

UNCLASSIFIED

ACP 200

MARITIME TACTICAL WIDE AREA NETWORKING (MTWAN)

ACP 200



July 2004

Original

I
UNCLASSIFIED

UNCLASSIFIED

ACP 200

FOREWARD

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, MARITIME WIDE AREA TACTICAL NETWORKING (MTWAN), 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.

**THE COMBINED COMMUNICATIONS-ELECTRONICS BOARD
LETTER OF PROMULGATION
FOR ACP 200**

1. The purpose of this Combined Communications-Electronics Board (CCEB) Letter of Promulgation is to implement ACP 200 within the Armed Forces of the CCEB Nations. ACP 200, MARITIME WIDE AREA NETWORKING (MTWAN), is an UNCLASSIFIED publication developed for Allied use under the direction of the CCEB Principals
2. ACP 200 is effective upon receipt for CCEB Nations and when directed by the NATO Military Committee (NAMILCOM) for NATO nations.

EFFECTIVE STATUS

Publication	Effective for	Date	Authority
ACP 200	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

W. QUENNELL
Squadron Leader
CCEB Permanent Secretary

TABLE OF CONTENTS

Forward.....	II
Letter Of Promulgation.....	III
Record of Message Corrections.....	IV
Table of Contents.....	V
List of Figures.....	XII
List of Tables.....	XIV

Chapter 1
Introduction

101. Overview.....	1-1
102. Background.....	1-1
103. Aim.....	1-2
104. Capability.....	1-2
105. Applicability.....	1-3
106. Document Structure.....	1-3
107. Conclusion.....	1-5

Chapter 2
Maritime Tactical WAN Concept Of Operations

201. Introduction.....	2-1
202. AIM.....	2-1
203. Overview.....	2-1
204. System Objectives.....	2-1
205. Operational Requirements.....	2-2
206. Functional Capability.....	2-3
207. MTWAN System Description.....	2-5
208. MTWAN Deployment.....	2-7

Chapter 3
Information Management (IM)

301. Introduction.....	3-1
302. Aim.....	3-1
303. Overview.....	3-1
304. IM Impediments.....	3-4
305. IM Principles.....	3-5
306. Information Dissemination Management (IDM).....	3-6

Annex A to Chapter 3
Information Management Standard Operating Procedures

3A01. Introduction.....	3-8
3A02. Aim.....	3-8
3A03. Guidelines.....	3-8

3A04. Security	3-9
3A05. Information Dissemination Plan	3-9

Annex B to Chapter 3
OPTASK Knowledge Management (KM)

A. Overview	3-12
B. Administration	3-12
C. KM Requirements	3-13

Annex C to Chapter 3
Example of OPTASK Knowledge Management (KM)

Example of OPTASK KM	3-16
----------------------------	------

Chapter 4
SPARE

Chapter 5
Security

501. Introduction	5-1
502. Aim	5-1
503. Definitions	5-1
504. Network Topology	5-2
505. Points Of Presence / Boundary Protection Device	5-3
506. Risks	5-4
507. Responsibilities	5-6
508. Export Sanction	5-6
509. Assumptions	5-6
510. Recommended Security Architectures	5-7
511. Accreditation	5-11
512. Security Device Interoperability	5-11

Chapter 6
Messaging

601. Introduction	6-1
602. Aim	6-1
603. Overview	6-1
604. Types of Messaging	6-2
605. Multicast Messaging	6-3
606. Public Key Infrastructure (PKI)	6-3
607. Web Page Messaging	6-4
608. Command and Control	6-4
609. Messaging Selection	6-5
610. Summary	6-6

**Annex A to Chapter 6
Messaging Standard Operating Procedures**

6A01. Aim.....	6-7
6A02. E-Mail.....	6-7
6A03. OPNOTES.....	6-8
6A04. Chat.....	6-8

**Chapter 7
Common Operating Picture (COP)**

701. Introduction.....	7-1
702. Aim.....	7-1
703. Overview.....	7-1
704. Requirement.....	7-2
705. TOP COP (Fusion and Filtering).....	7-2
706. COP Management.....	7-3
707. COP Dissemination.....	7-3
708. Multicast Transport Services.....	7-4
709. Architecture.....	7-4
710. Selection of Appropriate COP Dissemination Method.....	7-6
711. Summary.....	7-7

**Chapter 8
Web Information Services**

801. Introduction.....	8-1
802. Aim.....	8-1
803. Overview.....	8-1
804. Objective.....	8-1
805. Information Quality.....	8-2
806. Network Architecture/Design.....	8-2
807. Concept of Operations.....	8-3
808. Software Environment.....	8-4
809. Domino Features.....	8-5
810. Posting of Information.....	8-6

**Annex A to Chapter 8
Web Services Standard Operating Procedures**

8A01. AIM.....	8-7
8A02. Web Architecture.....	8-7
8A03. Web Administration.....	8-7
8A04. Web Services Components.....	8-8
8A05. Posting Documents.....	8-10
8A06. Editing.....	8-10
8A07. Web Changes.....	8-10
8A08. MTWAN Replications.....	8-11

Chapter 9
Distributed Collaborative Planning

901. Introduction.....	9-1
902. Aim	9-2
903. Overview.....	9-2
904. Configuration.....	9-6
905. Bandwidth Limitations.....	9-7
906. Security	9-8
907. Tools	9-8
908. Requirements	9-8
909. Conclusions.....	9-9

Annex A to Chapter 9
Distributed Collaborative Planning Standards

9A01. Introduction.....	9-11
9A02. Standards.....	9-11

Annex B to Chapter 9
Distributed Collaborative Planning Standard Operating Procedures

9B01. Introduction.....	9-14
9B02. Aim.....	9-14
9B03. Description	9-14
9B04. User Access.....	9-17
9B05. Planning Order	9-18
9B06. Conduct.....	9-19
9B07. Tool Selection	9-21
9B08. Security.....	9-21
9B09. Network Engineering	9-22
9B10. Principles of Effective Meetings.....	9-22
9B11. Warnings and Precautions.....	9-23

Chapter 10
MTWAN Network Architecture

1001. Introduction.....	10-1
1002. Aim	10-2
1003. Technical Architecture.....	10-2
1004. Communication Links.....	10-6
1005. Security Architecture	10-7

Annex A to Chapter 10
Amphibious Operation Standard Operating Procedures

10A01. Introduction.....	10-8
10A02. Aim.....	10-8
10A03. Procedure	10-8

Chapter 11
Network Traffic Prioritization

1101. Introduction.....	11-1
1102. Aim	11-1
1103. Overview.....	11-1
1104. Implementation of Commander's Policy.....	11-3
1105. Implementation	11-4
1106. Conclusion	11-4

Chapter 12
Network Management

1201. Introduction.....	12-1
1202. Aim	12-1
1203. Overview.....	12-1
1204. NM Architecture (Hierarchy)	12-1
1205. NM Elements	12-2
1206. Remote or Local Management.....	12-4
1207. Generation of Reports.....	12-4
1208. Security Responsibility	12-4
1209. Tools	12-4

Annex A to Chapter 12
Network Management Standard Operating Procedures

12A01. Introduction.....	12-5
12A02. Aim.....	12-5
12A03. Scope.....	12-5
12A04. Network Management Tools.....	12-5
12A05. Network Management Strategy	12-5
12A06. Network Management Tools Set-up.....	12-7
12A07. Troubleshooting	12-8

Annex B to Chapter 12
OPTASK Net

A. Overview.....	12-10
B. Administration.....	12-10
C. Duties	12-10
D. Naming and Addressing.....	12-11
E. Routing	12-11
F. Subnets.....	12-11
G. Network Management.....	12-12
H. Applications	12-12

Appendix 1 to Annex B to Chapter 12
OPTASK Net (Example)

OPTASK Net (Example)	12-14
----------------------------	-------

Chapter 13 Transport Services

1301. Introduction.....	13-1
1302. Aim	13-1
1303. Overview.....	13-1
1304. Requirement.....	13-1
1305. Reliable Transport Tools.....	13-2

Annex A to Chapter 13 Multicast Service Gateway (MSeG)

13A01. Introduction.....	13-3
13A02. Aim.....	13-3
13A03. Overview.....	13-3
13A04. Supported Applications.....	13-4
13A05. Example Configurations	13-6
13A06. Graphical User Interface (GUI)	13-10

Chapter 14 Network Naming and Addressing

1401. Introduction.....	14-1
1402. Aim	14-1
1403. Overview.....	14-1

Annex A to Chapter 14 Naming and Addressing Standard Operating Procedure

14A01. Introduction.....	14-2
14A02. Aim.....	14-2
14A03. Host Naming Convention.....	14-2
14A04. Domain Naming Convention	14-4
14A05. IP Subnetting and Multicast Addressing.....	14-5
14A06. IP Addressing Convention	14-7
14A07. IP Address Authority Tasks	14-8
14A08. Unit Assignment of Hosts.....	14-8

Appendix 1 to Annex A to Chapter 14 IP Addressing

IP Addressing.....	14-9
--------------------	------

Annex B to Chapter 14 Domain Name Service Standard Operating Procedure

14B01. Introduction.....	14-11
14B02. Aim.....	14-11
14B03. Overview.....	14-11
14B04. DNS Servers.....	14-12
14B05. DNS Clients.....	14-14

UNCLASSIFIED

ACP 200

14B06. SMTP Mail and P_MUL14-14
14B07. Delegation for MTWAN Sub-domains14-15
14B08. Procedures for Setting-up DNS Servers.....14-16

**Chapter 15
Routing**

1501. Introduction.....15-1
1502. Aim15-1
1503. MTWAN System Description.....15-1
1504. Technical Architecture.....15-1
1505. Exterior Autonomous System Routing15-3
1506. Interior Autonomous System Routing Protocols15-8
1507. Reducing Routing Protocol Traffic to the Allied WAN15-10

**Annex A to Chapter 15
Metrics**

15A01. SPF Metric Values15-13

**Chapter 16
Communications Subnets
(for inclusion in change 1)**

List of Abbreviations

GlossaryLOA-1

List of Effective Pages

List of Effective PagesLOEP-1

List of Figures

Figure 1-1: Maritime Network Domains of Interest	1-3
Figure 1-2: ACP 200 Architecture	1-4
Figure 1-3: Document Structure	1-4
Figure 2-1: Determinants of Information Value	2-2
Figure 2-2: MTWAN High Level Network Concept.....	2-4
Figure 2-3: Routing Domain Architecture.....	2-5
Figure 2-4: MTWAN Topology.....	2-6
Figure 3-1: IM Hierarchy.....	3-2
Figure 3-2: C2 Decision Cycle	3-2
Figure 3-3: IDM.....	3-7
Figure 3-A-1: Sample Daily Operations Cycle.....	3-9
Figure 5-1: MTWAN Topology.....	5-2
Figure 5-2: Boundary protection devices between domains.....	5-5
Figure 5-3: MTWAN Connectivity	5-8
Figure 5-4: Air Gap Architecture.....	5-9
Figure 5-5: Networked Architecture.....	5-10
Figure 5-6: “Fully Integrated” Target Architecture	5-11
Figure 7-1: Traditional Environment (with IXS networks and CST).....	7-5
Figure 7-2: Full IP Environment (MTWAN).....	7-5
Figure 8-1: MTWAN Hub Configurations	8-2
Figure 8-A-1: MTWAN Architecture.....	8-7
Figure 8-A-2: Sample Web Page	8-9
Figure 9-1: Collaborative Planning Spectrum	9-2
Figure 9-2: DCP Characteristics	9-5
Figure 9-3: DCP Configurations.....	9-7
Figure 9-B-1: Bandwidth Aggregation.....	9-14
Figure 9-B-2: Operator Number Impact on Bandwidth.....	9-16
Figure 10-1: MTWAN Overview	10-1
Figure 10-2: MTWAM Autonomous System Description	10-2
Figure 10-3: Generic Ship Node Configuration.....	10-3
Figure 10-4: Generic Shore Node Configuration.....	10-4
Figure 10-5: Multiple Shore MTWAN Connections.....	10-5
Figure 10-6: CFMCC Node	10-6
Figure 10-7: MTWAN Subnet Combinations.....	10-7
Figure 10-A-1: MTWAN Transit Network Connectivity.....	10-8
Figure 10-A-2: MMF Node Configuration in Transit Phase	10-9
Figure 10-A-3: MTWAN Connection in Assault Phase.....	10-10
Figure 10-A-4: MMF Shore Node Configurations – Assault Phase.....	10-11
Figure 10-A-5: Ship Node in Assault Phase.....	10-11
Figure 10-A-6: MTWAN Network Connection in Lodgment Phase.....	10-12
Figure 10-A-7: MMF Network Nodes in Lodgment Phase.....	10-12
Figure 10-A-8: MTWAN Network in Sustainment Phase.....	10-13
Figure 10-A-9: MMF Unit 2 Node Configuration in Sustainment Phase.....	10-14

Figure 14-A1-1: IP Address.....14-9
Figure 14-B-1: Domain Name Schema.....14-11
Figure 14-B-2: DNS Servers.....14-13
Figure 15-1: MTWAN Router Protocol Stack.....15-3
Figure 15-2: Sample BGP Configuration15-5
Figure 15-3: Unicast Routing Layers.....15-8
Figure 15-4: Multicast Routing Layers.....15-9
Figure 15-A-1: Example of MTWAN Bandwidth for Coalition & National Subnets..15-14
Figure 15-A-2: Link Metric Values (Notional)15-15

List of Tables

Table 3-A-1: Information Dissemination Plan (IDP)3-11
Table 7-1: COP Dissemination Methods7-6
Table 9-1: DCP Spectrum.....9-3
Table 9-B-1: Bandwidth Toolset Spectrum9-13
Table 14-A-1: Abbreviations for ‘use’14-3
Table 14-A-2: Abbreviations for ‘type’14-3
Table 14-A1-1: IP Address Classes14-9
Table 15-A-1: Recommended Metric Values15-13

Chapter 1

INTRODUCTION

101 OVERVIEW

- a. A maritime mobile environment imposes unique limitations in terms of sharing information between maritime air, sea and embarked marine forces from different nations. A Maritime Tactical Wide Area Network (MTWAN) is an affordable IP based network developed to promote the effective and efficient sharing of information within this environment.
- b. A MTWAN can operate as a standalone network in the tactical environment. However, to support maritime information requirements it is most effective if the network is integrated into other operational and strategic networks. This then provides the tactical user with access to information that was previously unobtainable but is required to enable effective decision making in today's maritime environment.

102 BACKGROUND

- a. Due to the increased requirement for naval forces to operate in a coalition environment, operational commanders mandated the requirement to provide them with a "force multiplier" through the extension of IP based networking to sea. This would improve C4 effectiveness and enhance information exchange within joint and combined forces, across the spectrum of maritime operations (which includes amphibious and maritime air operations), by improving interoperability. This was initially achieved through the transfer of medium size data streams through strategic satellite bearers. However, the end goal of an efficient maritime mobile tactical WAN is the ability for Multi-national Naval Task Group (MNTG) units with varying communications capabilities to operate in a low bandwidth environment without the reliance on SATCOM. This will improve intra Task Force/Task Group information exchange, reduce unit reliance on SATCOM, support units that are not SATCOM capable and enable the efficient employment of communications assets (ie equipment and frequencies).
- b. The most practical approach to achieving the goal of an IP based network at sea was to "build a little, test a little" using already programmed exercises and demonstrations, real world operations, bilateral/multilateral operations and trials, test beds, and the Combined Federated Battle Laboratory Network (CFBLNet). This allowed for the development, trial, and refinement of

Concepts of Operation (CONOPS) and Standard Operating Procedures (SOPS). It also facilitated the re-configuration or refinement of various aspects of technical architectures and operational procedures found to be incompatible or inefficient during demonstrations.

- c. The initial aspects of a multi-national maritime WAN were demonstrated by AUSCANNZUKUS in JWID 97. This architecture was built on through the fielding of the RIMPAC 98 WAN. The AUSCANNZUKUS networking initiative with the influence of NATO C3 Agency representatives continued to evolve through R and D efforts while the US commenced fielding the closely aligned COWAN capability.
- d. In 1997 AUSCANNZUKUS was mandated to demonstrate and field a robust Maritime Tactical Wide Area Network (MTWAN). The documentation required to establish, operate and maintain this network resulted in the development and promulgation of this ACP. The network architectures, policies and procedures described herein closely align with those used in COWAN and NATO. While not a stand alone document, ACP 200 can be used as the principal reference for Multi-national Maritime IP Networking.

103 AIM

The aim of this publication is to provide guidance for the design, implementation, and operation of a MTWAN.

104 CAPABILITY

- a. A MTWAN is an important step towards a full network centric environment. Figure 1-1 illustrates information exchange domains within the tactical environment. A MTWAN enables full information exchange within the planning and coordination domains and has linkages to the support and real time tactical information exchange domains.
- b. Figure 1-1 represents a network approach vice the current 'stovepipe' approach. This provides a more effective and efficient employment of finite C4 resources and facilitates timely information flow between disparate C4 users

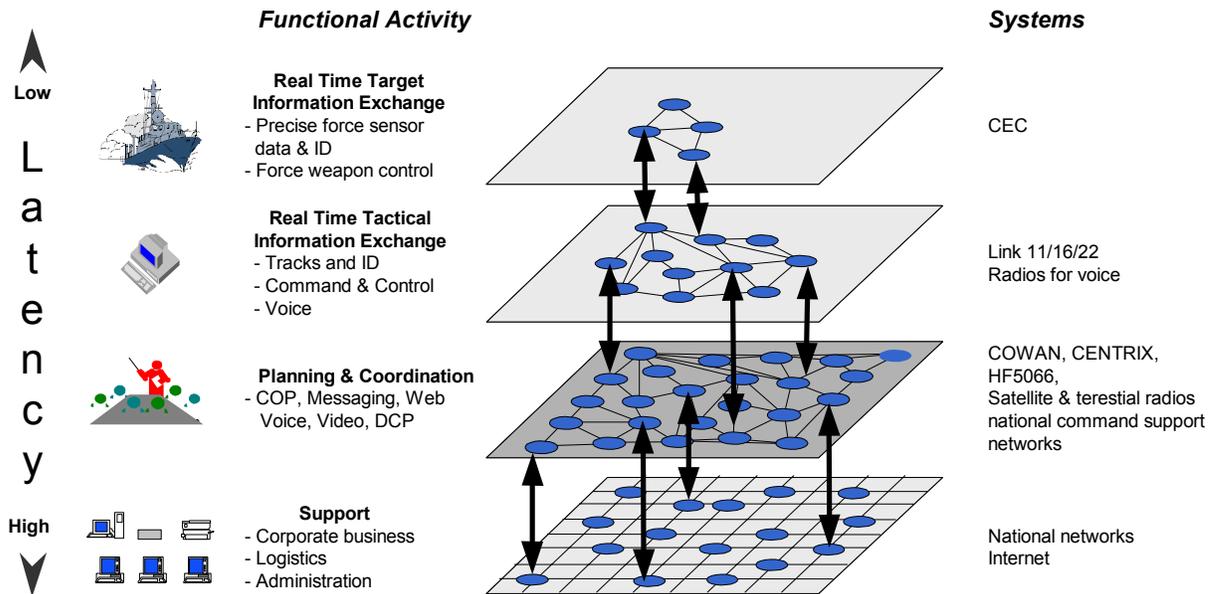


Figure 1-1: - Maritime Network Domains of Interest

105 APPLICABILITY

This publication is applicable to the operators and technicians who are responsible for the establishment, operations and maintenance of a Wide Area Network in a mobile tactical environment. This publication is designed for use in conjunction with other operational documents.

106 DOCUMENT STRUCTURE

Figures 1-2 and 1-3 describe the detailed document structure of the publication. Part 1 (indicated in yellow in Figure 1-2) is focussed towards the operators. It addresses the information infrastructure (the ‘infostructure’) and associated front-end application. For the most part, the information in Part 1 is of a general nature, which sets the framework for information transfer over a tactical WAN and highlights important issues for consideration. Part 2 (indicated in green in Figure 1-2) describes the technical infrastructure. These chapters are descriptive in content while the annexes, which comprise SOPs, and Technical Operating Instructions (TOIs) are prescriptive in the detail.

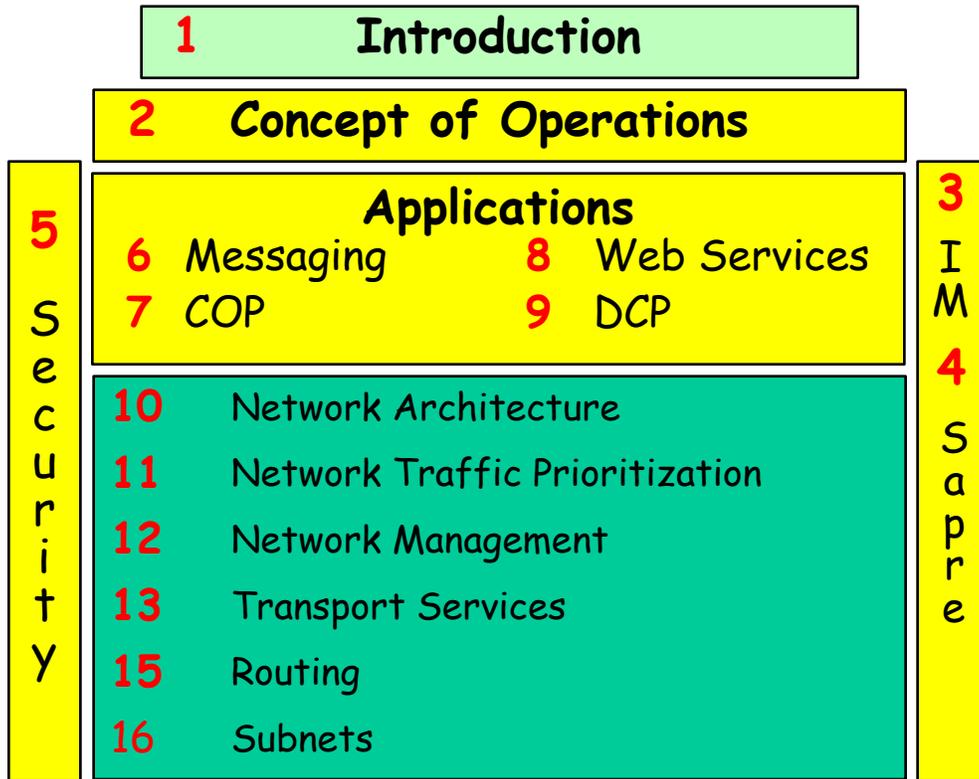


Figure 1-2: - ACP 200 Architecture

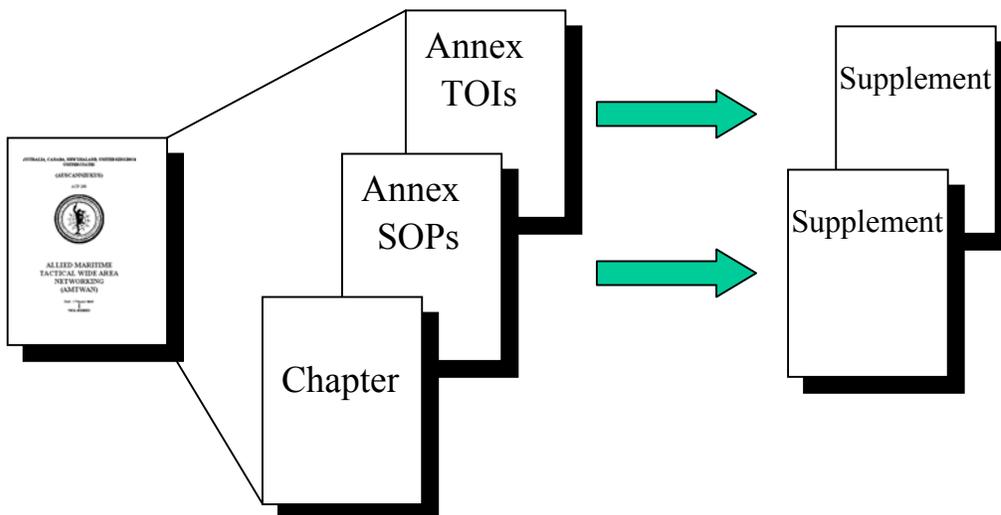


Figure 1-3: - Document Structure

107 CONCLUSION

A MTWAN provides an affordable, scalable high-level interoperability solution that can be integrated into existing and future national, combined, joint, allied, and coalition networks to support the tactical user. A MTWAN is a valuable system that enhances a Commander's ability to fight and win at sea.

Chapter 2

MARITIME TACTICAL WAN CONCEPT OF OPERATIONS

201 INTRODUCTION

Maritime units generally operate as a force whether as a part of a Task Force, Battle Group or Task Group. A MTWAN is designed to facilitate information sharing within this force structure, exploiting the benefits of IP technology. This chapter details the operational user requirements for information transfer, and documents the functional and systems views.

202 AIM

This chapter will provide the requirement and a CONOPS for the establishment and operation of a MTWAN.

203 OVERVIEW

A MTWAN is based on the following principles:

- An IP based network is the most efficient and effective method for transferring planning information within a force.
- Information transfer will take place in a peer-to-peer Secret-High network.
- Connections into/from other networks of a different security domain will be via approved border protection devices.
- Ship-to-ship and ship-shore information transfers will be via a variety of strategic and tactical communications (subnets).

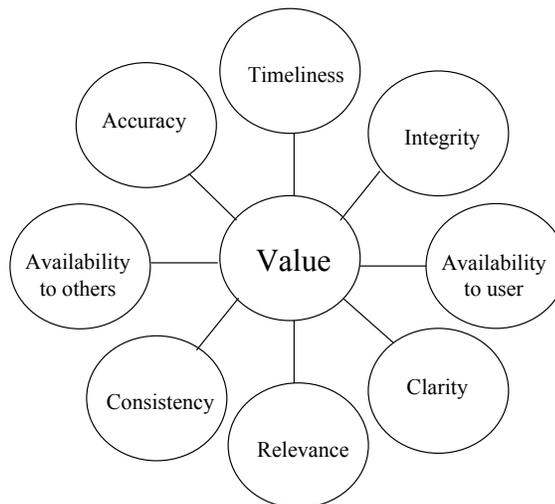
204 SYSTEM OBJECTIVES

A MTWAN must provide authorities at all levels and functions with timely and adequate data and information to plan, direct and control their activities, including operations, intelligence, logistics, personnel, and administration. Specific objectives include:

- Collaboration and Unity of Effort.
- Exploitation of Total Force Capabilities.
- Proper Positioning of Critical Information.
- Information Fusion.

205 OPERATIONAL REQUIREMENTS

- a. Generically, the two types of information used by the tactical user are Action and Planning information. Action information requires immediate action such as to attack the enemy or avoid attack from the enemy. Action information is therefore extremely time sensitive and is often unique to each individual and platform within the battlespace. Planning information is used as a basis for determining future action and is generally not so time sensitive. This information is common to planners and decision-makers throughout the battlespace and is normally stored in databases, web pages or files.
- b. Both types of information are valuable commodities. The extent of their value is determined by the characteristics represented in Figure 2-1. This can be further distilled to describe information in terms of the quality of information or its richness (ie the content, accuracy, timeliness and relevance of the information etc), and the degree to which it can be shared or its reach. The operational requirement for a MTWAN is to improve the richness and reach of planning information across the spectrum of maritime operations (which includes amphibious and maritime air operations).

**Figure 2-1: Determinants of Information Value**

- c. Regardless whether it is planning or action information, a fundamental precept of the MTWAN is the requirement for Information Management which is designed to promote the collection, collation, storage, processing and display of information enabling Commanders to gain superior knowledge, thus allowing them to make faster and more informed decisions in order to successfully complete their mission.

206 FUNCTIONAL CAPABILITY

- a. Allied maritime forces have traditionally employed “stovepipe” communications systems to support information exchange requirements. While stovepipe systems can be individually effective, collectively they are equipment intensive, do not enable the efficient use of bandwidth or data throughput and require use of military specific equipment and applications. In contrast, IP based networks allow the convergence of many types of data onto a single network. This simplifies network management, and enables efficient use of communication bearers, COTS applications and network equipment. An IP Network allows information to be presented to the warfighter in a variety of forms.
- b. A peer-to-peer secure network established at a secret high level enables the timely and efficient exchange of data (voice, video, e-mail, chat, web-services etc). A single security domain at the secret high level opposed to multiple security domains reduces the network resources, costs and complexity.
- c. The ability to exchange information between other networks and the tactical WAN through approved border protections devices enable information flows between National and Allied domains of different security levels. Approved border protection devices may include physical separation (air gaps) policies, approved security guards and firewalls.
- d. The network should support the following information types and applications while making the most efficient use of available communication capabilities:
 - Text messaging,
 - E-mail,
 - Video,
 - ATO and other large message files,
 - Imagery including maps and graphics,
 - Meteorological and Oceanographic data,
 - Indications and Warning,
 - Targeting Environment,
 - Intelligence,
 - Common Operational Picture,
 - Collaborative planning data,
 - Web Browsing, and
 - Voice.
- e. The large volume of information capable of being exchanged over a tactical WAN necessitates the use of robust and efficient network protocols. Where

appropriate and practical, multicast (one-to-many) transport protocols are used.

- f. When data types (Voice, Video, e-mail, web and chat) are converged onto a single network, the requirement for prioritisation becomes an important consideration to ensure that time sensitive information is delivered before less urgent traffic. For example, Indications and Warnings information needs to be received ahead of admin traffic. Current networks do not discriminate between information content but can be manipulated to control data streams. Therefore, information, network and communications management techniques must be applied to ensure that the Commanders priorities for information delivery are met.
- g. To accommodate the disparate communications capabilities of maritime platforms, it is essential that information exchange within a force can be achieved by a variety of communications bearers. Figure 2-2 illustrates the communication bearers available to transfer information within a network e.g. commercial satellite communications (INMARSAT B), military ship-to-ship satellite nets (UHF SATCOM, SHF SATCOM), HF extended and beyond line of sight (HF ELOS/BLOS) and UHF line of sight (UHF LOS).

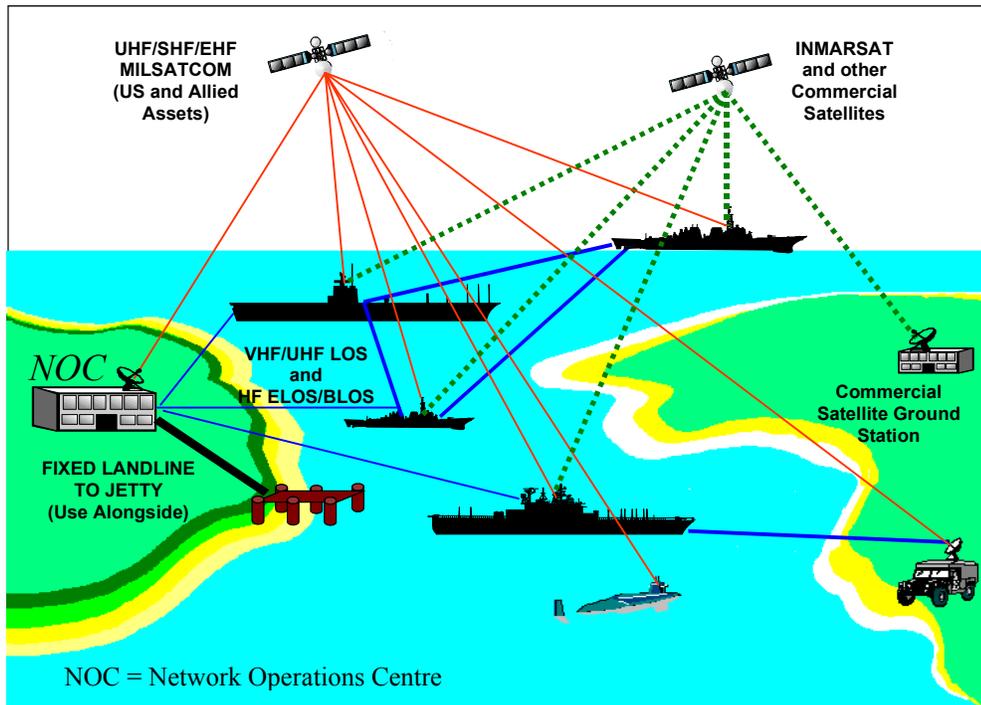


Figure 2-2: - MTWAN High Level Networking Concept

- h. Currently IP connectivity between maritime units is achieved by ship to shore point to point satellite communications links. The Tactical WAN seeks to

provide a seamless architecture between multiple maritime units networked with differing communications capabilities. Key to this will be a LOS relaying capability called Sub Net Relay(SNR) which is under development.

207 MTWAN SYSTEM DESCRIPTION

- a. **System Architecture.** A MTWAN architecture is driven by the constraints of the standard IP routing protocols used to achieve the operational connectivity. Routing will be accomplished using Open Shortest Path First (OSPF) and Protocol Independent Multicast (PIM) for interior-domain routing, and Border Gateway Protocol (BGP4) for exterior-domain routing. The result is that the network will be divided into Autonomous Systems (AS) and areas within an AS, as shown in Figure 2-3. The areas within an AS are connected by backbone subnets. All routing information is hidden within an AS and only reachable destinations are advertised between the AS.

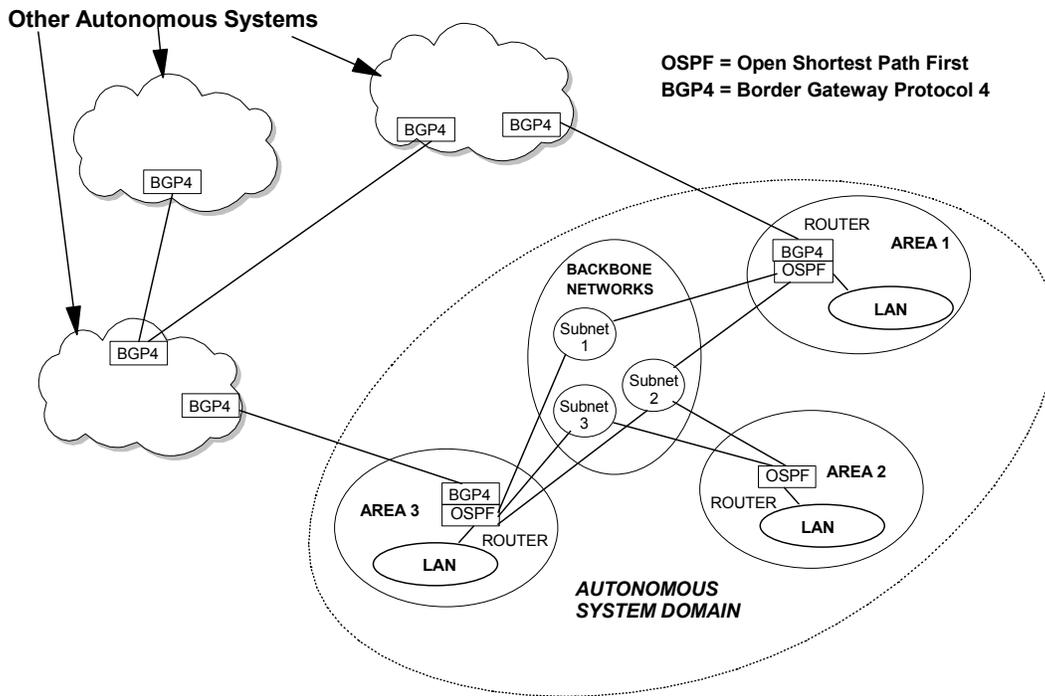


Figure 2-3: - Routing Domain Architecture

- b. **MTWAN Topology.** The architecture, translated to military network operations, is shown in Figure 2-4. Each MTWAN AS is a collection of allied units (a unit is defined as an area) and ultimately a shore communication station all connected by a collection of backbone subnets. Each shore communication station will have a router dedicated to each MTWAN AS,

shown as a building within the MTWAN AS. The MTWAN will operate via connection to an allied WAN. National systems may be connected to the allied WAN via security guards implemented as Boundary Protection Devices (BPDs). If no approved BPDs are available, information will be provided to the MTWAN via established national releasability procedures and channels as required. The MTWAN can be established and operated independent of other WANs. The shore station is the gateway into an allied backbone WAN, which is basically a network service provider much like the Internet. Multiple national shore stations and MTWAN systems can be included as operationally required. Other WANs, which participate in the coalition operations, are shown attached to the allied WAN. A separate AS within the MTWAN supports the Multinational Marine Force (MMF).

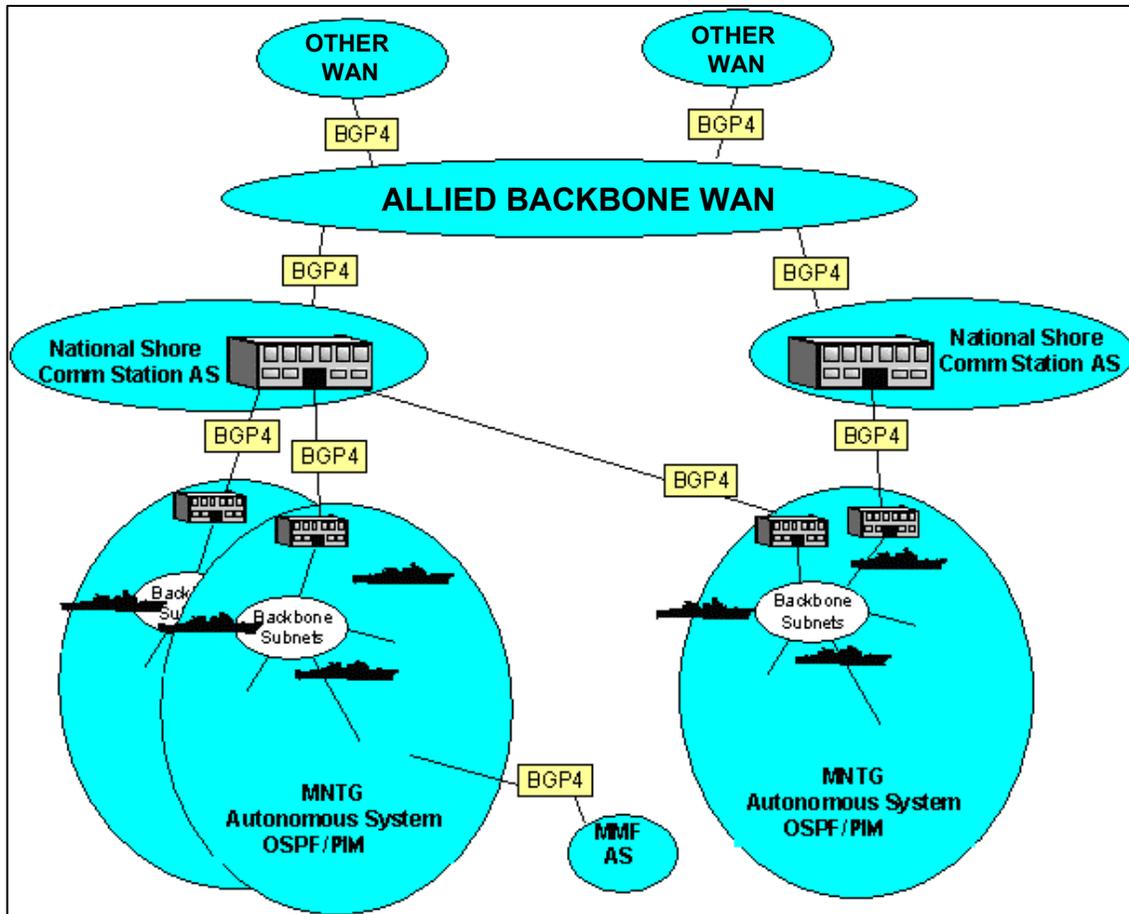


Figure 2-4: - MTWAN Topology

- c. **Evolution** . A MTWAN architecture can be expected to evolve as technology matures. This is particularly pertinent to security and the impact of various national security policies upon the development of the architecture. Currently, security policy within AUSCANNZUKUS nations requires a physical separation (i.e. air gap) between national and allied network enclaves in mobile platforms. As BPDs and multilevel security systems become available to nations, policy regarding interconnections between national and allied networks should allow for more efficient use of communication resources to support both allied and national connectivity. Until then, nations will have to support separate networks for each security domain.

208 MTWAN DEPLOYMENT

Regardless of the restrictions noted above, the networking concepts discussed in this publication assumes nations are developing and deploying systems compatible with these capabilities. Until all nations are fully outfitted with the nodes and subnets required to support this concept of integrated networking, there are likely to be situations where nations will participate under limited conditions. For instance, a unit joining a Multi-national Task Group may only have the capability to support a single HF point-to-point subnet with email capability. In fact, it is likely in the near term that a MTWAN would be made up of a combination of stand-alone point-to-point circuits and subnets tied together by nodes using common routing protocols. The integration of networking nodes tied together by multiple subnets into Autonomous Systems (AS) is the target architecture described in this publication.

Chapter 3

INFORMATION MANAGEMENT (IM)

301 INTRODUCTION

Advances in military communications and information systems (IS) provide information and data faster and more efficiently than at any time in the past. However, these new capabilities are challenging the ability of military commanders to assimilate an ever-increasing flow of information, without becoming overloaded. *More* information delivered faster and more efficiently is only worth the extensive intellectual and funding effort if the information presented enables *faster* and *better* decisions.

302 AIM

The aim of this Chapter is to promote the efficient collection, collation, storage, processing and display of information to enable faster and more informed decision making in order to successfully complete the mission.

303 OVERVIEW

- a. **Definition.** IM is a set of integrated management processes and services, that enable or allow the capability for collectors, producers and users to store, locate, retrieve and transfer the right information, in the right form and of adequate quality, by the most timely, effective and efficient means in a manner consistent with the Commander's mission.
- b. **The IM Environment.** Data is only as important as the context within which it is used and the expertise of the individuals using it. It is the application of standards, procedures, policies and training (processing), that turns data into information which, when placed within a context and compared with historical information (cognition), leads to knowledge. This, in turn leads to improved situational awareness, allowing an assessment to be made resulting in understanding and an informed decision. This hierarchy is summarized in Figure 3-1.

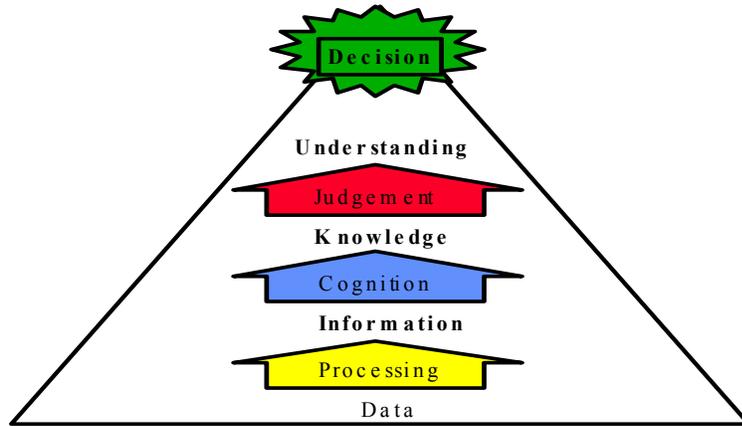


Figure 3-1: - IM Hierarchy

- c. **Command and Control (C2) Decision Cycle.** The C2 decision cycle is often described as a series of sequential steps similar to Figure 3-2. The cycle begins with the collection of information on the current military situation followed by evaluation of this information. A number of Courses of Action (CoA) will then be developed from this situational awareness. One or more of

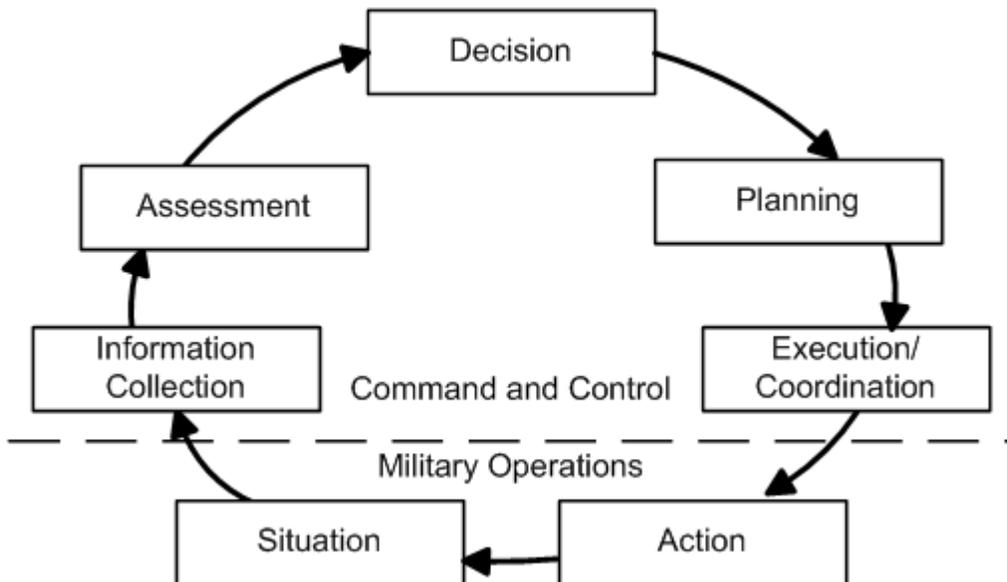


Figure 3-2: - C2 Decision Cycle

these CoAs will be expanded to become a plan (or series of plans) that may then be executed. On completion, the situation is summarized, reassessed and modified before the cycle begins again. The challenge for information managers is to co-ordinate and synchronize these cycles so that the decision cycle time is minimal.

- d. **Information Requirements.** Users require different degrees of completeness, relevance and exactness of information. Unfortunately, there is often a trade off between completeness and relevance. Highly specific inquiries require a high degree of relevance. General inquiries require a high level of completeness. Therefore in order to maximize effectiveness for any given situation or mission, there may be no single solution. Solutions must effectively exploit:
- (1) **Filtering.** The use of appropriately skilled staff or technology to remove unwanted information according to predetermined criteria set by the end-user.
 - (2) **Brokering.** The provision of an intermediary between the end-user and the wider community of potential sources of information so that information is collated and customized according to the user's needs.
 - (3) **Searching and artificial intelligence.** The use of search engines and smart agents to facilitate the location, acquisition and retrieval or automatic forwarding of relevant information from multiple sources.
- e. **Information Flow.** IM procedures must provide instructions for the rapid flow of information between subordinate and superior commands (vertical) as well as between peers across the command structure (horizontal). Effective flow of information requires it to be:
- (1) **Positioned Properly.** The needs for specific types of information are often predictable. Positioning the required information at the anticipated points where it will be needed speeds the flow and reduces overall demands on communication systems and bearers.
 - (2) **Mobile.** The reliable and secure flow of information must be commensurate with the mobility and the tempo of the operation(s). Information flow must immediately adjust to support the vertical and horizontal information flows of the planning system.
 - (3) **Accessible.** All levels of command must be able to access / receive the

information needed to support concurrent or parallel planning and mission execution. If possible, information should be channelled to the end-user via automated means, thus reducing the need for manual information exchange.

- (4) **Fused.** Users receive information from many sources, in many mediums, and in different formats. Fusion is the logical blending of information from multiple sources into an accurate, concise, and complete summary. One of the goals of IM is to reduce information and information flow to a minimum, commensurate with the successful completion of the mission.

f. **Push / Pull**

- (1) **Push.** Information, necessary for decision-making is *directed* (or forced) from the originator to the recipient(s). It should be noted that this action could usually be achieved even during radio silence or EMCON restrictions.

- (2) **Pull.** Information necessary for decision-making is *obtained* (or requested) by the user. It should be noted that this action requires two-way communications and is not achievable during radio silence or EMCON restrictions.

g. **Information Composition.** The composition of information (whether it is obtained through push or pull) will be influenced by:

- (1) The level of the user's and sender's situational awareness,
- (2) The communications system and/or bearer(s) to be employed (i.e. reliance on an asynchronous system such as one that may be required during EMCON restrictions will dictate push),
- (3) The time available to acquire and process the information, and
- (4) The criticality of the information.

304 IM IMPEDIMENTS

a. There are four main IM impediments or issues facing a Commander:

- (1) **Information Overload.** Information overload is where the amount of information received exceeds the ability of users to process it.

Information overload can occur through the introduction of ambiguous, duplicate, irrelevant or outdated information. It can also occur when information preparation such as tailoring and fusion has failed to meet the operational requirement. This can devalue the IM processes and decreases situational awareness.

- (2) **Information Accessibility.** Information should be accessible regardless of its location, timeliness, and ownership.
- (3) **Information Management Infrastructure (IMI) training.** IM training is required to standardize procedures and human-machine interfaces to reduce inconsistencies.
- (4) **Infrastructure Availability.** The IMI must remain dynamic with sufficient capacity to meet peak demands during the execution of a mission.

305 IM PRINCIPLES

- a. The application of key IM principles to all operational and business processes is necessary in order to achieve improvements to the management of information. Best practice must be mandated through management that has a thorough understanding of these processes and a firm commitment to the following principles.
 - (1) **Relevance.** Information products and information delivery processes must satisfy the warfighter requirements. Information should be provided in form and content relevant to the needs of the user.
 - (2) **Effectiveness.** The information should be of sufficient value that it influences the plan or mission.
 - (3) **Efficiency.** The information should only be captured once and updated as necessary.
 - (4) **Accessibility.** Information should be available to all people that have a legitimate need to know, subject to justifiable operational and confidentiality considerations.
 - (5) **Accountability.** Ownership, responsibility and accountability, or level of trust if not owned, for information and information management should be clearly defined.

- (6) **Assurance.** Information should be managed to ensure its integrity is maintained, because the value of information is diminished if compromised. This is clearly linked to stewardship, accountability and confidentiality.
- (7) **Flexibility.** Information should provide the ability to enable and facilitate operational and administrative changes in support of the mission.
- (8) **Presentation.** Information must be presented to decision makers in a way that can be easily and quickly understood so that the right decision is based on an accurate grasp of the data presented. This requires clear, uncluttered presentation in the most appropriate medium to enable decision makers to convert information into knowledge.
- (9) **Timeliness.** It is rarely worthwhile if the information is out of date or reaches the decision maker after the decision has been made. Most information has a time after which its value is negligible. Information is a very perishable commodity.
- (10) **Consistency.** Information should have the same meaning wherever it is used in terms of value, eg distance could be in miles, nautical miles, kilometres etc. To remain consistent it must be used with a common understanding by all decision makers.

306 INFORMATION DISSEMINATION MANAGEMENT (IDM)

- a. IDM is a subset of IM that addresses information awareness, information access and delivery. In essence it directs the end-to-end information flows in accordance with the Command's dissemination policy. It involves the compilation, cataloguing, caching, distribution and retrieval of data (Figure 3-3).

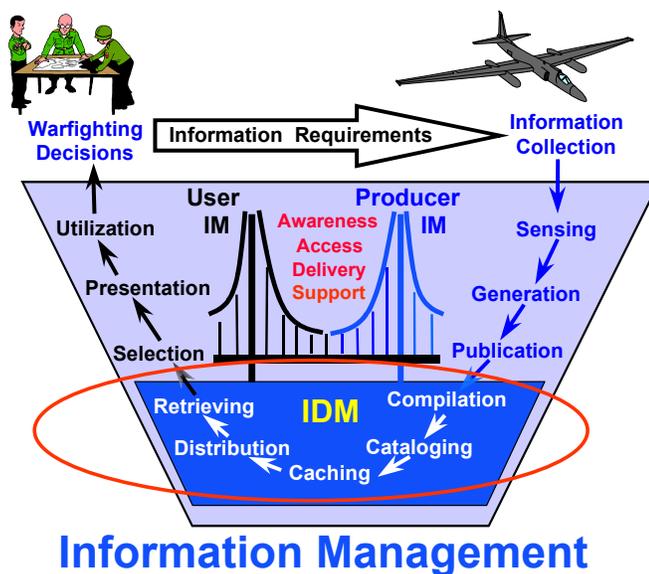


Figure 3-3: - IDM

- b. Effective information dissemination management is essential in providing the right information to the right place at the right time over the right communications path.
- c. **Commander's Intent.** Commanders have an important role in the development of their Information Dissemination Plan (IDP). Commanders will typically adjust information delivery priorities based on operational conditions and communications availability. The current priorities and any subsequent changes should be promulgated in the IDP. The IDP may include the promulgation of authoritative data sources, required reports and submissions, unique characteristics of the information architecture, push / pull guidelines and procedures to be followed.
- d. **Battle Rhythm.** Information requirements are often predictable. Consequently, it is often possible to position information at its anticipated points of need, thus speeding information flow and reducing demands on communications systems. This requires an appreciation of the Battle Rhythm / Daily Operations Cycle and should be reflected in the IDP.

INFORMATION MANAGEMENT SOP

3A01 INTRODUCTION

- a. Information is power, and information superiority is essential for successful mission completion. The ability to provide the right information in a timely and efficient way is not always straightforward or obvious and requires planners to have a good knowledge of the IM infrastructure, as well as a thorough understanding of operations. An efficient information management system requires all users to work in cooperation, have a good understanding of the procedures and an appreciation of the information requirements of the mission as a whole.

3A02 AIM

- a. The aim of this Annex is to establish IM standards and procedures to ensure that the right amount of the right information is available at the right time in the right place and in the right format.

3A03 GUIDELINES

- a. Information should only to be captured once and updated as necessary. All data should be routinely checked to ensure accuracy, integrity, relevance and timeliness. Redundant, duplicate or irrelevant information should be eliminated. Out-of-date data should be archived.
- b. Information is to be provided at a level consistent with the task for which it is intended. Tailoring is to be carried out.
- c. Data definition is to be consistent within a single information domain.
- d. Where information is considered to form part of an official record, additional steps are to be taken to ensure all changes can be tracked (for example, a document could be backed up before changes so that copies of all old versions are available).
- e. Information system managers are to ensure that disaster recovery plans exist, are effective, and are periodically tested.
- f. Information is to be gathered and maintained in compliance with relevant legal, security and data protection obligations.
- g. Ownership of information will not change throughout its life cycle; ownership, or the authority under which information is published, is to be clear and unambiguous at all times.

- h. Where information is incomplete, this should be highlighted.

3A04 SECURITY

- a. Users who have an appropriate security clearance and a valid need to know will be provided access to information.
- b. Information is to be given the appropriate level of protection against unauthorized access and/or manipulation.
- c. Information is to be labeled according to the classification and releasability level assigned by the originator. Labeling is to be consistent with the data labeling policy agreed between nations and implemented across a MTWAN.

3A05 INFORMATION DISSEMINATION PLAN (IDP)

- a. To help ensure information is available when and where required an IDM plan that is reflective of the daily operations cycle is prudent. This cycle is synonymous with “battle rhythm” and is represented in Figure 3-A-1. All units and supporting agencies should be cognizant of the daily operations cycle.

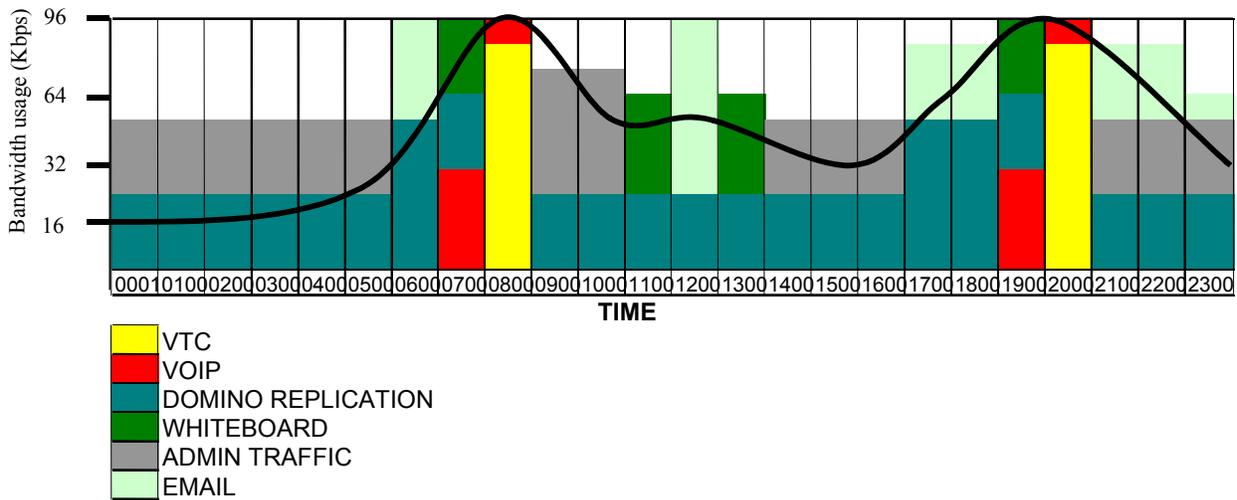


Figure 3-A-1: - Example of a Daily Operations Cycle

- b. An understanding of peak bandwidth and information usage requirements will assist in the assignment of communications bearers and management of information flow. In the sample daily operations cycle provided in Figure 3-A-1, ships may have to assign higher data rate bearers during the peak times. Low priority traffic (admin and personal or QoS requirements) should also be timed for quieter periods.

UNCLASSIFIED

Annex A to Chapter 3 of ACP 200

- c. An Information Dissemination Plan (IDP), such as Table 3-A-1, can help to regulate the flow of information and assist operators in storing and locating information. Additionally, authoritative information sources, information awareness, information access and delivery and support requirements become more readily apparent to the user community.
- d. The matrix may reflect the following information:
 - (1) **Report Type.** Report title or type of information provided.
 - (2) **Submitted By.** The unit or agency normally responsible for submitting the report.
 - (3) **As of Time.** Close out time for recurring reports, not applicable (N/A) for nonrecurring reports.
 - (4) **Posted NLT.** Time to post the report for review.
 - (5) **Where Posted.** The discussion group or web page location to post the report.
 - (6) **Notify.** Who should be notified after posting a report. Normally not required for recurring reports.
 - (7) **Notification.** The preferred method of notifying users following posting.
 - (8) **Precedence.** The precedence to use when notifying the report is available (not applicable to some notification methods).
 - (9) **Push / Pull Guidelines.** Implicit in the development of the IDP is the consideration of what information should be pushed and pulled. Generally, the following push / pull guidelines should be considered:
 - (a) Timeliness of the chosen medium
 - (b) Type of information to be passed. Urgent information should not be published under Pull guidelines unless notification is sent to all recipients via a secondary method.
 - (c) Awareness of information:
 - i. Is the information expected?
 - ii. Can notification of the information be sent by direct means?

UNCLASSIFIED

Annex A to Chapter 3 of ACP 200

(d) Do security implications preclude wider access?

Report Title	Submitted by	Submit As Of	Arrive NLT	Transmission Type	Precedence	Addressee	Info To
OPTASK Unit	All units	1200	1500	E-mail	Priority	CTG	As required
Casualty Spot Report	All units	As required	As required	E-mail	Priority	CTG	As required
Intel RFI							
Comm Spot	All units	As required	As required	E-mail	Priority	NRS XXX CTG	As required
ROE	Intel	As required	As required	Web site (Intel folder)	Priority	CTG CTU	CTF
ATO	Air Wing CMDR	1200	1500	Web site (Strike Ops/ ATO/ Air Plan folder)	Immediate	All	
OPORDERS	Originator	As required	As required	Web site (operations folder)	Routine	As required	As required
OPGEN	CTG	As required	As required	Web Site (OPTASK folder)	Routine	CTU	As required
OPTASK	Warfare Commander	As required	As required	Web Site (OPTASK folder)	Routine	CTG CTU	As required
Wx Observation	MET Guard	1200 2359	1300 0100	Email (Action) Web Site (METOC folder) for info addressee	Priority (action) Routine (info)	MHQAUST	CTG CTU

Table 3-A-1: - Information Dissemination Plan (IDP)

OPTASK KNOWLEDGE MANAGEMENT (KM)

A. OVERVIEW

A1. Purpose

The purpose of this OPTASK is to list dynamic KM issues pertinent to IP networking in the maritime environment. This OPTASK supplements SOPs, relative publications and other OPTASK messages (OPTASK COMMS and OPTASK NETWORK).

A2. Objectives

- A2.1 Timely and accurate delivery of the right information to the right persons
- A2.2 Standardise KM requirements for joint, combined and geographically dispersed forces
- A2.3 Optimised bandwidth management
- A2.4 Optimised network management

B. ADMINISTRATION

B1. Scope

Stipulate operation and effective period.

B2. File Size

Stipulate the maximum permissible file size. This should not exceed 2 Mbytes.

B3. Attachment Policy

All attachments are to be scanned for viruses prior to transmission. Stipulate policy for transfer of attachments to national domains.

B4. Archival policy

Stipulate the length of time that records are to be retained. This would normally be until the end of the exercise / operation. Archival policy IAW national rules.

B5. Special caveats

List any unique labelling and/or caveats. Messages not bearing the necessary classification and caveats will not be transmitted through the Secure Mail Guard (SMG).

B6. Minimise procedures

The purpose of minimise is to limit or curtail the transmission of routine administrative data in order that information essential to the current operation / emergency / exercise can be transferred.

Minimise affects all users of the network and will be imposed by a high level authority.

This message should indicate the level of minimise required being cognisant of the nature of the emergency versus the network requirements. An example is: minimise in force for OPERATION XXXX. Attachments to be limited to 50 Kb.

B6.1. Keyword

Minimise may be enforced through the use of automated word search. Only messages with the nominated keyword would be passed through SMG or server. A keyword may be an exercise or operation title or “minimise considered”.

C. KM REQUIREMENTS

C1. Information Exchange Requirements (IERS)

Stipulate commander IERS relative to current operations / exercise. (The IERS below are indicative of the types of IERS that a commander may wish to identify. This is not a definitive list.)

Intelligence	ROE
METOC	Medical
Logistic	Operations
Admin	Engineering
	NBC

C2. Prioritisation Levels of IP Services / Application

This paragraph is for a commander to set the prioritisation level of both services and applications that share common bearers (MTWAN and national services).

Bearer/communication priorities should be promulgated via the OPTASK COMMS. The commander’s IERS will largely determine the prioritisation order.

UNCLASSIFIED

Annex B to Chapter 3 of ACP 200

A. Classified Email	I. DCP: Chat
B. Classified Email with attachments	J. DCP: Whiteboarding
C. Classified Email with attachments/PKI	K. DCP: Screen Sharing
D. Unclassified Email	L. DCP: Application Sharing
E. Personal Email	M. DCP: Voice
F. Web Services	N. VoIP
G. COP	O. DCP: VTC
H. INTERNET Browsing	OP. VTC
	PR. POTS

C3. Replication Policy

Web replication is necessary between MTWAN units and the NOC to ensure all units have up to date information while limiting the use of RF. Further replication is necessary between a MTWAN and external domains. Indicate the web services replication cycle to be implemented, normally 30 mins. It should be noted that when transferring information across external domains the replication requirement can be accumulative thereby increasing total time to 60, 90 or 120 minutes.

C4. Information Dissemination Plan (IDP)

The IDP delineates the requirements for units to report standard TG information to include daily intention messages, OPTASKS, OPSTATS UNITS, and OPREP 5. The IDP should be presented as a matrix located on a MTWAN Web page and listing title, reporting and receiving units, reporting time and format (i.e. web page or email).

C5. Web pages

Design of web pages are to be IAW Web Services SOPs or as directed in this OPTASK KM.

C6 Messaging

Detail the authority for which each messaging type can be used. The following table serves as a guide:

Message Type	Approved Authority
A. EMAIL	Administrative and Non Mission Essential Traffic
B. EMAIL with PKI	Executive Orders, Mission Essential Traffic, Acknowledgement
C. Web Page Messaging	Administrative and commonly promulgated Orders
D. Web Replication	Administrative and commonly promulgated Orders
E. Web Replication with PKI	Regularly promulgated Operational Orders

UNCLASSIFIED

Annex B to Chapter 3 of ACP 200

Message Type	Approved Authority
F. ACP 127/128	ROE, Mission Essential Coalition Traffic
G. CHAT	Tactical Messaging as detailed in chat policy
H. VOIP	Tactical orders and instructions, Authenticated Formal Instructions

C7. CHAT

Chat will be employed to support tactical and operational objectives and may be utilised in all warfighting environments. List the standard chat rooms that will be created, including indication of manning requirements. (The Chatrooms below are indicative of the of those that a commander may wish to identify. This is not a definitive list.)

MIO Watch – continuous guard C4I Watch – continuous guard Bridge to Bridge – as required INTEL – continuous guard Air Co-ordination – as required	Operations (EW, AAW, ASW) – when ordered High Command – as required Logistics – as required Data Link Coord – continuous guard
---	---

UNCLASSIFIED

Annex C to Chapter 3 of ACP 200

EXAMPLE OF OPTASK KM

A. OVERVIEW

A1. Purpose

The purpose of this OPTASK is to list dynamic KM issues pertinent to IP networking in the maritime environment. This OPTASK supplements SOPs, relative publications and other OPTASK messages (OPTASK COMMS and OPTASK NETWORK).

A2. Objectives

- A2.1 Timely and accurate delivery of the right information to the right persons
- A2.2 Standardise KM requirements for joint, combined and geographically dispersed forces
- A2.3 Optimised bandwidth management
- A2.4 Optimised network management

B. ADMINISTRATION

B1. Scope

This OPTASK KM is specific to the AUSCANNZUKUS At Sea Trial (AST) 02 and is effective from 01 JAN – 31 DEC 02 for MTWAN participants.

B2. File Size

Not to exceed 1.4 Mb.

B3. Attachment Policy

All attachments are to be scanned for viruses prior to transmission. Files with attachments can be transmitted between the MTWAN and other domains as listed below:

- Coalition Enclave 1 – yes
- Coalition Enclave 2 – no
- Nation A System - yes
- Nation B System – no
- Nation C System – yes

(Note: As this is unclassified document, a generic example is used to demonstrate this point.)

B4. Archival policy

Records are to be retained until 31 Jul 02. Archival policy IAW national rules.

B5. Special caveats

The following caveats are to be implemented:

REL: AU/CA/NZ/UK/US

UNCLASSIFIED

Annex C to Chapter 3 of ACP 200

Messages not bearing the necessary classification and caveats will not be transmitted through the Secure Mail Guard (SMG).

B6. **Minimise procedures**

If imposed for AST 2002 attachments shall be limited to 50 kb unless minimise considered is authorised. "MINIMISE CONSIDERED" will be placed in the subject heading.

C. **KM REQUIREMENTS**

C1. **Information Exchange Requirements (IERs)**

INTEL, METOC, HICOM, SUW, ASW, AAW, EW are primary IER.

C2. **Prioritisation Levels of IP Services/Application**

Prioritisation is as follows: I, G, A, B, F, P, J, D, K, L, M.

C3. **Replication Policy**

Web replication cycle is 30 mins. It should be noted that when transferring information across external domains the replication requirement can be accumulative thereby increasing total time to 60, 90 or 120 minutes.

C4. **Information Dissemination Plan (IDP)**

The IDP is presented as a matrix on the RIMPAC 02 Web page and lists the requirements for units to report standard TG information. This includes title, reporting and receiving units, reporting time and format (i.e. web page or email).

C5. **Web pages**

Design of web pages are to be IAW Web Services SOPs or as directed in this OPTASK KM.

C6 **Messaging**

B. EMAIL with PKI - Executive Orders, Mission Essential Traffic, Acknowledgement

E. Web Replication with PKI - Commanders Intent, Tasking, Operational and Administrative Orders

F. ACP 127/128 ROE, Mission Essential Coalition Traffic

G. CHAT - Tactical Messaging as detailed in chat policy

H. VOIP - Tactical orders and instructions,

C7. **CHAT**

Standing Chat rooms will be initiated by commander as follows:

MIO Watch – continuous guard

C4I Watch – continuous guard

Bridge to Bridge – as required

INTEL – continuous guard

Air Co-ordination – as required

Operations (EW, AAW, ASW) – when ordered

High Command – as required

UNCLASSIFIED

Annex C to Chapter 3 of ACP 200

Logistics – as required
Data Link Coord – continuous guard

UNCLASSIFIED

ACP 200

Chapter 4

SPARE CHAPTER

4-1

UNCLASSIFIED

Original

Chapter 5

SECURITY

501 INTRODUCTION

The challenge in a MTWAN is to promote information sharing between allies / coalitions while protecting the information and the information systems that may be logically or electronically connected.

502 AIM

The aim of this chapter is to provide an overview of the security architecture and procedures necessary for a MTWAN.

503 DEFINITIONS

The following definitions apply:

- a. **Allied** — two or more of the five CCEB nations operating together.
- b. **Coalition** — one of more of the five CCEB nations operating together with other nations (including NATO).
- c. **Joint** — two or more of the armed services from one nation operating together.
- d. **Combined** — joint forces from two or more Allied nations operating together.
- e. **Point of Presence (POP)** — is an access point from one geographical location to another. A POP may actually reside in rented space owned by the telecommunications carrier to which the Bearer is connected. A POP usually includes routers, digital/analog call aggregators, servers, and frequently frame relay s or ATM switches (whatever you need to access the cloud).
- f. **Boundary Protection Device (BPD)** — a mechanism, which protects the information system and information located on one side of the POP from the other side of the POP.

504 NETWORK TOPOLOGY

- a. The network topology comprises at a minimum national networks and the MTWAN; the MTWAN being the Local Area Network's (LAN) located in national platforms and connected by RF bearers. More realistically the topology would include connection to an Allied and/or possibly Coalition WAN (CWAN) as represented in Figure 5-1.
- b. Fundamental to the topology is the appropriate separation and security between the national, allied, maritime and coalition domains. Without proper security measures the network will not be accredited for use by respective nations and the Multinational Security Accreditation Board (MSAB).

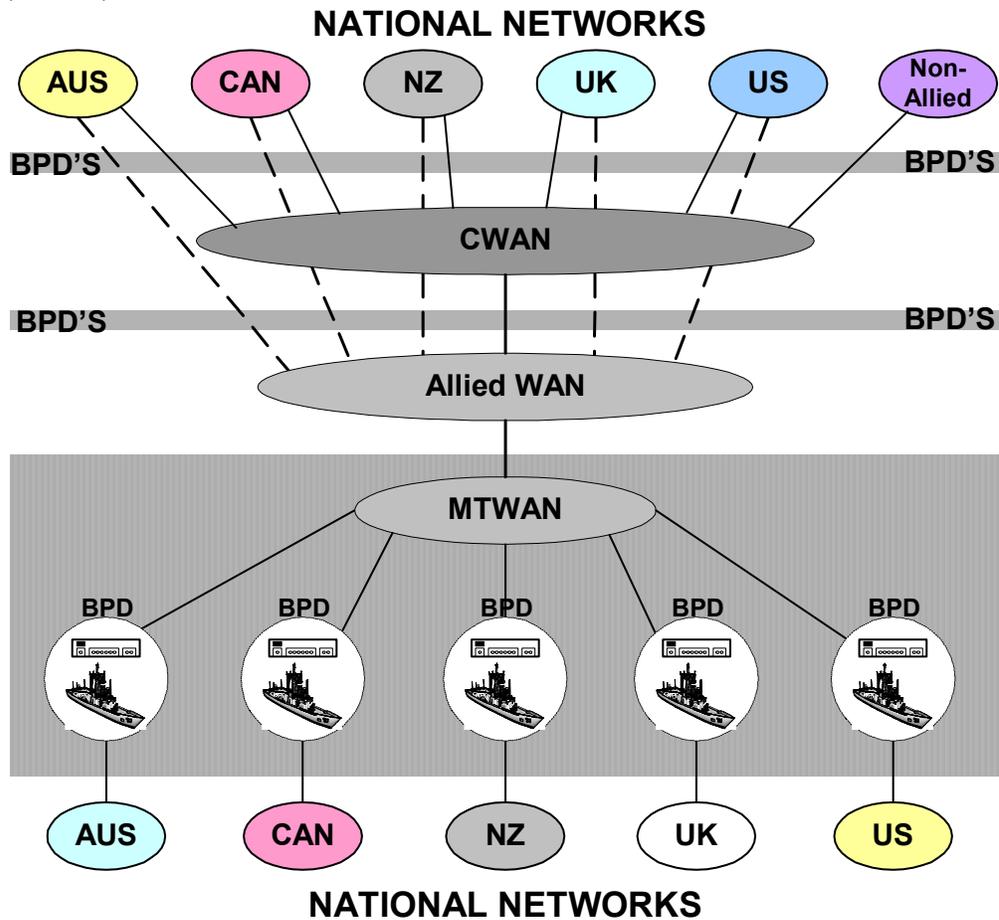
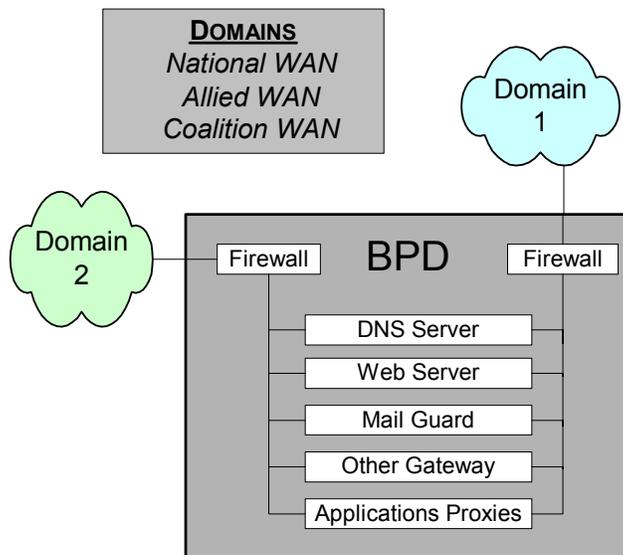


Figure 5-1: – MTWAN Topology

- c. Point of Presence (POP) within this typology exists at the interface of the MTWAN and Allied WAN to the national networks and also the CWAN. The MTWAN domain is treated as a peer-to-peer network. i.e. There are no protection devices to control access between the MTWAN LAN's located on the national platforms. In Figure 5-1, the Allied WAN is also assumed to be part of its peer-to-peer network (this may not always be the case).
- d. Boundary Protection Devices (BPD) designed to protect national information system and its information from the CWAN, Allied WAN and MTWAN are located before the crypto and POP.

505 POINTS OF PRESENCE / BOUNDARY PROTECTION DEVICES

- a. The POP represents the first presence within a sovereign nation that is the ownership and responsibility of that nation (i.e. network passport, terminal adapter, etc or in other words, it is the first point (box) of a communications bearer). Current management methodologies identify the POP as the line of responsibility for specific security, IT and accreditation tasks.
- b. BPDs are employed behind both the POP and crypto, specifically to provide protection services for the sovereign domain of each participating country. Figure 5-2 illustrates a demilitarized zone (DMZ) where the BPD acts to prevent logical connections across domains, but allows the transfer of approved information via a range of services (ie DNS, Web, Mail etc).



5-3

Original

Figure 5-2: – Boundary protection devices between domains

- c. The BPD's may either be an electronic device, software suite or a person which provide the following functionality:
 - (1) **Guard** - to control the release of information between National, Allied and Coalition networks; and
 - (2) **Firewall** - to protect the National, Allied and Coalition networks against unwanted intrusion.
- d. Typically, the BPD will provide some or all of the following functions:
 - (1) packet-level filtering;
 - (2) address translation;
 - (3) port number filtering; and
 - (4) application proxying.

506 RISKS

Leakage of unauthorized information and penetration by unauthorized users are inherent risks in networks and may result in compromises to the confidentiality, integrity or availability of either the system or the information it contains. These risks are summarized below:

- a. **Confidentiality.** Assurance that information is not disclosed to unauthorized persons, processes, or devices.
- b. **Integrity.** Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.
- c. **Availability.** Timely, reliable access to data and information services for authorized users.
- d. **Accidental Leakage.** When information is released inadvertently by either the system itself or an operator contrary to the security regulations pertaining to that information. A risk exists if the outbound data is

transferred unscreened or without label checks, either in real time or off line.

- e. **Deliberate Leakage.** When information is released by an operator contrary to the security regulations pertaining to that information. A risk exists if the outbound data is transferred unscreened, either in real time or off line.
- f. **Stimulated Leakage (Masquerade).** When an attacker pretends to be someone else to stimulate the release of information contrary to the security regulations pertaining to that information.
- g. **Stimulated Leakage (Trojan Horse).** When malicious software stimulates the release of information contrary to the security regulations pertaining to that information.
- h. **Corruption of Information (Malicious Code).** When a harmful payload (virus, worm or Trojan Horse) is introduced into a system, either deliberately or inadvertently via the protocol being passed, which corrupts data contained within that system. A risk exists, however this risk can be reduced by the use of screening software and Intrusion Detection Systems.
- i. **Denial of Service from Malicious Code.** When a harmful payload (virus, worm or Trojan Horse) is introduced into a system, either deliberately or inadvertently via the protocol being passed, which prevents the operation of applications or services within that system. A risk exists, however this risk can be reduced by the use of screening software and Intrusion Detection Systems.
- j. **Denial of Service from Flooding.** When applications or services within a system are prevented from operating after its memory devices have been swamped by the introduction of large volumes of data via the inbound leg. A risk exists, however this risk can be reduced by the use of screening software and Intrusion Detection Systems.
- k. **Spoofing (Masquerade).** Where an attacker masquerades as someone else to distort the view of the reader about the incoming information.

507 RESPONSIBILITIES

- a. Nations have a requirement to protect sensitive and national “eyes-only” information on national networks. The responsibility for the protection of this information resides with the individual nations. Nations will be responsible for ensuring that approved cryptographic devices and IA

products (e.g. guards) are employed where required and that national COMSEC standards, including key management, are met at all times.

- b. Any BPD placed between these national networks and a MTWAN will be nationally owned and controlled. However, the protection of information on a MTWAN itself is the responsibility of the Allied participants as a whole. Autonomous System(s) (AS) that leave a MTWAN remain responsible for the continued protection of data that had been externally provided to a MTWAN. This is of particular concern if the AS is to connect to a third party network.

508 EXPORT SANCTION

It is envisaged that BPDs should be able to carry out Export Sanction to guard against accidental and stimulated leakage from the National domain. In addition, BPDs should provide audit and traceability capabilities to limit the attractiveness of deliberate leakage across the boundary. This function is mandatory in the BPD between a MTWAN/Allied WAN and the CWAN or any other Coalition network. Between a National domain and Allied or Coalition domains, this functionality is entirely the responsibility of the nation concerned.

509 ASSUMPTIONS

The following assumptions are made:

- Nations have agreed security principles and tenets.
- Nations have accepted information protection requirements and are working toward a yet to be determined commonality.
- A MTWAN will operate at the SECRET system high level with information releasable to all MTWAN participants.
- All personnel with access to a MTWAN will be cleared to the appropriate level.
- National networks will have been accredited through a mutually agreed process prior to any connection to a MTWAN.
- No connections to National networks will be permitted without passing through a BPD.
- All communications subnets will be protected by High Grade military crypto devices.
- Network nodes are to have appropriate physical, personnel and procedural security measures in place.
- Proposed architectural solutions will not mandate the use of specific applications or products on nations.
- COTS hardware and software will be used where ever possible.

510 RECOMMENDED SECURITY ARCHITECTURES

- a. **Network Connectivity.** A MTWAN will be an AS connected to the Allied WAN through a Network Operations Center (NOC) as shown in Figure 5-3. There are three potential shipboard architectures that have the potential to meet the security requirements. Current technology does not permit the implementation of the integrated solutions; it is intended to migrate to these solutions as technology and policy allows.

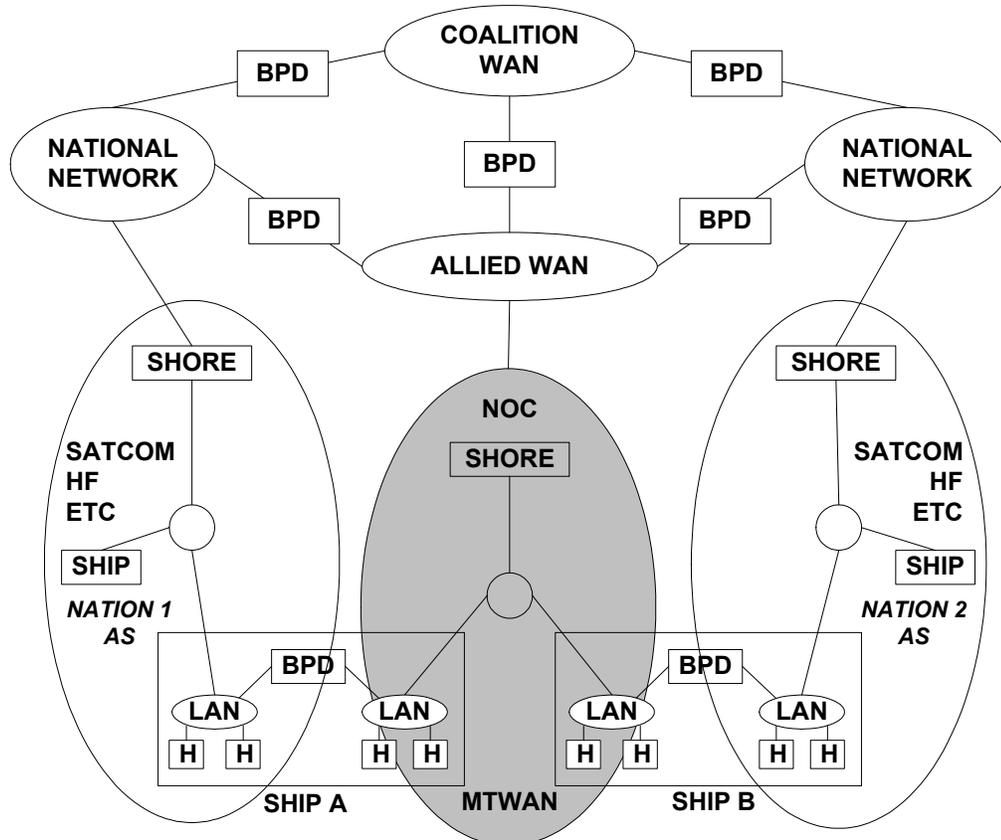


Figure 5-3: - MTWAN Connectivity

- b. **Shipboard “Air Gap” Architecture.** An air gap between the National network and a MTWAN, as shown in Figure 5-4, provides information security for mobile platforms. This air gap architecture relies on physical access control — manual intervention is required to sanitise and transfer information between the two networks via magnetic media such as floppy disks, or keyboards. This is a short-term solution until a faster, efficient and secure process is developed and accredited.

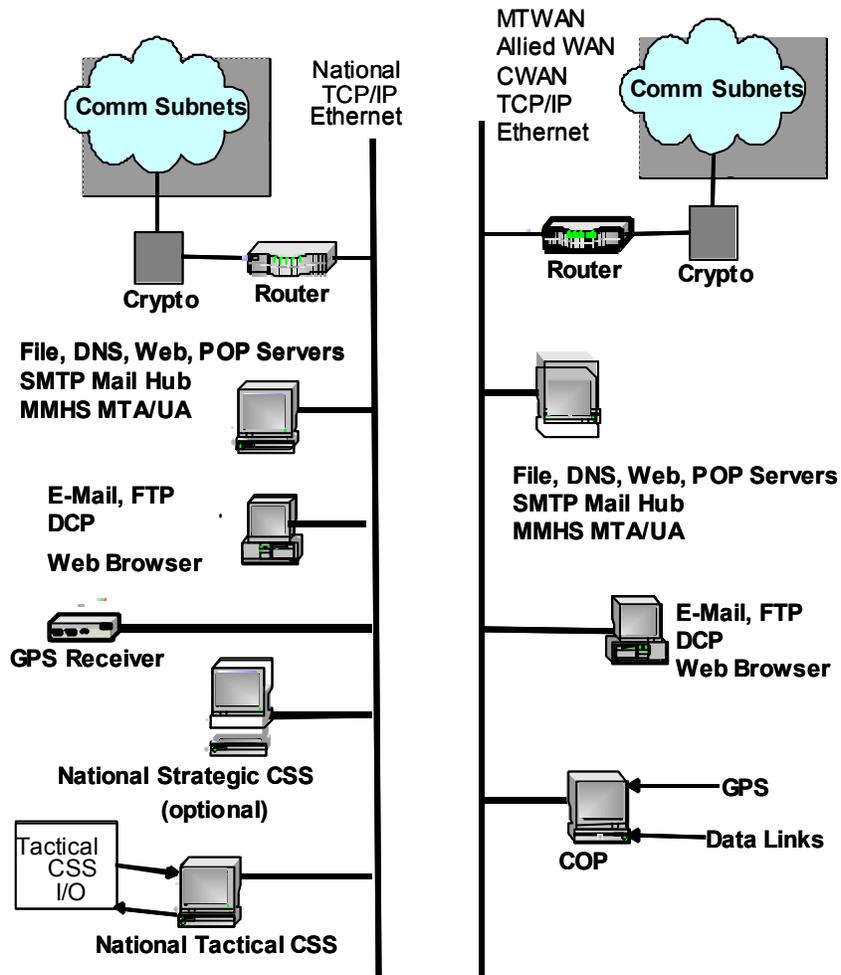


Figure 5-4: - Air Gap Architecture

- c. **Shipboard “Networked” Architecture.** The ability to exchange information electronically will be required to support the increasing amount of information against the requirement for timely delivery. The architecture shown in Figure 5-5 supports electronic transfers between two

networks. Information security will be achieved through a combination of physical, technical and procedural methods. Shipboard “Fully Integrated” Target Architecture. A result of the air-gap and networked solutions is the duplication of resources (e.g. multiple LANs and workstations). This imposes considerable penalties in terms of cost, space and weight. The preferred solution, therefore, is to provide access to both a MTWAN and National networks from a single on-board network.

- d. By increasing the capability of the security gateway, the duplicate services supported on a MTWAN can be reduced and ultimately eliminated. This will depend on the availability of suitable application proxies and guards. For example, existing COTS/GOTS technology would allow screening routers and bastion hosts to provide guards for e-mail; however, DCP will need to be supported by a workstation directly connected to a MTWAN.

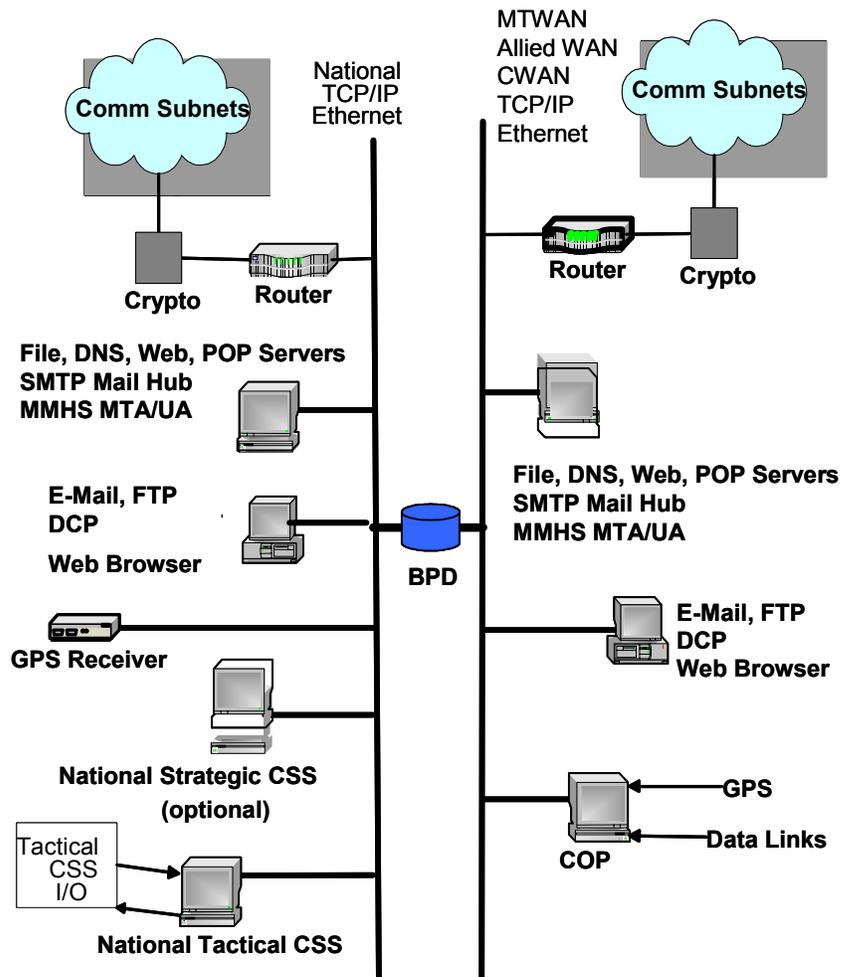


Figure 5-5: - Networked Architecture

- e. A screened subnet architecture employing both network and application layer firewalls, as shown in Figure 5-6, offers a very high level of protection for the LAN from users on a remote network.

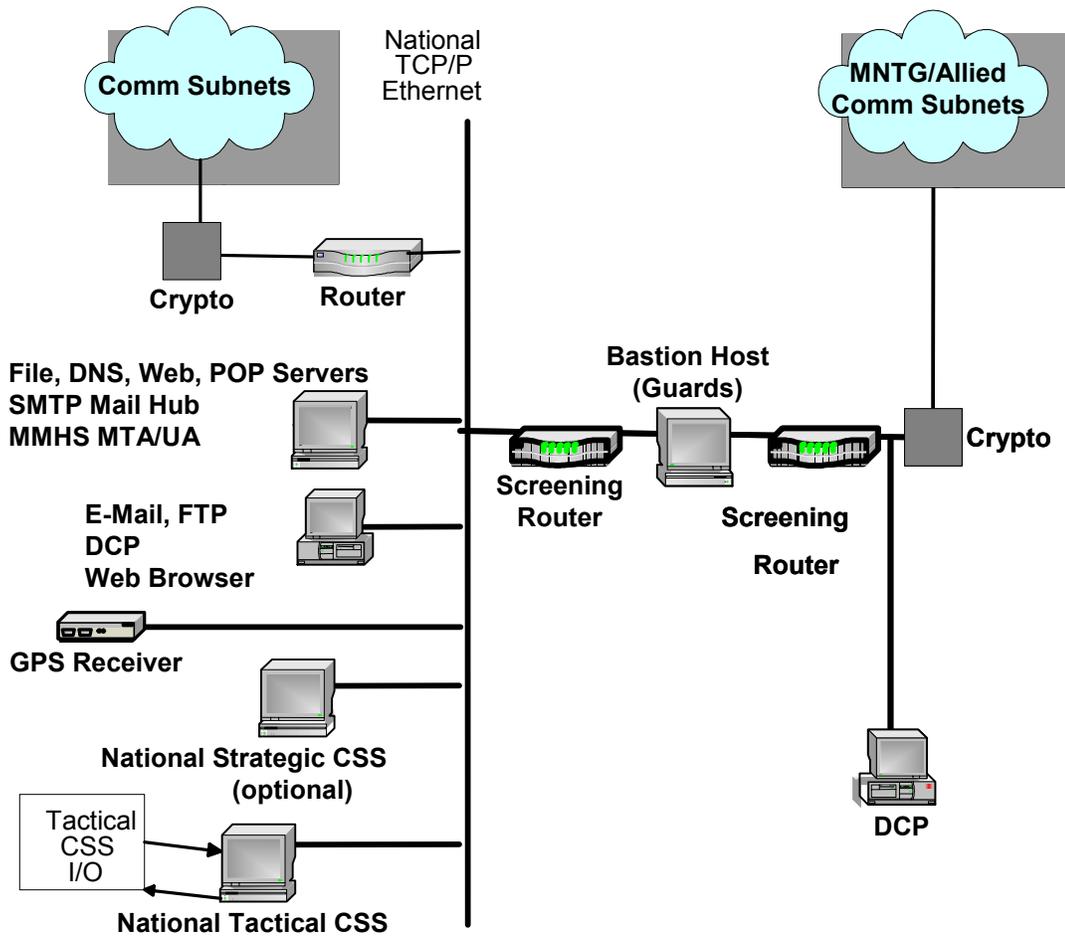


Figure 5-6: - "Fully Integrated" Target Architecture

- f. The bastion host controls and audits all information flowing between the National networks and a MTWAN. It can provide proxy services to users

for certain applications (e.g. FTP). The application layer proxy is used to implement virtual connections to application services on the local network. The host may be used to enforce strong authentication on connections from the allied to the national network.

- g. The bastion host also contains application level guard functionality which will control the release of certain information by checking markings and content and, where necessary, by modification to meet sanitization requirements. It should be noted that particular implementations may require the guard functions to be located in machines physically separate from, but connected to, the bastion host.
- h. Servers directly accessible to the Allied network will be housed in the screened subnet created between two-network layer screening routers.
- i. The outer router will only permit remote users or services to access servers and application gateway on the screened subnet. Also, the outer router will only pass traffic originating from the screened subnet.
- j. For incoming traffic, the inside router will be configured to accept only traffic originating from the screened subnet. For outgoing traffic, the inside router will permit access only to the screened subnet.
- k. Virtual Private Network (VPN), operating with approved cryptographic devices, provide network security for interoperable communications between nodes and dynamically controllable membership within private security domains (or layers).

511 ACCREDITATION

A lead nation will sponsor accreditation of a MTWAN through the Multinational Security Accreditation Board (MSAB).

512 SECURITY DEVICE INTEROPERABILITY

ACP 176 NATO SUPP 1 provides configuration settings necessary to ensure interoperability when different cryptographic devices (e.g. KIV-7/KG84/BID1650) are employed together.

Chapter 6**MESSAGING****601 INTRODUCTION**

- a. The primary purpose of military communications is to exercise command and control over assigned forces. The secondary purpose is to facilitate and expedite the transfer of information between individuals and groups of individuals. Exchange of information can be via traditional military messaging and more recently email, web replication and chat.
- b. Historically inter and intra Task Force/Task Group information transfer was achieved by a variety of low data rate broadcast and point-to-point circuits using formatted messages (ACP 127 etc). Increased information transfer resulted in traffic backlogs, delays, and non-delivery during periods of high intensity operations. During the 1991 Gulf War a single day's message traffic surpassed the total Allied messages exchanged during the whole of the Second World War.
- c. The ability to send emails and replicate web databases within a Task Group enhances traditional methods of information transfer. Email and web replication in conjunction with Local/Wide Area Networks (LAN/WAN) have been shown to:
 - (1) Improve the timeliness of information delivery
 - (2) Reduce message traffic congestion
 - (3) Improve the information richness of the message (by use of multimedia attachments)
- d. Text Chat is increasingly being employed to support command and control.

602 AIM

The aim of this chapter is to provide guidance for the employment of messaging within a maritime IP network.

603 OVERVIEW

- a. ACP 127/128 provides many Elements of Service (EoS), which support Command and Control over assigned forces. These EoS, or key features,

includes; precedence handling, Plain Language Address Designator (PLAD), and distribution by subject.

- b. The principal limitation of ACP 127/128 messaging is that it does not support a wide variety of characters, symbols, case formats, font styles, sizes and color or the inclusion of attachments. As such, traditional messaging does not support multimedia formats.
- c. Email provides rich text formats (i.e. a variety of fonts, styles, characters and symbols), in addition to allowing the drafter to send a message to a reader without any intermediaries. This latter aspect is referred to as 'writer to reader' messaging. A significant benefit of email over traditional messaging is the speed at which information can be exchanged.
- d. Chat provides the capability to exchange short instantaneous text messages with an individual or individuals over an IP network.
- e. Web replication offers an efficient alternative to formal message traffic by enabling information previously encapsulated in formal messages to be posted to a database for access by "addressees" on a "pull" basis in a multi-media format. This places the emphasis upon the "action addressee" to retrieve the information posted vice the traditional "push" mechanism of formal messaging circuits.
- f. EoS such as message integrity, message confidentiality, non-repudiation and authentication provide greater assurance in the exercise of command and control — the primary purpose of military communications.

604 TYPES OF MESSAGING

- a. Messaging can be either text based or multimedia. ACP 127/128, Gold and Chat messaging are text-based formats while email supports multimedia capability. ACP 123 (when implemented) will support message integrity, message confidentiality, non-repudiation and authentication.
- b. To reduce network congestion and promote efficiency, reliable and robust messaging protocols and services should be used.

605 MULTICAST MESSAGING

- a. Currently no agreed IP military messaging exists and hence this document describe the employment of SMTP and add on services as an interim solution for an IP based messaging service.
- b. Multicast messaging allows the same message to be sent to several addressees simultaneously rather than the generation of a separate copy for each addressee.
- c. Standard SMTP email uses Transmission Control Protocol (TCP). In instances when a single message is being delivered to several recipients that are served by different Message Transfer Agents (MTAs), standard SMTP email must establish a connection and transfer the message to each of the destination MTAs in turn. This is very inefficient, as the same message must be transmitted several times, once for each destination MTA, consuming considerable network bandwidth. To resolve this inefficiency, P_MUL was developed to take enable multicasting. The MTA can be configured to deliver SMTP mail using the P_MUL protocol. P_MUL also supports the use of email during periods of emission control (EMCON), by allowing SMTP email to be sent with a delayed acknowledgement. Other transport mechanisms such as MSeG, which multicasts GOLD messages, and MCHAT (Multicast Chat) provide similar efficiencies.
- d. The importance of bandwidth efficiency cannot be understated. An SMTP mail transmission typically involves 19 exchanges of data in addition to those required to transmit the message. These exchanges add up to 11000 bytes. The SMTP mail message typically contains approximately 400 bytes of message headers generated by mail user and mail transport agents. A single email of 1000 bytes therefore requires about 2500 bytes to be transmitted in 20 exchanges. Any measure that reduces the number of emails is therefore advantageous.

606 PUBLIC KEY INFRASTRUCTURE (PKI)

- a. PKI is being introduced to email services to provide an element of military assuredness. By using public key encryption and a digital signature, authentication and non-repudiation can be guaranteed.
- b. Use of a digital signature and/or encryption of email messages is not always needed or recommended. When used, these features will typically increase the

email overheads by 3 to 9 Kbytes. The requirement for public key encryption is not normally required on any secure military network.

607 WEB PAGE MESSAGING

- a. The ability to post a message such as the Air Tasking Order (ATO) or general operational messages (OPGEN) to a TG Web Page reduces the amount of Broadcast Messaging (Multi-cast Email, and ACP 127/128 messages) to be sent across a network. Through the use of replication logs, Web Replication provides increased information traceability, authenticity, and integrity over non-replicated systems. Chapter 8 — Web Information Services provides further guidance on the use of Web Services for information exchange.
- b. Within a tactical WAN, messages posted to web pages have replaced traditional broadcast messages as the most efficient mechanism for disseminating signals, such as Daily Tasking, Operational Reports (OPREP's), ATO's, Operational Tasking messages (OPTASK's) and OPGEN's that are promulgated on a regular basis. The fact that this information must be pulled from a web site by users must be taken into consideration by the promulgator. Information posted in this manner requiring response or action would normally require action addressees to acknowledge receipt of the information by another mechanism such as email or chat.

608 COMMAND AND CONTROL

The OPTASK Knowledge Management (KM) should promulgate the authorized methods for executing command and control. The table below provides guidance but is not yet accepted doctrine.

Information Transfer Application	Authentication	Non-repudiation	Message Confidentiality	Message Integrity	Recommendations
ACP 127/128	Yes	Yes	Yes	Yes	Use for brevity to authenticate all operational tasking. Priority and delivery is guaranteed. Provides redundancy for tactical WAN
Email	No	No	No	No	Delivery not guaranteed. Operational direction sent by email should be supplemented by ACP 127/128 message

Information Transfer Application	Authentication	Non-repudiation	Message Confidentiality	Message Integrity	Recommendations
Email with digital signature	Yes	Yes	No	No	<ol style="list-style-type: none"> 1. May be considered for transfer of operational direction without formal message backup but delivery is not guaranteed. 2. Provides proof of originator's identity and confidence to act on direction. 3. Not needed for admin traffic.
Email with digital signature & public key encryption	Yes	Yes	Yes	Yes	<ol style="list-style-type: none"> 1. May be considered for transfer of operational direction without formal message backup but delivery is not guaranteed. 2. Provides proof of originator's identity, confidence to act on direction, confidentiality and confidence in the accuracy of the message 3. Not needed for admin traffic.
Text Chat	No	No	Yes (secure net)	No	Can be used for tactical direction provided that the Commander can guarantee that all units are on the net.
GOLD (Opnotes)	No	Yes	Yes (secure net)	No	Suitable for the exchange of tactical information but not direction.
Web Page Messaging	No	No	Yes	No	Suitable for administrative information only
Web Replication (Webpage Messaging with replication)	Yes	Yes	Yes	Yes	Suitable for commonly promulgated Orders and Schedules. Acknowledgment by action addressees required.
Web Replication with PKI	Yes	Yes	Yes	Yes	<ol style="list-style-type: none"> 1. Suitable for commonly promulgated Orders and Schedules. 2. Acknowledgment by action addressees required. 3. PKI provides extra assuredness in Authentication and Non-repudiation

609 MESSAGING SELECTION

- Commanders should select the most effective method of transferring information, being cognizant of all the issues outlined in this chapter. Furthermore, Commanders should provide guidance with regard to the messaging method used for operational direction. This guidance should be promulgated in the OPTASK KM.

- b. Until an ACP 123 capability is fully adopted; there will be a requirement to duplicate some information via ACP 127/128. This duplication can be minimized by careful consideration and a clear understanding of the information that must be supplemented by ACP 127/128 messages.

610 SUMMARY

- a. The primary purpose of military messaging remains to support command and control. Alternative methods are now available that significantly enhance the ability and flexibility of Commanders to pass information.
- b. It is important that Commanders promulgate the messaging options that they intend to use for operational and administrative traffic.

MESSAGING SOP

6A01 AIM

The aim of this Annex is to provide procedures for the employment of messaging within a maritime IP network.

6A02 EMAIL

- a. **User Access.** Email access shall be restricted to personnel whom have an operational or tactical requirement.
- b. **Establishing Accounts.** Email accounts shall be established at the unit level in accordance with the agreed TG naming convention.
- c. **Types of Email Accounts.** Individual or Functional accounts, or a combination of both may be used on maritime networks. The policy delineating the use of Individual and/or Functional accounts will be promulgated in OPTASK KM. Examples:
 - (1) Individual Accounts – john.citizen@unit.service.country
 - (2) Functional Accounts - opso@unit.service.country
- d. **High Assurance Guard (HAG) / Secure Mail Guard (SMG).** The configuration of the HAG /SMG may preclude the transmission of email attachments, or attachments of specific file types i.e. .exe, macro files, java etc. The HAG / SMG configuration policy will be promulgated in the attachment policy of the OPTASK KM.
- e. **Email Size.** The size of email shall be in accordance with the OPTASK KM. Attachments should be zipped and presented in the recommended format listed in Table 6A-1. Large files should be posted to an appropriate Domino web page.

Common Application	Recommended Format
Word	Preference is to incorporate text into email Alternative format: RTF
Powerpoint	HTML Alternative format: Powerpoint presentation

Table 6-A-1

- f. **Retention.** Email traffic is to be retained in accordance with the archival policy in the OPTASK KM, or as required by national policies.
- g. **Trusted Labeling.** A trusted label is a sequence of characters inserted in an email that determines the releasability of an email through a HAG/SMG. A trusted label is separate from the security classification and does not reflect the classification, but only denotes releasability. However, although its position within the email will be dependent on the configuration of the HAG/SMG, it will normally be associated with the classification, for example, CONFIDENTIAL REL AUSCANNZUKUS. The designation for trusted labels will be promulgated in the OPTASK KM. Configuration of the HAG/SMG will be IAW the OPTASK NET.
- h. **Acknowledgement.** Message acknowledgment can be obtained through in-built email features, but can only be guaranteed across different domains by instructing addressee(s) to manually acknowledge. The “reply to all” button should not be used to respond to a request for acknowledgement. Email traffic providing operational direction should instruct addressee(s) to acknowledge.

6A03 OPNOTES

Opnotes are principally used to assist the FOTC to manage the COP. Users should be aware that Opnotes compete with other messages over IP networks.

6A04 CHAT

Can be used for tactical direction provided that the Commander can guarantee that all units are on the net.

Chapter 7**COMMON OPERATIONAL PICTURE (COP)****701 INTRODUCTION**

- a. Situational awareness is of vital importance to both warfighters and Commanders in that it enables them to make more-informed decisions. The COP provides a Commander the ability to see, at a glance, the true disposition of all forces and ships within his/her area of interest. Thus the COP is an essential decision-making tool and a force multiplier.
- b. Within a MNTG, tactical situational awareness can be provided from data/information received from organic sensors being captured and displayed on combat data systems. However, this data, while real-time, is limited in coverage to the extent of the TG/TU dispositions and their sensor capabilities. On the other hand, the COP provides near real-time information to the Commander from a theatre-wide perspective. This picture is often enriched from information sources external to a MNTG, and includes land and air tracks.

702 AIM

This chapter describes the COP and its dissemination in a MTWAN environment.

703 OVERVIEW

- a. The COP is an amalgamation or fusion of data and information from a number of combined and/or joint sensors, data-links and other sources into a single (or common) operational picture. The COP provides Near-Real Time (NRT) (current, planned or projected) disposition and amplifying information on friendly, hostile, neutral and unknown forces / units in the sea, land, air and space environments through a Graphical User Interface (GUI).
- b. Other products such as imagery, mapping and weather / oceanography may be overlaid. Ideally future information such as force status, logistic, weather and intelligence is integrated to increase the overall value of the information. This information is either in the form of overlays or can be 'pulled down' by opening windows; (providing a 'drill-down' capability).

- c. At the tactical level, access to the COP augments situational awareness while at the operational and strategic levels it provides an authoritative picture or theatre-wide overview. Traditionally the COP has been disseminated to maritime forces through satellite Information eXchange Sub-Systems (IXS) or via a High Interest Tracks (HITS) broadcast. Both are inefficient and costly to support because they are 'stovepipes' and require dedicated subnets. New COP dissemination techniques employing Internet Protocol (IP) allow the convergence of COP information onto the one maritime tactical network. These IP COP methods provide for the more timely delivery of track information.

704 REQUIREMENT

It is essential a Commander has confidence in the COP, and therefore willing to act on the information displayed. To this end, the information must be:

- a. **Accurate** - it must convey the true situation.
- b. **Relevant** - it must apply to the mission, task, or situation at hand.
- c. **Timely** - it must be received in time to make the right decisions.
- d. **Useable** - it must be in easy to understand format and displays.
- e. **Complete** - it must contain all the information necessary to make an informed decision.
- f. **Concise** - it must contain the level of detail required.
- g. **Secure** - it must be afford adequate protection.
- h. **Common** - data and tracks must be identical across the theatre.

705 TOP COP (FUSION AND FILTERING)

- a. The TOP COP denotes a hierarchical architecture where information is fused (merged, enriched, correlated and if necessary de-conflicted) from subordinate pictures so that the 'TOP COP' has a fully integrated and accurate picture. This is then fed back down to subordinate pictures, which are updated. The COP Synchronisation Tool (CST) seamlessly provides much of this capability, to sites that have sufficient bearer bandwidth. The use of a Force Over-the-horizon Track Coordinator (FOTC) ensures COP fusion at the tactical level where CST is often not available.

- b. At the tactical level, an important requirement is to ensure relevancy. This also adheres to IM principles and requires coordinators to be able to filter unwanted information captured at operational and strategic levels. The principle here is “keep it relevant”. It is unlikely that a tactical Commander needs information from outside of his area of interest.

706 COP MANAGEMENT

- a. The COP is a distributed fused picture. In order to achieve a “synchronised” fused picture with multiple units that may all be reporting similar pictures a method of synchronisation is necessary. Traditionally this has been accomplished procedurally by the designation of a FOTC who maintains responsibility for all tracks within the AOR. The COP Synchronisation Tool (CST) provides a “distributed” rather than “dictated” management of the database. There are three methods of COP Management as follows:
 - (1) **FOTC**. Traditional COP management has been achieved through the establishment of a FOTC, which correlates and associates, where possible, the various source track data and then provides a “dictated and validated” broadcast back to the participants. The validated track database is centrally managed and maintained within the TF/TG.
 - (2) **CST**. CST enables the unit that has the most information on a particular track with the ability to be the one responsible for managing that track within the database. Based on TCP/IP communication protocols, CST provides the user with faster, more reliable communications and an improved synchronized picture.
 - (3) **DUAL FOTC/CST**. In many cases there are requirements to support both CST and FOTC. A CST / FOTC Gateway platform enables units within a TF/TG to receive the benefits of a CST fused picture.

707 COP DISSEMINATION

- a. **CSTMdxNET/CST**. CSTMdxNET is the transport protocol associated with CST. It enables the transmission of COP track data via TCP/IP. The minimum recommended bandwidth to participate in a CST environment is 40 kbps. Platforms not meeting these bandwidth criteria should continue the use of the traditional FOTC-based broadcast.
- b. **UID**. Unit Identifier (UID) is a TCP/IP transport protocol that enables the transmission of Over The Horizon (OTH) Gold Formatted messages. This

requires less oversight than OTCIX/HITS/FOTC Broadcast and yields greater commonality in the database. Within a maritime tactical WAN environment the use of UID is the simplest mechanism for COP distribution but carries a large overhead because the dissemination is unicast.

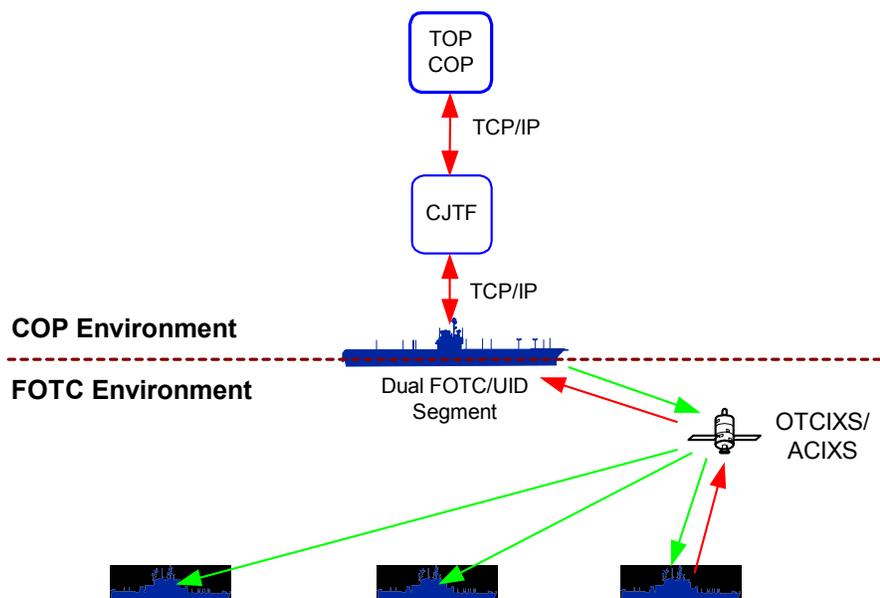
- c. **NETPREC.** NETPREC is subset of UID that enables FOTC to group units for dissemination of tailored COP. NETPREC is designed for LAN application and is seldom used within a WAN environment.

708 MULTICAST TRANSPORT SERVICE

The Multicast Service Gateway (MSeG) is a reliable packet assembler software program that will receive the TCP/IP COP feed (FOTC or CST), and rebroadcast them using a reliable MDP transport service. The MSeG host at each site receives the multicast MDP service and delivers each IP “data-gram” via a local TCP/IP connection to a local host running software compatible with the Global Command and Control System- Maritime (GCCS-M). The use of MSeG dramatically increases network efficiency.

709 ARCHITECTURE

- a. Figures 7-1 and 7-2 provide the generic architecture for the generation and distribution of the COP. They show both a top-down and bottom-up approach in that strategic and theatre information is assimilated and passed downwards at the shore NOC, while a force picture is generated and passed upwards.



7-4

Figure 7-1: Traditional Environment (with IXS networks and CST)

- b. Figure 7-2 represents a full IP environment with CST operating upwards from the MCC and subordinate units participating via MSeG or UID.

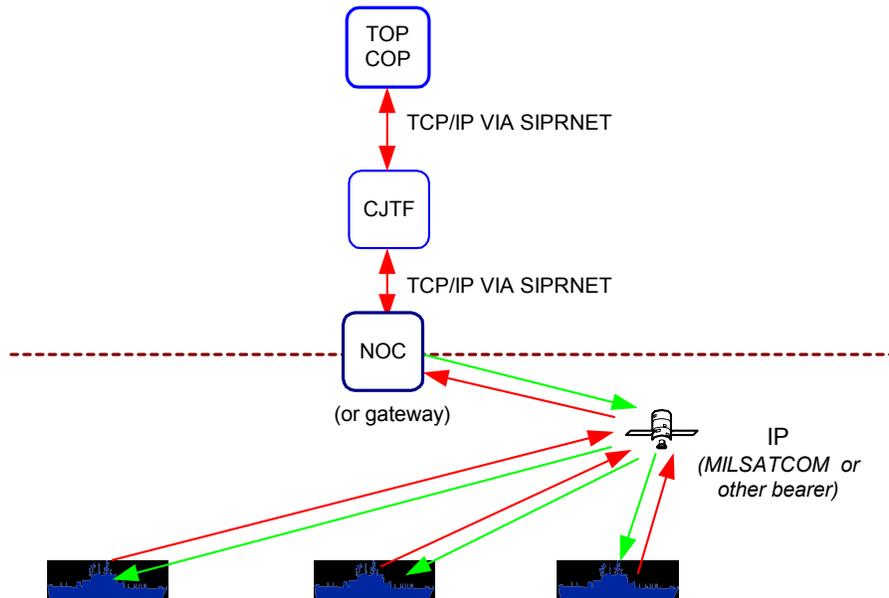


Figure 7-2: Full IP Environment (MTWAN)

- c. The World Wide OPTASK Force Over-the-Horizon Track Coordinator (FOTC) provides detail on construction, compilation, collation and dissemination of the COP. CTF will promulgate variations in COP procedures specific to local operations in an OPTASK FOTC Supplement. Necessary guidance for supporting the COP using MSeG on a MTWAN should be promulgated in the OPTASK NET.

710 SELECTION OF APPROPRIATE COP DISSEMINATION METHOD

The following table provides guidance for the selection of COP dissemination.

Method	Transport Service	Description	Considerations
CST	CSTMdxNET	<ul style="list-style-type: none"> Reporting responsibility assigned to unit with best track information. 	<ul style="list-style-type: none"> Not recommended unless WAN bandwidth 64Kbps or greater

Method	Transport Service	Description	Considerations
		<ul style="list-style-type: none"> • Synchronised track databases • Automatic process • Utilises TCP/IP 	<ul style="list-style-type: none"> • Can be employed with 20 Kbps bandwidth with degradation in service (i.e. functionality)
FOTC	UID	<ul style="list-style-type: none"> • Maintains FOTC procedures • Dictated and validated COP • Simple and efficient • Utilises TCP/IP 	<ul style="list-style-type: none"> • Point to Point
FOTC	MSeG	<ul style="list-style-type: none"> • Packet assembler enabling multicast of COP via TCP/IP • Has a Broadcast mode 	<ul style="list-style-type: none"> • FOTC procedures unclear • Higher track latency • Can be utilised in EMCON
FOTC	IXS	<ul style="list-style-type: none"> • Maintains FOTC procedures • Dictated and validated COP • Has a Broadcast mode • Legacy system 	<ul style="list-style-type: none"> • Dedicated stovepipe system (independent of network traffic) • Higher track latency • Can be utilised in EMCON

Table 7-1. COP Dissemination Methods

711 SUMMARY

- a. The COP is a vital tool for improving the Commander's situation awareness and aiding in decision making. However, the COP is only as good as the information fed into it and, conversely, could seriously damage situational awareness if allowed to become out of date or contain inaccurate, irrelevant or incomplete data. In fact, an inaccurate picture is worse than *no picture at all* because it can cause the wrong decisions to be made, possibly with devastating results. Consequently, a Commander will have confidence in the COP *only* if he/she knows that the system is reliable and accurate. This can only be achieved through users being knowledgeable, aware of the system requirements and diligent in its upkeep.

- b. The ability to display global track information through stovepipe IXS networks will soon be replaced by integration onto IP networks. In the case of Allied nations, this will be via a MTWAN. This will allow the COP to be displayed and viewed through a variety of media that will continue to provide a picture, even during EMCON restrictions (radio silence). Conversely, it also means that units not capable of accessing a MTWAN, may not be able to view the same picture within the same timeframe. Commanders must therefore be aware of the capabilities and limitations of the units within their force.

Chapter 8

WEB INFORMATION SERVICES

801 INTRODUCTION

Operators are faced with ever-increasing amounts of data and information, which they must process, assimilate, correlate and apply to a wide range of ongoing operational activities. Furthermore, they need to share or dispatch information, often with other users that are geographically dispersed and have disparate communication and information systems. Web Services provide an important means to manage and disseminate this information to a large number of users within a low bandwidth environment. Web Services complements Information Management (IM) by:

- Providing an asynchronous collaboration tool
- Giving the Operator control over relevant information
- Providing easy sharing of rich information
- Enhancing the relevancy of information.
- Improving the assimilation of information.
- Increasing the level of situational awareness and understanding.
- Filtering information
- Reduce BW demands via Web Replication

802 AIM

The aim of this Chapter is to provide guidance for the employment of web information services within a networked military maritime environment.

803 OVERVIEW

Web Services is a means of information exchange designed to support planning and coordination activities. Web Services supplements the current suite of communications tools, such as e-mail, military messaging, distributed collaborative planning and voice communications, to enhance overall shared awareness, speed of command, and collaboration capabilities afloat. A Maritime Tactical Wide Area Network (MTWAN) Web Site provides a means for users to post information and files directly to a web site through an on-line user interface without the support of a web specialist. The Operator is able to become a Content Manager, focusing on relevant warfighting information.

804 OBJECTIVE

The primary objective of web services is to present relevant and timely information to the user in the most appropriate format that aids the user's assimilation and understanding. Subsequently, this aids decision-making as well as situational/tactical awareness. The secondary objective of web services is to reduce the necessity for reliance upon formatted

ACP 127/128 messages for distributing regular summary information by organizing, distributing and presenting information in an appropriate and interactive format, using imagery, spreadsheet and/or databases.

805 INFORMATION QUALITY

To ensure information is accurate and qualitative, and avoid duplication, there needs to be authoritative data sources and data consolidation. This means information or data can be posted and controlled only by the owner. No one else should be able to make changes or amendments without approval from the owner. The “owner” here is envisioned to be a specific individual or position, such as a Watch Officer. All information posted to any web site should bear the name and contact details of the posting authority (this can be equated to the releasing authority of a message rather than to the drafter).

806 NETWORK ARCHITECTURE / DESIGN

- a. A MTWAN Web site relies upon a hub-spoke or a multiple hubs-spokes topology as depicted in Figure 8-1. Key to this architecture is the concept, use of web replication and the supporting software environment. The web replication process mirrors the Task Group web site at each ship and shore node. The replication process transfers only the differences between each web site, conserving scarce bandwidth. At the end of a replication cycle, each ship and shore node will contain the updated information store and mirror the hub server. Operators then can browse the task group web site locally, rather than reaching off-ship, again conserving scarce bandwidth.

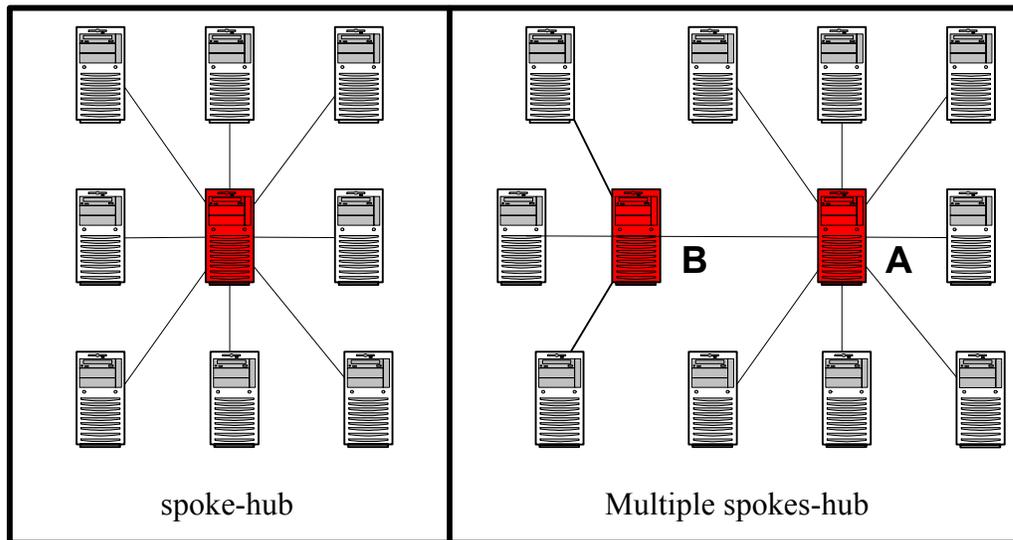


Figure 8-1: - MTWAN Hub Configurations

- b. Network connectivity will largely determine the hub-spoke topology employed. For example, if ship A were acting as a gateway for ship B, it would not be necessary for ship B to replicate with the central server. It could replicate with ship A server. This would save bandwidth but may result in the delay of ship B receiving its information by one replication cycle.
- c. There is therefore a timeliness versus bandwidth usage trade-off. It is possible that ship B could lose administration visibility. Careful preplanning of topologies and replication scheduling will minimize these issues.

807 CONCEPT OF OPERATIONS

- a. An operator should be able to post and access organic and non-organic information that is pertinent to the mission. The combination of web browsers, databases and replication technologies provide the means for operators to store, distribute and browse information generated locally or remotely without imposing large bandwidth and administrative overheads.
- b. Organic and non-organic information is effectively pushed and pulled respectively, and automated via the web replication process. This information could include weather data, Rules of Engagement (ROEs), electronic charts, etc. Nevertheless, the tools and information will be available to all ships even when disconnected from the MTWAN. Subsequently, operators have a central authoritative repository of information or 'electronic binder' that is managed by personnel from the functional warfare areas to ensure the relevancy, currency, and accuracy of the information and to avoid duplication of information. Clearly constructed templates replicated and used across all MTWAN sites enable users to quickly locate any desired information. The universal nature of browser technology enables differing IT systems, capabilities and users to be connected, thereby assuring interoperability.
- c. Information posted to the local server will be replicated transparently to the operator, allowing the other participants to view the information. This information is to be sent only once, with only the 'delta' transmitted for amended documents.
- d. Network Operations Centers (NOC's) will act as information transfer gateways providing releasable material to pass into other security domains, such as national secret networks. At present this is achieved through manual, air-gap procedures. In the future, Multiple Security Level (MSL) devices are envisioned to pass appropriate web information between security enclaves more efficiently, providing the information meets security requirements.

808 SOFTWARE ENVIRONMENT

- a. As is the practice on most networks, web data is added, deleted or changed at frequent intervals. As a result, the content of local web servers rapidly diverges making it very difficult to maintain a common data repository and web site at each location. To minimise the requirement to transfer large amounts of data backwards and forwards whenever servers are being updated, IBM's Domino Server software suites are being used to support MTWAN web services. The Domino web sites are composed of unstructured document databases. Individual documents in the Domino database can be composed of ASCII text fields, Rich Text Format (RTF) fields, graphics, a file attachment of any type, or any combination of the above. Documents and files of any type can be added to a Domino web site. Templates provide tailored views of documents from within a web browser or Notes client. The web replication feature of Domino automates the replication process. During each replication cycle, the servers compare their document databases with those of the hub server and vice versa. The differences in the data fields (or the delta) is noted and then exchanged between the servers. Use of ASCII Text and RTF fields provides the most efficient means of replication, as text fields are compared and only the differences in text are sent. File attachments are treated as one data field, any change to an attached file would require the whole file to be retransmitted, which takes the least advantage of field level replication. At the end of the replication cycle, all MTWAN servers at all sites contain an identical set of documents. Transaction logging within Domino keeps track of the replication status. If communications (or connectivity) are lost for any reason, replication will cease. However, when communication is re-established, replication will automatically recommence at the point it ceased, thus limiting duplication and consequently (often) expensive communication and satellite time.
- b. Domino web replication provides the capability for asynchronous collaboration between sites. Consequently operators at each site become information/knowledge managers with the responsibility of populating and managing each local site with documents, briefs and other pertinent information rather than on the mechanics of developing web pages. With a common MTWAN web site at each location, operators are able to browse the site on their local MTWAN LAN (or work station) without having to browse off-ship in order to reach the remote server, further reducing the bandwidth requirement/utilisation for external communications.
- c. The Domino Server provides an open, secure web application server, a

scalable server infrastructure and local/remote administration services for a MTWAN. Domino servers can operate in a heterogeneous computing environment, including Microsoft Windows NT, 2000, Sun Solaris and Linux. The web application server also provides support for integrated Web security, native HTML, JAVA agents and services and an integrated Domino address book. Finally, Domino provides native support for all the major internet standards and for Web applications, including CORBA support.

- d. The Domino server interface has a task-oriented approach, easing deployment, use and management locally or remotely. Domino R5 also supports messaging features to web browsers and Internet mail clients. Furthermore, directory features are available to browsers and LDAP clients; discussion features are available to browsers and NNTP newsreader clients; and administration features are available to browsers as well as the Notes client. In summary, Domino makes it easy to design dynamic web applications that look and run the same for both the web and Notes clients.

809 DOMINO FEATURES

- a. **Replication.** The replication feature is the key to the distributed nature of Domino and Notes software and is one of the driving factors behind Collaboration at Sea. Replication is best understood when compared with the traditional file-copy process, an all-or-nothing operation. For example, a database on Server A also needs to exist on Server B. With the file copy system, this is a simple task of copying the database from Server A to Server B. However, problems will begin once users start adding documents to either of these copies; they will immediately become 'out of sync'. To regain 'sync' it would be necessary to re-copy the updated database from B to A. However, this would then wipe out any changes that had also been made to server B. So, how is it possible to maintain a single database in multiple locations in a synchronized fashion? The answer lies in replication. Instead of copying the whole database from Server A to Server B, you create a new database on Server B. The next time replication occurs between these servers, the source database and its replica exchange new and modified information. This can include an entire document or just updates in a document. In simplistic terms, replication is Server A saying to Server B, "Give me all of your new and modified information since the last time we spoke, and I'll give you mine."
- b. **Transactional Logging.** A transactional log provides a sequential record of every operation that has occurred during a given period of operation. Logging helps to ensure complete data integrity for updates and will enable MTWAN to perform incremental database backups. With transactional logging, Domino will permit 24/7 online server backup and recovery support.

- c. **Administration.** A central site is capable of administering servers separated geographically.
- d. **Security.** Users accessing the Domino server over any supported Internet Protocol (IP) can now use SSL for certificate-based authentication and encryption. It is also possible to issue X.509 certificates to Notes users or use X.509 certificates instead of Notes certificates. Notes clients can then use these Internet-certificates for secure access to Web servers (SSL) and for secure Internet mail (S/MIME). Domino also supports VeriSign Global Server IDs that uses a 128-bit cipher when communicating with international browsers and servers over HTTP, NNTP, LDAP, IMAP or POP3. Separate key rings for SSLv3 are supported for each Domino virtual server. This means each virtual server can have its own certified identity and can authenticate its users with its own set of certificates. For file-level security, it is possible to implement access control for HTML, image, and other types of files in the file system.

810 POSTING OF INFORMATION

MTWAN web services are a suitable conduit for disseminating, sharing or publishing most information and/or data. However, it is important to understand that the web is a “pull” rather than a “push” system and therefore is not suitable for dissemination of urgent information that is of a time-critical or a tactical nature. Notwithstanding this limitation, urgent and tactical information could be posted to the web providing the posting authority can ascertain that all of the intended recipients are able to access the information in a timely fashion. This can only be done by means of a secondary communications service (voice call, email, message, text chat) to alert all recipients of the existence and whereabouts of the new information, (email should include a hyperlink), together with acknowledgment instructions. In exceptional circumstances, it is possible to manually “force” the replication of critical information outside of the normal, automated replication cycle. It should be noted that, although this procedure is safe and, in exceptional circumstances may be necessary, it also increases the overall data-flow and possibly creates additional stress on low/shared bandwidths.

WEB SERVICES STANDARD OPERATING PROCEDURES

8A01 AIM

The aim of this annex is to provide procedures for the employment of web services within a networked maritime environment.

8A02 WEB ARCHITECTURE

A MTWAN Web Site relies on an asynchronous hub and spoke architecture, which are managed by master servers at the Network Operations Center(s) (NOC). The architecture minimises bandwidth consumption by replicating only changes in data between remote web servers and master servers. Replication to the master servers can be scheduled to occur on any periodic basis, as dictated by the overall operational needs of the Task Group Commander. External (off ship) connectivity is required only for replication of web site databases. This minimizes the requirements for connectivity and increases operational capability and effectiveness. It also provides a means for continuing operations during short periods of EMCON silence.

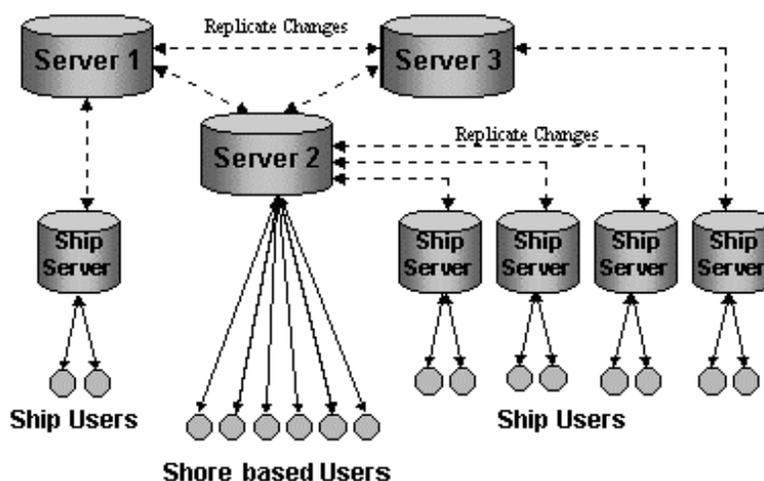


Figure 8-A-1: - MTWAN Architecture

8A03 WEB ADMINISTRATION

- a. **MTWAN Administration.** A MTWAN Administrator is responsible for maintaining the portal to the web. This will include registering and supporting local web administrators, ensuring user registration requests are properly routed, overseeing system architecture, and tracking trouble reports.
- b. **Web Developer.** The Web Developer is responsible for developing the portal and assisting the web administrator as necessary.

- c. **Ship Web Administrator.** The Ship Web Administrator is responsible for approving new users and assigning their access privileges to the local web site. They may be granted editorial privileges such as add, remove, and manage links on the home page and navigation pane.
- d. **Functional Area Information Manager.** The Functional Area Information Manager oversees all content within a given functional area to ensure the timeliness, relevancy and accuracy of information. Functional areas can include, but is not limited to Intel, METOC, AAW, SuW and ASW. Duties include enforcing maximum file size rules, monitoring users' adherence to formatting rules, and assisting users.

8A04 WEB SERVICES COMPONENTS

- a. **Web Site.** A MTWAN web site is intended for non-real-time collaboration and dissemination of operational information, and not for time critical tactical information. It should be used for information that is of interest to external users and is not for local requirements.
- b. **Design.** A standard MTWAN web site could be designed for example with 3 frames:
 - a left navigation frame placed vertically on the left side of the window;
 - an upper navigation bar placed horizontally across the top of the window;
 - a main viewing frame, the larger of the three, in the central part of the frame.

The left navigation frame provides links to information of immediate concern, information about the organisation, and administrative tools for users. The upper navigation frame provides links to information along traditional operational and administrative organizational lines. The main window is the target area for viewing navigation results such as libraries, reports, and documents.

Web designs must be standardized to provide a common look. Templates will be provided for posting functional information. A sample web-page is at Figure 8-A-2.

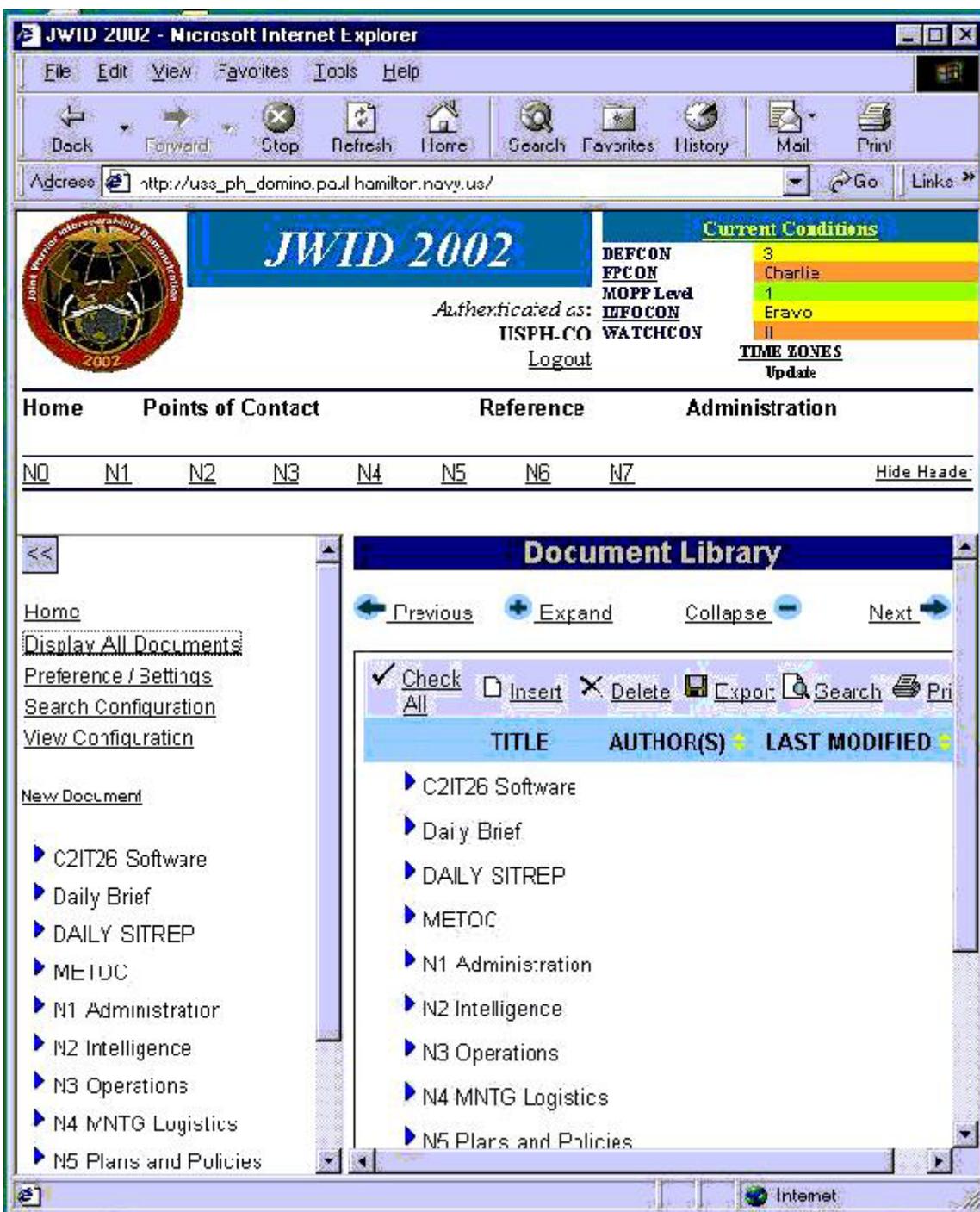


Figure 8-A-2: - Sample Web Page

8A05 POSTING DOCUMENTS

- a. Instructions for posting documents.
 - Select appropriate functional area and click the "New Document" button displayed above the categorized list of documents in the functional area.
 - The user will be prompted to authenticate using the Web Services username and password received in the registration process. Upon successful authentication, the document input form will appear.
 - Enter document title in the subject field.
 - Assign a category to the document from the drop-down list or add a new category. To add a new category, ensure the category drop-down list is defaulted to blank.
 - Select the appropriate classification for the document.
 - Enter or paste text into the content field and/or attach file.
 - Click Save button

- b. Guidelines
 - Use colored text to highlight important or changed items.
 - Move or eliminate unnecessary text to aid comprehension.
 - Use the formatting features provided in the template. (Formatting of text in a source file will not carry through to the final display when pasted into a template document).
 - Attach images or files to better present information. Graphics and other attachments are to be the minimum necessary to convey a message. Compression products such as Imagery Compression Engine (ICE) or PK Zip are to be employed. Attachments are not to exceed 2 Mbps.

8A06 EDITING

- a. Documents are only to be edited or deleted by authorized users. Policy guidance should be promulgated by the Web Administrator to delineate rights and responsibilities. This should be posted in the Admin folder of the web page.

- b. Since the Web Services system only replicates changes in content, care should be exercised in making deliberate add-edit-delete decisions.

8A07 WEB CHANGES

Requests for changes to web design and/or functionality should be requested through the MTWAN Web Administrator.

8A08 MTWAN REPLICATIONS

- a. Replication should be set to occur IAW the OPTASK KM.
- b. Users should be cognizant that a number of replication cycles are often required to transfer documents from one unit to all participants. The accumulated replication time will be dependent on the total network architecture.

Chapter 9**DISTRIBUTED COLLABORATIVE PLANNING****901 INTRODUCTION**

- a. Military forces rely upon shared information — news, thoughts, plans, and ideas. This information is used to plan, deploy and execute operations. The act of sharing this information to develop plans collectively is called collaboration. As such, information sharing and collaboration are essential aspects to warfighting.
- b. Until recently, collaboration between dispersed units was confined to formatted messages, voice circuits, and tactical data sets. This limited both the scope of information that could be conveyed and the format which this information could be presented. Lengthy messages were often required to convey a commander's plan and good comprehension skills were required to assimilate details and understand the commander's intent at the other end. The system was formalized and best implemented by a 'top down' planning approach. In such an environment, collaboration was limited.
- c. Today, real-time technologies, such as instant messaging chat, audio conferencing, shared whiteboards, screen sharing and application sharing provide a new, rich dimension to collaboration. Planning can effectively reach all members who need to be involved despite their geographic location. Information can be presented in a wider range of media formats. 'Bottom up' planning and informal or offline planning provide alternative means of collaboration vice the traditional 'top down' and formal approaches. Real-time technologies have:
 - enhanced the relevancy of information.
 - improved assimilation of information by the warfighter.
 - promoted information sharing and the generation of new ideas.
 - increased the level of situational awareness and understanding.
- d. Furthermore, recent experiences have highlighted the effectiveness of employing these synchronous collaboration tools in combination with the asynchronous collaborative infrastructures such as E-mail and Web Services.

902 AIM

The aim of this chapter is to provide guidance for the employment of Distributed Collaborative Planning (DCP) within a maritime military environment.

903 OVERVIEW

- a. **Importance.** Critical to gaining and sustaining the initiative in warfare is the ability to stay inside the enemy's planning-cycle time. This requires real-time collaborative tools to store, share, and distribute information and knowledge to warfighters that may be geographically dispersed.
- b. **Timeliness.** Real-time capabilities provide many benefits to maritime communication and collaboration. These include:
 - Faster, better decision making, reducing the decision cycle.
 - Additional modalities of expression to communicate meaning, helping to make communication rich and complete.
 - Improved communication with the Task Group members.
 - Foster closer ties among the diverse Task Group members in a Coalition environment
- c. **Effectiveness.** It is the combination of the awareness (who is available?); conversation (text, audio, video); and shared objects ('here, let me show you') features which provide the war fighter with a powerful collaborative tool. Together they make collaboration as convenient and as effective as face-to-face conversations.

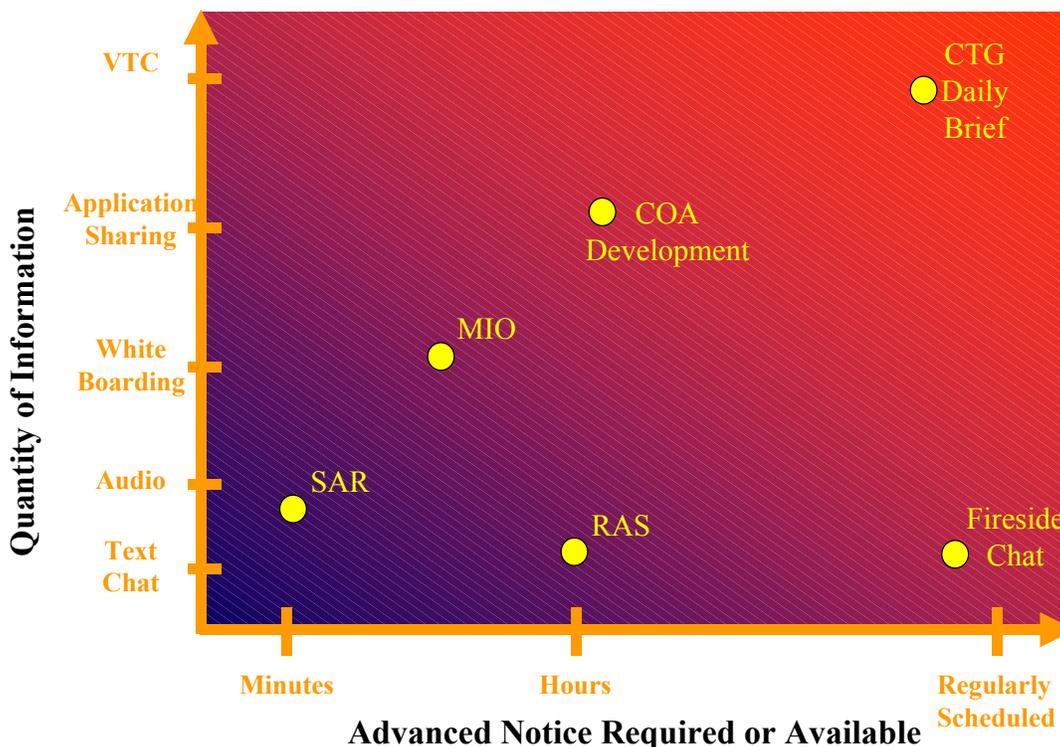


Figure 9-1: - Collaborative Planning Spectrum

- d. **Collaborative Planning Spectrum.** Figure 9-1 and Table 9-1 illustrates the broad spectrum of planning that can be conducted using DCP. Generically, the spectrum can be delineated by time and to the degree the session is planned. This concept therefore enables DCP tools to be tailored for each type of meeting with a subsequent set of protocols being standardized for each session
- e. **Awareness.** Awareness makes real-time network conversations as convenient as deciding to talk to someone simply because one is aware of their presence. Effective real-time collaboration relies on the same ad hoc feeling as a hallway encounter, instead of making users go through cumbersome efforts to set up a simple meeting or a conference call. This facilitates the dissemination of information and improves situational awareness.
- f. **Conversation.** Critical to successful collaboration is the capability to select from a suite of tools to maximize efficiency and minimize any loss of information. Operators should have the ability to select from a suite of real-time conversation tools; instant messages, text chat, audio, and video. For quick clarification, chat may be appropriate. Voice or video may be

more efficient for longer or more detailed conversations. Other interaction may require the precision of the written word so that the accurate and complete meaning is captured and agreed upon.

	DELIBERATE	ADHOC	Notes
UNCONSTRAINED	Daily Briefing	Fireside Chat	Documents provided in advance Replication able to take place Bandwidth Efficient Higher level tools such as VTC can be utilised
CONSTRAINED	Contingent Operations	MEDIVAC SAR CRISIS THREAT WARNING RED	No time to replicate in advance. Extensive use of Whiteboarding Bandwidth intense VTC not supportable due to extensive use of lower bandwidth tools
Notes	Planned Follows a set format Standard Topics	Unplanned No Format	

Table 9-1: - DCP Spectrum

- g. **Shared Objects.** Collaboration between people predominantly involves conversation. Frequently, these conversations refer to some sort of object: a message, a presentation or the deployment of forces. When some or all of the participants have shared access to that object, the conversation — the collaboration — is richer and more complete.
- h. **Global Address Book.** The need for an integrated Global Address Book cannot be overemphasized. This Global Address Book:
 - provides Awareness of who is on-line and available to collaborate synchronously
 - authenticates users in establishing DCP sessions
 - authenticates users in the access and posting of web documents
- i. **Blending Asynchronous and Real-time Collaboration.** The impact of real-time collaboration is maximized when it is combined with traditional or asynchronous collaboration. Together, they make computer-based

collaboration a more natural way to work. This blend is critical, since users naturally move from one mode of interaction and work to another, usually without giving the matter much thought. The value of these technologies is enhanced when they are integrated in a way that mirrors MTWAN business practices. From real-time awareness, an operator can determine that a colleague is available to talk. In a blended real-time and asynchronous environment, the user could open a database and look up the name of the person the operator wants to meet with. If that person is currently online, the user can engage them in an online meeting immediately; if not, the user could send them an e-mail to schedule an online meeting later. Instead of replying to an e-Mail, a user could start a conversation with one or many e-Mail recipients. After editing a document as a shared object, a user could save the revised document in any number of places, such as in discussion databases, bulletin boards, or internal Web sites, for review by others. An informative online meeting, such as the Commanders Intent, could be archived. Colleagues who missed the meeting could replay both the conversation and the shared objects.

- j. Figure 9-2 highlights the possibilities in terms of synchronous and asynchronous collaborative tools with respect to the location of participants.

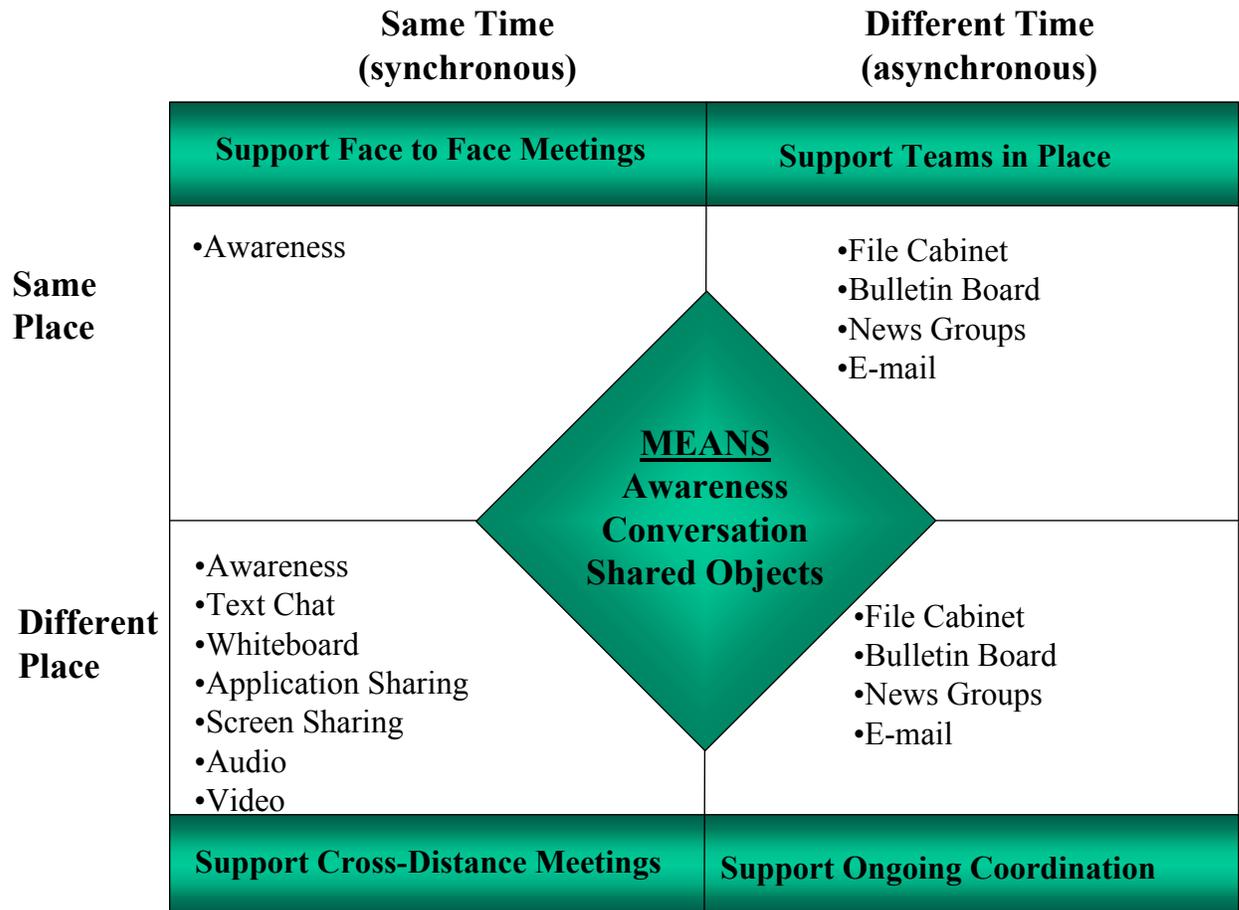


Figure 9-2: - DCP Characteristics

904 CONFIGURATION

Generically, there are three DCP configurations: peer to peer, server – client, server – server. These are represented in Figure 9-3, along with their characteristics. Peer-peer configurations are a low cost solution for engineering temporary interoperability between low number of users when a server is no available. Server-client configurations can support greater number of users and is more robust. In a hub-spokes environment servers could be connected, sharing the Global Address Book, and allow users to Collaborate across multiple Sametime servers. The server-server solution avoids a single point of failure and provides some load-sharing capability.

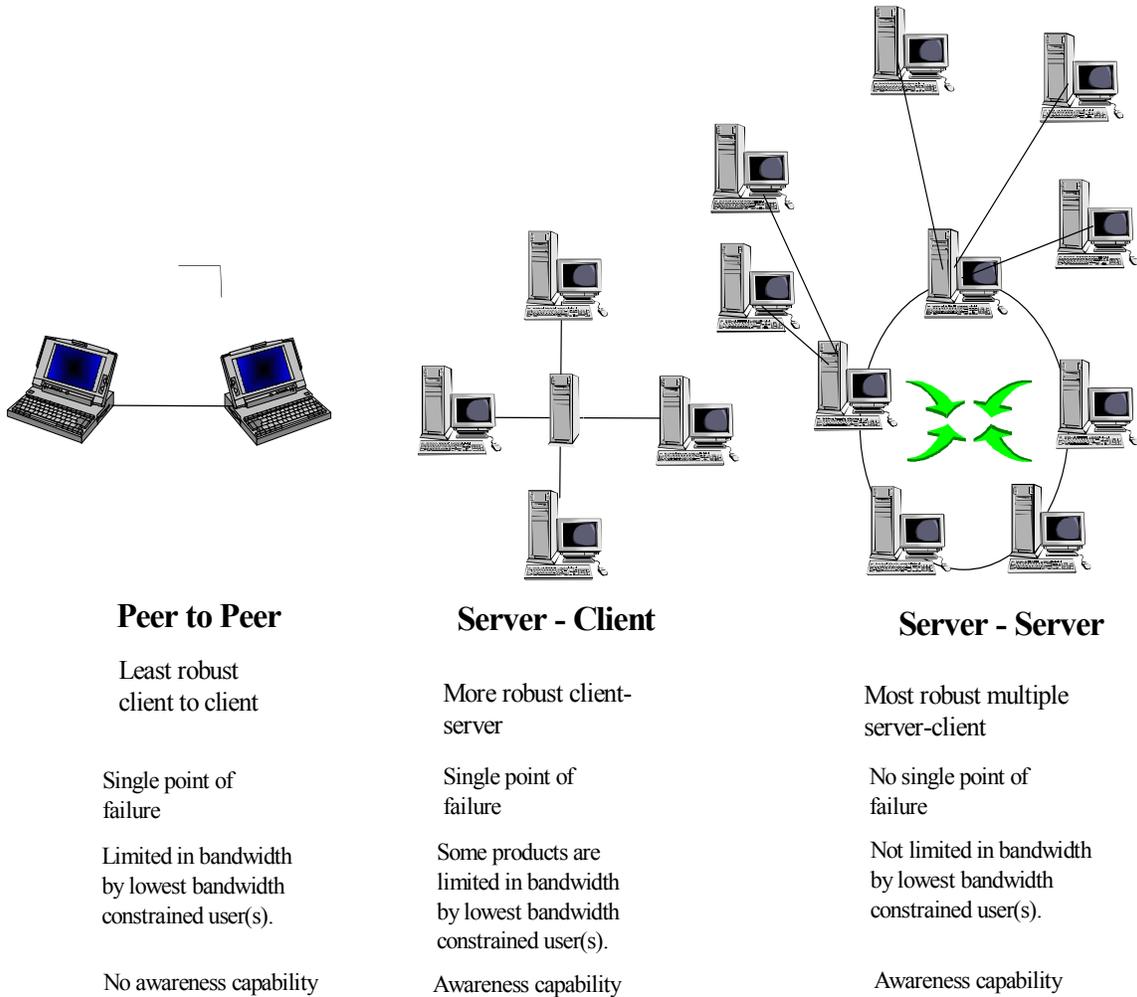


Figure 9-3: - DCP Configurations

905 BANDWIDTH LIMITATIONS

- a. The configurations in Figure 9-3 assume efficient connectivity and high data rates. In the low bandwidth maritime environment these conditions will seldom exist and in almost every circumstance efficiency of the Network, whatever its configuration, will be determined by the data rate achievable by the communications bearer. It is therefore important that information management practices be implemented within all DCP sessions to ensure that information quantity and detail does not overload the network and prevent its subsequent use in a timely and effective manner.

- b. Scalability, whether inherent in the tool or achieved through the selection of tool(s), combined with effective standard operating procedures are required to support DCP in a low bandwidth environment.

906 SECURITY

A MTWAN operates as a coalition secret high level network. Normal security procedures as for any other data or voice are to be followed.

907 TOOLS

Efficient, flexible, instantaneous communication is critical for successful Service, Joint, Combined and Coalition Operations. DCP tools must meet these objectives as well as being intuitive and easy to use. The selected DCP suite should provide the following tools and features to the MTWAN user:

Awareness	Knowledge of who is on-line and available for collaboration
Text Chat	Multicast or private mode chat over IP
File Cabinet	For retention of common documents
Bulletin Board	Interactive bulletin board in each collaborative session
News Groups	Running discussion news group capability
Whiteboard	Persistent on-line whiteboard capability
Application Sharing	Persistent sharing of applications across the network
Screen Sharing	Persistent and dynamic sharing of an Operators screen across the network
Audio	Broadcast or private mode audio over IP
Video	Common desktop VTC
Knowledge Engines	For visibility and retrieval of information
Auditable	Track changes capability

908 REQUIREMENTS

In a coalition environment, DCP requires a tool that:

- is capable of providing reliable and scalable services within the constraints of the tactical communications environment.
- supports both deliberate and adhoc planning.
- supports the tool sets and functions listed in para 907.

- conforms to the developing standards listed in Annex 9A.

909 CONCLUSION

The adoption of DCP tools and processes are critical to improving the effectiveness and speed of the commander's planning and operational decision-making process. This chapter outlines the scope, applicability and requirements of DCP. It is for the commander to make the maximum use of this capability by clear direction in their operational intentions.

DCP STANDARDS

9A01 Introduction

The early adoption and implementation of agreed-upon standards was the key to widespread implementation and industry-wide innovation in networks. The success of real-time collaboration will be no exception. In each of the critical elements of real-time collaboration — awareness, conversation, and shared objects — there are varying degrees of standards development and industry acceptance. The chief benefit of standards, of course, is the promise of interoperability among products, applications, and tools from a variety of vendors. Furthermore, as standards are adopted and mature, they raise the level of functionality and ease-of-use across the entire spectrum of applications that are developed in accordance with those standards. While the integration of awareness, conversation, and shared objects is critical to real-time collaboration, each element has unique characteristics that justify different protocols for each one.

9A02 Standards

- a. **Awareness — IMPP.** Today there is no generally accepted standard for the exchange of awareness or presence information. Awareness is a low-overhead activity — the interactions are usually short in duration and there is little bandwidth required. Currently, several companies have proprietary protocols for exchanging awareness information. Lotus, Microsoft, and others are joined in an IETF effort to produce a single protocol. This working group is called IMPP (Instant Messaging and Presence Protocol).
- b. **Conversation — H.323.** The requirements of conversation protocols differ greatly from awareness. Conversations can be text, audio, or video, and therefore require varying levels of bandwidth. For audio and video communications, the main protocol is H.323. The H.323 specification was ratified by the International Telecommunications Union (ITU). H.323 provides a foundation for audio and video communications across IP-based networks, including the Internet. Additional key benefits include:
 - i. **Interoperability.** H.323 establishes standards for compression and decompression of audio and video data streams, allowing equipment from different vendors to communicate. H.323 also sets methods for clients to communicate capabilities to each other.
 - ii. **Platform and application independence.** H.323 is not tied to any hardware or operating system.

- iii. **Bandwidth management.** Video and audio traffic is bandwidth-intensive. Network managers can limit the number of simultaneous H.323 connections within their network or the amount of bandwidth available to H.323 application.
 - iv. **Security.** H.323 addresses four general aspects of security: Authentication, Integrity, Privacy, and non-Repudiation. These are important so vendor products can provide security measures to ensure privacy for the end user and to secure the corporate or service provider networks.
- c. **Shared Objects — T.120.** High interaction and long duration are characteristics of shared object sessions. The T.120 standard contains a series of communication and application protocols and services that provide support for real-time, multipoint data communications. Established by the International Telecommunications Union (ITU), T.120 is a family of open standards that was defined by leading data communication practitioners and is supported by Lotus, Microsoft, Intel, and many other vendors in the communications industry. The T.120 family of standards has the following benefits:
- i. **Interoperability.** T.120 allows endpoint applications from multiple vendors to be interoperable.
 - ii. **Reliable, multipoint data delivery.** T.120 provides an elegant abstraction for developers to create and manage a multipoint domain with ease. From an application perspective, data is seamlessly delivered to multiple parties in "real-time." Error-corrected data delivery ensures that all endpoints will receive each data transmission.
 - iii. **Network transparency.** Applications are completely shielded from the underlying data transport mechanism being used. Furthermore, T.120 supports vastly different network transports, operating at different speeds, which can easily co-exist in the same multipoint conference.
 - iv. **Application flexibility.** While T.120 includes defined whiteboarding, application sharing, and file transfer protocols, it also provides a generic, real-time communications service that can be used by many different applications.

UNCLASSIFIED

Annex A to Chapter 9 to ACP 200

- v. **Scalability.** T.120 is defined to be easily scalable from simple PC-based architectures to complex multi-processor environments characterized by their high performance.

DCP Standard Operating Procedures

9B01 INTRODUCTION

- a. Distributed Collaborative Planning (DCP) can significantly improve overall warfighting planning processes whether in a Service, Joint, Combined or Coalition operation. By improving plan content and understanding, timeliness of plan development and objective plan assessment processes, commanders can make better and faster decisions while geographically dispersed.
- b. While efficient and effective employment of DCP tools can be a force-multiplier, uncontrolled access and ill-defined procedures can result in degraded network performance, unnecessary (and excessive) bandwidth consumption, confusion, and time late information. Subsequently, DCP needs to be considered from an Information Management (IM) perspective.

9B02 AIM

The aim of this Chapter is to establish the framework for planning, controlling and participating in DCP sessions to ensure maximum effectiveness and efficiency.

9B03 DESCRIPTION

- a. DCP is a set of applications or tools which enable geographically dispersed members to collaborate; collaboration is the act of sharing information to develop plans collectively.
- b. **Toolset.** Generally a DCP suite comprises the following synchronous and asynchronous tools and functions:
 - ◆ Awareness Knowledge of who is on-line and available for collaboration
 - ◆ Text Chat Multicast or private mode chat over IP
 - ◆ File Cabinet For retention of common documents
 - ◆ Bulletin Board Interactive bulletin board in each collaborative session
 - ◆ News Groups Running discussion news group capability

- ◆ Whiteboard Persistent on-line whiteboard capability
- ◆ Application Sharing Persistent sharing of applications across the network
- ◆ Screen Sharing Persistent and dynamic sharing of an Operators screen across the network
- ◆ Audio Broadcast or private mode audio over IP
- ◆ Video Common desktop VTC
- ◆ Knowledge Engines For visibility and retrieval of information
- ◆ Auditable Track changes capability

Kbps	Chat	WB	Audio	Sharing	Video
2.4	YES	POOR	POOR	NO	NO
4.8	YES	SLOW	POOR	SLOW	NO
16	YES	YES	POOR	YES	NO
32	YES	YES	YES	YES	LIMITED
64	YES	YES	YES	YES	YES
128	YES	YES	YES	YES	YES
Broadcast Type	Periodic updates	Periodic updates	Periodic updates	Periodic updates	Continuous

Table 9-B-1 — Bandwidth Toolset Spectrum

- c. **Bandwidth Consumption.** Bandwidth requirements for DCP is dependent on the particular DCP product used, the tool employed, the scalability features chosen (if available) and in cases of posting or sharing information, the file format selected. Diagram 1 depicts DCP tools relative to bandwidth consumption.
- d. Table 9-B-1 also reveals that DCP transmissions are typically of limited duration bursts. The exception is video, which is a continuous transmission. The implication is that numerous DCP sessions can often be supported if they involve burst transmissions. Diagram 2 illustrates the case in point. The use of a continuous transmission, such as VTC, will

drastically increase the likelihood of network congestion, as evidenced in Figure 9-B-1.

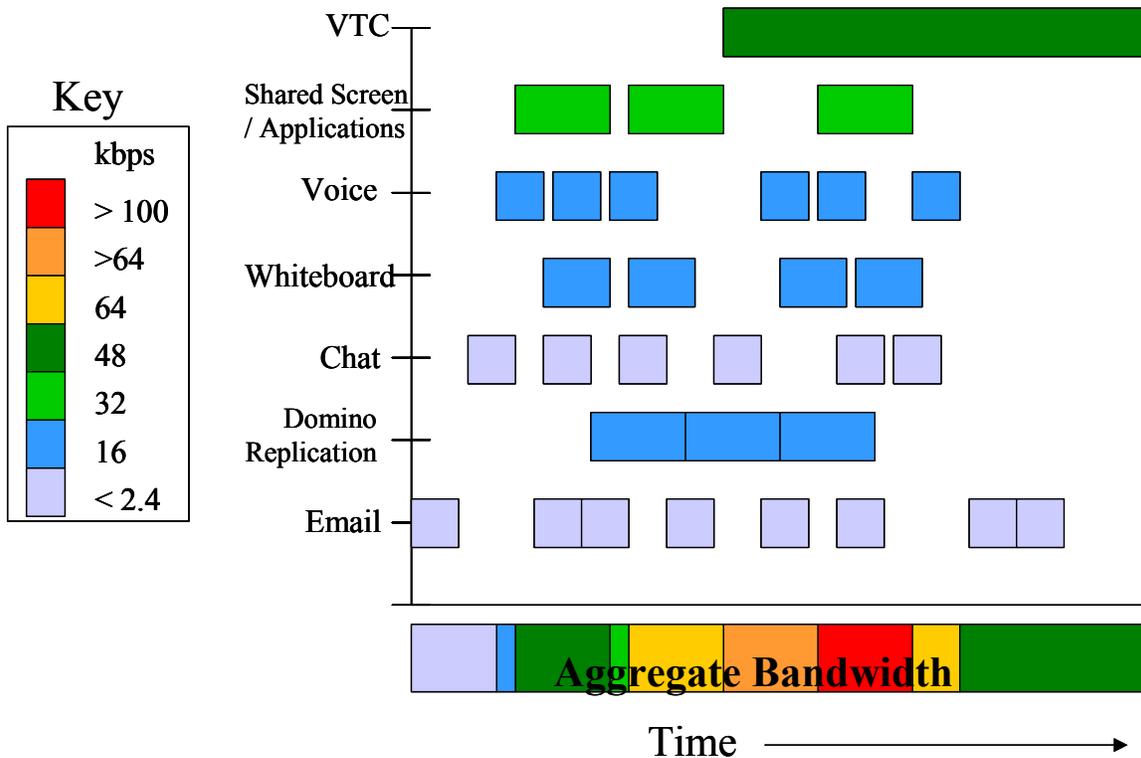


Figure 9-B-1 — Bandwidth Aggregation

- e. **Conference Types.** The major distinctive features between DCP products are in the conferencing venue and whether the product is scalable. DCP products either employ a ‘public meeting room’ system or a private invitational system.
- f. In a meeting room system members conduct collaborative sessions in meeting rooms. This system makes it easy to establish a meeting providing members have the DCP application running. Members join via a lobby or common meeting place to be informed of the location of the meeting room. Well designed buildings (a suite of conference rooms) can make knowing the location of the conference room intuitive. i.e. A meeting involving the Task Group Logistic Officers would occur in the Logistics room. This requires a dedicated DCP administrator to establish planning rooms and buildings in accordance with the Plan of Day (POD). It does mean that operational users are not required to set up, or to know, the communication paths or other user addresses/locations; they need only to

UNCLASSIFIED

Annex B to Chapter 9 to ACP 200

enter a pre-defined room to start or join DCP sessions. The system can be open, in that members without invitations can listen in, unless the room is capable of being locked as in CVW.

- g. An invitational system is where members can only join once invited by the Session Leader. In the case of Sametime, this can occur even if the member does not have the application open. An invite system ensures that no uninvited guests can participate.
- h. **Scalability.** Some DCP products have built in scalability features. An example is COMPASS where different bandwidth / quality levels can be selected for VTC and voice.
- i. **Type of Planning Sessions.** Deliberate and adhoc planning sessions can be conducted in either a time constrained or unconstrained environment. Adhoc planning sessions tend to be less formalized. Collaboration can therefore occur in a formalized (scheduled and controlled) or informal setting.

9B04 USER ACCESS

- a. **Access.** Access to DCP applications should be restricted to personnel whom have an operational or tactical requirement.
- b. **Employment.** As indicated by its name, DCP is for collaborative planning. It is provided to share information of an operational or tactical nature. Common uses are to:
 - Develop operational or tactical plans
 - Briefing operational or tactical plans
 - Brief Commanders intentions
 - Discuss or report situations / events as they occur
 - Conduct review of plans or doctrine
- c. DCP is not provided to send personal correspondence or exchange greetings. Private use of DCP can easily result in network congestion.
- d. **Role-based Access Control.** Users should be granted access rights for DCP tools by the system administrator on a user requirement. Figure 9-B-2 depicts the likely result where a large number of personnel would have access to chat but as the tools become more bandwidth hungry, users access steadily declines.

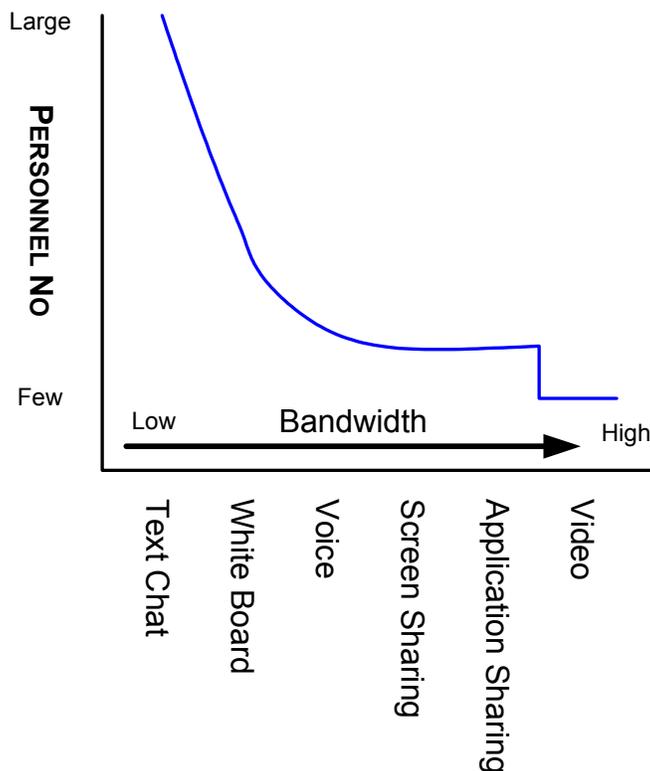


Figure 9-B-2 – Operator Number Impact on Bandwidth Usage

9B05 PLANNING ORDER

- a. **Preparation.** Where possible, planning sessions should be organized in advance and reflected in the Plan Of the Day (POD) or Schedule Of Events (SOE). This will ensure efficient allocation of resources, especially bandwidth. Special care should be exercised to observe all normal chain of command protocols and approval procedures.
- b. The benefits of informal or adhoc collaborations should be balanced against the additional bandwidth loading could impose on the network. The military commander/planner must balance time against the operational situation to determine whether to proceed in an orderly, unconstrained planning mode or in an adhoc mode. Ideally, higher bandwidth applications, especially VTC, should be left to programmed sessions.
- c. **DCP Plan of the Day.** The CTF/CTG should develop a POD for DCP that is based on inputs from operational commanders/planners. It should be reviewed by the CTF/CTG staff. As a minimum it should include:
 - Mission

UNCLASSIFIED

Annex B to Chapter 9 to ACP 200

- Scenario synopsis/situation/status
 - Linkages to other activities or objectives
 - Sessions start and end times
 - Session Leader and alternate (different locations recommended)
 - Participants
- d. **DCP Planning Order.** The Session Leader should release a planning order which publishes:
- guidance and tasking well in advance of the DCP session
 - any participants DCP constraints (i.e. unit 'x' has no VTC capability)
 - early what information is to be provided by whom
- e. **Planning for Degraded DCP Operations.** Graceful DCP degradation procedures are required in the event of communications bandwidth limitations. Typically this is accomplished by “stepping down” to less bandwidth intensive DCP tools and services.
- f. **Predefined User Communities.** It is recommended but not necessary that predefined user communities such as Ops Planning, Intel, C4I watch and Logistics are established to reduce administration overhead and assist coordination.

9B06 CONDUCT

- a. **Authority.** Units are to exercise positive control over the number and type of DCP sessions conducted.
- b. **Session Leader.** The initiating participant for a planning session is the Session Leader. The Session Leader is responsible for controlling the session. A key responsibility is the management of bandwidth demand.
- c. **Establishing / Joining a session.** To establish or join a session will depend upon whether a meeting room or invitational system is employed. In a meeting room environment all members should join the meeting place or lobby 10 minutes prior to the schedule start unless informed otherwise. For an invitational system, members should wait for an invitation. The session leader should issue the invitation 10 minutes before scheduled commencement unless briefed otherwise.
- d. **Posting Material to a session.** The use of objects in collaboration can enhance conversations. The benefits of posting material needs to be balanced by the additional bandwidth loading imposed on the network.

UNCLASSIFIED

Annex B to Chapter 9 to ACP 200

- e. Where possible, JPEG graphic formats should be preferred over higher memory formats such as Bitmap and TIF. Formats can be converted by using the 'save as' function and selecting a more appropriate format under the 'save as type' window.
- f. Where, editing is not required, Powerpoint presentations should be converted to JIF files. This will significantly reduce the file size. At the minimum powerpoint presentations should be saved in the 'Presentation' format rather than the other available formats.
- g. All files of a large nature should be zipped. Files containing imagery should be compressed by ICE.
- h. **Leaving / Closing a session.** Members should indicate their intention to leave a session. The Session Leader will be responsible for closing a session.
- i. **Inadvertent loss of session.** DCP sessions should be re-established as soon as possible. In a meeting room system, members should rejoin the designated room as soon as possible. For an invitational system, members will have to wait until they are re-invited.
- j. **VTC.** Care should be taken to monitor and actively control video sessions. If left uncontrolled, video bandwidth requirements from ad hoc users could easily degrade performance of the entire DCP network, with significant reductions in data flow rates for all network users. Additionally, scalable DCP products that allow bandwidth setting should be left at the default setting unless stipulated by Command.
- k. **Records.** The Session Leader should keep a copy of any presentation given in a collaborative session. Each unit should retain a copy of all chat correspondence. All records should be retained for a minimum of two weeks, after which time they can be erased. The records should be stored in a folder specially created for holding records (with sub folders delineating days) to ensure individual records do not become misplaced. Where the Session Leader deems necessary, minutes should be made and disseminated. (Technology does not exempt the established procedures for meetings.) The use of screen capture feature (*shift+ Print Scrn*) is a useful way to record information.

9B07 TOOL SELECTION

- a. DCP is most beneficial to the warfighter when the suite of DCP tools are used in combination. The most effective combination is the share program facility or whiteboarding facility used in conjunction with text and voice chat.
- b. Conducting meetings relying only on text chat is tedious and slow. The conduct of meetings tend to jump around because of the slow response time. By the time a participants types a message and then sends it (especially if lengthy), the discussion will have often moved on. A better solution is to use text chat to support voice chat; ie. the session would principally be voice but where important information was reinforced on text chat. Important information would be information other participants would want to record, such as key timings, positions and orders.
- c. If a session is to be conducted principally with text chat, it is clear a procedural process is required. One recommendation, which is similar to tactical voice procedures is that a participant indicates first he/she wants to make an entry. The first such entry which appears has the 'floor' unless the conveyer or OTC beaks in. The participant with the 'floor' would indicate completion of the transmission where the process begins again.
- d. Careful consideration as to the best tool(s) to employ in a collaborative session will assist in the sessions objectives being met and efficient use of bandwidth. For example, if the collaboration was to review of an OPTASK signal. This could be easily accomplished by posting the document to the homepage and using chat and if necessary voice. Text documents need not necessarily need to use the application or screen sharing tool which are more bandwidth hungry. The synchronous and asynchronous combination has been proven to be very effective. Similarly, graphics, pictures or charts need not necessarily be the sole purview of screen or application sharing tools. The homepage may be a more suitable alternative if examination is necessary prior to the collaborative session.

9B08 SECURITY

- a. Normal security procedures as for any other data or voice are to be adopted.
- b. **Inadvertent transmission.** Caution should be exercised with Voice and Video transmissions as unintended background discussions or classified

material may be captured and broadcast. Unattended Video and Audio sessions may also constitute a security breach depending on the classification and need to know of the broadcast environment. It is recommended that headsets are used for all audio sessions.

- c. **Multi-Level Security (MLS).** DCP is currently limited to accessing common networks at the same level of security as there are no MLS devices.
- d. **Firewalls.** Firewalls and filters should be configured to permit TCP/IP, FTP, and Multicast services transmissions. Coordination with network administrators controlling participating platforms operating behind firewalls and packet filters is required.
- e. **Encryption Data rates.** Encryption equipment employed should support data rates necessary for video.

9B09 NETWORK ENGINEERING

As part of the DCP network planning process, the following considerations should be factored into the backbone network design:

- Key sites requiring redundancy
- Potential single point of failures and identified work-around solutions
- Specific network bottleneck locations / equipment that might impact DCP across the entire backbone network (including encryption)
- Impact of various types of transmission media on DCP processes — the number of satellite hops, type of commercial landlines, packet loss etc

9B10 PRINCIPLES OF EFFECTIVE MEETINGS

- a. The convenience and user friendliness of DCP does guarantee collaborative sessions will be effective. The principles that govern effective meetings and military appreciation and planning remain as relevant and important (if not more). In fact, the ability to connect anyone with access to the network, will mean that many who participate will be uneducated and inexperienced in conducting successful meetings.
- b. The following general principles are worthy to consider:
 - i. Employ an agenda to help control the direction of a meeting.
 - ii. Solicit input for an agenda and circulate the agenda well in advance.

UNCLASSIFIED

Annex B to Chapter 9 to ACP 200

- iii. The Session Leader should consider summarizing what has been agreed or discussed for each agenda item.

9B11 WARNINGS AND PRECAUTIONS

The following is a listing of warnings and precautions that network administrators should be cognizant of:

- a. **Bandwidth Loading.** DCP Network Administrators and Mission Planners should be aware of bandwidth limitations and traffic demands on the network, not only from their own DCP session tools, but also from other systems sharing the network. Network overload can result in loss of DCP capabilities, and interruption of data exchange for other network users.
- b. **Inadvertent Transmission.** Mission Planners should ensure microphones and cameras are deselected when not in use. Failure to do so will result in unnecessary bandwidth usage and may constitute a security breach.
- c. **Central Processing Unit (CPU) Loading.** Some applications are computing-intensive as well as bandwidth-intensive. It is common for a number of applications to be running at the same time. The CPU load should be monitored. If the CPU load exceeds 50%, the operator should consider shutting down some applications.
- d. **Overuse of Action Planning.** The convenience of real-time technology combined with the awareness capability (see DCP CONOP) will increase the number of action (or impromptu) planning sessions. This will no doubt improve the dissemination of information and ideas, but if uncontrolled, it could also result in network congestion and the associate flow-on effect. Stringent user access, formalized procedures and education will avoid these problems.

Chapter 10

NETWORK ARCHITECTURE

1001 INTRODUCTION

A MTWAN comprises several autonomous systems, including: Task Group Area Network (TGAN), Maritime Marine Force (MMF) and the Maritime Air Group (MAG). The MAG architecture is not yet defined and will be included at a later date. The high-

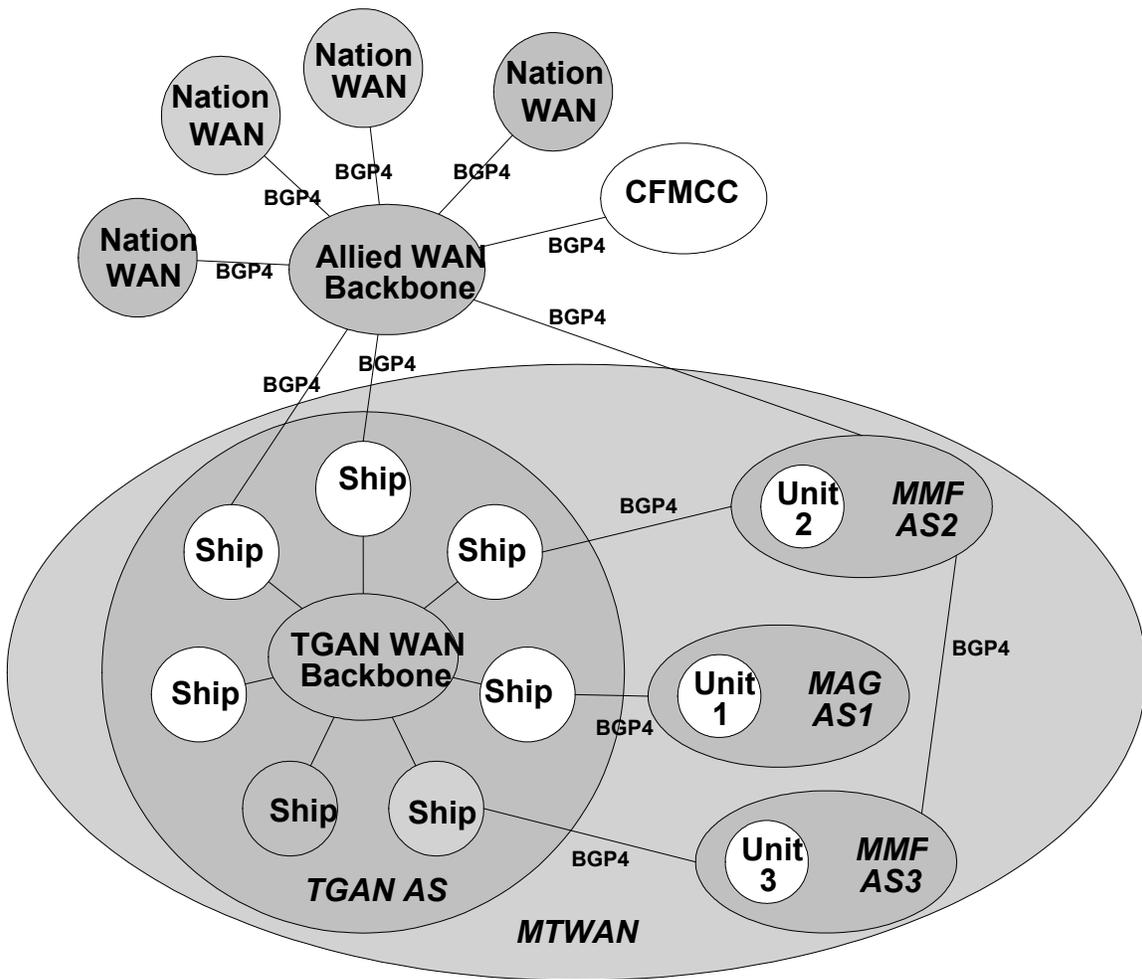


Figure 10-1: - MTWAN Overview

level network concept, first defined in Chapter 2, is a collection of maritime forces, shore forces, and shore communication stations, connected by a diverse collection of communication subnets as shown in Figure 10-1.

1002 AIM

The aim of this chapter is to detail the architecture for a MTWAN

1003 TECHNICAL ARCHITECTURE

- a. **System Architecture.** A MTWAN domain architecture is driven by the limits imposed by using standard routing protocols in order to achieve the operational connectivity. Routing will be accomplished using the standard IP protocols OSPF and PIM for interior-domain routing, and BGP4 for exterior-domain routing. The result is that the world will be divided into Autonomous Systems (AS) and areas within an AS, as shown in Figure 10-2. The areas within an AS are connected by backbone subnets.

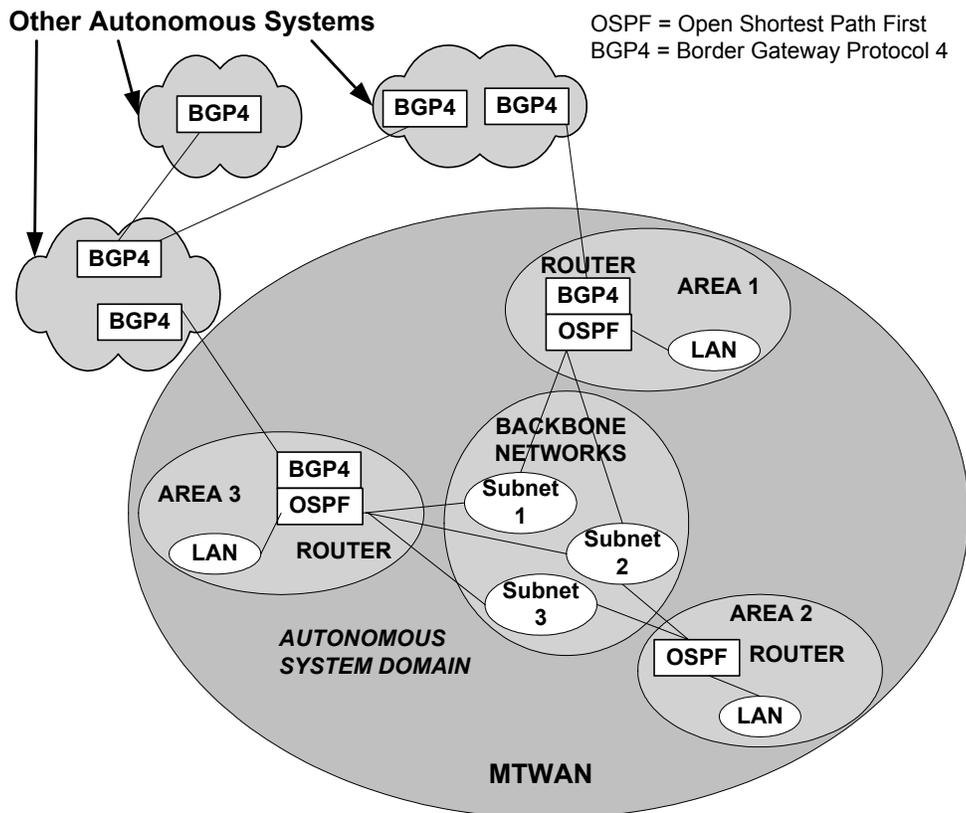


Figure 10-2: - MTWAN Autonomous System Description

An AS can have more than one exit point to other AS. When two or more exit points exist, some information must be provided to the interior routers to decide which BGP4 border router to select to reach an exterior destination. The multiple BGP4 border routers need to exchange routing information to support multiple entry and exit points of their own AS. This may be accomplished by running interior BGP4 or redistributing BGP routing information to OSPF. Detailed information on the routing domain architecture can be found in chapter 15.

b. MTWAN Node Descriptions

(1) Generic MTWAN Afloat Node Architecture. The generic node configuration for a ship is shown in Figure 10-3.

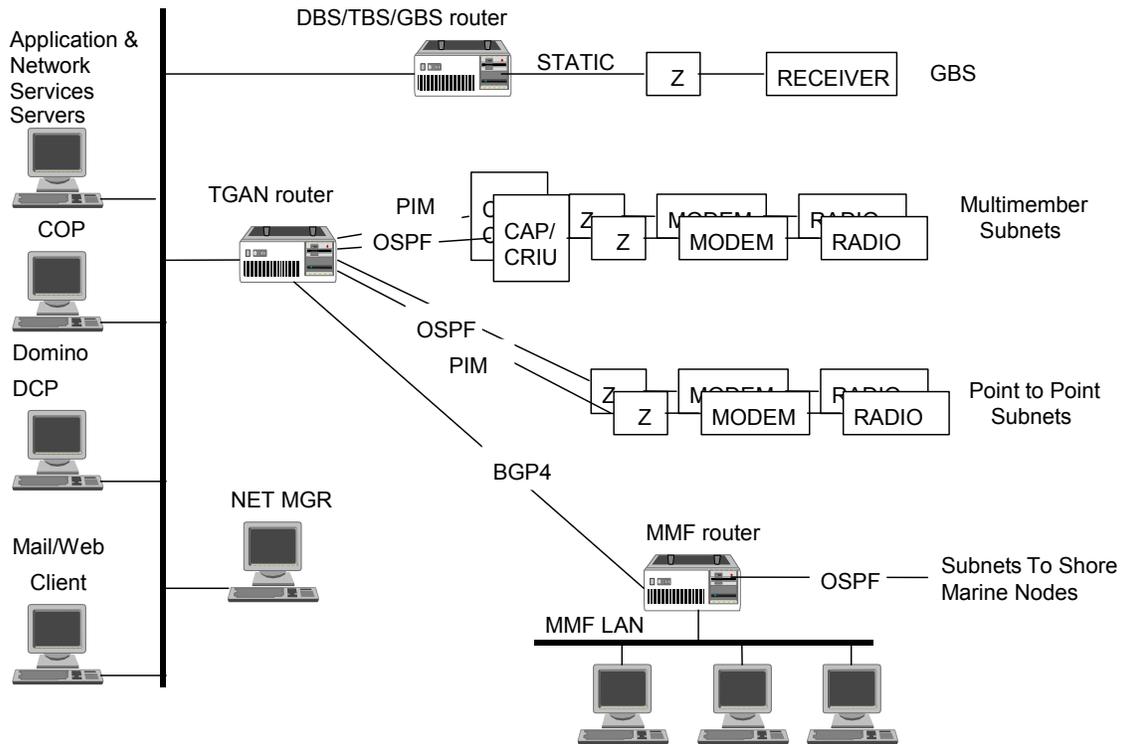


Figure 10-3: - Generic Ship Node Configuration

(2) For multi-member RF subnets, an MCAP (combined CAP and CRIU) acting as an Ethernet bridge, is required to support IP forwarding. The MCAP has an Ethernet connection to the TGAN router and a synchronous serial connection to a cryptographic device. It should be noted that, due to

the low data rates over RF, this connection will not be able to support the full load of an Ethernet connection.

- (3) On a point-to-point full-duplex link, the TGAN router will be connected directly to a cryptographic device via a synchronous serial interface.
- (4) The GBS router will interface the GBS receiver to the shipboard Ethernet LAN via a static routing serial port. There will be no exchange of routing information over this link.
- (5) MMF Node. This node includes the MMF LAN, the MMF router, and the MMF links. The MMF can also use other ships MTWAN subnets by connecting to a MTWAN router using BGP4. The connection to other coalition MMF will use BGP4 between the MMF routers.
- (6) **Generic Shore Node.** Figure 10-4 is the generic shore node configuration. The purpose of this node is to connect a MTWAN to an allied WAN AS.

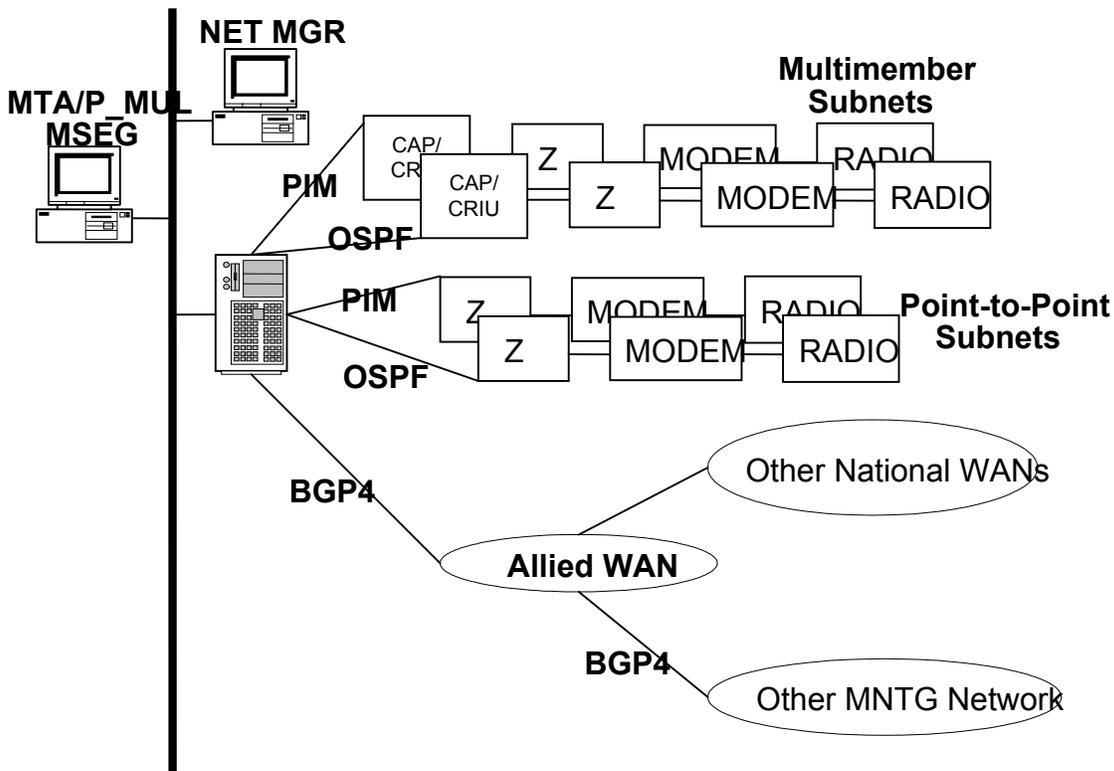


Figure 10-4: - Generic Shore Node Configuration

- (7) The shore node serves as a gateway between the MTWAN and an allied WAN. It also provides services such as mail and COP distribution.. The

shore node is connected to an Allied WAN using BGP4.

- (8) Each shore node can support multiple MTWAN ASs as shown in Figure 10-5. Each MTWAN AS will have its own router, which will be connected to the other MTWAN border routers, and to the allied WAN using BGP4. The use of a separate shore AS is optional, and is mainly used to support network security.

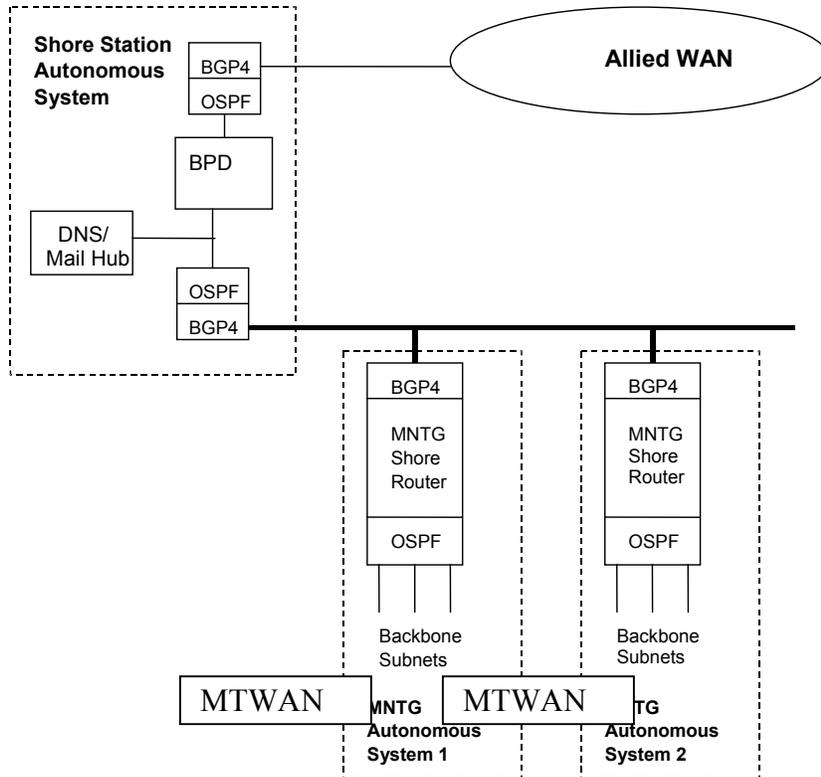


Figure 10-5: - Multiple Shore MTWAN Connections

- (9) **Generic CFMCC Node.** The CFMCC will normally be located ashore, either co-located with a MTWAN shore node or attached to an allied or national WAN. In principle, the CFMCC could be afloat, if adequate bandwidth is available. Figure 10-6 illustrates the generic configuration. CFMCC provides the tailoring of the COP and web-based information services to support MNTG operations. The CFMCC node will use BGP4 to connect to the WAN backbone.

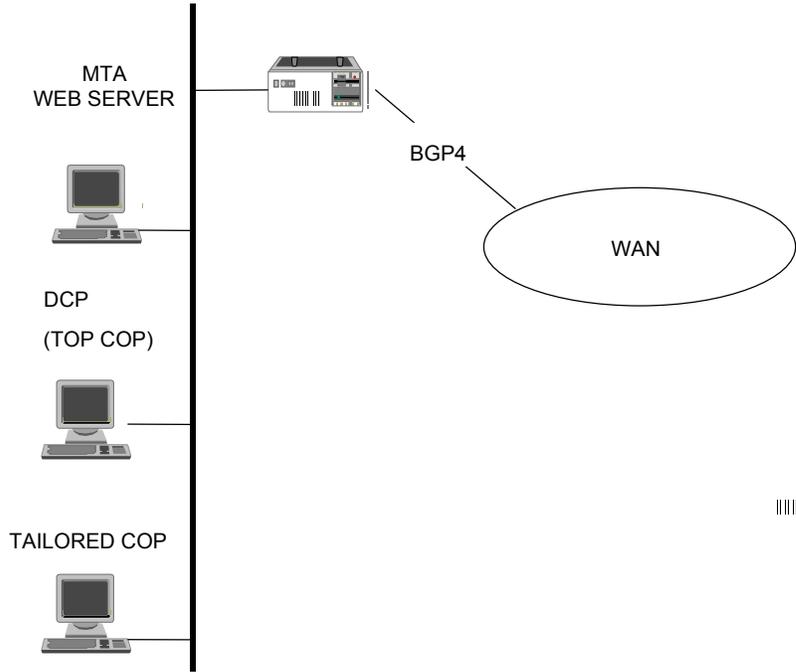


Figure 10-6: - CFMCC Node

1004 COMMUNICATION LINKS

The backbone subnets within a MTWAN AS consist of both point-to-point links and multimember (shared) subnets. Wide ranges of subnet combinations exist, as shown in the Figure 10-7. Subnets that can be employed with a MTWAN are described in Chapter 16.

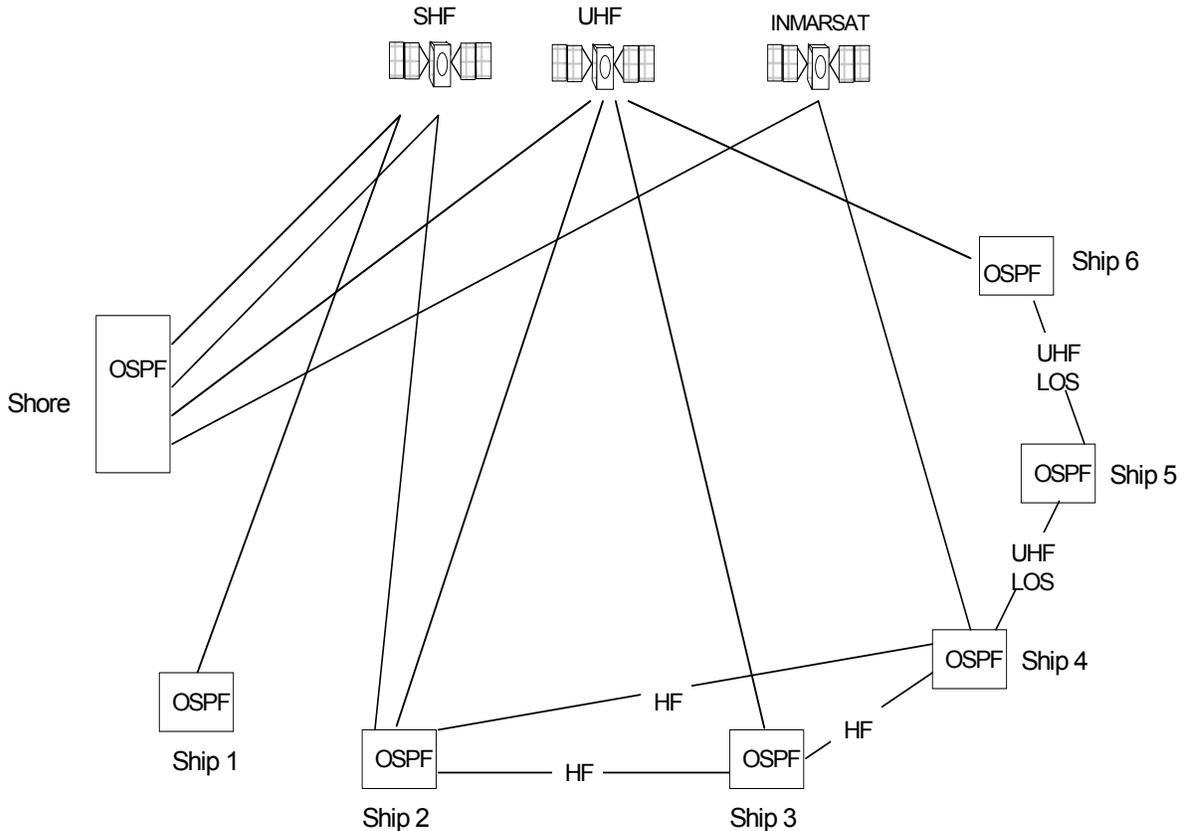


Figure 10-7: - MTWAN Subnet Combinations

There are two types of communication links, point-to-point and multi-member. Some of the point-to-point links are SHF SATCOM and INMARSAT. The bandwidth available to each ship is fixed by the link bandwidth. Congestion in a hub and spoke network would take place in the hub when many ships are trying to send to one ship. The multi-member subnets, such as UHF SATCOM, require some form of access protocol, as implemented in the MCAP, to share the available bandwidth.

1005 Security Architecture

The security architecture is designed to promote the flow of information at the tactical level while abiding by Allied security policies. This is achieved through a layered system of networks with a peer to peer tactical network isolated from Coalition and National networks by Boundary Protection Devices (BPD). The protection mechanism(s) between a MTWAN and National Networks will be consistent with the security policy of the respective nation. Network security details can be found in **Chapter 5**.

AMPHIBIOUS OPERATION STANDARD OPERATING PROCEDURES

10A01 INTRODUCTION

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.

10A02 AIM

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

10A03 PROCEDURE

A Multi-national Marine Force (MMF) amphibious operation is a four step process which consists of transit, assault, lodgment and sustainment. A typical network configuration in the transit phase is shown in Figure 10-A-1.

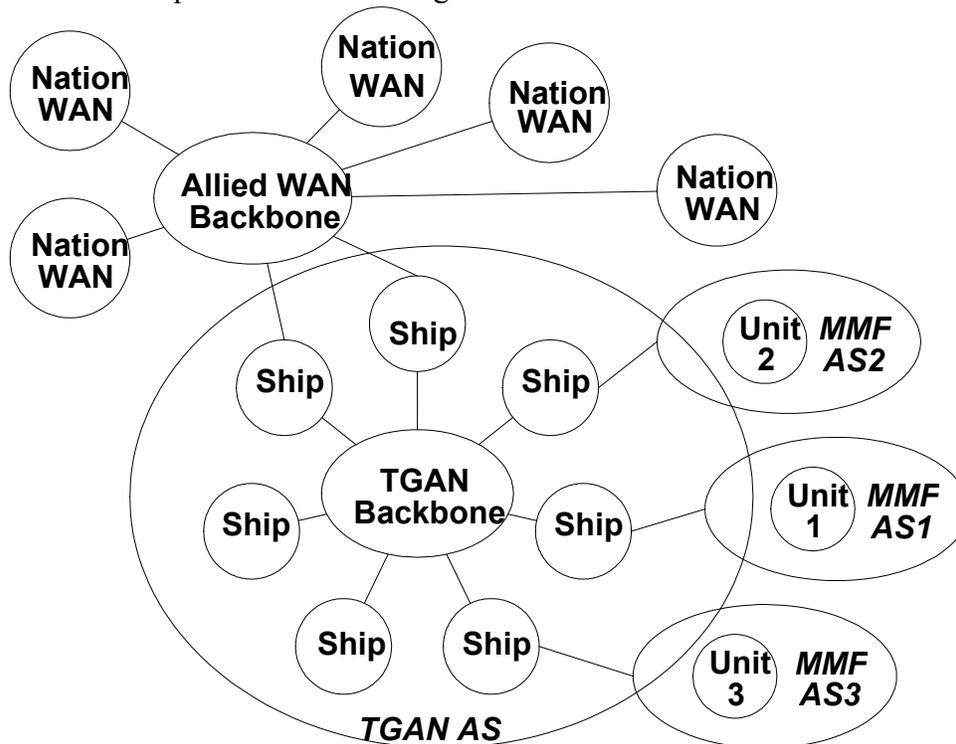


Figure 10-A-1: - MTWAN Transit Network Connectivity

In this example, three MMF units are located on three amphibious ships. Unit 2 is a US Marine force on a US ship. Unit 1 is a UK Marine force on a UK ship. Unit 3 is an Australian Forces on a AU ship. 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 10-A-2. Any communication between the MMFs in the transit phase would use the TGAN backbone subnets.

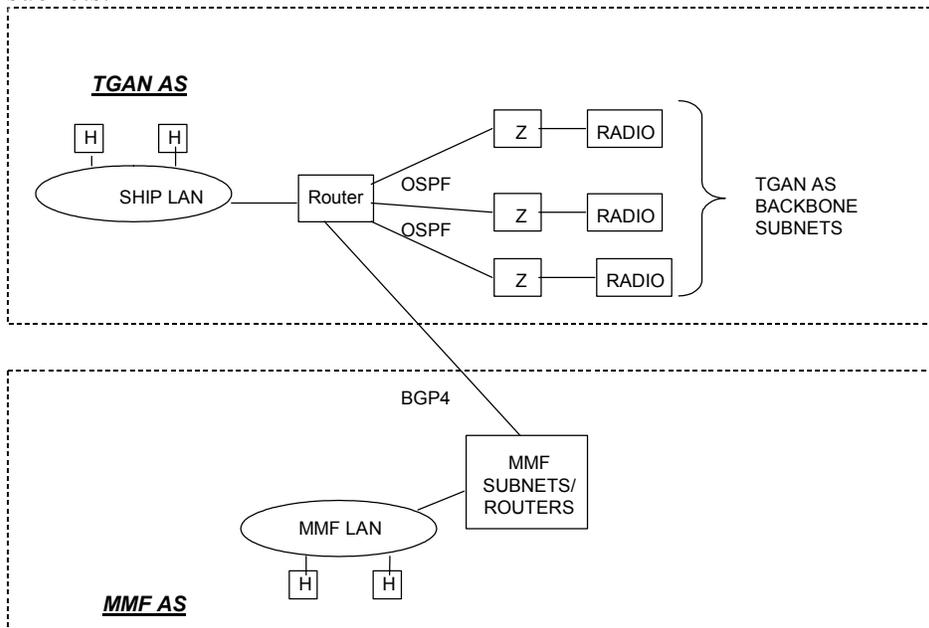


Figure 10-A-2: - MMF Node Configuration in Transit Phase

In a typical assault phase the network connections are shown as in the example, Figure 10-A-3.

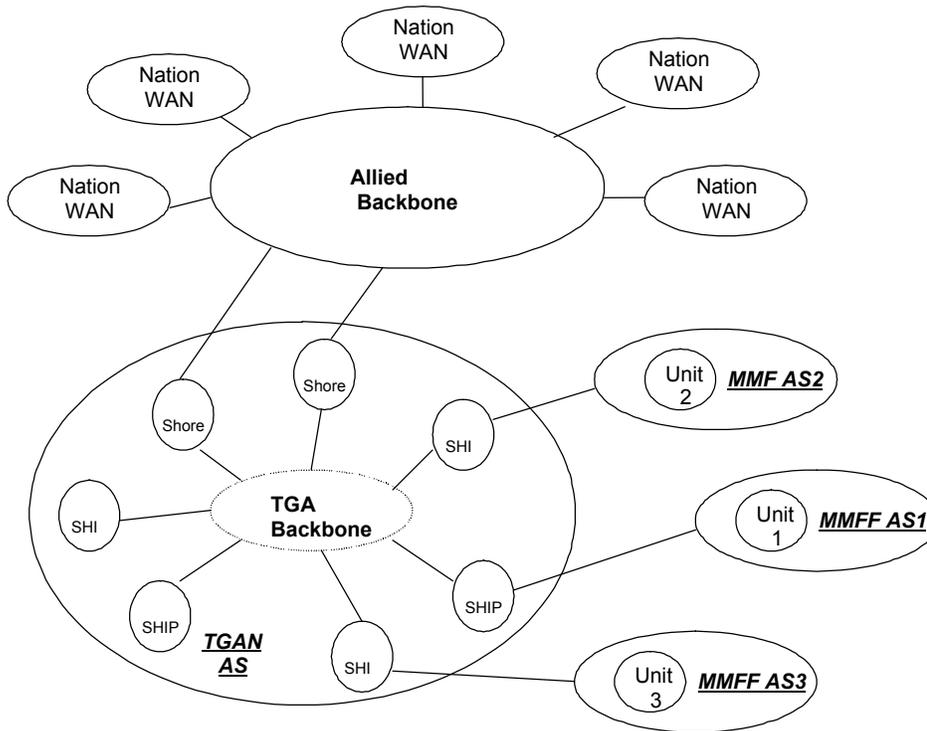


Figure 10-A-3: - MTWAN Network Connection in Assault Phase

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.

Typical MMF shore nodes are shown in Figure 10-A-4.

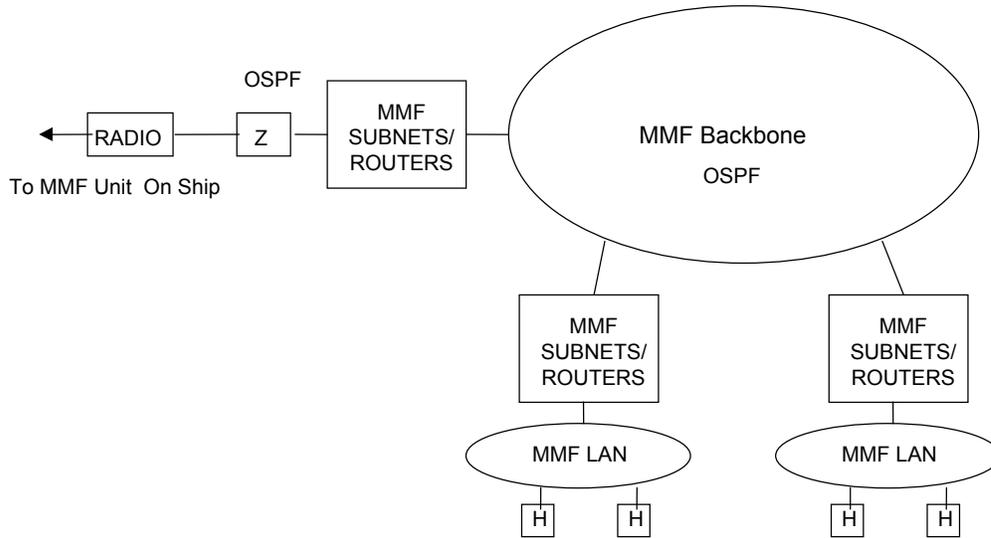


Figure 10-A-4: - MMF Shore Node Configurations – Assault Phase.

The ship node in the assault phase is shown in Figure 10-A-5.

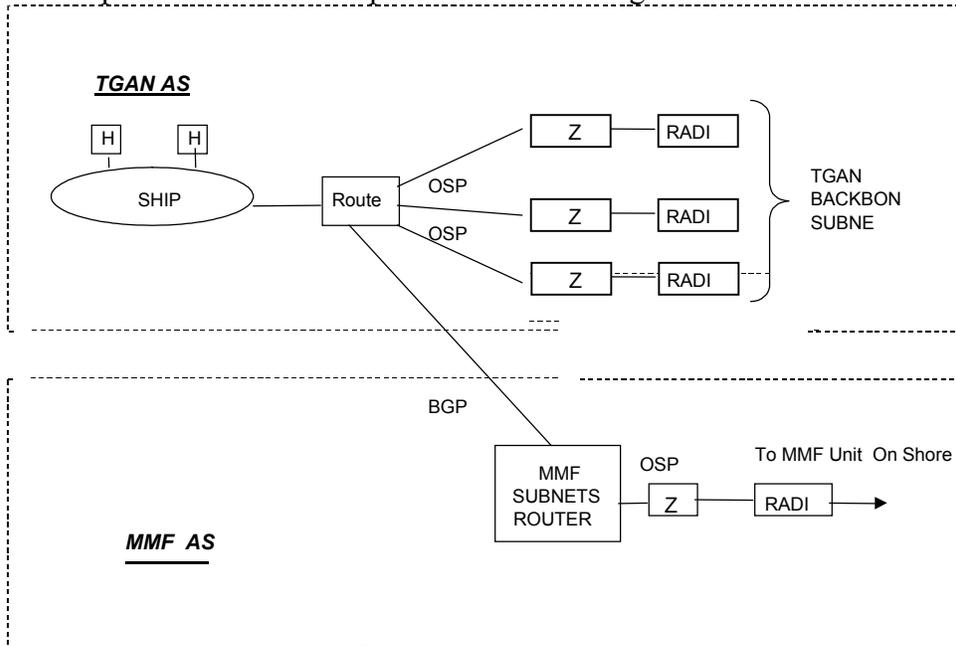


Figure 10-A-5 - Ship Node in Assault Phase

A typical lodgment phase configuration, shown in Figure 10-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.

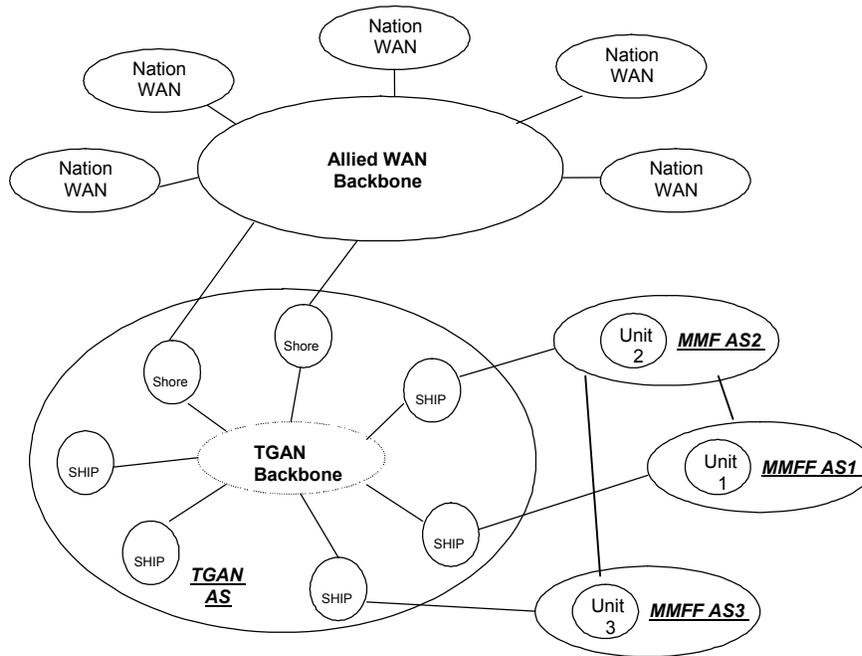


Figure 10-A-6: - MTWAN Network Connection in Lodgment Phase

The general MMF unit node configurations are likely to be as shown in Figure 10-A-7. In this configuration the MMF node will include a router connected to another MMF network using BGP4.

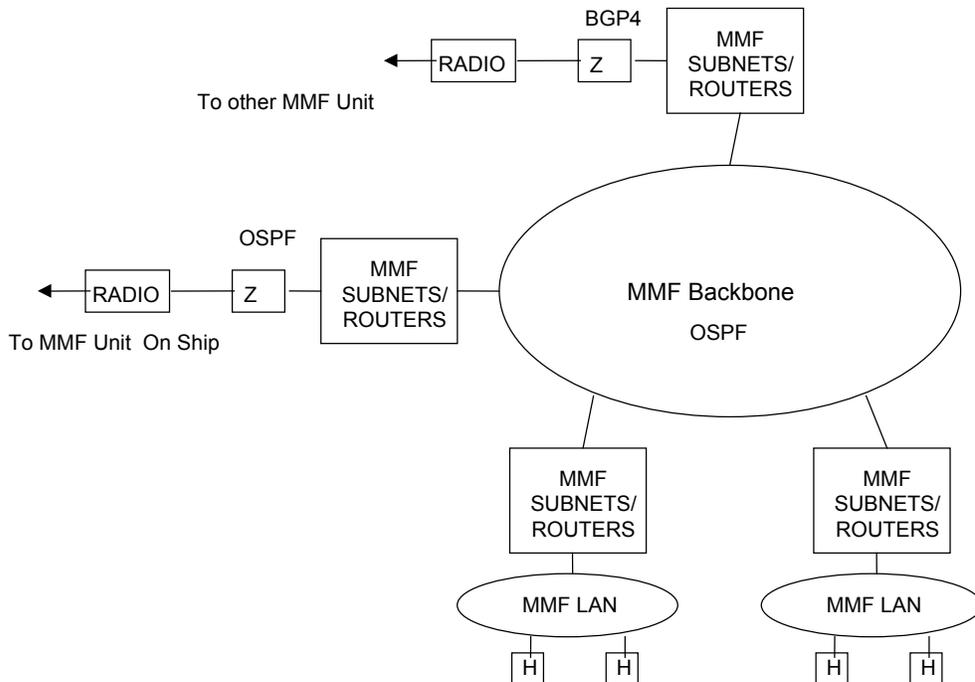


Figure 10-A-7: - MMF Network Nodes in Lodgment Phase

A typical sustainment phase is shown in Figure 10-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.

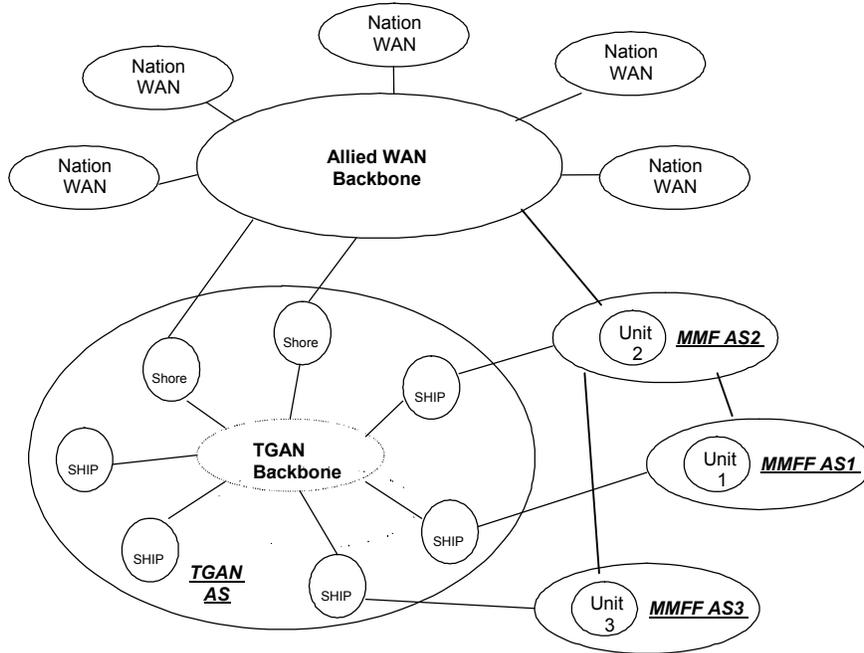


Figure 10-A-8: - MTWAN Network in Sustainment Phase

The node configuration for unit 2 in the sustainment phase is shown in Figure 10-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.

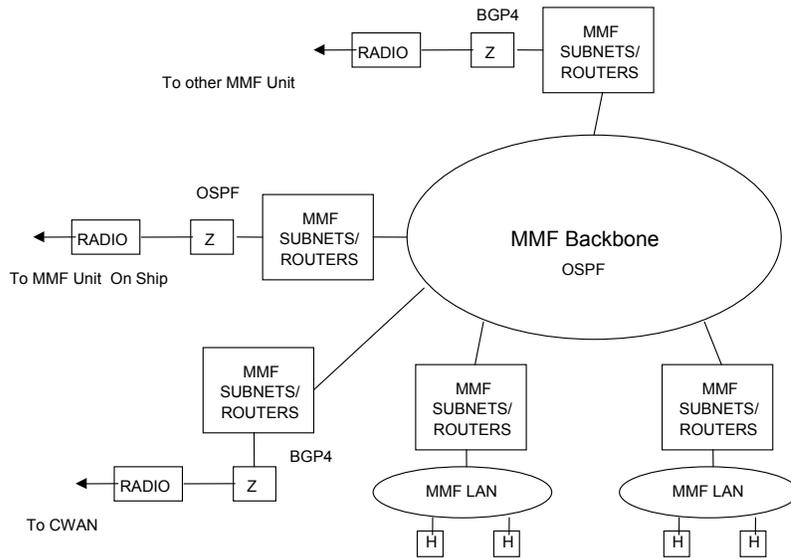


Figure 10-A-9: - MMF Unit 2 Node Configuration in Sustainment Phase

Chapter 11

NETWORK TRAFFIC PRIORITIZATION

1101 INTRODUCTION

The limited bandwidth available in maritime tactical networks is often insufficient to effectively transport the total offered traffic. Furthermore, the best-effort nature of IP networking can result in significant performance degradation when a network approaches overload. To minimise the operational impact of these effects, it is highly desirable to implement prioritization techniques to ensure that more important traffic is afforded an improved grade of service.

1102 AIM

The aim of this chapter is to address the requirement for traffic prioritization mechanisms and procedures.

1103 OVERVIEW

- a. **Bandwidth Reservation.** Bandwidth may be reserved in the network on the basis of a number of criteria, including source address, destination address, source port, destination port, protocol type, or Type of Service (TOS) byte value. When enough features are selected (such as source address, destination address, and protocol type), bandwidth is reserved for a single flow. Bandwidth may also be reserved for a single class of traffic, perhaps indicated by the TOS byte value. Control information must be exchanged to set up any bandwidth reservation and, therefore, is a connection-oriented operation. Reserving bandwidth on a per flow basis provides a finer grade of control at the expense of an increase in overhead and more complicated network management. Reserving bandwidth for a particular traffic class reduces overhead but may require additional control at the network injection points so that the number of flows of a particular type do not overwhelm the available reservation. Reserved bandwidth is made available to other traffic when it is unused
- b. **Differentiated QoS.**
 - (1) **Traffic Management.** Traffic arriving at a network node may receive access to transmission opportunities on the basis of its identifying

characteristics (such as source address, destination address, and traffic class). This is often referred to as “priority.” Strictly speaking, the term priority implies a linear ordering on the arriving traffic types; however, more sophisticated mechanisms for allocated transmission assets are available. Bandwidth allocation mechanisms, or schedulers include: (i) First In-First Out (FIFO), (ii) strict priority mechanisms, (iii) mechanisms which allocate transmission opportunities in an unequal fashion such as weighted round robin and Weighted Fair Queuing (WFQ). There are also other mechanisms, as well as various combinations. FIFO schedulers are the default mechanism for IP networks that provide undifferentiated service. All traffic is equal and the oldest traffic enqueued is served first. Strict priority mechanisms serve all traffic of higher priority waiting before any traffic of a lower priority is transmitted. Traffic requiring timely delivery, may be assigned a higher priority than traffic which is not delay-sensitive. Without any further constraints, traffic of the highest priority if arriving in sufficient quantity, may deny service to any other traffic. To prevent this, there is some merit in applying bounds on the amount of bandwidth allocated to each priority if strict priority scheduling is to be employed. WFQ and related schedulers can, through manipulation of the weights, provide relatively more service to one class over another without denying service to any. Thus, a form of “soft priority” is maintained.

- (2) **Buffer Management.** Traffic waiting for transmission must be buffered. Just like transmission bandwidth, buffer space is a finite resource at each network node. In the presence of congestion, the buffers will fill and eventually traffic must be dropped. The default mechanism is ‘tail drop’ where traffic arriving at a node with full buffers is dropped. As traffic dropping is detected (e.g by higher layer protocols such as TCP operating at the source) the traffic injection rate can be reduced to help relieve the congestion in the network. Schemes besides ‘tail drop’ may be employed to manage buffer resources at a network node. Traffic which is time-sensitive and which has already expired may be dropped from the buffer to make room for a packet just arrived to a full buffer. Other mechanisms such as Random Early Drop (RED) begin to drop packets randomly as the buffers fill with the dropping probability increasing with buffer size. Higher layer mechanisms such as TCP are thereby given a chance to react more quickly to network congestion. A scheme which applies random early dropping to different traffic classes differently is called Weighted Random Early Dropping (WRED).

c. Control Mechanisms.

- (1) **Admission Control.** Mechanisms that control the amount of traffic entering the network at injection points perform admission control. Such mechanisms are needed when bandwidth is reserved for a flow, for example, to insure that the offered traffic load does not exceed the bandwidth reservation. It is possible that no admission control is performed, particularly for best-effort traffic.
- (2) **Flow Control.** Flow control mechanisms act to control the amount of traffic entering the network from flows already admitted. Flow controls include those that are feedback-based and those that are not. Feedback-based controls rely on responses from destinations to indicate congestion. The most widely deployed of these is TCP. TCP uses acknowledgements of packet receptions from destinations to assess network congestion levels and control traffic injection appropriately. Examples of flow control mechanisms that do not rely on feedback are 'source quench' techniques and 'traffic shaping' mechanisms. In the former, explicit notification of congestion is sent back to sources with a request to limit their injection rates. In the latter, sources unilaterally enforce limitations on the traffic they offer to the network. Among traffic shapers, leaky bucket shapers are the most widely deployed.

1104 IMPLEMENTATION OF COMMANDER'S POLICY

- a. **Operational requirements.** A commander will have a position on the relative importance of particular classes of traffic, and of specific information sources or destinations. This view will change as an operation develops. Therefore, the priority mechanisms must be able to be reconfigured as necessary to respond to these changes.
- b. **Application requirements.** Some applications may require enhanced quality of service for effective operation - for example voice over IP. However, these applications may not be as critical as others to the success of the operation. Again the decision on the priority mechanisms to be used and priority level to be assigned must be derived from the commander's policy.
- c. **Policy interpretation.** The selection of priority mechanisms and assignment of priority to specific classes of traffic and source, destination addresses will be co-ordinated by the primary NOC.

1105 IMPLEMENTATION

- a. Configuration.** Individual platforms will configure their network elements (e.g routers, traffic shapers) in accordance with direction from the Primary NOC.
- b. Monitoring.** The NOCs will monitor traffic flow. If necessary, the NOCs will vary the priority instructions to respond to changes in traffic demand.

1106 CONCLUSION

The use of prioritization is important to maintain effective operation in bandwidth-limited networks. The network manager is responsible for the management of the priority mechanisms to meet the commander's operational requirements.

Chapter 12

NETWORK MANAGEMENT

1201 INTRODUCTION

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

1202 AIM

The aim of this chapter is to provide guidance for the Network Management of a maritime tactical WAN.

1203 OVERVIEW

- a. 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)
- b. 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).
- c. 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 Level NOC.

1204 NM ARCHITECTURE (HIERARCHY)

- a. **Primary NOC.** 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.

- b. **National NOC.** The national NOCs are responsible for coordinating network services within their national boundaries and to coordinate activities with the primary NOC.
- c. **Node Level.** 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.

1205 NM ELEMENTS

The elements of network management are:

- a. Configuration Management which controls the behaviour of the network and can be considered to comprise:
 - (1) Configuration, monitoring and control of routers, other SNMP-managed network devices and CAP/CRIU;
 - (2) Provisioning, bandwidth management and monitoring;
 - (3) Route Policy Management (which networks carry transit traffic, diversity routing, tunnelling and overlay network management, security service levels for routing protocols, etc.); and
 - (4) Management of DNS, network time service, and other required infrastructure services
- b. Performance Management which measures the performance of the network hardware, software and media. It comprises:
 - (1) Monitoring of Links, Routers, network connectivity and Services;
 - (2) Net loading, congestion control monitoring;
 - (3) Performance optimisation for bandwidth-disadvantaged users;
 - (4) Service Prioritisation;
- c. Fault Management
 - (1) Fault detection, isolation and troubleshooting;

- (2) Fault-logging and analysis.
- d. Security Management which control access to information on the network, and can be considered to comprise:
 - (1) Intrusion detection and response, including co-ordination of multiple detections received from diverse locations;
 - (2) Vulnerability assessment;
 - (3) Security Policy Establishment, Monitoring, & Enforcement;
 - (4) Firewall Management;
 - (5) Response Centre activities (route attack notifications to CERTs, co-ordinate fixes);
 - (6) 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); and
 - (7) Encryption Device Management (e.g., TACLANE/FASTLANE Management).
- e. Administration which comprise the generation of reports, pertaining to:
 - (1) Robust Network Management under varying operational conditions (i.e., EMCON);
 - (2) DNS Co-ordination;
 - (3) Interface with other non-MTWAN network management entities (e.g., national NOCs and their network management systems);
 - (4) Provisioning requests up to national NOCs; responses down to MTWAN NOC;
 - (5) Critical fault alerts/alarms sent up to national NOCs; and
 - (6) Configuration and performance summary status/statistics sent up to national NOCs.

1206 REMOTE OR LOCAL MANAGEMENT

- a. 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.
- b. 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.

1207 GENERATION OF REPORTS

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.

1208 SECURITY RESPONSIBILITY

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

1209 TOOLS

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.

NETWORK MANAGEMENT SOP

12A01 INTRODUCTION

The management of an MTWAN involves monitoring the operation of application servers (ie Domino, Sametime and mail servers), network servers (i.e. DNS and multicast transport protocols) and network devices (i.e. routers). 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.

12A02 AIM

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

12A03 SCOPE

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

- Gathering LAN and WAN traffic statistics to support future planning and network optimisation;
- Monitoring the health of network devices and application servers;
- Monitoring the operation of network services and C2 applications;
- Identifying network changes; and
- Troubleshooting network and application problems.

12A04 NETWORK MANAGEMENT TOOLS

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

12A05 NETWORK MANAGEMENT STRATEGY

- a. A MTWAN NOC will be operated on a 24/7 basis. The MTWAN Network manager will be responsible for the following:
 - Configuration of routers, servers and user workstations;
 - Installation of NM station;

UNCLASSIFIED

Annex A to Chapter 12 to ACP 200

- Installation of applications and network services;
 - Configuration of WAN links including CAP/CRIU, radio
 - Configuration of cryptographic equipment;
 - Configuration of applications and network in support of EMCON; and
 - Collection of local network statistics.
- b. 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.
- c. 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.
- d. 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.
- e. 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.
- f. 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).
- g. 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.
- h. 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.
- i. 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

UNCLASSIFIED

Annex A to Chapter 12 to ACP 200

application servers. The view will be updated at least every 30 minutes and be accessible to units network managers via a Web browser.

- j. 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.
- k. An FTP server is to 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.

12A06 NETWORK MANAGEMENT TOOLS SET -UP

- a. To establish NM tools discussed above, the following installation and set-up is required:
 - (1) Install Mchat (a multicast text chat for use by network managers).
 - (2) 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.
 - (3) 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.
 - (4) Enable SNMP on all hosts and set their “read-only” Community Name (editing SNMP Agent’s Management Information Base {MIB} is not allowed).
 - (5) 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.
 - (6) 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.*

UNCLASSIFIED

Annex A to Chapter 12 to ACP 200

- (7) 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.
- (8) Enable the collection of local network statistics.

12A07 TROUBLESHOOTING

- a. The most common problems that occur in an operational IP network are:
 - Slow Responses;
 - Connectivity Problems; and
 - Application Problem.
- b. Slow Responsiveness
 - (1) When an application is running slowly, the cause of the problem may be a congested network or an overloaded server.
 - (2) 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.
 - (2) 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.
- b. Connectivity Problem
 - (1) When connection to a remote server cannot be established, the problem may be caused by one of the following: DNS; unreachable host; or routing.
 - (2) Use the Lookup tool to verify name & address resolutions and resolve any DNS problems.
 - (3) Use Ping command to verify that the remote host is reachable.
 - (4) If the remote host is unreachable, verify with the remote network manager that the remote host is operational.
 - (5) If the remote host is operational, use the 'TraceRoute' command to locate

UNCLASSIFIED

Annex A to Chapter 12 to ACP 200

any routing problems and inform the NOC of the problems.

c. Application Problem

(1) The most likely causes of application problems are:

- Remote server hardware is faulty;
- Remote server software is badly configured; and/or
- Local client software is badly configured.

(2) 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.

**OPTASK NET
(CONFIDENTIAL WHEN COMPLETED)**

A. OVERVIEW

A1. Purpose

The purpose of this OPTASK is to provide information and direction to setup and configure a Maritime Tactical Wide Area Network (MTWAN).

A2. Objective

Provide maritime units operating with a multinational task group with the capability to maintain access to an allied tactical network.

B. ADMINISTRATION

B1. Period

Stipulate effective period.

B2. Scope

Provide the technical information for the provision of an MTWAN including the setup, configuration, maintenance and management.

B3. Change Management

Stipulate the procedure for recommending changes to OPTASK and for promulgation of changes.

B4. References

Provide list of references. For example:

- B4.1. ACP 200 (MTWAN)
- B4.2. OPTASK COMMS
- B4.3. OPTASK KM
- B4.4. OPTASK FOTC

C. DUTIES

Describe duties / responsibilities for network and NOC managers.

UNCLASSIFIED

Annex B to Chapter 12 to ACP 200

- C1. **CTG Network Manager**
- C2. **NOC Manager**
- C3. **Unit Network Manager**
- D. **NAMING AND ADDRESSING**
 - D1. **Unit name**
 - D2. **IP address/Mask**
 - D3. **Multi-cast group and class D address**
 - D4. **DNS Root Server(s)**
 - D5. **Domain responsibility**
 - D5.1. Primary (Primary NOC/service.country/primary IP address/secondary IP address) (eg: MTWAN NOC/NAVY.US/A.B.C.D/A.B.C.D)
 - D6. **Host names and IP addresses**
- E. **ROUTING**
 - E1. **AS number**
 - E2. **Bandwidth**
 - E3. **OSPF settings (area/dead time/hello interval/retransmit/cost)**
 - E4. **PIM settings (mode/ R/V point)**
- F. **SUBNETS**
 - F1. **UHF SATCOM**
 - F1.1 CAP ID (unit/unique ID number)
 - F1.2 IP address/Mask (A.B.C.D/Hex)
 - F1.3 Baud rate
 - F1.4 Guard time
 - F1.5 Time Bytes
 - F1.6 Unique crypto settings
 - F2. **INMARSAT B**

- F2.1 Unit/number
- F2.2 IP address/Mask
- F2.3 Baud rate
- F2.4 Unique crypto settings

F3. HF BLOS

- F3.1 CAP ID (unit/unique ID number)
- F3.2 IP address/Mask (A.B.C.D/Hex)
- F3.3 Modem mode
- F3.4 Baud rate
- F3.5 Interleave mode
- F3.6 Transmit frequencies (ship freq/shore freq)
- F3.7 Eval interval
- F3.8 Unique crypto settings

F4. IP 5066

- F4.1 Unit ID (unit/unique ID number)
- F4.2 IP address/Mask (A.B.C.D/Hex)
- F4.3 Modem mode
- F4.4 Baud rate
- F4.5 Interleave mode
- F4.6 Transmit frequencies
- F4.7 Unique crypto settings

G. NETWORK MANAGEMENT

G1. Unit NM reporting requirements

Stipulate the Network Management (NM) reporting requirements of individual units.

G2. Help desk policy

Promulgate help desk policy.

G3. NOC telephone numbers

Stipulate telephone numbers for the Network Operations Centre (NOC).

H. APPLICATIONS

List applications. Include application version number, IP address and other important relevant information.

H1. **Messaging**

- H1.1 MSeG version nr
- H1.2 Sendmail version nr
- H1.3 Mx record
- H1.4 Mailer table
- H1.5 Multicast IP address
- H1.6 Outbound configuration file
- H1.7 MSeG configuration
- H1.8 Sendmail.cf configuration

H2. **Common Operational Picture (COP)**

- H2.1 MSeG version nr
- H2.2 Multicast address
- H2.3 Congestion control
- H2.4 MSeG configuration

H3. **Web Services**

- H3.1 Domino version nr
- H3.2 Primary DOMINO server IP address
- H3.3 DOMINO name structure
- H3.4 Web browser version nr.

H4. **DCP**

- H4.1 SAMETIME version nr
- H4.2 SAMETIME server IP address

OPTASK NET (Example)

**(CONFIDENTIAL WHEN COMPLETED
OUTSIDE OF ACP 200)**

A. OVERVIEW

A1. Purpose

The purpose of this OPTASK is to provide information and direction to setup and configure the networks in support of the Maritime National Task Group (MNTG) for the Joint Warrior Interoperability Demonstration 2003 (JWID 03).

A2. Objective

Provide maritime units operating with MNTG the capability to maintain access to the JWID network(s).

B. ADMINISTRATION

B1. Period

Effective on receipt. Cancel upon completion of JWID 03 or when superseded.

B2. Scope

This OPTASK provides the technical information necessary to setup, configure, maintain and manage a MTWAN.

B3. Change Management

Proposed changes to this OPTASK are to be forwarded to the CTG Network Manager for inclusion in an OPTASK NET Supplement or re-publishing.

B4. References

- B4.1. ACP 200 (MTWAN)
- B4.2. OPTASK COMMS
- B4.3. OPTASK KM
- B4.4. OPTASK FOTC

C. DUTIES

C1. CTG Network Manager

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

C1.1. The CTG Network Manager is responsible to the CTG for maintaining the good working of the networks under the CTG responsibility. He is also to collect and publish the following information daily at 1200Z:

- C1.1.1. All network status
- C1.1.2. Overall performance
- C1.1.3. Network troubles if any
- C1.1.4. Planned Network outage if any
- C1.1.5. Misc. information

C2. NOC Network Manager

C2.1. The NOC Network Manager is responsible for network maintenance. This includes establishment and monitoring of networks to support MNTG, and customer service support.

C2.2. The NOC Network Manager is also responsible to the CTG to provide IP addresses to units requiring them via an OPTASK NET supplement containing all pertinent information.

C2.3. Assigned NOC Network Managers follow (to be read in 4 columns: country/poc/phone number/e-mail).

a-us/Mr. John Citizen/612 6266 XXXX/john.citizen@defence.gov.au
b-ca/Lt(N) John Doe/819 994 XXXX/Doe.J@forces.gc.ca
c-nz/Lt John Kirwin/632 7098 XXXX/john.kirwin@nzdf.mil.nz
d-uk/Mr. Andrew Citizen/44 9380 XXXX/Andrew.citizen@gtnet.gov.uk
e-us/Ms. Jane Doe/619 553 XXXX/jane.doe@navy.mil

C3. Unit Network Manager

C3.1. The Unit Network Manager is responsible to his/her CO for the maintaining and good functioning of the Network under the CO responsibility. He is also responsible to the CTG Network Manager to report the network status and deficiencies.

C3.3. Assigned Unit Network Managers follow (to be read in 4 columns: country/poc/phone number/e-mail).

a-us/Mr. John Citizen/612 6266 XXXX/john.citizen@defence.gov.au
b-ca/Lt(N) John Doe/819 994 XXXX/Doe.J@forces.gc.ca
c-nz/Lt John Kirwin/632 7098 XXXX/john.kirwin@nzdf.mil.nz
d-uk/Mr. Andrew Citizen/44 9380 XXXX/Andrew.citizen@gtnet.gov.uk

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

e-us/Ms. Jane Doe/619 553 XXXX/jane.doe@navy.mil

D. NAMING AND ADDRESSING

D1. Unit name

D1.1. Unit names are promulgated below (Read in 2 columns: unit/letters desig):

D1.1.1.	AU NOC/aunoc
D1.1.2.	HMAS Canberra/can
D1.1.3.	HMAS Manoora/man
D1.1.4.	HMAS Robertson/rob
D1.1.5.	CA NRS Bras D'Or/nrsbdo
D1.1.6.	HMCS Coaticook/coa
D1.1.7.	HMCS Renfrew/ren
D1.1.8.	NZ NOC/nznoc
D1.1.9.	HMNZS Waka/wak
D1.1.10.	UK NOC/noc
D1.1.11.	HMS Albion/alb
D1.1.12.	HMS Ocean/oce
D1.1.13.	HMS Illustrious/ill
D1.1.14.	UK 3 CDO BDE/uk3cdo
D1.1.15.	UK 40 CDO/uk40cdo
D1.1.16.	US NRS/nrssd
D1.1.17.	USS Bataan/bat
D1.1.18.	USS Paul Hamilton/pha

D2. IP address/Mask

The following IP addresses/Netmasks are promulgated. (Read in 4 columns: unit/network/netmasks/broadcast.)

D2.1 Australia

a-NOC/xxx.xxx.42.0/255.255.255.240/xxx.xxx.42.15
b-HMAS Canberra/xxx.xxx.42.16/255.255.255.240/xxx.xxx.42.31
c-HMAS Manoora/xxx.xxx.42.32/255.255.255.240/xxx.xxx.42.47
d-HMAS Sydney/xxx.xxx.42.48/255.255.255.240/xxx.xxx.42.63
e-Spare/xxx.xxx.42.64/255.255.255.240/xxx.xxx.42.79
f-Spare/xxx.xxx.42.80/255.255.255.240/xxx.xxx.42.95
g-Spare/xxx.xxx.42.96/255.255.255.240/xxx.xxx.42.111

D2.2. Canada

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

a-NRS Bras D'Or/xxx.xxx.192.0/255.255.255.0/xxx.xxx.192.255
b-HMCS Coaticook/xxx.xxx.192.0/255.255/255.0/xxx.xxx.194.255
c-HMCS Renfrew/xxx.xxx.192.0/255.255.255.0/xxx.xxx.196.255

D2.3. New Zealand

a-NZ NOC/xxx.xxx.42.128/255.255.255.240/xxx.xxx.42.143
b-HMNZS Te Mana/xxx.xxx.42.144/255.255.255.240/xxx.xxx.42.159
c-NZ FE/xxx.xxx.42.160/255.255.255.240/xxx.xxx.42.175
d-Spare/xxx.xxx.42.176/255.255.255.240/xxx.xxx.42.191
e-Spare/xxx.xxx.42.192/255.255.255.240/xxx.xxx.42.207
f-Spare/xxx.xxx.42.208/255.255.255.240/xxx.xxx.42.223
g-Spare/xxx.xxx.42.224/255.255.255.240/xxx.xxx.42.239
h-Spare/xxx.xxx.42.240/255.255.255.240/xxx.xxx.42.255

D2.4 United Kingdom

a-UK NOC/xxx.xxx.xx.xxx/255.255.255.240/xxx.xxx.xx.xxx

D2.5. United States

a-NRS SD/xxx.xxx.43.0/255.255.255.240/xxx.xxx.43.15
b-USS Bataan/xxx.xxx.43.16/255.255.255.240/xxx.xxx.43.31
c-USS Paul Hamilton/xxx.xxx.43.32/255.255.255.240/xxx.xxx.43.47
d-USMC Det/xxx.xxx.43.48/255.255.255.240/xxx.xxx.43.63
e-Spare/xxx.xxx.43.64/255.255.255.240/xxx.xxx.43.79
f-Spare/xxx.xxx.43.80/255.255.255.240/xxx.xxx.43.95
g-Spare/xxx.xxx.43.96/255.255.255.240/xxx.xxx.43.111
h-Spare/xxx.xxx.43.112/255.255.255.240/xxx.xxx.43.127
j-Spare/xxx.xxx.43.128/255.255.255.240/xxx.xxx.43.143
k-Spare/xxx.xxx.43.144/255.255.255.240/xxx.xxx.43.159
l-Spare/xxx.xxx.43.160/255.255.255.240/xxx.xxx.43.175
m-Spare/xxx.xxx.43.176/255.255.255.240/xxx.xxx.43.191
n-Spare/xxx.xxx.43.192/255.255.255.240/xxx.xxx.43.207
o-Spare/xxx.xxx.43.208/255.255.255.240/xxx.xxx.43.223
p-Spare/xxx.xxx.43.224/255.255.255.240/xxx.xxx.43.239
q-Spare/xxx.xxx.43.240/255.255.255.240/xxx.xxx.43.255

D3. Multi-cast group and class D address

D3.1. The following Class D address groups are promulgated for JWID 03.
(Read in 3 columns: group name/IP address/port number.)

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

a-MSEG (fast)/XXX.100.100.11/5011
b-MSEG (slow)/XXX.100.100.12/5012
c-AU MNTG NOC/XXX.100.100.21/5021
d-HMAS MANOORA/XXX.100.100.22/5022
e-HMAS ROBERTSON/XXX.100.100.23/5023
f-HMAS CANBERRA/XXX.100.100.24/5024
g-HMCS COATICOOK/XXX.100.100.25/5025
h-HMCS RENFREW/XXX.100.100.26/5026
j-NRS BRAS D'OR/XXX.100.100.27/5027
k-NRS RENFREW/XXX.100.100.28/5028
l-NZ TAC NOC/XXX.100.100.29/5029
m-HMNZS WAKA/XXX.100.100.30/5030
n-UK MNTG NOC/XXX.100.100.31/5031
o-HMS ALBION/XXX.100.100.32/5032
p-RFA ARGUS/XXX.100.100.33/5033
q-HMS OCEAN/XXX.100.100.34/5034
r-UK 40 Commando/XXX.100.100.35/5035
s-NRS SSCSD/XXX.100.100.36/5036
t-USS BATAAN/XXX.100.100.37/5037
u-USS PAUL HAMILTON/XXX.100.100.38/5038

D4. DNS Root Server(s)

D4.1.

a-./999999999/IN/NS/root1.
a.1-root1./999999999/IN/A/ xxx.xxx.48.20
b-./999999999/IN/NS/root2.
b.1-root2./999999999/IN/A/ xxx.xxx.248.10
c-./999999999/IN/NS/root3.
c.1-root3./999999999/IN/A/ xxx.xxx.8.10
d-./999999999/IN/NS/root4.
d.1-root4./999999999/IN/A/ xxx.xxx.8.20

D5. Domain responsibility

D5.1. Primary (Primary NOC/service.country/primary IP address/secondary IP address) (eg: MTWAN NOC/NAVY.US/A.B.C.D/A.B.C.D)

a-AUS NOC/navy.au/xxx.xxx.42.2/xxx.xxx.43.21
b-CA NOC/navy.ca/xxx.xxx.192.20/xxx.xxx.43.21
c-NZ NOC/navy.nz/xxx.xxx.43.133/xxx.xxx.43.21
d-UK NOC/navy.uk/xxx.xxx.ccc.ddd/aaa.bbb.ccc.ddd
e-US NOC/navy.us/xxx.xxx.43.21/xxx.xxx.192.20

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

f-US NOC/usmc.us/xxx.xxx.43.21/xxx.xxx.192.20

D6. Host names and IP addresses

Major host names follow (Read in 4 columns: Function/Hostname/IP Address/Netmask):

D6.1. AUSTRALIA

D6.1.1. HMAS Robertson

a-Gccs-m/goanna.robertson.navy.au/xxx.xxx.43.1/255.255.255.240
b-General Server/emu.robertson.navy.au/xxx.xxx.43.2/255.255.255.240
c-C2pc/possum.robertson.navy.au/xxx.xxx.43.4/255.255.255.240
d-Domino/wombat.robertson.navy.au/xxx.xxx.43.5/255.255.255.240
e-HF BLOS CAP/hfbloscap.robertson.navy.au/xxx.xxx.43.10/255.255.255.240
f-UHF SATCOM CAP/uhfcap.robertson.navy.au/xxx.xxx.43.11/255.255.255.240
g-Router/gateway.robertson.navy.au/xxx.xxx.43.13/255.255.255.240
h-Printer/gum.robertson.navy.au/xxx.xxx.43.14/255.255.255.240

D6.1.2. HMAS Manoora

a-Gccs-m/bream.manoora.navy.au/xxx.xxx.43.17/255.255.255.240
b-General Server/galah.manoora.navy.au/xxx.xxx.43.18/255.255.255.240
c-Domino/bogong.manoora.navy.au/xxx.xxx.43.20/255.255.255.240
d-HF BLOS CAP/hfbloscap.manoora.navy.au/xxx.xxx.43.26/255.255.255.240
e-UHF SATCOM CAP/uhfcap.manoora.navy.au/xxx.xxx.43.27/255.255.255.240
g-Router/gateway.manoora.navy.au/xxx.xxx.43.29/255.255.255.240

D6.1.3. HMAS Canberra

a-Gccs-m/goanna.canberra.navy.au/xxx.xxx.43.1/255.255.255.240
b-General Server/emu.canberra.navy.au/xxx.xxx.43.2/255.255.255.240
c-C2pc/possum.canberra.navy.au/xxx.xxx.43.4/255.255.255.240
d-Domino/wombat.canberra.navy.au/xxx.xxx.43.5/255.255.255.240
e-HF BLOS CAP/hfbloscap.canberra.navy.au/xxx.xxx.43.10/255.255.255.240
g-UHF SATCOM CAP/uhfcap.canberra.navy.au/xxx.xxx.43.11/255.255.255.240
h-Router/gateway.canberra.navy.au/xxx.xxx.43.13/255.255.255.240

D6.1.4. AUS NOC

a-Gccs-m/goanna.aunoc.navy.au/xxx.xxx.43.1/255.255.255.240
b-General Server/emu.aunoc.navy.au/xxx.xxx.43.2/255.255.255.240
c-C2pc/possum.aunoc.navy.au/xxx.xxx.43.4/255.255.255.240
d-Domino/wombat.aunoc.navy.au/xxx.xxx.43.5/255.255.255.240
e-HF BLOS CAP/hfbloscap.aunoc.navy.au/xxx.xxx.43.10/255.255.255.240
f-UHF SATCOM CAP/uhfcap.aunoc.navy.au/xxx.xxx.43.11/255.255.255.240
g-Router/gateway.aunoc.navy.au/xxx.xxx.43.13/255.255.255.240

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

D6.2. CANADA

D6.2.1. NRS Bras D'Or

a-Router/gateway.nrsbdo.navy.ca/xxx.xxx.248.1/255.255.255.0
b-Time server/time-serv.nrsbdo.navy.ca/xxx.xxx.248.2/255.255.255.0
c-General server/dns.nrsbdo.navy.ca/xxx.xxx.248.3/255.255.255.0
d-Mseg/mseg.nrsbdo.navy.ca/xxx.xxx.248.3/255.255.255.0
e-Domino/domino.nrsbdo.navy.ca/xxx.xxx.248.4/255.255.255.0
f-GCCS-M/gccsm.nrsbdo.navy.ca/xxx.xxx.248.5/255.255.255.0
g-Cisco Call Manager/ccm.nrsbdo.navy.ca/xxx.xxx.248.6/255.255.255.0
h-IP Phone/phone.nrsbdo.navy.ca/xxx.xxx.248.9/255.255.255.0
j-SNR/snr.nrsbdo.navy.ca/xxx.xxx.248.248

D6.2.2. HMCS Coaticook

a-Router/gateway.coa.navy.ca/xxx.xxx.248.1/255.255.255.0
b-Time server/time-serv.coa.navy.ca/xxx.xxx.248.2/255.255.255.0
c-General server/dns.coa.navy.ca/xxx.xxx.248.3/255.255.255.0
d-Mseg/mseg.coa.navy.ca/xxx.xxx.248.3/255.255.255.0
e-Domino/domino.coa.navy.ca/xxx.xxx.248.4/255.255.255.0
f-GCCS-M/gccsm.coa.navy.ca/xxx.xxx.248.5/255.255.255.0
g-IP Phone/phone.coa.navy.ca/xxx.xxx.248.9/255.255.255.0
h-SNR/snr.coa.navy.ca/xxx.xxx.248.248

D6.2.3. HMCS Renfrew

a-Router/gateway.ren.navy.ca/xxx.xxx.248.1/255.255.255.0
b-Time server/time-serv.ren.navy.ca/xxx.xxx.248.2/255.255.255.0
c-General server/dns.ren.navy.ca/xxx.xxx.248.3/255.255.255.0
d-Mseg/mseg.ren.navy.ca/xxx.xxx.248.3/255.255.255.0
e-Domino/domino.ren.navy.ca/xxx.xxx.248.4/255.255.255.0
f-GCCS-M/gccsm.ren.navy.ca/xxx.xxx.248.5/255.255.255.0
g-IP Phone/phone.ren.navy.ca/xxx.xxx.248.9/255.255.255.0
h-SNR/snr.ren.navy.ca/xxx.xxx.248.248

D6.3. NEW ZEALAND

D6.3.1. NZ NOC

a-Router/rout.nznoc.navy.nz/xxx.xxx.42.65/255.255.255.240
b-GCCS-M/gccs.nznoc.navy.nz/xxx.xxx.42.66/255.255.255.240
c-Domino Server/dom.nznoc.navy.nz/xxx.xxx.42.67/255.255.255.240

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

d-Sun Sparc/gen1.nznoc.navy.nz/xxx.xxx.42.69/255.255.255.240

D6.3.2. HMNZS Waka

a-Router/rout.waka.navy.nz/xxx.xxx.42.81/255.255.255.240

b-GCCS-M/gccs.waka.navy.nz/xxx.xxx.42.83/255.255.255.240

c-Domino Server/dom.waka.navy.nz/xxx.xxx.42.84/255.255.255.240

d-Sun Sparc/gen1.waka.navy.nz/xxx.xxx.42.86/255.255.255.240

e-Cap/cap.waka.navy.nz/xxx.xxx.42.88/255.255.255.240

f-Criu/criu.waka.navy.nz/xxx.xxx.42.89/255.255.255.240

D6.4. United Kingdom

D6.4.1. UK NOC

a-Router/rout.uknoc.navy.uk/xxx.xxx.42.81/255.255.255.240

b-GCCS-M/gccs.uknoc.navy.uk/xxx.xxx.42.83/255.255.255.240

c-Domino Server/dom.uknoc.navy.uk/xxx.xxx.42.84/255.255.255.240

d-Sun Sparc/gen1.uknoc.navy.uk/xxx.xxx.42.86/255.255.255.240

f-Cap/cap.uknoc.navy.uk/xxx.xxx.42.88/255.255.255.240

g-Criu/criu.uknoc.navy.uk/xxx.xxx.42.89/255.255.255.240

D6.4.2. HMS ALBION

a-Router/rout.alb.navy.uk/xxx.xxx.42.81/255.255.255.240

b-GCCS-M/gccs.alb.navy.uk/xxx.xxx.42.83/255.255.255.240

c-Domino Server/dom.alb.navy.uk/xxx.xxx.42.84/255.255.255.240

d-Sun Sparc/gen1.alb.navy.uk/xxx.xxx.42.86/255.255.255.240

f-Cap/cap.alb.navy.uk/xxx.xxx.42.88/255.255.255.240

g-Criu/criu.alb.navy.uk/xxx.xxx.42.89/255.255.255.240

D6.4.3. RFA ARGUS

a-Router/rout.arg.navy.uk/xxx.xxx.42.81/255.255.255.240

b-GCCS-M/gccs.arg.navy.uk/xxx.xxx.42.83/255.255.255.240

c-Domino Server/dom.arg.navy.uk/xxx.xxx.42.84/255.255.255.240

d-Sun Sparc/gen1.arg.navy.uk/xxx.xxx.42.86/255.255.255.240

f-Cap/cap.arg.navy.uk/xxx.xxx.42.88/255.255.255.240

g-Criu/criu.arg.navy.uk/xxx.xxx.42.89/255.255.255.240

D6.4.4. HMS OCEAN

a-Router/rout.oce.navy.uk/xxx.xxx.42.81/255.255.255.240

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

b-GCCS-M/gccs.oce.navy.uk/xxx.xxx.42.83/255.255.255.240
c-Domino Server/dom.oce.navy.uk/xxx.xxx.42.84/255.255.255.240
d-Sun Sparc/gen1.oce.navy.uk/xxx.xxx.42.86/255.255.255.240
f-Cap/cap.oce.navy.uk/xxx.xxx.42.88/255.255.255.240
g-Criu/criu.oce.navy.uk/xxx.xxx.42.89/255.255.255.240

D6.4.5.UK 40 CDO

a-Router/rout.uk40cdo.navy.uk/xxx.xxx.42.81/255.255.255.240
b-GCCS-M/gccs.uk40cdo.navy.uk/xxx.xxx.42.83/255.255.255.240
c-Domino Server/dom.uk40cdo.navy.uk/xxx.xxx.42.84/255.255.255.240
d-Sun Sparc/gen1.uk40cdo.navy.uk/xxx.xxx.42.86/255.255.255.240
f-Cap/cap.uk40cdo.navy.uk/xxx.xxx.42.88/255.255.255.240
g-Criu/criu.uk40cdo.navy.uk/xxx.xxx.42.89/255.255.255.240

D6.5. United States

D6.5.1. NRS San Diego

a-router/rout.nrssd.navy.us/xxx.xxx.43.17/255.255.255.240
b-Whatsup/whatsup.nrssd.navy.us/xxx.xxx.43.19/255.255.255.240
c-JMUG/jmug.nrssd.navy.us/xxx.xxx.43.21/255.255.255.240
d-DNS/jmug.nrssd.navy.us/xxx.xxx.43.21/255.255.255.240
e-PMUL/pmul.nrssd.navy.us/xxx.xxx.43.22/255.255.255.240
f-Domino/domino.nrssd.navy.us/xxx.xxx.43.24/255.255.255.240
g-Sametime/sametime.nrssd.navy.us/xxx.xxx.43.25/255.255.255.240
h-Taclane/taclane.nrssd.navy.us/xxx.xxx.43.27/255.255.255.240
j-UHF-CAP1/uhf-cap1.nrssd.navy.us/xxx.xxx.43.29/255.255.255.240
k-CRIU/uhf-criu.nrssd.navy.us/xxx.xxx.43.30/255.255.255.240

D6.5.2. USS Bataan

a-Router/rout.bat.navy.us/xxx.xxx.43.49/255.255.255.240
b-Whatsup/whatsup.bat.navy.us/xxx.xxx.43.50/255.255.255.240
c-JMUG/jmug.bat.navy.us/xxx.xxx.43.52/255.255.255.240
d-DNS/jmug.bat.navy.us/xxx.xxx.43.52/255.255.255.240
e-Intel/intel.bat.navy.us/xxx.xxx.43.54/255.255.255.240
f-Ops/ops.bat.navy.us/xxx.xxx.43.55/255.255.255.240
g-GCCS-M/gccsm.bat.navy.us/xxx.xxx.43.56/255.255.255.240
h-Domino/domino.bat.navy.us/xxx.xxx.43.57/255.255.255.240
j-Taclane/taclane.bat.navy.us/xxx.xxx.43.60/255.255.255.240
k-bridge1/bridge1.bat.navy.us/xxx.xxx.43.61/255.255.255.240
l-bridge2/bridge2.bat.navy.us/xxx.xxx.43.62/255.255.255.240

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

D6.5.3. USS Paul Hamilton

a-Router/rout.pha.navy.us/xxx.xxx.43.49/255.255.255.240
b-Whatsup/whatsup.pha.navy.us/xxx.xxx.43.50/255.255.255.240
c-JMUG/jmug.pha.navy.us/xxx.xxx.43.52/255.255.255.240
d-DNS/jmug.pha.navy.us/xxx.xxx.43.52/255.255.255.240
e-Intel/intel.pha.navy.us/xxx.xxx.43.54/255.255.255.240
f-Ops/ops.pha.navy.us/xxx.xxx.43.55/255.255.255.240
g-GCCS-M/gccsm.pha.navy.us/xxx.xxx.43.56/255.255.255.240
h-Domino/domino.pha.navy.us/xxx.xxx.43.57/255.255.255.240
j-Taclane/taclane.pha.navy.us/xxx.xxx.43.60/255.255.255.240
k-bridge1/bridge1.pha.navy.us/xxx.xxx.43.61/255.255.255.240
l-bridge2/bridge2.pha.navy.us/xxx.xxx.43.62/255.255.255.240

D6.5.4. US Marine Corps

a-Router/gateway.31meu.usmc.us/xxx.xxx.43.129/255.255.255.224
b-Domino/domino.31meu.usmc.us/xxx.xxx.43.130/255.255.255.224
c-MIDB/ias.31meu.usmc.us/xxx.xxx.43.131/255.255.255.224
d-Printer/printer.31meu.usmc.us/xxx.xxx.43.132/255.255.255.224
e-C2PC/nt1mntg.31meu.usmc.us/xxx.xxx.43.133/255.255.255.224
f-C2PC/nt2mntg.31meu.usmc.us/xxx.xxx.43.134/255.255.255.224
g-GCCS/mntgcop.31meu.usmc.us/xxx.xxx.43.135/255.255.255.224
h-C2PC/nt3mntg.31meu.usmc.us/xxx.xxx.43.136/255.255.255.224
j-C2PC/nt4mntg.31meu.usmc.us/xxx.xxx.43.137/255.255.255.224
k-C2PC/nt5mntg.31meu.usmc.us/xxx.xxx.43.138/255.255.255.224
l-C2PC/nt6mntg.31meu.usmc.us/xxx.xxx.43.139/255.255.255.224

E. ROUTING

E1. AS number

Following Autonomous System area number are promulgated. (Read in 3 columns: country/network/AS number.)

a-Australia/MNTG/1011
b-Canada/MNTG/1012
c-New Zealand/MNTG/1013
d-United Kingdom/MNTG/1014
e-United States/MNTG/1015

E2. Bandwidth

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

- E2.1. SHF
 - a-128 kbps
- E2.2. INMARSAT B
 - a-128 kbps dual
 - b-64 kbps
- E2.3. UHF SATCOM
 - a-6 kbps/32 kbps 5 members net
 - b-4.8 kbps/ 16 kbps 3 members net
- E2.4. HF BLOS
 - a-19.2 kbps 110b coded waveform
 - b-9.6 kbps 110b coded waveform
 - c-2.4 kbps 4285 coded waveform
- E2.5. SNR UHF LOS
 - a-41 kbps at 78.6 kbps single net with 6 members
 - b-34 kbps at 78.6 kbps in-line topology with 4 relays
 - c-20 kbps at 78.6 kbps 2 nets with 1 relay
- E3. **OSPF settings** (bw in kbps/area/dead time/hello interval/retransmit/cost)
 - E3.1. SHF
 - a-128/0/40/10/5/800
 - E3.2. INMARSAT
 - a-128/0/40/10/5/750
 - b-64/0/40/10/5/750
 - E3.3. UHF SATCOM
 - E3.1 5Khz Channel
 - a-2.4/0/120/30/10/3400
 - b-4.8/0/120/30/10/2660
 - c-9.6/0/120/30/10/2220

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

E.3.2 25Khz Channel

- a-16/0/120/30/10/1500
- b-32/0/120/30/10/1300
- c-38.4/0/120/30/10/1250
- d-48/0/120/30/10/1200
- e-56/0/120/30/10/1150

E3.4. HF BLOS

- a-19.2/0/120/30/10/1500
- b-9.6/0/120/30/10/1900
- c-2.4/0/120/30/10/3200

E3.5. SNR UHF LOS

- a-78.6/0/40/10/5/1125
- b-64/0/40/10/5/1150
- c-32/0/40/10/5/1300

E4. **PIM settings** (mode/ R/V point/priority)

E4.1. AU NOC

a-sparse-dense/xxx.xxx.421/50

E4.2. CA NOC

a-sparse-dense/xxx.xxx.192.1/100

E4.3. NZ NOC

a-sparse-dense/xxx.xxx.42.129/50

E4.4. UK NOC

a-sparse-dense/xxx.xxx.ccc.ddd/50

E4.5. US NOC

a-sparse-dense/xxx.xxx.43.1/100

F. **SUBNETS**

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

F1. UHF SATCOM

- F1.1 Router Interface IP
- F1.2 IP address/Mask (A.B.C.D/Hex)
- F1.3 Baud rate
- F1.4 Guard time
- F1.5 Time Bytes
- F1.6 Unique crypto settings

F2. INMARSAT B

- F2.1 Unit/number
- F2.2 IP address/Mask
- F2.3 Baud rate
- F2.4 Unique crypto settings

F3. HF BLOS

- F3.1 CAP ID (unit/unique ID number)
- F3.2 IP address/Mask (A.B.C.D/Hex)
- F3.3 Modem mode
- F3.4 Baud rate
- F3.5 Interleave mode
- F3.6 Transmit frequencies (ship freq/shore freq)
- F3.7 Eval interval
- F3.8 Unique crypto settings

F4. IP 5066

- F4.1 Unit ID (unit/unique ID number)
- F4.2 IP address/Mask (A.B.C.D/Hex)
- F4.3 Modem mode
- F4.4 Baud rate
- F4.5 Interleave mode
- F4.6 Transmit frequencies
- F4.7 Unique crypto settings

G. NETWORK MANAGEMENT

G1. Unit NM reporting requirements

Report network status via local web services. NOC to provide URL.

G2. Help Desk Policy

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 12 to ACP 200

The NOC will maintain a 24/7 help desk to address network issues

G3. NOC telephone numbers.

To be promulgated separately.

H. APPLICATIONS

H1. Messaging

- H1.1 MSE version nr
- H1.2 Sendmail version nr
- H1.3 Mx record
- H1.4 Mailer table
- H1.5 Multicast IP address
- H1.6 Outbound configuration file
- H1.7 P_Mul configuration
- H1.8 Sendmail.cf configuration

H2. Common Operational Picture (COP)

- H2.1 MSEG version nr
- H2.2 Multicast address
- H2.3 Congestion control
- H2.4 MSEG configuration

H3. Web Services

- H3.1 Domino version nr
- H3.2 Primary DOMINO server IP address
- H3.3 DOMINO name structure
- H3.4 Web browser version nr.

H4. DCP

- H4.1 SAMETIME version nr
- H4.2 SAMETIME server IP address

H5. MSEG

- H5.1 Version Nr
- H5.2 Multicast address

H6. ICE

- H6.1 Version nr

Chapter 13

TRANSPORT SERVICES

1301 INTRODUCTION

In order to meet the overall intention to provide a network, which uses minimum bandwidth to achieve network interoperability, a MTWAN is designed to utilize multicast network features in all areas possible. As part of this strategy the network and applications are being driven to employ User Datagram Protocol (UDP) IP services vice Transport Control Protocol (TCP) IP services.

1302 AIM

This chapter describes the strategy and tools used to enable reliable multicast IP packet networking.

1303 OVERVIEW

IP networks use two main transport protocols for IP packet transport:

- a. **TCP.** This is a connection-oriented protocol, which has control mechanisms built into each packet that provides numerous functions, primarily designed to achieve robust and reliable data transfer. This however, provides a significant overhead that is appended to any packet of user data. Also, in order for these control mechanisms to operate, TCP uses a 4-way session protocol to setup a link, confirm receipt, request next packet and tear down a link. Again this adds significant data overhead to the transport of user data.
- b. **UDP.** This is a connectionless protocol, which uses no control mechanisms beyond the inclusion of a source and destination address and a sequence number for each packet of user data sent. The purpose of the sequence number is to allow the application at the source to reorder the packets and to request retransmission of missed packets. The lack of control mechanisms makes this protocol inherently unreliable, however the overhead per packet is significantly lower thus making it a more efficient protocol to use in low bandwidth networks.

1304 REQUIREMENT

- a. To achieve maximum efficiency of a multimember MTWAN network multicast routing protocols are to be used as much as possible as should

UDP transport protocols. The two systems are complimentary and together significantly improve the efficiency of information services on a MTWAN network.

- b. The requirement is to provide mechanisms for the reliable data transfer of UDP based application information within this environment. By using reliable transport protocols UDP based application data can be preferably used to enhance the overall efficiency of use of the available bandwidth on all subnets of a MTWAN.

1305 RELIABLE TRANSPORT TOOLS

- a. Multicast Service Gateway (MSeG) used in a MTWAN is a reliable transport service for UDP packet transfer. The MSeG's engine is based upon a reliable transport protocol developed by Navy Research Labs called Multicast Dissemination Protocol. The MSeG has the ability to intercept the TCP traffic generated from a GCCS-M machine, convert it to UDP and relay this on as a multicast to a number of Multicast address groups. The tool also has the ability to relay smtp email packets as UDP again to a number of multicast address groups.
- b. Finally the MSeG embodies two native applications:
 - (1) MCHAT – This is a multicast Chat tool primarily used as an engineering order wire or Task Group Order wire.
 - (2) MFTP – This is a multicast FTP tool to efficiently transfer large files to numerous members of the MTWAN.
- c. One other important feature of the MSeG tool is that it is capable of delivering the UDP packets from the four applications GCCS-M, MCHAT, MFTP and smtp e-mail when the receiving station is in EMCON silence. This capability can only be achieved with UDP packets. The mechanism used to achieve the delivery is a broadcast of the packets. The system simply broadcasts the packets a number of times within a given timeframe so as to attempt to ensure all members of the multicast group get full delivery of the required information.
- d. At this time the EMCON feature requires manual intervention by administrators when exiting EMCON silence to ensure data was effectively transferred while silent. The tool is being enhanced to allow for some storing of ACKs and NACKs and to then sequentially coordinate these with the source upon exiting EMCON silence.

MULTICAST SERVICE GATEWAY (MSeG)

13A01 INTRODUCTION

- a. The MSeG is to provide a multicast IP capability in a network comprising links of low bandwidth and high latency whilst not having to change the originating applications code.
- b. Applications like GCCS-M have been developed to send data using unicast protocols such as TCP or UDP. For instance, a GCCS-M terminal sends data to another GCCS-M terminal via a TCP connection. To broadcast data to “n” x GCCS-M terminals, the sending GCCS-M will open “n” number of TCP connections to send the same data to “n” number of receiving GCCS-M. Before IP multicast was available, this was the only option to broadcast data for most applications.

13A02 AIM

The aim of this Annex is to provide a functional overview of Multicast Service Gateway (MSeG) and its application.

13A03 OVERVIEW

- a. The modifications of existing applications to send data using IP multicast can require significant resources and effort. In some cases, it is impossible to access the source codes for modification. A much simpler approach is to develop software such as MSeG to provide multicast capability to existing unicast applications without having to modify the source codes. Instead of sending data direct from one GCCS-M terminal to many other GCCS-M terminals using unicast traffic, the sending GCCS-M terminal sends data to a MSeG which sends the data to other MSeGs using multicast Class D IP addresses. When a MSeG receives data, it will forward data to the local GCCS-M terminal. Therefore, GCCS-M data is being broadcast in the most efficient way. Multicast IP addresses are used for transmission.
- b. For reliable data transfer between MSeGs, a reliable multicast transport protocol called Multicast Dissemination Protocol (MDP) is utilised. MDP has features useful in a military network such as Dynamic Congestion and Flow Control, TCP Friendly, EMCON support, and Forward Error Correction. More information on MDP can be found at <http://manimac.itd.navy.mil>

- c. In general, MSeG receives unicast data from an application and relays the data to other MSeGs using multicast Class D IP address. All MSeGs are transparent to the application. The MSeGs are configured to run as both server and client from the application point of view. To use the services of the MSeG, the application needs to be configured to send data to the MSeG.

13A04 SUPPORTED APPLICATIONS

- a. MSeG supports the following applications; GCCS-M, Email, Multicast File Transfer, and Multicast Chat.
 - (1) **GCCS-M.** In general, MSeG receives GCCS-M data over the TCP/IP socket. The data is then sent via MDP to other MSeGs. When a MSeG receives data from another MSeG over MDP protocol, it sends the data back to GCCS-M terminal over TCP/IP the socket. The TCP/IP socket port number is 2020. This port number is a unique port number used by all GCCS-M terminals.
 - (2) All MSeGs are transparent to the GCCS-M terminals. From the GCCS-M terminal point of view, a MSeG is like another GCCS-M terminal. When a MSeG is initialized, it creates a TCP server on port 2020. Before GCCS-M sends data, it opens a TCP connection on this port. After data is sent, the connection is closed. GCCS-M opens a connection for each message that is sent. When MSeG detects the connection is closed by the GCCS-M , it re-arms and waits for a new connection from the GCCS-M terminal.
 - (3) Each GCCS-M message is saved in file format and copied into the transmit directory of MDP. Periodically, MDP will scan the directory and pick up the files to send to other MDPs. When a MDP receives the message completely, it will save the message as a file and copy it to the Received Directory.
 - (4) After opening the file in the received directory, MSeG opens a TCP connection to the local GCCS-M to send the data. Once the data is sent over the TCP connection, MSeG closes the connection and scans the directory until another file arrives.

UNCLASSIFIED

Annex A to Chapter 13 of ACP 200

- (5) Each MSeG can service up to 4 GCCS-M terminals. Four GCCS-M terminals can send to, and receive from, MSeG simultaneously for multicast services. This feature is useful for GCCS-M terminals that are located in places where IP multicast is not supported at the network layer.
- (6) **E-MAIL.** MSeG supports a Unix email version of Solaris Operating System called "sendmail". MSeG is installed and run in the same Solaris host of an E-mail system or a Mail Transfer Agent (MTA). Standard SMTP email uses TCP protocol. In instances when a single message is being delivered to several recipients that are served by different MTAs, standard email must establish a connection and transfer the message to each of the destination MTAs sequentially. This is inefficient as the same message must be transmitted several times, once for each destination MTA, consuming additional bandwidth.
- (7) To enable the use of MSeG, sendmail is reconfigured to send messages to the MSeG processor for multicast transfer.
- (8) MSeG joins a multicast group, sends and receives multicast data on behalf of the MTA. MSeG can be configured to operate in two different modes: 'static group' and 'dynamic group' membership mode.
- (9) In static group membership mode, all MTAs are members of a multicast address. The email message is sent to all MTAs. The email message will be discarded at the receiving MTAs whose names are not on the recipient list.
- (10) In dynamic group membership mode, a MTA will join a multicast group dynamically based on the address list of a message. It works as follows. At the transmitting MTA, the MSeG examines the addressee lists of the message. The MSeG will send the list and a multicast address to all MTAs. Any MTA that has its name on the addressee list will join the provided multicast address. Once the email message is received, the receiving MTA will leave the multicast group. In this mode, the MSeG delivers the email message more efficiently than the static membership mode because there is no BW wasted on non-intended MTAs.

- (11) **MULTICAST FILE TRANSFER PROTOCOL(Mftp).**
Another application of the MSeG is Mftp. Mftp allows a user to reliably transfer a file from one host to others. Similar to File Transfer Protocol (ftp), a user selects the source file to send with the option to change the destination file name. When a file is received, the MSeG will generate an alert message to indicate that the file is ready for moving or copying to another directory.
- (12) **MCHAT.** The Multicast Chat Tool is designed to be a lightweight, simple to use application of MSeG for collaborative multicast chat. Each Mchat user can send and receive simple text messages from all other Mchat users. Each message is sent using multicast transport protocol MDP for reliable service.

13A05 EXAMPLE CONFIGURATIONS

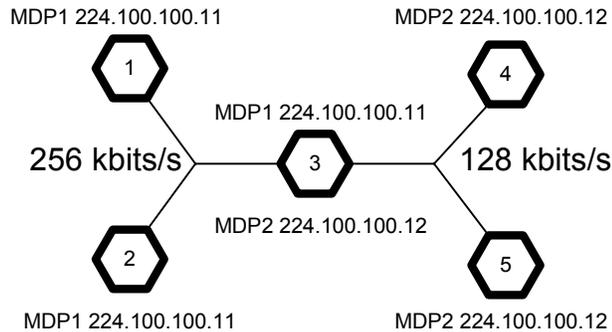
Example 1: This example demonstrates how an MSeG can be configured to run 2 MDP instances. If only one MDP instance is used in this network, the maximum sending rate at each node will be 128 kbps.

In this 5 node network, MSeG at node 1,2 are configured to run one MDP1 instance for 224.100.100.11. The MSeGs at node 4 and 5 are configured to run one MDP2 instance for 224.100.100.12. However at node 3, the MSeG is configured to run 2 MDP instances. One is MDP1 for 224.100.100.11 and the other is MDP2 for 224.100.100.12.

MDP1 is configured to send at a maximum rate of 256 kbps. MDP2 is configured to send at a maximum rate of 128 kbps.

Observation:

- MSeG at node 3 relays data from MDP1 @ 256 kbps to MDP2 @ 128 kbps and vice versa.
- MSeG 1 and 2 send and receive data @ 256 kbps or less depending on how much BW is being used by other TCP/UDP traffic.
- MSeG 3 and 4 send and receive data @ 128 kbps or less.

**Example 2:**

Three more nodes were added to network in example 1.

MSeGs at nodes 1,3,4 and 5 are configured the same as in example 1.

MSeG at node 2 is configured to run 2 MDP instances. One is MDP1 for 224.100.100.11 and one is MDP3 for 224.100.100.13.

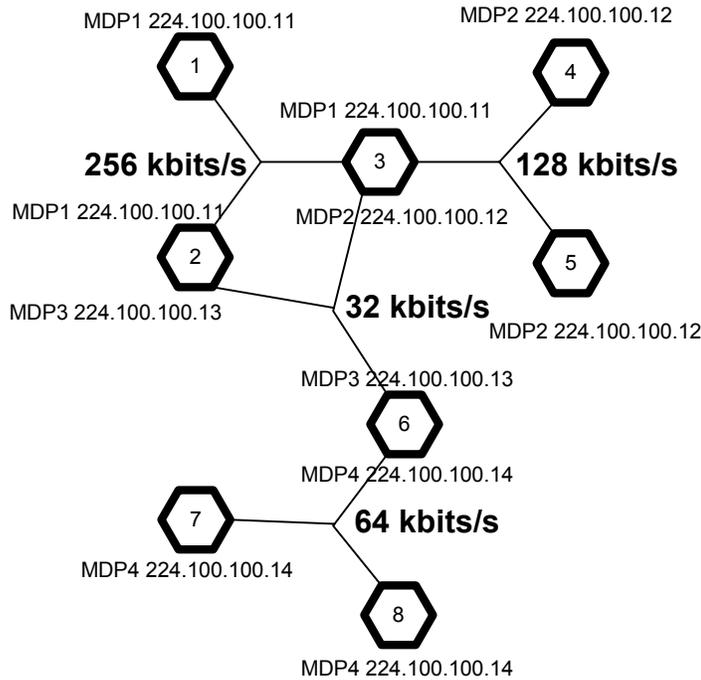
MSeGs at node 7 and 8 are configured to MDP4 for 224.100.100.14.

MSeG at node 6 is configured to run 2 MDP instances. One is MDP3 for 224.100.100.13 and one is MDP4 for 224.100.100.14.

MDP3 is configured to send at a maximum rate of 32 kbps, and MDP4 is configured to send at a maximum rate of 64 kbps.

Observations:

- MSeG at node 2 relays data from MDP1 @ 256 kbps and to MDP3 @ 32 kbps and vice versa.
- MSeG at node 6 relays data from MDP3 @ 32 kbps and to MDP4 @ 64 kbps and vice versa.
- MSeG 7 and 8 send and receive data @ 64 kbps or less depending on how much BW is being used by other TCP/UDP traffic.



Example 3: This example demonstrates when MSeG can be used to service more than one GCCS-M terminals.

Two more nodes 9 and 10 are added to the network in example 2. These nodes are connected to node 8 via P-t-P links at 2.4 kbps and 9.6 kbps.

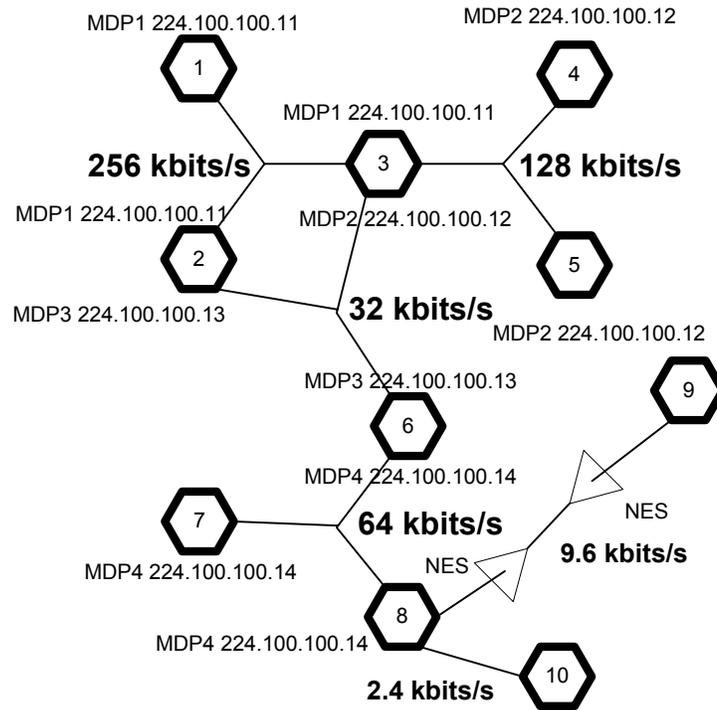
MSeGs at node 1,2,3,4,5,6,7 and 8 are configured the same as in example 2.

Node 8 and 9 are connected via a pair of NES devices. These NES devices do not support multicast. Therefore, MSeG at node 8 is configured to service 3 GCCS-M terminals: MSeG terminals at nodes 8,9, and 10.

Observations:

- Since MSeG at node 8 is configured to service 3 GCCS-M terminals, two SPARC stations to run MSeGs at node 9 and 10 are not needed.

While MSeG at node 8 sends and receives data from the GCCS-M terminal at node 10 @ 2.4 kbps, the remainder of the system is sending data at much higher rate.

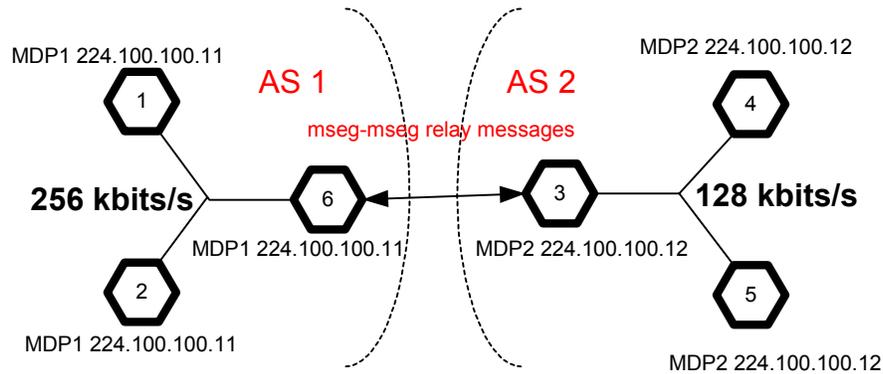


Example 4: This example demonstrates how MSeGs can be configured and used to relay data from one MSeG to another to support Multicast across two different Autonomous Systems (AS). The messages are relayed between two ‘border’ MSeGs using TCP.

MSeGs at nodes 1,2 and 6 are in AS 1 and configured to run MDP1. In addition MSeG 6 is configured to relay data between MDP 1 and MSeG 3 in AS 2. MSeGs at nodes 3,4 and 5 are in AS 2 and configured to run MDP2. In addition MSeG 3 is configured to relay data between MDP 2 and MSeG 6 in AS 1.

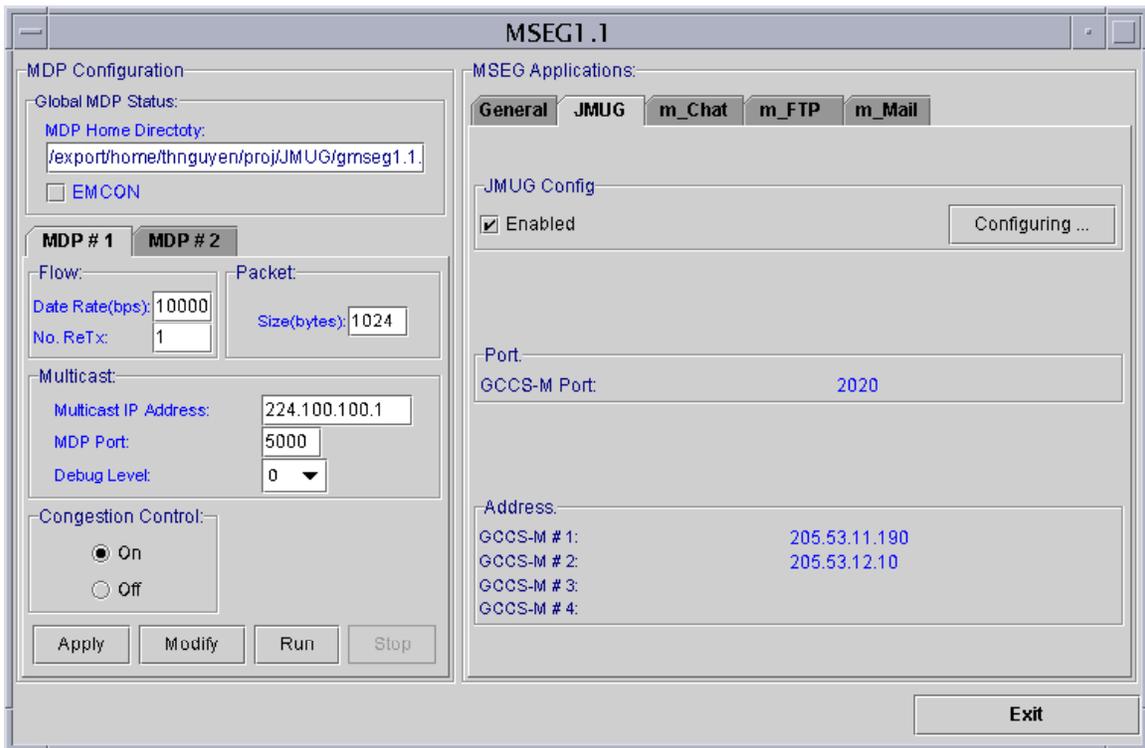
Observations:

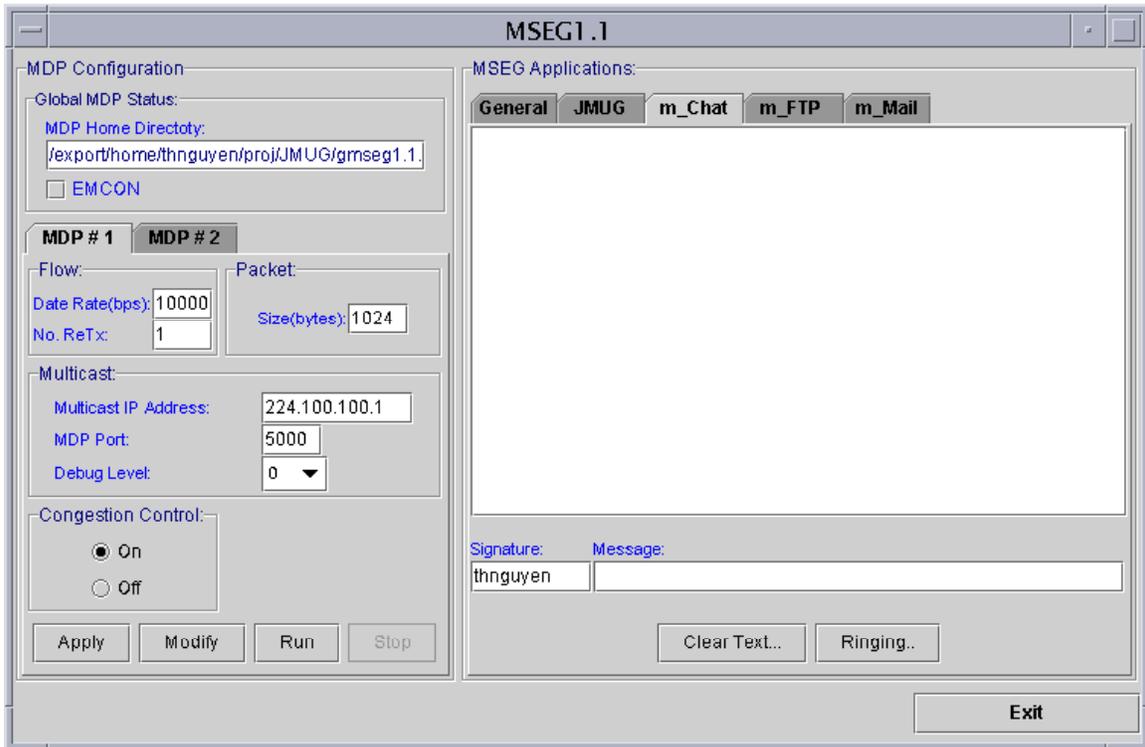
- All MSeGs in both ASs receive the same multicast traffic.
- MSeG 6 relays TCP data from MSeG 3 of AS2 to MDP1 for MSeG 1 and 2.
- MSeG 3 relays TCP data from MSeG 6 of AS1 to MDP2 for MSeG 4 and 5.

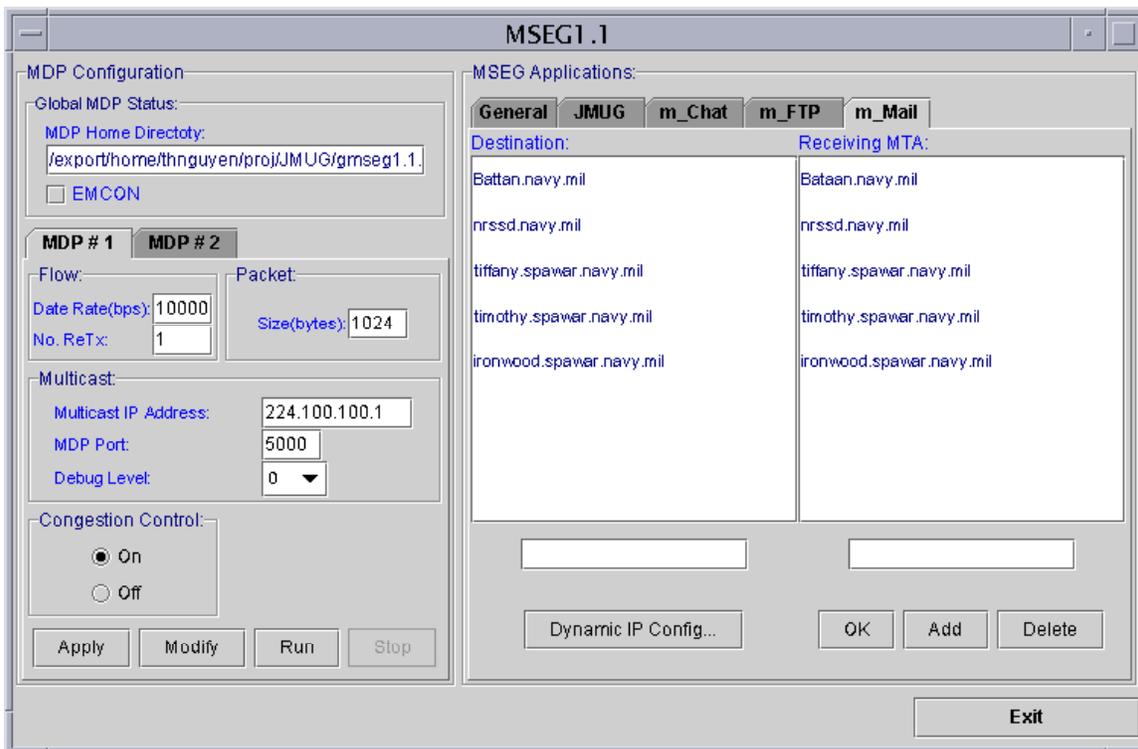


13A06 GRAPHICAL USER INTERFACE (GUI)

The following pictures are snap shots of the MSeG's GUI for each supported application







Chapter 14

NETWORK NAMING AND ADDRESSING

1401 INTRODUCTION

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.

1402 AIM

The aim of this chapter is to firstly define how names and addresses for entities in a MTWAN should be allocated and managed, and secondly how DNS should be configured and linked to national name services.

1403 OVERVIEW

- a. One of the major activities in establishing a MTWAN is to identify and promulgate the names and addresses of network elements, including attached end systems and workstations. 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.
- b. The domain name service (DNS) has to be linked in to DNSs in national and coalition networks in order to provide address information relating to entities outside the MTWAN, and to publish similar information on MTWAN entities in these external networks.

NAMING AND ADDRESSING SOP

14A01 INTRODUCTION

Host and Domain naming has a direct bearing on IP addressing. In turn, because IP addressing underlies the configuration of both node hardware and software applications, a small amount of time spent developing a realistic IP address pre-assignment scheme pays significant dividends¹. The standard operating procedures for assignment of IP addressing used in the MTWAN is addressed within this document.

14A02 AIM

This SOP details the standard convention to be used for the naming of hosts and domains utilised in the MTWAN networking environment, and the procedure to be followed when assigning IP addresses associated with host and domain names.

14A03 HOST NAMING CONVENTION

- a. 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:

- (1) **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. GCCS-M, Email, DCP) taken from the mandatory list at Table 14-A-1.

Use Abbreviation	Use	Remarks
gccsm	GCCS-M or similar COP	
uhf	particular use of a CAP VME card	see Type
cvat	Vulnerability assessment workstation	
time	LAN time generator	
mail	Email or messaging	generally a server

- 1 The use of IP sub-netting is also highly recommended, when there is routing protocol support for this. In an environment of OSPF and BGP-4, the use of sub-netting can significantly reduce the number of IP addresses that are required.

UNCLASSIFIED

Annex A to Chapter 14 to ACP 200

dns	Domain Name Service	generally a server
web	world wide web	generally a server
gbs	Global Broadcast System	generally a server
dcp	Distributed Collaborative Planning workstation	
gen	general workstation	e.g. MS Office
		Spare
		Spare
		Spare

Table 14-A-1: Abbreviations for ‘Use’

(2) **Type** — an abbreviation with a maximum of four letters to indicate the type of equipment taken from the mandatory list at Table 14-A-2.

Type Abbreviation	Type	Remarks
cap	Channel Access Processor (CAP)	Equivalent to SNAC
card	VME Card	
criu	CAP to Router Interface Unit (CRIU)	Equivalent to SRIU
pntr	Printer	
rout	Router	
serv	Server	
snac	Subnet Access Controller (SNAC)	Equivalent to CAP
sriu	SNAC to Router Interface Unit (SRIU)	Equivalent to CRIU
wkst	Workstation	PC, X-terminal etc
		Spare
		Spare
		Spare

Table 14-A-2: Abbreviations for ‘Type’

(3) **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 otherwise have the same name (e.g. pntr-a and pntr-b or pntr-4m and pntr-

UNCLASSIFIED

Annex A to Chapter 14 to ACP 200

colr if greater delineation is required).

- b. 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.
- c. Note that host names can not begin with a number (ie. the 'use' field of the host name may not start with a number).
- d. Tables 12-A-1 and 12-A-2 can be amended for specific events (e.g. operations, exercises, demonstrations, trials). However, such amendments will only apply to that event.
- e. From the above mandatory values for Use and Type some example host names could be generated as follows:

mail-serv
uhf-cap
gccsm-serv
hf-criu
gbs-rout
dcp-wkst-a
dcp-wkst-b
cvat-wkst

14A04 DOMAIN NAMING CONVENTION

- a. Used to generate the names for domains within which the hosts will operate, the domain naming convention will comprise:
 - (1) **Unit** — representing the name of the node or site;
 - (2) **Service** — selected from: navy, army, air, marines, joint; and
 - (3) **Country** — the two-letter country code as used on the Internet.
- b. For naval units, the above convention translates to "shipname.navy.country". For

UNCLASSIFIED

Annex A to Chapter 14 to ACP 200

example, the USS BATAAN will have the DNS domain "bataan.navy.us". For the US marines this convention translated to "unit.marines.us", i.e., "us2mef.marines.us". The UK Marines utilised the "navy" domain, i.e., "uk3cdobde.navy.uk" and "uk40cdo.navy.uk".

- c. 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.
- d. Although there are no DNS imposed restrictions on the length of the “Unit” component, for reasons of usability the length for MTWAN purposes shall be constrained to 15 characters. Further it 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 another ottawa.navy.ca.
- e. As with host names, the domain name can not begin with a number (ie the ‘unit’ field may not start with a number); therefore units like 3 CDO BDE will have to have a prefix (see examples).

(1) Examples:

canterbury.navy.nz
p3korion.air.nz
lcomd.army.nz
pnoc.navy.us
ottawa.navy.ca
us2mef.marines.us
uk3cdobde.marines.uk

(2) Finally some complete name examples:

mail-serv.canterbury.navy.nz
dcp-wkst-b.p3korion.af.nz
rout.lcomd.army.nz
gbs-rout.pnoc.navy.us
criu-card.ottawa.navy.ca
gccsm-serv.us2mef.marines.us
dcp-wkst-a.uk3cdobde.marines.uk

14A05 IP SUBNETTING AND MULTICAST ADDRESSING

- a. Internet Protocol (IP) addressing consists of a series of four byte addresses separated by dots. 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.

- b. **Class D Multicast Addressing.** 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.
- c. The Primary NOC is responsible for the allocation of Class D addresses within the MTWAN. It will need to co-ordinate with the network control centre of any attached WAN (such as a CWAN) to ensure that the addresses are unique.
- d. **Unicast Class C IP Subnetting.** 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.
- e. 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.

- f. **Multicast Subnetting.** 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.

14A06 IP ADDRESSING CONVENTION

- a. 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.
- b. 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.
- c. 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.
 - c. 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.

14A07 IP ADDRESS AUTHORITY TASKS

- a. 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.
- b. 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 are part of the same subnet.

14A08 UNIT ASSIGNMENT OF HOSTS

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

IP ADDRESSING

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 all the 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>

IP addresses are divided into a number of categories called classes. These classes are summarised at Table 14-A1-1 and represented in Figure 14-A1-1.

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 14-A1-1 – IP Address Classes

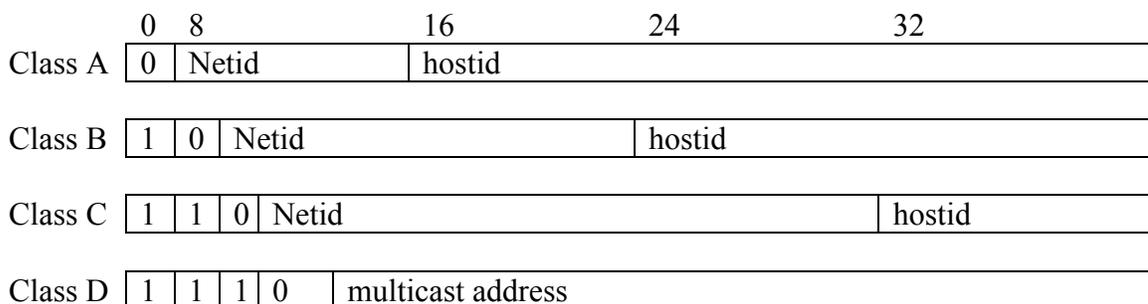


Figure 14-A1-1 – IP Address

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 added 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

UNCLASSIFIED

Appendix 1 to Annex A to Chapter 14 to ACP 200

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.

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).

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.

DOMAIN NAME SERVICE SOP

14B01 INTRODUCTION

- a. 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.
- b. 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.

14B02 AIM

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

14B03 OVERVIEW

- a. The DNS hierarchical structure adopted to support multi-national operations is shown in Figure 14-B-1. The naming scheme selected for the MTWAN is unit.service.country. For naval units the convention translates to shipname.navy.country. For details on the naming scheme, refer to the SOP for Network Naming and Addressing.

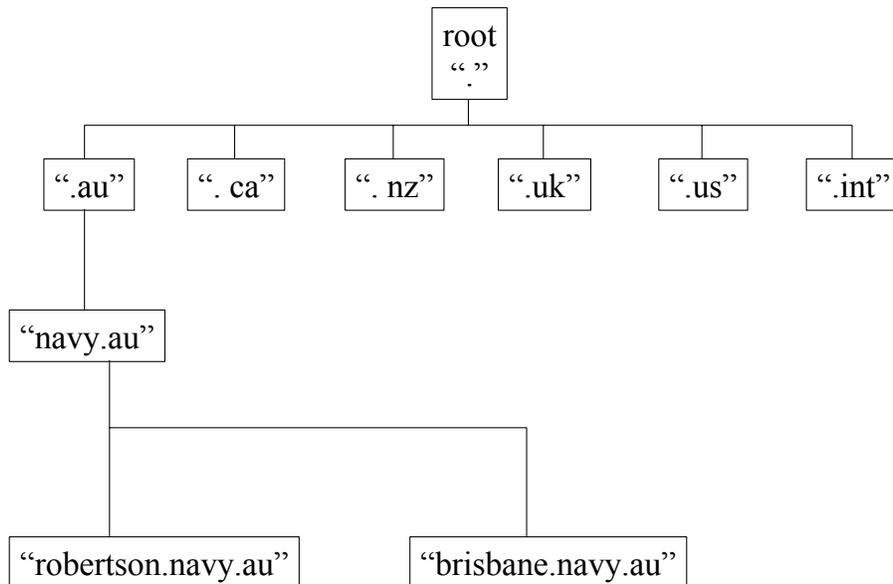


Figure 14-B-1: - Domain Name Schema

UNCLASSIFIED

Annex B to Chapter 14 to ACP 200

- b. 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.

14B04 DNS SERVERS

- a. 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.
- b. Multiple domains can be supported by a single server.
- c. More than one server should be set up for each domain for robustness.
- d. 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.
- e. 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 14-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.

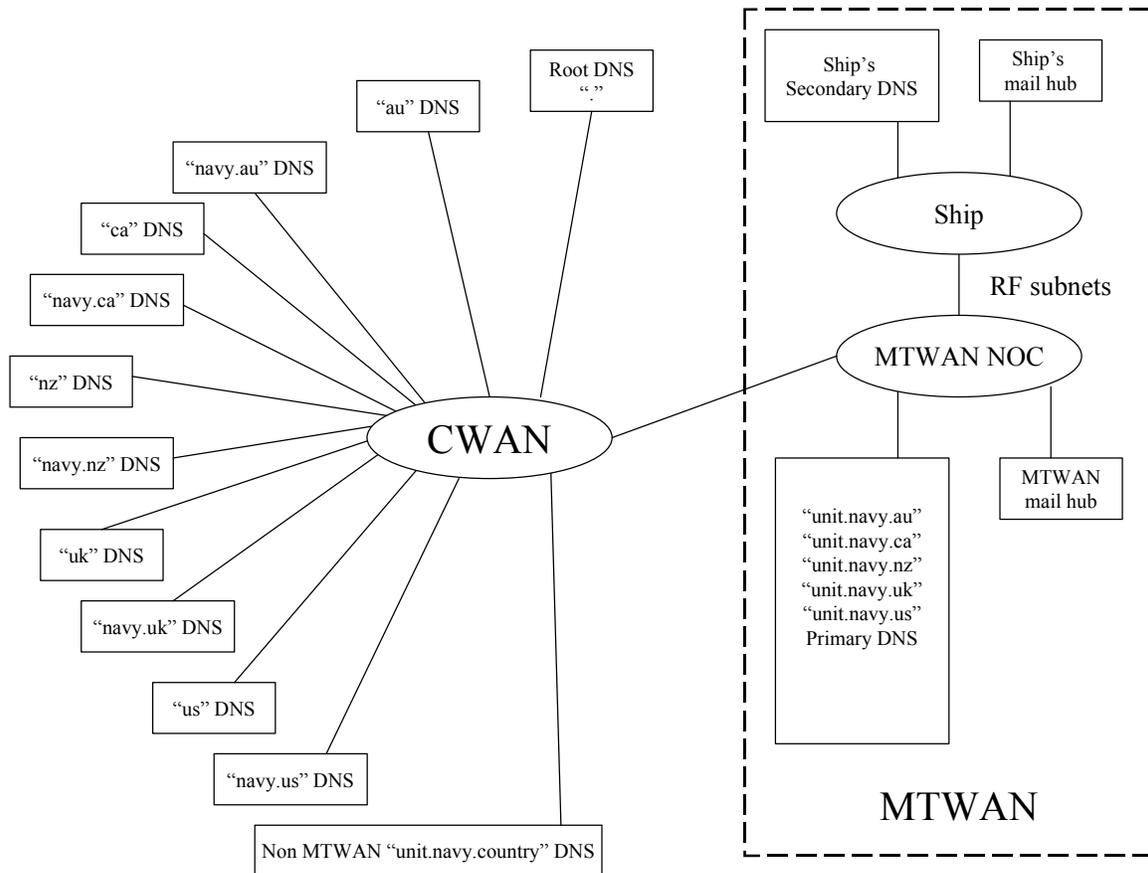


Figure 14-B-2: - DNS Servers

- f. 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.
- g. 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 personnel. When the ship requires

UNCLASSIFIED

Annex B to Chapter 14 to ACP 200

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.

- h. 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.
- i. 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.
- j. It is recommended that when assembling a MTWAN, consideration be 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.

14B05 DNS CLIENTS

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.

14B06 SMTP MAIL AND P_MUL

- a. DNS is intimately connected to the operation of standard Internet email (i.e., SMTP email). SMTP mail forwarders (email MTAs) consult DNS to determine which machines or sub-domains accept email directly and which machines or sub-domains want their mail redirected to a mail forwarder. In

UNCLASSIFIED

Annex B to Chapter 14 to ACP 200

the case of the MTWAN, mail originating on a shore network will be directed to the MTWAN shore mail hub located at the MTWAN NOC. This allows mail for ships to be accepted and stored when the ships are not “on-line”. It also allows the shore mail hub to multicast shore-to-ship mail via the P_MUL protocol, which can conserve RF bandwidth.

- b. Redirecting mail to the MTWAN shore mail hub will be accomplished by having each ship’s mail exchanger (MX) record point to the shore mail hub. For example, mail to “ops@brisbane.navy.au” will result in a DNS lookup of the MX record for “bristbane.navy.au”. The MX record will point to the MTWAN shore mail hub. This causes the ship’s mail to be delivered to the shore mail hub.
- c. Mail from MTWAN ships to shore will be sent from the ship to the MTWAN shore mail hub. The mail will then be forwarded from the shore mail hub to the shore network. This method allows P_MUL to be used over the ship-to-shore RF links, which conserves bandwidth. It should be noted that when P_MUL is used for ship-to-shore delivery, it will not query DNS before delivering the mail. The P_MUL protocol will be used for locations specified in the standard SMTP “mailertable” configuration file. The mail will be directed to its final destination using the P_MUL “mx_table” configuration file, rather than DNS.
- d. SMTP mail from one MTWAN ship to another will be sent directly from ship to ship using the P_MUL protocol. P_MUL will use the “mx_table” configuration file, rather than DNS, for ship-to-ship deliver within the MTWAN.

14B07 DELEGATION FOR MTWAN SUB-DOMAINS

- a. 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.
- b. It is essential that delegation be obtained not only for the name domain but also for the in-addr.arpa domain.
- c. Subnetting is used extensively by the MTWAN to make efficient use of the IP address space. As in-addr.arpa subdomains are organised on IP address byte

UNCLASSIFIED

Annex B to Chapter 14 to ACP 200

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.

14B08 PROCEDURES FOR SETTING UP DNS SERVERS

- a. Each MTWAN unit will assign host names, aliases if any, and IP addresses to all local hosts. It will then forward the names and IP addresses to the MTWAN NOC to enable the creation of configuration and db files for the primary DNS server at the NOC.
- b. Each nation, with the assistance of the NOC, will obtain delegation for the domain of its MTWAN units so that they will be visible to non-MTWAN hosts.
- c. The NOC will obtain names and IP addresses of all root servers to enable the creation of the root cache files for the primary and secondary servers.
- d. The NOC will generate the configuration and the db files for secondary servers, and forward them together with instructions on how to start the secondary servers, to all units to enable the setting up of the secondary servers.
- e. The NOC will advise all units of any changes to the configuration and db files.
- f. Instructions for configuring and running DNS servers using BIND implementations for UNIX platforms, and configuring DNS clients (resolvers) for UNIX and Windows platforms, can be found in the DNS TOI.

CHAPTER 15**ROUTING****1501 INTRODUCTION**

The high-level network concept documented in Chapter 2, is a collection of maritime forces, shore forces, and shore communication stations, connected by a diverse collection of communication subnets with information forwarded between them using routes set up by COTS routing protocols.

1502 AIM

This Chapter describes routing within a MTWAN.

1503 MTWAN SYSTEM DESCRIPTION

System Architecture. The MTWAN architecture is described in Chapters 2 and 10. For the purposes of this document, note that each MTWAN AS is a collection of maritime units (a unit is defined as a routing area) which may be Ships, Marine forces or Maritime Air Forces, Network Operation Centres and other shore communication station(s) all connected by a collection of backbone subnets. Each shore communication station will have a router or router ports dedicated to each MTWAN AS, that it supports.

1504 TECHNICAL ARCHITECTURE

- a. **Routing Domain Architecture.** Routing will be accomplished using the standard IP protocols OSPF and PIM for intra-AS routing, and BGP4 and DVMRP/MBGP for inter-AS routing. OSPF is used for routing over backbone subnets within an AS, and BGP4 is used for routing between ASs. OSPF is a dynamic routing protocol that quickly finds the best subnet to reach the destination. BGP4 is a policy-based routing protocol that selects the AS it will talk to based on policy entered manually by the AS manager. It operates on top of TCP and requires very stable subnets, which are more applicable to shore commercial connections.
- b. OSPF and PIM are the routing protocols used within each of the MTWAN ASs. The ASs are connected together using BGP4. All multicasting within an AS will use PIM. Multicasting between ASs will require the use

of MBGP or DVMRP to tunnel multicast messages through the BGP4 routers.

- c. An AS can have more than one exit point to other ASs. When only one exit point is used it becomes the default router for all traffic leaving the AS. However, when two or more exit points exist, some information must be provided to the interior OSPF routing protocol to decide which BGP4 border router to select to reach the exterior destination. The two BGP4 border routers need to exchange routing information to keep their databases in sync. This may be accomplished by an interior BGP4 to BGP4 protocol or exterior routing information that is imported from BGP4 that can be transferred to OSPF routing tables by Link State Advertisement (LSA) flooding throughout the AS.
- d. OSPF uses two types of external metrics for advertising the best exit point. 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 path to reach the external destination. Type 2 external metrics are an order of magnitude larger and are considered greater than any path 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 exterior metrics, and it does not require any interior lowest cost path calculations.
- e. The protocol stack used in MTWAN is shown in Figure 15-1. The OSPF and PIM protocols operate at the network level and provide dynamic routing. The route selection is based on the lowest cost path to reach the destination. 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 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.

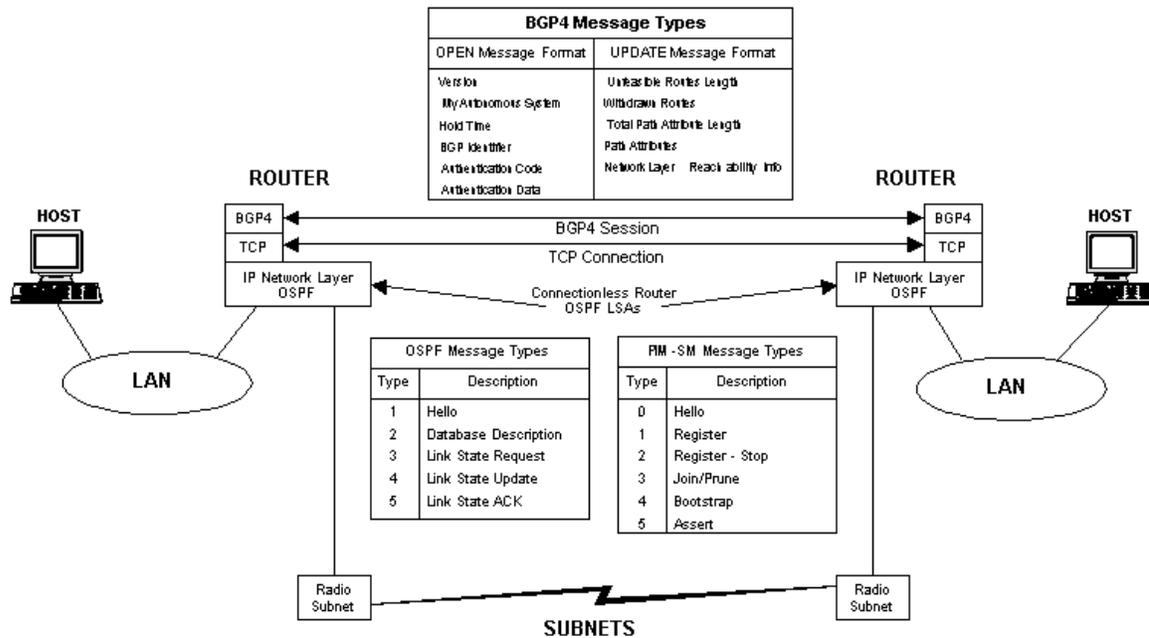


Figure 15-1: - MTWAN Router Protocol Stack

1505 EXTERIOR AUTONOMOUS SYSTEM ROUTING

a. Single allied WAN Access Point

- (1) When a single access point is available to the allied WAN, BGP4 is used. The BGP4 routing administrator can 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 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.
- (2) 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 BGP4 router administration both labor intensive and error-prone.
- (3) The primary use of BGP4 policy is to limit the amount of router protocol traffic seen inside the MTWAN as a result of external links. An allied WAN, as a global network, has the potential to generate large amounts of router protocol traffic. If this router protocol traffic

were allowed into the MTWAN, 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 MTWAN and between MTWAN ASs.

- (4) A global backbone network, e.g., the allied WAN, cannot use default routes and must have specific route advertisements for every network that is reachable across the backbone. Hence, all networks in the MTWAN must be advertised to the allied WAN. This is accomplished by setting the policy on the autonomous system boundary routers (ASBRs) in the MTWAN ASs to send all internal network advertisements to the allied WAN.

b. **Exterior Secondary allied WAN Access Points.**

The MTWAN may have the need to operate with more than one connection to the allied WAN. In this situation there is a requirement to have a means by which secondary and tertiary paths to the allied WAN can be established when the primary connection is unavailable.

(1) AS-Path

- (a) 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 path between the local AS and the destination AS. Routers typically 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. Routers have the ability to alter the AS-PATH of network routes by prepending their ASN to the AS-PATH.
- (b) BGP supports two types of sessions: External BGP (EBGP) and Internal BGP (IBGP). EBGP can be used between BGP-enabled routers in two adjacent autonomous systems, while IBGP can be 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.
- (c) Figure 15-2 illustrates an autonomous system with two external connections housed in two distinct border routers that speak

EBGP with border routers within a neighboring AS. The network also includes a series of backbone routers that interconnect other ASs. External routes learned via EBGP need to be communicated to the backbone routers to permit optimal routing to external destinations.

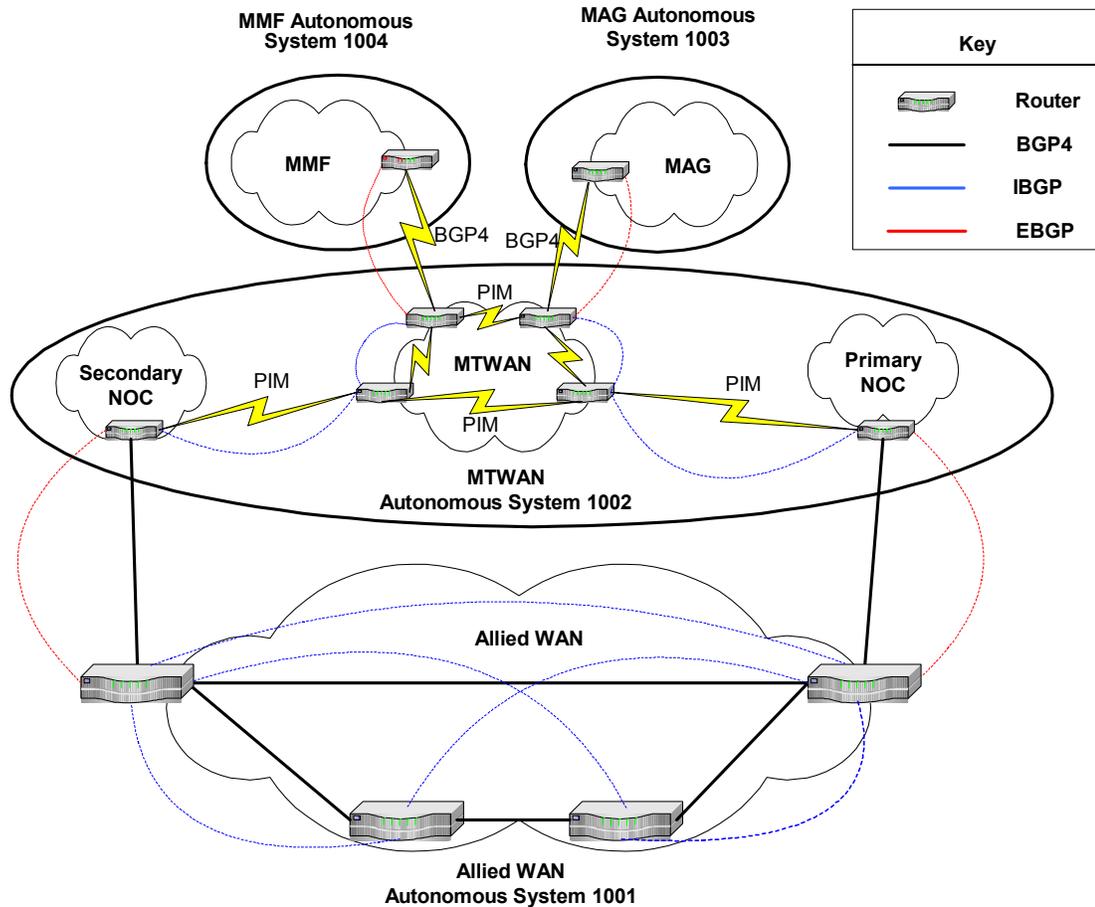


Figure 15-2: - Sample BGP Configuration

- (d) Depending on the network architecture, it is sometimes necessary to configure IBGP within routers of one AS that does not house 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 MTWAN. 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. This is not usually 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 MTWAN domain. Instead, IBGP should be used between the border routers and the backbone routers. In the network illustrated in Figure 15-2 an IBGP session is configured between each border router and each individual backbone router. The external routing information communicated to the backbone routers via IBGP permits optimal routing to external destinations without flooding the external routes throughout the autonomous system.

(2) Preferred Paths

- (a) A technique known as AS-PATH pre-pending can be used to establish the external connection at the primary site as the preferred path between an MTWAN AS and an allied WAN.
- (b) The MTWAN border router at the secondary site needs to be configured to pre-pend the MTWAN ASN to the AS-PATH before communicating routes via EBGP to the allied WAN border router. The MTWAN border router at the primary site cannot alter the AS-PATH it presents to the allied WAN. The AS-PATH in routes advertised by the MTWAN border router at the secondary site then consist of the MTWAN pre-pended to the allied WAN AS e.g. “1002 1002”, while the AS-PATH in routes advertised by the MTWAN border router at the primary site simply consists of “1002”, the MTWAN ASN. Since the AS-PATH advertised at the primary site is shorter than the AS-PATH advertised at the secondary site, traffic destined for the MTWAN network from the allied WAN would be routed via the primary site. When the connection between the MTWAN network and the allied WAN at the primary site is not available, traffic will be re-routed via the secondary site.
- (c) To ensure a symmetrical path between the MTWAN 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 EBGP to the MTWAN. The allied WAN border router at the primary site also needs to alter the AS-PATH it presents to the MTWAN.

- (d) The primary and secondary border routers communicate via an IBGP sessions to ensure a consistent view of external routing within an MTWAN AS. Using IBGP, the secondary border router will be aware of the preferred path 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.

c. **Failure recovery**

- (1) If either of the two exit points fails, then it is highly desirable that all traffic uses the remaining MTWAN -to-allied WAN connection.
- (2) For outgoing traffic, failure recover can be ensured by carefully setting up the default routes on the boundary routers. When a boundary router has a connection to the allied WAN, we want it to generate a default route and distribute it throughout the MTWAN. 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 route(s).
- (3) Within Cisco routers, this can be accomplished by using the “default-information originate” statement in the OSPF configuration. This statement causes the default route to be dynamically generated and injected into OSPF. However, if the router does not have an active route to the allied WAN, then this statement will not inject the default route into OSPF. That is, the “default-information originate” statement will not actually generate the default route unless the router knows for certain that it can pass the traffic to the allied WAN. When the link to the allied WAN fails, the router stops sending the default, and all traffic from the MTWAN will then use the remaining (active) exit point. This system will recover from failure of either boundary router.
- (4) Likewise, we want the system to revert to normal behavior when the failed exit is returned to service. When the boundary router again has a route to the allied WAN, the “default-information originate” statement will again automatically generate a default route. The default route will cause the MTWAN nodes connected to that router to again send allied WAN traffic to that router.

- (5) Use of the “AS-prepend” feature to direct traffic to the boundary also allows for automatic recovery from the failure of a boundary router for incoming traffic. If a boundary router fails, then the allied WAN will see routes to all the networks through the alternate router.

1506 INTERIOR AUTONOMOUS SYSTEM ROUTING PROTOCOLS.

a. Unicast

Unicast operation using OSPF is shown in Figure 15-3. The OSPF routers send 5 types of LSA’s 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.

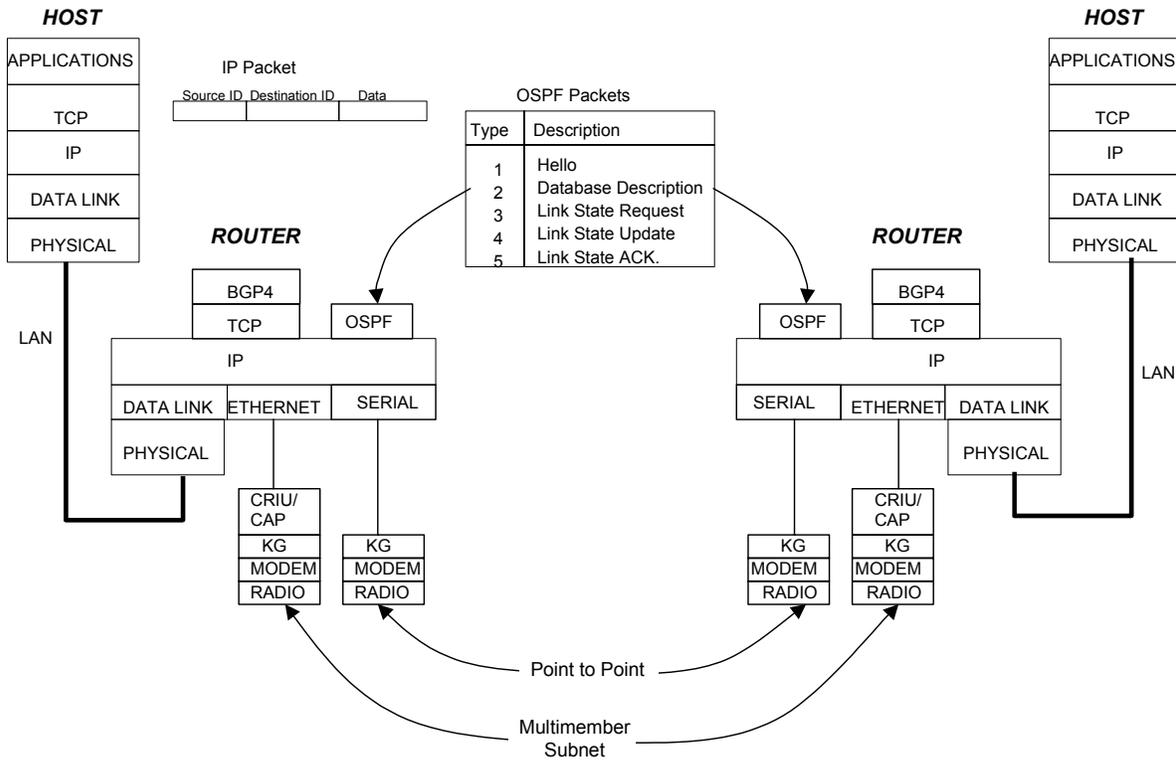


Figure 15-3: - Unicast Routing Layers

b. Multicast

- (1) The protocol layers for multicast are shown in Figure 15-4
- (2) The IP header for multicast now includes a Class A, B, or C unicast source address and a Class D multicast group address. The basic

approach is that Class D addresses are not assigned to any host and as such do not need to be registered. For full details on network naming and addressing refer to the MTWAN SOP for Naming & Addressing at Chapter 14.

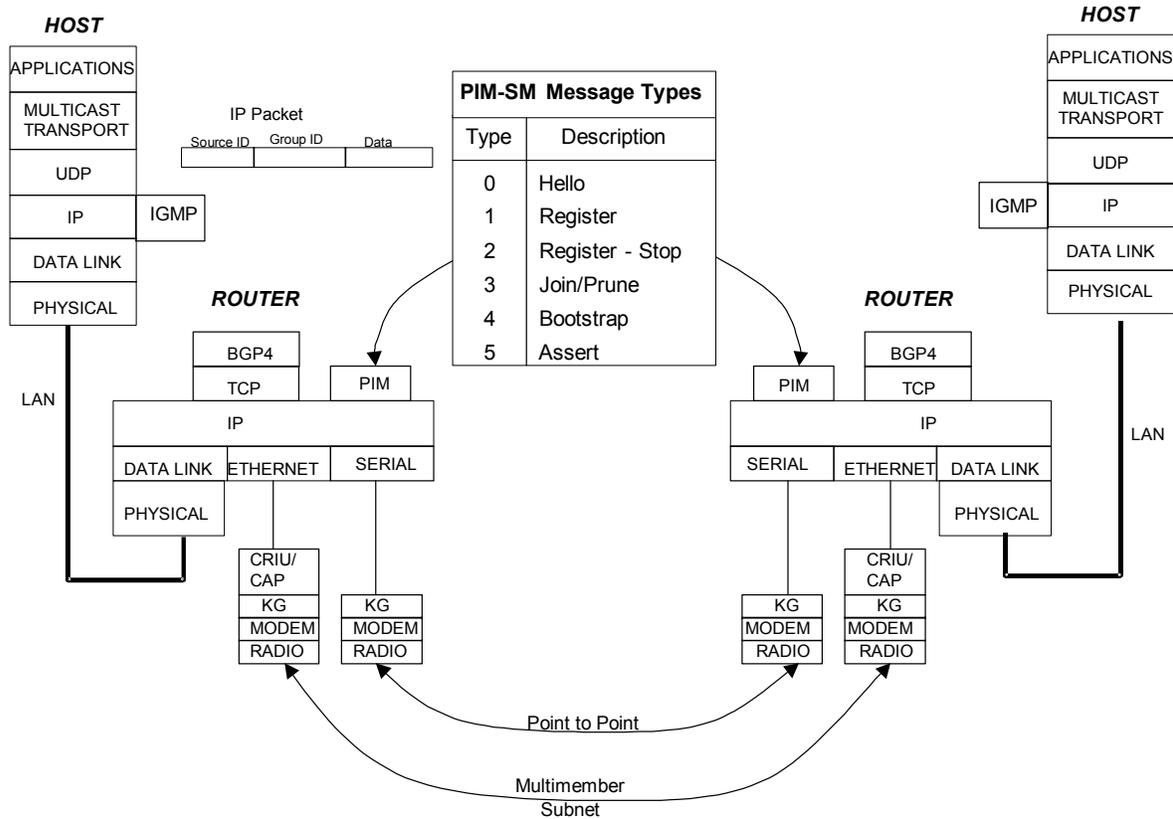


Figure 15-4- Multicast Routing Layers

- (3) When a host sends a message it simply broadcasts it on the local net, it does not send it to a destination. PIM establishes a “rendezvous point” (RP) where multicast senders and receivers can meet to coordinate delivery. Hosts use Internet Group Management Protocol (IGMP) to announce to multicast routers that they wish to join a class D group IP address. When a host sends a multicast message, the routers determine where groups are that have announced interest in the group, and the message is forwarded to those routers for local distribution. The destination routers then broadcast the packets on their local LAN and local hosts that have announced group membership accept the packets

- (4) Multicast receivers register with the RP and wait. Multicast transmitters send multicast packets to the RP, and the RP sends them on to the receivers. In a large network with few multicast receivers, the rendezvous point reduces the amount of multicast routing information flooded throughout the domain.
- (5) PIM begins by having the transmitter send all traffic directly to the RP, after which the RP sends the multicast packets down a shared tree. All receivers are located somewhere on the shared tree. The shared tree may be somewhat inefficient if it leads to longer paths for the multicast packets. The shared tree is also prone to congestion on the primary branches. However, when the multicast traffic reaches a certain volume, PIM converts its distribution pattern. By default, the switchover comes when the volume exceeds one packet. Thus, in practice PIM uses the RP to introduce transmitters and receivers, but then allows the actual transmission to take the shortest path.
- (6) Under PIM, 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. For the MTWAN, the static RP has been chosen and the NOC node selected as the RP.
- (7) Broadcast traffic will have a serial connection to a static routing port to convert from serial to Ethernet. The router will be configured as a static subnet so no link state protocols will be exchanged.

1507 REDUCING ROUTING PROTOCOL TRAFFIC TO THE ALLIED WAN

- a. The backbone network must be default-free, and therefore requires specific network routing information for every network in the backbone domain, as well as routing information for every network in every satellite domain. For large networks, such as the Internet, this can lead to an unacceptably large number of network advertisements. In response, the Internet has required network advertisements to be aggregated using the "Classless Inter-Domain Routing" (CIDR) address aggregation techniques.
- b. A simple example of CIDR would be the combination of two Class C IP network addresses into a single CIDR advertisement. Traditionally, if a MTWAN 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 MTWAN would advertise a single network, starting at 192.200.200.0, that contained 512 addresses. Exactly the same host addresses are advertised in both formats, but CIDR produces 50% fewer routing advertisements. This is critical on large backbones such as the Internet.

- c. Typically, the network design would specify that numerous coalition units would receive a fraction of a Class C IP network address. For example, Naval Radio Station San Diego (NRSSD) would have a fraction of the A.B.C.0 network (A.B.C.16-A.B.C.31) and USS BATAAN would have another fraction of the same network (A.B.C.48-A.B.C.63). All these subnet addresses would be summarized to a single A.B.C.0 network before they were advertised to the allied WAN. This reduces the number of MTWAN network advertisements that the allied WAN needs to carry on its backbone network.
- d. 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 backbone bandwidth.
- e. To implement this scheme, two Cisco-specific commands are used on the boundary routers. The initial BGP4 design calls for redistributing all the OSPF routing information into the BGP protocol, so that it can be carried across the BGP4 connection from the MTWAN to the allied WAN. This is implemented by using the “redistribute ospf <process ID>” command within the BGP configuration. This command ensures that all MTWAN routes will be sent to the allied WAN.
- f. To aggregate the routes before they are sent to the allied WAN, the MTWAN will use the Cisco “aggregate-address” statement. Thus, OSPF injects both XXX.XXX.62.16 (NRSSD) and XXX.XXX.62.48 (BATAAN) into BGP on the MTWAN router. But, the BGP aggregate-address statement condenses these subnets into a single CIDR advertisement before sending the information to the allied WAN router. As far as the allied WAN backbone is concerned, the MTWAN advertises a Class C IP network address, XXX.XXX.62.0. Within the allied WAN, any traffic for any host on this network is directed to the MTWAN. By contrast, within the MTWAN, the traffic is routed to specific nodes according to the more specific OSPF information, which advertises each subnet individually.

METRICS**15A01 OSPF METRIC VALUES**

- a. OSPF is the intra-AS routing protocol for the MTWAN. OSPF assigns a metric value to each link, used to determine the lowest cost path from source to destination. The cost is the sum of the metric values.
- b. The algorithm used for selecting the metric value is $MV_n = C \times MV_{n-1}$ for each doubling of the bandwidth. The recommendation is $C = 1.2$. The metric values shown in Table 15A-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.

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	

Table 15-A-1: Recommended Metric Values

- c. In order to implement rough load balancing, a default route cost (such as 100) should be used by all MTWAN boundary routers. All boundary routers must use the same type external default route, such as OSPF type II external routes. All boundary routers should dynamically

originate the default route through the use of the Cisco “default-information originate” command in the OSPF configuration. Finally, all boundary routers must have local routes to the allied WAN, such as a static route from the boundary router to the allied WAN router.

- d. Figure 15A-1 shows a typical MTWAN topology with the link bandwidths and Figure 15A-2 shows the metric values for those links. To determine the lowest cost path between any source and destination pair, just sum the metric values shown and the path with the lowest cost will be selected by the router.

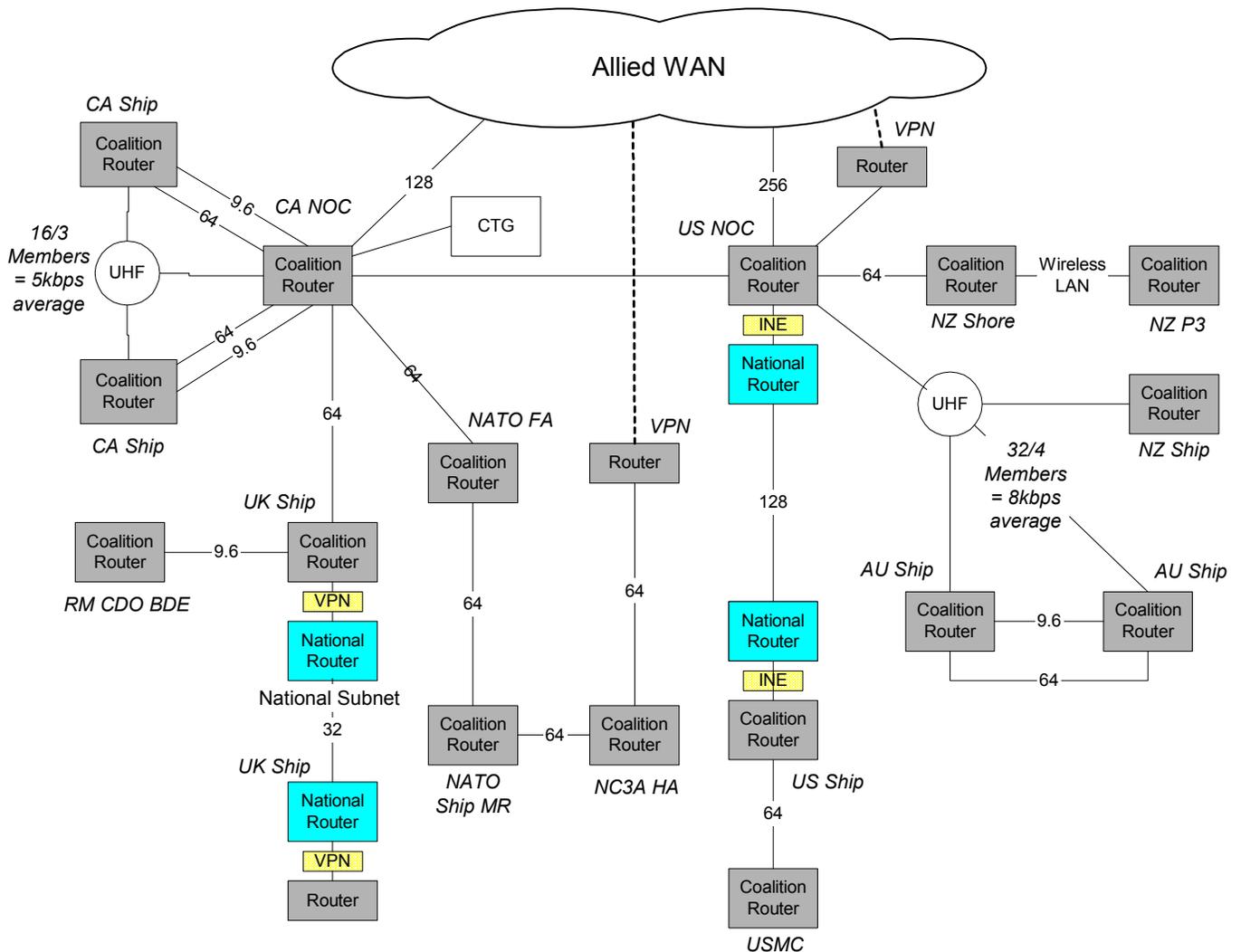


Figure 15-A-1: Typical MTWAN Bandwidth for Coalition and National Subnets

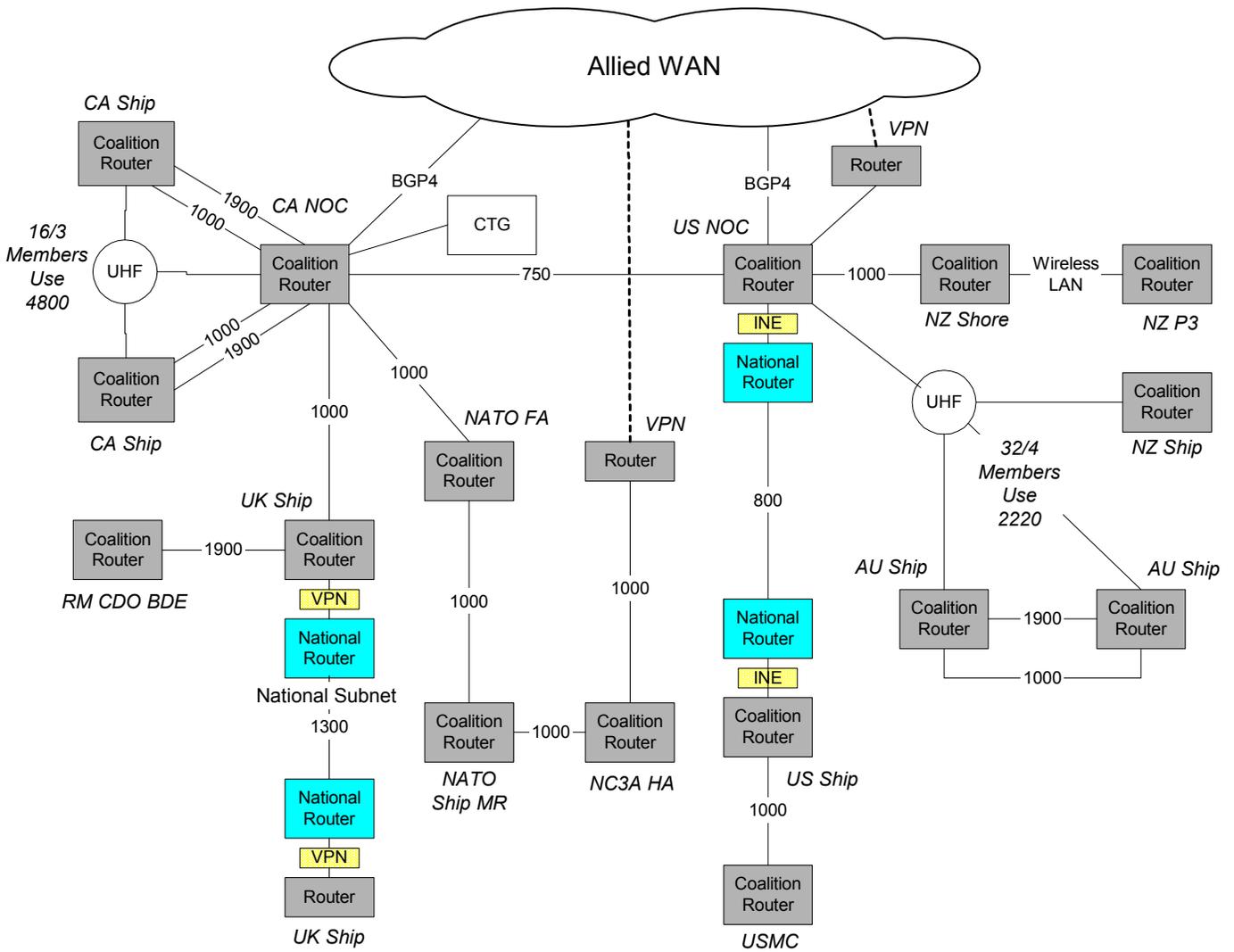


Figure 15-A-2: Link Metric Values

UNCLASSIFIED

ACP 200

Chapter 16

COMMUNICATIONS SUBNETS

To be included in ACP 200 Change 1

16-1

UNCLASSIFIED

Original

LIST OF ABBREVIATIONS

ACIXS	Allied Communication Information Exchange System
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
CAS	Collaboration At Sea
CATF	Commander Amphibious Task Force
CCEB	Combined Communications-Electronics Board
CCI	Controlled Cryptographic Item
CELP	Code Book Excited Linear Predictive
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFE	CENTRIXS Four Eyes
CFLCC	Coalition Force Land Component Commander

UNCLASSIFIED

ACP 200

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
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
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
EoS	Elements of Service
FF	Fire Fly
FIFO	First In, First Out

LOA-2

UNCLASSIFIED

Original

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
ISDN	Integrated Services Digital Network
IXS	Information eXchange System

UNCLASSIFIED

ACP 200

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
NCW	Network Centric Warfare
NES	Network Encryption System
NM	Network Management
NNTP	Network News Transport Protocol

LOA-4

UNCLASSIFIED

Original

UNCLASSIFIED

ACP 200

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
PT	Plain Text
QOS	Quality of Service
RED	Random Early Drop
RIP	Routing Internet Protocol
RF	Radio Frequency
RP	Rendezvous Point
RTF	Rich Text Format
SHF	Super High Frequency
SIPRNET	Secret Internet Protocol Router Network (United States)
SMG	Secure Mail Guard
SMTP	Simple Mail Transfer Protocol

LOA-5

UNCLASSIFIED

Original

UNCLASSIFIED

ACP 200

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 Drop
Z	Cryptographic Device

LOA-6

UNCLASSIFIED

Original

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 XI
List of Figures	XII to XIII
List of Tables	XIV
Chapter 1	1-1 to 1-5
Chapter 2	2-1 to 2-7
Chapter 3	3-1 to 3-18
Chapter 4	4-1
Chapter 5	5-1 to 5-11
Chapter 6	6-1 to 6-8
Chapter 7	7-1 to 7-7
Chapter 8	8-1 to 8-11
Chapter 9	9-1 to 9-22
Chapter 10	10-1 to 10-14
Chapter 11	11-1 to 11-4
Chapter 12	12-1 to 12-27
Chapter 13	13-1 to 13-12
Chapter 14	14-1 to 14-16
Chapter 15	15-1 to 15-14
Chapter 16	16-1
List of Acronyms	LOA-1 to LOA-6
List of Effective Pages	LOEP-1