proven network architectures suitable for supporting a MTWAN.

OVERVIEW

103. The term 'network architecture' is commonly used to describe a set of abstract principles for the technical design of protocols and mechanisms for computer communication. The MTWAN Network Architecture (NA) represents a set of deliberate choices from a set of design alternatives, where the choices are informed by an understanding of the requirements canvassed in Chapter 2. In turn, this architecture provides a guide for the many technical decisions required to standardize network protocols, algorithms and schemas that appear in the subsequent chapters. The purpose of the architecture is to provide coherence and consistency to these decisions and to ensure that the requirements are met.

104. A Network Architecture describes:

a. The overall geographic layout of the network;

b. How it is connected to other networks;

c. How computers will communicate with one another;

d. How entities, such as computers and domains, are named;

e. Where security boundaries are drawn and how they are enforced; and

f. How management boundaries are drawn and selectively pierced.

DESCRIPTION

105. An MTWAN (Figure 1–1) comprises one or more Task Group Area Networks (TGANs) where a TGAN is a collection of mobile units such as ships and submarines. It may

Uncontrolled copy when printed

also include Maritime Marine Force (MMF) and Maritime Air Groups (MAG) as well as Network Operation Centers (NOCs).

106. Within an MTWAN, connectivity between mobile units is via Radio Frequency (RF) communications (although NOC-to-NOC connectivity may be terrestrial).

107. In terms of topology and routing protocols, an MTWAN is influenced by its distributed and low bandwidth, high latency environment. An important key to the MTWAN routing architecture (and any routing architecture) is the design and management of Autonomous Systems.

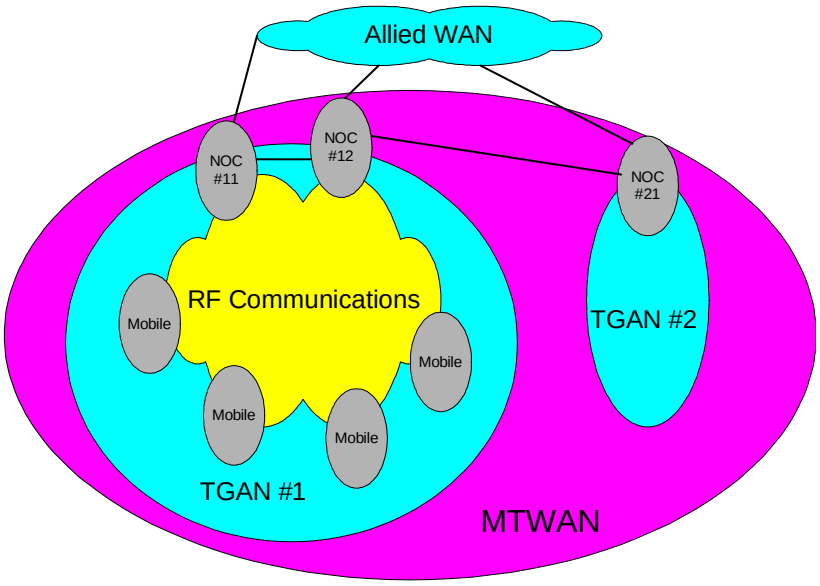

Figure 1-1 Notional MTWAN Architecture

ROUTING ARCHITECTURE (RA)

AUTONOMOUS SYSTEMS (AS)

108. An MTWAN comprises one or more AS. An AS is a collection of networks, or more precisely, the routers joining those networks that are under the same administrative authority and that share a common routing strategy. An AS has a single 'interior' routing protocol and policy, and is also sometimes referred to as a routing domain. Interior routing information is shared among routers within the AS, but not with systems outside the AS. However, an AS may announce its internal networks to other AS that it is linked to. On the Internet, an AS is an Internet Service Provider (ISP), but universities, research institutes, and private organizations also usually have their own AS.

Uncontrolled copy when printed

TOPOLOGY

109. The MWTAN is a distributed system. As a distributed network, there are two considerations: the network topology ('what is connected to what, with what constraints?') and the physical location ('what is physically near what?'). In terms of topologies, MTWAN employs either a single-AS TGAN topology or a multiple-AS TGAN topology. The latter is generally employed to allow nations within an MTWAN to administer their own mobile units.

SINGLE AS TGAN TOPOLOGY

110. An example of a single-AS TGAN is shown in Figure 1–2. All mobile units and the NOC belong to the same AS. The TGAN may have multiple connections to the allied WAN for redundancy and load sharing.

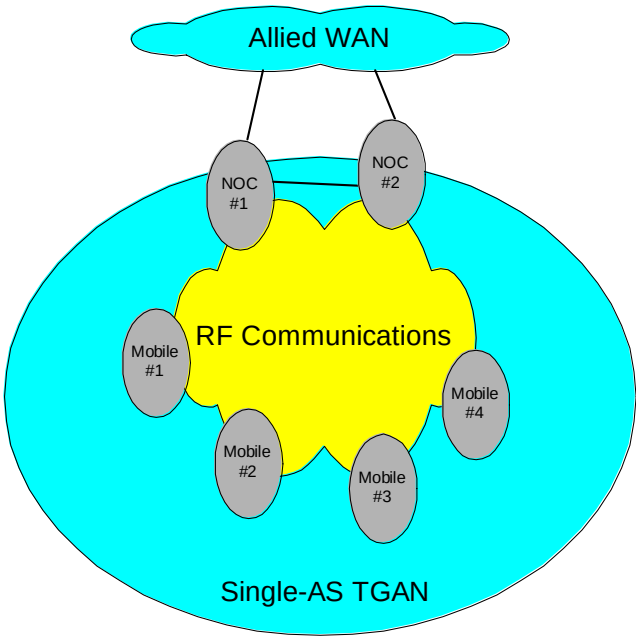

Figure 1-2 Single-AS TGAN

MULTIPLE AS TGAN TOPOLOGY

111. A nation may set up its own AS within a TGAN. Each AS will contain a group of mobile units as illustrated in Figure 1–3. Each mobile unit will have peer-to-peer connections to other mobile units; these connections may be via any communications path but are typically via tactical circuits such as HF/UHF. Some of the mobile units may have connectivity back to the Allied WAN via a national node or NOC. When this connectivity is achieved, the NOC forms part of the AS. Communication between the mobile unit and the NOC is typically done

Uncontrolled copy when printed

via Military or Commercial SATCOM. National NOCs may host connections from other nations' mobile units.

112. Design and implementation of unicast and multicast routing in support of a multiple-AS TGAN is much more difficult in comparison to a single-AS one. However, a multiple-AS topology will allow each nation to control and manage its own AS. Moreover, route changes inside an AS can be hidden from other AS. As a result, the new routing information will not need to be propagated throughout the TGAN and therefore will not consume valuable communication bandwidth.

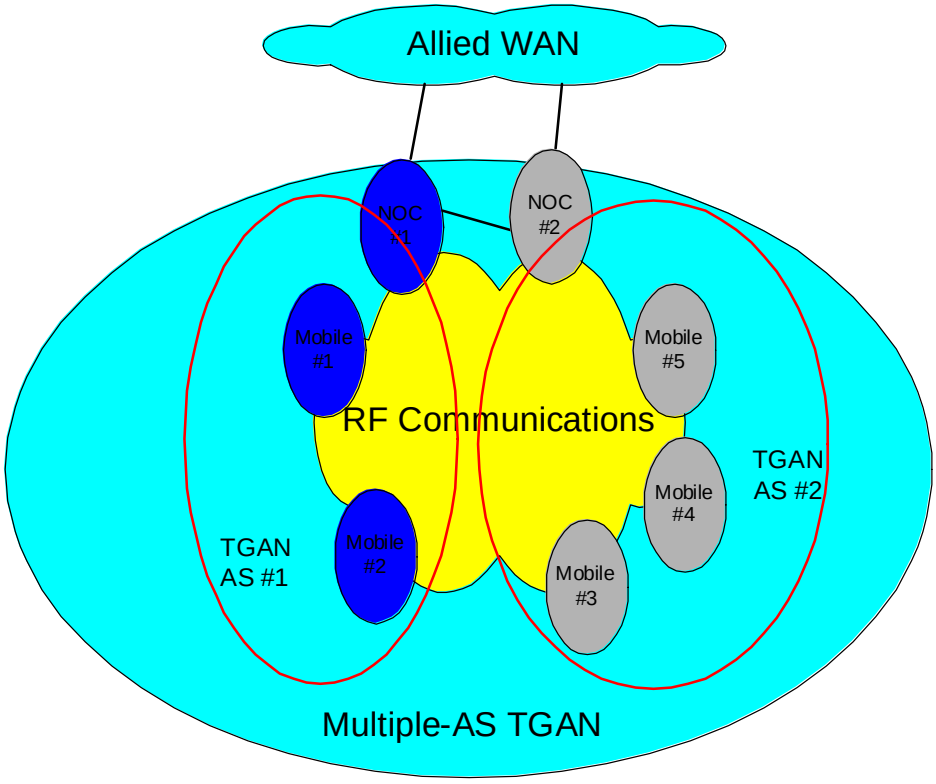

Figure 1-3 Multiple-AS TGAN

Uncontrolled copy when printed

ROUTING PROTOCOLS

113. An MTWAN employs standard IP routing protocols to achieve connectivity. This has the advantage of utilizing Commercially-Off-The-Shelf (COTS) equipment, but constrains the amount of configuration that can be done to the network. Routing is achieved using standard protocols Open Shortest Path First (OSPF) and Protocol Independent Multicast (PIM) for routing within the AS (interior-AS routing), and Border Gateway Protocol Version 4 (BGP4) for routing between AS's (exterior-AS routing). Figure 1-4 shows a MTWAN that comprises a single-AS TGAN and depicts where BGP4 and OSPF are deployed. Detailed information on the routing architecture can be found in Chapter 15

COMMUNICATIONS ARCHITECTURE (CA)

114. The communication subnets within a TGAN, such as those shown in Figure 1–4 are supported by point-to-point and multi-member (shared) links.

POINT-TO-POINT

115. Point-to-point links are communication bearers that connect two nodes in either full-duplex or half-duplex mode. Examples of full-duplex point-to-point links are INMARSAT and SHF. A half-duplex point-to-point link between two nodes can be established using radios operating on a single frequency as only one node can transmit at any one time.

Uncontrolled copy when printed

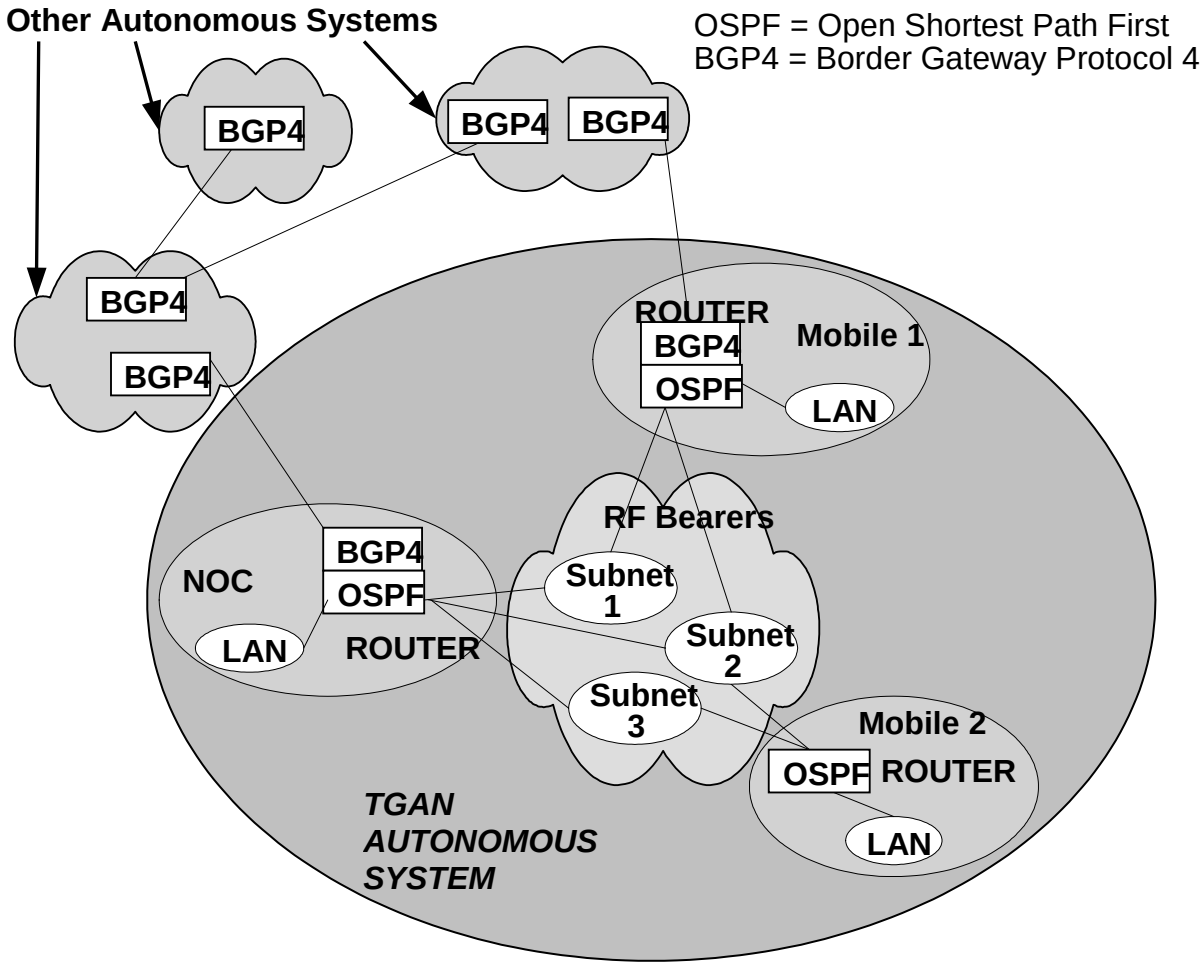

Figure 1–4 MTWAN Routing

Uncontrolled copy when printed

MULTI-MEMBER

116. Multi-member links are those that connect two or more nodes, whereas a point-to-point link supports two nodes only. In a multi-member or half-duplex point-to-point link, a single RF channel is shared. As an example, this can be achieved by a Time Division Multiple Access (TDMA) technique. Multi-member links are further divided into two categories: Broadcast and Non-Broadcast Multiple-Access (NBMA). In a Broadcast subnet, all members can hear each other. UHF SATCOM is an example of a broadcast multi-member link when all members are within the footprint of a satellite. In a NBMA subnet, full connectivity among all members can not be guaranteed, that is, not every member can hear every other member. An example of a NBMA subnet is UHF Line-Of-Sight (LOS). Due to its movement, a member may be out of the UHF LOS range of some, but not all, members of the subnet.

117. A wide range of subnet combinations exist, some of which are shown in the Figure 1–5. Communications subnets that can be employed with a MTWAN are described in Chapter 7.

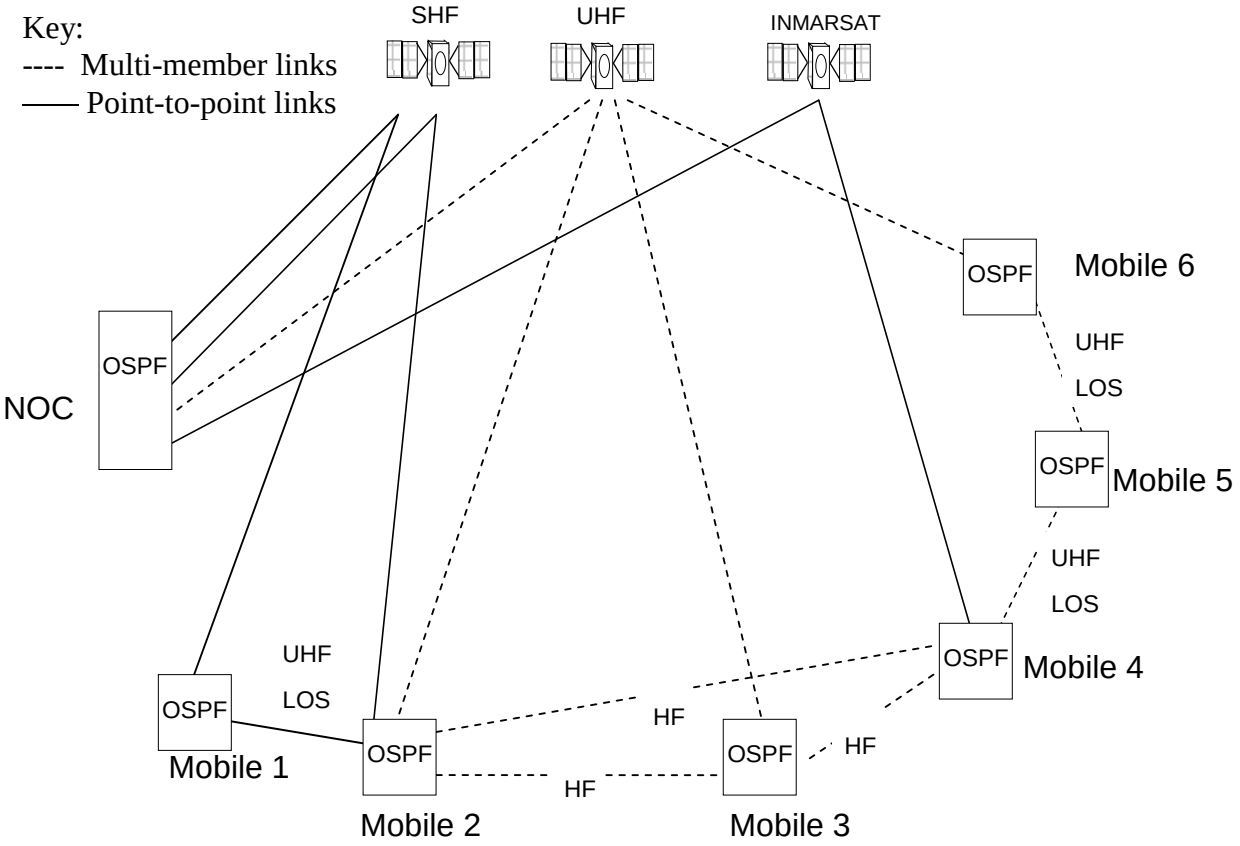

Figure 1–5 Subnet Combinations

Uncontrolled copy when printed

SECURITY ARCHITECTURE (SA)

118. The security architecture is designed to promote the flow of information at the tactical level while abiding by Allied security policies. This can be achieved through the use of the following:

a. a. Allied peer-to-peer tactical communications networks that are isolated from Coalition and National networks;

b. b. Boundary Protection Devices (BPD) to enable the exchange of applications data between different security levels;

c. c. Inline Network Encryptor (INE) to support Virtual Private Networks (VPN) over an existing IP infrastructure of a different security level;

119. For example, an INE such as TACLANE can be used to create an allied VPN and tunnel allied IP traffic through national networks, subject to the security policy of the respective nation. Network security details can be found in Chapter 5.

NODE DESCRIPTIONS

GENERIC MOBILE NODE

120. The generic architecture of a typical mobile node consists of the following: RF communication systems, modems, link cryptographic devices, a router, any necessary interface equipment needed to interface RF channels to the router, and a LAN. Examples of the RF communication systems include INMARSAT, MILSATCOM, HF and UHF. Details of the communication systems and their interface equipment can be found in Chapter 16. The LAN equipment includes servers, workstations, printers and hubs on which information resides and applications run. Examples of applications are E-mail, GCCS-M, Web services and Distributed Collaborative Planning (DCP) tools.

121. Subject to national security policy, connection between nodes can be done via the infrastructure provided by another IP network of a different security level. An INE will connect the MTWAN router to the router of the other network.

CONCLUSION

122. The MTWAN Network Architecture is designed for low bandwidth, high latency, and mobile environments. It reflects present operational networks and continually evolves to reflect technology improvements.

Uncontrolled copy when printed

NETWORK ARCHITECTURE TO SUPPORT AMPHIBIOUS OPERATIONS

INTRODUCTION

1. The requirement to support marine elements with a MTWAN imposes further complexities to network design and management. The principle challenge to have a network that can facilitate the transition from the CATF to CFLCC while not impeding operations.

AIM

2. The aim of this Annex is to present a potential solution for supporting amphibious operations.

OVERVIEW

3. A Multi-national Marine Force (MMF) amphibious operation is a four-phase process: transit, assault, lodgement, and sustainment.

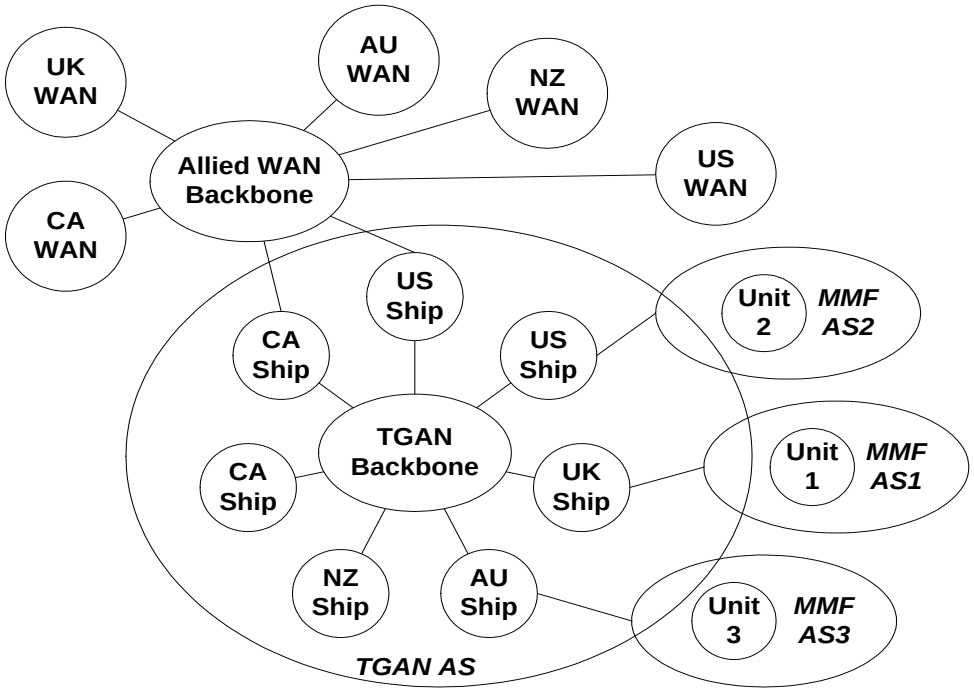

Figure 1-A-1 Transit Network Connectivity

Uncontrolled copy when printed

TRANSIT

4. A typical network configuration in the transit phase is shown in Figure 1–A–1. In this example, three MMF units are located on three amphibious ships. The ships are part of the TGAN autonomous system (AS). Each MMF unit consists of a collection of host computers, LANs and routers, which operate in a separate MMF autonomous system, connected to the ships TGAN autonomous system using the BGP4 protocol as shown in Figure 1–A–2. Any communication between the MMFs in the transit phase would use the TGAN backbone subnets.

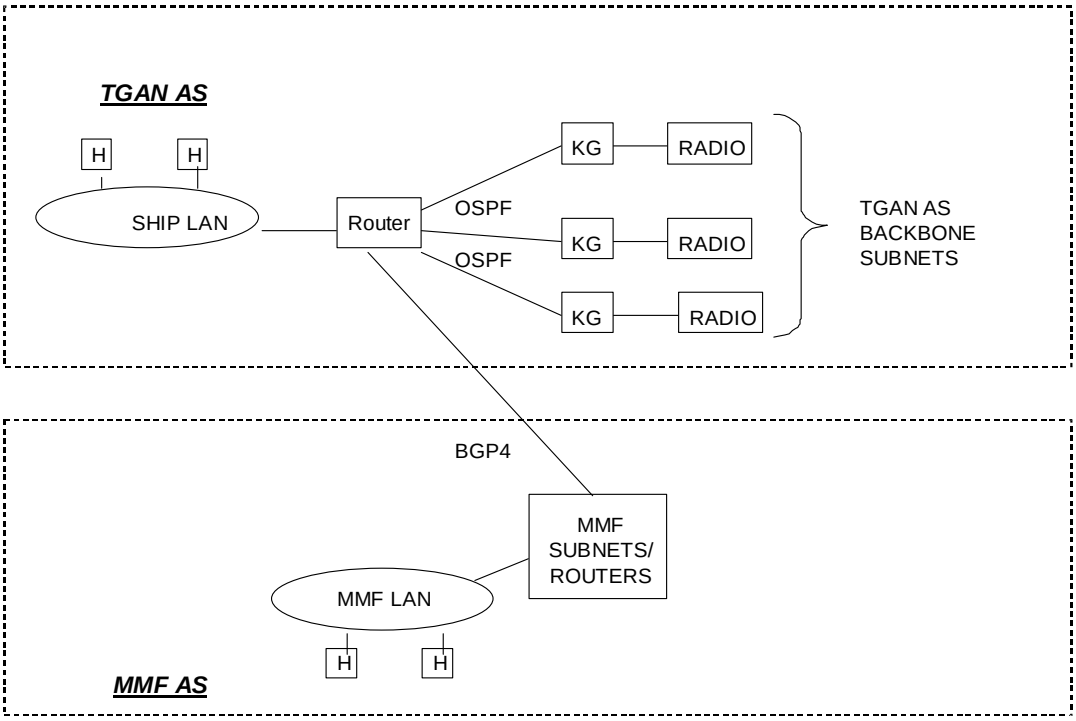

Figure 1-A-2 MMF Node Configuration in Transit Phase

ASSAULT

5. In a typical assault phase the network connections are shown as in the example, Figure 1–A–3. In this phase the MMF units have disembarked and set up subnets back to the units command ship. The MMF units remain in their own AS. Any communications between the ashore units will be through their command ships and over the MMF backbone subnets. The ship node configuration remains the same as in the transit phase except the MMF subnets are placed in operation.

6. Typical MMF shore nodes are shown in Figure 1–A–4.

7. The ship node in the assault phase is shown in Figure 1–A–5.

Uncontrolled copy when printed

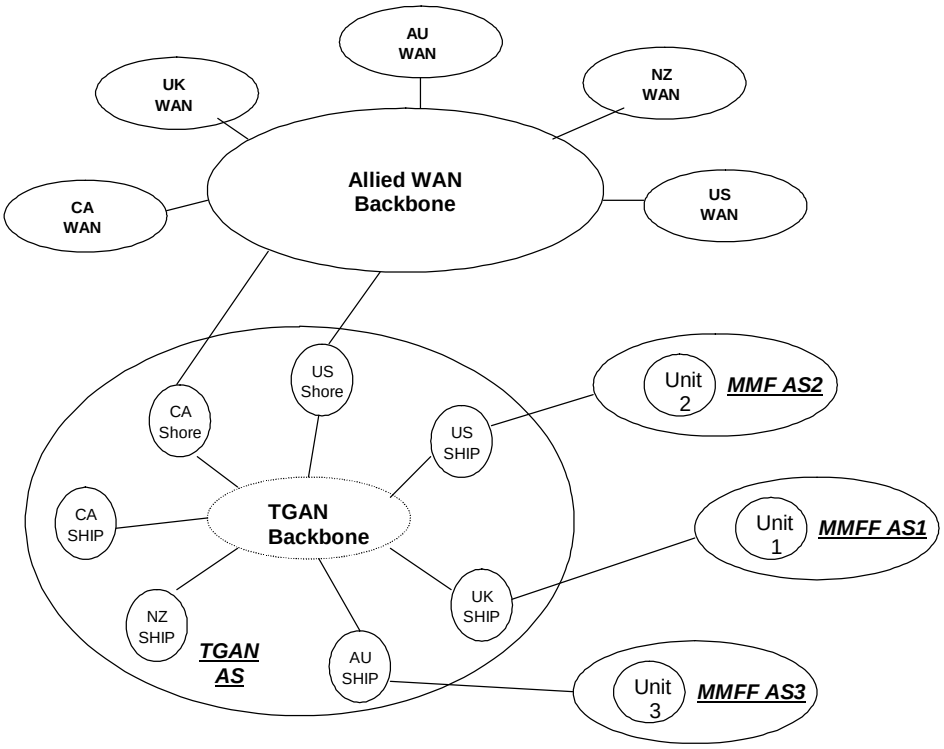

Figure 1–A–3 Network Connection in Assault Phase

LODGEMENT

8. A typical lodgement phase configuration, shown in Figure 1–A–6, is where the three MMF units establish a subnet between their AS. This removes the dependency on the MTWAN backbones subnets for unit to unit connectivity.

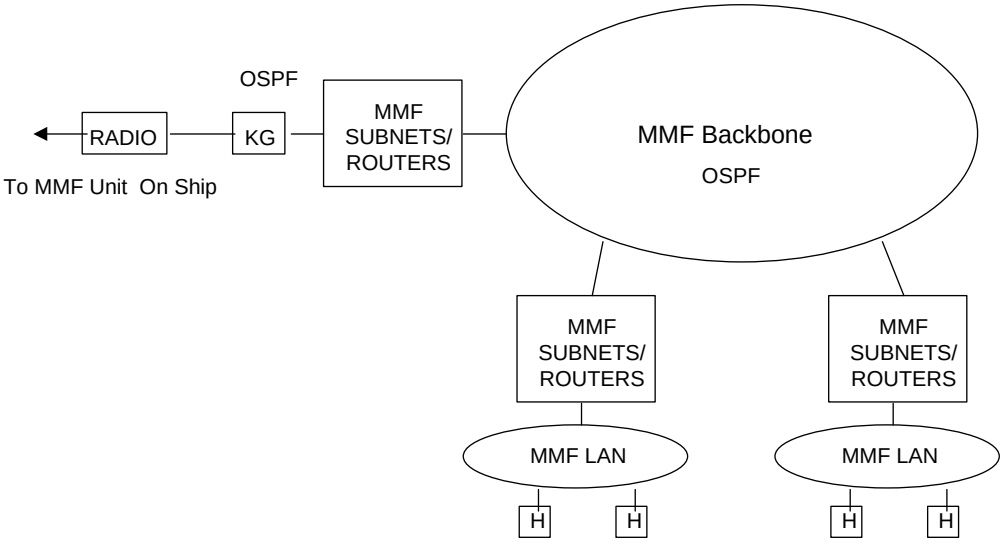

Figure 1–A–4 MMF Shore Node Configurations – Assault Phase

Uncontrolled copy when printed

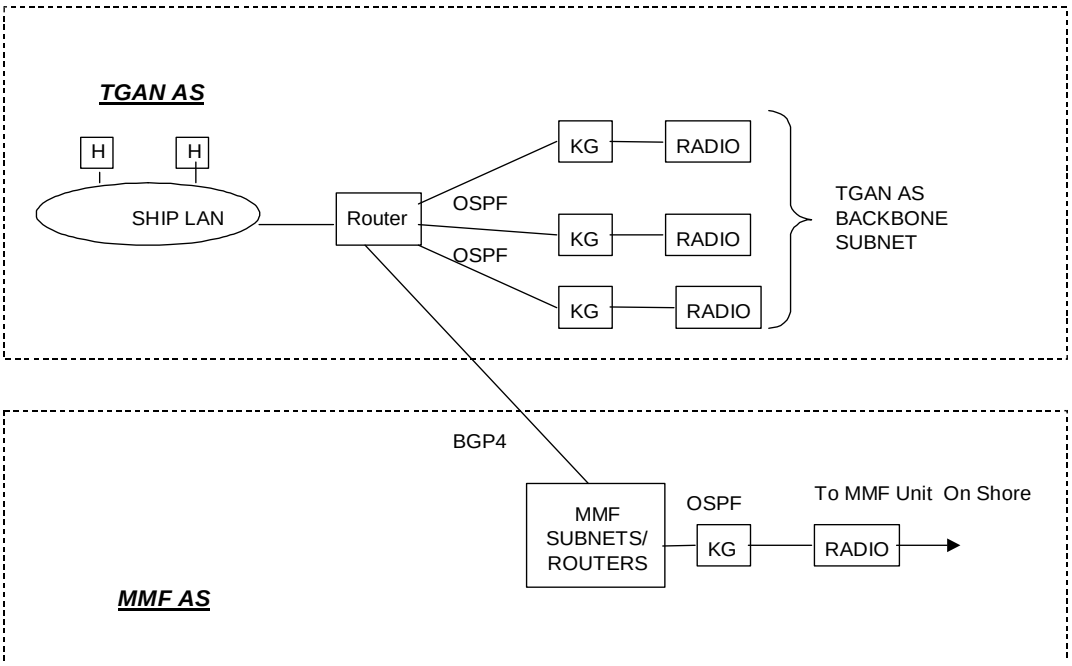

Figure 1–A–5 Ship Node in Assault Phase

9. The general MMF unit node configurations are likely to be as shown in Figure 1–A–7. In this configuration the MMF node will include a router connected to another MMF network using BGP4.

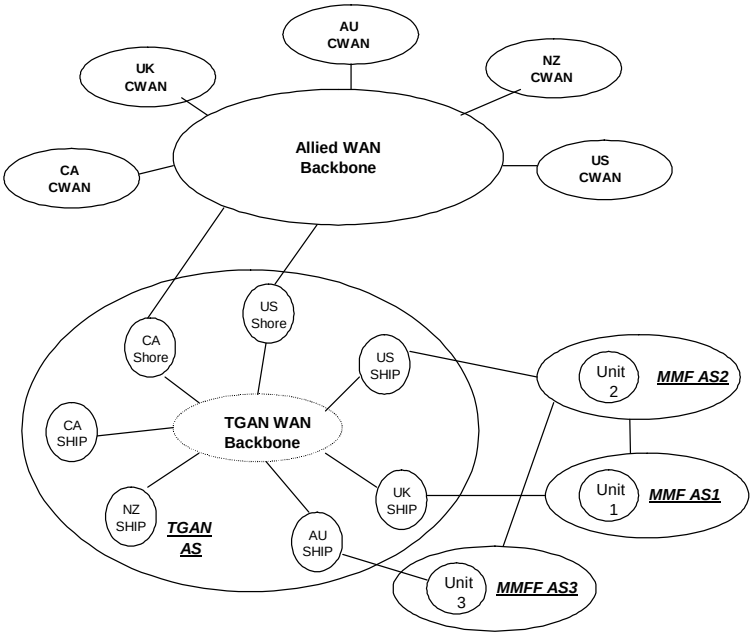

Figure 1–A–6 Network Connection in Lodgement Phase

Uncontrolled copy when printed

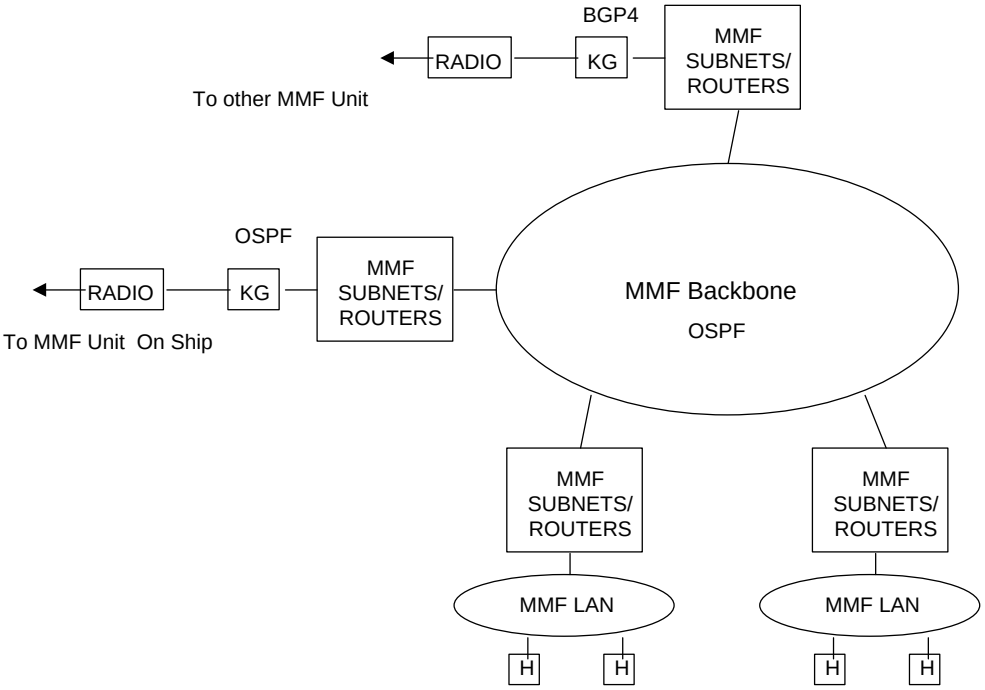

Figure 1–A–7 MMF Network Nodes in Lodgement Phase

SUSTAINMENT

10. A typical sustainment phase is shown in Figure 1–A–8. In this phase there is actually a transition step when the direct connection to the Allied WAN is established and the subnets to the MTWAN are still in operation. The final phase would be when the MTWAN subnets are no longer used. The connection to the allied WAN would be established by Unit 2 only and Units 1 and 3 connections to the allied WAN would be through unit 2.

Uncontrolled copy when printed

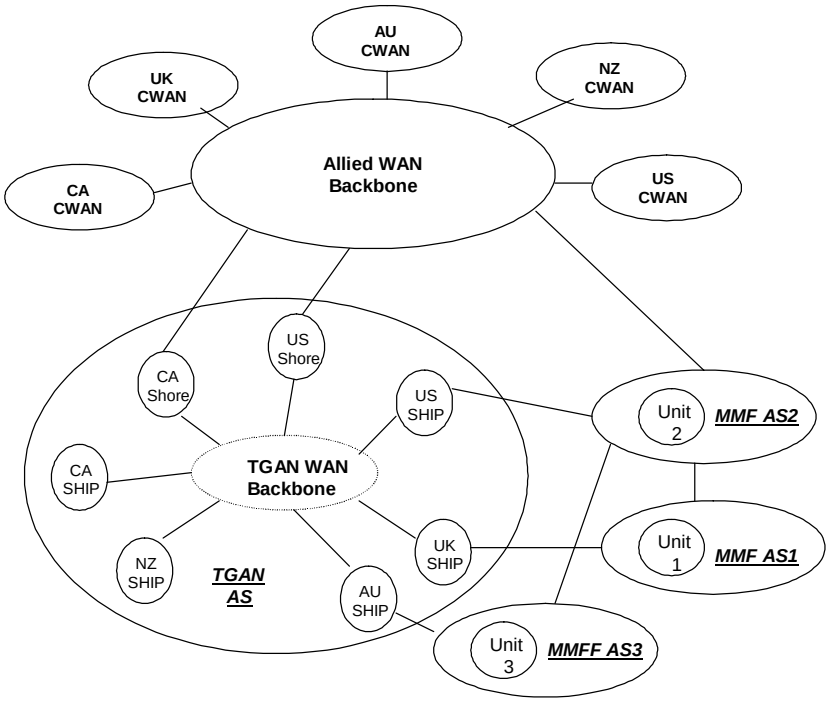

Figure 1–A–8 Network in Sustainment Phase

11. The node configuration for unit 2 in the sustainment phase is shown in Figure 1–A–9. In this example, this node acts as the gateway for other MMF nodes to the shore CWAN. The connection to the ship can be deleted as required. All other MMF nodes remain the same as the lodgment phase.

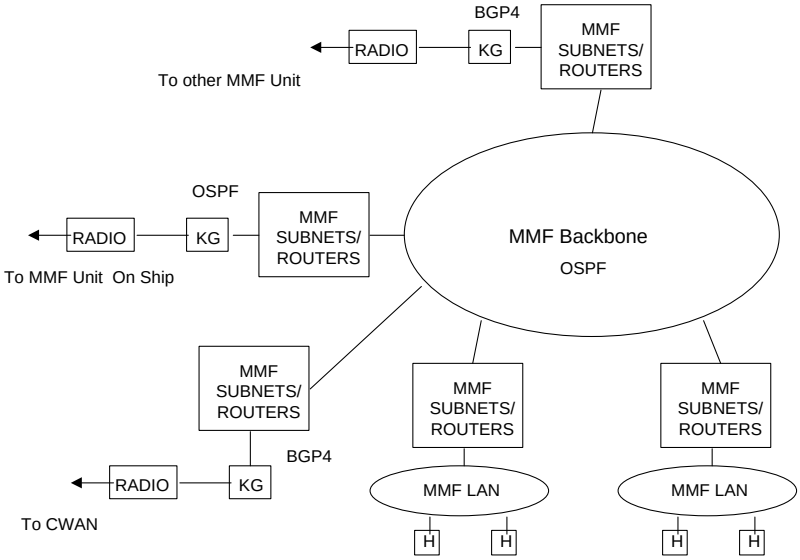

Figure 1–A–9 MMF Unit 2 Node Configuration in Sustainment Phase

Uncontrolled copy when printed

CHAPTER 2

QUALITY OF SERVICE

INTRODUCTION

201. The "best-effort" nature of IP-based networking can result in significant performance degradation when a network becomes congested. This is more likely to occur in bandwidth constrained and high latency environments such as Wide Area Networks (WANs) than within Local Area Networks (LANs).

202. To minimise the operational impact of congestion within WANs, it is highly desirable to implement Quality of Service (QoS) to optimise the traffic flow across WAN links and to ensure that more important traffic is afforded an improved grade of service. This becomes essential when data, voice and video are converged onto a single network.

AIM

203. This chapter presents a framework for providing QoS in a wireless mobile tactical network.

OVERVIEW

204. IP only provides Best Effort Service in that traffic is processed as quickly as possible, but there is no guarantee as to timeliness or actual delivery. However, the fundamental concept behind QoS is that better service to certain traffic flows can be provided by either raising the priority of a flow or limiting the priority of another flow.

205. This chapter concentrates on improving the performance of IP packet flow through the network(s). The challenge from a technical perspective is how to make the right trade-off between simplicity and control to ensure a predictable and manageable network.

DEFINITION

206. Quality of Service (QoS) is an encompassing term describing the collection of activities, management functions and strategies that aim at guaranteeing the end-to-end, predictable and consistent behaviour of network-dependent applications. This definition of QoS highlights:

a. Predictability and Consistency – A service response is predictable when the conditions for its delivery are known over a period of time. Consistency is the difference between the nature of an expected response and the actual one;

b. Guarantee – There needs to be some level of assurance in terms of predictability and consistency;

Uncontrolled copy when printed

c. Management – A management function is necessary in achieving predictability and consistency and includes such mechanisms as negotiation, admission control and monitoring; and

d. End-to-end – QoS is really only achieved in a distributed application if it has been addressed at every level of the OSI 7-layer model.

LINK THROUGHPUT / BOTTLENECK

207. The available bandwidth interconnecting shore-based IP routers can be very large (e.g. fiber). In an MTWAN, the available bandwidth is very limited, but the processing power and storage capabilities – both increasing rapidly due to hardware advances – are relatively unconstrained considering the router throughputs and network sizes that must be supported. Subsequently, the principal bottlenecks for any MTWAN is the throughput of its WAN links. Unmanaged congestion at speed-conversion bottlenecks on WAN-access links leads to unpredictable delays.

208. The primary causes of slow throughput on WANs are well known: high delay (i.e. high latency), limited bandwidth, and “chatty” application protocols. This chapter addresses how to improve the performance of IP packets through WAN links. In doing so, a secondary result will likely be performance improvements within LANs.

209. The temptation to define communication subnets using simplistic measures such as raw bandwidth alone should be avoided. Instead it is necessary to look for measures that directly relate to the ability of the facilities to support the higher-level services, measures that specify QoS parameters such as bandwidth, delay, and loss characteristics.

MAXIMIZING LINK THROUGHPUT

210. If link throughput is sub-optimal, simply adding bandwidth or compression will not necessarily solve the problem of application performance on WANs. One reason is because critical applications that suffer poor performance are not necessarily the applications that get access to extra capacity. Paradoxically, it usually is the less-urgent, bandwidth hungry applications that monopolize increased bandwidth.

LATENCY

211. First, the ‘round-trip time’ of a packet of data (i.e. the network latency), has a direct effect on the performance or throughput of a window-based protocol like TCP or any request-response protocol. High round trip times slow down "chatty" applications, even if the actual amounts of data transmitted in each transaction are not large.

212. Adding bandwidth (or compressing data) does not improve throughput when the round-trip time exceeds the critical point where throughput is bounded, or when the problem is primarily latency and not bandwidth related. Once the latency exceeds the critical point, throughput decays quickly.

Uncontrolled copy when printed

213. This effect is easy to understand intuitively: the rate of work that can be performed by a client-server application that executes serialized steps to accomplish its tasks is inversely proportional to the round-trip time between the client and the server. If the client-server application is bottlenecked in a serialized computation (i.e., it is "chatty"), then increasing the round-trip time by a factor of two causes the throughput to decrease by a factor of two – it takes twice as long to perform each step (while the client waits for the server and vice versa).

214. More generally, the throughput of client-server applications that are not “chatty” but run over a window-based protocol (like TCP) can also suffer a similar fate. This can be modeled with a simple equation that accounts for the round-trip time (RTT) and the protocol window (W). The window is how much the sender can transmit before receiving acknowledgement from the receiver. Once a window's worth of data is sent, the sender must wait until it hears from the receiver. Since it takes a round-trip time to receive the acknowledgement from the receiver, the rate at which data can be sent is simply the window size divided by the round trip time: $T = W / RTT$.

TCP CONGESTION CONTROL

215. Secondly, an additional constraint on throughput has to do with the congestion control algorithm designed into TCP. This flaw can be significant even in WANs where bandwidth is above a few megabits and is probably the key reason why one often fails to see marked performance improvements of individual applications after bandwidth is substantially increased. This effect is so dramatic that at 100ms of delay (i.e. a typical cross country link); TCP is able to use only 4.5 Mbps of a 45 Mbps link.

CONTROLLING LESS URGENT TRAFFIC

216. Large packets delivered from lower priority, high bandwidth applications may affect the latency for higher priority, latency intolerant applications (such as voice). For example, a 1500-byte packet delivered as part of a file transfer over a 64-Kbps link will take 187 ms to be transmitted. This means a voice packet cannot be transmitted during this interval. As a result, voice cuts or delays will be heard for voice traffic queued behind this large packet.

217. Different speed links in the network may mean that packets may get queued internally in the network. When packets queue internally in the backbone of a network, latency and quality can be affected.

218. Subsequently, it is important to regulate less urgent traffic (such as Personal E-mail and internet access).

OBJECTIVE

219. The objective of QoS is to achieve end-to-end predictability of IP packet delivery for Command through:

a. Visibility of the WAN connection;

Uncontrolled copy when printed

b. Ensuring critical application performance;

c. Controlling less urgent traffic;

d. Maximising throughput; and

e. Analysing response times, link allocation, and network efficiency.

220. The goal of QoS is to apply the principle of shielding users from network limitations such as latency, unreliability, and other such network faults.

VISIBILITY

221. Visibility of the network is a necessary first step towards implementing any QoS solution. It is important to understand what is occurring in a network (i.e. precisely which applications transverse the network, what portion of the bandwidth they consume, how well they perform, and where the delays originate, etc.) before one can effectively control and compress any traffic intelligently. Ideally, this requires a solution capable of providing in-depth visibility, analysis, and trending the network.

TYPES OF APPLICATIONS

222. The application types play a major role in the network performance. Essentially there are three kinds of network applications:

a. Normal (dynamic) – Elastic applications such as email and FTP use the available bandwidth dynamically;

b. Tolerant real time (static) – These applications can tolerate delays by buffering the receiver to dampen variations. An example is streaming video broadcasts; and

c. Intolerant or non-dynamic real-time (live) – These applications require a preset level of bandwidth to function. Examples include VoIP and VTC. VoIP is characterized as relatively low bandwidth, but requiring a low latency and low jitter-delivery to ensure toll quality. VTC requires higher bandwidth, but still requiring low latency and low jitter for high quality video and sound.

223. These applications / services differ widely in the QoS they require. The result of inappropriate priority and precedence can vary from information arriving late (e.g. message delayed) to being incomprehensible (e.g. real-time video & voice with excessive latency and jitter).

PERFORMANCE MEASURES

224. The following measures are commonly used in describing network performance:

a. Service availability – the reliability of the user's connection to the network;

Uncontrolled copy when printed

b. Delay - the time interval between transmitting and receiving packets (i.e. latency);

c. Delay variation – the variation in duration between all packets in a stream taking the same route (i.e. jitter); and

d. Packet loss rate – the maximum rate at which can be discarded during transfer through a network. This actually results from congestion.

TRAFFIC CLASSIFICATION

225. To provide preferential service to a type of traffic, it must first be identified and then the packet may or may not be marked. These two tasks make up classification:

a. When the packet is identified but not marked, classification is said to be on a per-hop basis. With this per-hop basis, the classification pertains only to the device that it is on, and is not passed to the next router. This happens with Priority Queuing (PQ) and Custom Queuing (CQ); and

b. When packets are marked for network-wide use, IP precedence bits can be set.

226. Common methods of identifying flows include Access Control Lists (ACLs), policy-based routing, Committed Access Rate (CAR), and Network-Based Application Recognition (NBAR).

CONTROL

227. Flexible policies are required to protect critical applications, to regulation “greedy” traffic, to limit recreational usage, and block malicious traffic. These policies should be able to:

a. Protect the performance of important applications;

b. Contain unsanctioned and recreational traffic;

c. Provision steady streams for inelastic applications such as voice and VTC;

d. Stop applications or users from monopolizing the link;

e. Reserve or cap bandwidth; and

f. Provision bandwidth between multiple locations, groups or users.

SERVICE LEVELS

228. Service levels refer to the actual end-to-end QoS capabilities, meaning the capability of a network to deliver service needed by specific network traffic from end to end or edge to

Uncontrolled copy when printed

edge. The services differ in their level of QoS, which describes how tightly the service can be bound by specific bandwidth, delay, jitter, and loss characteristics.

229. Three basic levels of end-to-end QoS can be provided across a heterogeneous network, as shown in Figure 2–1:

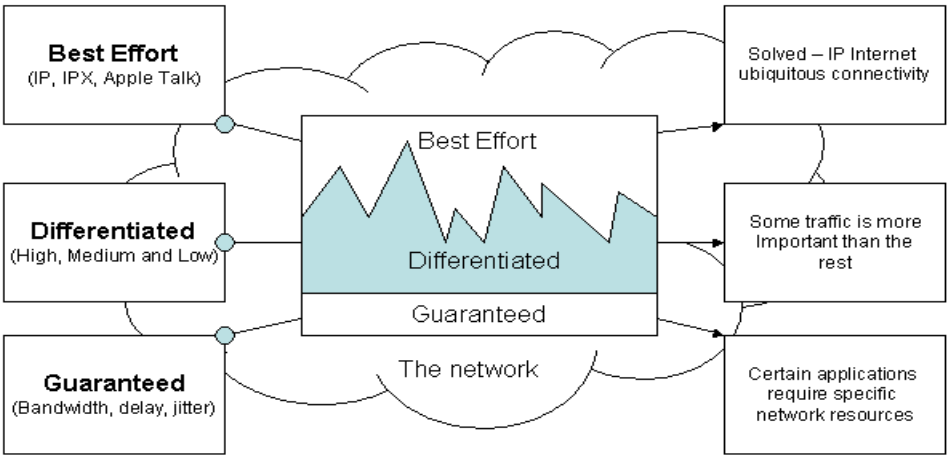

Figure 2–1 Grades of Service

Uncontrolled copy when printed

230. Deciding which type of service is appropriate to deploy in the network depends upon:

a. Whether the current infrastructure can support the specific QoS methods intended;

b. The application or problem that Command is trying to solve; and

c. Whether it is simple to deploy and simple to maintain.

PRIORITY MARKING OF MTWAN TRAFFIC

231. Quality of service management involves creating and monitoring specific traffic classes within the network. Creating traffic classes requires a baseline understanding of network utilization, specific application requirements, and business application priorities. Application requirements include knowledge of packet sizes, time-out issues, jitter requirements, burst requirements, batch requirements, and overall performance issues. With this knowledge, traffic-shaping plans and configurations can be created to provide for a more consistent application performance.

232. Class-Based Weighted Fair Queuing (CBWFQ) extends the standard priority queuing functionality to provide support for user-defined traffic classes. For CBWFQ, traffic classes are defined based on match criteria including protocols, access control lists (ACLs), and input interfaces.

233. Differentiated Service (diffserv) is defined by the IETF. This service provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Service classes are defined for a MTWAN as follows:

SERVICE CLASSES

234. Differentiated Service (diffserv) is defined by the IETF. This service provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Service classes are defined for a MTWAN as follows:

a. Best effort service: This is the current approach with no guarantee of delivery. This service does not need any specialized service from the network;

b. Differentiated service: The essence of this service is that some traffic is treated better than the rest (faster handling, more average bandwidth, lower average loss rate, etc). This is a statistical preference, not a hard and fast guarantee. This is provided by classification of traffic and the use of QoS tools such as PQ, CQ, Weighted Fair Queuing (WFQ), and Weighted Random Early Dropping (WRED). This also provides a definition of Assured Forwarding (AF); and

Uncontrolled copy when printed

c. Guaranteed Service: This service makes an absolute reservation of network resources with low latency and jitter. This service simulates a "leased-line" or legacy private channel. This service requires guaranteed bandwidth and priority delivery. This is provided through QoS tools Resource Reservation Protocol (RSVP) and Class Based Weighted Fair Queuing (CBWFQ). It is typically used for VoIP and video. This also provides a definition of Expedited Forwarding (EF).

235. Each of these groups has an associated per-hop-behavior (PHB) for supporting the service. The PHB is defined for a group or class of traffic that has a DSCP marking.

236. It should be noted that the Differentiated Service is not truly a single guaranteed delivery service, but rather multiple levels of an Assured Forwarding (AF) service for defined traffic classes, where each class has multiple drop precedence levels. The AF service for general use in the internet, defined in RFC 2597 is for four AF classes, each with three levels of drop precedence. The Expedited Forwarding (EF) service supports the Guaranteed Service and is defined in RFC 2598.

Uncontrolled copy when printed

ASSURED FORWARDING SERVICES CLASSES

HIGHER PRIORITY TRAFFIC CLASSES					
HIGHER PROBABLIDLIYT THE PACKETS WILL BE DROPPED		Class 1	Class 2	Class 3	Class 4
	Low Drop Precedence	AF11	AF21	AF31	AF41
	Medium Drop Precedence	AF12	AF22	AF32	AF42
	High Drop Precedence	AF13	AF23	AF33	AF43

Table 2-1 AF Service Classes

237. Class 1 traffic is lower priority than class 2 traffic and so on. The drop precedence means that packets with high drop precedence are more likely to be dropped in router queues than those with low drop precedence. With this order AF41 is the highest priority and AF13 is the lowest priority.

238. Differentiated Services Code Point (DSCP) is a field in the header of IP packets for packet classification purposes in a MTWAN. A higher DSCP value results in better packet treatment during times of network congestion, resulting in lower probability of packets being dropped and less delay.

Uncontrolled copy when printed

Application or Traffic Types	DSCP	Service Class
Routing Overhead	48	CS6
Voice, Video	46	EF
Precedence Marking Group 5		
Reserved for Fires Support	18	AF21
Chat and DNS	20	AF22
GCCS-M NETPREC	22	AF23
Mission Critical Email and Web	22	AF23
Precedence Marking Group 2		
Whiteboard, Web	10	AF11
Email	12	AF13
Precedence Marking Group 1		
Bulk Data (FTP)	14	AF13
Scavenger (Oracle, CST, CaS, TBMCS)	02	AF13
Precedence Marking Group 0		
Default	00	AF13

Table 2-2 Recommended QoS packet markings for a MTWAN

COMPRESSION

239. Compression allows more data to flow through constrained WAN links, freeing bandwidth for the critical applications that need it the most. While control prioritizes mission-critical applications and smoothes bursty traffic, compression enhances performance by creating greater throughput, faster performance, and increased network capacity.

TYPES OF COMPRESSION

240. There are several common types of compression:

a. File – addressed by Information Management practices;

b. Application; and

c. Network.

PAIR WISE CONFIGURATION

241. Application and network compression requires at least two compression devices, one deployed at each end of a connection. Each device compresses its outbound traffic, and each unit at the receiving end will decompress inbound traffic, restoring traffic to its original state.

242. Previously compressed traffic (such as VoIP and streaming video) and encrypted data (such as HTTPS, SSH and encrypted Domino databases) can not be compressed further.

Uncontrolled copy when printed

Binary files, and non-repeating data, do not fare as well as Web and text files, which are more compressible.

QOS SOLUTIONS

243. Today there are a plethora of vendors who offer end-to-end solution packages. These hardware devices called WAN accelerators or optimizers, compress and cache data, modify TCP parameters and enforce QoS (quality of service) using prioritization and rate shaping.

244. While some vendors claim their devices increase network performance tenfold, independent tests have typically demonstrated a fourfold improvement in throughput performance. Protocol prioritization and rate limiting QoS mechanism vice Differentiated Services (DiffServ) or Integrated Services (IntServ) technologies are typically employed.

245. Such solutions are attractive due to the fact that they are relatively simple to deploy and maintain. With the devices strategically positioned they can monitor and visualize the network. Once the traffic flow is understood then QoS mechanisms can be introduced to control optimize the flow, and if the infrastructure provides pair-wise configuration, then compression can also be applied.

INTEROPERABILITY

246. While most / all vendors implement industry standards, there is no interoperability between vendor solutions.

PASS THROUGH FAILOVER

247. It is desirable that any solution has pass through failover. That is if any hardware device is unplugged, traffic will nonetheless pass through the device as if it were part of the wire.

NETWORK TOPOLOGY

248. The hardware device should be able to be deployed in a hub-and-spoke or mesh topology. Those devices that require you to create links manually, however, are difficult to configure in a mesh environment.

FUTURE WORK

249. AUSCANNZUKUS nations are actively exploring QoS packages which should lead to a better understanding of QoS and vendors solutions. The information gleaned will be used to further develop this chapter in subsequent changes.

250. QoS approaches that can be implemented at the router (vice through WAN accelerators / optimizers) need also to be agreed.

Uncontrolled copy when printed

MAPPING IER TO QOS

251. An outstanding issue that remains is how to map the war fighters' Information Exchange Requirements (IERs) into QoS outcomes while maintaining transparency to Command. There is significant work being done in this field which will be reflected in the next change to this document.

IPV6

252. The development of IPv6 will enhance our ability to perform QoS and manipulate packet flows. Until 2003, all routers were packet routers that only examined the packet and kept no flow history. The duration, rate or byte count of the flow could not be determined. Flow State Aware (FSA) routing such as Multi Protocol Label Switching (MPLS) can determine the duration, rate or byte count of the flow. It can identify flow types and control the rate and delay per flow.

CONCLUSION

253. Link throughput, vice bandwidth is the most important consideration when addressing IP connection speeds. QoS mechanisms can significantly enhance throughput and improve transmissions, without requiring extra bandwidth.

254. In order to effectively and efficiently implement QoS, it is important to understand what is occurring in the network (i.e. visibility). Once this is understood, QoS control and compression can be implemented. The overall goal, however, should not be to squeeze improvement out of MTWANs, if it adds undue complexity to training and operations.

Uncontrolled copy when printed

CHAPTER 3

NETWORK MANAGEMENT

INTRODUCTION

301. Network Management is the process of controlling a data network to maximise its efficiency and productivity. It is therefore a critical aspect for any wide area network.

AIM

302. This chapter provides guidance for the Network Management of a maritime tactical WAN.

OVERVIEW

303. Network Management (NM), which includes configuration, performance, fault and security management, takes place within nodes (i.e. LAN) and throughout the wider network (i.e. WAN).

304. From a WAN perspective, NM is commonly associated with the duties and responsibilities of a Network Operations Centre (NOC). A NOC while logically in one location could physically be in a number of locations (i.e. distributive in nature).

305. Depending on the design of the MTWAN, there will be a number of NOCs. There will normally be three types of NOCs: Primary NOC, National NOC, and Node.

NETWORK MANAGEMENT ARCHITECTURE (HIERARCHY)

PRIMARY NOC

306. The MTWAN NOC or Primary NOC provides a single point of contact for network services within a maritime tactical network. The provision of services to this network and for coordinating connectivity of national NOCs to the network is a MTWAN NOC responsibility.

NATIONAL NOC

307. The National NOCs are responsible for coordinating network services within their national boundaries and to coordinate activities with the primary NOC.

NODE LEVEL

308. Individual nodes are responsible for management of local network elements. Each platform will have a limited capability to provide network management services on the LAN and is responsible first to the national NOC and then the primary NOC for overall network services.

Uncontrolled copy when printed

NETWORK MANAGEMENT ELEMENTS

309. The elements of network management are:

a. Configuration Management that controls the behaviour of the network and can be considered to comprise;

b. Configuration, monitoring and control of routers, other SNMP-managed network devices, and CAP/CRIU;

c. Provisioning, bandwidth management, and monitoring;

d. Route Policy Management (which networks carry transit traffic, diversity routing, tunnelling and overlay network management, security service levels for routing protocols, etc.); and

e. Management of DNS, network time service, and other required infrastructure services.

PERFORMANCE MANAGEMENT

310. Performance Management measures the performance of the network hardware, software, and media. It comprises:

a. Monitoring of Links, Routers, network connectivity and Services;

b. Net loading, congestion control monitoring;

c. Performance optimisation for bandwidth-disadvantaged users;

d. Service Prioritisation;

e. Fault Management.

f. Fault detection, isolation and troubleshooting;

g. Fault-logging and analysis.

SECURITY MANAGEMENT

311. Security Management control access to information on the network, and can be considered to comprise:

a. Intrusion detection and response, including co-ordination of multiple detections received from diverse locations;

b. Vulnerability assessment;

Uncontrolled copy when printed

c. Security Policy Establishment, Monitoring, & Enforcement;

d. Firewall Management;

e. Response Centre activities (route attack notifications to CERTs, co-ordinate fixes);

f. Guard Management ("Guards" = devices connecting 2 or more networks running under different security policies and/or sensitivities, e.g., a guard which connects the US National networks with the MTWAN);

g. Encryption Device Management (e.g. TACLANE/FASTLANE Management); and

h. Administration which comprise the generation of reports, pertaining to:

i. Robust Network Management under varying operational conditions (i.e., EMCON);

j. DNS Co-ordination;

k. Interface with other non-MTWAN network management entities (e.g., national NOCs and their network management systems); and

l. Provisioning requests up to national NOCs; responses down to MTWAN NOC;

m. Critical fault alerts/alarms sent up to national NOCs; and

n. Configuration and performance summary status/statistics sent up to national NOCs.

Uncontrolled copy when printed

REMOTE OR LOCAL MANAGEMENT

312. Centralised, remote management of the MTWAN elements by a NOC will be more efficient than co-ordinated local control. Remote management reduces the need for additional skilled staff on each mobile unit, minimises the risk of errors in configuration, and permits rapid reaction to events. However, the capability for remote management is limited at present by national policy.

313. National policies may prohibit remote control of network elements for safety or system integrity reasons. Monitoring may be acceptable, if specific equipment items can be configured to respond to remote requests for status information but ignore control messages. Network management procedures and protocols must be secure.

GENERATION OF REPORTS

314. An MTWAN NOC will provide network status information to the CTF, to network members and to the higher level Allied WAN management system. This information must be kept current and will be presented as a Web page. To enable an MTWAN NOC to collect and collate the latest status information, all platform network managers are to provide local status reports on a regular basis (or at least, when there has been any change since the last report). The NOC will compile these into an overall status report.

SECURITY RESPONSIBILITY

315. The MTWAN NOC should provide a capability for intrusion detection, primarily to minimise unauthorised traffic over the MTWAN.

TOOLS

316. Several tools are available to facilitate network status and traffic load monitoring, as well as tools using SNMP to implement centralized or remote control of network elements. All platforms should, as a minimum, have the ability to monitor local network status and traffic performance.

Uncontrolled copy when printed

NETWORK MANAGEMENT SOP

INTRODUCTION

1. The management of an MTWAN involves monitoring the operation of application servers (e.g. Domino, Sametime and mail servers), network servers (e.g. DNS and multicast transport protocols), network devices (e.g. routers) and cryptographic equipment. Network Management (NM) also includes the collection and analysis of network statistics to assist with troubleshooting of network or application problems, network optimisation and future planning.

AIM

2. The aim of this Annex is to provide the standard operating procedures for managing an MTWAN Network.

SCOPE

3. NM services to be supported within a typical MTWAN will be limited to:

a. Gathering LAN and WAN traffic statistics to support future planning and network optimisation;

b. Monitoring the health of network devices and application servers;

c. Monitoring the operation of network services and C2 applications;

d. Identifying network changes; and

e. Troubleshooting network and application problems.

NETWORK MANAGEMENT TOOLS

4. Simple Network Management Protocol (SNMP), an Internet Protocol, is the principal means employed to conduct NM. SNMP defines a set of parameters that a network manager can query (Management Information Base), the format of NM messages and the rules by which these messages are exchanged. *Openview* and *Network Node Manager* from *HP*, *Tivoli Netview* from *IBM*, *Spectrum* from *Aprisma* and *WhatsUpGold* from *Ipswitch* are common commercial tools that have been successfully employed in MTWANs. These tools have different capabilities, and user interfaces. Selection and installation of NM tools will be a national issue.

Uncontrolled copy when printed

NETWORK MANAGEMENT STRATEGY

5. A MTWAN NOC should be operated on a 24/7 basis. The network manager will be responsible for the following:

a. Configuration of routers, servers and user workstations;

b. Installation of NM station;

c. Installation of applications and network services;

d. Configuration of WAN links including CAP/CRIU, radio

e. Configuration of cryptographic equipment;

f. Configuration of applications and network in support of EMCON; and

g. Collection of local network statistics.

6. Network statistics will normally include protocol distribution; packet and byte counts sorted by protocol or by host, connection matrices, and error counts on different protocol layers.

7. Unit network managers must ensure that network devices, application servers, clients, and WAN interfaces on the local network have been correctly configured and remain functional.

8. NM stations will be capable of processing SNMP traps (unsolicited messages sent by an SNMP-enabled host indicating it is not fully operational) received from local hosts. The NM stations are to be configured to automatically generate audible alarms and notification messages whenever a trap is received.

9. The MTWAN NOC will manage AS Border Routers, network services (such as DNS, mail server, and multicast transport applications) and application servers (such as Domino and Sametime) for the MNTG.

10. Performance of the local network and its hosts must be continuously monitored. An automatic alert will be generated when warning or critical threshold limits for the network (such as error rates) or computing resources (such as memory and disk space) have been reached (or are being approached).

11. Under the direction or co-ordination of the MTWAN NOC, unit network managers will assist with the analysis and resolution of network and application problems as required.

12. Network bottlenecks are most likely to occur on low speed RF links and therefore NM traffic over these links must be kept to a minimum. A unit NM station shall only discover and manage hosts on its local network. No traffic generated by the local automated NM processes (such as network discovery) must be allowed to travel further than the unit's Area Border router.

Uncontrolled copy when printed

13. The NOC will monitor and provide a consolidated view of the health of the network backbone (Area 0). The view will also include the status of MNTG application servers. The view will be updated at least every 30 minutes and be accessible to units network managers via a Web browser.

14. Under the direction or co-ordination of the NOC, units network managers will conduct the analysis of network statistics to identify potential problems, and to anticipate and plan for additional hosts and services.

15. An FTP server may be provided at the NOC to support the collection and storage of software and configuration information for all configurable network devices and services within the MTWAN in support of a specific exercise or operation.

NETWORK MANAGEMENT TOOLS SET –UP

16. To establish NM tools discussed above, the following installation and set-up is required:

a. Set up an engineering order wire to enable network management coordination;

b. Select a suitable computer to be the NM station and install NM software. If the computer is being used for other applications, ensure that these will not be affected by the NM functionality;

c. Set up a Web server on the NM station to let users view the NM information using a Web browser. Enable Web server security to grant users “read-only” access to the Web pages;

d. Enable SNMP on all hosts and set their “read-only” Community Name (editing SNMP Agent’s Management Information Base {MIB} is not allowed);

e. Use the “Lookup” tool provided by the NM software to resolve IP addresses and names (forward and reverse mapping) of the local hosts using DNS. Rectify any DNS problems encountered;

f. Enable the Network Mapping function of the NM to discover the local network up to the local Area Border routers and generate a topology map. The map will include all the active interfaces of the routers. Set the default polling interval for the network discovery and monitoring to 30 minutes. For routers and servers, which are critical components of the network, the polling interval should be set to no longer than 10 minutes;

Uncontrolled copy when printed

g. Enable the monitoring function of the NM software to monitor the status of local hosts, the services running on those hosts and the WAN links. Colours and symbols will be used to indicate any changes to the network; and

h. Enable the collection of local network statistics.

TROUBLESHOOTING

17. The most common problems that occur in an operational IP network are:

a. Slow Responses;

b. Connectivity Problems; and

c. Application Problem.

SLOW RESPONSIVENESS

18. When an application is running slowly, the cause of the problem may be a congested network or an overloaded server.

19. Use NM tools to collect and analyse network statistics to determine whether the network is congested. If it is, identify hosts and applications that are causing the congestion and then co-ordinate with the NOC to shut down non-essential bandwidth users.

20. Request the network manager of the remote server to determine whether the server has too many clients and therefore it is overloaded, and then contact the NOC for problem resolution.

CONNECTIVITY PROBLEM

21. When connection to a remote server cannot be established, the problem may be caused by one of the following: DNS; unreachable host; or routing.

22. Use the Lookup tool to verify name & address resolutions and resolve any DNS problems.

23. Use Ping command to verify that the remote host is reachable.

24. If the remote host is unreachable, verify with the remote network manager that the remote host is operational.

25. If the remote host is operational, use the ‘TraceRoute’ command to locate any routing problems and inform the NOC of the problems.

Uncontrolled copy when printed

APPLICATION PROBLEM

26. The most likely causes of application problems are:

a. Remote server hardware is faulty;

b. Remote server software is badly configured; and/or

c. Local client software is badly configured.

27. Verify with the NOC that the remote server is operational and the local software configuration is correct. In coordination with the NOC resolve any configuration problems.

Uncontrolled copy when printed

NETWORK CONFIGURATION PLAN (NCP)

INTRODUCTION

1. The management of the MTWAN requires that the network be designed and documented to allow nations to efficiently and effectively configure their respective components of the AMTWAN. In the Coalition maritime environment there are two documents that are used to promulgate the required network configuration information to participating nations: the Network Configuration Plan (NCP) and, if required, the OPTASK Net message.

AIM

2. The aim of this annex is to amplify the NCP and OPTASK NET and provide an example of its content. The format for the creation of the NCP is included at Appendix 1 to this Annex. The OPTASK NET is a free text formal military message.

RESPONSIBILITY

3. High-level network configuration information will normally be provided in the NCP. The NCP is normally developed by the CCTF and may be published as an Appendix to the OPLAN or issued as a separate document if required.

4. Using this higher level guidance, the local Commander may detail specific tactical level requirements in the OPTASK NET. The creation of these documents requires close liaison with participating nations and their Network Operating Centers (NOCs) in order to achieve an accurate final document.

CLASSIFICATION

5. Where possible, the NCP should be kept at the UNCLASSIFIED level until such time as the document is populated and becomes approved for use. This will allow rapid collaboration with nations for its creation.

6. In its final format, the NCP should be classified as appropriate for the Operation or Exercise, with the appropriate releasability caveats.

FORMAT

7. Due to the nature of the contents of the NCP, it does not lend itself to the Maritime Tactical Format (MTF). During the collaboration phase with participating nations, the preferred format is a MS Word document format. The preferred final format is the Portable Document Format (PDF) file format.

Uncontrolled copy when printed

CLASSIFICATION

Command, Network, or Group

Title Page

Operation, Exercise or Experiment Name

Network Configuration Plan (NCP)

Version 1.00

Day, Month, Year

CLASSIFICATION

Uncontrolled copy when printed

This Network Configuration Plan based on the ACP 200 and developed under the direction of (Command or Group responsible for the Plan).

List Authors/Contributors by Nation or Function

Uncontrolled copy when printed

Prepared by:

RECORD OF CHANGES

Version Number	Date	Sections Updated	Comments

Uncontrolled copy when printed

TABLE OF CONTENTS
NETWORK CONFIGURATION PLAN (NCP)

A. OBJECTIVE.
B. ADMINISTRATION.
B1. PERIOD.
B2. SCOPE.
B3. CHANGE MANAGEMENT.
B4. REFERENCES.
C. DUTIES AND CONTACT INFORMATION
C1. COALITION TECHNICAL COORDINATOR
C2. MTWAN NETWORK MANAGERS
C3. NATIONAL NOC TROUBLE/HELP DESKS.
C4. UNIT/SITE NETWORK MANAGERS.
C5. APPLICATIONS AND TECHNOLOGIES POCS.
D. SUBNETS
D1. SATCOM, TERRESTRIAL AND LOS/ELOS SUBNETS
D2. HF IP (STANAG 5066 EDITION 2) CONFIGURATION PARAMETERS
D3. SUBNET RELAY MODEM AND SCRN NETWORK CONTROLLER PARAMETERS
E. ROUTING
E1. MTWAN NETWORK ROUTING TOPOLOGY
E1.2 MULTI-TOPOLOGY ROUTING.
E2. AS NUMBERS.
E3. OSPF PARAMETERS.
E4. LOCAL AREA NETWORKS
E4.1 LAN SUBNETS
E4.2 LAN HOST IP ADDRESSING TEMPLATE
E4.3 LINE OF SIGHT BEARERS
E4.3.1 SNR UHF IP ADDRESSING AND OSPF COST
E4.3.2 HF IP ADDRESSING AND OSPF COST
E4.4 SATCOM IP ADDRESSING
E4.5 GRE TUNNEL ADDRESSES AND COSTS
E4.6 LANDLINE WAN BEARERS IP ADDRESSING
E4.7 COI CONNECTIONS IP ADDRESSING
F. NAMING AND ADDRESSING
F1 DNS NAMING FORMAT FOR EXER/OPER
F2 DNS ROOT SERVERS
F2.1 DNS OVERVIEW
F2.3 DNS NAMESPACES FOR EXER/OPER
F3. HOST NAMES
F4. DNS DOMAIN RESPONSIBILITIES
F5. HOST NAMES AND IP ADDRESSES
G. APPLICATIONS
G1. MESSAGING
G1.1 MS-EXCHANGE MAIL SERVER
G1.2 IBM-LOTUS DOMINO WEB MAIL AND SECURE WEB MAIL SERVER

Uncontrolled copy when printed

G2. COMMON OPERATIONAL PICTURE (COP)
G2.1 COALITION COP ARCHITECTURE
G2.2 GCCS-M AND C2PC INFORMATION
G3. WEB SERVICES
G3.1 WEB BROWSER INFORMATION
G3.1.1 MINIMUM INTERNET EXPLORER VERSION
G3.1.2 JAVA VERSION
G3.2 LOTUS DOMINO CONFIGURATION
G3.2.1 LOTUS DOMINO VERSION
G3.2.2 DOMINO SERVER NAMING SCHEMA AND CONFIGURATION FOR EXER/OPER
G3.2.3 DOMINO ADMINISTRATION
G3.2.4.1 GROUP OR ROLE-BASED ACCOUNTS
G3.2.4.2 USER, OR PERSON-BASED, ACCOUNTS
G3.2.4.3 ESSENTIAL EXER/OPER DOMINO ACCOUNTS
G3.2.5 DOMINO REPLICATION TOPOLOGY
G3.2.6 DOMINO CONNECTION DOCUMENTS
G3.2.6.1 DOMINO WEB CONNECTION DOCUMENTS
G3.2.6.2 SAMETIME CONNECTION DOCUMENTS
G3.2.6.3 MAIL CONNECTION DOCUMENTS
G3.2.7 REPLICATION SCHEDULES
G3.2.8 DOMINO ADDRESS BOOK
G3.2.9 ROOT ADMINISTRATIVE SERVER
G4. DISTRIBUTED COLLABORATIVE PLANNING
G4.1 LOTUS SAMETIME
G4.1.1 SAMETIME VERSION
G4.1.2 SAMETIME CONFIGURATION
G4.1.3 SAMETIME AUDIO AND VIDEO
G4.2 INSTANT PERSISENT WAR ROOM (IPWAR)
G4.3 EXER/OPER SAMETIME AND IPWAR TOPOLOGY
G5. JPEG 2000 INTERACTIVE PROTOCOL (JPIP)
G5.1 KAKADU JPIP SERVER
G5.1.1 KAKADU SERVER INSTALLATION
G5.1.2 KAKADU JPIP SERVER CONFIGURATION PARAMETERS
G5.2.1 KAKADU CLIENT INSTALLATION
G5.2.2 JPIP IMAGE BROWSING
G5.3 IDELIX JPIP SERVER (CANADA)
G5.4 IDELIX JPIP CLIENT
G6. WEBSURVEYOR
G7. MINIMUM EXER/OPER CLIENT SOFTWARE BASELINE
H. NETWORK MANAGEMENT
H1. NETWORK MANAGEMENT INFORMATION
H2. NETWORK MANAGEMENT POC
H3. NTP ARCHITECTURE

Uncontrolled copy when printed

TABLES AND FIGURES

TABLE C-1: TECHNICAL POINTS OF CONTACT INFORMATION
TABLE D2-1: HF IP CONFIGURATION PARAMETERS
TABLE D3-1: MTWAN SNR NETWORK CONTROLLER PARAMETERS
FIGURE E1-1: MWTAN ROUTING TOPOLOGY
TABLE E1.2-1: SHIP-TO-SHIP BEARER PREFERENCE BASED ON TRAFFIC CLASS
FIGURE E1.2-1: EXER/OPER MTR WEIGHTS
TABLE E1.2-3: MULTI-TOPOLOGY ROUTING CLASSIFICATION, PRIORITIES AND WEIGHTS
TABLE E3-1: OSPF SETTINGS
TABLE E4.1-1: LAN SUBNET IP ADDRESSING
TABLE E4.2-1: RECOMMENDED MTWAN IP ADDRESSING TEMPLATE
TABLE E4.3.1-1: SNR IP ADDRESSING
TABLE E4.4-1: SATCOM IP ADDRESSING
TABLE E4.5-1: NOC TO NATIONAL NOC & NOC TO SHIP GRE TUNNEL INFORMATION
TABLE E4.6-1: LANDLINE WAN BEARERS IP ADDRESSING
TABLE E4.7-1: GCTF CONNECTIONS IP ADDRESSING
FIGURE F1.1-1: DOMAIN NAME SCHEMA
TABLE F1.3-1: EXAMPLE SITE NAMES, ABBREVIATIONS AND FULLY QUALIFIED DOMAIN NAMES
TABLE F2-1: HOST NAMES/ALIASES
FIGURE F4-1: NETMASK TRANSLATION TABLE
FIGURE F4.1-1: EXER/OPER AUNOC
FIGURE F4.1-2: EXER/OPER AUS SHIP 1
FIGURE F4.1-3: EXER/OPER AUS SHIP 2
TABLE F4.1-1: AUSTRALIA MTWAN WAN/LAN IP ADDRESS ALLOCATION
FIGURE F4.2-1: EXER/OPER MTWAN
FIGURE F4.2-2: EXER/OPER HMC SHIPS MTWAN CONFIGURATION
FIGURE 4.3-1: TW 06 UK NOC EXER/OPER MTWAN CONNECTIVITY
FIGURE 4.3-2: TW 06 UK SHIP 1 EXER/OPER MTWAN CONNECTIVITY
TABLE F4.3-1: UNITED KINGDOM MTWAN WAN/LAN IP ADDRESS ALLOCATION
TABLE F4.3-2: UNITED KINGDOM TACLANE SUB-NETWORK IP ADDRESS ALLOCATION
FIGURE 4.4-1: EXER/OPER US SHIP 2 MTWAN CONFIGURATION
FIGURE 4.4-2: EXER/OPER US SHIP 3 MTWAN CONFIGURATION
FIGURE 4.4-3: EXER/OPER US SHIP 1 MTWAN CONFIGURATION
FIGURE 4.4-4: EXER/OPER CFMCC (COMPACFLT) MTWAN CONFIGURATION
FIGURE 4.4-5: EXER/OPER PRNOC MTWAN CONFIGURATION
TABLE F4.4-1: UNITED STATES MTWAN WAN/LAN IP ADDRESS ALLOCATION
TABLE F4.4-2: UNITED STATES SNR IP ADDRESS ALLOCATION
TABLE F4.4-3: UNITED STATES TACLANE SUB-NETWORK IP ADDRESS ALLOCATION
FIGURE G2.1-1: EXER/OPER COALITION COP DISTRIBUTION ARCHITECTURE
TABLE G2.2-1: GCCS-M AND C2PC INFORMATION

Uncontrolled copy when printed

TABLE G3.2.2-1: EXER/OPER UNIT, DOMINO DOMAIN AND FULLY QUALIFIED DOMAIN NAMES
TABLE G3.2.4.3-1: ESSENTIAL DOMINO ACCOUNTS FOR EXER/OPER
FIGURE G3.2.5-1: EXER/OPER MTWAN DOMINO REPLICATION TOPOLOGY
FIGURE G4.3-1: EXER/OPER IPWAR SERVER HIERARCHY
FIGURE G4.3-2: EXER/OPER IPWAR MULTIPLE SAMETIME SERVER ARCHITECTURE
TABLE G5-1: JPIP SERVERS AND PLATFORMS
TABLE G5.1.2-1: KAKADU VER. 4.5 SERVER PARAMETERS
TABLE G7-1: EXER/OPER MINIMUM CLIENT SOFTWARE BASELINE

Uncontrolled copy when printed

EXAMPLE NETWORK CONFIGURATION PLAN

A. OBJECTIVE.

This Network Configuration Plan (NCP) provides maritime and shore units the capability to configure and maintain access to the Maritime Tactical Wide Area Network (MTWAN).

B. ADMINISTRATION.

This NCP may be supplemented by local commanders by use of an OPTASK NET.

When completing this document:

replace the term “MWTAN” with the name of the actual network throughout the document, and

replace the term “COI” with the approved four letter designator for the Community of Interest in question.

B1. PERIOD.

Effective for planning purposes from receipt and for use from execution of the operation or exercise. Cancel upon completion of the operation or exercise; or when superseded by a new NCP.

B2. SCOPE.

This NCP provides the technical and engineering information required for the provisioning of the MTWAN, including the setup, configuration, operation, maintenance and management.

B3. CHANGE MANAGEMENT.

The Engineering Lead and National Technical Leads must agree upon any changes to this NCP.

B4. REFERENCES.

B4.1 ACP 200(C) Maritime Tactical Networking at Sea

B4.2 OPTASK COMMS

B4.3 OPTASK IM

B4.4 OPTASK FOTC

B4.5 INFORMATION MANAGEMENT Plan (IMP)

Uncontrolled copy when printed

C. DUTIES AND CONTACT INFORMATION

C1. COALITION TECHNICAL COORDINATOR

The Coalition Technical Coordinator is responsible for coordinating all of the technical aspects of Coalition activities to ensure that the network infrastructure and applications are well integrated and in good working order to maximize operator and technical assessments during Operation or Exercise.

C2. MTWAN NETWORK MANAGERS

The MTWAN network managers are responsible for maintaining the network in good working order. There shall be a Primary and Alternate Points of Contact for each nation. The national network managers are responsible for their portion of network maintenance. This includes establishment, monitoring and reporting of network performance and customer service support. Each national network manager is also responsible to the Coalition Technical Coordinator for the provision of all IP addresses, DNS and other pertinent network information for those national units requiring them. Changes to the MTWAN network should be agreed upon by all nations, but the Primary Network Manager will have final configuration authority for the MTWAN. The network managers must also ensure the collection and publication of the following information at 1200Z daily:

All network status

Overall performance

Network troubles if any

Planned network outage if any

Other Miscellaneous Information

C3. NATIONAL NOC TROUBLE/HELP DESKS.

Nations shall supply contact information for NOC Trouble or Help Desks in order to provide customer service support.

C4. UNIT/SITE NETWORK MANAGERS.

Nations shall specify primary and alternate POC information for unit and site managers. The unit or site network manager is responsible to his/her Commanding Officer for the maintenance and proper functioning of their local network and associated connectivity. The unit/site network manager is also responsible to the MTWAN for configuration and reporting of network status and any deficiencies.

C5. APPLICATIONS AND TECHNOLOGIES POCS.

Services not normally supported by NOC services shall specify a Primary and Alternate POC to assist in troubleshooting and training of MTWAN personnel.

Uncontrolled copy when printed

Table C-1: Technical Points of Contact Information

Principal MTWAN POCs	Name	Site Phone Number	Mobile Phone Number	Office Phone Number	Unclassified Email Address(es)	MTWAN Email Address
Coalition Technical Coordinator						
MTWANNation 1 Primary Network Manager & NOC						
MTWANNation 1 Alternate Network Manager						
Nation 2 Primary Network Manager & NOC						
Nation 2Alternate Network Manager & NOC						
Nation 3 Primary Network Manager						
Nation 3Alternate Network Manager						
Nation 4 Primary Network Manager						
Nation 4 Alternate Network Manager						
Nation 5 Primary Network Manager						
Nation 5 Alternate Network Manager						

Uncontrolled copy when printed

Table C-1: Technical Points of Contact Information (Con't)

National Help Desks	Name	Site Phone Number	Mobile Phone Number	Office Phone Number	Unclassified Email Address(es)	MTWAN Email Address
Nation 1 MTWANHelp Desk						
MTWANNation 2 Help Desk						
MTWANNation 3 Help Desk						
MTWANNation 4 Help Desk						
Nation 5 Help Desk						
Nation 1 Maritime Units POC						
Ship 1 Primary POC						
Ship 1 Alternate POC						
Ship 2 Primary POC						
Ship 2 Alternate POC						
NOC Primary POC						
NOC Alternate POC						
Nation 2 Maritime Units POC						
Ship 1 Primary POC						
Ship 1 Alternate POC						
Ship 2 Primary POC						
Ship 2 Alternate POC						
NOC Primary POC						
NOC Alternate POC						

Uncontrolled copy when printed

Table C-1: Technical Points of Contact Information (Con't)

Nation 3 Maritime Units POC						
Ship 1 Primary POC						
Ship 1 Alternate POC						
Ship 2 Primary POC						
Ship 2 Alternate POC						
NOC Primary POC						
NOC Alternate POC						
Nation 4 Maritime Units POC						
Ship 1 Primary POC						
Ship 1 Alternate POC						
Ship 2 Primary POC						
Ship 2 Alternate POC						
NOC Primary POC						
NOC Alternate POC						
Nation 5 Maritime Units POC						
Ship 1 Primary POC						
Ship 1 Alternate POC						
Ship 2 Primary POC						
Ship 2 Alternate POC						
NOC Primary POC						
NOC Alternate POC						

Uncontrolled copy when printed

Table C-1: Technical Points of Contact Information (Con't)

National Account Approval Authorities	Name	Site Phone Number	Mobile Phone Number	Office Phone Number	Unclassified Email Address(es)	MTWAN Email Address
Nation 1 Primary National Approval Authority						
Nation 1 Secondary National Approval Authority						
Nation 2 Primary National Approval Authority						
Nation 2 Secondary National Approval Authority						
Nation 3 Primary National Approval Authority						
Nation 3 Secondary National Approval Authority						
Nation 4 Primary National Approval Authority						
Nation 4 Secondary National Approval Authority						
Nation 5 Primary National Approval Authority						
Nation 5 Secondary National Approval Authority						

Uncontrolled copy when printed

D. SUBNETS

D1. SATCOM, TERRESTRIAL AND LOS/ELOS SUBNETS

Coalition units in the Operation or Exercise will make use of traditional SATCOM (SHF, INMARSAT) subnets, LOS/ELOS subnets and terrestrial subnets. Table D1 - 1 delineates the bandwidth available on each of the various bearers on each unit. Each column represents the maximum aggregate bandwidth available for each subnet/bearer, which may contain other, non-coalition IP traffic and may be shared between multiple platforms. This table consolidates much of the information contained in ACP 200(C) NCP D1, D2, D3, D4 and D5.

Table D1-1: Available Bandwidth per bearer per Unit

Unit	SHF BW (kbps)	INMARSAT BW (kbps)	SNR BW Shared (kbps)	HF IP BW Shared (kbps)	Simulated SATCOM BW (kbps)	Landline or Pierside BW (kbps)
Nation 1						
Ship 1						
Ship 2						
Nation 2						
Ship 1						
Ship 2						
Nation 3						
Ship 1						
Ship 2						
Nation 4						
Ship 1						
Ship 2						
Nation 5						
Ship 1						
Ship 2						

Uncontrolled copy when printed

D2. HF IP (STANAG 5066 EDITION 2) CONFIGURATION PARAMETERS

Table D2-1 delineates the configuration parameters to be used for HF IP. Note that the HF IP software, version 3.0, incorporates "dynamic tap0 addressing," which is a "DHCP like" functionality for the serial interfaces of the HF IP controllers. The system managers of the HF IP controllers automatically negotiate specific IP addresses within a subnet and as limited by the netmask for their respective WAN tap0 addresses upon joining the token ring. The HF IP boxes will be configured for the x.y.192.0 subnet and /29 netmask. Individual IP addresses will be assigned and changed automatically as the nodes join and leave the HF network.

Table D2-1: HF IP Configuration Parameters

Number of Units in HF IP Subnet	3
Aggregate Bandwidth	19200 bps
STANAG 5066 Address Range	xxx.yyy.192.0/29
Nation 1 Shipname 5066 Address	xxx.yyy.192.z/29
Nation 1 Shipname 5066 Address	xxx.yyy.192.z/29
Nation 1 Shipname 5066 Address	xxx.yyy.192.z/29
Nation 2 Shipname 5066 Address	xxx.yyy.192.z/29
Nation 2 Shipname 5066 Address	xxx.yyy.192.z/29
HF IP Router IP Address/Mask	See Section E4.3
Nation 3 Shipname IP Address/Mask	See Section E4.3
Nation 3 Shipname IP Address/Mask	See Section E4.3
Nation 3 Shipname IP Address/Mask	See Section E4.3
Nation 4 ShipnameShip 1 IP Address/Mask	See Section E4.3
Nation 4 Shipname IP Address/Mask	See Section E4.3
Sideband (US)	ISB Note: SHIPNAME will use 2 HF radios, one for upper and one for lower sideband to achieve ISB
Sideband (AU)	ISB
Modem Mode	MIL-STD-110B Appendix F
Baud Rate	12800 bps
Interleave Mode	Very Short
Transmit Frequencies	Refer to OPTASK COMMS
Unique Crypto Settings	SYNC, EXT CLKS, FDX IND, OP2, AUTO

D3. SUBNET RELAY MODEM AND SCRN NETWORK CONTROLLER PARAMETERS

Table D3-1 contains the SNR Controller parameter settings to be used in the MTWAN.

Table D3-2 contains the SNR Modem settings and parameters to be used in MTWAN.

Uncontrolled copy when printed

Table D3–1: MTWAN SNR Network Controller Parameters

SCRN Settings	
Nation 1 SNR Controller Software Version	SCRN ver. 2.09
Nation 2 SNR Controller Software Version	SCRN ver. 2.08
Nation 3 SNR Controller Software Version	SCRN ver. 2.09
Nation 4 SNR Controller Software Version	SCRN ver. 2.09
Nation 5 SNR Controller Software Version	SCRN ver. 2.09
Data Rate	64000 bps
Crypto Type	Other
Crypto Synch Bytes	192
Crypto Pre-Pad	0
Crypto Post-Pad	0
Min. data Hold Off	500
Radio Overhead	40
Modem Interleaver	25
Modem Overhead	40
Slot Guard Time	40
Transmit Delay	110
Receive Delay	140
Tx Delay Opt	110
Slot Overlap	140
Slot Length	380
Slot Overhead Ratio	67.3
Quantization Error	0
Time Source	*As implemented*
Compression	Enabled
Compression Level	1
Slot Allocation	Deterministic
Tx Que TTL	120
Number RA slots	2
Number slots per cycle	32
Neighbor Sense	3 of 5
IPTM	Enabled
Slot Merging	Enabled
Max merged slots	4

Table D3–2: MTWAN SNR MODEM Parameters

SNR UHF Modem Settings	
Nation 1 SNR modem software version	IPDT-2000 Ver 8.01
Nation 2 SNR modem software version	
Nation 3SNR modem software	Comm. ISA 2004/12/14

Uncontrolled copy when printed

version	
Nation 4 SNR modem software version	
Nation 5 SNR modem software version	
Transmit Rate	64000
Tx Interleaver Length	Very short (25 ms)
Tx Constellation Setting	Normal
Rx Autobaud	Full
Loop Mode	No Loopback
Data Interface	Synchronous
Data Invert	Normal
Preamble Length	2
Duplex	Half
Frequency Tracking	Enable
Data Source	External
Optional EOM	On
Max Message Duration	0
Dropout Time	Fast
Min ALC setup time	0.00
Power level	0.0
Key line hang time	0
DTR Behavior	Ignore
DCD Behavior	VDP
Sync Tx Clock	Internal
COTS Async Mode	Disable
ADC Gain	Normal
BER Test (audio loopback)	1000
Config applies to	All modes

*Note: All ships must be using same parameters.

Uncontrolled copy when printed

E. ROUTING

E1. MTWAN NETWORK ROUTING TOPOLOGY

An all OSPF Area 0 routing topology will be used for this Operation / Exercise on the MTWAN and was designed to minimize routing loops and simplify configuration, especially for SNR and HF IP participants. The routing topology on each ship/site will have all possible subnets using the OSPF routing protocol residing in Area 0. OSPF Multi-Topology Routing (MTR) costs will be applied on interfaces to select the optimal path to a destination. OSPF and MTR cost metrics can be found in Tables E1.2-3 and E3-1.

The MTWAN router will exchange OSPF route advertisements with other coalition ships' routers over the SNR and HF IP subnets. It also requires that routing advertisements be exchanged over SATCOM subnets with the MTWAN national NOC routers. Since the TACLANE does not allow the exchange of routing protocols, a GRE tunnel will be established between the ship router and the NOC router. The tunnel will allow the OSPF routing protocol packets to go through the TACLANE, thus enabling routing advertisement between ship and shore. The router will only advertise the MTWAN sub-network onboard the ship and the routes it learned from its OSPF neighbors. Route summarization at the NOC from shore to ship will reduce Link State Advertisements and recalculations over SATCOM, SNR and HF IP to further minimize routing overhead.

Figure E1-1 illustrates the overall MTWAN Routing Topology, including the VPN tunnels and the GRE tunnels.

OSPF-based Multi-Topology Routing will maximize the simultaneous use of all available subnets.

Uncontrolled copy when printed

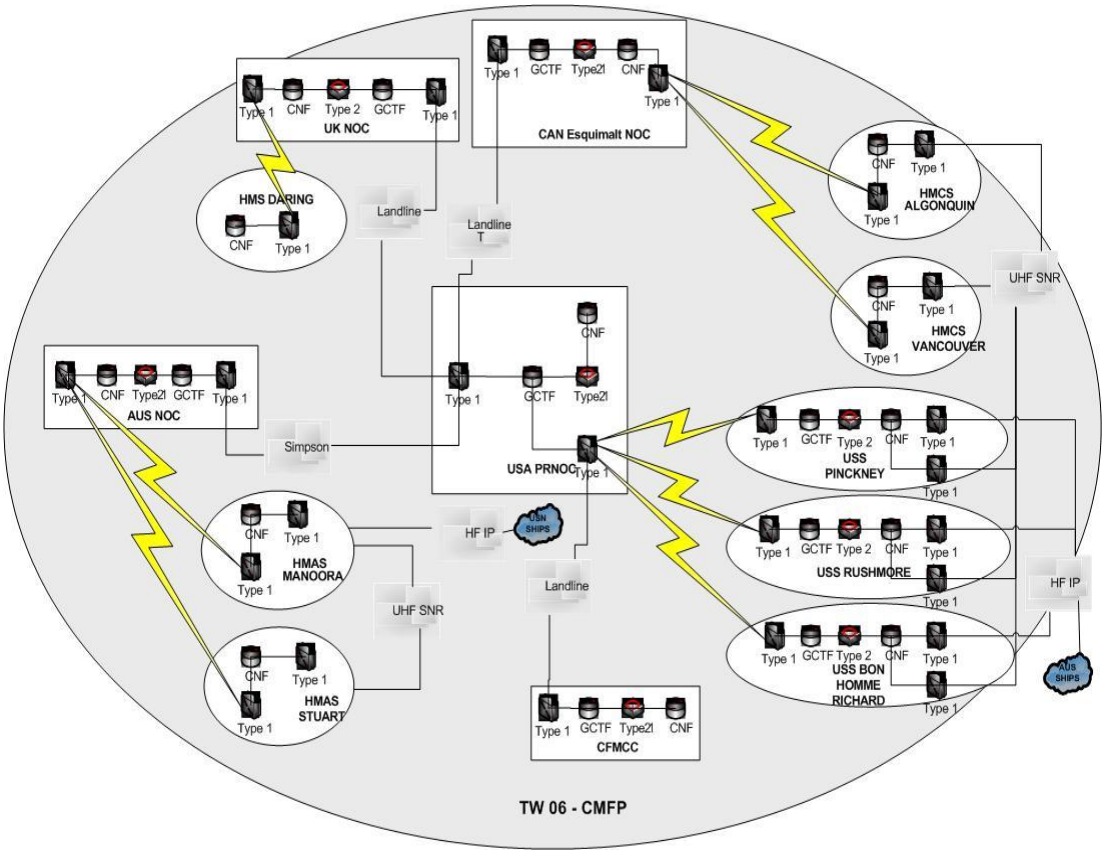

Figure E1–1: MWTAN Routing Topology

E1.2 Multi-Topology Routing.

The MTWAN routing architecture will employ Multi-Topology Routing (MTR) extensions to the Open Shortest Path First (OSPF) routing protocol to support the simultaneous use of multiple bearers – UHF Subnet Relay, HF Internet Protocol, and SATCOM. With unmodified OSPF, each router uses a single path towards each destination, the shortest path based on advertised link weights. A MTR router directs traffic along more than one path towards its destination by mapping the traffic to distinct logical topologies, where each logical (or colored) topology has its own distinct set of link weights. Traffic is mapped to a logical topology based on application type or Differentiated Services Code Point (DSCP) marking.

Because there are three bearers of interest for the MTWAN, three MTR topologies are supported: Delay Sensitive, Standard, and Delay Tolerant. In the event that multiple links between ships are available, the following table lists the order in which they will be preferred for each of these three classes.

Uncontrolled copy when printed

Table E1.2-1: Ship-to-ship bearer preference based on traffic class

Traffic Class	Delay Sensitive	Standard	Delay Tolerant
Bearer Preference	1. SATCOM 2. UHF SNR 3. HF IP	1. UHF SNR 2. HF IP 3. SATCOM	1. HF IP 2. UHF SNR 3. SATCOM

For the ship to shore links, each ship should of course prefer its own SATCOM connection to reach the shore before it employs LOS/ELOS relay using either SNR or HF IP. LOS/ELOS relay to another ship followed by a SATCOM connection from the relay ship provides a backup connection to shore when a ship does not have a direct SATCOM connection of its own. Under no circumstances do we wish to allow NOC to NOC traffic to transit the LOS/ELOS ship-to-ship links, as they would quickly become overwhelmed. This policy is enforced by applying strict access control at each of the shore access routers.

Figure E1.2-2 below provides a high level illustration of the OSPF link weights employed for each of the three topologies. The principal distinction between the three topologies is the weights assigned to the links between the shipboard MTWAN routers and SNR and HF IP. Since SNR acts as a layer 2 bridge, the link weights shown are for the single hop into the SNR "cloud." By contrast, HF IP runs a layer 3 router of its own, and the link weights shown are for the hop between the MTWAN and HF IP routers. Two such hops are required for any MTWAN to MTWAN connection over HF IP; in addition to the over the air HF hops. When the link weight is the same for all three topologies, only a single weight is shown. The connection from each shipboard MTWAN router to the shore MTWAN router via SATCOM in fact transits several pieces of equipment and is tunnelled over national network infrastructure. A GRE tunnel is thus established to which a nominal OSPF cost of 1000 (+/- 10 to prevent equal cost load balancing) is assigned. The NOC-to-NOC shore-based connections are assigned very low OSPF costs, as these are deemed to be much higher performing and more reliable than the other tactical links illustrated.

Uncontrolled copy when printed

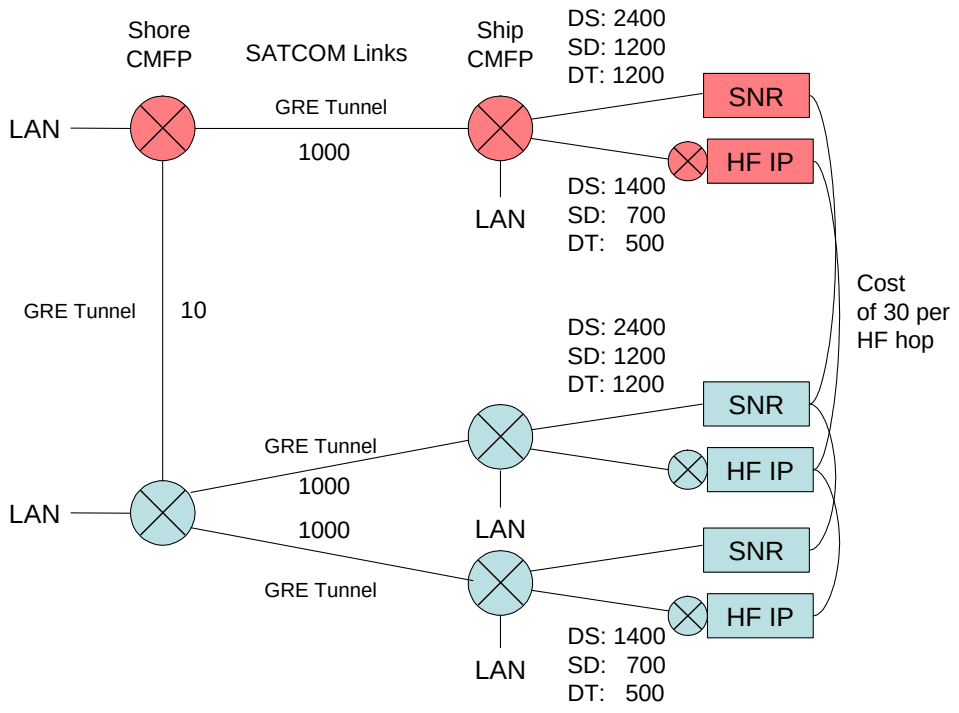

Figure E1.2-1: EXER/OPER MTR Weights

The situation is slightly more complicated than this figure suggests because in fact the shore-based MTWAN routers employed are not MTR capable. The shore routers participate only in the MTR base topology. In order to insure that delay sensitive (DS) traffic is preferentially routed via SATCOM links to the shore, the DS topology is employed as the base topology. The standard (SD) and delay tolerant (DT) topologies do not in fact include the shore routers per se, but the implementation of MTR employed falls back to the base topology forwarding tables when no route to the destination is found in the colored forwarding table. The desired routing behavior is achieved as a result.

The following table illustrates the mapping of applications to traffic classes.

Uncontrolled copy when printed

Table E1.2-2: Mapping Applications to Traffic Classes

Traffic Class	Delay Sensitive	Standard	Delay Tolerant
DSCP	AF21	AF12	AF13
MTR Topology	Base	MT30 (Blue)	MT20 (Red)
Applications	Sametime Persistent War Room DNS CCL+	Domino Domino Mail FIRE	C2PC C2PC Accelerator JPIP

Traffic type is recognized according to TCP/UDP port number employed. A known port number may be used by either a source or destination (or both). For example, port number 1533 is employed by Sametime Client, which is assigned a DSCP of AF21 and mapped to the delay sensitive class. On the Linux MTR routers, the initMTR configuration file includes the entry below.

```
iptables -t mangle -A PREROUTING -p tcp --dport 1533 -j DSCP
--set-dscp-class AF21
iptables -t mangle -A PREROUTING -p tcp --sport 1533 -j DSCP
--set-dscp-class AF21
```

A complete listing of port numbers for which marking is executed is in Table E1.2-3 below.

Uncontrolled copy when printed

Table E1.2-3: Multi-Topology Routing Classification, Priorities and Weights

Application	Port Number	DSCP Marking
Delay Sensitive (SATCOM, SNR, HF IP)		
Sametime Client	1533	AF21
ST Mtg Svc Connector	1503	AF21
ST Srvr Connector	1516	AF21
ST Meeting Center Event Connector ST Mtg Srv AV Connector St Mtg Srv Token Connector	9092 - 9094	AF21
ST Dynamic AV UDP	49252 - 65535	AF21
Web – http	80,8080	AF21
Web – secure http	443	AF21
DNS	53	AF21
VNC	5900	AF21
CCL+	7468	AF21
Standard (SNR, HF IP, SATCOM)		
Domino	1352	AF12
SMTP	25	AF12
POP3	110	AF12
LDAP	389	AF12
RTSP	554	AF12
JPIP Engineering	5050	AF12
Delay Tolerant (HF IP, SNR, SATCOM)		
Oracle	2030	AF13
Live Update Server	3100	AF13
Web Services Report	9090	AF13
AE Coordinator Port	8479	AF13
Analysis Engine Port	9680	AF13
Master Coordinator Port	9000	AF13
C2PC	2036, 2701, 2702	AF13
JPIP	5000	AF13

Other traffic of particular note that will be monitored: OSPF, SNR PDC traffic (local only), SNMP (local monitoring).

Uncontrolled copy when printed

E2. AS NUMBERS.

Autonomous System Numbers are not applicable for the duration of the Operation or Exercise, as the MTWAN network will be operating in a single AS. BGP boundaries will not be utilized.

E3. OSPF PARAMETERS.

OSPF timer parameters are shown in table E3-1. OSPF costs shown in figure E1-2.1 are summarized in table E3-2.1. More details on the tunnels are provided in table E4-5.1. As already stated, three distinct OSPF topologies will be supported by the Multi-Topology Routing (MTR) routers: delay-sensitive (base), standard, and delay-tolerant. Non-MTR routers participate only in the base topology and do not employ the standard and delay-tolerant link costs.

Table E3–1: OSPF Settings

Transport	BW (kbps)	OSPF Area	Dead Timer (Sec)	Hello Interval (Sec)	Retransmit (Sec)
SHF	512	0	40	10	5
INMARSAT	64	0	40	10	5
Subnet Relay	64.0	0	120	30	60
HF IP (ISB)	19.2	0	120	30	60
HF IP (SSB)	9.6	0	120	30	60

Table E3-2.1 OSPF Link Costs

Link	Base Topology Link Cost	Standard Topology Link Cost	Delay-Tolerant Topology Link Cost
MTWAN Router to LAN	10	Same as base	Same as base
MTWAN Router to SNR	2400	1200	1200
MTWAN Router to HF IP	1400	700	500
MTWAN Router to NOC (SATCOM)	1000 ± 10 (see table E4.5-1)	Same as base	Same as base
HF IP RF (tap0) interface	30	Same as base	Same as base
NOC-NOC Tunnels	10	Same as base	Same as base

Uncontrolled copy when printed

E4. LOCAL AREA NETWORKS

E4.1 LAN SUBNETS

The following table is the allocation of IP addressing for the MTWAN Red side LANs.

Table E4.1–1: LAN Subnet IP Addressing

Node	Subnet Network ID and mask bits	Subnet Size
Nation 1	Range x.x.1.0 -x.x.30.255	
NOC	x.x.1.0/24	256 (x.x.1.0 – x.x.1.255)
Spare	x.x.2.0/28	16 (x.x.2.32 – x.x.2.47)
Shipname	x.x.2.32/28	16 (x.x.2.32 – x.x.2.47)
Shipname	x.x.2.64/28	16 (x.x.2.64 – x.x.2.79)
Shipname	x.x.2.128/26	64 (x.x.2.128 – x.x.2.191)
CFMCC	x.x.20.0/26	64 (x.x.20.1 – x.x.20.63)
Nation 2	Range x.x.32.0 -x.x.39.255	
NOC	x.x.32.0/27	32 (x.x.32.128 – x.x.32.159)
Shipname	x.x.32.32/27	32 (x.x.32.32 – x.x.32.63)
Shipname	x.x.32.96/27	32 (x.x.32.96 – x.x.32.127)
Spare	x.x.32.128/27	
Nation 3	Range x.x.y.0 -x.x.y.255	
NOC	x.y.40.0/25	
Shipname	x.y.45.128/26	64 (x.y.45.128 – x.y.45.191)
Shipname2	x.y.44.128/27	32 (x.y.44.128 – x.y.44.159)
Nation 4	Range x.x.z.0 -x.x.z.255	
NOC	x.x.56.32/28	16 (x.x.56.32 – x.x.56.47)
Shipname	x.x.56.0/28	16 (x.x.56.0 – x.x.56.15)

E4.2 LAN Host IP Addressing Template

The following table provides a template for host addressing on the MTWAN LANs. The two most crucial addresses are the MTWAN router interface (at subnet + 1) and the PDC/DC01 address (at subnet +4). The broadcast – 1 address is left unassigned and is reserved for the NOC as the router id.

Uncontrolled copy when printed

Table E4.2-1: Recommended MTWAN IP Addressing Template

IP Address	Network Component
subnet + 0	LAN subnet network ID
subnet + 1	MTWAN router interface
subnet + 2	Managed switch
subnet + 3	Reserved for network device
subnet + 4	PDC/ Exchange Server
subnet + 5	BDC/C2PC Gateway Server
subnet + 6	CAS/Domino server #1 (old)
subnet + 7	CAS/Domino server #2 (new - US)
subnet + 8	Client
.....	.....
subnet + 11	Client
Additional addresses if available	Client
.....	.....
broadcast - 3	Data collection laptop #1
broadcast - 2	Data collection laptop #2
broadcast - 1	Unused
subnet + 15	Broadcast for /28 netmask
subnet + 31	Broadcast for /27 netmask
subnet + 63	Broadcast for /26 netmask
subnet + 255	Broadcast for /24 netmask

Uncontrolled copy when printed

E4.3 Line of Sight Bearers

E4.3.1 SNR UHF IP Addressing and OSPF Cost

SNR connects to the MTWAN router as a layer 2 bridge. This is not exposed to the IP layer and so is transparent to OSPF routing. The MTWAN SNR Subnet ID is x.x.224.0 with a 24-bit mask. Table E4.3.1-1 provides the IP addressing for UHF SNR.

Table E4.3.1-1: SNR IP Addressing

Node	Router Interface	SCRN Interface
Nation 1	Range x.x.224.1 – x.x.224.63	
NOC	N/A	N/A
Shipname	x.x.224.1	x.x.224.4
Shipname	x.x.224.2	x.x.224.5
Shipname	x.x.224.3	x.x.224.6
Nation 2	Range x.x.224.100 – x.x.224.127	
NOC	N/A	N/A
Shipname	x.x.224.100	x.x.224.101
Shipname	x.x.224.104	x.x.224.105
Nation 3	Range x.x.224.151 – x.x.224.200	
Shipname	x.x.224.151	x.x.224.152
Shipname	x.x.224.153	x.x.224.154

E4.3.2 HF IP Addressing and OSPF Cost

HF IP connects to the MTWAN router as a layer 3 router with an Ethernet segment. Three addresses are required: one for the MTWAN router interface to HF IP, one for the Ethernet interface on HF IP, and one for the HF WAN air interface on HF IP. The first two must be in the same subnet on each platform, whereas the third must be drawn from a subnet common to all platforms. A /30 netmask is sufficient for the MTWAN/HFIP connection since it has only two endpoints. The address x.x.192.0/24 is used for the HF WAN interface

HF IP OSPF costs are configured on the two interfaces that connect the Ships MTWAN Router and HFIP Router together. This must be done on each interface (e.g. on the MTWAN router and the HFIP Router). HF IP performs OSPF routing at layer 3 with a per-hop cost of 30. This configuration will allow the OSPF cost of any direct HF IP routes to be approximately 1000 (Delay Sensitive), 1400 (Standard) or 2800 (Delay Tolerant) between ships.

Table E4.3.2.1 lists the IP addressing for HF IP controllers. The MTWAN Router interface and HF IP Router interface have 30-bit masks. The HF IP WAN subnet has a 29-bit mask. Note that the last octet is negotiated and automatically assigned to each node by the HF IP network token ring owner.

Uncontrolled copy when printed

Table E4.3.2–1: HF IP Addressing

Node	MTWAN Router Interface	HF IP Router Interface	HF IP WAN Interface
Nation 1			Range xxx.yy.192.1-7/29
NOC	N/A	N/A	N/A
Shipname	xxx.yy.2.21/30	xxx.yy.2.22/30	xxx.yy.192.z/29
Shipname	xxx.yy.2.53/30	xxx.yy.2.54/30	xxx.yy.192.z/29
Shipname	xxx.yy.2.85/30	xxx.yy.2.86/30	xxx.yy.192.z/29
Nation 2			Range xxx.yy.192.1-7/29
Shipname	xxx.yy.46.241/30	xxx.yy.46.242/30	xxx.yy.192.z/29
Shipname	xxx.yy.46.245/30	xxx.yy.46.246/30	xxx.yy.192.z /29

Uncontrolled copy when printed

E4.4 SATCOM IP Addressing

Table E4.4.1 lists IP addressing between the MTWAN router and the MTWAN border encryption device that is connected to the national SATCOM systems. This could be the private side of a VPN concentrator or the PT side of a TACLANE.

The range x.x.31.0 to x.x.31.31 has been reserved for the host NOC's SATCOM links and can be sub-netted as required. All subnets in the table below have 30-bit masks.

Table E4.4-1: SATCOM IP Addressing

Node	Router Interface	TL/VPN Interface (plain text)	TL/VPN (cipher text)
Nation 1			
NOC	x.x.31.1	x.x.31.2	classified
Shipname	x.x.2.25	x.x.2.26	classified
Shipname	x.x.2.57	x.x.2.58	classified
Shipname	x.x.2.97	x.x.2.98	classified
CFMCC	x.x.31.85 /30	x.x.2.84 /30	x.x.x.51
Nation 2			
NOC	x.x.33.25	x.x.33.26	classified
Shipname	x.x.33.57	x.x.33.58	classified
Shipname	x.x.33.121	x.x.33.122	classified
Nation 3			
NOC	xxx.yy.46.1	xxx.yy.46.2	classified
Shipname	xxx.yy.46.129	xxx.yy.46.130	classified
Shipname	xxx.yy.46.153	xxx.yy.46.154	classified
Nation 4			
NOC	x.x.56.25	x.x.56.26	classified
Shipname	x.x.56.57	x.x.56.58	classified

Uncontrolled copy when printed

E4.5 GRE Tunnel Addresses and Costs

Table E4.5 - 1 lists the IP addresses of the GRE tunnels that are established from national NOC MTWAN routers to the National Ship routers. It also lists the OSPF costs that are to be assigned to the GRE tunnel interface that connects each Ship to its national NOC (SATCOM link). The tunnel costs include small offsets to prevent equal cost load balancing. All subnets in Table E4.5-1 have 30-bit masks.

Table E4.5-1: NOC to National NOC & NOC to Ship GRE Tunnel Information

Tunnel to	Tunnel #	Local	Remote	Tunnel Cost
Nation 1				
NOC				
Shipname	10	x.x.31.65	x.x.31.66	990
Shipname	11	x.x.31.69	x.x.31.70	991
Shipname	12	x.x.31.73	x.x.31.74	992
not assigned	13	x.x.31.77	x.x.31.78	993
CFMCC	14	x.x.31.81	x.x.31.82	994
Nation 2				
NOC TO NOC	1	x.x.39.1	x.x.39.2	10
Shipname	30	x.x.39.5	x.x.39.6	1000
Shipname	32	x.x.39.13	x.x.39.14	1002
Nation 3				
NOC to NOC	2	x.x.x.x	y.y.y.y	10
Shipname	50	x.y.47.36	y.y.y.y	1005
Shipname	?	x.y.47.30	y.y.y.y	1006
Nation 4				
NOC to NOC	4	x.x.63.1	x.x.63.2	10
Shipname	90	x.x.63.5	x.x.63.5	1030

Uncontrolled copy when printed

E4.6 Landline WAN Bearers IP Addressing

This table lists IP addressing of the Landline WAN that link all that national NOCs. This will be the subnet that connects the MTWAN router to the private side of a VPN Concentrator/TACLANE. The public side of the VPN Concentrator/TACLANE connects to the COI router.

The range x.x.31.32 to x.x.31.63 has been reserved for the NOC and can be sub-netted as required. All subnets in the table below have 30-bit masks.

Table E4.6-1: Landline WAN Bearers IP Addressing

Node	Router Interface	TL/VPN Interface
Nation 1 NOC	x.x.31.2	x.x.31.1
Nation 2 NOC	x.x.32.29	x.x.32.30
Nation 3 NOC	x.x.46.1	x.x.46.2
Nation 4 NOC	x.x.56.29	x.x.56.30

E4.7 COI Connections IP Addressing

This table lists the IP addresses between the public side of the VPN device and the interface on the COI Router. Once the MTWAN is established and operating at the classified level, these addresses may be added.

Table E4.7-1: GCTF Connections IP Addressing

Nodes	VPN Public Interface	GCTF Router Interface
Nation 1	classified	Classified
Nation 2	classified	Classified
Nation 3	classified	Classified
Nation 4	classified	Classified

Uncontrolled copy when printed

F. NAMING AND ADDRESSING

This section provides a single reference point within the NCP so that all relevant unit, network and server naming information is available within.

F1 DNS Naming Format for EXER/OPER

In accordance with ACP 200 Chapter 5, the DNS naming format for this Operation or Exercsie will be

[unit](<15 char)].[service].[country (3 char)].[network-COI].cmil.mil

i.e. prnoc.navy.usa.gctf-COI.cmil.mil

The SMTP email address format for role-based accounts will be;

[role]@[unit] (<15 char)].[service].[country (3 char)].[network-COI].cmil.mil

i.e. pwo@tek.navy.nzl.gctf-COI.cmil.mil

F2 DNS ROOT SERVERS

F2.1 DNS Overview

In accordance with ACP 200, DNS servers will be distributed throughout the MTWAN, with national NOCs hosting the primary DNS server for their domain and all the ships for which it is responsible. The national NOCs will also act as a secondary server for all other Coalition nodes. Ships will act as a secondary DNS server for all Coalition nodes including themselves. The reasons for putting the primary DNS servers at the shore sites are;

Eliminate DNS queries across the low speed and intermittent RF nets within the MTWAN. A ship must be able to resolve DNS queries while it does not have connectivity ashore.

Move DNS administration ashore where specialists can administer the DNS databases, simplifying network administration onboard the ships. The ships secondary servers will automatically download the data from the primary server via zone transfers as required, without intervention by ship's company. When the ship requires changes to the DNS database, it will contact the NOC via email or voice to request changes. The NOC will make the requested changes to the DNS db files of the primary server. The updated db files will then be copied by all secondary servers at the next database refresh or at a forced restart of the secondary servers.

For the Operation or Exercise, the host NOC will be the Root DNS Authority for the domain name "[domain-coi].cmil.mil" e.g. "gctf-COI.cmil.mil". National NOCs will point their Root Hint File to the PRNOC DNS server. All nations will pull a secondary of each other and be a Secondary DNS Authority for the "gctf-COI.cmil.mil" domain. This reduces the need for

Uncontrolled copy when printed

national NOCs to query the PRNOC Root DNS Authority for other nations' domains. See paragraph F3 for more detail.

To reduce network traffic and increase the authoritative life of data in the zone files for times of extended non-connectivity, the SOA parameters are to be altered to the following DNS Settings as recommended in ACP 200:

2001011001:	Serial yyyymmdd##
86400:	Refresh every 24 hours
3600:	Retry every hour
3600000:	Expire after a month
86400:	Minimum TTL of 1 day

Serial No: If any changes have been made to a db file, its serial number must be manually incremented. Secondary servers use the Serial number to check if they have the latest copies of the db files. If their serial numbers are lower than that of the primary server, they will request a new copy from the primary.

Refresh: The Refresh value in seconds determines how often the local secondary server checks that its db files are up to date.

Retry: If the attempt to refresh fails, the local secondary server will wait "Retry" seconds and then try again.

Expire: If the refresh fails for "Expire" seconds, the local secondary server will stop providing answers.

Time To Live: The value of TTL (Time To Live) in seconds is attached to answers provided by the local secondary server to tell other servers how long the answers will remain valid.

Uncontrolled copy when printed

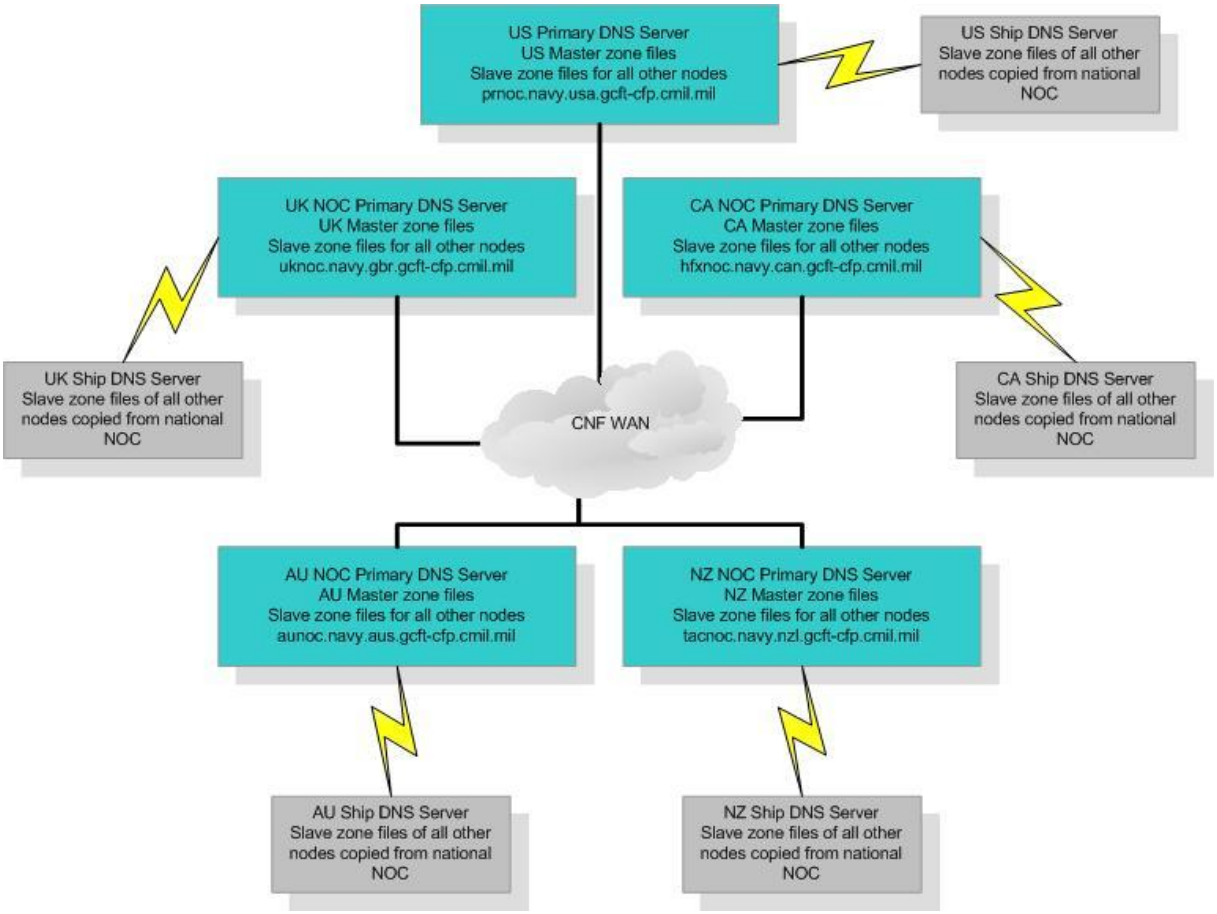

Figure F1.1-1: Domain Name Schema

F2.1.1 Domino Web-Mail Issues: Secure Domino Web Mail will be used as the email system of choice during the Operation or Exercise by all nations. The Web Mail domain names will be distinguished by the addition of a "-web" to the ship name.

US SHIP 1: shipname-web.navy.usa.gctf-COI.cmil.mil

US SHIP 2: shipname-web.navy.usa.gctf-COI.cmil.mil

US SHIP 3: shipname-web.navy.usa.gctf-COI.cmil.mil

PRNOC will create Zones that will route these "Email-only" Domain Names to the correct and actual Domino server. The actual Domino server DNS name will not change from that specified in Section F4.4 of this NCP. For example, the Domino server on US SHIP 1 will actually be shipname.navy.usa.gctf-COI.cmil.mil.

Separate Domino connection documents will be established that will route mail to other ships/nodes via SATCOM and SNR/HF IP. These connection documents will be weighted in order to use SATCOM first and SNR/HF IP second.

Uncontrolled copy when printed

F2.1.2 SMTP Email Issues: In the event that SMTP email is used during EXER/OPER, as well as to properly support the RIMPAC exercise, the Exchange Servers on the EXER/OPER ships will be configured to use DNS MX records to find the SMTP email server of the intended email recipient, and therefore letting the network find the best path to that server. Each node will advertise to the rest of the network its local SMTP email server in DNS. This will result in ship-to-ship email been routed directly over any LOS bearers if present. However if a ship has intermittent connectivity a method of relaying and queuing email ashore via SATCOM is required. Therefore each ship will also advertise its national NOC SMTP email server in DNS with a lower priority as described below.

a. MX 10 [Local SMTP Email Server].

b. MX 20 [National NOC SMTP Email Server].

Uncontrolled copy when printed

F2.3 DNS Namespaces for EXER/OPER

Table F1.3-1 delineates the Fully Qualified Domain Names to be used during EXER/OPER by ship and shore site.

Table F1.3–1: Example Site Names, Abbreviations and Fully Qualified Domain Names

Ship Name	EXER/OPER Unit Abbreviation	Fully Qualified Domain Name/Reverse Lookup
Royal Australian Navy		
AU NOC	AUNOC	aunoc.navy.aus.gctf-*COI*.cmil.mil[1]
AUS SHIP 1	SHIP	shipname.navy.aus.gctf-COI.cmil.mil
AUS SHIP 2	SHIP	shipname.navy.aus.gctf-COI.cmil.mil
	AUNOC	40.yy.xx.in-addr.arpa
	SHIP	44.yy.xx.in-addr.arpa
	SHIP	45.yy.xx.in-addr.arpa
Canadian Navy		
Esquimalt NOC	ESQNOC	esqnoc.navy.can.gctf-COI.cmil.mil
CA SHIP 1	SHIP	shipname.navy.can.gctf-COI.cmil.mil
CA SHIP 2	SHIP	shipname.navy.can.gctf-COI.cmil.mil
		32.yy.xx.in-addr.arpa
		39.yy.xx.in-addr.arpa
Royal Navy		
UK NOC	UKNOC	uknoc.navy.gbr.gctf-COI.cmil.mil
UK SHIP 1	SHIP	shipname.navy.gbr.gctf-COI.cmil.mil
		56.yy.xx.in-addr.arpa
		63.yy.xx.in-addr.arpa
US NAVY		
PACIFIC REGIONAL NOC	PRNOC	prnoc.navy.usa.gctf-COI.cmil.mil
US SHIP 1	SHIP	shipname.navy.usa.gctf-COI.cmil.mil
US SHIP 2	SHIP	shipname.navy.usa.gctf-COI.cmil.mil
US SHIP 3	SHIP	shipname.navy.usa.gctf-COI.cmil.mil
		1.yy.xx.in-addr.arpa
		2.yy.xx.in-addr.arpa
		31.yy.xx.in-addr.arpa

[1] Replace "COI" with the four letter designator for the Community of Interest.

Uncontrolled copy when printed

F3. HOST NAMES

The ACP 200 derived host naming is designed to give meaningful names to hosts on the network that can easily remembered by administrators and users. A host may be running several services so it will be aliased with as many names as required. For example the Domino server could be running the web, LDAP, and SMTP services; therefore it would be aliased with, web-serv, ldap-serv, and mail-serv.

Table F2-1: Host Names/Aliases

Host Names or Aliases	Function
Servers	
web-serv	Domino Web server
mail-serv	SMTP Mail server
key-serv	Key & Authentication Server
gccsm-serv	GCCS-M server
c2pc-serv	C2PC Gateway server
dcp-serv	Sametime Server (also hosts Persistent War Room)
ldap-serv	LDAP Directory server
jdcat-serv	JDCAT Assessment Server
jpip-serv	JPEG 2000 JPIP server
net-serv	Network Monitoring server
time-serv	NTP server
citrix-serv	Citrix server
Workstations	
gccsm-wkst-*x*	Dedicated C2PC Client(s)
jpip-wkst-*x*	Dedicated JPEG 2000 JPIP client(s)
pntr-*x*	Printer(s)
wkst-*x*	Multi-purpose Workstation
sniff-x	Network Sniffer
Network Devices	
Rout	Router LAN Gateway interface
Swit	LAN Switch
Opt	Network Accelerator/Optimizer (i.e. Peribit)
Vpn	VPN Concentrator

Uncontrolled copy when printed

F4. DNS DOMAIN RESPONSIBILITIES

The host NOC will maintain a Primary and Secondary Root Name Servers for the domain. The host NOC will delegate the Country Domain names (ccc.dddd-coi.cmil.mil where 'ccc' is the three letter country code for each respective country in accordance with ISO 3166, 'dddd' is the domain name and 'coi' is the community of interest. Therefore, each Coalition NOC DNS Servers will be the authority for their respective country Domain names. Each Coalition NOC DNS Servers will be Secondary name servers for all other Coalition Country Domains. Each Coalition NOC DNS Servers will also be Secondary name servers for their individual countries Ships.

For Coalition Ships that are outfitted with SNR and HF IP, each Coalition Ship DNS Server will be authority for their individual Ship Domain names and will be Secondary name servers for all Ship Domain names that also are outfitted with SNR and HF IP.

NOC DNS Server Root hints file will contain the following:

x.y.1.4	dns1-serv
x.y.1.7	dns2-serv

F5. HOST NAMES AND IP ADDRESSES

All major hosts for each nation, on each platform or at each shore node are included in the following sections. They are accompanied by a connectivity diagram for each node in order to give a better perspective on the configuration of each site. To aid in deciphering the Netmask information, Table F4-1 is provided

Figure F4-1: Netmask Translation Table

IP Netmask	"Slant" Netmask	Addresses Available
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2
255.255.255.254	/31	0

Uncontrolled copy when printed

F5.1 AUSTRALIA ADDRESSING

The figures F4.1-1 F4.1-2 and F4.1-3 illustrate the network architectures for the Australian nodes; the Australian NOC (AUNOC) located at the Fleet Information Systems Support Organization (FISSO), Bldg 89/90 Garden Island, AUS SHIP 1 and AUS SHIP 2.

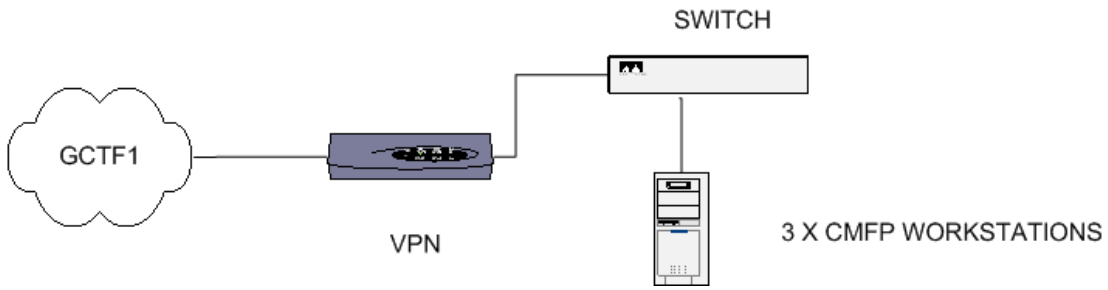

Figure F4.1-1: EXER/OPER AUNOC

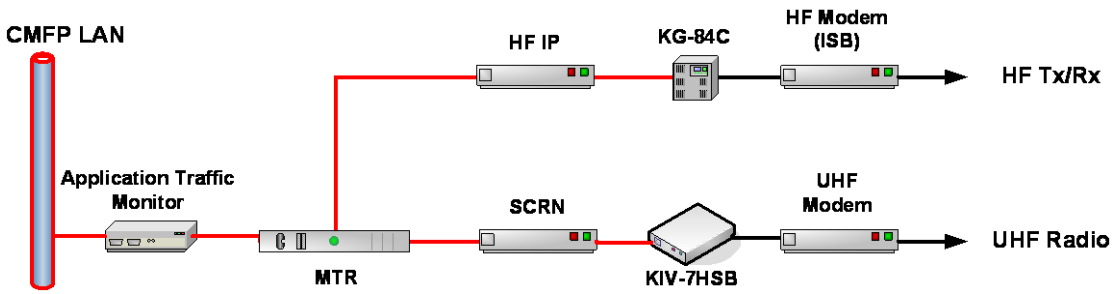

Figure F4.1-2: EXER/OPER AUS SHIP 1

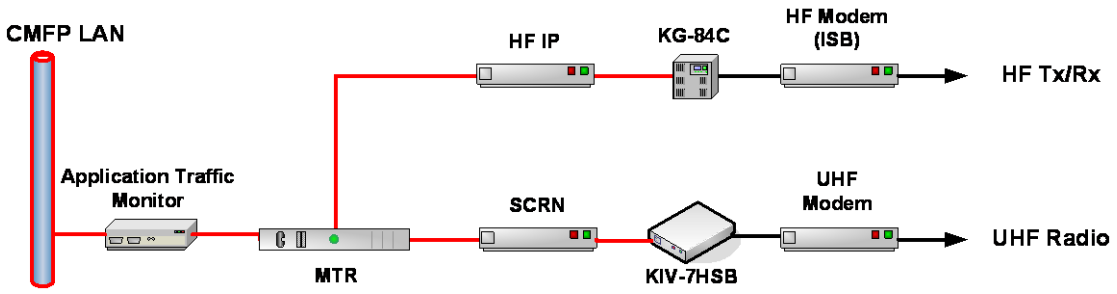

Figure F4.1-3: EXER/OPER AUS SHIP 2

For EXER/OPER, the following MTWAN IP addressing in Table F4.1-1 will be in use by the Australian NOC, AUS SHIP 1 and AUS SHIP 2.

Uncontrolled copy when printed

Table F4.1-1: Australia MTWAN WAN/LAN IP Address Allocation

MTWAN LAN IP ADDRESS	AUNOC (x.y.40.0/25)	AUS SHIP 1 (x.y.45.128/26)	AUS SHIP 2 x.y.44.128/27
Taclane (plain text)	N/A	N/A	N/A
VPN Concentrator (Plain Text Interface)	xxx.yy.46.2/29 vpn.aunoc.navy.aus.gctf-COI.cmil.mil	xxx.yy.46.154/30 vpn.shipname.navy.aus.gctf-COI.cmil.mil	xxx.yy.46.130/30 vpn.stu.navy.aus.gctf-COI.cmil.mil
Router (VPN Interface)	xxx.yy.46.1/29	xxx.yy.46.153/30	xxx.yy.46.129/30
Router (LAN Interface)	xxx.yy.40.1/25 rout.aunoc.navy.aus.gctf-COI.cmil.mil	xxx.yy.45.129/26 rout.shipname.navy.aus.gctf-COI.cmil.mil	xxx.yy.44.129/27 rout.stu.navy.aus.gctf-COI.cmil.mil
Switch 1	xxx.yy.40.5/25 swit1.aunoc.navy.aus.gctf-COI.cmil.mil	xxx.yy.45.130/26 swit1.shipname.navy.aus.gctf-COI.cmil.mil	xxx.yy.44.130/27 swit1.stu.navy.aus.gctf-COI.cmil.mil
Switch 2	N/A	xxx.yy.45.131/26 swit2.shipname.navy.aus.gctf-COI.cmil.mil	xxx.yy.44.131/27 swit1.stu.navy.aus.gctf-COI.cmil.mil
Switch 3	N/A	xxx.yy.45.132/26 swit3.shipname.navy.aus.gctf-COI.cmil.mil	N/A
Switch 4	N/A	xxx.yy.45.133/26 swit4.shipname.navy.aus.gctf-COI.cmil.mil	N/A
UPS	N/A	N/A	N/A
Primary Domain Controller Windows 2003	xxx.yy.40.20/25 FLTSDN01.aus.gctf-COI.cmil.mil	xxx.yy.45.150/26 SHIPNAMESDN01.aus.gctf-COI.cmil.mil	xxx.yy.44.140/27 STUSDN01.aus.gctf-COI.cmil.mil

Uncontrolled copy when printed

MTWAN LAN IP ADDRESS	AUNOC (x.y.40.0/25)	AUS SHIP 1 (x.y.45.128/26)	AUS SHIP 2 x.y.44.128/27
DNS Server	xxx.yy.40.20/25 FLTSDN01.aus.gctf-COI.cmil.mil Win2K3 Domain Controller DNS Alias per ACP 200 dns2-serv.aunoc.navy.aus.gctf-COI.cmil.mil	xxx.yy.45.150/26 SHIPNAMESDN01.aus.gctf-COI.cmil.mil Win2K3 Domain Controller DNS Alias per ACP 200 dns-serv.shipname.navy.aus.gctf-COI.cmil.mil	xxx.yy.44.140/27 STUSDN01.aus.gctf-COI.cmil.mil Win2K3 Domain Controller DNS Alias per ACP 200 dns-serv.stu.navy.aus.gctf-COI.cmil.mil
DNS Server	xxx.yy.40.30/25 AUSDN01.aus.gctf-COI.cmil.mil Win2K3 Standalone Server DNS Alias per ACP 200 dns1-serv.aunoc.navy.aus.gctf-COI.cmil.mil key-serv.aunoc.navy.gctf-COI.cmil.mil	N/A	N/A
NTP Server	xxx.yy.40.1/25 rout.aunoc.navy.aus.gctf-COI.cmil.mil DNS Alias per ACP 200 time-serv.aunoc.navy.aus.gctf-COI.cmil.mil	xxx.yy.45.129/26 rout.shipname.navy.aus.gctf-COI.cmil.mil DNS Alias per ACP 200 time-serv.shipname.navy.aus.gctf-COI.cmil.mil	xxx.yy.44.129/27 rout.stu.navy.aus.gctf-COI.cmil.mil DNS Alias per ACP 200 time-serv.stu.navy.aus.gctf-COI.cmil.mil

Uncontrolled copy when printed

MTWAN LAN IP ADDRESS	AUNOC (x.y.40.0/25)	AUS SHIP 1 (x.y.45.128/26)	AUS SHIP 2 x.y.44.128/27
Mail Server	xxx.yy.40.21/25 mail-serv.aunoc.navy.aus.gctf-COI.cmil.mil	xxx.yy.45.151/26 mail-serv.shipname.navy.aus.gctf-COI.cmil.mil	xxx.yy.40.141/27 mail-serv.stu.navy.aus.gctf-COI.cmil.mil
C2PC Gateway Server	xxx.yy.40.20/25 c2pc-serv.aunoc.navy.aus.gctf-COI.cmil.mil	xxx.yy.45.150/26 c2pc-serv.shipname.navy.aus.gctf-COI.cmil.mil	xxx.yy.40.140/27 c2pc-serv.stu.navy.aus.gctf-COI.cmil.mil
Domino Server	xxx.yy.45.21/25 web-serv1.aunoc.navy.aus.gctf-COI.cmil.mil (CLUSTERED) xxx.yy.45.22/25 web-serv2.aunoc.navy.aus.gctf-COI.cmil.mil	xxx.yy.45.151/26 web-serv1.shipname.navy.aus.gctf-COI.cmil.mil (CLUSTERED) xxx.yy.45.152/26 web-serv2.shipname.navy.aus.gctf-COI.cmil.mil	xxx.yy.44.140/27 web-serv1.stu.navy.aus.gctf-COI.cmil.mil (CLUSTERED) xxx.yy.44.142/27 web-serv2.stu.navy.aus.gctf-COI.cmil.mil
Sametime Server (PWR Host)	xxx.yy.45.22/25 dcp-serv1.aunoc.navy.aus.gctf-COI.cmil.mil	xxx.yy.45.152/26 dcp-serv.shipname.navy.aus.gctf-COI.cmil.mil	xxx.yy.44.142/27 dcp-serv.stu.navy.aus.gctf-COI.cmil.mil
GCCS-M Server	N/A	xxx.yy.47.254 jots1.navy.gov.au	xxx.yy.34.253 jots1.navy.gov.au
JPIP Server	N/A	xxx.yy.45.138/26 pip-serv.shipname.navy.aus.gctf-COI.cmil.mil	xxx.yy.44.153/27 pip-serv.stu.navy.aus.gctf-COI.cmil.mil

Uncontrolled copy when printed

MTWAN LAN IP ADDRESS	AUNOC (x.y.40.0/25)	AUS SHIP 1 (x.y.45.128/26)	AUS SHIP 2 x.y.44.128/27
LAN Sniffer **Network Monitor**	xxx.yy.45.22/25 FLTSN03.aunoc.navy.aus. gctf-COI.cmil.mil DNS Alias per ACP 200 net-serv.aunoc.navy.aus.gctf-COI.cmil.mil http://net-serv.aunoc.navy.aus.gctf-COI.cmil.mil/cacti	xxx.yy.45.153/26 SHIPNAMESN03.shipname.navy.aus. gctf-COI.cmil.mil DNS Alias per ACP 200 net-serv.shipname.navy.aus.gctf-COI.cmil.mil http://net-serv.shipname.navy.aus.gctf-COI.cmil.mil/cacti	xxx.yy.44.139/27 STUSN03.stu.navy.aus. gctf-COI.cmil.mil DNS Alias per ACP 200 net-serv.stu.navy.aus.gctf-COI.cmil.mil http://net-serv.stu.navy.aus.gctf-COI.cmil.mil/cacti
Workstation(s)	Workstations will be GCTF workstations connecting via Cisco VPN Software client 4.8x	x.y.45.160 through x.y.45.190 DNS names will be added through Active Directory	x.y.44.145 through x.y.44.149 DNS names will be added through Active Directory

Uncontrolled copy when printed

F5.2 CANADA ADDRESSING

The figures F4.2-1 through F4.2-4 illustrate the network architectures for the Canadian nodes. Reach-back from the ESQNOC to PRNOC is done via GCTF infrastructure. CA SHIP 1 and CA SHIP 2 connect to the ESQNOC via SATCOM and other coalition ships via UHF SNR.

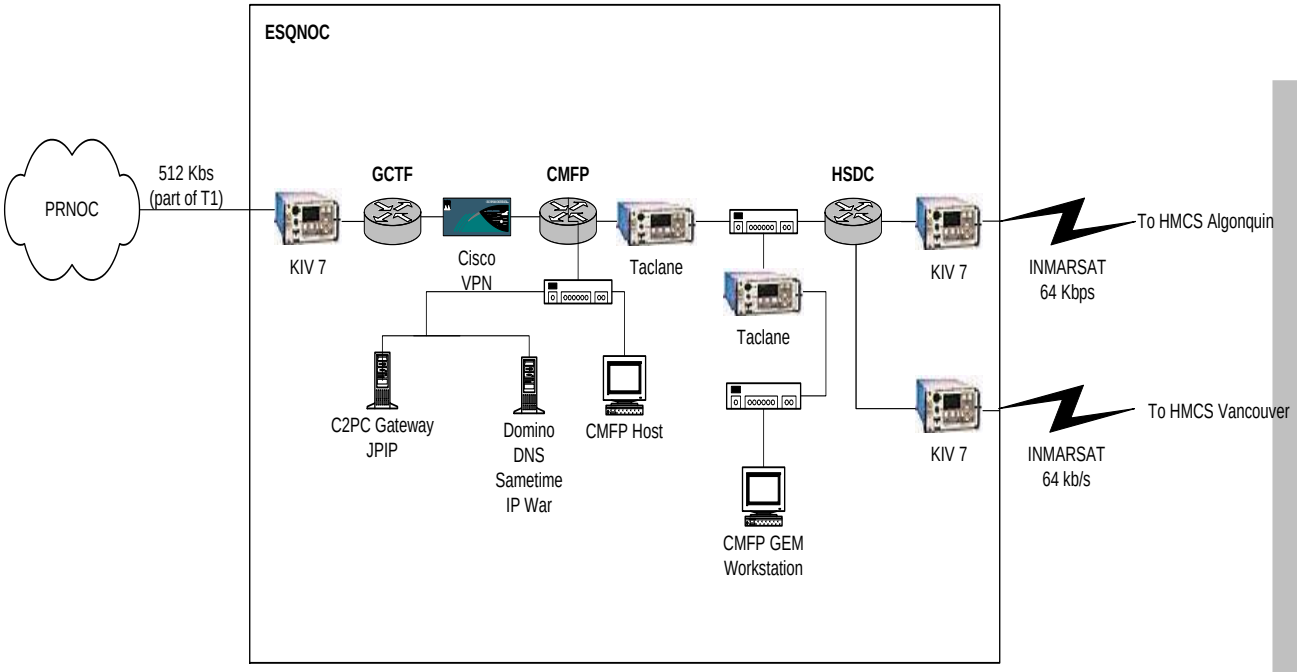

Figure F4.2-1: EXER/OPER MTWAN

Uncontrolled copy when printed

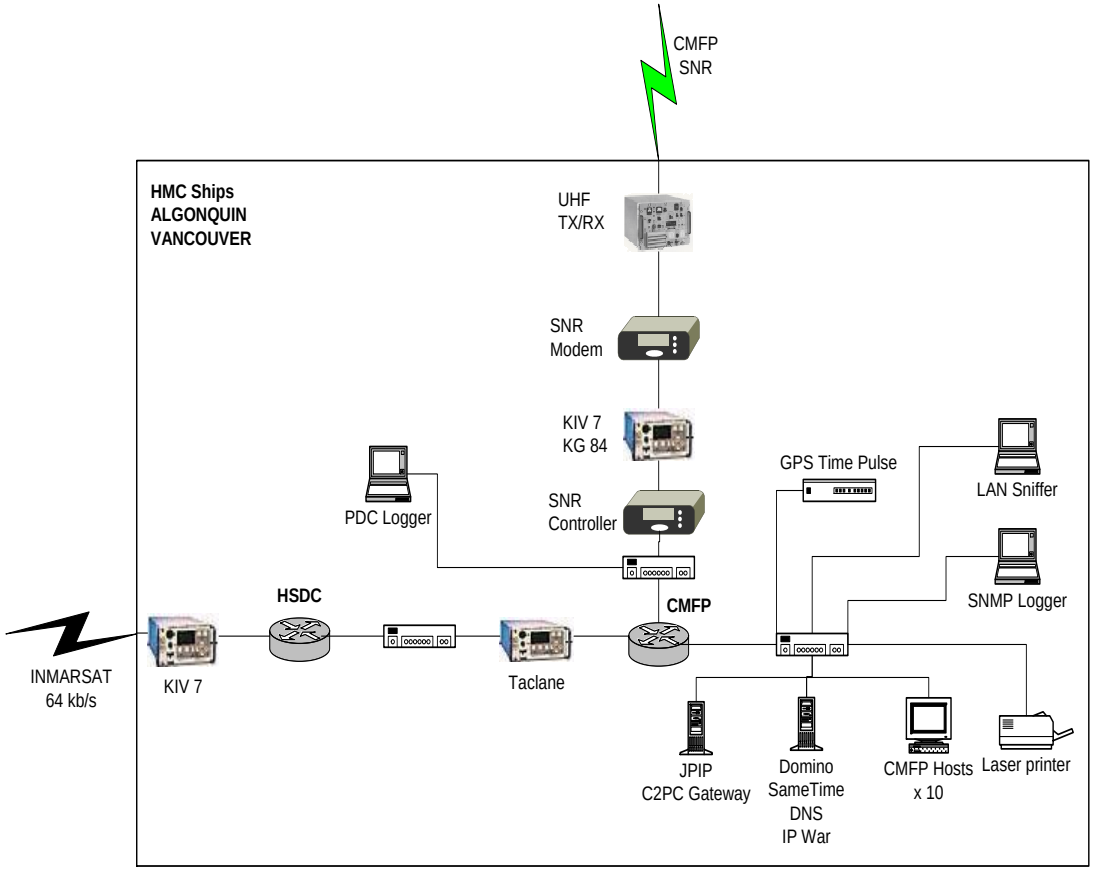

Figure F4.2-2: EXER/OPER HMC Ships MTWAN Configuration

For EXER/OPER, the following MTWAN IP addressing will be in use by ESQUIMALT NOC, CA SHIP 1 and CA SHIP 2:

Table F4.2-1: Canada MTWAN WAN/LAN IP Address Allocation

MTWAN IP ADDRESS	CA SHIP 1 (xxx.yy.32.32/27)	**CA SHIP 2** (xxx.yy.32.96/27)	**ESQUIMALT NOC** (xxx.yy.32.0/27)
VPN Concentrator (Plain Text Interface)	N/A	N/A	xxx.yy.32.30/30
Router (VPN Interface)	N/A	N/A	xxx.yy.32.29/30
NOC TO NOC (CANADA) MTWAN ROUTERS	N/A	N/A	xxx.yy.32.17/30
MTWAN ROUTER TL SUBNET	xxx.yy.32.57/30	xxx.yy.32.121/30	xxx.yy.32.25/30
MTWAN TACLANE TL SUBNET	xxx.yy.32.58/30	xxx.yy.32.122/30	xxx.yy.32.26/30

Uncontrolled copy when printed

MTWAN IP ADDRESS	CA SHIP 1 (xxx.yy.32.32/27)	CA SHIP 2 (xxx.yy.32.96/27)	ESQUIMALT NOC (xxx.yy.32.0/27)
Router (LAN Interface)	xxx.yy.32.33/27 rout.alg.navy.can.gctf-COI.cmil.mil	xxx.yy.32.97/27 rout.van.navy.can.gctf-COI.cmil.mil	xxx.yy.32.1/27 rout.esqnoc.navy.can.gctf-COI.cmil.mil
Switch (LAN)	xxx.yy.32.35/27	xxx.yy.32.99/27	xxx.yy.32.3/27
NTP Server	xxx.yy.32.37/27	xxx.yy.32.101/27	N/A
Mail Server	xxx.yy.32.36./27 mail-serv.alg.navy.can.gctf-COI.cmil.mil	xxx.yy.32.100/27 mail-serv.van.navy.can.gctf-COI.cmil.mil	xxx.yy.32.4/27 mail-serv.esqnoc.navy.can.gctf-COI.cmil.mil
DNS Server	xxx.yy.32.36./27 dns-serv.alg.navy.can.gctf-COI.cmil.mil	xxx.yy.32.100/27 dns-serv.van.navy.can.gctf-COI.cmil.mil	xxx.yy.32.4/27 dns-serv.esqnoc.navy.can.gctf-COI.cmil.mil
Domino Server	xxx.yy.32.36/27 web-serv.alg.navy.can.gctf-COI.cmil.mil	xxx.yy.32.100/27 web-serv.van.navy.can.gctf-COI.cmil.mil	xxx.yy.32.4/27 web-serv.esqnoc.navy.can.gctf-COI.cmil.mil
C2PC Client	xxx.yy.32.42/27 c2pc-wkst.alg.navy.can.gctf-COI.cmil.mil	xxx.yy.32.106/27 c2pc-wkst.van.navy.can.gctf-COI.cmil.mil	N/A
JPIP Server	xxx.yy.32.42/27 jpip-serv.alg.navy.can.gctf-COI.cmil.mil	xxx.yy.32.106/27 jpip-serv.van.navy.can.gctf-COI.cmil.mil	xxx.yy.32.11/27 jpip-serv.esqnoc.navy.can.gctf-COI.cmil.mil
Sametime / PWR Server	xxx.yy.32.36/27 dcp-serv.alg.navy.can.gctf-COI.cmil.mil	xxx.yy.32.100/27 dcp-serv.van.navy.can.gctf-COI.cmil.mil	xxx.yy.32.4/27 key-serv.esqnoc.navy.can.gctf-COI.cmil.mil
GCCS-M Server	xxx.yy.32.38/27 gccsm-serv.alg.navy.can.gctf-COI.cmil.mil	xxx.yy.32.102/27 gccsm-serv.van.navy.can.gctf-COI.cmil.mil	xxx.yy.32.6/27 gccsm-serv.esqnoc.navy.can.gctf-COI.cmil.mil

Uncontrolled copy when printed

MTWAN IP ADDRESS	CA SHIP 1 (xxx.yy.32.32/27)	CA SHIP 2 (xxx.yy.32.96/27)	ESQUIMALT NOC (xxx.yy.32.0/27)
LAN Sniffer	xxx.yy.32.40/27 sniff.alg. navy.can.gctf- COI.cmil.mil	xxx.yy.32.104/27 sniff.van. navy.can.gctf- COI.cmil.mil	N/A
Management Station(s)	xxx.yy.32.41/27 net-serv.alg. navy.can.gctf- COI.cmil.mil	xxx.yy.32.105/27 net-serv.van. navy.can.gctf- COI.cmil.mil	xxx.yy.32.11/27 net-serv.esqnoc. navy.can.gctf- COI.cmil.mil
SNR IP (router)	xxx.yy.224.100/24	xxx.yy.224.104/24	N/A
SNR IP (SCRN)	xxx.yy.224.101/24	xxx.yy.224.105/24	N/A
SCRN Module (LAN)	xx.yy.32.34/27	xxx.xy.32.98/27	N/A
Workstation(s)	xxx.yy.32.42-60./27 gen-wkst-a.alg. navy.can.gctf- COI.cmil.mil	xxx.yy.32.106- 124/27 gen-wkst-a.van. navy.can.gctf- COI.cmil.mil	xxx.yy.32.11/27 gen-wkst- a.esqnoc.navy.can.g ctf-COI.cmil.mil
GRE Tunnel	Tunnel 30 xxx.yy.39.5/30 local xxx.yy.39.6/30 remote (ESQNOC) Cost 1000	Tunnel 31 xxx.yy.39.9/30 local xxx.yy.39.10/30 remote (ESQNOC) Cost 1001	Tunnel 1 xxx.yy.39.2/30 local xxx.yy.39.1/30 remote (PRNOC) Cost 25

Uncontrolled copy when printed

F5.3 UNITED KINGDOM ADDRESSING

United Kingdom MTWAN nodes are shown in Figures F4.4-1, the UK NOC at PJHQ Northwood, and F 4.3-2, UK SHIP 1. To reach PRNOC, PJHQ Northwood must traverse links at EUCOM in Stuttgart, Germany.

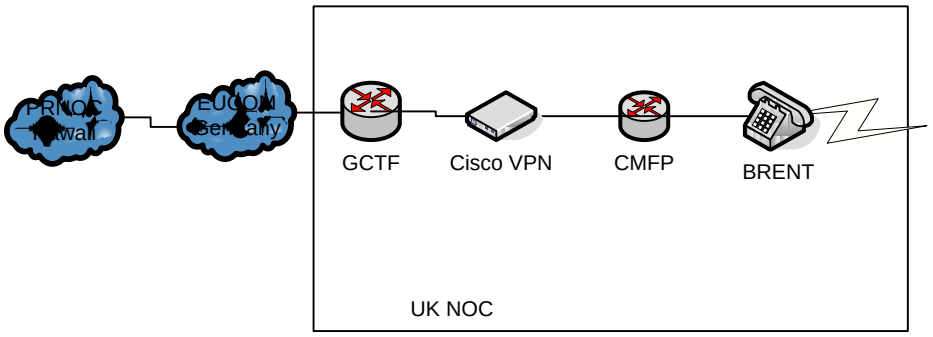

Figure 4.3-1: TW 06 UK NOC EXER/OPER MTWAN Connectivity

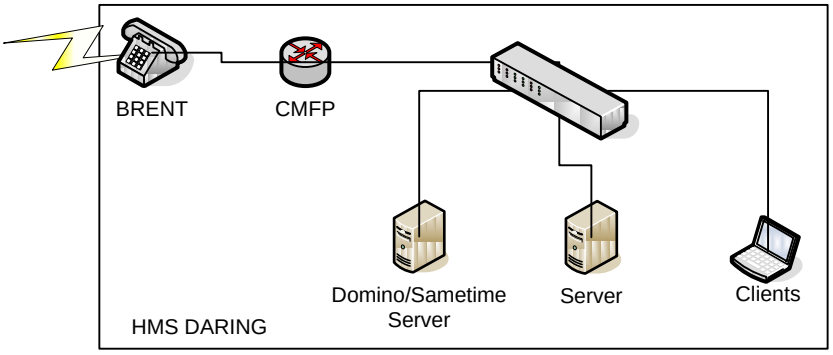

Figure 4.3-2: TW 06 UK SHIP 1 EXER/OPER MTWAN Connectivity

Uncontrolled copy when printed

For EXER/OPER, the following MTWAN IP addressing will be in use by the United Kingdom NOC at PJHQ Northwood and UK SHIP 1.

Table F4.3-1: United Kingdom MTWAN WAN/LAN IP Address Allocation

MTWAN LAN IP ADDRESS	UK SHIP 1 **(x.y.56.0/28)**	**UK NOC** **(x.y.56.32/28)**
Notes	32 addresses	32 addresses
GCTF Taclane Public Inteface	NA	NA
GCTF Taclane Private Interface	NA	NA
GCTF Router TL Subnet	NA	NA
GCTF Router VPN Subnet	NA	NA
VPN Concentrator (Public Interface)	NA	UK GCTF IP Address (classified)
VPN Concentrator (Private Interface)	x.y.56.33	x.x.56.29 vpn.uknoc.navy. gbr.gctf-COI.cmil.mil
MTWAN Router (VPN Interface)	x.x.56.34	x.x.56.30
GRE Tunnels	Tunnel 90 x.x.63.5/30 local x.y.63.6/30 remote (PRNOC) Cost 1030	Tunnel 4 x.x.63.1/30 local x.x.63.2/30 remote (PRNOC) Cost 25
MTWAN Router (LAN Interface)	xxx.yy.56.14/28 rout.darg.navy. gbr.gctf-COI.cmil.mil	xxx.yy.56.31/28 rout.uknoc.navy. gbr.gctf-COI.cmil.mil
Domino, Sametime (PWR Host), DNS Server	xxx.yy.56.2/28 web-serv.darg.navy. gbr.gctf-COI.cmil.mil dcp-serv.darg.navy. gbr.gctf-COI.cmil.mil dns-serv.darg.navy. gbr.gctf-COI.cmil.mil	

Uncontrolled copy when printed

MTWAN LAN IP ADDRESS	UK SHIP 1 **(x.y.56.0/28)**	**UK NOC** **(x.y.56.32/28)**
Mail Server	xxx.yy.56.3/28 mail-serv.darg.navy. gbr.gctf-COI.cmil.mil	NA
C2PC Gateway Server	xxx.yy.56.4/28 c2pc-serv.darg.navy. gbr.gctf-COI.cmil.mil	NA
LAN Sniffer	xxx.yy.56.8/28 sniff-a.darg.navy. gbr.gctf-COI.cmil.mil	xxx.yy.56.40/24 sniff-a.uknoc.navy. gbr.gctf-COI.cmil.mil
Management Station(s)	NA	NA
Workstation(s)	xxx.yy.56.9/28 wkst-a.darg.navy. gbr.gctf-COI.cmil.mil through wkst-e.darg.navy. gbr.gctf-COI.cmil.mil xxx.yy.56.13/28	xxx.yy.56.42/24 gen-wkst-a.uknoc.navy. gbr.gctf-COI.cmil.mil

Uncontrolled copy when printed

Table F4.3-2: United Kingdom TACLANE Sub-Network IP Address Allocation

TACLANE SUB-NETWORKS	UK SHIP 1	UK NOC
SATCOM Router	NA	NA
SATCOM TACLANE		
NOC-to-NOC Router	N/A	NA
NOC-to-NOC TACLANE	N/A	NA

Uncontrolled copy when printed

F5.4 UNITED STATES ADDRESSING

Figures F4.4-1 to F4.4-5 shows the MTWAN configurations of the US ships and shore facilities participating in EXER/OPER.

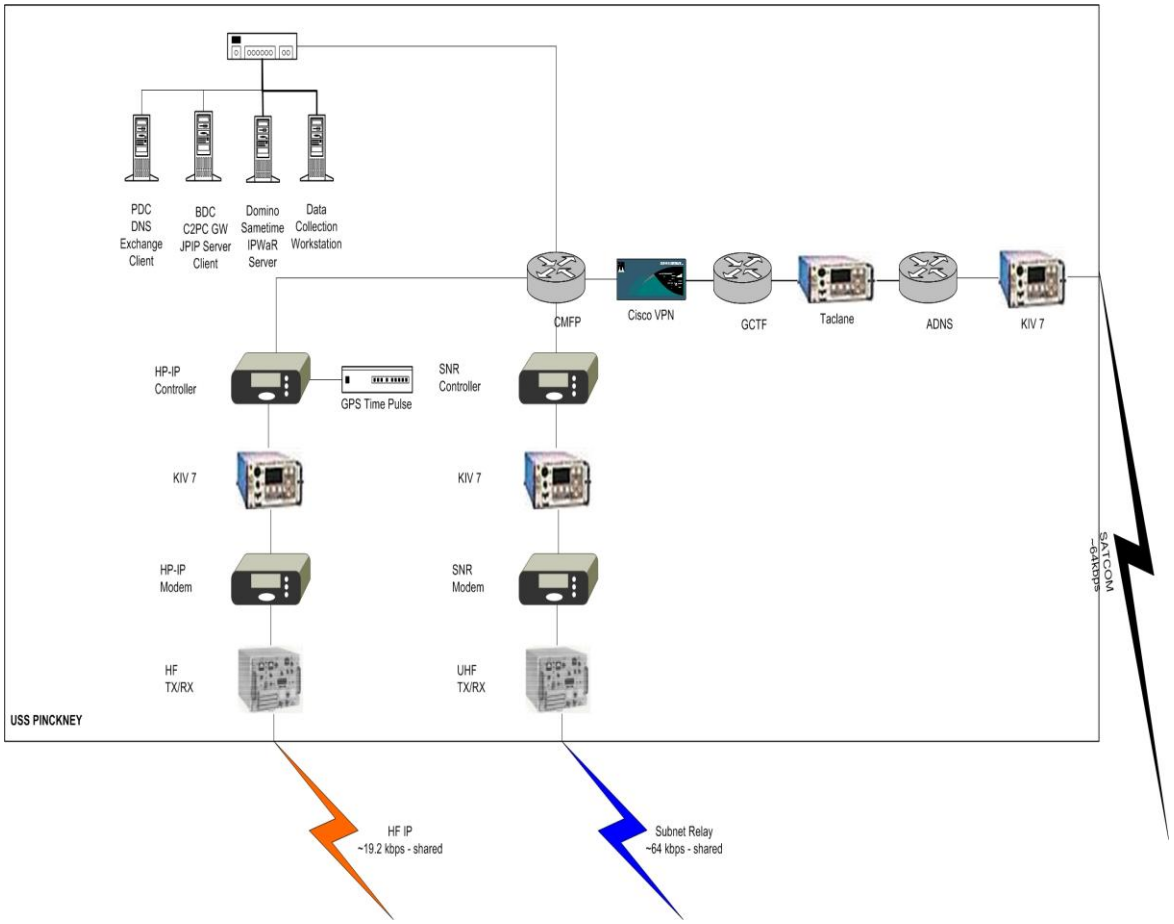

Figure 4.4-1: EXER/OPER US SHIP 2 MTWAN Configuration

Uncontrolled copy when printed

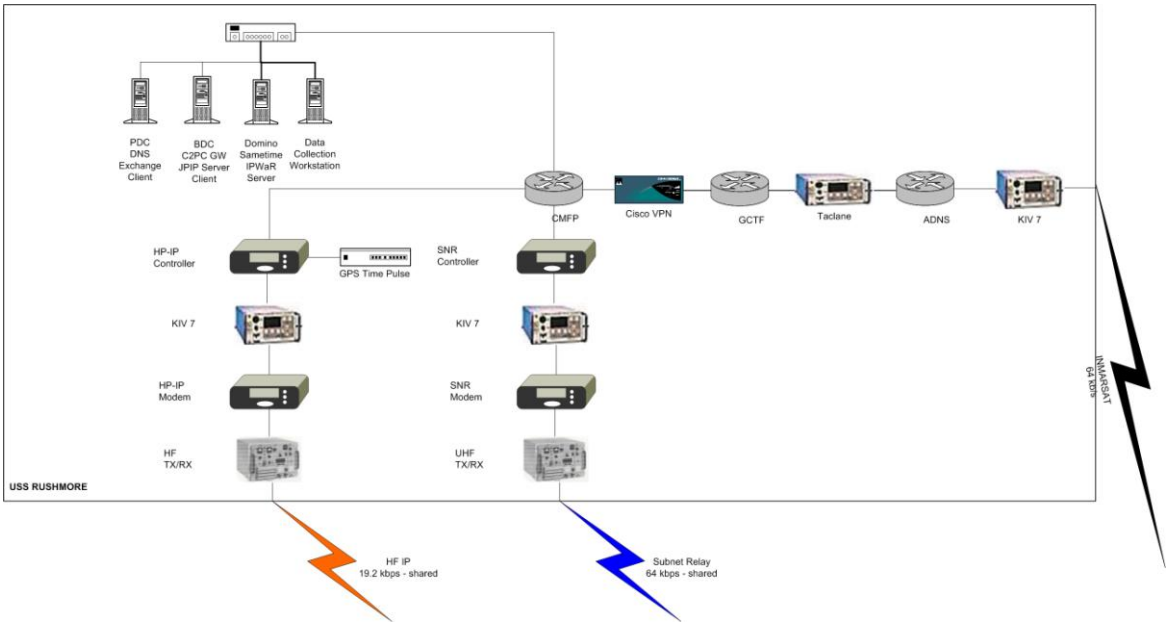

Figure 4.4-2: EXER/OPER US SHIP 3 MTWAN Configuration

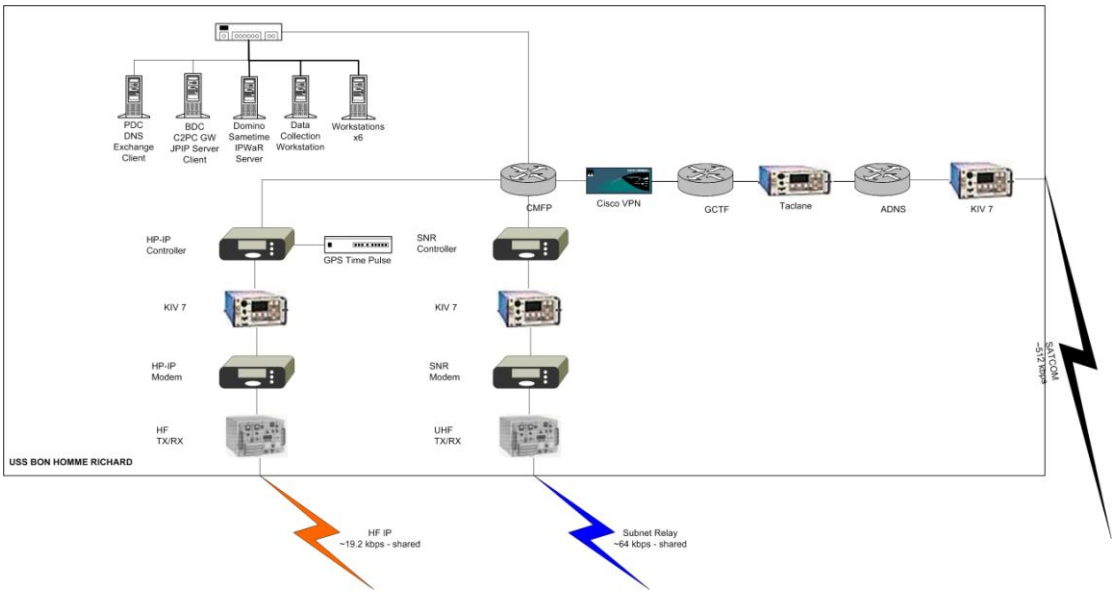

Figure 4.4-3: EXER/OPER US SHIP 1 MTWAN Configuration

Uncontrolled copy when printed

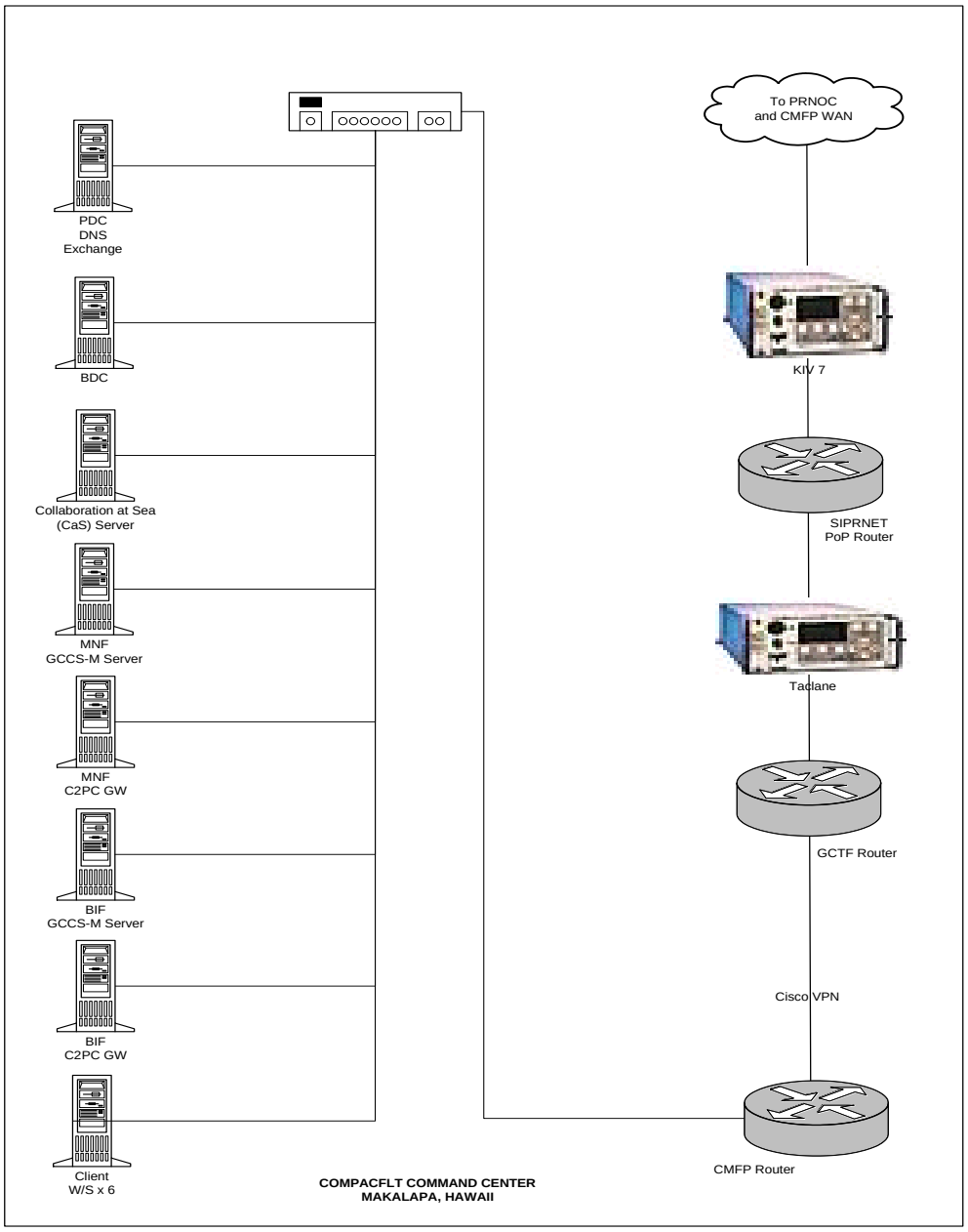

Figure 4.4-4: EXER/OPER CFMCC (COMPACFLT) MTWAN Configuration

Uncontrolled copy when printed

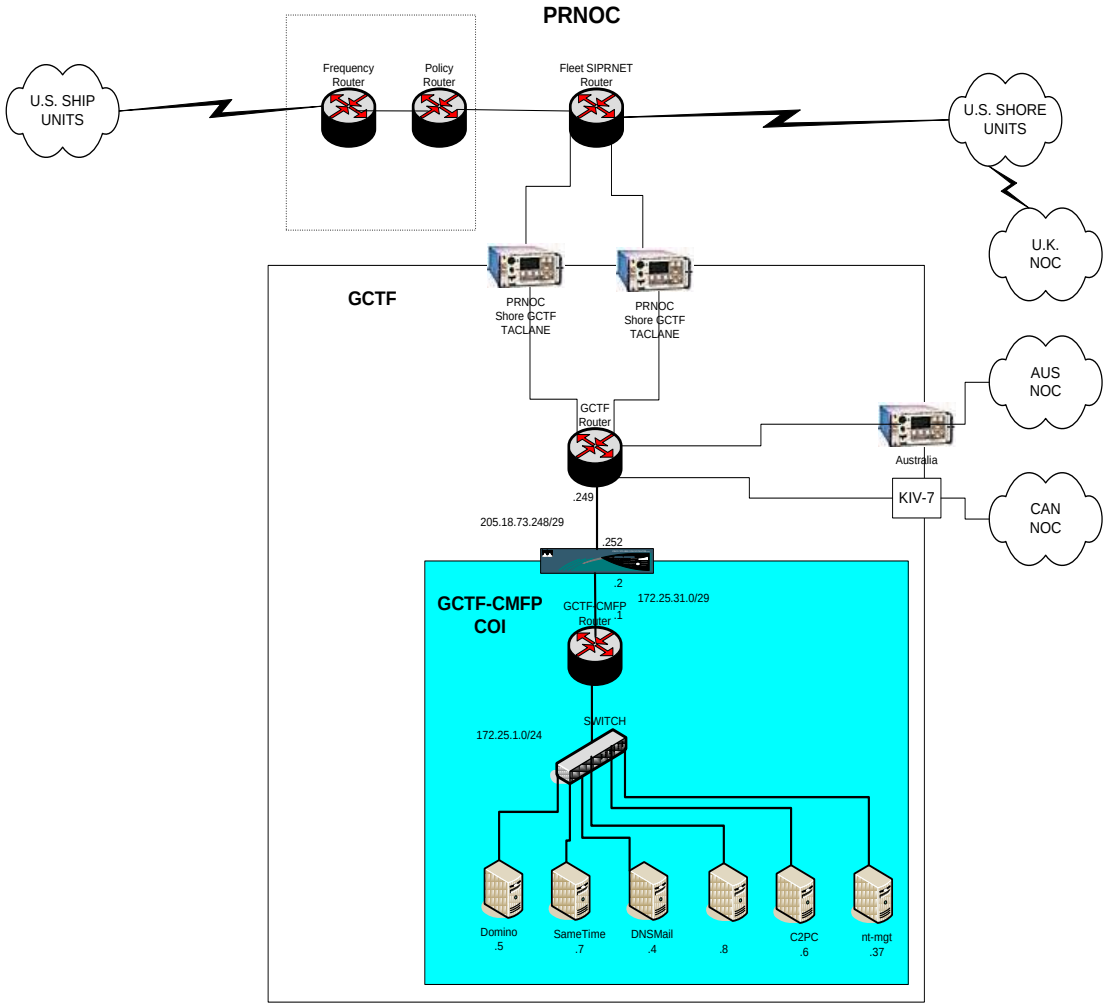

Figure 4.4-5: EXER/OPER PRNOC MTWAN Configuration

Uncontrolled copy when printed

For EXER/OPER, the following MTWAN IP addressing will be in use by PRNOC, US SHIP 2, US SHIP 3, US SHIP 1 and CFMCC at CPF HQ.

Table F4.4-1: United States MTWAN WAN/LAN IP Address Allocation

MTWAN LAN IP ADDRESS	US SHIP 1 **(x.y.2.64/28)**	**US SHIP 2** **(x.y.2.32/28)**	**US SHIP 3** **(x.y.2.128/26)**	**CFMCC CPF HQ** **(x.y.20.0/26)**	**PRNOC** **(x.y.1.0/24)**
Notes	16 addresses	16 addresses	64 addresses	64 addresses	256 addresses
GCTF Taclane Public Inteface	TBD	TBD	TBD	TBD	TBD
GCTF Taclane Private Interface	xxx.yy.66.131	xxx.yy.227.131	xxx.yy.5.131	TBD	xxx.yy.67.147
GCTF Router TL Subnet	xxx.yy.66.132	xxx.yy.227.132	xxx.yy.5.132	TBD	xxx.yy.67.148
GCTF Router VPN Subnet	xxx.yy.66.190	xxx.yy.229.190	xxx.yy.12.190	TBD	xxx.yy.73.249
VPN Concentrator Public Interface	xxx.yy.66.189	xxx.yy.229.189	xxx.yy.12.189	x.x.x.51	xxx.yy..73.252
VPN Concentrator (Private Interface)	xxx.yy.2.90/30 vpn.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.58/30 vpn.shipname.navy.usa.gctf-COI.cmil.mil	x.y.2.26/30 vpn.shipname.navy.usa.gctf-COI.cmil.mil	x.y.2.110/30 vpn.cfmcc.navy.usa.gctf-COI.cmil.mil xx.yy.20.84 /30	xxx.yy.31.2/24 vpn.prnoc.navy.usa.gctf-COI.cmil.mil
MTWAN Router (VPN Interface)	xxx.yy.2.89/30	xxx.yy.2.57/28	x.y.2.25/30	xxx.yy.2.109/30 xxx.yy.20.85 /30	xxx.yy.31.1/24
CFP Router (SNR Interface)	xxx.yy.224.5/24	xxx.yy.224.3/24	xxx.yy.224.1/24	N/A	N/A
SCRN Module	xxx.yy.224.6/24	xxx.yy.224.4/24	xxx.yy.224.2/24	N/A	N/A

Uncontrolled copy when printed

MTWAN LAN IP ADDRESS	US SHIP 1 (x.y.2.64/28)	US SHIP 2 (x.y.2.32/28)	US SHIP 3 (x.y.2.128/26)	CFMCC CPF HQ (x.y.20.0/26)	PRNOC (x.y.1.0/24)
CFP Router (HF IP Interface)	x.x.2.85/30	x.x.2.53/30	x.x.2.21/30	N/A	N/A
HF IP Router Interface	x.x.2.86/30	x.x.2.54/30	x.x.2.22/30	N/A	N/A
HF IP WAN Interface	x.x.192.3/29	x.x.192.2/29	x.x.192.1/29	N/A	N/A
GRE Tunnels	Tunnel 12 x.x.31.73/30 local x.y.31.74/30 remote (PRNOC) Cost 991	Tunnel 11 x.x.31.69/30 local x.y.31.70/30 remote (PRNOC) Cost 993	Tunnel 10 x.x.31.65/30 local x.y.31.66/30 remote (PRNOC) Cost 990	Tunnel 14 x.x.31.81/30 local x.y.31.82/30 remote (PRNOC) Cost 994 x.y.29.0 /30	
MTWAN Router (LAN Interface)	xxx.yy.2.65/28 rout.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.33/28 rout.shipname.navy.usa.gctf-COI.cmil.mil	x.y.2.129/26 rout.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.20.1/26 rout.cfmcc.navy.usa.gctf-COI.cmil.mil	xxx.yy.1.1/24 rout.prnoc.navy.usa.gctf-COI.cmil.mil
Switch	xxx.yy.2.66/28	xxx.yy.2.34/28	xxx.yy.2.130/26	xxx.yy.20.2 /26	xxx.yy.1.2/24
NTP Server	N/A	N/A	N/A	N/A	xxx.yy.1.37/24
PDC/C2PC Gateway Server	xxx.yy.2.68/28 DDG91CPD01.shipname.navy.usa.gctf-COI.cmil.mil Alias c2pc-serv.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.36/28 LSD47CPD01.shipname.navy.usa.gctf-COI.cmil.mil Alias c2pc-serv.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.131/26 LHD6MTWANDC01.lhd6.navy.usa.gctf-COI.cmil.mil Alias c2pc-serv.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.20.3 /26 mail-serv.cfmcc.navy.usa.gctf-COI.cmil.mil	xxx.yy.1.4/24 mail-serv.prnoc.navy.usa.gctf-COI.cmil.mil

Uncontrolled copy when printed

MTWAN LAN IP ADDRESS	US SHIP 1 (x.y.2.64/28)	US SHIP 2 (x.y.2.32/28)	US SHIP 3 (x.y.2.128/26)	CFMCC CPF HQ (x.y.20.0/26)	PRNOC (x.y.1.0/24)
DNS Server	xxx.yy.2.68/28 DDG91CPD01.shipname.navy.usa.gctf-COI.cmil.mil Alias dns-serv.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.36/28 LSD47CPD01.shipname.navy.usa.gctf-COI.cmil.mil Alias dns-serv.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.131/26 LHD6MTWANDC01.lhd6.navy.usa.gctf-COI.cmil.mil Alias dns-serv.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.20.4 /28 Alias dns-serv.cfmcc.navy.usa.gctf-COI.cmil.mil	xxx.yy.1.4/24 Alias dns-serv.prnoc.navy.usa.gctf-COI.cmil.mil
BDC/Exchange Mail Server	xxx.yy.2.70/28 DDG91CBD01.shipname.navy.usa.gctf-COI.cmil.mil Alias mail-serv.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.37/28 LSD47CBD01.shipnamee.navy.usa.gctf-COI.cmil.mil Alias mail-serv.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.132/26 LHD6MTWANDC02.lhd6.navy.usa.gctf-COI.cmil.mil Alias mail-serv.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.20.5 /26 c2pc-serv.cfmcc.navy.usa.gctf-COI.cmil.mil	xxx.yy.1.6/24 c2pc-serv.prnoc.navy.usa.gctf-COI.cmil.mil
Domino Server 1 Domino+Sametime (EXER/OPER)	xxx.yy.2.72/28 ____.shipname.navy.usa.gctf-COI.cmil.mil Alias web-serv.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.38/28 LSD47MTWANDS02.shipname.navy.usa.gctf-COI.cmil.mil web-serv.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.134/26 ___.lhd6.navy.usa.gctf-COI.cmil.mil Alias web-serv1.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.20.6 /26 web-serv.cfmcc.navy.usa.gctf-COI.cmil.mil	xxx.yy.1.5/24 web-serv.prnoc.navy.usa.gctf-COI.cmil.mil

Uncontrolled copy when printed

MTWAN LAN IP ADDRESS	US SHIP 1 **(x.y.2.64/28)**	**US SHIP 2** **(x.y.2.32/28)**	**US SHIP 3** **(x.y.2.128/26)**	**CFMCC CPF HQ** **(x.y.20.0/26)**	**PRNOC** **(x.y.1.0/24)**
Sametime Server (PWR Host)	xxx.yy.2.72/28 ____. shipname.navy.usa.gctf-COI.cmil.mil Alias dcp-serv. shipname. navy.usa.gctf-COI.cmil.mil	xx.yy.2.38/28 LSD47MTWANDS02.shipname.navy.usa.gctf-COI.cmil.mil Alias dcp-serv. shipname. navy.usa.gctf-COI.cmil.mil	xxx.yy.2.134/26 ___.lhd6.navy.usa.gctf-COI.cmil.mil Alias dcp-serv.shipname. navy.usa.gctf-COI.cmil.mil	N/A	xxx.yy.1.5/24 Alias dcp-serv. prnoc.navy.usa. gctf-COI.cmil.mil
Domino Server 2 Domino Only (POR/RIM PAC)	xxx.yy.2.69/28 ____. shipname.navy.usa.gctf-COI.cmil.mil Alias web-serv2.shipname. navy.usa.gctf-COI.cmil.mil	xxx.yy.2.39/28 ____. shipname.navy. usa.gctf-COI.cmil.mil Alias web-serv2.shipname . navy.usa.gctf-COI.cmil.mil	xxx.yy.2.133/26 ___.lhd6.navy.usa.gctf-COI.cmil.mil Alias web-serv2.shipname. navy.usa.gctf-COI.cmil.mil	N/A	N/A
Kakadu JPIP Server **(on DC02)**	xxx.yy.2.70/28 DDG91CBD01. shipname.navy.usa.gctf-COI.cmil.mil Alias jpip-serv.shipname. navy.usa.gctf-COI.cmil.mil	xxx.yy.2.37/28 LSD47CBD01. shipname.navy. usa.gctf-COI.cmil.mil Alias jpip-serv. shipname. navy.usa.gctf-COI.cmil.mil	xxx.yy.2.132/26 LHD6MTWANDC02. lhd6.navy.usa.gctf-COI.cmil.mil Alias jpip-serv.shipname. navy.usa.gctf-COI.cmil.mil	xxx.yy.20.7 /26 Alias jpip-serv.cfmcc. navy.usa.gctf-COI.cmil.mil	N/A

Uncontrolled copy when printed

MTWAN LAN IP ADDRESS	US SHIP 1 (x.y.2.64/28)	US SHIP 2 (x.y.2.32/28)	US SHIP 3 (x.y.2.128/26)	CFMCC CPF HQ (x.y.20.0/26)	PRNOC (x.y.1.0/24)
Kakadu Engineering JPIP Server (on DC02)	N/A	N/A	xxx.yy.2.133/26 LHD6MTWANDC02.lhd6.navy.usa.gctf-COI.cmil.mil Alias jpipeng-serv.shipname.navy.usa.gctf-COI.cmil.mil	N/A	N/A
SEADRAGON Domino Imagery Replicator	xxx,yyy.2.71	N/A	N/A	N/A	N/A
GCCS-M Server	N/A	N/A	N/A	xxx.yy.20.8 /26 gccsm-serv.cfmcc.navy.usa.gctf-COI.cmil.mil	N/A
Radiant Mercury (MTWAN Port)	N/A	N/A	N/A	xxx.yy.20.9 /26 radmerc.cfmcc.navy.usa.gctf-COI.cmil.mil	N/A
REPEAT	N/A	N/A	N/A	xxx.yy.20.10 /26 repeat.cfmcc.navy.usa.gctf-COI.cmil.mil	N/A
WebSurveyor	N/A	N/A	N/A	N/A	xxx.yy.1.14 /24 websurveyor.prnoc.navy.usa.gctf-COI.cmil.mil
F.I.R.E./ TACFIRE	N/A	N/A	N/A	N/A	xx.yy.1.20 /24 fire.prnoc.navy.usa.gctf-COI.cmil.mil

Uncontrolled copy when printed

MTWAN LAN IP ADDRESS	US SHIP 1 (x.y.2.64/28)	US SHIP 2 (x.y.2.32/28)	US SHIP 3 (x.y.2.128/26)	CFMCC CPF HQ (x.y.20.0/26)	PRNOC (x.y.1.0/24)
JDCAT (installed at PRNOC but not used)	N/A	N/A	N/A	N/A	xx.yy.1.21 jdcat.prnoc.navy.usa.gctf-COI.cmil.mil
LAN Sniffer	xxx.yy.2.76/28 sniff-a.shipname.navy.usa.gctf-COI.cmil.mil xxx.yy.2.77/28 sniff-b.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.40/28 sniff-a.shipname.navy.usa.gctf-COI.cmil.mil xxx.yy.2.41/28 sniff-b.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.2.188/26 ___.lhd6.navy.usa.gctf-COI.cmil.mil Alias sniff-a.shipname.navy.usa.gctf-COI.cmil.mil xxx.yy.2.189/26 ___.lhd6.navy.usa.gctf-COI.cmil.mil Alias sniff-b.shipname.navy.usa.gctf-COI.cmil.mil	xxx.yy.20.11 /26 sniff-a.cfmcc.navy.usa.gctf-COI.cmil.mil	sniff-a.prnoc.navy.usa.gctf-COI.cmil.mil
Management Station(s)	N/A	N/A	xxx.yy.2.140 ___.lhd6.navy.usa.gctf-COI.cmil.mil Alias net-serv.shipname.navy.usa.gctf-COI.cmil.mil	N/A	xxx.yy.1.15/24 netserv.prnoc.navy.usa.gctf-COI.cmil.mil
CCL+ Chat Language Translator	N/A	N/A	N/A	N/A	xx.yy..1.10/24 ccl-serv.prnoc.navy.usa.gctf-MTWAN.navy.mil

Uncontrolled copy when printed

MTWAN LAN IP ADDRESS	US SHIP 1 (x.y.2.64/28)	US SHIP 2 (x.y.2.32/28)	US SHIP 3 (x.y.2.128/26)	CFMCC CPF HQ (x.y.20.0/26)	PRNOC (x.y.1.0/24)
Work-station(s)	N/A	N/A	10 workstations xxx.yy.2.138/26 to x.y.2.147/26 wkst-a.shipname.navy.usa.gctf-COI.cmil.mil to wkst-i.shipname.navy.usa.gctf-COI.cmil.mil Available IP addresses for extra worksstations x.y.2.140/26 to x.y.2.186/26	Available IP addresses for workstations xxxx.yy.2.12 /26 to xxx.yy.20.63 /26 wkst-a.cfmcc.navy.usa.gctf-COI.cmil.mil to wkst-xx.cfmcc.navy.usa.gctf-COI.cmil.mil	xxx.yy.1.60/24 gen-wkst-a.prnoc.navy.usa.gctf-COI.cmil.mil

Uncontrolled copy when printed

Table F4.4-2: United States SNR IP Address Allocation

SNR IP ADDRESS	US SHIP 1	US SHIP 2	US SHIP 3
Router	xxx.yy.224.5/24	xxx.yy.224.3/24	xxx.yy.224.1/24
SCRN Module	xxx.yy.224.6/24	xxx.yy.224.4/24	xxx.yy.224.2/24

Table F4.4-3: United States TACLANE Sub-Network IP Address Allocation

TACLANE SUB-NETWORKS	US SHIP 1	US SHIP 2	US SHIP 3	CFMCC CPF HQ	PRNOC
SATCOM Router					
SATCOM TACLANE					
NOC-to-NOC Router					
NOC-to-NOC TACLANE					

Uncontrolled copy when printed

G. APPLICATIONS

The Applications section delineates the specific applications used within the context of this NCP along with pertinent amplifying information.

G1. MESSAGING

Nations participating in EXER/OPER will use either MS-Exchange or IBM-Lotus Domino as their mail server. Domino Secure Web Mail will be used for sending secure messages.

G1.1 MS-Exchange Mail Server

During EXER/OPER, the United States will be using MS-Exchange 2000 as their secondary e-mail server. All Exchange mail servers will be configured to deliver mail via SMTP using DNS MX record lookups to locate the recipients' mail server. The DNS will be configured with each zone advertising two MX records, with the higher priority MX record pointing to the local SMTP mail server and the lower priority MX record pointing to the unit's national NOC SMTP mail server. This will facilitate ship-to-ship mail delivery if a ship-to-ship network path exists. If the recipient's server is not contactable then the mail will be delivered to, and queued at the unit's national NOC server and delivered to the recipient when the connection is available.

G1.2 IBM-Lotus Domino Web Mail and Secure Web Mail Server

During EXER/OPER, all nations will be using Domino 6.5.1 IF 2 Web Mail and Secure Web Mail as their primary mail server and Client.

G2. COMMON OPERATIONAL PICTURE (COP)

G2.1 Coalition COP Architecture

The EXER/OPER Coalition COP Distribution Architecture will use the EXER/OPER COP Distribution Architecture, which is shown in Figure G2.1-1. It is a two-tiered model, with the upper tier using COP Synchronization Tools (CST) to share the COP with National COP servers and the lower tier connecting via C2PC Gateways. A GCCS-M Communications server, located at the COMPACFLT Command Center, will send the EXER/OPER US National COP to a Radiant Mercury guard device located at USPACOM. The Radiant Mercury will process the track information it receives, appropriately sanitize the track data and send it to a MTWAN GCCS-M 3.1.2.1P1 Communications Server also located at USPACOM. This server will use CST to synchronize the track databases at GCCS-M servers in Australia, Canada, the United Kingdom and two servers at COMPACFLT.

The CPF COP servers will each have an associated C2PC Gateway. Gateway to Gateway connections will be established with the other ships to provide them with the Coalition COP. The RIMPAC Multinational Force (MNF) C2PC Gateway will provide the Coalition COP to AUS SHIP 1, AUS SHIP 2, CA SHIP 1, CA SHIP 2 and CA SHIP 3. The RIMPAC Bi-National Force (BIF) C2PC Gateway will provide the Coalition COP to US SHIP 1 and US Ship 3MORE.

In addition to the C2PC Gateway connections with COMPACFLT, the United States and Canada will be prepared to establish C2PC Gateway connections between SNR equipped ships in support of EXER/OPER experimentation. At the end of EXER/OPER experimentation, all C2PC Gateways will be re-homed to the appropriate COMPACFLT gateway.

Uncontrolled copy when printed

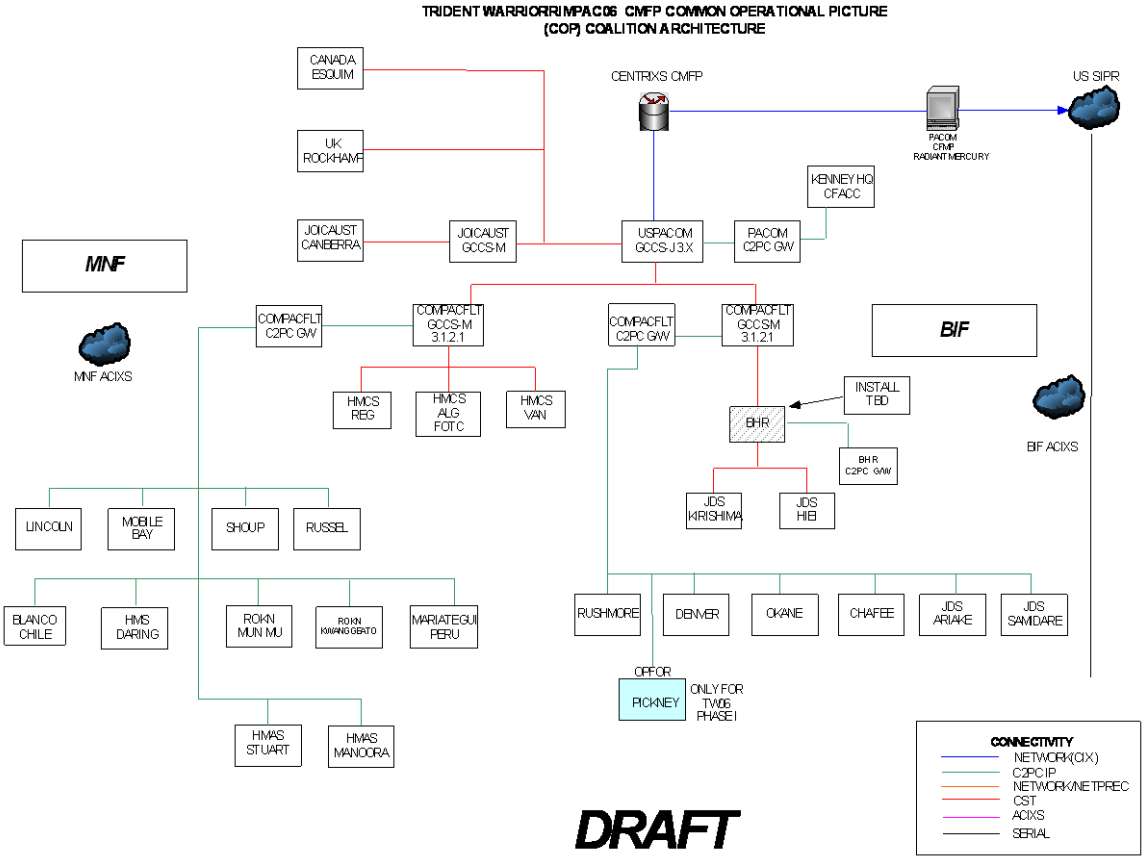

Figure G2.1-1: EXER/OPER Coalition COP Distribution Architecture

G2.2 GCCS-M and C2PC Information

Table G2.1-1 contains the GCCS-M and C2PC information required to establish COP distribution for EXER/OPER.

Uncontrolled copy when printed

Table G2.2-1: GCCS-M and C2PC Information

Unit	GCCS-M Version	GCCS-M Server IP Address	UID	C2PC Version	C2PC Gateway IP Address	Hostname	COP Source
AUS SHIP 1	3.1.2.1 P1	xxx.yy.47.254	SHIPNAME	**5.8.2**	xxx.yy.45.150/26 c2pc-serv.shipname.navy.aus.gctf-COI.cmil.mil	c2pc-serv.shipname.navy.aus.gctf-COI.cmil.mil	CPF MNF C2PC Gateway
AUS SHIP 2	3.1.2.1 P1	xxx.yy.34.253	STU	5.8.2	xxx.yy.45.150/26 c2pc-serv.shipname.navy.aus.gctf-COI.cmil.mil	STUSDN01.shipname.aus.gctf-COI.cmil.mil	CPF MNF C2PC Gateway
AUNOC	N/A	N/A	AUNOC	5.8.2	N/A	N/A	N/A
CA SHIP 1	3.1.2.1 P1	xxx.yy.32.38/28	ALG	N/A	N/A	N/A	CPF MNF GCCS-M Server
CA SHIP 2	3.1.2.1 P1	xxx.yy.32.102/27	VAN	N/A	N/A	N/A	CPF MNF GCCS-M Server
ESQUIMALT NOC	N/A	N/A	N/A	N/A	N/A	N/A	N/A
UK SHIP 1	N/A	N/A	DAR	???	x.y.56.4	dargc2pcgw c2pc-serv.shipname.navy.gbr.gctf-COI.cmil.mil	CPF MNF C2PC Gateway
PJHQ NOC	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Uncontrolled copy when printed

Unit	GCCS-M Version	GCCS-M Server IP Address	UID	C2PC Version	C2PC Gateway IP Address	Hostname	COP Source
US SHIP 1	N/A	N/A	SHIPNAME	**???**	x.y.2.6 C2PC Application Netmask: xxx.yy.255.255	shipnamec2pcgw c2pc-serv.shipname.navy.usa.gctf-COI.cmil.mil	CPF BIF C2PC Gateway and/or CPF BIF GCCS-M
US SHIP 2	N/A	N/A	PNK	**???**	x.y.2.38 C2PC Application Netmask: xxx.yy.255.255	shipnamec2pcgw c2pc-serv.shipname.navy.usa.gctf-COI.cmil.mil	CPF BIF C2PC Gateway
US SHIP 3	N/A	N/A	RSH	**???**	x.y.2.70 C2PC Application Netmask: xxx.yy.255.255	shipnamec2pcgw c2pc-serv.shipname.navy.usa.gctf-COI.cmil.mil	CPF BIF C2PC Gateway
CPF CFMCC MNF GCCS-M	3.1.2.1P1	x.y.21.2	PF1	5.9.0.3	x.y.21.4 C2PC Application Netmask: xxx.yy.255.255	**GCCS-M:** cpfmnf.cpf.navy.usa.gctf-COI.cmil.mil **C2PC:** c2pcmnf.cpf.navy.usa.gctf-COI.cmil.mil	USPACOM MTWAN GCCS Server
CPF CFMCC BIF GCCS-M	3.1.2.1P1	x.y.21.3	PF2	5.9.0.3	x.y.21.5 C2PC Netmask: xxx.yy.255.255	**GCCS-M:** cpfbif.cpf.navy.usa.gctf-COI.cmil.mil **C2PC:** c2pcbif.cpf.navy.usa.gctf-COI.cmil.mil	USPACOM MTWAN GCCS Server

Uncontrolled copy when printed

Unit	GCCS-M Version	GCCS-M Server IP Address	UID	C2PC Version	C2PC Gateway IP Address	Hostname	COP Source
Radiant Mercury	4.05 P2	???	N/A	N/A	N/A	N/A	N/A

G3. WEB SERVICES

G3.1 Web Browser Information

G3.1.1 Minimum Internet Explorer Version

The minimum Internet Explorer version must IE 5.5 or later in order to work properly with Persistent War Room

G3.1.2 Java Version

Use the JAVA version on the MTWAN Web Server. The link is located on the hub page. As of 7 FEB, this could either be SUN JAVA 1.5 or MS JVM version 3810.

G3.2 Lotus Domino Configuration

G3.2.1 Lotus Domino Version

The IBM Lotus Domino version required for use in EXER/OPER is Domino R6.5.1. Exact executable and associated ID files will be provided by Collaboration at Sea team.

G3.2.2 Domino Server Naming Schema and Configuration for EXER/OPER

The Domino Domain naming schema to be implemented in EXER/OPER is:

[Server Name (CN)] / [Country (OU1)] / [Organization (O)] @ Domino Domain

Where
Domino Domain Name: MTWAN
O = MTWAN
OU1 = AUS, CAN, NZL, GBR, or USA
CN = UNIT_NAME

The Domino Domain naming schema to be implemented in EXER/OPER is setup as follows shipname/country/CFP which can also be represented as

[Server Name (CN)] / [Country (OU1)] / [Organization (O)] @ Domino Domain

Where
Domino Domain Name: COI

Uncontrolled copy when printed

O = COI
OU1 = AUS, CAN, NZL, GBR, or USA)
CN = UNIT/SITE NAME

EXER/OPER will use all capital letters in the Domino Domain naming based on Lesson Learned from JWID03 and 04, where Domino Name and Address Book entries were found to be Case Sensitive. Server id's are already created and are mixed case as with all domains.

Table G3.2.2 - 1 delineates the Ships, Domino Domain Names, and Fully Qualified Domain Names and to be used in EXER/OPER.

Table G3.2.2–1: EXER/OPER Unit, Domino Domain and Fully Qualified Domain Names

Unit	Domino Domain Name	FQDN
AU NOC	N/A	N/A
AUS SHIP 1		web-serv.shipname.navy.aus.gctf-COI.cmil.mil
AUS SHIP 2		web-serv.shipname.navy.aus.gctf-COI.cmil.mil
CA NOC		web-serv.canoc.navy.can.gctf-COI.cmil.mil
CA SHIP 1		web-serv.shipname.navy.can.gctf-COI.cmil.mil
CA SHIP 2		web-serv.shipname.navy.can.gctf-COI.cmil.mil
CA SHIP 3		web-serv.shipname.navy.can.gctf-COI.cmil.mil
UK NOC		web-serv.uknoc.navy.gbr.gctf-COI.cmil.mil
UK SHIP 1		web-serv.shipname.navy.gbr.gctf-COI.cmil.mil
PRNOC		web-serv.prnoc.navy.usa.gctf-COI.cmil.mil
US SHIP 1		web-serv.shipname.navy.usa.gctf-COI.cmil.mil
US SHIP 2		web-serv.shipname.navy.usa.gctf-COI.cmil.mil
US SHIP 3		web-serv. shipname.navy.usa.gctf-COI.cmil.mil
CFMCC		web-serv.cfmcc.navy.usa.gctf-COI.cmil.mil

G3.2.3 Domino Administration

Domino Administration will be managed from PRNOC and requests for change to connection documents and addressing in support of SNR must be communicated to the Administrators at PRNOC for coordination and configuration.

Nations will be allowed Local Domino Administrator privileges.

Uncontrolled copy when printed

G3.2.4 The Domino User Naming schema for EXER/OPER

EXER/OPER will employ a limited number of Role-based accounts for watch standers, as well as User or Person-based accounts. When using Role-based accounts as a watch stander, particularly during chat sessions, operators must indicate who they are to the chat room(s) when signing in at the beginning of a watch. The ship must also maintain an audit trail of who was officially on watch and when.

G3.2.4.1 Group or Role-based Accounts

Group or Role-based accounts are those accounts which are used for more than one unique user. For Role-based accounts, the EXER/OPER Domino user naming convention (to the left of the @ character) is *<3-5 letter unit identifier>*, and *<3-5 letter position identifier>*. For example, the CA SHIP 1 would have user names such as OPS ALG or ORO ALG. To facilitate the use of Directory Lookup feature of Outlook (via Domino LDAP), the Domino User Identification (ID) will be as follows:

First Name = position; and
Last Name = ship/site.

Example:

ORO of the CA SHIP 1
First Name = ORO
Last Name = ALG

The Domino Short Name will be the **[Role + Unit]**, in this example – ORO ALG.

LDAP Directory Lookup = ALG, ORO

Sametime and PWR buddy list would display as **ALG ORO**, allowing operators to easily identify and sort chat users by unit.

Uncontrolled copy when printed

G3.2.4.2 User, or Person-based, Accounts

Person-based accounts will utilize the standard First Name – Last Name method to differentiate between Role-based accounts as well as facilitate the use of the Directory Look up feature of Outlook via Domino LDAP.

Accounts will be created through the registration website on the Domino domain whereby user accounts will be formatted First MI Last/Country-Command/CFP.

National Domino system administrators are to email **cashelp@fset.navy.mil** and request the Domino ID files and other supporting files and documentation.

Uncontrolled copy when printed

G3.2.4.3 Essential EXER/OPER Domino Accounts

The following Domino accounts must be established in order to support EXER/OPER Domino, Sametime and Persistent War Room usage during EXER/OPER.

Table G3.2.4.3-1: Essential Domino Accounts for EXER/OPER

Position	Domino Name	SMTP Address
AU NOC		
NOC Help Desk	RANFLEETHELPAU	ranfleethelpau@aunoc.navy.aus.gctf-COI.cmil.mil
AUS SHIP 1		
Principal Warfare Officer	AUS SHIP 1 PWO	pwo@shipname.navy.aus.gctf-COI.cmil.mil
CIS Officer	AUS SHIP 1 CIS	cis@shipname.navy.aus.gctf-COI.cmil.mil
AUS SHIP 2		
Principal Warfare Officer	AUS SHIP 2 PWO	pwo@shipname.navy.aus.gctf-COI.cmil.mil
CIS Officer	AUS SHIP 2 CIS	cis@shipname.navy.aus.gctf-COI.cmil.mil
CA NOC		
NOC Help Desk		
CA SHIP 1		
Operations Room Officer	CA SHIP 1 ORO	oro@shipname.navy.can.gctf-COI.cmil.mil
Operations Room Supervisor	CA SHIP 1 ORS	ors@shipname.navy.can.gctf-COI.cmil.mil
Technical Engineer		
CA SHIP 2		
Operations Room Officer	CA SHIP 2ORO	oro@shipname.navy.can.gctf-COI.cmil.mil
Operations Room Supervisor	CA SHIP 2 ORS	ors@shipname.navy.can.gctf-COI.cmil.mil
Technical Engineer		
UK NOC		
OSC Watch keeper	DCSA Northwood	dcsa.nwd@dharg.navy.gbr.gctf-COI.cmil.mil
UK SHIP 1		
Principal Warfare Officer	AUS SHIP 1 PWO	pwo@shipname.navy.gbr.gctf-COI.cmil.mil
Operations Officer	AUS SHIP 1 OPS	ops@shipname.navy.gbr.gctf-COI.cmil.mil

Uncontrolled copy when printed

PRNOC		
PRNOC Help Desk	PRNOC	prnoc@prnoc.navy.usa.gctf-COI.cmil.mil
CaS Help Desk	CASHELP	cashelp@prnoc.navy.usa.gctf-COI.cmil.mil
US SHIP 1		
Tactical Action Officer	US SHIP 1 TAO	tao@shipname-web.navy.usa.gctf-COI.cmil.mil
Radio Watch Supervisor	US SHIP 1 RADIO	radio@shipname-web.navy.usa.gctf-COI.cmil.mil
Coalition Chief Engineer		
Coalition Initiative Lead		
Coalition Data Coordinator		
Coalition Liaison Officer		
SNR Engineer		
HF IP Engineer		
Coalition HIS		
US SHIP 2		
Tactical Action Officer	US SHIP 2 TAO	tao@shipname-web.navy.usa.gctf-COI.cmil.mil
Radio Watch Supervisor	US SHIP 2 RADIO	radio@shipname-web.navy.usa.gctf-COI.cmil.mil
SNR Engineer		
HF IP Engineer		

Uncontrolled copy when printed

US SHIP 3		
Tactical Action Officer	US SHIP 3 TAO	tao@shipname-web.navy.usa.gctf-COI.cmil.mil
Radio Watch Supervisor	US SHIP 3 RADIO	radio@shipname-web.navy.usa.gctf-COI.cmil.mil
SNR Engineer		
HF IP Engineer		
CFMCC		
Tactical Action Officer	CFMCC TAO	tao@cfmcc-web.navy.usa.gctf-COI.cmil.mil
Operations Officer	CFMCC OPS	ops@cfmcc-web.navy.usa.gctf-COI.cmil.mil

Uncontrolled copy when printed

G3.2.5 Domino Replication Topology

During the initial setup and configuration of EXER/OPER Domino servers, all replication will be done directly with PRNOC in a hub-spoke topology.

Prior to the EXER/OPER underway period, PRNOC will alter the replication topology to a two stage topology where a national hub ship will be the focal point of Task Group replication. This is illustrated in Figure G3.2.5-1. In the first stage, all national NOCs and gateway ships will replicate with PRNOC. In the second stage, the remaining ships will replicate with the hub ship. This two-stage replication topology will facilitate experimentation of Multi-Topology Routing of Domino traffic over SNR and HF IP.

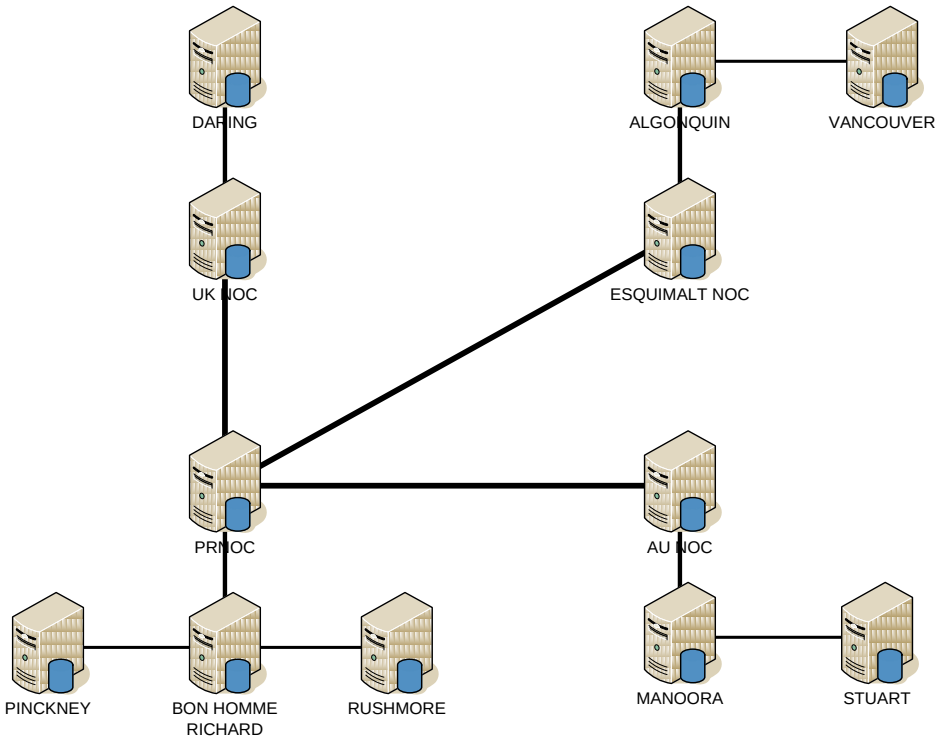

Figure G3.2.5–1: EXER/OPER MTWAN Domino Replication Topology

Uncontrolled copy when printed

G3.2.6 Domino Connection Documents

G3.2.6.1 Domino Web Connection Documents

The following units will have their Connection Documents configured so that they replicate with the Domino Hub Server at PRNOC:

AU NOC
ESQUIMALT NOC
UK NOC
US SHIP 1

The following units will have their Connections Documents configured so that they replicate with the AU NOC:

AUS SHIP 1

The following units will have their Connections Documents configured so that they replicate with the ESQUIMALT NOC:

CA SHIP 1

The following units will have their Connections Documents configured so that they replicate with the UK NOC:

UK SHIP 1

The following units will have their Connections Documents configured so that they replicate with AUS SHIP 1, which will act as a Hub Server for AUS afloat units:

AUS SHIP 2

The following units will have their Connections Documents configured so that they replicate with CA SHIP 1, which will act as a Hub Server for CAN afloat units:

CA SHIP 2

The following units will have their Connection Documents configured so that they replicate with the Domino Server on US SHIP 1, which will act as a Hub Server for the US afloat units:

US SHIP 2
US SHIP 3

Each replication path will have three replication documents, one to replicate the CAS web page databases, one to replicate the ITSessions database, and the other to replicate the Administrative databases.

Uncontrolled copy when printed

G3.2.6.2 Sametime Connection Documents

To create a full mesh of Sametime servers, the Domino/Sametime server on each ship shall have a Sametime connection document to all other ships and shore servers. These connection documents are required to share awareness information between the Sametime servers and for proper operation of Sametime and Persistent War Room clients in a fully meshed environment.

G3.2.6.2.1 AUSTRALIA

G3.2.6.2.2 CANADA

G3.2.6.2.3 UNITED KINGDOM

G3.2.6.2.4 UNITED STATES

G3.2.6.3 Mail Connection Documents

G3.2.7 REPLICATION SCHEDULES

EXER/OPER Coalition web pages will be replicated at 20-minute intervals unless otherwise changed by the CTG COMMANDER. Since the SNR and HF IP units replicate with a hub ship, these units will be 1 replication cycle behind those units replicating directly with PRNOC. On a 20-minute replication schedule, it will take 40 minutes or more for the information to reach the SNR/HF IP ships.

Administrative databases will be replicated every 60 minutes.

The Persistent War Room database, itsessions.nsf, will be replicated every two minutes.

G3.2.8 DOMINO ADDRESS BOOK

The Domino Name and Address Book will be used as the EXER/OPER LDAP Directory Service.

G3.2.9 Root Administrative Server

The PRNOC Domino server will be setup first and therefore will be the root admin server for the MTWAN Domino Domain. Each additional server will need to be entered into the names.nsf database and a gold setup disk created. This gold disk will then be distributed to all nations and used when setting up the servers. Each additional server will also need to connect and a full replication performed with the PRNOC server 2-3 times.

The PRNOC Domino server will be setup first and therefore will be the root admin server for the CFP Domino Domain. PRNOC will produce ID files for all of the EXER/OPER servers. They will advise countries of the download location on the CFP Network for NAMES.NSF, ADMIN4.NSF and ID Files when nations are ready to install their Domino servers. Once

Uncontrolled copy when printed

built, each additional server will need to replicate and synchronize with the PRNOC Hub Server.

G4. DISTRIBUTED COLLABORATIVE PLANNING

G4.1 Lotus Sametime

G4.1.1 Sametime Version

IBM-Lotus Sametime version 6.5.1 IF2 (Intermediate Fix 2) shall be used on the MTWAN Sametime Server.

G4.1.2 Sametime Configuration

For EXER/OPER, Sametime shall be used in a distributed configuration, with Sametime servers located on all EXER/OPER units and sites.

G4.1.3 Sametime Audio and Video

Sametime Audio/Video capabilities will be disabled for EXER/OPER. There are no plans to use these capabilities over SATCOM, SNR or HF IP at any time during Trident Warrior.

G4.2 Instant Persisent War Room (IPWaR)

Instant Persistent War Room is composed of Instant Technologies Team Sessions (chat persistence) software. Teams Sessions version V2 Build 6 shall be used during EXER/OPER.

G4.3 EXER/OPER Sametime and IPWaR Topology

EXER/OPER will configure Instant Persistent War Room (Teams Sessions) in the "Multiple Sametime Servers + Multiple Domino Servers" architecture, shown in Figure G4.3-1. In addition to the Collaboration at Sea (CaS) Domino servers at each node, a Sametime server will also be added as an additional service. This configuration takes advantage of Domino servers already fitted onboard the ships and shore nodes that support CaS replicated web sites, eliminating the requirement to fit separate Sametime server hardware on the ship or shore node. All users will be hosted on the Sametime Server at their site. The chat side of the collaboration room is connected directly from the workstation to the local Sametime server. The local Sametime servers will exchange Chat, Awareness and other information between each other. Chat logging (persistence) will be done on the Master Server at PRNOC.

Users have the same replication and local storage advantages as they would in a distributed, multiple Sametime server environment. Team Sessions applets will be replicated to local Domino servers. IPWaR will be initialized by accessing the applet from the local Domino server and then caching it in the local web browser. This eliminates the requirement to download the 4.7 Mbyte JAVA applet from the PRNOC server and prevents unnecessary applet traffic from traversing the MTWAN WAN. Users will have to wait for replication of

Uncontrolled copy when printed

data before information appears in “tabbed” areas or newly created rooms can be seen or accessed, which should be on the order of 3-5 minutes.

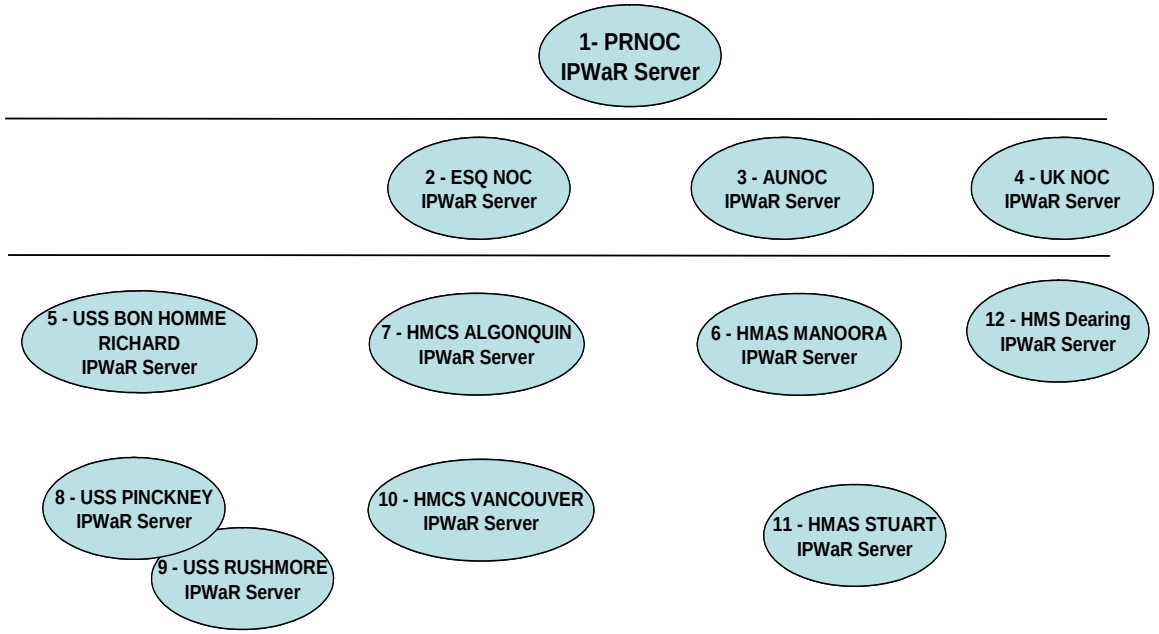

Figure G4.3-1: EXER/OPER IPWaR Server Hierarchy

Figure G4.3-2 illustrates an IPWaR architecture containing multiple Domino and Multiple Sametime servers. This drawing shows 5 nodes in a full mesh environment. A drawing showing all 12 nodes in the EXER/OPER environment would be much too busy for easy analysis. In EXER/OPER, a mesh of Domino/Sametime servers will be established. The goal is to minimize off-ship IPWaR traffic and utilize the Sametime server federation functionality in conjunction with IPWaR.

Uncontrolled copy when printed

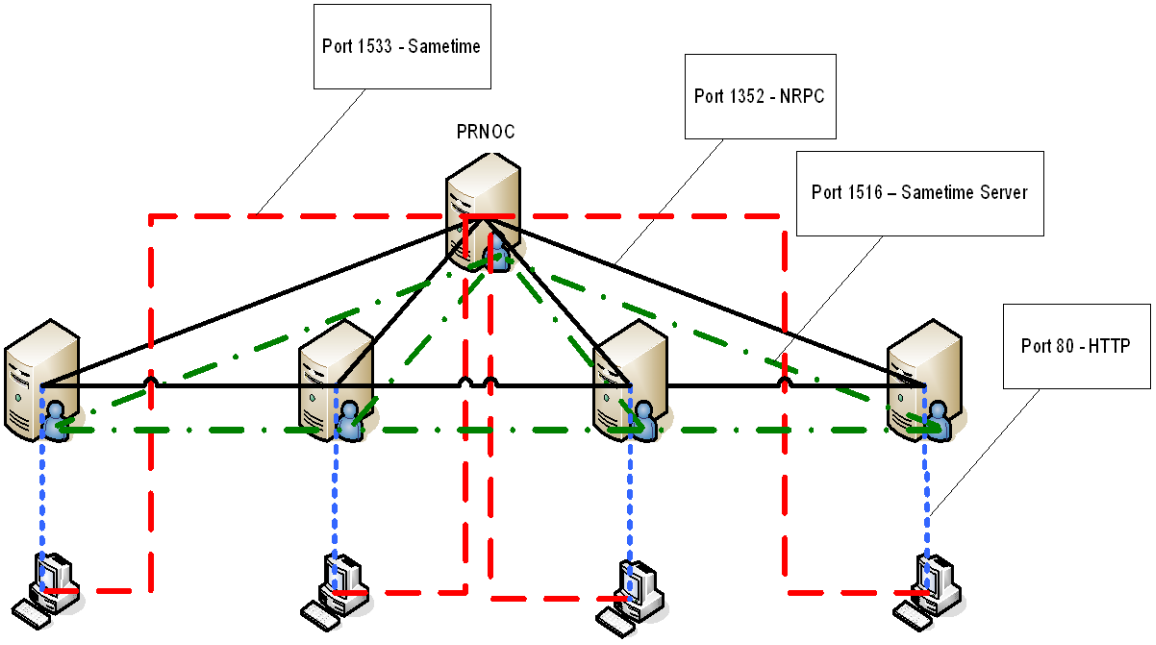

Figure G4.3-2: EXER/OPER IPWaR Multiple Sametime Server Architecture

In this configuration, all HTTP traffic from the local user workstation goes to the local Domino server. The Domino servers replicate with the PRNOC Hub server using Notes Remote Procedure Calls (NRPC) over Port 1352. The Sametime servers communicate with each other in a full mesh environment over Port 1516. All IPWaR Instant TeamSessions traffic will go from the client to the PRNOC Sametime server on Port 1533.

Uncontrolled copy when printed

G5. JPEG 2000 INTERACTIVE PROTOCOL (JPIP)

The JPEG 2000 image compression standard supports interactive access to large images for bandwidth-disadvantaged mobile units by offering progressive refinement and a highly efficient compression mechanism. During EXER/OPER, two JPIP server and client variants will be trialed; the Australian KAKAKDU server and client and the Canadian Idelix server and client (formerly ITT/Kodak).

Table G5-1: JPIP Servers and Platforms

Unit/Site	Kakadu Server 4.5	Idelix Server
AUNOC	No	No
AUS SHIP 1	Yes	Yes
AUS SHIP 2	Yes	Yes
ESQUIMALT NOC	No	Yes
CA SHIP 1	No	Yes
CA SHIP 2	No	Yes
UK SHIP 1	Yes	No
PRNOC	No	No
US SHIP 1	Yes	No
US SHIP 2	Yes	No
US SHIP 3	Yes	No
COMPACFLT	No	No

Uncontrolled copy when printed

G5.1 KAKADU JPIP SERVER

During EXER/OPER, KAKADU JPIP server version 4.5 will be hosted aboard multiple platforms and sites with the goal to work towards a more distributed environment.

G5.1.1 Kakadu Server Installation

1. Create the following directory on a hard drive, C:\JPEG2000

2. Copy the following files to the directory created in Step 1:

kdu_server.exe
kdu_v45R.dll
run_kakadu_server.bat

Edit the run_kakdu_server.bat file so that it has the switches and parameters set in accordance with the example below and Table G6.1.1-1.

kdu_server -max_rate 2000 -time 1800 -port 5000 -clients 24 –sources 16 -max_rtt 16

-initial_timeout 16 -completion_timeout 64 –max_chunk_size 8192 –connection_threads 5

-log C:\jpeg2000\logs\kdu_server.log -wd c:\jpeg2000\images

Start a “Command Prompt” window

Click “Start” – “Run”

Type “**cmd**” (without the quotes) in the Run window. This should bring up a DOS command prompt window

Working in the Command Prompt window, change the current working directory to the directory created in Step 1 - **cd c:\jpeg2000 .**

Start the Kakadu JPEG 2000 server by executing the “run_kakadu_server.bat” file. Type “run_kakadu_server” (without the quotes) in the Command Prompt Window. This should start the JPIP server.

Uncontrolled copy when printed

G5.1.2 Kakadu JPIP Server Configuration Parameters

Table G6.1.2-1 delineates the Kakadu JPIP server configuration settings.

Table G5.1.2-1: Kakadu ver. 4.5 Server Parameters

Parameter	Settings	Comment
max_rate	2000	Max. data rate (bytes/sec) at which data will be sent to any given client
Time	1800	Max. client connection time in seconds
Port	5000	Listen for JPIP requests on this port
Clients	24	max. number of clients served simultaneously
Sources	16	max. number of different images that can be served simultaneously
max_rtt	16	Max. value (seconds) to be used as server's target round-trip time (RTT)
initial_timeout	16	Specifies the timeout value (seconds) to use for the handshaking which is used to establish persistent connection channels
completion_timeout	64	Time (seconds) within which the client must complete all persistent connections
max_chunk	8192	Max. size (bytes) of image data chunks sent by server. 8192 or 16384 seemed to be the best settings for SNR and HF IP from the RR LOE.
connection_threads	5	Max. number of threads dedicated to managing the establishment of new connections.
Log	C:\jpeg2000\logs\kdu_server.log	Log file
Wd	C:\jpeg2000\images	Working directory for imagery

Uncontrolled copy when printed

G5.2 KAKADU JPIP CLIENT

Kakadu Client version 4.5 will be loaded on EXER/OPER workstations. Users will access the JPEG2000 server via the web browser and the JPIP protocol.

G5.2.1 Kakadu Client Installation

1. Create a directory on a hard drive, C:\JPEG2000

2. Copy the following files to the directory created in Step 1:

   a. kdu_show.exe

   b. kdu_v45R.dll

3. Start a "Command Prompt" window

4. Change the current working directory to the directory created in Step 1, e.g. cd c:\jpeg2000

5. Run the kdu_show.exe file once *(kdu-show will register itself with Internet Explorer as the target for URLs commencing with "jpip://", that is "kdu_show" will be run automatically from IE whenever a URL commencing with "jpip://" is encountered)*

6. Exit "kdu_show".

G5.2.2 JPIP Image Browsing

1. Start IE

2. Enter the URL of the selected image, for EXER/OPER this should be

   jpip://jpip-serv.aunoc.navy.aus.gctf-cfp.cmil.mil:5000/<filename>.jp2

3. This starts the Kakadu client and the download of the selected image.

4. Zoom in an area of the image. There are two ways to select an area.

   a. Position the cursor at the Top Left Hand corner of the area

   b. Hold down the Left Mouse button

   c. Drag the cursor to the Bottom Right Hand corner of the area

   d. Release the mouse button

   e. Click on the button showing the Plus (+) sign

Uncontrolled copy when printed

OR:

a. Position the cursor at the Top Left Hand corner of the area

b. Click the Left Mouse button

c. Position the cursor at the Bottom Right Hand corner of the area

d. Click the Left Mouse button

e. Click on the button showing the Plus (+) sign

5. The operator is also able to Pan the image, right and left and up and down.

G5.3 Idelix JPIP Server (Canada)

An objective of EXER/OPER is to demonstrate that the IDELIX JPEG2000 implementation is a bandwidth efficient mechanism for image transfer to HMC Ships. IDELIX offers means to adapt the transmission to changing channel conditions allowing an efficient transmission of the summary data. It provides selective access to the image metadata that may be contained within JPEG 2000 files, thus allowing users on HMC Ships to extract portions of images and reducing the total number of packets used to transfer the complete image.

An IDELIX server will be located at the Esquimalt NOC and on CA SHIP 1 and CA SHIP 2. This will allow users to extract image data with the utilization of the IDELIX client locally via the onboard MTWAN workstations.

G5.4 Idelix JPIP Client

IDELIX Software Inc. specializes in the design and integration of advanced visualization technologies. The Pliable Display Technology (PDT) developed by IDELIX enhances the visualization capabilities of the host JPEG2000 applications. The PDT Software Development Kits (SDKs) enable developers to integrate detail-in-context viewing and editing techniques within their applications to address the growing concerns of information overload in 2D and 3D applications. The IDELIX PDT lens acts as a direct user interface to the data being displayed. PDT lenses can provide a unique combination of precision, speed and improved situational awareness to users that are performing visually intensive tasks. The IDELIX client is launched, when the user points the Internet Explorer browser to a specific port on the IDELIX server, searching for a specific image.

G6. WEBSURVEYOR

WebSurveyor is a COTS, web-based survey tool that collects survey data for Sea Trial - Trident Warrior experimentation. Each survey will have a unique URL that will be resident in the CENTRIXS-MTWAN WebSurveyor server located at the PRNOC. Operators will be prompted to go to a specific URL and take surveys at designated times, using their web browser, from their respective work stations. There is no client required for the user PC.

Uncontrolled copy when printed

Bandwidth usage for this process is minimal, simply the transfer of survey HTML text. No pictures or logos will be included within the surveys.

PRNOC will host three (3) rack mounted WebSurveyor servers, one for each network, (CENTRIXS, SIPR, and NIPR). All computers will have identical software loads and function identically. All equipment, hardware, and installation will be satisfied by the Naval Postgraduate School. During the Trident Warrior Experiment, the Naval Postgraduate School will have personnel present at PRNOC to satisfy any unanticipated repair requirements.

G7. MINIMUM EXER/OPER CLIENT SOFTWARE BASELINE

Table G7-1 delineates the minimum software baseline required by clients for EXER/OPER. Dependencies exist for Persistent War Room.

Persistent War Room requires MS Internet Explorer version 5.5 or later in order in order for the client to operate properly.

Instant Persistent War Room (IPWaR) V2 B8 was successfully tested with SUN Java 1.5 and MS JVM 3810 during the EXER/OPER Coalition Risk Reduction LOE. However as of mid-April, V2 B6 will be the MTWAN IPWaR standard load pending further operational testing.

Table G7-1: EXER/OPER Minimum Client Software Baseline

Application	Minimum Version	Preferred Version	Dependency
Client Operating System	Windows 2000, SP4 DISA STIG	Windows 2000, SP4, DISA STIG	
E-mail Client	Domino Web Mail	Domino Web Mail	Domino Server
Web Browser	Internet Explorer 5.5	Internet Explorer 6.01	Persistent War Room
SUN Java	1.4.2	1.5	Persistent War Room
MS JVM	3810	3810	Persistent War Room
C2PC	5.8	5.9.0.3 P4	GCCS-M and COP
Adobe Reader	5.0	7.0	none
WinZip	7.0	7.0	none
JPIP Client	Kakadu 4.5	Kakadu 4.5	none
Instant Technologies Team Sessions	V2 B6	V2 B6	Persistent War Room Client
Sametime Connect Client	6.5.1	6.5.1	Sametime Server
NxPowerlite	1.5	1.53	none

Uncontrolled copy when printed

H. NETWORK MANAGEMENT

H1. NETWORK MANAGEMENT INFORMATION

Units are to provide regular network status using automated updates (e.g. Whatsup Gold) via local web services. National NOCs will provide the appropriate URL or URLs. The NOC will maintain a help desk to address network issues at least one hour before start of EXER/OPER day and at least one hour after close of EXER/OPER day. NOCs will provide at least one regular telephone line for EXER/OPER usage.

PRNOC and CaS Help Desk support hours will be 0600-2300 Hawaii Standard Time (1600-0900Z).

H1.1 AUSTRALIA

Network status information can be obtained at the following URLs:

AUNOC: http://net-serv. aunoc.navy.aus.gctf-COI.cmil.mil/cacti

AUS SHIP 1: http://net-serv.shipname.navy.aus.gctf-COI.cmil.mil/cacti

AUS SHIP 2: http://net-serv.stu.navy.aus.gctf-COI.cmil.mil/cacti

H1.2 CANADA

Network status information can be obtained at the following URLs:

Esquimalt NOC:

CA SHIP 1

CA SHIP 2

H1.3 UNITED KINGDOM

Network status information can be obtained at the following URLs:

UKNOC

UK SHIP 1

H1.2 UNITED STATES

Network status information can be obtained at the following URLs:

PRNOC Whatsup Gold URL: http://whatsup.prnoc.navy.usa.gctf-COI.cmil.mil

US SHIP 1

Uncontrolled copy when printed

US SHIP 2

US SHIP 3

H2. NETWORK MANAGEMENT POC

For NOC POCS please refer to Table C-1.

H3. NTP ARCHITECTURE

PRNOC will maintain an NTP Server on its nt-mgmt server. Each Country will maintain an NTP Server in their respective NOC. Each Country will synchronize their device with respective NTP server.

Uncontrolled copy when printed

CHAPTER 4

TRANSPORT SERVICES

INTRODUCTION

401. Maritime platform communication systems are bandwidth constrained and subject to high latency (transmission delay) and high bit error rates as a result of having to use SATCOM or other RF bearers. The shore environment is typically characterized by wired and fixed communications systems of high bandwidth, low latency, and low bit error rates. In addition to latency, IP networks built on wired and fixed communications systems are also subject to jitter (variation in latency) and packet loss due to network congestion and transmission errors. Networking over SATCOM further aggravates these problems with higher bit error rate, higher latency, and larger jitter due to atmospheric conditions and distance of signal propagation. Networking over RF multi-member nets aggravates these problems even further due to media access control mechanisms and bit error rates higher that those of SATCOM.

AIM

402. The aim of this chapter is to explain why IP-based applications may not perform as well as expected in a MTWAN. This chapter also describes techniques and strategies that may be implemented in a MTWAN to improve degraded application performance caused by the characteristics of networking over RF links.

OVERVIEW

403. End user applications use either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) as their transport layer protocol. Applications such as Web services, e-mail, chat, file transfers, and GCCS-M (or equivalent) require reliable data transmission and therefore were designed to make use of TCP. Other data types such as Voice over IP (VoIP) and Video, which can tolerate a small number of packet losses but are sensitive to latency and jitter, often use UDP.

404. TCP is a connection-oriented protocol, which has control mechanisms in the form of TCP headers that facilitate robust and reliable data transfer from source to destination. TCP also uses a 4-way session protocol that sets up a source to destination link, confirms the receipt of the packet, actions a request for the next packet, and tears down a link after the data transfer is complete.

405. TCP compensates for lost packets and transmission errors. TCP also responds to network congestion by adjusting its transmission rate. This process requires acknowledgements by the destination and flow-control commands, which makes a TCP connection susceptible to the Round Trip Time (RTT) of the network, which is normally used to measure the latency.

Uncontrolled copy when printed

406. Although TCP provides a reliable data transfer mechanism that guarantees packet delivery, it has significant network overhead as compared to UDP.

407. UDP is a connectionless transport protocol, as it does not establish an end-to-end connection between the sender and the receiver before data is sent. UDP does not guarantee the delivery of the data to the destination, or that data packets will be delivered to the destination in the order in which they were sent by the source, and it does not detect duplicate packets. However, it does provide data integrity using checksums that are added to data packets by the sender before transmission. The lack of flow and congestion control mechanisms makes this protocol inherently unreliable. However, the overhead per packet is significantly lower than TCP, thus making it a more efficient protocol to use in low bandwidth networks.

408. As UDP does not detect lost or out-of-sequence data packets, applications that use UDP must implement some form of error detection and correction to guarantee successful delivery of data in the correct order at the destination. In addition, UDP does not provide flow or congestion control, therefore applications using UDP as their transport protocol should have their transmission rates restricted so that they do not monopolize the WAN link.

Uncontrolled copy when printed

TCP OVER HIGH LATENCY LINKS

409. TCP provides reliable point-to-point transmissions, however the performance of TCP is susceptible to packet loss caused by network congestion and transmission errors and latency.

410. TCP was originally developed for wired terrestrial links that have low latency and low transmission error. SATCOM and multi-member RF nets have higher latency and higher transmission error rates which can result in frequent IP datagram retransmissions. In addition, the flow and congestion control mechanisms of TCP may severely restrict the TCP throughput that can be achieved over a WAN link, resulting in the available bandwidth of the link not being fully utilized.

411. To achieve reliable transmissions, the sender expects an acknowledgement (ACK) for each successful receipt of a packet. If the ACK is not received, the sender resends the packet. Often, on a high latency link the packet is retransmitted before the ACK has time to arrive, adding to unnecessary traffic on the WAN. To accomplish flow control to avoid network congestion, TCP uses a sliding window to limit the amount of data that can be sent before receiving an ACK from the destination. This could result in inefficient use of available bandwidth.

412. To avoid congestion, TCP implements a slow-start mechanism, which restricts the transmission rate at the beginning of a data transfer. Furthermore, TCP will reduce its transmission rate if it does not receive an ACK for a packet after a pre-set timeout. TCP assumes that the packet has been lost due to congestion if no ACK is received before the pre-set timeout period expires. This assumption is not always true because the ACK can

arrive late due to a high latency network. The packet may have also been discarded due to transmission errors.

IP FRAGMENTATION

413. In-line Network Encryptors (INE) such as TACLANE enable networks of different security classifications to share the same communications link in a more efficient way, in comparison to multiplexing techniques based on circuit switching. However, the use of INE will increase the IP packet size due to the overhead imposed by the encryption process, and this will have an effect on the Maximum Transmission Unit (MTU) size that can be tolerated before fragmentation takes place. Fragmentation will increase network latency and therefore reduce application performance.

414. The MTU size is the maximum number of bytes that can be transmitted as a single IP packet over a network. The maximum MTU size for an Ethernet network is 1500 bytes. Any packet that exceeds this size will be fragmented into two new packets if the original packet is not marked “Don’t Fragment”. The network will discard packets that cannot be fragmented. At the packet’s final destination, the fragments of a packet will be reassembled before forwarding to the transport layer.

415. A solution to the fragmentation is to set the MTU to a smaller value in order to allow the INE overhead to be added without taking the datagram size over 1500 bytes. One must also be cognizant of the fact that the size of the INE overhead varies depending on the encryption algorithm used. The use of routing mechanisms, such as Generic Routing Encapsulation (GRE) tunnels, will also introduce additional overheads that need to be addressed in determining appropriate MTU size. A further consideration with the MTU size is that if it is too small, the efficiency of data throughput over the WAN will be significantly reduced.

PERFORMANCE ENHANCING TECHNIQUES

416. Performance enhancing techniques offer a more efficient use of limited bandwidth and tolerance of high latency and high bit-error rate. Any performance enhancing techniques employed must be transparent to applications. These techniques can be grouped into four categories:

a. TCP acceleration;

b. Multicasting;

c. Compression; and

d. Caching.

417. These techniques are discussed in the following sections.

Uncontrolled copy when printed

418. TCP Acceleration is used to overcome the limitations of TCP in a maritime environment. One technique is known as “TCP Spoofing”: this is where ACK replies are generated locally, making the WAN link appear to TCP to be a high data rate lossless connection. In doing so, the high reliability of TCP is maintained without the detrimental effects of flow control mechanisms causing the link to be inefficiently used.

419. Another technique to enhance WAN performance is to use another transport protocol across high latency, high error rate links. In this case, a proxy device is placed at either end of the WAN link. The proxy device then converts the TCP to a transport protocol better suited to low data rate, high bit error, and high latency links. The destination proxy converts the received data back to TCP, thus appearing transparent to sender and receiver.

420. Other acceleration techniques may be employed and there are several others being developed. Generally, acceleration devices are integrated into WAN Optimizers. WAN Optimizers are discussed later in this chapter.

421. Multicast Gateways are designed to provide reliable multicast data services over a WAN. These gateways are located on the LAN side of a router and transparently convert a TCP connection into a multicast transfer, using an application transport protocol, such as MDP (Multicast Dissemination Protocol), which runs on top of UDP. Figure 4-1 illustrates the operation of multicast routing and multicast gateways.

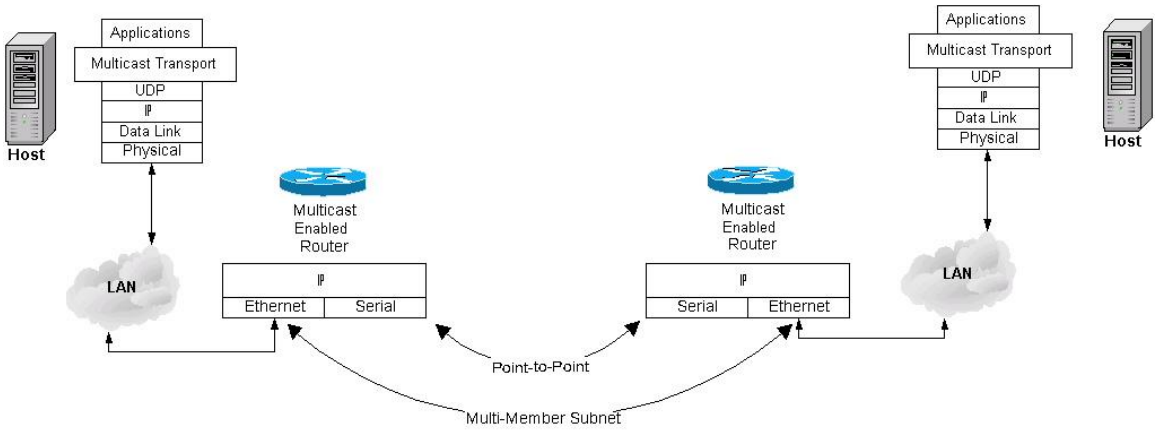

Figure 4-1 Multicasting and Multicast Gateways

Uncontrolled copy when printed

422. As UDP is an unreliable transport protocol, the multicast gateways must implement some form of error control to guarantee successful delivery of the UDP datagrams.

423. In addition, UDP does not provide flow or congestion control, therefore the multicast gateways should have their transmission rate restricted so that they will not monopolize the WAN link.

424. Multicast implementation is normally hindered by the lack of multicast gateways and multicast-capable networks. Several multicast gateways for SMTP E-mail, FTP, Text Chat, and OTH-GOLD messaging, have been developed by AUSCANNZUKUS nations, although none have reached the point where they can be operationally deployed.

425. Compression – If data is compressible and repetitive, lossless data compression techniques can be used to reduce the number of bits to be sent over a WAN link using some form of compression or pattern matching and replacement.

426. A device sitting between the LAN and its router normally carries out compression. The same device is required at the destination to restore incoming compressed data to its original state. It should be noted that compression will not work efficiently on data that is already compressed such as voice and video datagrams, pre-compressed files, and encrypted data (e.g. VPN or INE encrypted data). Current compression technologies typically yield a 2:1 to 5:1 savings in bandwidth for a typical mix of applications.

427. Caching saves bandwidth and improves application performance by storing a copy of data, which is accessed frequently or was previously retrieved by a user over the WAN, in a cache on the user's local LAN. Whenever the user requests access to the data, the cache will transparently intercept the user's request and respond directly to the user. If the cache does not have a copy of the requested data, it then retrieves it from the source.

428. WAN Optimizers are typically multi-function devices that can incorporate several WAN optimization techniques, including Data Compression, Caching, Traffic Marking and Shaping (QoS policy enforcement), TCP Acceleration, and Network Monitoring. Presently, these WAN Optimization techniques are vendor specific and generally not interoperable with each other. By installing such devices, the overall WAN efficiency and use of the available bandwidth can be increased.

429. A compression ratio of 2:1 may effectively double the bandwidth. For example, the effective throughput for a 64Kbps link can attain 128Kbps. However, an increase in bandwidth does not typically translate directly into an improvement in performance of mission-critical applications because there is no guarantee that the added bandwidth will be used by these mission-critical applications. In addition to compression, WAN Optimizers usually offer traffic shaping where applications will be guaranteed a defined

Uncontrolled copy when printed

minimum amount of bandwidth and will be able to access to excess bandwidth, or can have their traffic limited to a defined maximum amount of bandwidth.

430. WAN Optimizers allow users to control how the bandwidth is used on the fly without having to reload routers with new QoS policies. The reloading of routers with new configurations will cause disruption to the network.

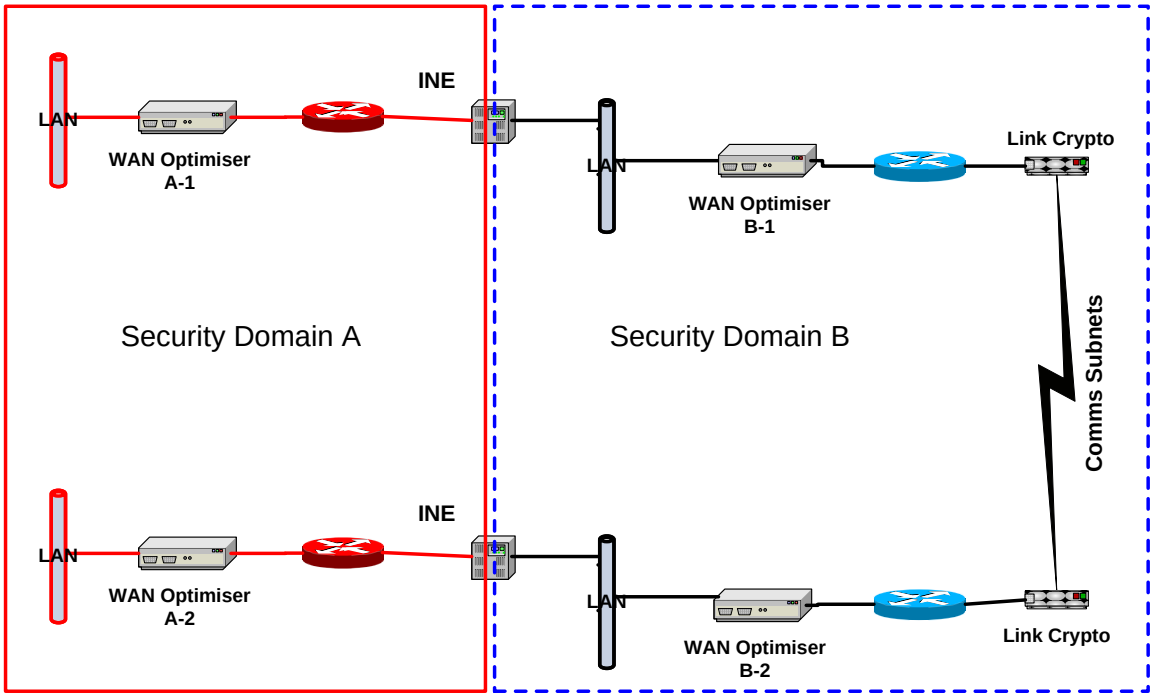

Figure 4-2 WAN Optimizers

431. Figure 4-2 shows a typical deployment of WAN Optimizers in an MTWAN where IP traffic of one security domain is tunneled through a network of a different security domain using INEs. WAN Optimizers A-1 and A-2 can be used to compress, cache, monitor, and shape traffic from Security Domain A. As IP traffic from Security Domain A will be encrypted by the INEs before it arrives at WAN Optimizers B-1 and B-2, these optimizers will not be able to compress it, or exercise control over individual applications or TCP connections of the Security Domain A.

Uncontrolled copy when printed

CHAPTER 5

NETWORK NAMING AND ADDRESSING

INTRODUCTION

501. There are three important aspects for naming and addressing within a MTWAN: the allocation of IP addresses, the assignment of unique names for the network domains and computers, and the installation and management of Domain Name Service (DNS) servers that support the network.

AIM

502. This chapter defines how names and addresses for entities can be allocated and managed.

OVERVIEW

503. One of the major activities in establishing any mobile tactical network (especially allied and coalition networks) is to identify and promulgate the names and addresses of network elements, including attached end systems and workstations.

504. Addresses should be allocated with attention to the network topology in order to maximise the efficiency of routing information distribution, and hence the data throughput.

505. Any MTWAN DNS has to be linked to the DNS structure of other appropriate national and coalition networks in order to provide address information to-from these other networks.

HOST NAMING CONVENTION

506. Used to generate the names for individual pieces of equipment (such as computers, printers, routers etc) the host name will be comprised, in order, of the following three fields:

a. Use an abbreviation with a maximum of five letters designating the use of the individual item of equipment, or name of the demonstration which this item of equipment hosts (e.g. COP, Email, DCP) taken from the suggested list at Table 5–1;

b. Type an abbreviation with a maximum of four letters to indicate the type of equipment taken from the mandatory list at Table 5–2;

c. Unique Identifier – a letter of the alphabet (starting at ‘a’), or combination of letters up to 4 letters maximum, used only where necessary to differentiate between two or more machines within a unit which would

Uncontrolled copy when printed

otherwise have the same name (e.g. pntr-a and pntr-b or pntr-4m and pntr-colr if greater delineation is required).

507. To improve readability, the host name elements are to be separated by a hyphen ("-") (see examples below). If the "Type" component provides sufficient information, for example if there is only one router, then the "Use" component and following hyphen may be dropped. This will most commonly occur with devices, which have only one specific function and are the only one of their kind, e.g. printers and routers.

508. Note that host names can not begin with a number (i.e. the "use" field of the host name may not start with a number).

509. Tables 14- 1 and 14- 2 can be amended for specific events (e.g. operations, exercises, demonstrations, trials). However, such amendments will only apply to that event. Devices and conventions that become de facto "Use" and "Type" standards should be submitted for inclusion into ACP 200.

Use Field Abbreviation	Description	Remarks
AUTH	PKI or similar Authentication Service	generally a server
COP	Common Operational Picture/Recognized Maritime Picture	generally a server. e.g. GCCS-M or similar COP service
CT	Cipher-text side of INE device	see INE in TYPE
CVAT	Coalition Vulnerability Assessment Team service	could be a server or a workstation
DCP	Distributed Collaborative Planning	generally a server, e.g. Sametime
DIR	Directory service	generally a server
DNS	Domain Name Service	generally a server
DOM	Domino Web Replication	generally a server
GBS	Global Broadcast System	generally a server
GEN	general purpose device	typically a workstation e.g. MS Office
HI	High Side of a Data Diode device	see DIODE in Type
KEY	PKI or similar Key Server	generally a server
LO	Low Side of a Data Diode device	see DIODE in Type
MAIL	Email or messaging	generally a server

Uncontrolled copy when printed

Use Field Abbreviation	Description	Remarks
PT	Plain-text side of INE device	see INE in TYPE
TIME	LAN time service generator	generally a server
UHF	For use with UHF LOS and SATCOM networks	see Type
WEB	Traditional Web Service	generally a server
		Spare
		Spare

Table 5–1 Abbreviations for “Use” Field

Uncontrolled copy when printed

Type	Abbreviation	Type Remarks
CAP	Channel Access Processor (CAP)	equivalent to SNAC
CARD	VME Card for MCAP	
CRIU	CAP to Router Interface Unit (CRIU)	equivalent to SRIU
DIODE	Data Diode device	one-way IP data transfer
INE	In-line Network Encryptor	IP encryption device
HFIP	HF IP (STANAG 5066 Ed. 2) gateway	IP over HF; typically a server
HF5066	STANAG 5066 Ed. 1 gateway	email only over HF; typically a server
MLGRD	Mail Guard	
PRNTR	Printer	
ROUT	Router	
SNR	Subnet Relay Network Controller	
SERV	Server	
SNAC	Subnet Access Controller (SNAC)	equivalent to CAP
SRIU	SNAC to Router Interface Unit (SRIU)	equivalent to CRIU
SWIT	Network Switch	
WKST	Workstation PC, X-Terminal, etc.	
		Spare
		Spare

Table 5–2 Abbreviations for “Type” Field

Uncontrolled copy when printed

The following are some examples of the Host Names that can be generated from the above guidance:

mail-serv;
dom-serv;
dcp-serv;
cop-serv;
gbs-rout;
uhf-snr;
uhf-cap;
gen-wkst-a;
gen-wkst-123

DOMAIN NAMING CONVENTION

510. Used to generate the names for domains within which the hosts will operate, the domain naming convention shall be composed of elements of the following:

a. Unit – representing the name of the ship, unit, command or other site;

b. Theater Commands – represents Theatre / AOR Commands, such as the United States Combatant Commanders (COCOMs);

c. Service – selected from: navy, army, air, marines, joint;

d. Country – the letter country code as defined in ISO 3166 (this may either be the di-graph code described in ISO 3166-2 or the tri-graph code in ISO 3166-3);

e. Enclave – the security enclave of the network;

f. COI – a community of interest (if any) within the enclave;

g. Coalition Military Network Identifier – CMIL; and

h. Military Network Identifier – MIL.

511. The nation or other entity sponsoring a given Allied/Coalition network shall specify in the OPTASK NET which of the above naming elements are required for use in that network as well as define the naming. This provides standardization with flexibility of implementation.

512. For CENTRIXS, this convention translates to "{ship|unit|command} {3-letter-ISO3166 country-code|cocom} {enclave|enclave-coi}.cmil.mil". "

Uncontrolled copy when printed

513. Examples of CENTRIXS naming include:

UNIT		ADDRESS
CFE Enclave		
	US Pacific Command	US Pacific Command
	MHQ Australia	mhqaust.aus.cfe.cmil.mil
CNFC COI in GCTF Enclave		
	HMNZS Te Kaha	tekaha.nzl.gctf-cnfc.cmil.mil
GCTF Enclave		
	COMPACFLT	cpf.pacom.gctf.cmil.mil

514. The “country code” for NATO is “INT”. NATO enclaves include NIDTS, NSWAN, CRONOS, BISCES and LOCE.

515. For temporary, single-enclave activities, such as used by the MNTG during JWID/CWID, the above convention can allow a simpler DNS structure, such as “{ship|unit|command}.service.country”.

516. Examples of the MNTG JWID/CWID naming include:

UNIT	ADDRESS
HMNZS Te Mana	temana.navy.nz
31st MEU	meu31.marines.us
Fleet Injection Point	fip.nato.int

517. Standard formal National prefixes should not be included in the “unit” portion, as this is implied via the “country” portion. For example, in the case of Ships, unit names are not to include “HMAS”, “HMCS”, “HMNZS”, “HMS” or “USS” etc.

518. Although there are no DNS imposed restrictions on the length of the “Unit” component, for reasons of usability the length for MTWAN purposes should be constrained to 15 characters. Further the DNS entity must be unique within the service and country, e.g. there could be an ottawa.navy.ca, ottawa.navy.us and ottawa.air.ca, but not a second ottawa.navy.ca.

519. As with host names, the domain name cannot begin with a number. In other words, the ‘unit’ field may not start with a number. Therefore units like 3 CDO BDE will require a lettered prefix. DNS examples for “Numbered Units” include:

UNIT	**ADDRESS**
II MEF	us2mef.marines.us
3rd Commando Brigade	uk3cdobde.gbr.cfe.cmil.mil
40th Commando Brigade	uk40cdobde.gbr.gctf-mnfi.cmil.mil

Uncontrolled copy when printed

Fully Qualified Domain Names (FQDN) are composed of the Host names, whose convention is defined in ACP 200, Section 506 and the DNS name. Complete, FQDN examples include (NOTE: These examples are illustrative only):

HOST NAME	DNS NAME
Email Server	mail-serv.canterbury.navy.nz
Domino Server	dom-serv.ottawa.can.cfe.cmil.mil
Workstation	gen-wkst-b.uk3cdobde.gbr.cfe.cmil.mil
GCCS-M Server	gccsm-serv.adelaide.aus.gctf-cnfc.cmil.mil
Router	rout-1.mhqaust.aus.cfe.cmil.mil
TACLANE-cyphertext side	ct-ine-a.3mef.usa.gctf-mnfi.cmil.mil
TACLANE-plaintext side	pt-ine-a.3mef.usa.gctf-mnfi.cmil.mil

IP SUBNETTING AND MULTICAST ADDRESSING

520. Internet Protocol (IP) addressing consists of a series of four byte addresses separated by periods. These four bytes uniquely identify each node in a network and distinguish it from every other node in the world. Addresses are classified as Class A, B, C or D. A full description of IP addressing is provided at Appendix 1.

CLASS D MULTICAST ADDRESSING

521. The IP packet header includes a Class A, B, or C unicast source address, or a Class D multicast group address. When a host sends a multicast message (using the PIM routing protocol) it simply broadcasts it on the local net, it does not send it to a destination. If the router knows of other routers that have advertised that they have members of this group, it accepts the packets and forwards them to the other routers. The destination routers then broadcast the packets on their local LAN and local hosts that have announced group membership accept the packets. The basic approach is that Class D addresses are not assigned to any host and as such do not need to be registered. Note that Class D multicast addressing applies only to connectionless transport protocols, such as UDP. TCP does not support multicasting.

522. The Primary NOC is responsible for the allocation of Class D addresses within the MTWAN. It will need to co-ordinate with the NOC of any attached WAN (such as a CWAN) to ensure that the addresses are unique.

Uncontrolled copy when printed

UNICAST CLASS C IP SUBNETTING

523. Unicast operation is performed using the OSPF routing protocol. The OSPF routers send 5 types of LSAs to build up the routing tables. For unicast the IP header includes both the source and destination Class A, B, or C IP address. Each address is unique to the host computers. Class C IP subnetting is used to reduce the number of IP addresses required for MTWAN Networking. By subnetting, it is meant that a single Class C IP network address is used on multiple physical links. For example, the Class C IP network address 204.34.48.0 contains 256 individual IP addresses. Sections of this network can be used on approximately 10 different node-to-node links. Without subnetting, these node-to-node links would require 10 separate Class C networks. Given a general shortage of IP address availability, and for naval operations in particular, this provides a useful saving.

524. In order to realise the reduction in IP addresses which is possible with subnetting, support is required in the intra-domain and inter-domain routing protocols. The routing protocols used at present to provide this support are OSPF and BGP-4. These have been tested for router subnet support on a wide variety of routers and applications. Specifically, routers from Proteon, 3Com, Cisco, and Bay Networks seamlessly support subnetting via OSPF and BGP-4. To date no application appears to be impacted by subnetting Class C IP addresses.

MULITCAST SUBNETTING

525. Multicast is accomplished using PIM and IGMP in the host computers. IGMP is used to announce to PIM routers that they are interested in a group of information. This is done by IGMP joining groups of class D IP addresses. PIM then announces to other routers that it has members of the group. When a host sends a multicast message, the routers determine where hosts are that have announced interest in the group, and the message is forwarded to those routers for local distribution.

IP ADDRESSING CONVENTION

526. The starting point for IP address allocation is to determine the connectivity of the network. There are three possibilities: either the network will be connected to another already established one, or it will be connected in the future to another yet to be established network, or it will remain standalone. The two latter network cases are similar in the amount of responsibility the network must take on, and so will be considered together.

527. For the purposes of this convention an IP address will be considered as being made up of two parts: the Class and the Host (where Class is the conventional IP address class). These parts correspond to the domain and host names used earlier. The Class part will be assigned by an IP Address Authority, with the Host part assigned by the owning unit (e.g. HMCS OTTAWA). An IP Address Authority is charged with co-ordinating the range of IP address that will be used by individual units when assigning their Host parts. This convention only covers the use of Class C and sub-netted Class C addresses.

Uncontrolled copy when printed

528. The IP Address Authority for a MTWAN (with no external connection to an existing network) is the MTWAN NOC. Nations will utilise their existing public IP addresses where possible, and advise the MTWAN NOC before joining the network. The MTWAN NOC will assign IP addresses for multi-national WAN links and to nations unable to utilise national IP addresses.

529. If the network will be joining another already established network, then it is assumed that they will already have an IP Address Authority. Consequently they will assign either a Class C or a subnet of a Class C address to each unit in the network. In the standalone and being joined by another yet to be established network cases no IP Address Authority exists; so one will be created.

IP ADDRESS AUTHORITY TASKS

530. The function of the IP Address Authority is to co-ordinate the IP addressing architecture and will assign IP addresses to units unable to utilise national addresses. Consideration will need to be given to the number of network nodes the particular unit has with allowance for growth.

531. The IP Address authority will also allocate address ranges to multi-national WAN links. Where multi-member communication bearers are used, the authority will ensure that each member is part of the same subnet.

UNIT ASSIGNMENT OF HOSTS

532. Each unit is responsible for allocating the Host portion of the IP address for their hosts and inter-unit communications links.

533. CONCLUSION

534. A well-planned IP addressing scheme can provide an organization with important benefits, especially in a dynamic network.

Uncontrolled copy when printed

IP ADDRESSING PRIMER

1. Internet Protocol version 4 (IPv4) defines IP addresses as 32 bits long, consisting of a series of 4 address bytes separated by dots. These 4 bytes uniquely identify each node in a network and distinguish it from every other node in the world. For example, if the address for a PC is 146.143.240.90, then that 4-byte address is unique throughout the entire world. It is in fact, similar to a telephone number. Other members wishing to communicate with this node simply send all the packets to this IP address. IP addresses are assigned by the Internet Assigned Numbers Authority (IANA) whose web site can be found at http://www.iana.org

2. IP addresses are divided into a number of categories called classes. These classes are summarised at Table 5-1 and represented in Figure 5-A-1.

Class	Most Significant Bits of Address	Network MASK Value	No. of ADDRESSES Available	No. of HOSTS Available
Class A	0000	255.0.0.0	128	16,777,214
Class B	1000	255.255.0.0	16,384	16,382
Class C	1100	255.255.255.0	2.1 million	253
Class D (Multicast)	1110	N/A	N/A	N/A

Table 5-A-1: IP Address Classes

3. IP addresses are often represented in *dotted decimal* notation. Each byte (with a value between 0 and 255) is separated from other bytes by a dot (or period), as in the example 146.143.240.90 from above. Note that each IP address has an associated 32-bit *mask value*. The mask, when ANDed with the address, divides the address into two parts. One part is a *network* address that uniquely identifies the network, and the other is a host address that uniquely identifies the *host* within a given network. In other words, besides being a unique addressing scheme for individual nodes, the IP address is also a mechanism for addressing networks within networks.

4. An organisation that receives a Class B address might not have 16,000 odd computers, but it is likely to have a couple of hundred computers at each of a number of sites. The organisation can simply re-define the network mask value, incrementing the number of bits that constitute the mask (as shown diagrammatically above). This process is called *subnetting*. Obviously subnetting reduces the number of addresses available for host computers and routers (hostid), but increases the number of available networks (netid).

Uncontrolled copy when printed

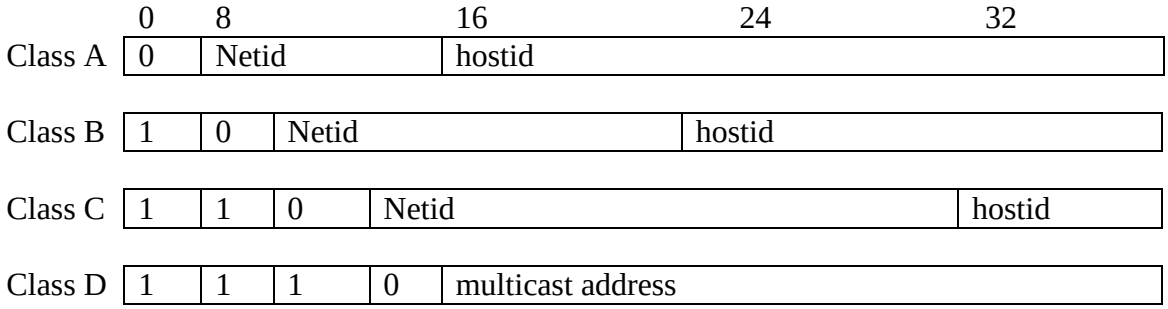

Figure 5-A-1: IP Address

5. For instance, the 146.143.240.90 example above actually consists of two networks, a Class B network and a Class C network. The Class B network is identified by the first 2 bytes of the network IP address. All nodes in that network are further identified by the third byte in the IP address (the three bytes forming a Class C address). Accordingly, the node with address 146.143.240.90 is a member of the Class C Network, or subnet, known as 146.143.240. This subnet, in turn, is a member of a Class B Network known as 146.143. Nodes on different Class C networks are accessed through routers.

Uncontrolled copy when printed

DOMAIN NAME SERVICE SOP

INTRODUCTION

1. The primary services of DNS are:

Name-to-IP-address mapping;

IP-address-to-name mapping; and

Locating the correct mail hub for any given machine or sub-domain.

2. Applications such as SMTP mail, Telnet, FTP and Web Browsers are the primary users of DNS. In any particular deployment of an MTWAN, the adopted Domain Name Service (DNS) topology should seamlessly support the host and domain naming structure specified in this document.

AIM

3. This document explains how to set up and configure DNS to support an MTWAN.

OVERVIEW

4. Each network host or more specifically each network interface has two identifiers: an IP address (which is a 32-bit number) and a Host Name (which is a string). DNS provides forward and reverse mapping between maps the host name(s) and IP address(es).

5. As applications refer to hosts by names, while packets carry source and destination IP addresses correct configuration and maintenance of DNS is critical to the effective operation of any IP network.

DOMAIN NAMESPACE

6. The naming system on which DNS is based is a hierarchical and logical tree structure called the *domain namespace*. An example using a simple naming schema of *unit.service.country* is employed in Figure 5–B–1. This naming schema complies with the naming convention describe in paragraph 505. A di-graph (i.e. two letter) country code is employed.

Uncontrolled copy when printed

7. Each host has both a name and at least one IP address. Applications that run on a host and require name or address resolution will use a resolver to access a DNS server to satisfy the resolution request. The resolver is a set of library routines which are linked to applications to perform the functions of a DNS client.

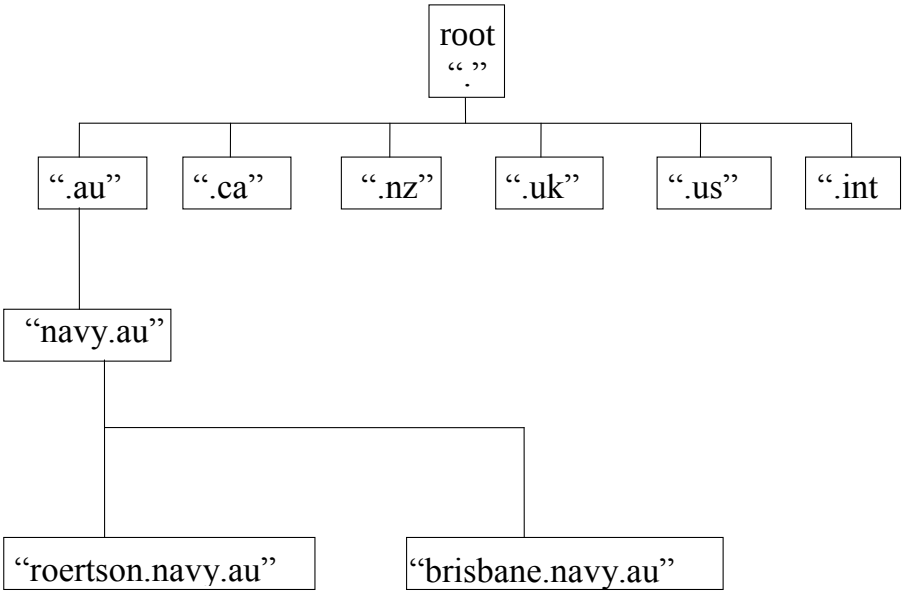

Figure 5–B–1 Domain Name Schema

DNS SERVERS

8. The following example illustrates a typical implementation of DNS for a MTWAN when the MTWAN is connected to a larger network such as the JWID CWAN. CWAN DNS servers will be distributed throughout the CWAN. The CWAN will provide the servers for the root domain (“.”). Each country will provide servers for its country domain, and also servers for the “service.country” and “unit.service.country" domains.

Multiple domains can be supported by a single server.

More than one server should be set up for each domain for robustness.

9. There are two types of name servers: primary (also known as master) and secondary (also known as slave). The main difference between the primary and the secondary is where the server gets its data. A primary server gets its data from files created by users on the host it runs on. A secondary server gets its data over the network from a primary. This is known as a “zone transfer”. When a secondary starts up, it loads data from a primary. Once it is operational, it will poll the primary at pre-determined intervals to see if its data is current.

Uncontrolled copy when printed

10. For each ship in the MTWAN, the primary DNS server will be located at the MTWAN NOC ashore, and the secondary DNS will be located on the ship as shown in Figure 5-B-2. The main purposes of putting the ship's primary DNS server at the NOC is to reduce DNS traffic over the low speed RF nets within the MTWAN and to simplify network administration onboard the ship.

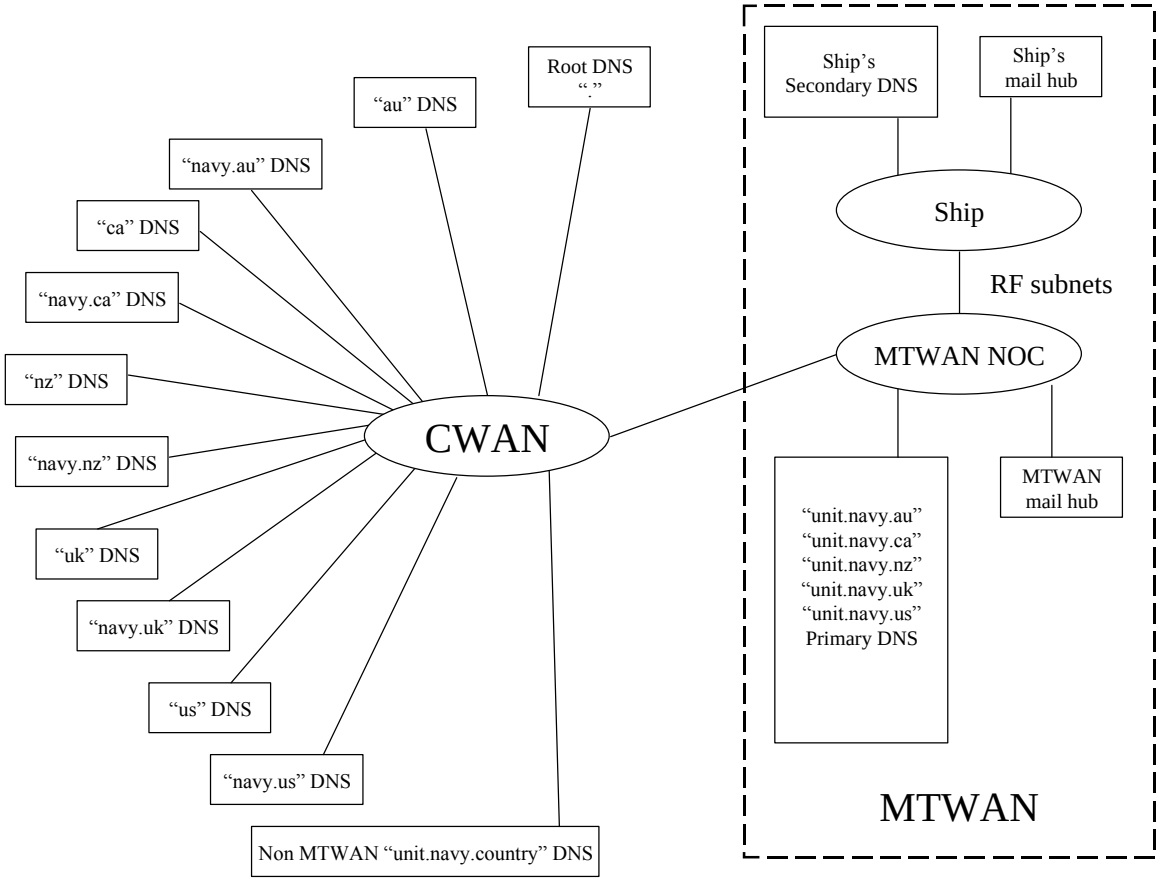

Figure 5–B–2 DNS Servers

11. Putting the primary DNS server on the shore reduces DNS traffic over the low speed RF nets because users on the shore-based CWAN can obtain the DNS data from the shore-based MTWAN DNS server. For example, if a CWAN user wants to send e-mail to a user on USS BATAAN, the query would be passed to the root DNS server, the "us" server, the "navy.us" server, and finally the "bataan.navy.us" server. All this could occur on land without using the extremely limited RF bandwidth within the MTWAN.

12. Putting the primary DNS server ashore simplifies network administration onboard the ships. DNS requires specially trained network administrators who are familiar with the configuration and maintenance of DNS. By putting the ship's primary DNS on shore, the shore-based experts can maintain the DNS database, and the ship's DNS server will automatically download the data as required, without intervention by the ship's

Uncontrolled copy when printed

personnel. When the ship requires changes to the DNS database, it contacts the NOC by voice or electronic mail to request the changes. The NOC will make the requested changes to the db files of the primary server. The updated db files will then be copied by all secondary servers at the next database refresh or at a forced restart of the secondary servers.

13. The disadvantage of having the primary name server for ships located at the NOC will be that changes to the DNS db files will require the ships to send requests to the NOC. The ships will have to wait until the NOC has modified the shore-based DNS db files and the updated db files have been copied by all the secondary servers before any changes to the DNS will take effect. Where the rate of changes is low, and where there is sufficient advanced DNS planning, this should not be a problem.

14. In addition, ships in the MTWAN will act as secondary DNS servers for all other ships in the MTWAN. This allows each ship to get DNS information on all other ships in one (or a few), efficient bulk transfer transactions, rather than needing a large number of relatively inefficient individual DNS queries.

15. It is recommended that when assembling a MTWAN, consideration is given to combining elements of the DNS name space onto a single DNS server, where such combinations improve efficiency. One area where efficiency can be improved is in careful planning of which national DNS servers can be combined to reduce the amount of network engineering support required at the national level. Another area where efficiencies can be improved is by consolidating multiple ships into a single shore-based DNS server. Both of these efficiencies have been successfully employed during previous deployments of the MTWAN.

DNS CLIENTS

16. Hosts on each ship will be configured to refer their DNS queries to the local server. Name-to-address and reverse mapping of an MTWAN host can always be resolved locally, as each ship will act as a secondary server for every other ship. The root servers will only be contacted by the ship's server for mapping of non-MTWAN hosts.

Uncontrolled copy when printed

DELEGATION FOR MTWAN SUB-DOMAINS

17. Delegation will be required from the root or parent sub-domain if hosts in the MTWAN sub-domains are to be visible to non-MTWAN hosts. This can be achieved by adding a NS record pointing to the ship's primary DNS server together with its glue record (a glue record is an A record for a name that appears on the right-hand side of a NS record) to the database of the root or parent DNS server.

18. It is essential that delegation be obtained not only for the name domain but also for the in-addr.arpa domain.

19. Subnetting is used extensively by the MTWAN to make efficient use of the IP address space. As in-addr.arpa sub-domains are organised on IP address byte boundaries, the use of subnetting could complicate in-addr.arpa delegation. Creating database files in this domain should be a straightforward task if delegated zones (a zone is defined as part of the domain delegated to a single server) are on byte boundaries. If a delegated zone is not on a byte boundary but it does not share its in-addr.arpa sub-domain with another zone belonging to a different AS, delegation should also be simple. However, if a node within the MTWAN is to share its in-addr.arpa sub-domain with a non-MTWAN node, special techniques will be required to implement in-addr.arpa delegation across autonomous systems. These techniques are discussed in RFC 2317 entitled Classless IN-ADDR.ARPA Delegation.

Uncontrolled copy when printed

CHAPTER 6

ROUTING

INTRODUCTION

601. A solid network foundation is a critical requirement for effective and efficient communications in a mobile tactical network environment. In this respect routers, together with routing protocols and router configurations, are central to a strong network foundation. They enable the intelligent, end-to-end movement of converged data, voice, and video information within or outside a MTWAN.

AIM

602. This Chapter describes routing within a MTWAN and also between an MTWAN and external networks.

OVERVIEW

603. Routers implement and control information flow. They are internetworking devices that perform two basic functions—they select a route between networks, and they transmit information in the form of IP data packets across that route toward an intended destination. In so doing, they draw on routing protocols and algorithms. The routing protocols, such as OSPF and BGP4 are designed to discover and plot routes using such criteria as throughput, delay and priority so that the most efficient route can be selected for each transmission. This process is similar to maps created by auto clubs that show drivers where roadwork is under way so that they can avoid potential areas of congestion. When a packet is received at a router, the router opens it, looks at the network destination address, and then calculates the next hop in the best route to the destination.

604. In an MTWAN, routing is accomplished using the following standard IP protocols:

a. Open Shortest Path First (OSPF) for interior AS routing;

b. Border Gateway Protocol Version 4 (BGP4) for exterior AS routing; and

c. Protocol Independent Multicast (PIM) for multicasting.

605. The running of the three protocols over a WAN is depicted in Figure 6–1. Annex A contains further information on these protocols, while paragraphs 605 and 606 discuss the implementation of these protocols within an MTWAN.

606. Networks, or more precisely, the routers that are under the same administrative authority and use a common interior routing protocol are usually grouped into the same Autonomous System (AS). Interior routing policies and protocols must be established within each AS, enabling it to route packets internally. Exterior routing, using an exterior routing

Uncontrolled copy when printed

protocol such as BGP4, is used to interconnect the various AS's, with their independent interior routing protocols, into a larger network.

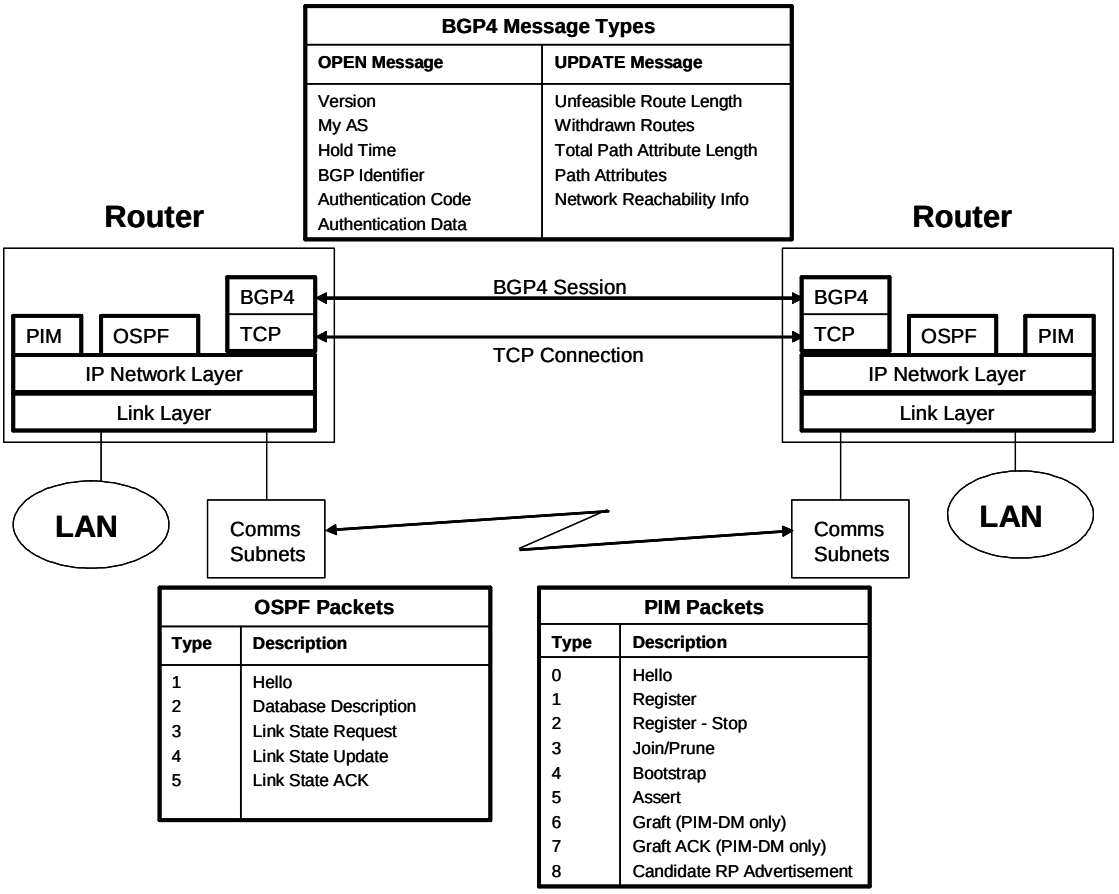

Figure 6–1 Routing Protocol Stacks

ROUTING ARCHITECTURES

607. In terms of topologies, MTWAN's either employ a single-AS TGAN topology or a multiple-AS TGAN topology. The latter is generally employed to allow nations within an MTWAN to administer their own mobile units.

608. Single-AS TGAN. In a single-AS TGAN, all mobile and fixed nodes of the TGAN belong to a single AS, as illustrated in Figure 6–2. OSPF is used to select routes for all IP traffic flows among TGAN nodes.

609. The TGAN is divided into OSPF areas where all communication subnets are included in the backbone area, known as Area 0. The local network at each node is contained in a separate OSPF area whose number is the network address of the node. In the example shown in Figure 15–2, nations in the TGAN are allocated two Class C addresses: A.B.C.0 and

Uncontrolled copy when printed

D.E.F.0. The two Class C networks are divided into 16 subnets with up to 30 individual IP addresses each. Mobile #1 is assigned the network address A.B.C.32 which is also the mobile's OSPF Area Number.

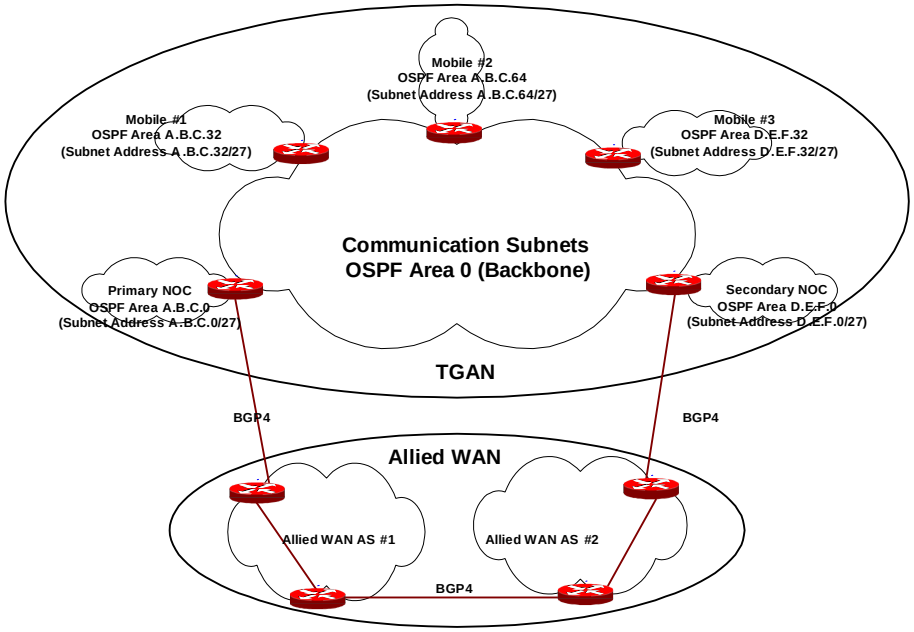

Figure 6–2 Interior and Exterior TGAN Routing

610. Multiple-AS TGAN. Each nation can form a separate AS within a TGAN. The TGAN is then considered as a virtual Autonomous System (AS) comprising of a number of actual ASs. Each AS will have an independent entry into the allied WAN. OSPF will run internally within the TGAN, controlling path selection for all (ship and shore) traffic flows within the TGAN. If connectivity between different ASs does not exist, to extend OSPF routing domain over the whole TGAN, Generic Routing Encapsulation (GRE) tunnels through the allied WAN can be used to provide a mechanism for supporting multicast and the OSPF adjacencies by encapsulating the internal OSPF and multicast routing from the allied WAN.

611. Figure 6–3 depicts a scenario where each nation forms its own AS within the TGAN. Each AS has an independent entry into an allied WAN. Within each national AS, the national backbone is used to provide connectivity between TGAN routers using In-line Network Encryptors (INE) and GRE tunnels.

Uncontrolled copy when printed

612. Allied routers in the national NOC are connected to the allied WAN comprising a number of ASs via BGP, and TGAN entries into the allied WAN are in different AS. This architecture can support direct RF connectivity between TGAN ASs as part of the OSPF routing domain. Generic Routing Encapsulation (GRE) tunnels through the allied WAN are used to support multicast and OSPF adjacencies within the TGAN.

613. Direct connectivity between mobile units of different nations or between a NOC of a nation and a mobile unit of another nation can be supported within the OSPF routing domain of the virtual AS of the TGAN. In Figure 6–3 an allied LOS subnet is used to support direct ship-ship networking. A satellite link connecting Mobile #21 to NOC #1 can also be provided as a redundant backup route for Mobile #21 when the backbone of Nation #2 is not operational.

614. Private Routing. Figure 6–4 provides an overview of a Private Routing architecture where a secure IP backbone is set up to support Virtual Private Networks of various security levels.

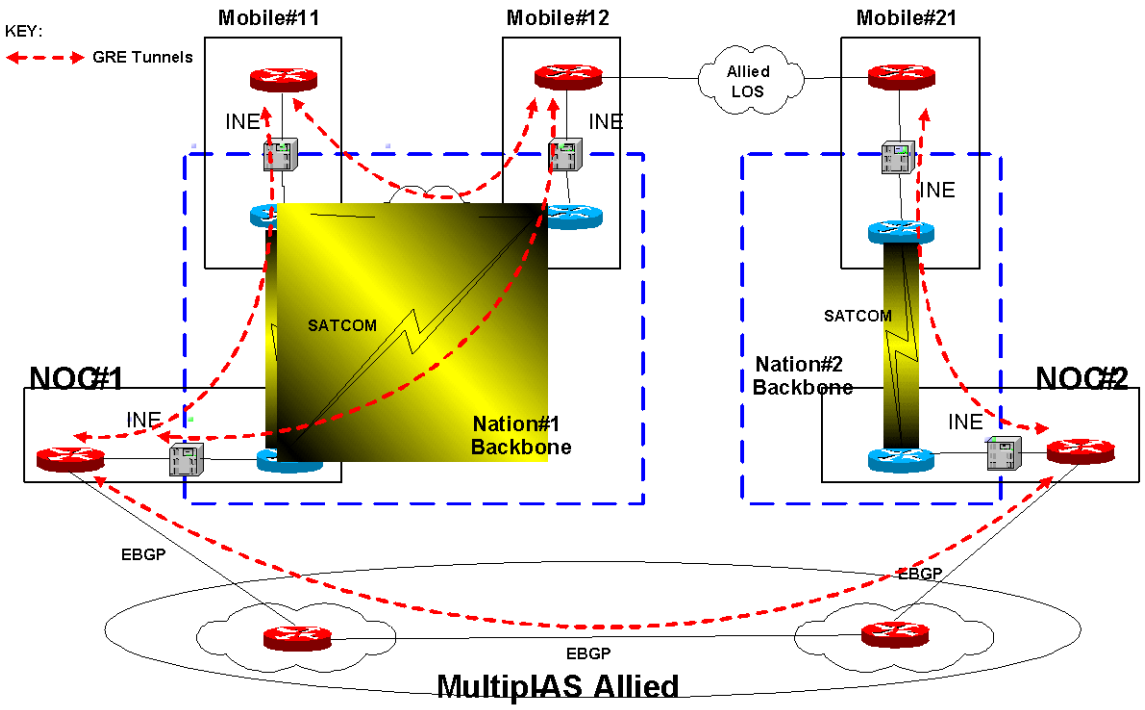

Figure 6–3. An Example of a Multi-AS TGAN

615. The introduction of LOS connectivity can significantly reduce traffic on national SATCOM links by enabling traffic between mobile units to travel via a direct mobile-to-mobile route in lieu of a mobile-to-NOC-to-mobile route involving two SATCOM hops. This conserves SATCOM bandwidth for traffic between mobile units and NOCs. However, the introduction of OSPF-based LOS connectivity can adversely affect route selection behavior

Uncontrolled copy when printed

unless appropriate measures are taken on allied NOC routers. The routing configuration must be exercised with care to prevent inappropriate route selection for traffic within the TGAN and also for traffic between the TGAN and the allied WAN.

616. The GRE tunnels can be limited to mobile-to-NOC links only. This means that any direct mobile-to-mobile traffic must go to the NOC first even if national LOS links are available. If a point-to-point GRE tunnel is set up for every national link including LOS, the number of GRE tunnels will get very large and management will be more difficult. Furthermore, the use of GRE tunneling will also reduce the maximum transfer unit for the route because of the overhead of GRE encapsulation. As a result, the network can suffer from packet fragmentation.

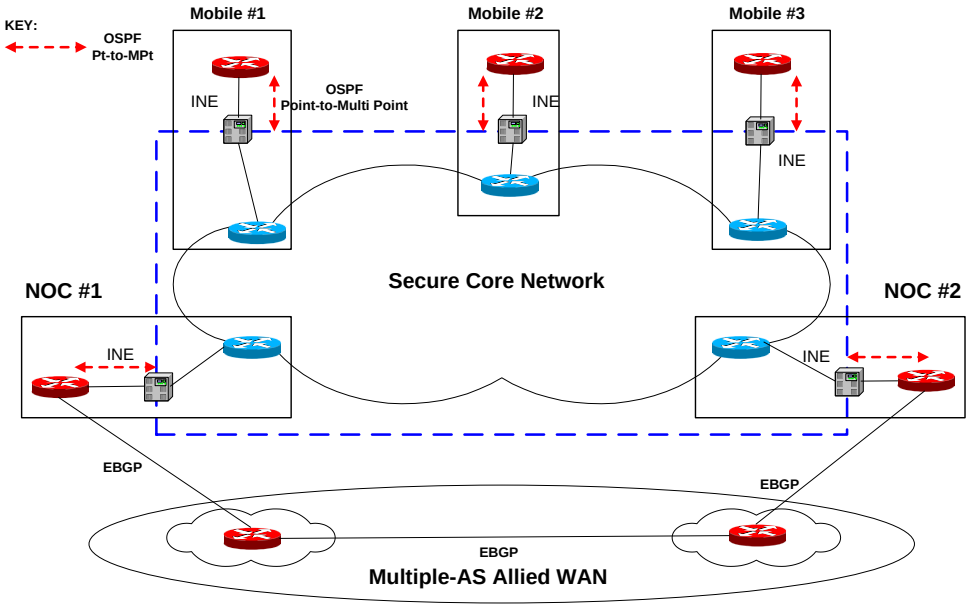

Figure 6–4 Private Routing

617. The alternative to GRE tunneling is to use OSPF point-to-multipoint between the mobiles and the NOC. This will avoid the overhead of a fully meshed network of GRE tunnels, but will allow the mobiles announce their reachability to the NOC and, hence, inform the allied WAN of their presence. Using OSPF point-to-multipoint rather than GRE results in a simpler and more efficient configuration.

618. Connectivity between an allied node and an access router of the backbone is via an INE. As neighbor relationships between routers of two separate and different networks do not exist, connectivity between allied nodes is done via GRE tunnels or a routing protocol that can work through the INE. The use of a routing protocol will require allied networks to be routable over the backbone. However, this option will support a dynamic TGAN and enable mobiles to join or leave the TGAN without re-configuring any allied routers. In Figure 6-4, OSPF point-

Uncontrolled copy when printed

to-multipoint is used to establish OSPF adjacencies and exchange routing information between mobiles and the NOC.

INTERIOR TGAN ROUTING

619. Route selection will meet the following requirements:

620. Direct LOS connectivity, where available, will be used for mobile-to-mobile traffic to better utilize available bandwidth.

621. Whenever possible, fixed terrestrial subnets will be selected for traffic between non-mobile units.

622. Whenever possible, the fixed terrestrial connectivity to the RF subnet of the specific mobile unit that hosts the traffic endpoint will be used for fixed-to-mobile traffic.

623. Unless a mobile is acting as a relay for another mobile, its RF subnet will not be used as a transit subnet for the other mobile.

624. Route selection is to be symmetrical; traffic between two nodes should flow over the same route in both directions.

625. Within a TGAN, route selection is governed entirely by OSPF costs. The small adjustments to the recommended OSPF metric values given in Annex B may be required so that the requirements of route selection specified above can be met.

626. OSPF uses two types of external metrics – Type 1 and Type 2 – to determine the best exit point to external networks. Type 1 external metrics are expressed in the same units as the OSPF internal metric values and can be directly summed with the internal metrics to form the lowest cost route to reach the external destination. Type 2 external metrics are an order of magnitude larger and are considered greater than any route internal to the AS. Type 2 metrics assume that routing between ASs is the major cost and eliminate the need for conversion of external costs to internal costs. The route selection from the interior nodes is based on the lowest cost Type 2 external metrics, and it does not require any internal lowest cost path calculations.

627. Type 1 external metrics are preferred as mobile units learn of several exit points, but will choose the best exit point based on OSPF costs. When the link supporting the best exit point fails, the mobile units will dynamically adjust their routes and select the next best exit point.

628. Multicasting within a TGAN is supported by PIM. All COTS routers can support SM, DM and a combination of SM and DM known as Spare-Dense Mode (S-DM). When a router is configured for S-DM and an RP is not known for a group, the router will send data using DM. However, if the router discovers an RP either dynamically or statically, SM will take over. As S-DM allows the use of both SM and DM for different groups for different

Uncontrolled copy when printed

applications, TGAN routers will be configured for S-DM when multicast is required. Whenever PIM-SM is selected, a static RP at a NOC will be configured.

EXTERIOR TGAN ROUTING

629. Single Allied WAN Access Point. BGP4 is used to control which internal networks are advertised to, and which network advertisements are accepted from, other autonomous systems. This control is at least as fine-grained as the ability to send or receive individual network advertisements. This means the TGAN network administrator has the ability to control whether to advertise or hide each individual internal network. Likewise, the administrator also has the capability to accept or reject each external network advertisement.

630. The ability of BGP4 to implement routing policy is both a strength and a severe constraint. While the ability to develop routing policy gives significant power to the administrator, it also makes the configuring of BGP4 labor intensive and error-prone.

631. The primary use of BGP4 policy is to limit the amount of routing protocol traffic seen inside the TGAN as a result of external links. An allied WAN, as a global network, has the potential to generate large amounts of routing protocol traffic. If this routing protocol traffic were allowed into the TGAN, it might consume a significant amount of bandwidth. To prevent this, BGP4 policy is used to block the allied WAN routing protocol traffic into the TGAN.

632. A global backbone network, such as the allied WAN, cannot use default routes and must have specific route advertisements for every network that is reachable across the backbone. Hence, all nodes in the TGAN must be advertised to the allied WAN.

633. Multiple Allied WAN Access Points. When the TGAN has multiple connections to the allied WAN, one of the connections will be configured to be the primary (preferred) route for all traffic between the TGAN and allied WAN. In some cases, there may be a requirement to configure a connection to be the primary route for some nodes and the secondary (backup) route for some other nodes.

634. In order to manipulate the route selection of BGP, either of the following two BGP attributes will be used: AS-Path and Multi-Exit-Discriminator (MED).

635. AS-Path. BGP permits BGP–enabled routers to exchange routing information with full AS-Path information. The AS-Path is a list of ASNs that describes the route between the local AS and the destination AS. When all other BGP attributes are the same, routers use the length of the AS-Path (the number of ASNs in the AS-Path) to determine the best route to a destination AS and its associated networks. A route with a shorter AS-Path is preferred.

636. A router can make the AS-Path of a route longer than the AS-Path of another route by pre-pending its own ASNs to the route's AS-Path attribute.

Uncontrolled copy when printed

637. The TGAN border router at the secondary site needs to be configured to pre-pend its own ASN to the AS-Path before communicating routes via BGP to the allied WAN border router. The TGAN border router at the primary site does not alter the AS-Path it presents to the allied WAN.

638. For example, let 1002 be the number of the TGAN AS. The AS-Path in routes advertised by the TGAN border router at the secondary site then consist of the TGAN ASN pre-pended to the route's AS-Path attribute, that is "1002 1002", while the AS-Path advertised by the TGAN border router at the primary site simply consists of "1002". Since the AS-Path advertised at the primary site is shorter than the AS-Path advertised at the secondary site, traffic destined for the TGAN network from the allied WAN would be routed via the primary site. When the connection between the TGAN network and the allied WAN at the primary site is not available, traffic will be re-routed via the secondary site.

639. To ensure a symmetrical path between the TGAN and the allied WAN, allied WAN routers need to be configured in a similar fashion. The allied WAN border router at the secondary site needs to be configured to pre-pend the allied WAN ASN to the AS-Path before communicating routes via BGP to the TGAN.

640. The primary and secondary border routers communicate via an IBGP session to ensure a consistent view of external routing within a TGAN AS. Using IBGP, the secondary border router will be aware of the preferred route to the allied WAN via the primary border router because allied WAN routes advertised at the primary site possess a shorter AS-Path than the same routes advertised at the secondary site.

641. Multi-Exit-Discriminator (MED). MED is an alternative technique that can be used to influence route selection for traffic flowing from the allied WAN into the TGAN. The MED feature will enable inbound route selection to be governed entirely by the OSPF costs internal to the TGAN. The MED effectively extends internal cost information in order to automatically control inbound route selection from the allied WAN. The BGP MED attribute is a hint to external ASs about the preferred path into an AS.

642. MED provides a dynamic way to influence routers in another external AS to choose the best route into a given AS from among multiple entry points into that AS.

643. As MED attribute only transits between a single pair of ASs. That is, the receiving AS will not pass the original MED value to another AS. When the allied WAN consists of multiple ASs and the allied WAN access points are in different ASs, the BGP configuration will have to ensure that the allied WAN will make cohesive and coordinated routing decisions with respect to the preferred route to the TGAN. This objective can be achieved by a fully meshed BGP between the AS border routers of the TGAN and those of the allied WAN.

644. Failure recovery. If an exit point fails, all traffic should use the remaining exit points.

645. For outgoing traffic, failure recovery can be ensured by carefully setting up the default routes on the AS boundary routers. When a boundary router has a connection to the

Uncontrolled copy when printed

allied WAN, we want it to generate a default route and distribute it throughout the TGAN. When a boundary router loses it connection to the allied WAN, we want it to automatically stop generating the default route. When the failed exit stops generating the default route, allied WAN traffic will automatically be directed to the remaining exit points by the remaining default routes.

REDUCING ROUTING PROTOCOL TRAFFIC TO THE ALLIED WAN

646. The allied WAN must be default-free, and therefore requires specific network routing information for every network in the allied WAN, as well as routing information for every node in the TGAN. For large networks, this can lead to an unacceptably large number of network advertisements. To reduce the amount of traffic generated by routing protocols, a technique known as "Classless Inter-Domain Routing" (CIDR) can be used to aggregate network advertisements.

647. A simple example of CIDR would be the combination of two Class C IP network addresses into a single advertisement. If a TGAN had two sequential IP network addresses, such as 192.200.200.0 and 192.200.201.0, then it would advertise two separate networks to the allied WAN. Each of these networks would contain 256 addresses. Using CIDR, the TGAN would advertise a single network, starting at 192.200.200.0, that contained 512 addresses. The same host addresses are advertised in both formats, but CIDR produces 50% fewer routing advertisements.

648. Typically, the network design would specify that numerous coalition units would receive a fraction of a Class C IP network address. For example, a NOC would have a fraction of the A.B.C.0 network (A.B.C.16-A.B.C.31) and a mobile unit would have another fraction of the same network (A.B.C.48-A.B.C.63). All these subnet addresses would be summarized in a single A.B.C.0 network before they were advertised to the allied WAN. This reduces the number of TGAN network advertisements that the allied WAN needs to carry on its backbone network. However, CIDR should not be implemented if the larger network contains one or more sub-networks external to the TGAN, as those networks will not be reachable.

649. Although the actual number of network advertisements on the allied WAN is unlikely to be excessive, it is considered good practice to use CIDR address aggregation, when possible, to conserve bandwidth.

CONCLUSION

650. An MTWAN comprises one or multiple AS's, where each AS shares a common routing strategy. Internal routing is accomplished by OSPF, or in the case of multicast PIM (SM or DM), while external routing is carried out with BGP4. The routing architecture can be complicated by multiple WAN access points. These routing approaches have been validated at sea in low bandwidth, high latency tactical environments. It is capable of exploiting transient communication links when they are up and avoid them when they are down.

Uncontrolled copy when printed

ROUTING PROTOCOLS

ROUTING PROTOCOLS (UNICAST)

1. Open Shortest Path First (OSPF). OSPF is a dynamic routing protocol that quickly finds the best route based on the lowest cost to reach the destination. OSPF assigns a metric value to each link, which is used to determine the lowest cost path from source to destination. The recommended metric values can be found in Annex A to this chapter. OSPF runs directly on top of the IP network layer. IP packets containing OSPF data will have their IP protocol number set to 89.

2. The OSPF routers exchange 5 types of Link State Advertisements (LSA's) with each other to build up the routing tables. For unicast, the IP header includes both the source and destination Class A, B, or C IP address. Each address is unique to the host computer.

3. Border Gateway Protocol Version 4 (BGP4). BGP4 is a policy-based routing protocol that selects the AS to which it will talk to based on a policy entered manually by the AS manager. It operates on top of TCP and requires very stable subnets, which are more applicable to fixed infrastructure connections.

4. BGP4 operates on top of TCP and requires two routers to set up a connection and establish a session to exchange routing information. BGP4 selects the path based on a policy that is converted into attributes. Each AS is assigned a unique AS Number (ASN) that is contained within the BGP4 protocol header. Policies then can be used to determine which AS to route traffic through or which to avoid. BGP4 does not provide the dynamic response of OSPF.

5. An AS can have more than one exit point to other AS's. When only one exit point is used, the single BGP4 border router of the AS becomes the default router for all traffic leaving the AS. However, when two or more exit points exist, routing information must be provided to OSPF to decide which BGP4 border router to select to reach the external destination. In addition, the multiple BGP4 border routers of the AS need to exchange routing information to keep their databases synchronized. This may be accomplished using the internal BGP4 protocol.

6. BGP supports two types of sessions: External BGP (EBGP) and Internal BGP (IBGP). As illustrated in Figure 6-A-1, EBGP is used between BGP-enabled routers in two adjacent autonomous systems, while IBGP is used between BGP-enabled routers in the same AS. IBGP is sometimes necessary to achieve a consistent view of external routing within an AS. Typically IBGP is configured in a fully meshed configuration such that each BGP-enabled router maintains a distinct IBGP session with all other BGP-enabled routers within the AS.

Uncontrolled copy when printed

7. External routes learned via EBGP need to be communicated to all routers within the TGAN to permit optimal routing to external destinations.

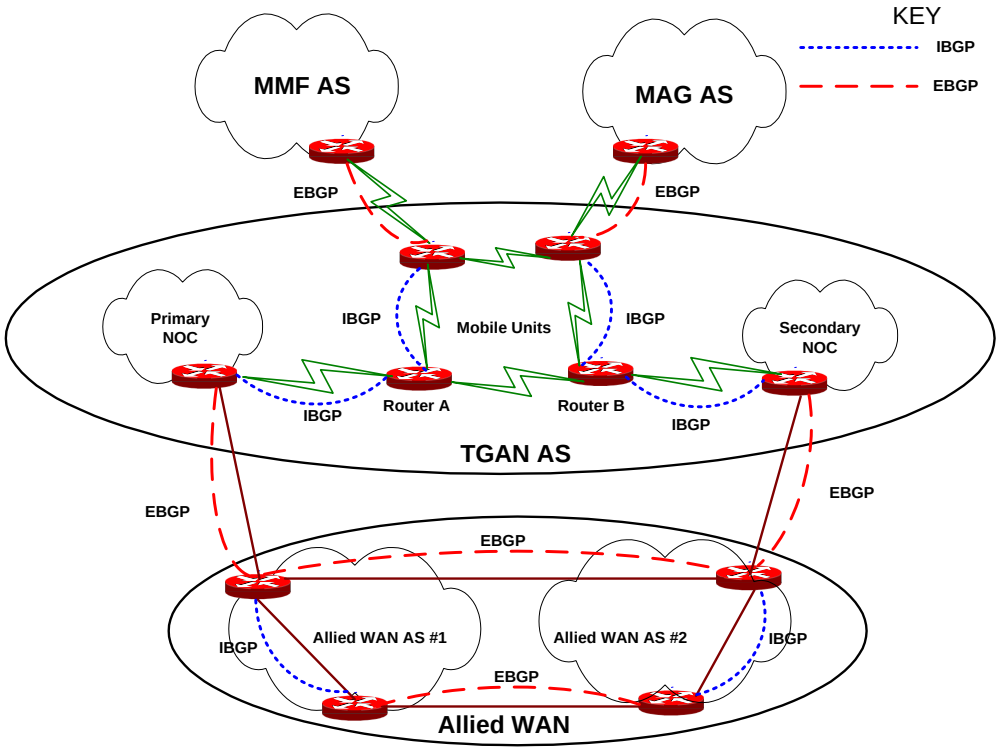

Figure 6–A–1 Sample BGP Configuration

8. Depending on the network architecture, it is sometimes necessary to configure IBGP within routers of one AS that does not host external connections. This has the advantage of controlling the router table update so as not to flood the internal network. This is particularly advantageous in narrowband networks such as the TGAN. Intra-AS routing protocols such as OSPF have the ability to distribute external routes throughout an AS, but this requires that the external routes be flooded throughout the OSPF routing domain. Usually, this is not good practice as external routes are not needed or wanted on low-end access routers that are typically connected with lower-bandwidth connections as exhibited in the TGAN. Instead, IBGP should be used. In the TGAN illustrated in Figure 6–A–1 IBGP sessions are configured between AS border routers and Routers A and B. The external routing information communicated to Routers A and B via IBGP permits optimal routing to external destinations without flooding the external routes throughout the TGAN.

ROUTING PROTOCOLS (MULTICAST—PIM)

9. The protocol stack for Protocol Independent Multicast (PIM) is shown in Figure 6–1. PIM is directly on top of the IP network layer. IP packets containing PIM data will have their IP protocol number set to 103.

Uncontrolled copy when printed

10. PIM runs over an existing unicast protocol (including static routes), and uses the information provided by the unicast protocol and the static routes to build the distribution tree which the routers will use to forward multicast packets to all the members of the multicast group.

11. Host computers use Internet Group Management Protocol (IGMP) to announce to their local multicast routers that they wish to join a multicast group (a group D IP address). The IP header for multicast now includes a source Class A, B, or C unicast address and a destination Class D multicast group address.

12. There are two modes of operation with PIM: PIM-SM (Sparse Mode) and PIM-DM (Dense Mode).

SPARE MODE

13. PIM-SM is designed for situations where group members are sparsely distributed across all WANs, that is, the number of nodes with group members present is significant smaller than the total number of nodes. PIM-SM assumes that no node wants multicast data unless it is explicitly requested.

14. PIM-SM uses some selected router as a Rendezvous Point (RP), which is the root of the distribution tree where multicast senders send their IP packets by unicast. The RP then forwards the packets to all the routers that have registered with the RP.

15. The RP can be dynamic if it is announced throughout the routing domain. In that case, all other routers rely on the RP broadcast to establish the multicast tree. The RP can also be static, in which case every multicast router in the domain must be manually configured with the RP's address.

16. In a large network with few multicast receivers, PIM-SM reduces the amount of multicast traffic flooded throughout the network.

17. In a mobile environment, NOCs will be a logical choice for an RP.

DENSE MODE

18. Dense Mode. PIM-DM is designed for situations where group members are densely distributed. That is, most nodes are members of the multicast group. Multicast data is initially sent to all nodes in the network. Routers that do not have any member of the group attached to them will send a control message to remove themselves from the distribution tree.

19. PIM-DM is simpler to implement than PIM-SM as PIM-DM does not use RPs. In small networks, PIM-DM is an efficient protocol when most nodes are members of the group.

Uncontrolled copy when printed

OSPF METRICS

OSPF METRIC VALUES

1. The routing protocol OSPF is used to control path selection for all IP traffic flows within the MTWAN. Path selection is governed by OSPF link costs. Each link will be assigned a Metric Value (MV) that will be the cost used by OSPF to determine the optimum path from source to destination, which is a path with the lowest cost.

Metric Value	Bandwidth (Hz)	Link
100	512,000,000	
120	256,000,000	
140	128,000,000	Pier
170	64,000,000	
200	32,000,000	
250	16,000,000	
300	8,000,000	
360	4,000,000	
400	2,000,000	
500	1,000,000	
600	512,000	
700	256,000	
750	128,000	Dual ISDN
800	128,000	SHF
1,000	64,000	INMARSAT B/ISDN
1,300	32,000	
1,500	16,000	
1,900	9,600	HF
2,220	6,000	32 kbps UHF/5 Member
2,660	4,800	16 kbps UHF/3 Member
3,200	2,400	HF
3,830	1,200	
4,600	512	
5,520	256	
Note: ‘X’ in Figures 15-B-1 and 15-B-2 signifies information that is classified.		

Table 6–B–1 Recommended Metric Values

Uncontrolled copy when printed

2. The algorithm used for selecting the metric value is MVn = C x MVn-1 for each halving of the bandwidth. The recommendation is C = 1.2. The metric values shown in Table 6–B–1 are based on C=1.2 rounded off to make the selection simple. The metric values are multiplied by 10 in order to increase the space between bandwidth increments for management purposes.

3. To illustrate the OSPF metric values, a hypothetical typology is represented in the next two figures. Figure 6–B–1 details the link bandwidth while Figure 6—2 shows the metric values for those links. To calculate the OSPF link costs between any source and destination pair in the example, sum the metric values shown. The router will select the path with the lowest cost.

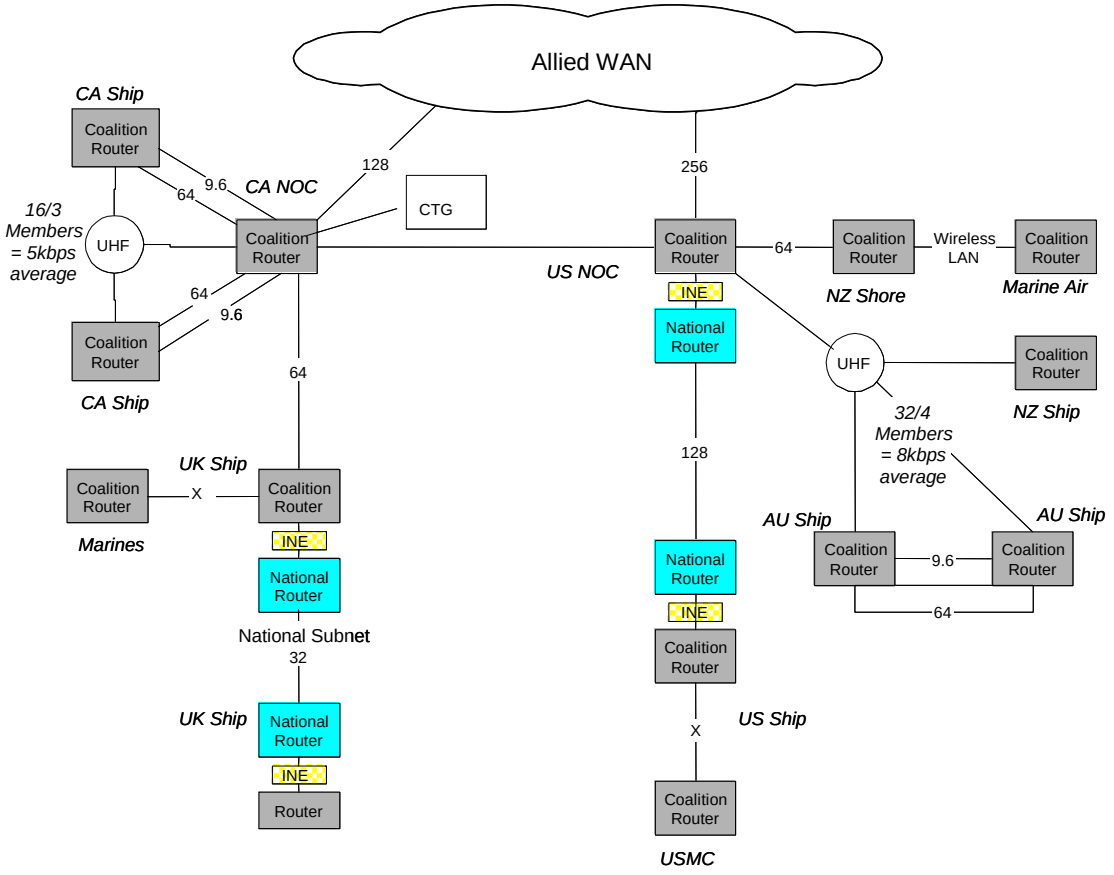

Figure 6–B–1 Example of Coalition and National Subnets Bandwidth (Notional)

Uncontrolled copy when printed

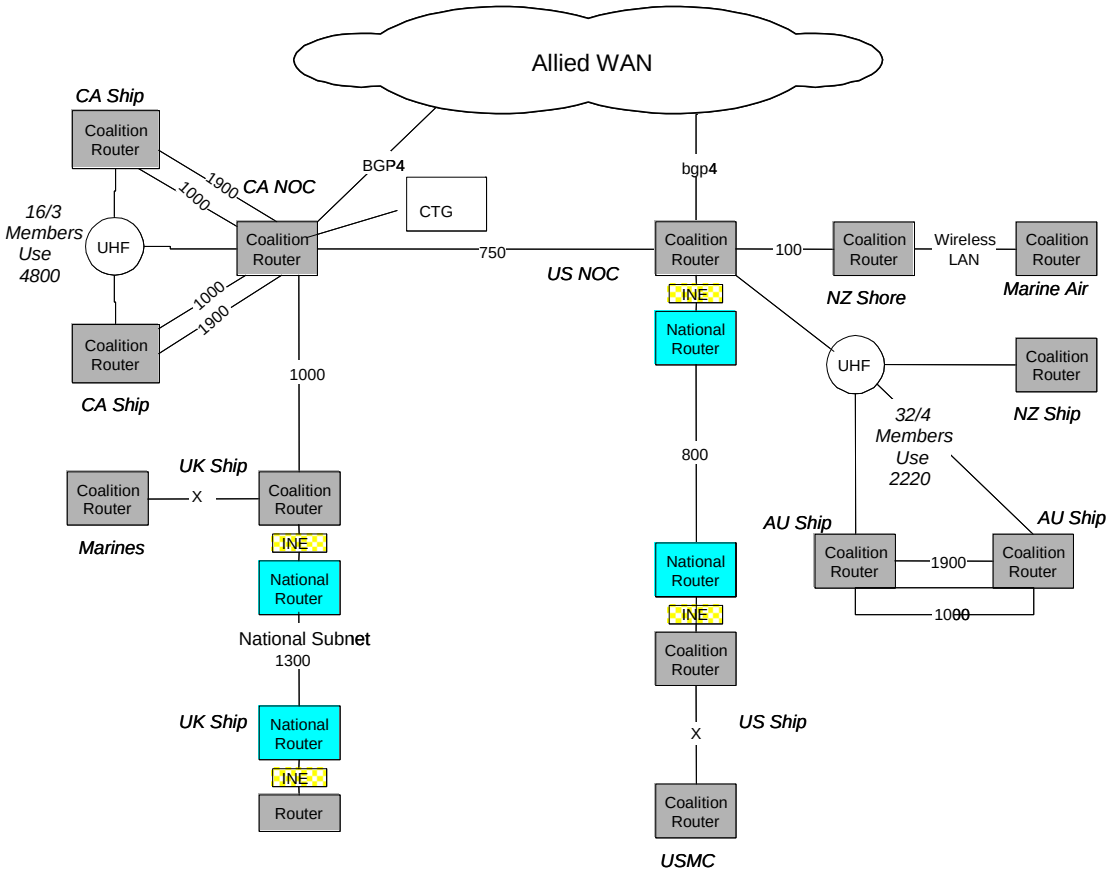

Figure 6–B–2 Link Metric Values (Notional)

Uncontrolled copy when printed

CHAPTER 7

COMMUNICATION SUBNETS

INTRODUCTION

701. A MTWAN is a collection of subnets (short for "subnetworks") that are connected to each other by routers. In the context of IP networking, a wire, optical fiber or an RF bearer together with its associated interface and cryptographic equipment form a subnet that connects two or more routers together.

702. While modern commercial RF communication bearers may already have the capability to support IP, many military communication bearers were not initially designed to provide IP connectivity. In these cases, special interfaces will need to be deployed in order for them to support IP.

703. The deployed tactical military environment is typically a very mobile one, where wireless communications bearers find wider use than wired (wire or optical fiber) communications. This chapter shall focus primarily on wireless, tactical bearers.

AIM

704. This chapter provides an overview of communication subnets and their utilization within a MTWAN.

OVERVIEW

705. A typical MTWAN is formed between geographically dispersed LANs connected to one another through the use of disparate communication links. The communication subnets over wireless communication bearers such as INMARSAT, UHF SATCOM, UHF and HF connect routers through the use of the first three layers of the OSI model. This is illustrated in Figure 7–1.

706. The end state is to achieve a seamless LAN-to-LAN connection, and thus enable the exchange of IP packets.

DEFINITIONS

707. The following definitions are provided:

a. Subnet —a segment of a data network connecting two or more network devices. A subnet is therefore a network within a network and operates at Layer 3 of the OSI model;

b. Subnetting —the division of a network into smaller networks (subnets); and

Uncontrolled copy when printed

c. Communication Bearer —a system that can establish a channel to pass data. A communication bearer operates at the physical layer (layer 1) of the OSI model.

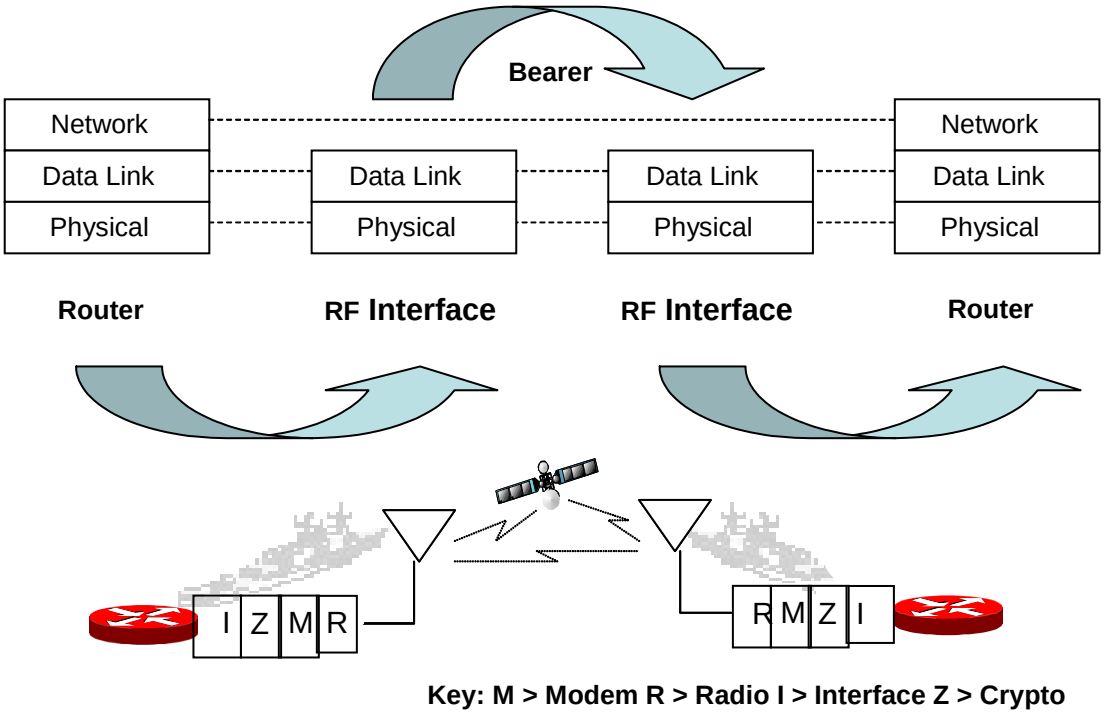

Figure 7–1 Communication Subnet(s)

Uncontrolled copy when printed

COMMUNICATIONS ARCHITECTURE (CA)

708. The design objective of a MTWAN is to maximize capacity, efficiency and mobility of the communication bearers. The Communication Architecture (Figure 7–2) shown is designed to maximize capacity, efficiency and mobility. The three segments shown are shore, RF, and deployed.

709. Figure 7–2 shows three of the four tiers that this publication uses to classify communication bearers. The four Tiers are:

a. Tier 1 —Intra platform and handheld radios. This tier, not visible in the diagram as it is internal to the deployed segments, includes shipboard LANs (wired and wireless) and handheld radios;

b. Tier 2 —Wireless networking. Tier 2 is networked LOS and BLOS communications between platforms and expeditionary forces ashore. This would be the equivalent of a Metropolitan Area Network (MAN);

c. Tier 3 —Wireless trunking. This involves trunked LOS and BLOS communication links, which provide point-to-point connectivity, such as HF BLOS and Digital Wideband Transmission System (DWTS); and

d. Tier 4 —Satellite communications. This involves military and commercial satellites in the UHF, L-, X-, C-, Ku-, Ka- and Q-bands, such as UHF SATCOM, INMARSAT, IRIDIUM, DSCS, CWSP, and. GBS/TBS.

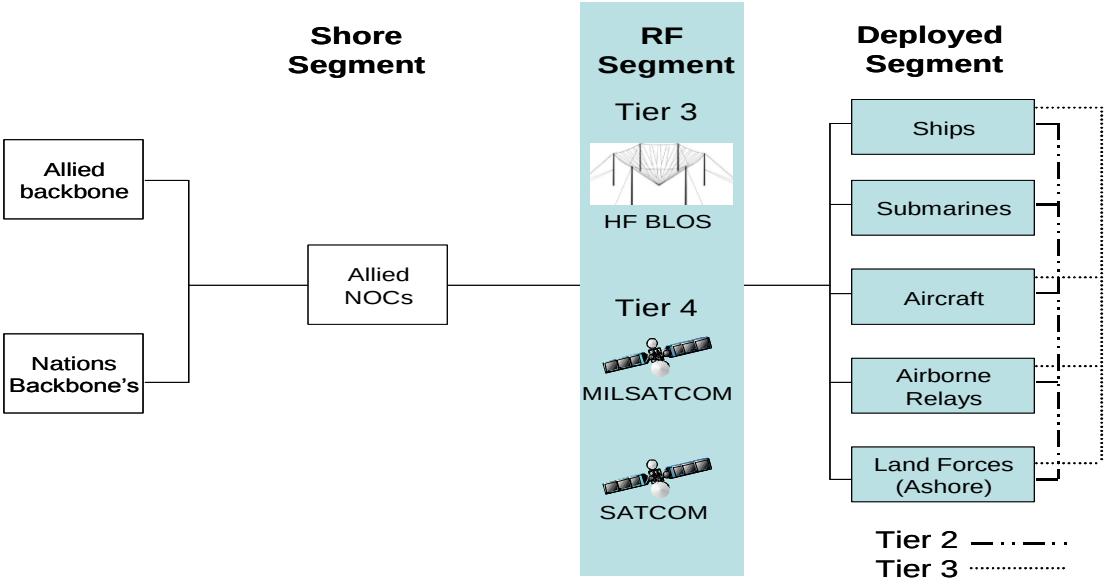

Figure 7–2 Communications Architecture

Uncontrolled copy when printed

710. The goal is for each traffic flow to be routed over the lowest tier capable of servicing the flow, thereby mitigating congestion at the higher tiers, which offer greater distances and more consistent connectivity.

COMMUNICATION SUBNETS / COMMUNICATION BEARERS

711. IP was designed around a land-based communications infrastructure that would be built on highly reliable, wideband and low-latency transmission media such as copper wires or optical fibres. A MTWAN relies on RF bearers of various forms including half-duplex and point-to-multipoint with a limited number of radios and radio frequencies. Full-duplex point-to-point bearers (such as ISDN, INMARSAT) can interface directly to routers. However, interface equipment is usually required to facilitate connection between routers with standard Serial or Ethernet interfaces over tactical RF bearers.

712. The characteristics of the bearer in question (i.e. whether it is half-duplex or full-duplex, whether it is broadcast or non-broadcast and whether it is a high-latency circuit over a satellite) will determine the interface technology. Table 7–1 lists the bearers as well as subnets.

Bearers / Subnets	Link Rate	Typical Use	Subnet Characteristics
INMARSAT B	64- 128 Kbps	1. Main Data Bearer providing reachback capability to National 2. Network Operations Centers.	Full-duplex, point-to-point. Increased data rates and multiplex capability achievable with improved Modems
UHF SATCOM 25Khz	up to 48Kbps	Email, Chat, Low data DCP, COP	Limited IP capability, multi-member subnet
UHF SATCOM 5 Khz	up to 9.6kbps	Email, Chat, COP	Requires astute operation to optimise performance, multi-member subnet
HF 5066 IP	4.8-9.6 Kbps	Email, Chat, COP, Low data DCP	Data rate dependent on range and atmospheric propagation characteristics High Overhead.
Subnet Relay: VHF/UHF	up to 96Kbps (25KHz channel BW)	Email, Chat, Low data rate DCP, COP, non-constant bit rate traffic.	Multimember network Limited to LOS (UHF ~20nm, VHF ~80nm) Capable of relaying beyond LOS
Subnet Relay: HF	up to 9.6 kbps (SSB) 19.2Kbps (ISB)	Email, Chat, Low data rate DCP, COP, non-constant bit rate traffic.	Multimember network Limited to ELOS (HF ~150nm) Capable of relaying beyond LOS
HF BLOS	4.8-9.6Kbps (SSB)	Email, Chat, COP, Low data DCP	HF Skywave, Ranges of 2000-3000 Nm achievable Increased data rates achievable with ISB

Uncontrolled copy when printed

HF ELOS	4.8-9.6Kbps (SSB)	Email, Chat, COP, Low data DCP	HF Surface Wave, Ranges of 200-300Nm achievable Increased data rates achievable with ISB
GBS/TBS/DBS	512Kbps+	Receive only broadcast	Capability available in many large platforms Integration into MTWAN Under development
ISDN	64-2048 s	Used while units are alongside or for trunk communication between NOCs. May solve land based point-to-point connectivity requirements.	Full-duplex, point-to-point Low latency

Table 7–1 Communication Subnets Matrix

COMMUNICATION BEARERS/SERVICES

713. A variety of RF and telecommunication services are available to resolve MTWAN connection requirements. Selection of a service or bearer will depend on a variety of factors including information exchange requirements, radio assets, geographic location and resource constraints. This section provides a brief overview of some typical Communication Bearer/Services available to solve WAN connectivity issues.

INTEGRATED SERVICES DIGITAL NETWORK (ISDN)

714. ISDN is a set of protocols that allow the user to fully integrate voice and data services over a single communication telephone line. ISDN lines are normally leased from the local telecommunication service provider and can provide a dedicated full-duplex, point-to-point link for digital network communication. ISDN lines are often used as a means to provide connectivity between fixed land-based units such as Communication Stations and shore-based NOCs. As ISDN is a public data network, information transmitted over ISDN must be protected with a Type 1 encryption device.

INMARSAT B

715. INMARSAT is a commercial satellite system used for voice and up to 128Kbps data connectivity. The system uses geostationary satellites to provide near global coverage for maritime and land force elements. Because it uses geostationary satellites the connection has a high latency, which makes it less efficient for TCP. Regardless, it has been extensively used by nations to provide reachback connectivity between mobile units and shored-based NOC.

Uncontrolled copy when printed

As a commercial satellite system the expense of this connection can be prohibitive. To limit budget over-runs and provide fixed cost many nations lease dedicated INMARSAT channels.

716. Several variances of INMARSAT exist and various methods exist to improve data throughput. More detail on the INMARSAT system can be found at Annex A to this chapter.

HIGH FREQUENCY BEYOND LINE-OF-SIGHT (HF BLOS)

717. Various investigations have been conducted in order to provide a viable HF BLOS solution. HF BLOS subnets use skywave RF links to provide connectivity. As such, these types of connections are generally point-to-point solutions with very low data rates. The high BER of HF makes this type of channel unsuitable for TCP connectivity. Various techniques have been developed to improve this; however, as yet no deployable HF BLOS solution exists.

HIGH FREQUENCY EXTENDED LINE-OF-SIGHT (HF ELOS)

718. HF ELOS uses the HF ground wave to provide data connectivity between MTWAN units. The high BER and narrow bandwidth limit this connection to relatively low data rates; however, this may provide a viable solution for disadvantaged units with low Information Exchange Requirements (IERs). Several technologies have been employed to provide ELOS solutions although no nation has yet adopted this as a primary network connection between mobile units.

SUBNET TECHNOLOGIES

719. Various subnet technologies can be employed in a MTWAN to provide IP connectivity over tactical RF bearers, several of which are described below.

SUBNET RELAY (SNR)

720. SNR provides a multi-node, multi-hop mobile-to-mobile IP connectivity over VHF/UHF LOS and HF ELOS. SNR uses relay nodes to extend the coverage of a subnet beyond a single hop. SNR also fulfils the requirement to allow subnets to be formed when network connectivity between all Task Group members is not complete. SNR is seen as a viable solution to providing a tactical IP network, reducing the reliance on satellite circuits, and providing communication redundancy. SNR has been proven at sea using existing radio equipment. SNR is further explained at Annex B to the chapter.

HF IP

721. HF IP provides IP networking over a HF data communications system. The system is based on STANAG 5066 and uses a modified Token Ring protocol. The system is intended for use with surface wave paths which provide Extended Line Of Sight (ELOS) coverage of up to 200 nm at sea. However, it can be used to support Beyond Line Of Sight (BLOS) using sky wave with proper selection of frequency, antenna and data rate. HFIP is further explained in Annex C to this chapter.

Uncontrolled copy when printed

MEDIUM-RATE CHANNEL ACCESS PROCESSOR (MCAP)

722. MCAP provides a solution for IP forwarding over broadcast communication systems such as UHF SATCOM. The MCAP has been designed by the USN and is not available for commercial release.

STANDARD NATO AGREEMENT (STANAG) 5066 EDITIONS 1 AND 2

723. STANAG 5066 Edition 1 is a link protocol for data transmissions over HF. The standard also provides the recommended requirements for an IP Router interface and an interface for SMTP email. Edition 2 of the standard, in advanced draft phase, will provide the mandatory requirements for a multi-member, full IP services subnet over HF ELOS. More details of STANAG 5066 can be found at Annex C.

CONCLUSION

724. Military and Commercial communication subnets engineered to provide IP networking can support MTWAN operation in the mobile environment. A variety of methods are used to improve the efficiency over MTWAN subnets. These methods are deployed dependant upon the data type and operational limitations imposed. Efficiency of a data transfer will largely be dependant upon capability of the RF bearers available and the protocols and tools used during the data exchange.

Uncontrolled copy when printed

SUBNET RELAY

INTRODUCTION

1. A relay capability is essential to provide effective ship-ship information transfer. Subnet Relay (SNR) provides for the formation of *ad hoc*, self-configuring, multi-platform, multi-hop, tactical IP Internet at sea using conventional HF/VHF/UHF LOS and ELOS bearers, and existing radio equipment. It fulfils the requirement to allow for the formation of subnetworks when network connectivity between Task Group members is incomplete. SNR can provide efficient near real-time tactical IP networking connectivity within a MTWAN while reducing the reliance on SATCOM, providing indirect access to SATCOM to ships without such resources, and providing communication redundancy.

AIM

2. The document provides a Concept of Operations for Subnet Relaying.

OVERVIEW

3. This document defines the user requirements, operational concept, capabilities and technical limitations and initial assumptions for a mobile tactical WAN SNR network.

USER REQUIREMENT

4. Satellite communications is used extensively in naval operations. Nevertheless, there are many naval platforms that have insufficient or are not equipped with SATCOM resources. This situation is expected to worsen as the availability of SATCOM channels is becoming limited and very expensive. While bandwidth requirements continue to increase, it is becoming increasingly difficult for the military to compete with high-paying commercial customers for access to commercial satellite channels. For cost and availability reasons, navies must reduce their reliance on such resources. Moreover, there are vulnerability and survivability issues that dictate a requirement for a backup or alternative to SATCOM. Consequently, satellite communications cannot provide an all-encompassing solution for operational network communications between ships at sea. While satellite communications are an important element of the solution, there is a requirement to make use of all available communication bearers to provide an affordable naval task group ubiquitous networking capability.

5. The operational requirements are thus to:

a. Alleviate the reliance on SATCOM;

Uncontrolled copy when printed

b. Provide communications redundancy;

c. Provide an IP networking capability to non-SATCOM ships;

d. Provide indirect access to SATCOM to ships without SATCOM; and

e. Significantly improve interoperability within our Allies as well as within a coalition task group, in particular to improve interoperability with lesser equipped navies.

6. The operational requirements are complemented with the functional requirements to provide:

a. An *ad hoc* tactical IP internetworking capability between ships in a national and/or coalition task group using LOS/ELOS tactical communication bearers; and

b. A multi-node, multi-hop, ship-to-ship network with a relay capability (i.e. at Layer 2) using IP protocols.

7. Maximising the use of all available bearers within the task group provides a feasible alternative to SATCOM, in forming a communications backbone for the MTWAN. UHF LOS and HF ELOS are bearers available on most naval platforms, while VHF LOS and HF BLOS provide useful additions. The operational networking communications concept is shown at Figure 7–A–1.

OPERATIONAL CONCEPT

8. SNR is most easily explained with a few scenario diagrams where ships are not all within LOS. The scenario that will be considered is that of two battle groups where a ship moves from one battle group to the other. The scenario is depicted through Figures 7–A–2 to 7–A–8. The notion of relaying is depicted in Figure 7–A–2. This figure illustrates a ship (red ship to the left) wanting to communicate with another ship (red ship to the right) within the same battle group but beyond its line-of-sight (black circles). Since direct communication is not possible, the ship originating the traffic will call upon another ship, a relay ship (blue), which is within LOS communications of the source and destination ships to relay the information.

9. Each ship within the battle group becomes aware of those ships it can reach directly and those it can reach via relay(s). Thus, all ships within this battle group automatically form a single SNR (self-configuring) subnetwork.

Uncontrolled copy when printed

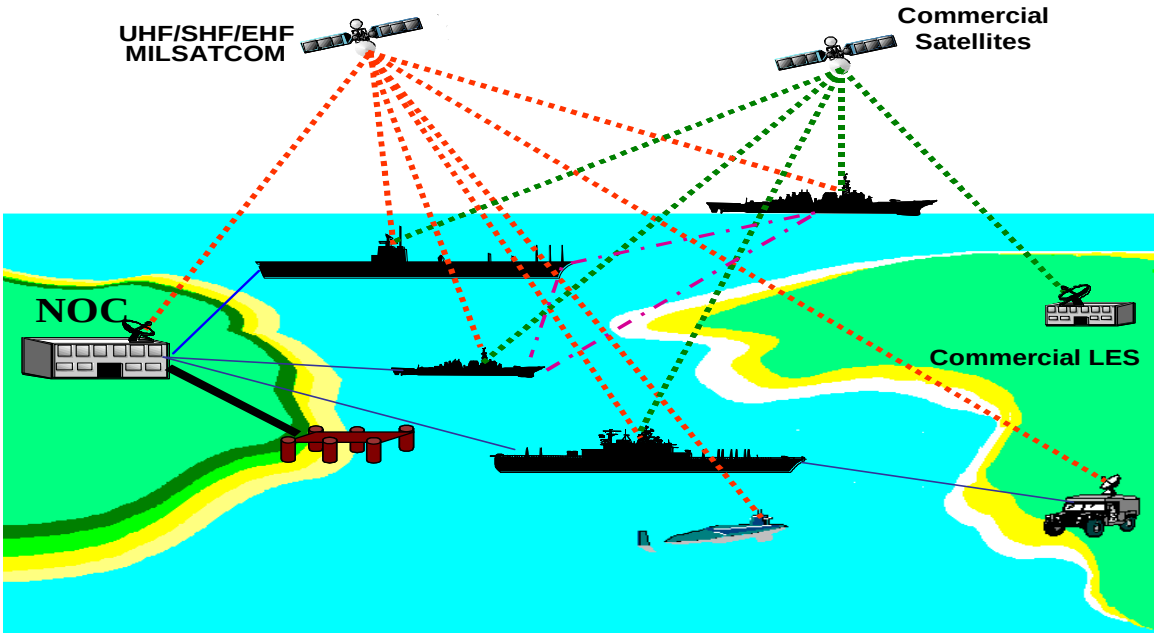

Figure 7–A–1 Operational View

10. Figure 7–A–3 merely illustrates that a ship is moving from one battle group to the other battle group. During the move, it will continue to communicate with members of the battle group.

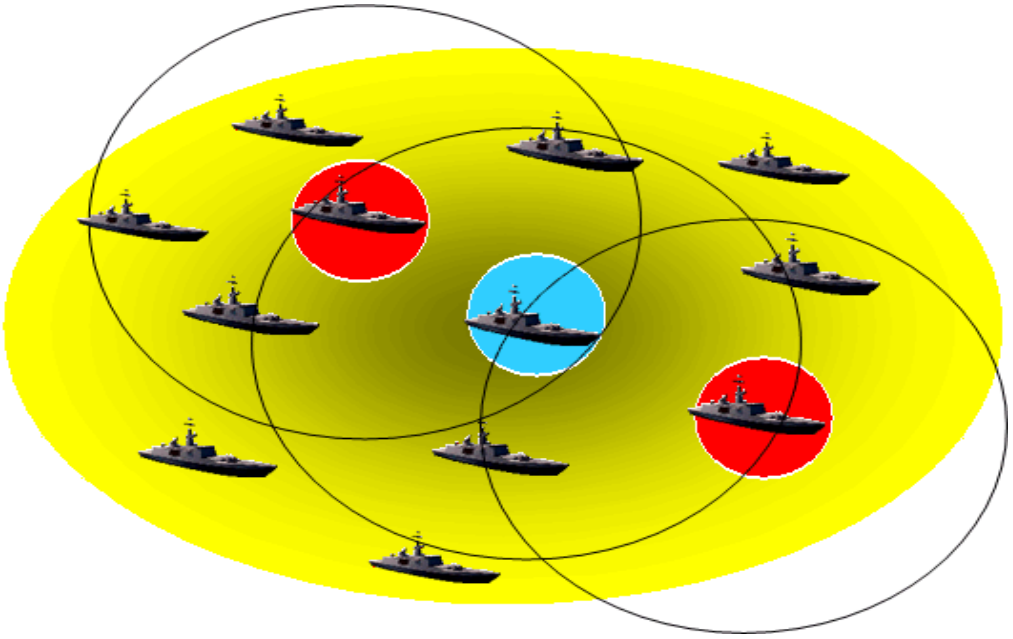

Figure 7–A–2 Relaying Concept

Uncontrolled copy when printed

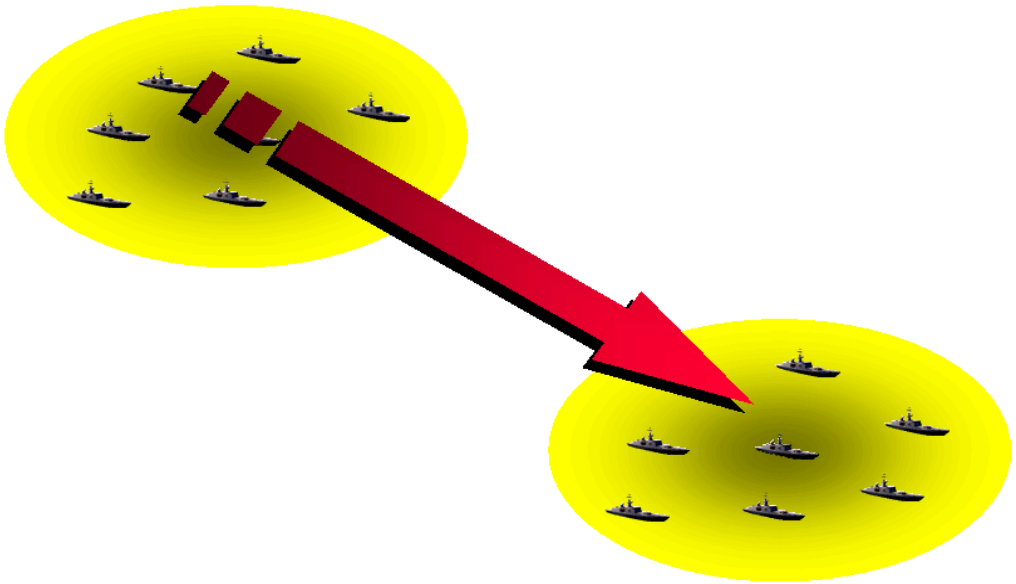

Figure 7–A–3 Ship Moving from one Battle Group to Another

11. Figure 7–A–4 illustrates that as our ship is moving toward the other battle group, it may change its relay ships. In this example, the moving ship has moved outside of direct communication with the ship it was using as a relay before and, therefore, picks another ship that is in contact with him as the relay point. This illustrates that the subnetwork is dynamically updating its relay architecture as the ships move. It is also shown that the ship can use other ships as relay, as appropriate, to reach other ships within the battle group. Any ship can have more than one relays and relays are picked up dynamically.

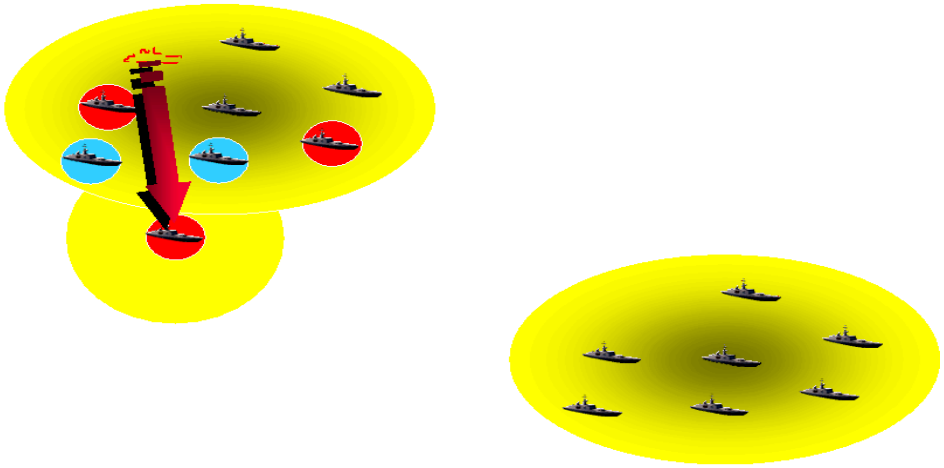

Figure 7–A–4 Multiple, Dynamic Relays

12. As the ship is moving toward the other battle group, it may find itself within LOS communication range from another ship. In such a case (Figure 7–A–5), the two ships can communicate directly, without the need for a relay ship.

Uncontrolled copy when printed

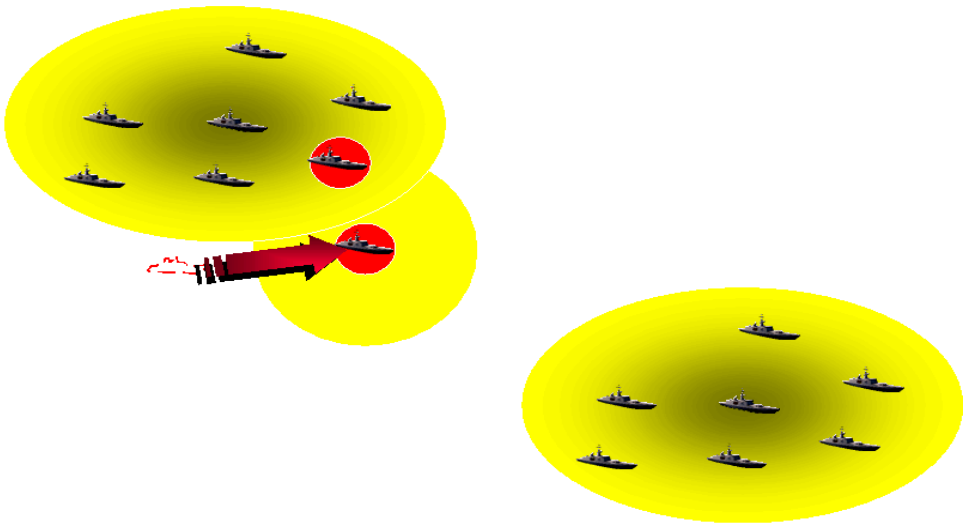

Figure 7–A–5 Relaying only when needed

13. As the ship continues to move away from its initial battle group, it may find itself outside of communication range from any ships in either of the two battle groups. In such a case (Figure 7-A-6), he will be de-affiliated from its initial battle group SNR subnetwork, and the ship will form its own SNR subnetwork.

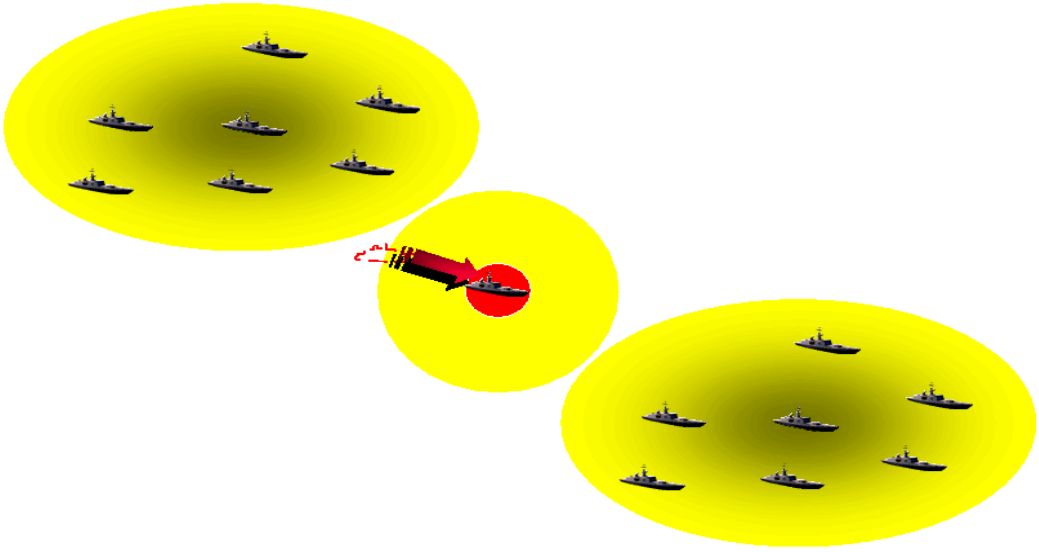

Figure 7–A–6 Subnetwork Splitting

14. Eventually the ship arrives within LOS communication range of the other battle group. At that time, the two SNR subnetworks (single ship and second battle group) will merge to form a single SNR subnetwork (Figure 7–A–7). As before (Figure 7–A–5), the ship can communicate directly, without relay, with other ships within LOS.

Uncontrolled copy when printed

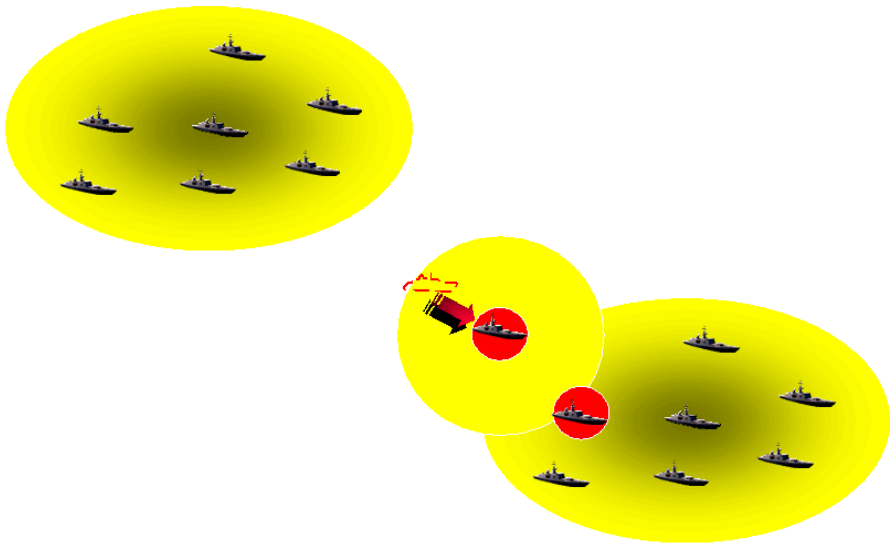

Figure 7–A–7 Subnetwork Merging

15. Figure 7–A–8 illustrates that in this new battle group, multiple relays may be required from source to destination. SNR can accommodate up to 4 relays (5 hops) from source to destination.

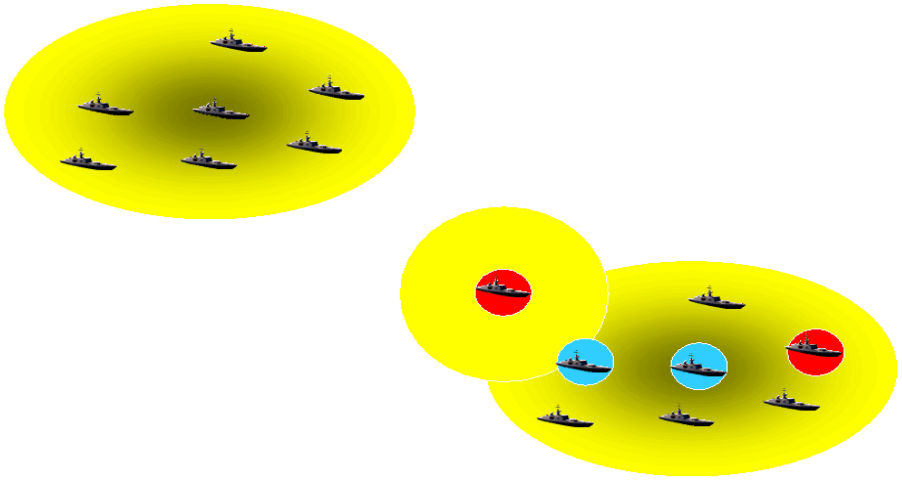

Figure 7–A–8 Multiple Relays to Destination

Uncontrolled copy when printed

CAPABILITIES

16. A MTWAN SNR network is limited to 16 users (platforms), with the maximum number of relays being 4 (allowing 5 hops, which will cover approx 150nm in a straight line assuming 30nm LOS distance, or more than a 1000 nm for HF ELOS).

17. A MTWAN SNR network will be capable of fully distributed (e.g. masterless) and automatic operations.

18. A MTWAN SNR network will be capable of allocating bandwidth in proportion of each platform instantaneous traffic load.

19. SNR is a self-configuring, self-organizing network technology. The SNR will re-configure within 2-3 minutes when a UHF link or many links are lost, or when a new link (new member) appears.

20. SNR will be capable of supporting medium bandwidth applications such as DCP, COP dissemination, web browsing, FTP, email with attachments, etc.), and be capable of supporting more bandwidth intensive applications if faster communication links are provided.

21. SNR will allow for bulk encryption at the Link Layer. The encryption strength will be dictated by the cryptos used in conjunction with the SNR system. SNR will be capable of interfacing to national cryptos used in AUSCANNZUKUS nations.

22. Achieve coded data rate of 2.4kbps to 16kbps using HF ELOS (SSB) with high speed HF modems. In the future, higher data rates could be achieved using new waveforms, ISB radio, or multiple non-adjacent HF channels.

23. Achieve coded data rate of 16kbps to 96kbps using UHF LOS over a standard 25 kHz audio frequency interface channel. In future, much higher than 96kbps coded data rate could be achieved using greater than 25kHz bandwidth, such as the intermediate frequency (IF) channel on radios that support this function.

24. Provide capability to manually initiate and terminate relays (used in an EMCON environment).

Uncontrolled copy when printed

TECHNICAL LIMITATIONS AND INITIAL ASSUMPTIONS

25. A number of design parameters were provided by AUSCANNZUKUS for the design of an SNR system. In addition, to the items listed in the previous section, they are:

a. There are a limited number of radios available onboard sea-going units, therefore subnets will probably be limited to a single radio/frequency. A SNR system will be capable of operation when untethered (mobile) platforms have a single half-duplex radio per subnet;

b. All nodes (platforms) are mobile, therefore relay platforms must be selectable automatically and dynamically;

c. Reliable and unreliable link operations must be supported;

d. A subnet will be made up of bearers of a single nature (e.g. all HF BLOS, all UHF LOS etc);

e. Platforms have access to a reliable clock; and

f. Tx/Rx switching times of the order of 20 ms using HF and 50 ms using UHF are expected of current naval radios.

Uncontrolled copy when printed

HIGH FREQUENCY INTERNET PROTOCOL (HF IP)

INTRODUCTION

1. HF IP provides IP forwarding over a HF data communications system. The system is based on STANAG 5066 and uses a modified Token Ring protocol as a media access control protocol over a shared broadcast HF channel. HF IP also provides dynamic routing based on the OSPF routing protocol.

2. HF IP supports multi-node IP networking over the air at data rates up to 9600 bps for single sideband and up to 19200 bps for two independent sidebands. Data rates are dependent on propagation conditions, distance and equipment.

3. The system is intended for use with surface wave paths which provide Extended Line Of Sight (ELOS) coverage of up to 200 nm at sea. However, it can be used to support Beyond Line Of Sight (BLOS) using sky wave with proper selection of frequency, antenna and data rate.

4. The only implementation of the HF IP has been jointly developed by the USN Space and Naval Warfare Systems Center San Diego and NATO C3 Agency. This implementation is currently not commercially available.

AIM

5. This Annex provides general guidance on the set-up and use of HF IP.

OVERVIEW

6. HF has traditionally been used for low data rate communications, often in a broadcast manner, in which broadcast transmissions will be received by many stations at the same time.

7. With current modem technology, HF can support data rates over the air of up to 9,600 bps over Upper Side Band (USB) operations and up to 19,200 bps over Independent Side Band (ISB).

8. Commercial implementations based on STANAG 5066 Edition 1.2 support Simple Mail Transfer Protocol (SMTP) E-mail or IP forwarding using the Carrier Sense Multiple Access (CSMA) protocol to allow multiple nodes to share a half-duplex and single channel. The CSMA protocol is simple to implement, but very inefficient as the data throughput suffers from retransmissions due to collisions.

Uncontrolled copy when printed

9. The Token Ring protocol proposed for STANAG 5066 Edition 2 provides a more efficient media access protocol for multi-node ad-hoc networks, in comparison with CSMA. The protocol is distributed as there is no master-slave relationship between nodes, and nodes can join and leave at any time.

DESCRIPTION

10. HF IP provides a means to forward IP traffic over a HF data communications system comprising modems, transmitters, receivers, power amplifiers and antennas. Figure 7-B-1 shows a typical network configuration of a node that makes use of HF IP. The installation of an HF IP system consists of an HF IP Interface, known as RF Controller, a link crypto, an HF modem capable of supporting ISB, and HF radio equipment. The figure also shows other communications subnets to which the node can be connected.

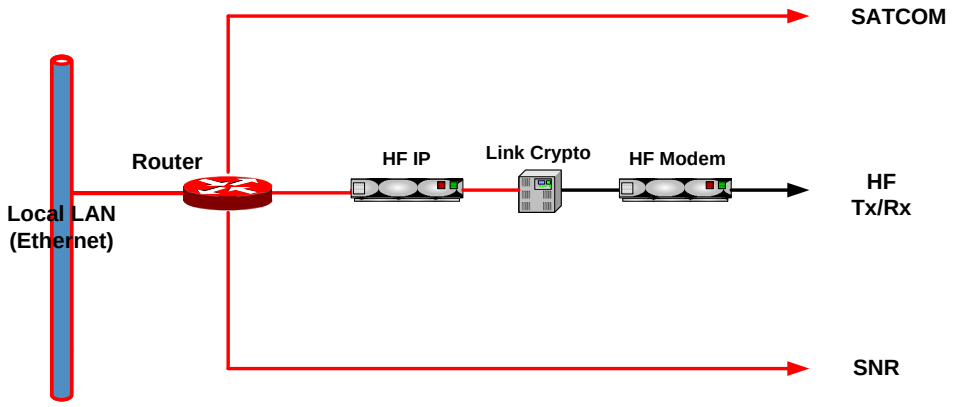

Figure 7–B–1 Typical Network Node Configuration

11. HF IP can be used in various network topologies. An example scenario will be that non-SATCOM ships will use HF IP to connect to a Wide Area Network (WAN) via a gateway ship that has a high bandwidth SATCOM connection to a Network Operations Center (NOC) ashore.

12. The HF IP interfaces with a COTS router that acts as the gateway for the local LAN. The router will determine whether HF or some other bearers will be used to forward IP packets, based on OSPF metrics or policy-based routing policies.

13. The HF IP is connected to the router via an Ethernet sub-net and to a HF modem via a link crypto over a synchronous serial interface.

14. The HF IP supports the OSPF routing protocol and therefore can act as a default gateway for the local LAN without the use of a separate COTS router.

Uncontrolled copy when printed

CRYPTOGRAPHIC REQUIREMENTS

15. KG-84C or KIV-7HSB can be used to provide Type 1 (High Grade) protection for exchanges of classified data over the air. The equipment will need to be configured to support Time Division Multiple Access operations.

TECHNICAL LIMITATIONS

16. A ring can fail if one node of the ring loses two-way communications to any other members of the ring.

17. Some TCP-based applications may not work over HF IP due to its low bandwidth and high latency. When multiple bearers are available, HF IP should only be selected for forwarding IP packets of delay-tolerant applications. In order to control the IP traffic flow across multiple bearers, Quality-of-Service (QoS) or policy-based routing will have to be used.

18. The system can support two-hop relays. However, this capability only functions in a three-node network, so that the network latency can be kept down to an acceptable level.

Uncontrolled copy when printed

GLOSSARY OF TERMS

ACRONYMS

ACIXS	Allied Communication Information Exchange System
ACL	Access Control List(s)
ACP	Allied Communications Publication
ADNS	Automated Digital Network System
ALE	Automatic Link Establishment
ARQ	Automatic Repeat Request
AS	Autonomous System
ASN	Autonomous System Number
ASBR	Autonomous System Boundary Router
ASCII	American Standard Code Information Interchange
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Organisation
AUS	Australia
BER	Bit Error Rate
BERT	Bit Error Rate Test
BIND	Berkeley Internet Name Domain
BGP	Border Gateway Protocol
BLOS	Beyond Line of Sight
BPD	Boundary Protection Device
CA	Canada
CAP	Channel Access Processor
CAR	Committed Access Rate
CAS	Collaboration At Sea
CATF	Commander Amphibious Task Force
CBWFQ	Class Based Weighted Fair Queuing
CCEB	Combined Communications-Electronics Board
CCI	Controlled Cryptographic Item
CELP	Code Book Excited Linear Predictive
CENTRIXS	Combined Enterprise Regional Information Exchange System

Uncontrolled copy when printed

CFE	CENTRIXS Four Eyes
CFLCC	Coalition Force Land Component Commander
CFMCC	Coalition Force Maritime Component Commander
CIDR	Classless Inter-Domain Routing
CIK	Crypto Ignition Key
CJTF	Commander Joint Task Force
CODS	Coalition Data Server
CONOPS	Concept of Operations
COP	Common Operational Picture
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off The Shelf
COWAN	Coalition Operations Wide Area Network
CQ	Custom Queuing
CRIU	CAP to Router Interface Unit
CST	COP Synchronization Tool
CSU	Crypto Support Unit
CT	Cipher Text
CTF	Commander Task Force
CTG	Commander Task Group
CWAN	Coalition Wide Area Network
CWC	Composite Warfare Commander
DAC	Discretionary Access Control
DAMA	Demand Assigned Multiple Access
DBS	Direct Broadcast Service
DCP	Distributed Collaborative Planning
DNS	Domain Name Service
DTD	Data Transfer Device
DVMRP	Distance Vector Multicast Routing Protocol
EKMS	Electronic Key Management System
ELOS	Extended Line of Sight
EMCON	Emission Control

Uncontrolled copy when printed

EoS	Elements of Service
FF	Fire Fly
FIFO	First In, First Out
FOTC	Force Over The Horizon Track Coordinator
FTP	File Transfer Protocol
GBS	Global Broadcast System
GCCS-M	Global Command Control System – Maritime
GCTF-1	Global Coalition Task Force One
GEM	General Dynamics Encryptor Management
GOTS	Government off the Shelf
GUI	Graphical User Interface
HAG	High Assurance Guard
HDR	High Data Rate
HF	High Frequency
HIT	High Interest Track
HSD	High Speed Data
HTML	Hyper Text Mark-up Language
HTTP	Hyper Text Transport Protocol
IANA	Internet Assigned Numbers Authority
ICE	Imagery Compression Engine
IDM	Information Dissemination Management
IDP	Information Dissemination Plan
IGMP	Internet Group Management Protocol
IIS	Internet Information Service
IM	Information Management
IMI	Information Management Infrastructure
IMAP	Internet Message Access Protocol
IMPP	Instant Message and Presence Protocol
INE	In-line Network Encryptors
INMARSAT	International Maritime Satellite Organisation
IP	Internet Protocol

Uncontrolled copy when printed

ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IWC	Information Warfare Commander
IXS	Information eXchange System
JCSS	Joint Command Support System (Australia)
JMUG	JMCIS Multicast Gateway
KMID	Key Management Identification
LAN	Local Area Network
LDAP	Light Directory Access Protocol
LES	Land Earth Station
LMD/KP	Local Management Device / Key Processor
LOS	Line of Sight
LSA	Link State Advertisements
MAC	Media Access Control
MAG	Maritime Air Group
MCAP	Medium Data Rate Channel Access Processor
MCOIN	Maritime Command Operations Information Network (Canada)
MDP	Multicast Dissemination Protocol
MDR	Medium Data Rate
METOC	Meteorological/Oceanographic
MFTP	Multicast File Transfer Protocol
MMF	Multi-National Marine Force
MNTG	Multi-National Naval Task Group
MOSPF	Multicast Open Shortest Path First
MPLS	Multi-Protocol Label Switching
MSAB	Multinational Security Accreditation Board
MSeG	Multicast Service Gateway
MSL	Multi- Security Levels
MTA	Message Transfer Agent
MTWAN	Maritime Tactical Wide Area Network
NBAR	Network-Based Application Recognition

Uncontrolled copy when printed

NCW	Network Centric Warfare
NES	Network Encryption System
NM	Network Management
NNTP	Network News Transport Protocol
NOC	Network Operations Center
NRS	Naval Radio Station
NZ	New Zealand
OPCON	Operational Control
OPGEN	Operational General Messages
OPTASK	Operational Tasking Messages
OSI	Open System Interconnect
OSPF	Open Shortest Path First
OTCIXS	Officer in Tactical Command Information eXchange System
PAD	Packet Assembler Disassembler
PC	Personal Computer
PCM	Pulse Code Modulation
PIM	Protocol Independent Multicast
PKI	Public Key Infrastructure
PLAD	Plain Language Address Designator
P_MUL	Protocol Multicast
POP3	Post Office Protocol Version 3
PPK	Pre-Placed Keys
PPP	Point-to-Point Protocol
PQ	Priority Queuing
PT	Plain Text
QOS	Quality of Service
RED	Random Early Drop
RIP	Routing Internet Protocol
RF	Radio Frequency
RP	Rendezvous Point
RSVP	Resource ReServation Protocol

Uncontrolled copy when printed

RTF	Rich Text Format
RTT	Round-Trip Time
SHF	Super High Frequency
SIPRNET	Secret Internet Protocol Router Network (United States)
SMG	Secure Mail Guard
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNR	SubNet Relay
SOPS	Standard Operating Procedures
TBS	Theatre Broadcast Systems
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEK	Transmission Encryption Key
TG	Task Group
TGAN	Task Group Area Network
TOIS	Technical Operating Instructions
TOS	Type Of Service
TTL	Time To Live
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UID	Unit Identifier
UK	United Kingdom
US	United States
USS	United States Ship
VHF	Very High Frequency
VPN	Virtual Private Network
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Dropping
Z	Cryptographic Device

Uncontrolled copy when printed

LIST OF EFFECTIVE PAGES

Subject Matter	Page Numbers
Title Page	i
Forward	ii
Letter of Promulgation	iii
Record of Message Corrections	iv
Table of Contents	v to vii
List of Figures	viii
List of Tables	ix
Chapter 1	1-1 to 1-8
Annex A to Chapter 1	1A-1 to 1A-6
Chapter 2	2-1 to 2-12
Chapter 3	3-1 to 3-4
Annex A to Chapter 3	3A-1 to 3A-5
Annex B to Chapter 3	3B-1
Appendix 1 to Annex B to Chapter 3	3B1-1 to 3B1-87
Chapter 4	4-1 to 4-6
Chapter 5	5-1 to 5-9
Annex A to Chapter 5	5A-1 to 5A-2
Annex B to Chapter 5	5B-1 to 5B-5
Chapter 6	6-1 to 6-9
Annex A to Chapter 6	6A-1 to 6A-3
Annex B to Chapter 6	6B-1 to 6B-3
Chapter 7	7-1 to 7-7
Annex A to Chapter 7	7A-1 to 7A-8
Annex B to Chapter 7	7B-1 to 7B-3
Glossary of Terms	Glossary-1 to Glossary-6
List of Effective Pages	LEP-1

Uncontrolled copy when printed

ACP 200(C) Vol 2

Uncontrolled copy when printed