

UNCLASSIFIED

ACP 200(A)

MARITIME TACTICAL WIDE AREA NETWORKING (MTWAN)

ACP 200(A)



May 2005

UNCLASSIFIED

UNCLASSIFIED

ACP 200(A)

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(A), 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.

UNCLASSIFIED

UNCLASSIFIED

ACP 200(A)

**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(A)	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 RNZAF
CCEB Permanent Secretary

III

UNCLASSIFIED

UNCLASSIFIED

ACP 200(A)

RECORD OF MESSAGE CORRECTIONS

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

IV

UNCLASSIFIED

TABLE OF CONTENTS

Foreward	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	1-1
104. Scope	1-2
105. Capability	1-2
106. Document Structure	1-3
107. Conclusion	1-5

Chapter 2
Concept Of Operations

201. Introduction	2-1
202. Aim	2-1
203. Scope	2-1
204. Overview	2-1
205. Operational View	2-2
206. Systems View	2-4
207. Technical View	2-8
208. Conclusion	2-11

Chapter 3
Information Management (IM)

301. Introduction	3-1
302. Aim	3-1
303. Overview	3-1
304. Definition	3-2
305. Principles	3-2
306. Fitness of Information	3-3
307. C2 Decision Cycle	3-5
308. Information Requirements	3-5
309. Information Dissemination Management (IDM)	3-6
310. Information Tools	3-8
311. Information Impediments	3-8
312. Conclusion	3-9

Annex A to Chapter 3
Information Management Standard Operating Procedures

3A01. Introduction.....	3-10
3A02. Aim.....	3-10
3A03. Guidelines	3-10
3A04. Security	3-11
3A05. Information Dissemination Plan	3-11
3A06. OPTASK IM	3-14
3A07. PowerPoint.....	3-14
3A08. Minimise	3-14
3A07. File Naming Convention.....	3-15

Annex B to Chapter 3
OPTASK Information Management (IM)

A. Overview.....	3-16
B. Information Exchange Requirements.....	3-16
C. Electronic Exchange Policies.....	3-17
D. Storage Policies.....	3-19
E. General	3-19

Annex C to Chapter 3
Example of OPTASK IM

Example of OPTASK IM.....	3-21
---------------------------	------

Annex D to Chapter 3
MS PowerPoint File Size Management

3D01. Introduction.....	3-26
3D02. Aim.....	3-26
3D03. Objective	3-26
3D04. Deactivate Fast Save	3-27
3D05. Images and Pictures	3-27
3D06. Utilise Master Slide.....	3-29
3D07. Conclusion	3-30

Chapter 4
Security

401. Introduction.....	4-1
402. Aim	4-1
403. Definitions.....	4-1
404. Overview.....	4-1
405. Reference	4-2
406. Network Topology	4-2
407. Points Of Presence / Boundary Protection Device	4-4

UNCLASSIFIED

ACP 200(A)

408. Threats.....	4-5
409. Responsibilities.....	4-6
410. Export Sanction.....	4-6
411. Assumptions.....	4-7
412. Recommended Security Architectures.....	4-7
413. Accreditation.....	4-12
414. Security Device Interoperability.....	4-12

Chapter 5 Training and Interoperability

501. Introduction.....	5-1
502. Aim	5-1
503. Overview.....	5-1
504. Training.....	5-1
505. Interoperability Level.....	5-1
506. Determining Interoperability Level	5-2

Chapter 6 Messaging

601. Introduction.....	6-1
602. Aim	6-1
603. Overview.....	6-1
604. Types of Messaging.....	6-2
605. Text-Based Formats.....	6-2
606. Multimedia Formats.....	6-3
607. Messaging Selection	6-4
608. Multicast Messaging.....	6-6
609. Public Key Infrastructure (PKI).....	6-6
610. Conclusion	6-6

Annex A to Chapter 6 Email User Guide

6A01. Introduction.....	6-8
6A02. Aim.....	6-8
6A03. Overview.....	6-8
6A04. E-Mail Processes.....	6-9
6A05. Sending Email (Creation, Dissemination)	6-9
6A06. Forwarding Email (Actioning).....	6-14
6A07. Receiving Email (Reading, Sorting, Actioning)	6-14
6A08. Replying to Email (Actioning).....	6-15
6A09. Attachments	6-15
6A10. Effective Use of Email (Management)	6-16
6A11. Records Management.....	6-16
6A12. Administration	6-17
6A13. Conclusion	6-18

VII

UNCLASSIFIED

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.....	7-4
708. Multicast Transport Services	7-4
709. Architecture.....	7-4
710. Selection of Appropriate COP Dissemination Method.....	7-6
711. Conclusion	7-7

Chapter 8 Web Services

801. Introduction.....	8-1
802. Aim	8-1
803. Overview.....	8-1
804. Objective.....	8-2
805. Definitions.....	8-2
806. Functional Description.....	8-3
807. Web Administration.....	8-4
808. Principles.....	8-5
809. Requirements	8-6
810. Connectivity.....	8-6
811. Web Content / Pages.....	8-7
812. Web Page Guidelines.....	8-8
813. Posting Documents	8-9
814. Web Interfaces	8-10
815. Conclusion	8-11

Annex A to Chapter 8 Web-Enabled Database Replication

8A01. Introduction.....	8-12
8A02. Aim.....	8-12
8A03. Overview.....	8-12
8A04. Replication Architecture	8-12
8A05. Replication Process.....	8-15
8A06. Concept for Employment.....	8-16

Appendix 1 to Annex A to Chapter 8 Typical Replication web Page

8A101. Introduction.....	8-18
8A102. Aim.....	8-18
8A103. Overview.....	8-18
8A104. Page-Level Structures	8-18

Chapter 9 Distributed Collaborative Planning (DCP)

901. Introduction.....	9-1
902. Aim	9-2
903. Overview.....	9-2
904. Configuration	9-5
905. Bandwidth Limitations.....	9-6
906. Security	9-7
907. Tools	9-7
908. Requirements	9-7
909. Conclusions.....	9-7

Annex A to Chapter 9 DCP Standards

9A01. Introduction.....	9-8
9A02. Standards.....	9-8

Annex B to Chapter 9 DCP Standard Operating Procedures

9B01. Introduction	9-11
9B02. Aim.....	9-11
9B03. Description	9-11
9B04. User Access.....	9-14
9B05. Planning Order	9-15
9B06. Conduct	9-16
9B07. Tool Selection	9-18
9B08. Security.....	9-18
9B09. Network Engineering	9-19
9B10. Principles of Effective Meetings	9-19
9B11. Warnings and Precautions.....	9-20

Appendix 1 to Annex B to Chapter 9 Chat User Guide

9B101. Introduction.....	9-21
9B102. Aim.....	9-21
8A103. Overview.....	9-21
8A104. Chat Types	9-21

UNCLASSIFIED

ACP 200(A)

9B105. Benefits.....	9-22
9B106. Disadvantages.....	9-23
9B107. Inappropriate Employment.....	9-24
9B108. “The Golden Rules”	9-25

Chapter 10 Network Architecture

1001. Introduction.....	10-1
1002. Aim	10-1
1003. Overview.....	10-1
1004. Description.....	10-1
1005. Routing Architecture.....	10-2
1006. Communications Architecture	10-5
1007. Security Architecture	10-7
1008. Node Descriptions.....	10-7
1008. Conclusion	10-7

Annex A to Chapter 10 Amphibious Operation Standard Operating Procedures

10A01. Introduction.....	10-8
10A02. Aim.....	10-8
10A03. Overview.....	10-8
10A05. Assault.....	10-9
10A06. Lodgment	10-11
10A07. Sustainment.....	10-12

Chapter 11 Quality of Service

1101. Introduction.....	11-1
1102. Aim	11-1
1103. Overview.....	11-1
1104. Definition	11-2
1105. Link Throughput / Bottleneck.....	11-2
1106. Maximising Link Throughput.....	11-3
1107. Controlling less Urgent Traffic.....	11-4
1108. Objective.....	11-4
1109. Visibility	11-5
1110. Control	11-6
1111. Compression	11-8
1112. QoS Solutions	11-8
1113. Future Work.....	11-9
1114. Conclusion	11-10

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 SOP

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	12-13

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

OPTASK Net (Example)	12-15
----------------------------	-------

Chapter 13 Transport Services

1301. Introduction.....	13-1
1302. Aim	13-1
1303. Overview.....	13-1
1304. Requirement.....	13-1

Annex A to Chapter 13

Multicast Service Gateway (MSeG)

13A01. Introduction.....	13-3
13A02. Aim.....	13-4
13A03. Overview.....	13-4
13A04. Supported Applications.....	13-4
13A05. Example Configurations	13-7
13A06. Graphical User Interface (GUI)	13-11

Chapter 14

Network Naming and Addressing

1401. Introduction.....	14-1
1402. Aim	14-1
1403. Overview.....	14-1
1404. Host Naming Convention	14-1
1405. Domain Naming Convention	14-4
1406. IP Subnetting and Multicast Addressing.....	14-6
1407. IP Addressing Convention.....	14-8
1408. IP Address Authority Tasks	14-9
1409. Unit Assignment of Hosts.....	14-9
1410. Conclusion	14-9

Annex A to Chapter 14

IP Addressing

IP Addressing.....	14-10
--------------------	-------

Annex B to Chapter 14

Domain Name Service SOP

14B01. Introduction.....	14-12
14B02. Aim.....	14-12
14B03. Overview.....	14-12
14B04. Domain Name Space.....	14-12
14B05. DNS Servers.....	14-13
14B06. DNS Clients.....	14-15
14B07. Delegation for MTWAN Sub-domains	14-16

Chapter 15

Routing

1501. Introduction.....	15-1
1502. Aim	15-1
1503. Overview.....	15-1
1504. Routing Architecture.....	15-3
1505. Interior TGAN Routing.....	15-6
1506. Exterior TGAN Routing	15-8
1507. Reducing Routing Protocol Traffic to the Allied WAN	15-11

1508. Conclusion	15-11
------------------------	-------

Annex A to Chapter 15 Metrics

15A01. Routing Protocol (Unicast)	15-13
15A02. Routing Protocol (Multicast)	15-15

Annex B to Chapter 15 Metrics

15B01. OSPF Metric Values.....	15-17
--------------------------------	-------

Chapter 16 Communications Subnets

1601. Introduction.....	16-1
1602. Aim	16-1
1603. Overview.....	16-1
1604. Definitions.....	16-2
1605. Communications Architecture	16-2
1606. Communication Subnets / Communication Bearers.....	16-4
1607. Communication Bearers/Services.....	16-5
1608. Subnet Technologies.....	16-6
1609. Conclusion	16-7

Annex A to Chapter 16 INMARSAT B

16A01. Introduction.....	16-8
16A02. Aim.....	16-8
16A03. Overview.....	16-8
16A04. Description.....	16-8
16A05. Limitations	16-9
16A06. Setup.....	16-10
16A08. Establishing a Connection.....	16-10
16A09. Maintaining a Connection.....	16-11

Annex B to Chapter 16 Subnet Relay

16B01. Introduction	16-12
16B02. Aim.....	16-12
16B03. Overview	16-12
16B04. User Requirement.....	16-12
16B05. Operational Concept.....	16-14
16B06. Capabilities.....	16-19
16B07. Technical Limitations and Initial Assumptions	16-20

List of Abbreviations

GlossaryLOA-1

List of Effective Pages

List of Effective PagesLOEP-1

List of Figures

Figure 1-1: Maritime Network Domains	1-3
Figure 1-2: Document Architecture	1-4
Figure 1-3: Document Structure	1-4
Figure 2-1: Determinants of Information Value	2-2
Figure 2-2: Operational View (OV-1)	2-3
Figure 2-3: Systems View (SV-1.1).....	2-4
Figure 2-4: Systems View (SV-1.2).....	2-5
Figure 2-5: Systems View (SV-1.3).....	2-7
Figure 2-6: Technical View (TV-1.1)	2-9
Figure 2-7: Technical View (TV-1.2)	2-10
Figure 3-1: IM Hierarchy.....	3-2
Figure 3-2: Determinants of Information Value	3-4
Figure 3-3: Impact of Presentation Form.....	3-4
Figure 3-4: C2 Decision Cycle	3-5
Figure 3-3: IDM.....	3-6
Figure 3-A-1: Daily Operations Cycle.....	3-12
Figure 4-1: MTWAN Topology.....	4-3
Figure 4-2: Boundary protection devices between domains	4-4
Figure 4-3: MTWAN Connectivity	4-8
Figure 4-4: Air Gap Architecture.....	4-9
Figure 4-5: Networked Architecture	4-10
Figure 4-6: “Fully Integrated” Target Architecture	4-11
Figure 6-A-1: Email Processes	6-9
Figure 6-A-2: Examples of Email Subject Lines	6-11
Figure 6-A-3: Inverted Pyramid Concept	6-13
Figure 7-1: Traditional Environment (with IXS networks and CST)	7-5
Figure 7-2: Full IP Environment (MTWAN).....	7-5
Figure 8-1: Service Orientated Architecture	8-3
Figure 8-A-1: Generic Replication Architecture	8-13
Figure 8-A-2: Mesh Replication Architecture	8-14
Figure 8-A-3: Federated Hub-Spoke Replication Architecture	8-14
Figure 8-A1-1: Typical Page Structure	8-19
Figure 8-A1-2: Global Area Content	8-20
Figure 9-1: Collaborative Planning Spectrum	9-2
Figure 9-2: DCP Characteristics	9-5
Figure 9-3: DCP Configurations	9-6
Figure 9-B-1: Bandwidth Aggregation.....	9-13
Figure 9-B-2: Operator Number Impact on Bandwidth.....	9-15
Figure 10-1: Notional MTWAN Architecture	10-2
Figure 10-2: Single-AS TGAN	10-3
Figure 10-3: Multiple-AS TGAN	10-4
Figure 10-4: MTWAN Routing	10-5
Figure 10-5: Subnet Combinations	10-6

UNCLASSIFIED

ACP 200(A)

Figure 10-A-1: MTWAN Transit Network Connectivity	10-9
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	10-10
Figure 10-A-5: Ship Node in Assault Phase	10-11
Figure 10-A-6: MTWAN Network Connection in Lodgment Phase.....	10-11
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.....	10-13
Figure 11-1: Grades of Service	11-7
Figure 14-A1-1: IP Address	14-10
Figure 14-B-1: Domain Name Schema	14-13
Figure 14-B-2: DNS Servers.....	14-14
Figure 15-1: Router Protocol Stacks	15-2
Figure 15-2: Interior and Exterior TGAN Routing.....	15-3
Figure 15-3: An Example of a Multi-AS TGAN	15-5
Figure 15-4: Private Routing	15-6
Figure 15-A-1: Sample BGP Configuration	15-15
Figure 15-B-1: Example of Coalition and National Subnets Bandwidth	15-18
Figure 15-B-2: Link Metric Values (Notional).....	15-19
Figure 16-1: Communication Subnet(s).....	16-2
Figure 16-2: Communications Architecture	16-3
Figure 16-A-1: Global INMARSAT Coverage	16-8
Figure 16-A-2: INMARSAT B Configuration	16-9
Figure 16-B-1: Operational View	16-14
Figure 16-B-2: Relaying Concept.....	16-15
Figure 16-B-3: Ship Moving from one BG to Another	16-15
Figure 16-B-4: Multiple, Dynamic Relays	16-16
Figure 16-B-5: Relaying only when needed	16-17
Figure 16-B-6: Subnetwork Splitting.....	16-17
Figure 16-B-7: Subnetwork Mapping	16-18
Figure 16-B-8: Multiple Relays to Destination	16-18

List of Tables

Table 3-A-1: Information Dissemination Plan (IDP)	3-14
Table 5-1: WAN Link	5-2
Table 5-2: Minimum Dedicated Bandwidth	5-2
Table 5-3: Supported Applications	5-2
Table 5-4: Interoperability Matrix	5-3
Table 6-1: Messaging Selection.....	6-6
Table 6-A-1: Guideline for selection of Communication Method.....	6-10
Table 7-1: COP Dissemination Methods	7-6
Table 8-1: Standards behind Web Services	8-4
Table 9-1: DCP Spectrum	9-3
Table 9-B-1: Bandwidth Toolset Spectrum	9-12
Table 14-A-1: Abbreviations for 'Use' Field	14-2
Table 14-A-2: Abbreviations for 'Type' Field	14-3
Table 14-A1-1: IP Address Classes	14-10
Table 15-B-1: Recommended Metric Values	15-17
Table 16-1: Communication Subnet Matrix	16-5

Chapter 1

INTRODUCTION

101 OVERVIEW

A Maritime Tactical Wide Area Network (MTWAN) is an affordable, effective and efficient means to share information in a tactical environment. This publication provides guidance as to the procedures, applications, infrastructure and data attributes required for tactical mobile IP networking. To enable widest distribution, the information contained within the main part of this document is unclassified. Classified information will be incorporated in separate supplements.

102 BACKGROUND

- a. In the mid to late 1990s, Operational Commanders recognized that the existing procedures, applications, infrastructure and data standards could not support Allied and Coalition Information Exchange Requirements (IER). Increased levels of formal message traffic resulted in message traffic backlogs, delays, and non-delivery. This was especially poignant during periods of high intensity operations. Furthermore, the large amount of information could not be easily assimilated due to the way it was presented.
- b. To address this issue a number of related initiatives were implemented; in Joint Warrior Interoperability Demonstration (JWID) 97 the initial aspects of a multi-national maritime WAN were demonstrated and in RIMPAC 98, Commander Pacific Fleet (COMPACFLT) established what was to become a Wide Area Network (WAN) between Australia, Canada, United Kingdom and the United States.
- c. Subsequently, there have been many incremental advances driven by operational requirements that led to the creation of a number of tactical mobile WANs or the extension of shore-based networks to sea. AUSCANNZUKUS also continued refining doctrine and solutions through participation in JWID, involvement in At Sea Trials (AST) and feedback from the naval warfighter.

103 AIM

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

104 SCOPE

This publication is applicable to the operators and technicians who are responsible for the establishment, operation and maintenance of a WAN in a mobile tactical environment. It is designed for use in conjunction with other operational documents and provides:

- a. an overarching document for current maritime networks,
- b. guidance to the establishing a MTWAN, and
- c. a goal MTWAN architecture.

105 CAPABILITY

- a. A MTWAN is a maritime Internet Protocol (IP) based network developed to promote the effective and efficient sharing of information within the maritime tactical environment. The term “MTWAN” used in the context of this document describes generic “networking at sea” capabilities and not a specific network. There are currently a number of tactical operational networks fielded within the allied and coalition communities, the most common being CENTRIXS.
- b. 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 layer and has linkages to the support and real time tactical information exchange layer.

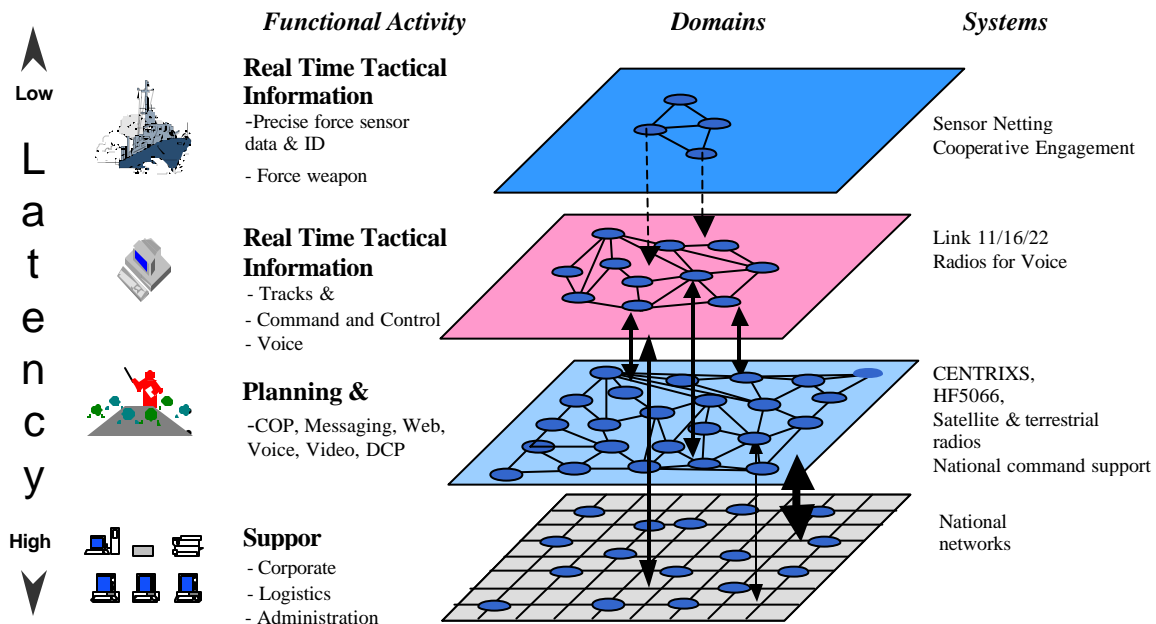


Figure 1-1 Maritime Network Domains

- c. A network-enabled approach vice a 'stovepipe' platform approach provides a more effective and efficient employment of finite C4 resources and facilitates timely information flow between disparate C4 users.
- d. Until nations have implemented the infrastructure required to support the 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 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.

106 DOCUMENT STRUCTURE

- a. The document structure is detailed at Figures 1-2 and 1-3. Part 1 (indicated in yellow in Figure 1-2) is focused towards the operators and addresses the information infrastructure (the 'infostructure') and associated front-end applications. For the most part, the information in Part 1 is of a general nature that sets the framework for information transfer over a MTWAN and highlights important issues for consideration. Chapters 3 (Information Management) and 5 (Security) are applicable across the breadth of the publication, hence their position within Figure 1-

2. Part 2 (indicated in green in Figure 1-2) describes the technical infrastructure. These Chapters provide generic description, while the Annexes are more detailed and include user guides, and technical detail.

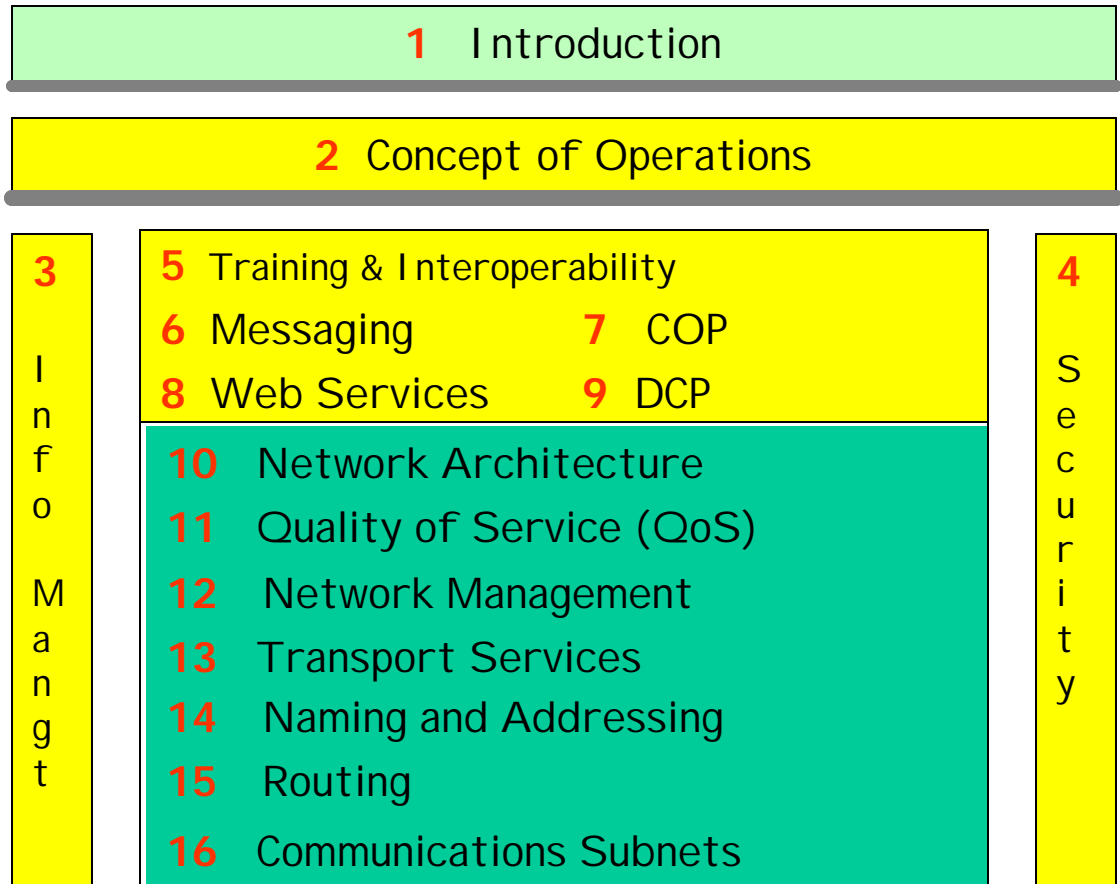


Figure 1-2 Document Architecture

- b. The structure of ACP 200 is graphically represented at Figure 1-3. National / Organisational / Enclave variants will be documented in supplements or separate standalone handbooks. Such supplements may or may not refer back to this publication (e.g. ACP 200 NATO-Supp, ACP 200 UK-Supp, CFE CONOPS, CNFC CONOPS). The supplements and handbooks will provide greater detail and information relating to the conduct and operation of national, organisation or specific network.

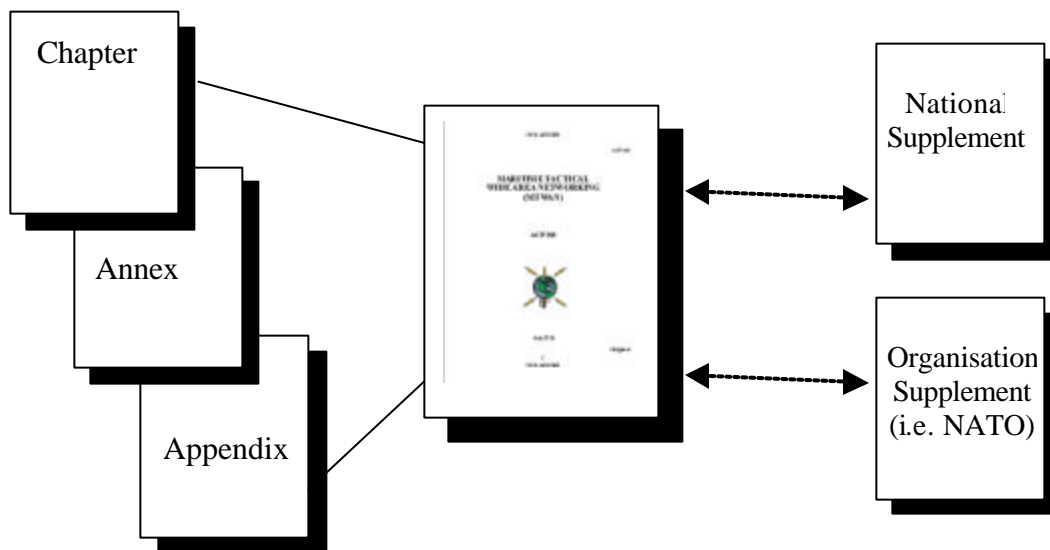


Figure 1-3 Document Structure

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 an information environment that enhances a Commander's ability to fight and win at sea.

Chapter 2**CONCEPT OF OPERATIONS****201 INTRODUCTION**

- a. Allied 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 the use of military specific equipment and applications.
- b. In contrast, IP based networks allow the convergence of many types of data onto a single network. This simplifies the installation, operation and management of equipment and applications, enables the efficient use of communication bearers, and exploits the benefits of IP technology. COTS IP networking products and IP-based information systems support interoperability and provide a large technological base and a cost-effective solution to information exchange requirements.
- c. Subsequently, a MTWAN is designed to facilitate information sharing within a maritime force structure, exploiting the benefits of IP technology.

202 AIM

This chapter provides the CONOPS for the establishment and operation of a MTWAN.

203 SCOPE

This chapter uses operational, systems and technical architectural views to describe the MTWAN Concept of Operations (CONOPS). A fuller understanding of maritime tactical wide area networking comes from reading the whole publication.

204 OVERVIEW

A MTWAN is based on the following principles:

- a. An IP based network is the most efficient and effective method for transferring planning information within a force.

- b. Information transfer will take place in a Secret-High network.
- c. Connections into/from other networks of a different security domain will be via approved border protection devices.
- d. Ship-to-ship and ship-shore information transfers will be via a variety of strategic and tactical communication systems.

205 OPERATIONAL VIEW

- a. The MTWAN operational view captures, at a high level, the nature and purpose of information exchanges in an allied tactical environment.
- b. Generically, the two types of information used by the tactical user are Action and Planning information. Action information requires immediate action such as attacking the enemy or avoiding 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.
- c. 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/ric hness of the information (i.e. the content, accuracy, timeliness and relevance of the information etc), and the degree to which it can be shared (the reach of the information).

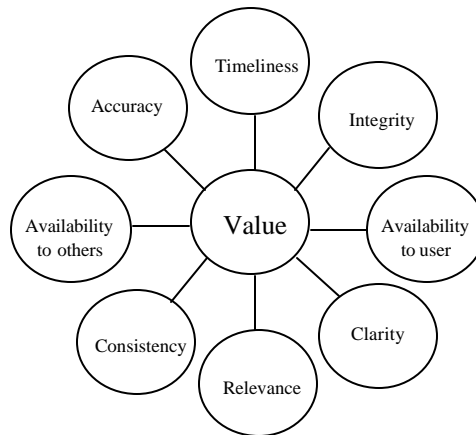


Figure 2–1 Determinants of Information Value

- d. The OV-1 (Figure 2–2) provides a high-level graphical description of the MTWAN operational concept. It illustrates a maritime Task Force organisation:
- (1) Comprising allied / coalition ships, submarines, aircraft, marine and ground forces as well as associated infrastructure such as Network Operations Centers (NOCs).
 - (2) Capable of performing the span of maritime operations (i.e. diplomacy, constabulary and military).
 - (3) With units possibly geographically dispersed.
 - (4) With units connected to each other by a variety of RF paths.

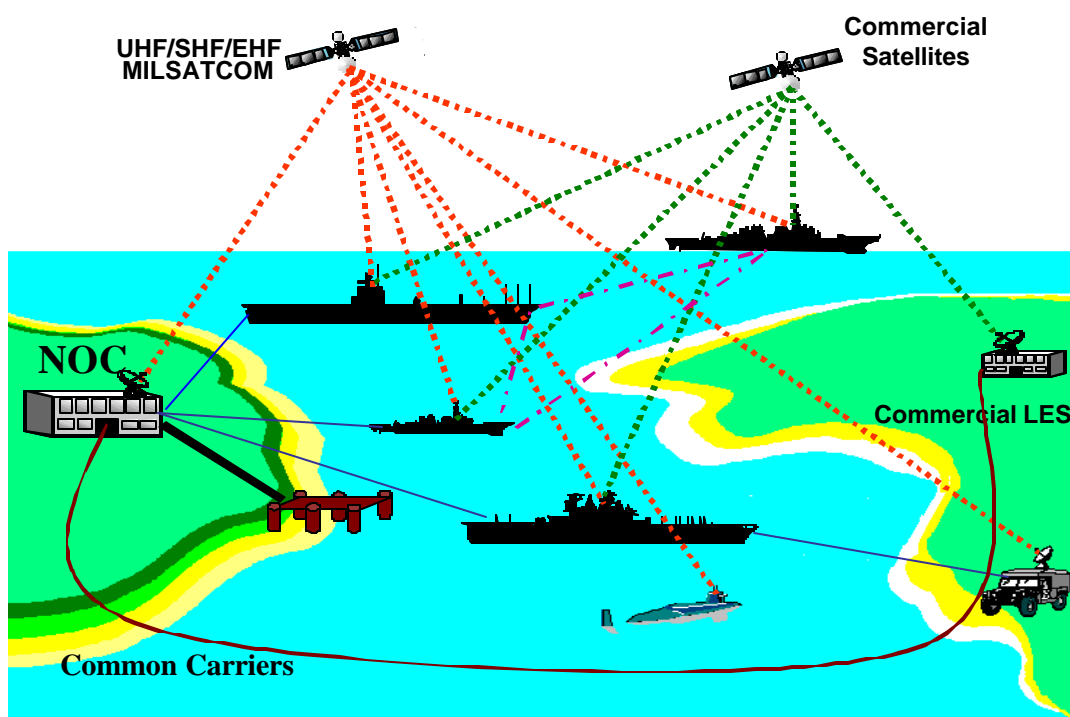


Figure 2–2 Operational View (OV-1)

- e. The end state for any MTWAN is to improve the richness and reach of planning information across the spectrum of maritime operations through IP networking.

206 SYSTEMS VIEW

- a. The MTWAN architecture is designed to maximise wide area networking capacity, efficiency, and mobility in a mobile tactical environment. The MTWAN architecture must recognize network limitations and shield them from the users. The infrastructure must be able to change quickly to accommodate intermittent connectivity; varying bandwidth, quality of service and security; and hostile environments.
- b. The following systems view provides a description of systems and interconnections to accomplish this in order to support the warfighting functions mentioned in the operational view.
- c. The first systems view (Figure 2–3) illustrates a diverse set of communication and information technology infrastructures made interoperable by resources and connectivity protocols (i.e. IP, TCP, UDP, etc). Interoperability is possible because the services and applications above the waist in Foster’s hourglass model (Figure 2–3) and communication subnets, and computer infrastructure below the waist is channeled through internationally agreed interfaces and protocols.

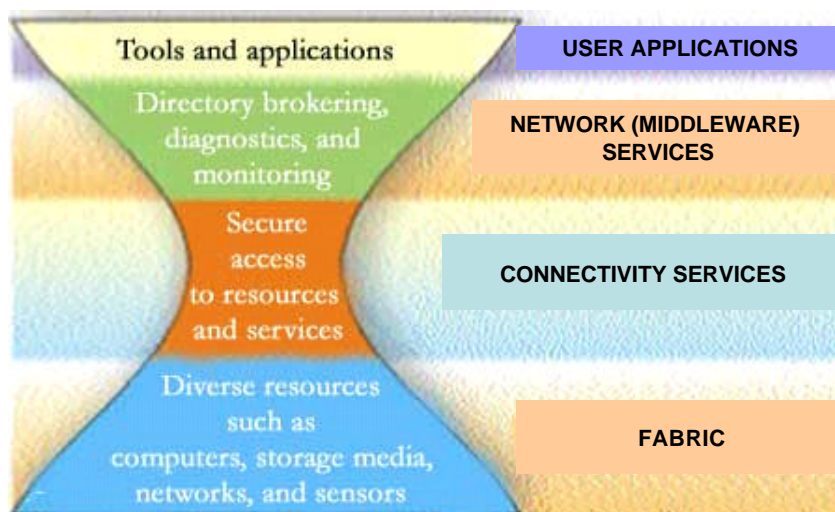


Figure 2–3 Systems View (SV–1.1)

- d. IP provides the connectivity needed by user applications and network services, while leaving all other details for definition by whatever lower-level technology is used to realise connectivity services in a particular situation. IP is a very minimal protocol and, essentially, it

only has two features—the source and destination end-node addresses carried in the datagram, and the best-effort delivery service.

- e. **Communications Architecture.** The second systems view (Figure 2–4) provides a physical and link view of system components and their interfaces within a MTWAN and also between a MTWAN and external components. In this systems view, the MTWAN is broken up into three segments: shore, space, and deployed.

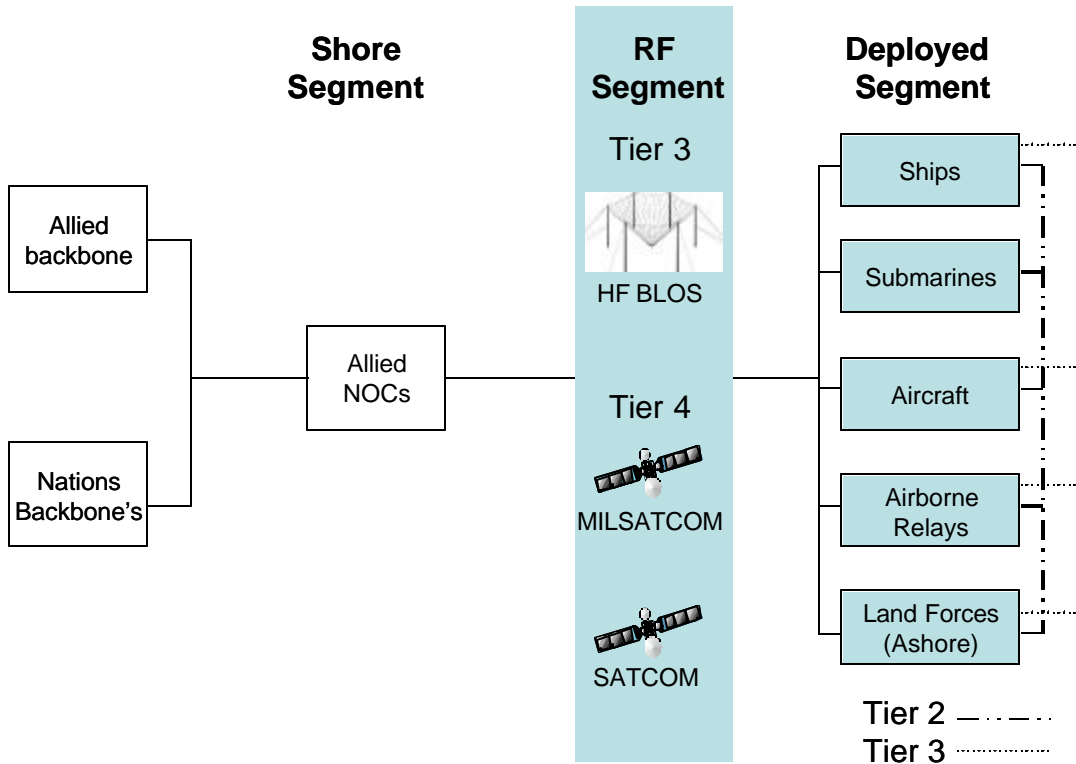


Figure 2–4 Systems View (SV-1.2)

- f. Also shown in SV-1.2 are the communication bearers that support the deployed units. These bearers are divided into four classes (tiers):
- 1) **Tier 1 (intra platform and handheld radios).** This tier includes shipboard LANs (wired and wireless) and handheld radios. As they are internal to the deployed units they are not actually depicted in the SV-1.2.
 - 2) **Tier 2 (wireless networking).** Tier 2 is networked LOS and

BLOS communications between platforms and expeditionary forces ashore.

- 3) **Tier 3 (wireless trunking).** This involves trunked LOS and BLOS communication links, which provide point-to-point connectivity, such as HF BLOS and Digital Wideband Transmission System (DWTS).
- 4) **Tier 4 (satellite communications).** This involves military and commercial geosynchronous satellites, such as UFO, GBS/TBS, DSCS, CWSP, IRRIDIUM and INMARSAT.

A more detailed explanation of the tier system is provided in Chapter 16 (Communication Subnets).

- g. Currently IP connectivity between maritime units (the “as-is” architecture) is achieved by ship-shore point-to-point, or point-to-multipoint satellite communications links (i.e. Tiers 3 and 4).
- h. However, the key to the success of the maritime communications system is making effective use of all available RF assets (i.e. Tiers 2, 3 and 4). In this regard, the MTWAN seeks to provide a seamless architecture between multiple maritime units networked with differing communications capabilities. An important key to this will be LOS wireless networking (Tier 2) capability such as Sub Net Relay (SNR) whose technology is being validated.
- i. This “to-be” architecture emphasizes dense and mesh connectivity. Unlike traditional wireless networks that have a rigid point-to-point or point-to-multipoint structure providing a hub-spoke topology, these networks offer multiple redundant paths and load sharing.
- j. **Routing Architecture.** In terms of the tier system, the MTWAN should route traffic over the lowest tier, whenever possible, in order to mitigate congestion at the higher tiers and make better use of available RF bandwidth.
- k. The third system view (Figure 2–5) presents a MTWAN in terms of network topology. SV-1.3 illustrates that a typical MTWAN consists of one or more Autonomous Systems (AS), each of which in turn comprises a collection of allied units and possibly shore communication stations all connected by a collection of backbone subnets. The MTWAN may be connected to a larger allied network.

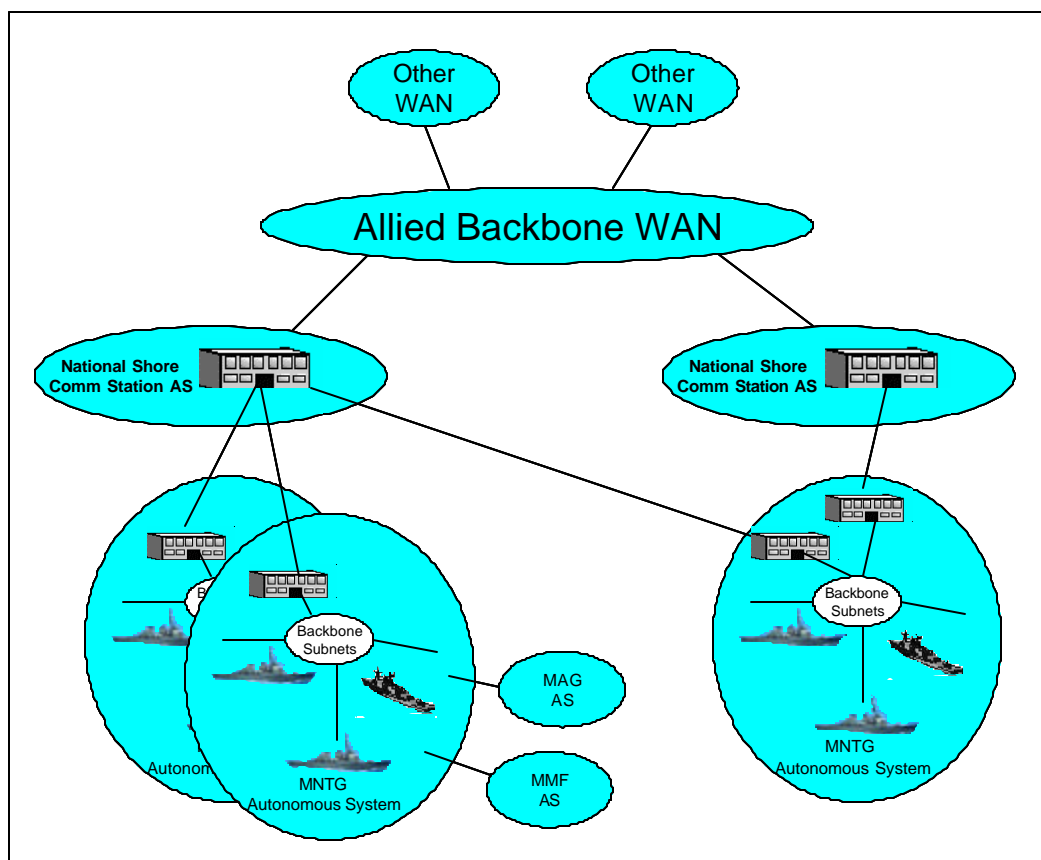


Figure 2-5 Systems View (SV-1.3)

- l. The implementation of a robust and efficient MTWAN and the provision of a better than 'best-effort' level of service will become essential as data, video and voice are converged onto a single network.
- m. **Security Architecture.** The SV-1.3 also represents a secure network established at a Secret-High level. A single security domain at the Secret-High level, as opposed to multiple security domains, enables the timely and efficient exchange of data and reduces network complexity.
- n. Approved Boundary Protections Devices (BPD) can be used to allow information to be exchanged between National and Allied domains of different security levels. These may include physical separation (air gaps) policies, approved security guards and firewalls.

- o. The 'to-be' multi-level security architecture will be dependent on the development of Multi Level Security (MLS) products. As BPDs and multi-level security systems become available to nations, policy regarding information flows between national and allied networks should allow for more efficient use of communication resources to meet both allied and national requirements. Until then, nations will have to support separate networks for each security domain.
- p. **Applications / Information Types.** The network should support the following information types and applications:
 - 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.

207 TECHNICAL VIEW

- a. The technical view provides the technical foundation for interoperability and the seamless flow of information between maritime forces. Specifically, it provides the minimal set of rules and standards governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure the interoperability among allied units. The technical view is illustrated in Figures 2-6 and 2-7; and is shown to include technical standards, conventions, and rules that govern services and interfaces to support the establishment and operation of a MTWAN.

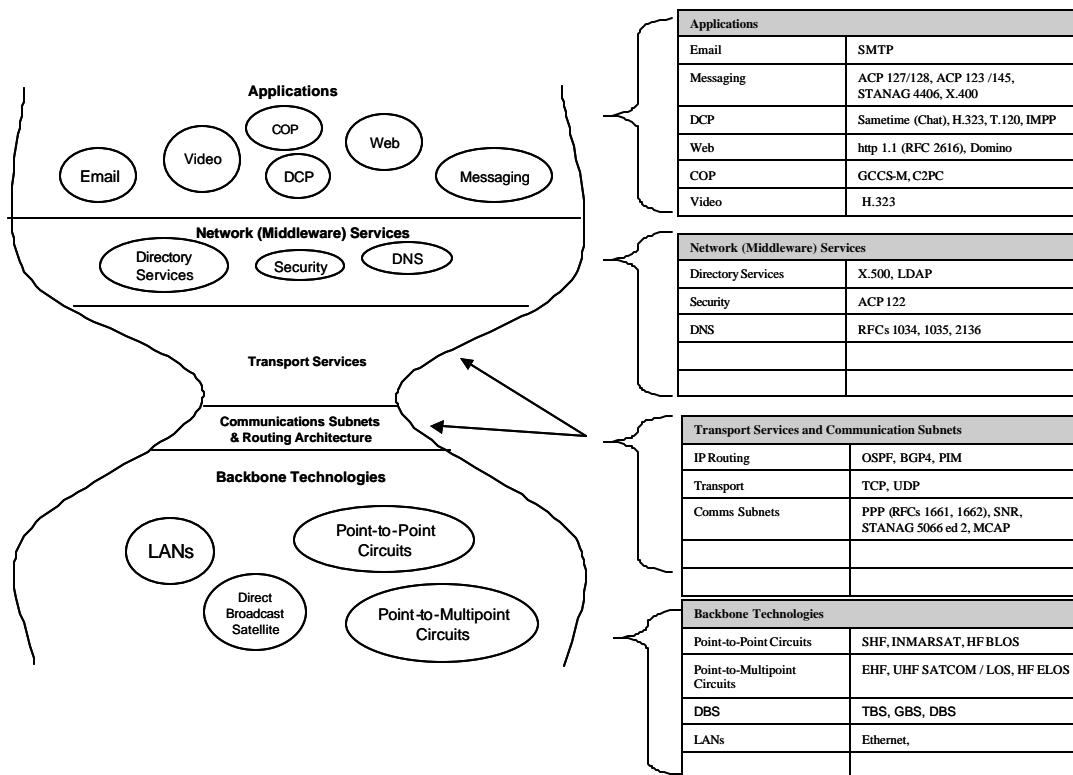


Figure 2-6 Technical View (TV-1.1)

- b. The Communications Subnets, Routing Architecture and Transport Services are the most important layers in a MTWAN technical view. These layers provide a scalable, flexible, interoperable architecture that support a variety of end-user applications and backbone technologies.
- c. The implementation of applications and network services in maritime tactical WANs may differ to this publication; and not all backbone technologies listed in TV-1.1 may be employed. Any such differences will be reflected in local network handbooks or supplements to ACP 200. Also, not all end-user applications, network services and backbone technologies are listed in TV-1.1.
- d. **Routing.** A MTWAN may comprise one or more Autonomous Systems (AS). Open Shortest Path First (OSPF) and Protocol Independent Multicast (PIM) will be used for interior routing within an AS, and Border Gate way Protocol (BGP4) for exterior routing between ASes. Figure 2-7 depicts a single-AS MTWAN that is divided into a number of OSPF areas. LAN-to-LAN connectivity is provided by the backbone subnets. Details on MTWAN routing can be found in Chapter 15.

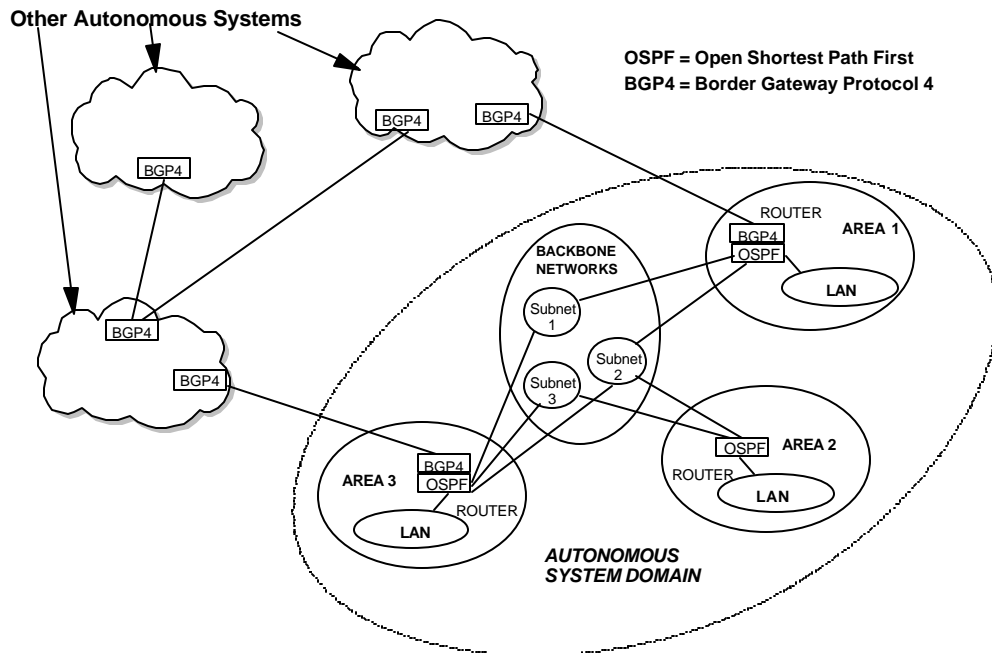


Figure 2-7 Technical View (TV-1.2)

- e. **Communication Subnets.** As shown in Figure 2-7, sending information to a destination on a different LAN, which is itself a subnet, will rely on the forwarding service provided by routers. The routers are connected to each other via the MTWAN backbone subnets and each is supported by a communication circuit. Some communication subnets, such as those supported by UHF LOS, HF and UHF SATCOM, require special equipment to interface communication systems to the routers. Details on the communication subnets can be found in Chapter 16.
- f. **Transport Services.** Most end-user applications use Transmission Control Protocol (TCP) as the transport layer protocol. However, TCP performs poorly over satellite and multi-member subnets due to long delay and large jitter. As a result, utilization of available bandwidth by applications is low. Some form of TCP Proxies can be used to improve data throughput for applications over the available communication bandwidth.
- g. Multicast (one-to-many) provides an alternative solution to efficient use of bandwidth. As most information transfers within a MTWAN are multicast in nature and the transfers mostly take place over point-to-

multipoint communication subnets, multicast will save a significant amount of the available bandwidth. Efficient information transfers using multicast have been proven in JWID using the multicast gateway P_MUL for email and MSeG for email, COP, engineering text chat and file transfers. Details on the use of multicast can be found in Chapter 13.

208 CONCLUSION

The MTWAN provides a scalable, flexible, interoperable architecture that support information sharing within a maritime force. The MTWAN improves the richness and reach of planning and coordination information across the span of maritime operations.

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

This Chapter promotes 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

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 illustrated in Figure 3-1.

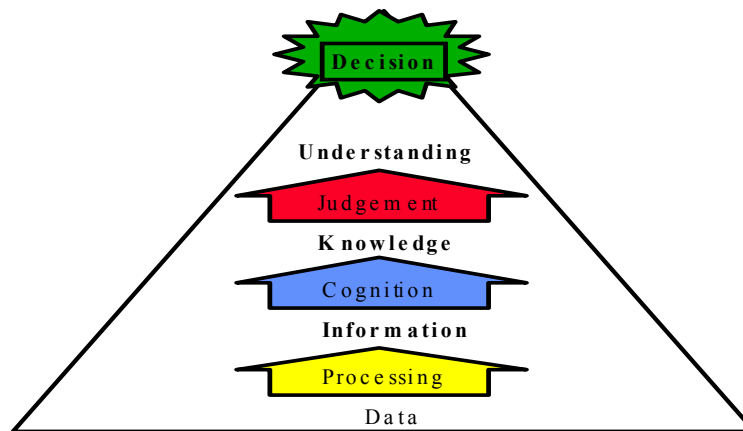


Figure 3-1 IM Hierarchy

304 DEFINITION

IM is a set of integrated management processes and services, that enable or allow information producers and consumers 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.

305 PRINCIPLES

The management of information quality requires a shared concern and pride in quality among information producers and consumers at all levels of Command. The following principles guide best practice in this respect:

- a. **Relevance.** The information should be of sufficient value that it influences the plan or mission. (i.e. the information should address the real needs of the user.)
- b. **Accessibility.** Information has multiple, even simultaneous uses. Therefore, information should be available to all people that have a legitimate need to know.
- c. **Accountability.** Individuals are responsible for protecting the confidentiality and integrity of any information they create, utilise, receive, store, or send.

- d. **Integrity.** Information must be accurate and complete, and requires protection from unauthorised, unanticipated or unintentional modifications.
- e. **Clarity.** Information should be presented to users in a way that they can understand, and properly use and analyse the information.
- f. **Timeliness.** Information is inehaustible, but its value may perish with time. Rarely is information of value if it is out of date or reaches the decision-maker late. Timeliness is typically involved in a trade-off against *accuracy*. The timeliness of information will also influence its *relevance*.
- g. **Consistency.** Values and defintions of data must be maintained consistently to ensure that information is understood in the same way when it is shared. Implicit in this is that the data should ideally be correct.

306 FITNESS OF INFORMATION

- a. Most of the above principles are also reflected as dimensions that affect the fitness or quality of information (Figure 3-2). These dimensions often overlap and are often interrelated. Actions taken to address one dimension of quality may affect other dimensions, often in ways that cannot be fully predicted.
- b. 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.

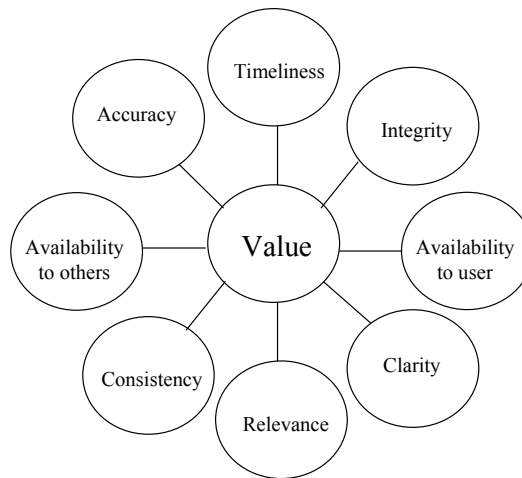


Figure 3-2 Determinants of Information Value

- c. **Clarity / Interpretability.** Information has to be well organised and presented so that the human beings can use it effectively. Unlike computers, human beings do not simply manipulate numbers according to predefined mathematical rules. They are more adept at recognizing patterns of information and comparing them with past experience or training. Consequently, the way that information is presented needs to focus on displaying those patterns explicitly and without requiring the user to waste time and effort in peripheral tasks, such as extracting information from unformatted text. Figure 3-3 is notional, intended to make the point that pictures are better than words most of the time and that formatted presentations are easier to work with than simple narrative text.

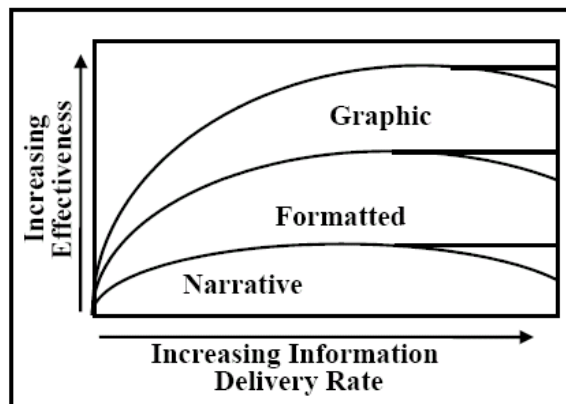


Figure 3-3 Impact of Presentation Form

307 C2 DECISION CYCLE

The C2 decision cycle describes how information contributes to the Command and Control decision-making process. Often described as a series of sequential steps similar to Figure 3-4, 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 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 synchronise these cycles so decision cycles are compressed.

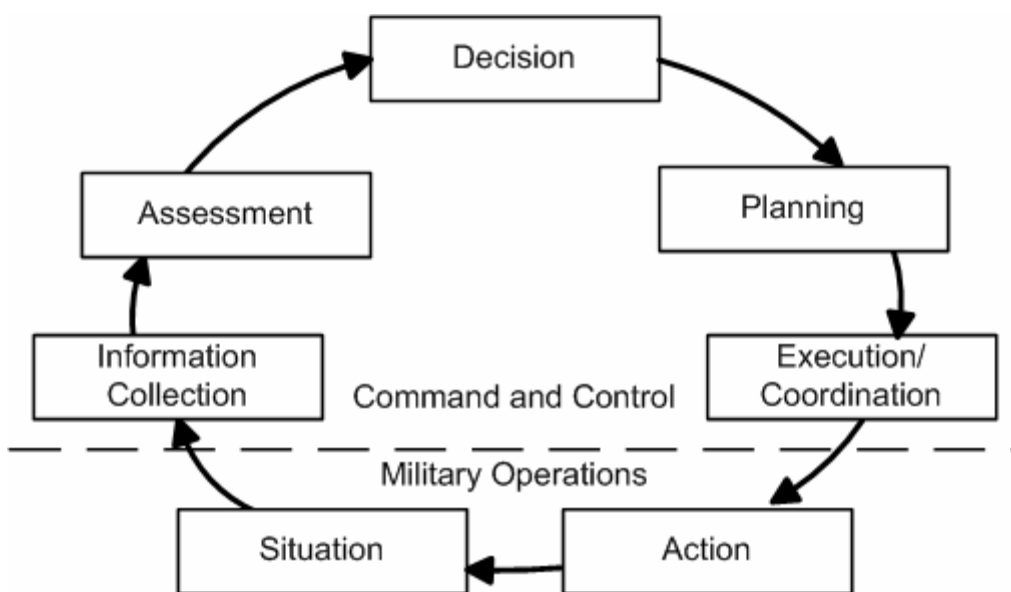


Figure 3-4 C2 Decision Cycle

308 INFORMATION REQUIREMENTS

- a. **Filtering.** The use of appropriately skilled staff or technology to remove unwanted information according to predetermined criteria set by the end-user.

- b. **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 customised according to the user's needs.
- c. **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.

309 INFORMATION DISSEMINATION MANAGEMENT (IDM)

- a. IDM is the subset of IM that addresses the end-to-end flow of information—specifically, the compilation, cataloguing, caching, distribution and retrieval of data (Figure 3-5). The goal is to provide a managed flow of relevant information based on a commander's mission. This is often referred to as providing the right information to the right place at the right time in the proper format.

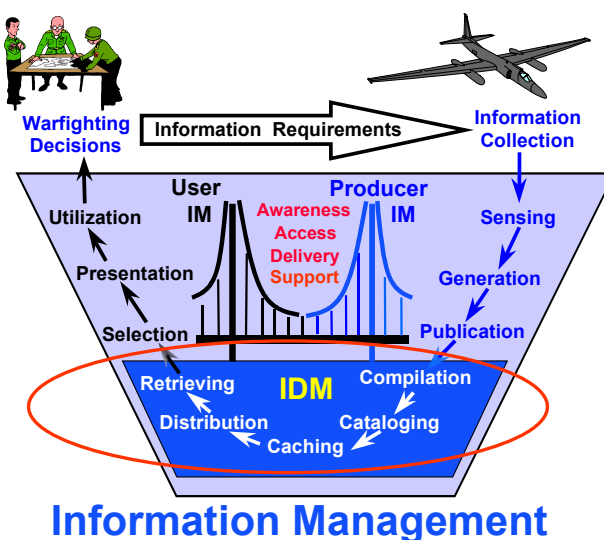


Figure 3-5 IDM

- b. This end-to-end flow of information includes both the flow of information between subordinate and superior commands (i.e. vertical flows) as well as between peers across the command structure (i.e. horizontal flows). IDM requires information 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) **Accessible.** To support concurrent or parallel planning and mission execution information needs to be accessible to a wide range of information consumers.
 - (3) **Fused.** Users receive information in many kinds of formats; from many separate sources, via a range of media. Fusion is the logical blending of this information from multiple and disparate sources into an accurate, concise, and complete picture / summary.
- c. **Distribution / Retrieval of Information.** Information can be positioned properly through push or pull mechanisms.
- (1) **Push.** Information necessary for decision-making is *directed* (or forced) from the originator to the recipient(s). This can 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 (i.e. when a covert EMCON plan is in force).
 - (3) The decision to push or pull can be influenced by:
 - (a) The relevance of the information;
 - (b) Information producer and consumer situational awareness level. (i.e. Is the information producer aware of the relevance of the information? Is the information consumer aware that the information is available?); and
 - (c) The network infrastructure available and emission control state in force (i.e. a broadcast system may be the only available asset or a COVERT EMCON policy may preclude other means).
- d. **Information Dissemination Plan (IDP).** A Commander's dissemination policy is captured in the IDP. An IDP describes how the flow of relevant information necessary to support the mission will be managed. It may include the following information: the promulgation of authoritative data sources; required reports and submissions; unique characteristics of the information architecture; push / pull guidelines and procedures to be

followed. More detailed information as to the contents is provided at 3A05(d) and in Table 3-A-1.

- e. Commanders have an important role in the development of the IDP. They 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. Further information on the IDP is provided at the Annexes.

310 INFORMATION TOOLS

- a. People have always used information tools—paper and pen are among the earliest and are still used. The rapid development of computing and telecommunications, however, has made possible an unprecedented range and variety of information tools, some of which are discussed in Chapters 6 through 9.
- b. Information tools are themselves both products and determinants of sense-making. Tools are not neutral. Information tools rely upon and reify a conception, not only of how people do information work (such as searching for information), but also of how they do their work, how they map their cognitive domain, and they make sense of their situation.
- c. Changing the information tools available can change users' goals (for their work, or for their information tasks), cognition (how they understand their task, their context, and the data), behavior (their work, and their information seeking and use), and their relationships and interactions with their environment. Information systems can alter the relationships between users and tools, and the techniques, and systems for data interpretation. In other words, altering the tool can alter the cognitive work. For instance, a decision to promote the use of Web Services (and TTPU: Task, Post, Process, Use) vice email could lead to a greater culture shift in freeing information and make it immediately available.

311 INFORMATION IMPEDIMENTS

Impediments / challenges for improvements in information management are:

- a. **Information Overload.** Overload occurs when the amount of information received exceeds the ability of users to process it. This can be the result of ambiguous, duplicate, irrelevant or outdated information. It can also occur when information preparation such as tailoring and fusion has failed.

Overload can adversely affect IM processes and decrease situational awareness.

- b. **Infrastructure Availability.** The network must have sufficient capacity and fail-overs to meet peak demands.
- c. **Information Accessibility.** Information should be accessible regardless of its location, timeliness, and ownership.
- d. **Resources.** The previous two points reflect that a significant feature of information management is the balancing of information quality objectives against the constraints of financial and human resources, and competing demands for more information.
- e. **Information Management Culture.** An IM culture is required to promote and implement IM best practices. Developing a culture that embraces IM will take much longer than actually deploying the technical infrastructure. Education and understanding at all levels is required before substantial gains in information sharing can truly be enjoyed.

312 CONCLUSION

Information has always been a source of power, but it is now increasingly a source of confusion. Understanding and implementing the concepts of this chapter will reduce confusion and allow the ready assimilation and use of information by the warfighter to enhance decision-making.

INFORMATION MANAGEMENT SOP

3A01 INTRODUCTION

- a. The capacity to generate and disseminate information needs to be balanced against the human ability to process it and take advantage of it. The key role of IM to mission success has been identified in the covering chapter to this annex. Lessons that are learnt, and in cases re-learnt in operations and exercises; and the implementation of various information systems continue to show both the advantages of good IM, but also the consequences of deficiencies in our ability to manage this commodity. The following procedures will assist the warfighter in effectively and efficiently managing information.
- b. These procedures will be more effective if a shift in training and culture accompanies it. IM requires an enterprise-wide Navy response.

3A02 AIM

This Annex establishes 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. Redundant, duplicate or irrelevant information should be eliminated. Out-of-date data should be archived.
- b. Information is to be tailored.
- c. Data definitions are 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, is effective, and is periodically tested.
- f. Information is to be gathered and maintained in compliance with relevant legal, security and data protection obligations.

UNCLASSIFIED

Annex A to Chapter 3 to ACP 200(A)

- 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 unauthorised 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.

UNCLASSIFIED

Annex A to Chapter 3 to ACP 200(A)

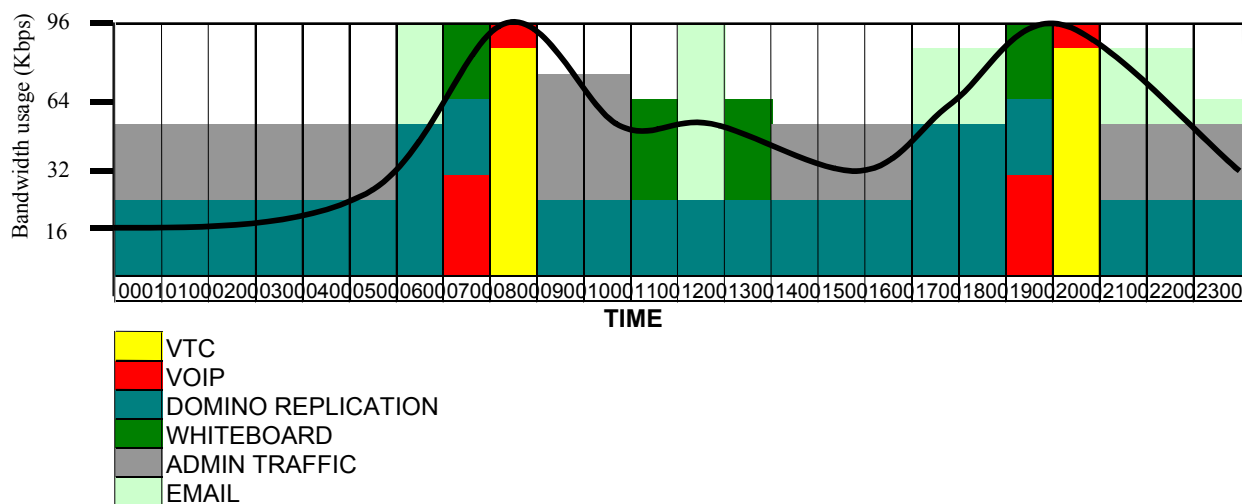


Figure 3-A-1 Daily Operations Cycle (Notional)

- 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) should also be timed for quieter periods.
- c. An Information Dissemination Plan (IDP), such as Table 3-A-1, can help to regulate the flow of information and assist information producers and consumers in storing and locating information. Additionally, authoritative information sources, information awareness, information access and delivery and support requirements become more readily apparent to the information consumer.
- d. The IDP is a dynamic document and is likely to change throughout an Operation or Exercise.
- e. 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

UNCLASSIFIED

Annex A to Chapter 3 to ACP 200(A)

(N/A) for nonrecurring reports.

- (4) **Posted NLT.** Time to post the report for review.
- (5) **Where Posted / Transmission Type.** The discussion group or web page location to post the report, or the electronic method the information was distributed (i.e. web, e-mail etc).
- (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) **Action Addressees.** Lists those that are required to action information that is provided within the document.
- (10) **Info To.** Lists information addressees.

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	As	As	Web Site	Routine	CTG	As

UNCLASSIFIED

Annex A to Chapter 3 to ACP 200(A)

Report Title	Submitted by	Submit As Of	Arrive NLT	Transmission Type	Precedence	Addressee	Info To
	Commander	required	required	(OPTASK folder)		CTU	required
Wx Observation	MET Guard	1200 2359	1300 0100	Email (Action) Web Site (METOC folder) for info addressee	Priority (action) Routine (info)	All units	

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

3A06 OPTASK IM

- a. The OPTASK IM incorporates the best IM practices from AUSCANNZUKUS navies to produce a 'Best of Breed' document suitable for establishing IM policies for a network or series of related networks. The OPTASK IM may be employed for a particular operation / exercise or as a Standing OPTASK IM.
- b. Annex B provides guidance as to the information that can be used for an OPTASK IM, while Annex C is an example of an OPTASK IM. Read together, these annexes inform task units of their IM requirements. Mandatory and optional fields are indicated for guidance.
- c. As it stands, the OPTASK IM is in a free text message format. Plans are underway to develop a Message Text Format (MTF) variant for publication over the next publication revision cycle.
- d. **Promulgation.** CTF or possibly CTG, CWC, IWC would normally be responsible for developing and promulgating the OPTASK IM.

3A07 POWERPOINT

PowerPoint is widely employed as a briefing tool. Annex D describes best practices to be used when producing PowerPoint presentations. Commanders may provide further instructions in terms of format within the OPTASK IM.

3A08 MINIMISE

- a. Minimise limits or curtails the transmission of routine administrative traffic in order that information essential to the current operation /

UNCLASSIFIED

Annex A to Chapter 3 to ACP 200(A)

emergency / exercise can be transferred. Traditionally, employed in messaging systems, it can be used effectively across information systems.

- b. Minimise will be imposed by a high level authority and can 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”.

3A09 FILE NAMING CONVENTION

- a. Users should focus on providing a meaningful description as the file name. The document naming convention allows other users to locate, read and ascertain exactly WHAT it is, WHEN the file was created, WHO created it, and the CLASSIFICATION.
- b. The following naming convention is to be used:
 - (1) Name — provide a meaningful name (e.g. INTSUM)
 - (2) Date — This date may be the date that the document was signed, or the brief was presented, or the authoring date. The date format should be DD/MM/YY. If the year is unnecessary it does not need to be included.
 - (3) Author — who created document (e.g. J2)
 - (4) Classification / Releasability abbreviations — as detailed in the OPTASK IM. Eg U = UNCLASSIFIED
- c. An example of what an INTSUM document created on 21MAY05 by the CJTF 950 Intel Department that is UNCLASSIFIED could look like: INTSUM_21MAY_J2_U.

OPTASK IM (INSTRUCTIONS)

A. OVERVIEW

A1. Purpose (*mandatory*)

State the purpose of this OPTASK IM.

A2. References (*mandatory*)

List appropriate references. This will normally include the OPGEN, and OPTASKS Comms, Net, Link and FOTC.

A3. Scope (*mandatory*)

Stipulate the operation or exercise and the effective period for the OPTASK.

B. INFORMATION EXCHANGE REQUIREMENTS (IER)

B1. Remarks (*optional*)

An optional set format that allows Commanders to emphasize specific aspects. It can be used to explain the intent behind the policies listed below.

B2. Objectives (*optional*)

List the objectives of this OPTASK IM.

B3. Information Dissemination Plan (IDP) (*mandatory*)

An IDP regulates information flow, promotes authoritative data and advertises the availability of information. Provide in set or table form key information IAW guidance provided at Annexes A and C.

B4. Priority of Service (PoS) (*mandatory for QoS enabled networks*)

This set format established the Command priorities for applications and services. It will be used to inform QoS settings. The table below provides a key / shorthand for use in this set. This can be added to by the inclusion of an amplification remark located within brackets immediately after the letter identifier. e.g. I/A/F (CAS)/G/ F/C/Q/P means priority one is Chat, two is Classified Email, three is CAS, four is COP, five is all other Military Web Servicesetc

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
	P. VTC

H. Internet Browsing	Q. POTS
----------------------	---------

C. ELECTRONIC EXCHANGE POLICIES

C1. **Remarks** (*optional*)

An optional set format that allows Commanders to emphasize specific aspects. It can be used to explain the intent behind the policies listed below.

C2. **File Size** (*mandatory*)

Stipulate the maximum permissible file size for email attachments and if necessary for web pages / links. It is unlikely that there will be a uniform policy across a TF due to the different IER for platforms and communication capabilities. i.e. Force level ships can be expected to have greater Information Exchange Requirements and communication capabilities than unit level ships.

C3. **Attachment Policy** (*optional*)

All attachments are to be scanned for viruses prior to transmission. Stipulate the file extensions permitted. It is possible that different guard rule sets will be enforced within nations and possibly between enclaves. In such cases the OPTASK should clearly list the attachment policy for each domain if relevant.

C4. **Compression Policy** (*optional*)

File compression results in a reduction in required storage space and bandwidth for transmission. Stipulate any file compression policy to be adopted. For instance large files could be ZIPped. Any network compression measures will be detailed in the OPTASK NET.

C5. **Special Caveats** (*mandatory*)

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).

C6. **OPSEC / River City Procedures** (*mandatory*)

Stipulate OPSEC requirements. This would normally include River City procedures, these can be articulated within the OPTASK IM, but it will raise the classification level of the signal. Alternatively the OPTASK IM can reference River City procedures.

C7. **Minimise Procedures** (*mandatory*)

Stipulate the authority and procedure to be followed for Minimise.

C8. **Web Services** (*optional*)

Web Services promotes authoritative data and its reuse and allows information consumers the capability to access the data they need, when they need it, from wherever they are. This set format allows the Command to emphasis key aspects of its web services

UNCLASSIFIED

Annex B to Chapter 3 to ACP 200(A)

strategy. It is a repeatable set that can be employed to distinguish each separate web service.

C9. Replication Policy (*mandatory*)

Stipulate how often web sites should replicate and provide indication of likely replication times across the TF/TG (see paragraph 8A05(e)) for explanation on replication). Include other pertinent information.

C10. Messaging (*mandatory*)

Detail the authority for which each media type can be used by drawing from the below two tables. i.e. B5 means that the Commander has approved that information up to regular operational orders can be disseminated and acted upon if received by email accompanied with PKI (without any other verification).

Message Format	
A	Email
B	Email with PKI
C	Web Page Messaging
D	Web Replication
E	Web Replication with PKI
F	ACP 127/128
G	CHAT
H	VoIP

Content	
1	Administrative and Non Mission Essential Traffic
2	Executive Orders, Mission Essential Traffic, Acknowledgement (& inclusive 1)
3	Administrative and commonly promulgated Orders (& inclusive of 1 & 2)
4	Administrative and commonly promulgated Orders (& inclusive of 1 – 3)
5	Regularly promulgated Operational Orders (& inclusive of 1 – 4)
6	ROE, Mission Essential Coalition Traffic (& inclusive of 1 – 5)
7	Tactical Messaging as detailed in chat policy (& inclusive of 1 – 6)
8	Tactical orders and instructions, Authenticated Formal Instructions (& inclusive of 1 – 7)

UNCLASSIFIED

Annex B to Chapter 3 to ACP 200(A)

C11 **Chat** (*mandatory*)

Stipulate chat policies. List the standard chat rooms that will be created, including indication of manning requirements.

C12 **VTC** (*optional*)

Detail VTC requirements, policies and procedures.

C13 **VOIP** (*optional*)

Stipulate VOIP requirements, policies and procedures.

C14 **PowerPoint** (*mandatory*)

Stipulate PowerPoint policies. List the standard PowerPoint policies that are to be used when creating presentations in PowerPoint and/or reference ACP 200 - Annex D to Chapter 3 (or other reference documentation).

C15 **Software** (*mandatory*)

Detail the policies and procedures for downloading and installation of software.

D. **STORAGE POLICIES**

D1. **Remarks** (*optional*)

An optional set format that allows Commanders to emphasize specific aspects. It can be used to explain the intent behind the policies listed below.

D2. **Archival Policy** (*mandatory*)

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.

D3. **File Structure Policy** (*optional*)

Stipulate File Directory structure / taxonomy to be used.

D4. **File Naming Policy** (*mandatory*)

All file names will adhere to following naming convention Name _DD/MM/YY_Author_Classification. This allows users to locate, and ascertain exactly what the file is, when the file was created, who created the file and the file classification.

E. **GENERAL**

E1. **Declassify** (*mandatory*)

Stipulate when / if and to what extent the document can be declassified.

E2. **Miscellaneous** (*optional*)

UNCLASSIFIED

Annex B to Chapter 3 to ACP 200(A)

E3. **Acknowledge** (*optional*)

Stipulate acknowledgement policy for this message.

UNCLASSIFIED

OPTASK IM (EXAMPLE)

A. OVERVIEW

A1. Purpose

The purpose of this OPTASK is to list dynamic IM issues pertinent to IP networking in the maritime tactical environment.

A2. References

- A2.1 OPGEN
- A2.2 OPTASK COMMS
- A2.3 OPTASK NET
- A2.4 ACP 200 Change 1
- A2.5 etc.....

A3. Scope

This OPTASK is specific to EXERCISE EXAMPLE and is effective from 01 DEC – 31 DEC 05.

B. INFORMATION EXCHANGE REQUIREMENTS (IER)

B1. Remarks

Improving the management of information is a responsibility that is shared by all information producers and users. The improvement in the quality of information through IM can result in better and faster decisions.

B2. Objectives

- B2.1 Users get all the information needed (but no more) in the desired context.
- B2.2 Promote authoritative data and its reuse.
- B2.3 Allow users to collaborate effectively regardless of geographic location.
- B2.4 etc.....

B3. Information Dissemination Plan (IDP)

An IDP regulates information flow, promotes authoritative data and advertises the availability of information. Read following in fields as Report/ Submit by/ Submit as of /Transmission Type/Addressee/Info To

ATO/Air Wing Cdr/1200/Web Site – Strike Ops, ATO Folder/All/-
COMM SPOT/All unit/As reqd/Email/CTG/As reqd
OPGEN/CTG/As reqd/ Web site – OPTASK folder/CTU/As reqd
OPORDERS/Originator/As reqd/Web site – ops folders/As reqd/As reqd/

UNCLASSIFIED

Annex C to Chapter 3 to ACP 200(A)

OPREP FEEDER/All units/2359/Email/CTG/As reqd
OPTASK Unit/All units/ 1200/Email/CTG/As reqd
ROE/Intel/As reqd/ Web Site – ROE folder/All units/-
WX Reports/MET Guard/1200 and 2359/Web site – METOC folder/ All units/-
...etc

Note: Alternate solution is to provide a web site location where information is provided in a more readable form such as a table.

B4. Priority of Service (PoS)

I/A/F(CAS)/G/F/C/Q/P

C. ELECTRONIC EXCHANGE POLICIES

C1. Remarks

The ease of employment of electronic exchange tools such as email and chat should not result in informality or lax practices. Best practices provided in the email and chat user guides within ACP 200 should be followed.

C2. File Size

File sizes are not to exceed 1.4 Mb for unit level platforms. Force level platforms have unrestrained use but should exercise best practices. Information producers are to reduce file sizes where possible. No unnecessary graphics are to be included. Files are to be compressed.

C3. Attachment Policy

All attachments are to be scanned for viruses prior to transmission. Allowed file extension are: CSV, DOC, GIF, HTM, JPG, PDF, PPT, RTF, TIF, TXT, XLS

Note: The file extension provided are examples and should not be viewed as definitive or approved by the respective security agencies.

C4. Compression Policy

Large files should be ZIPped. Network compression measures are detailed at Ref A2.3.

UNCLASSIFIED

Annex C to Chapter 3 to ACP 200(A)

C5. Special Caveats

The following caveats are to be implemented:

REL: AU/CA/NZ/UK/US

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

C6. OPSEC / River City Procedures

Include River City procedures.

C7. Minimise Procedures

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

C8. Web Services

Web Services promotes authoritative data and its reuse and allows information consumers the capability to access the data they need, when they need it, from wherever they are. Web editors are to ensure web pages are accurate and current on a per watch basis. Early posting of information facilitates parallel processing of information via the Task, Post, Process, Use (TTPU) model. Preference is to pass email with links vice attachments IOT promote authoritative data sources and supplant the amount and circulation of email.

C9. Replication Policy

Domino Servers are to be scheduled to replicate every 30 mins. Note: A replication policy of 30 mins means that domino server will replicate with master server every 30 mins. However, for information to transfer from one client server to another utilising a master server it will take two replication cycles (i.e. 1 hour) to receive the information as client (ship) A has to replicate with the master server (NOC) and then the master server on the next replication cycle will replicate with the second client (ship) B.

C10. Messaging

C2 information is to be disseminated IAW the following guidance: B2/E6/F6/G7/H8.

UNCLASSIFIED

Annex C to Chapter 3 to ACP 200(A)

C11. Chat

Chat will be employed to support tactical and operational objectives and may be utilised in all warfighting environments. The following chat rooms (including manning requirements) are provided:

Chat Room	Watch Requirements	Moderator	Amplifying Remarks
MIO	Guard	XJ	
C4I	Guard		
Bridge to Bridge	WHENDI		
INTEL	Listening		
Air Co-Ord	WHENDI		
High Command	Listening		
Logistics	WHENDI		
Data Link Co-Ord	WHENDI		

ACP 200 Chapter 9, Appendix 1 to Annex B (Chat User Guide) provides further guidance on the use of chat. Moderators shall maintain circuit discipline, ensure that room members are properly identified and the chat room is being used for its stated purpose. Slang and uncommon jargon should be avoided. Entries are to be time stamped in Zulu time.

C12. VTC

VTC to be only used at Commanders discretion and IAW IDP.

C14. PowerPoint

PowerPoint shall conform with best practices stated in ACP 200 Chapter 3 Annex D.

C15. Software

Software is not to be downloaded and installed by unauthorised personnel. Units are to ensure that they have the necessary software prior to exercise commencement.

D. STORAGE POLICIES

D2. Archival Policy

Records are to be retained until 3 months after the completion of OPERATION EXERCISE to allow for the compilation of lessons learnt. This does not override national archive policies which may require extend archiving.

D3. File Structure Policy

The following file structure is to be adopted

EX 05_Unit Name

UNCLASSIFIED

Annex C to Chapter 3 to ACP 200(A)

- + Administration
- + Assessreps
- + Briefs
- + N1
- + N2
- + N3 / N5
- + N4
- + N6

D4. **File Naming Policy**

All file names will adhere to following naming convention Name
_DD/MM/YY_Author_Classification. This allows users to locate, and ascertain exactly
what the file is, when the file was created, who created the file and the file classification.

E. **GENERAL**

E1. **Declassify**

Effective 31 Dec 06 this OPTASK becomes unclassified.

E3. **Acknowledge**

All addresses are to acknowledge receipt and compliance.

MS POWERPOINT

3D01 INTRODUCTION

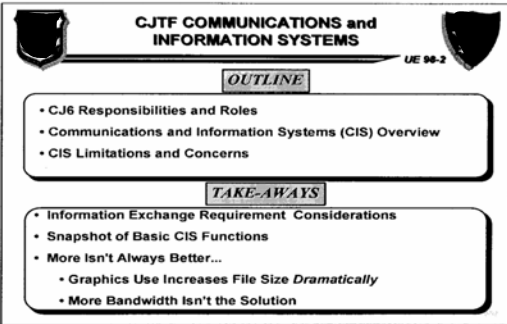
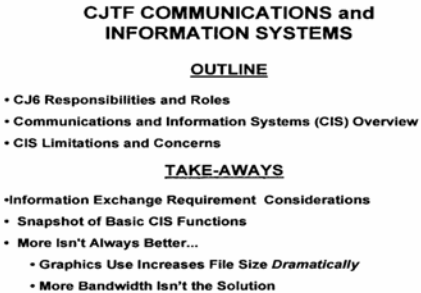
PowerPoint is widely employed as a briefing tool. However, the file size of these presentations can become exceedingly large due to sub-optimal default settings and poor practices.

3D02 AIM

This Annex provides guidance for the preparation of PowerPoint presentations to ensure the file size is manageable and practical for dissemination.

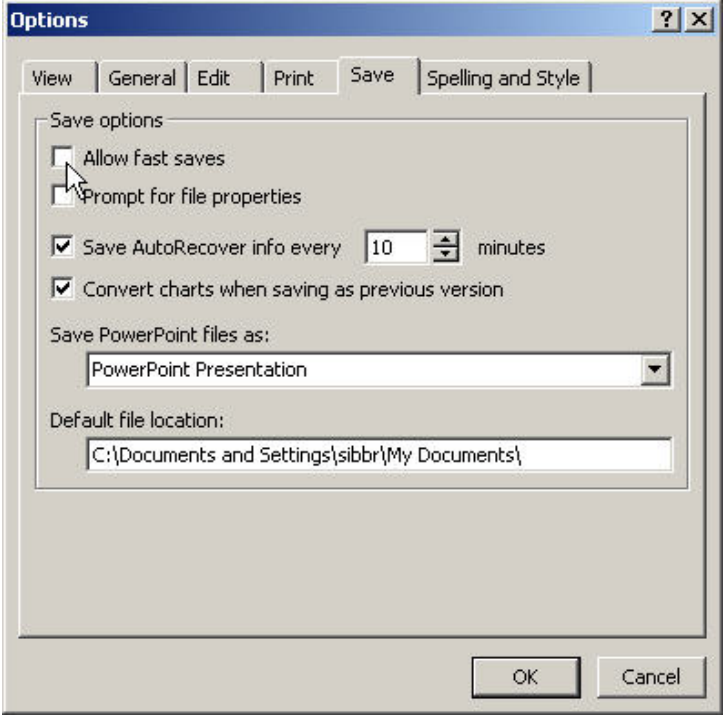
3D03 OBJECTIVE

The objective is to reduce the size of PowerPoint while not affecting the content. The below diagram highlight the consequences when these practices are not followed. The operational impact from just one slide can be significant.

CJTF COMMUNICATIONS and INFORMATION SYSTEMS	
	
With graphics, etc. 558,592 bytes	Without graphics, etc. 15,872 bytes
<i>Reduces transmission time at 64 Kbps from 70 seconds to 2 seconds!</i>	

3D04 DEACTIVATE FAST SAVE

Fast Save reduces the time to save a brief by only saving changes, but imposes additional file size overhead. Every time a brief is saved using *Fast Save*, an additional 7 KB of overhead is added to the file size regardless of what changes have been made.

<p>To disable the <i>Fast Save</i> feature</p> <ol style="list-style-type: none"> 1. Go to the “Tools” menu and select Options.” 2. Click on the “Save” tab. 3. Turn off the <i>Fast Save</i> feature by deselecting the checkbox next to “Allow fast saves.” <p>Note: The <i>Fast Save</i> feature is not used if briefs are saved using the “Save As” option from the “File” menu.</p>	
--	---

3D05 IMAGES AND PICTURES

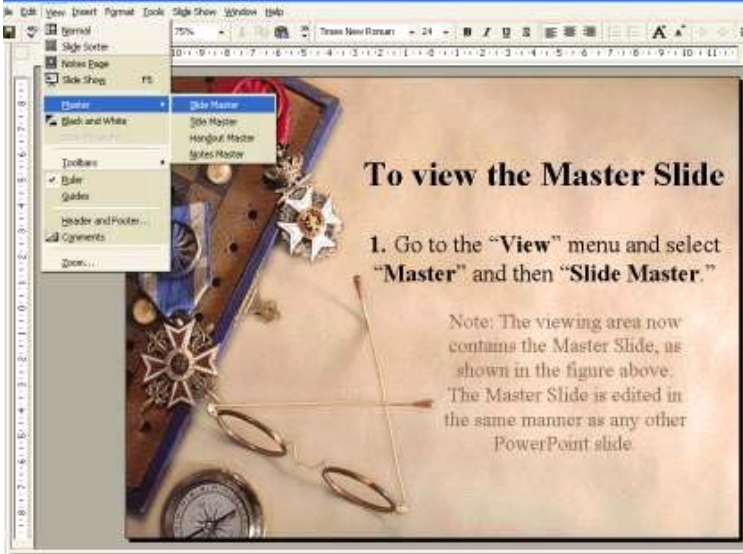
- a. Images and pictures require significantly greater memory than text. An understanding of how PowerPoint saves these images and pictures, and the application of simple techniques will reduce the memory requirements for PowerPoint presentations.
- b. **Picture / Image Utilisation.** Only images and pictures that are necessary for the clarity of the presentation should therefore be included.
- c. **Picture / Image Resizing.** Reducing the size of an image (i.e. ‘click and drag’ the corner or sides of the image window to resize) will not reduce the file size.
- d. **Backgrounds.** An image as the background for a slide should also be avoided. However, colours schemes and fill effects (such as gradient, texture, and pattern)

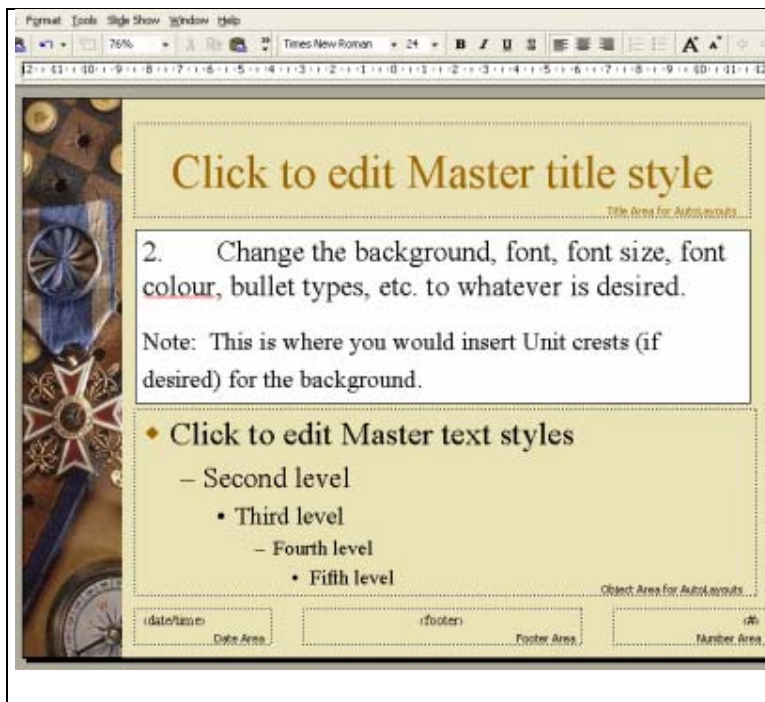
can be employed for presentational effects with little additional memory requirements.

- e. **Techniques to reduce file size.** There are a number of ways to reduce the file size of images, including:
 - (1) Cropping out background (sky, water, horizon) unless required to “tell the story.”
 - (2) Reduce the image size using compacting software (e.g. Microsoft Photo Editor).
 - (3) Use jpeg, jpg or png or other minimizing file formats.
 - (4) If available, use lower quality images (which are smaller in size).
- f. **Logos / Unit Insignias.** These should be included only in the Master Slide. If the size of the logo has to be reduced (so that it fits nicely into the corner of a slide) it should be resized in a graphics program, such as Microsoft Photo Editor.
- g. **Fonts and Colours.** There is no additional memory required by using different colours or fonts.
- h. **Bullets.** Bullet types should be set in the Master Slide and not changed in the briefing slides. The cost is about 1 KB for each deviation.
- i. **Footer Information.** Presentations should include the following information within the footer:
 - (1) Lower Left - DTG of briefing version in local time.
 - (2) Lower Centre - POC information and web posting location.
 - (3) Lower Right – Slide Number

3D06 UTILISE MASTER SLIDES

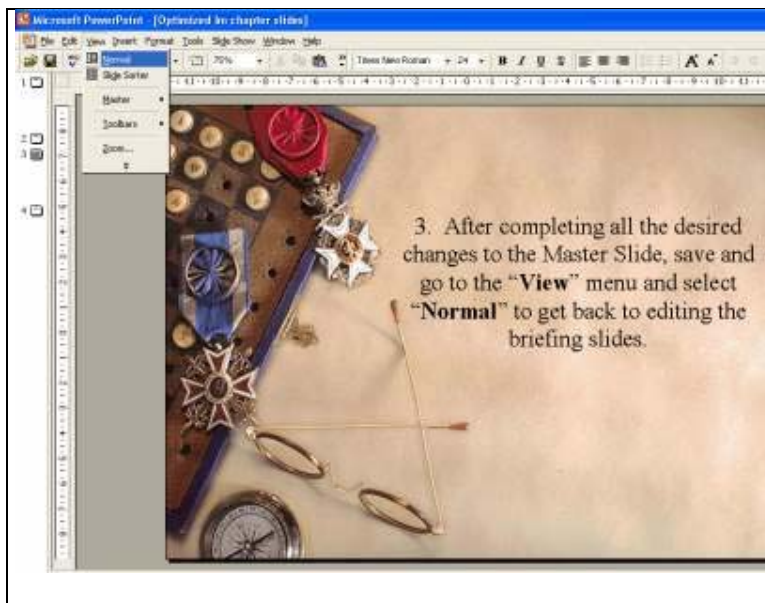
Master Slides are used to select the background, fonts, fonts sizes, bullet type, colours, etc. When these changes are made on individual slides, as opposed to the Master Slide, each change costs several kilobytes of additional space.

	<p>To view the Master Slide</p> <p>1. Go to the “View” menu and select “Master” and then “Slide Master.”</p> <p>Note: The viewing area now contains the Master Slide, as shown in the figure above. The Master Slide is edited in the same manner as any other PowerPoint slide.</p>
--	--



2. Change the background, font, font size, font colour, bullet types, etc. to whatever is desired.

Note: This is where you would insert Unit crests (if desired) for the background.



3. After completing all the desired changes to the Master Slide, save and go to the “View” menu and select “Normal” to get back to editing the briefing slides.

3D07 CONCLUSION

PowerPoint is employed regularly as a briefing tool in operations and exercises, but can be very large in terms of its file size. By following the procedures in this Annex, the size of these presentations can be reduced, without effecting the information. This promotes efficient employment of the network.

Chapter 4

SECURITY

401 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.

402 AIM

This chapter provides an overview of the security architecture and procedures necessary for a MTWAN.

403 OVERVIEW

For Combined Communications-Electronics Board (CCEB) nations, ACP 122—Information Assurance for Allied Communications and Information Systems—provides Information Assurance (IA) policies, procedures and doctrine, which enable interconnection and interoperability of IP networks. This chapter applies the policies, procedures and doctrine established in ACP 122 to maritime tactical IP networks.

404 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.

405 REFERENCE

The principal security reference for any MTWAN is ACP 122. In terms of security policies and procedures this publication is subordinate to ACP 122. Where / if any discrepancies occur, doctrine within ACP 122 should be followed.

406 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 4-1.
- 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).

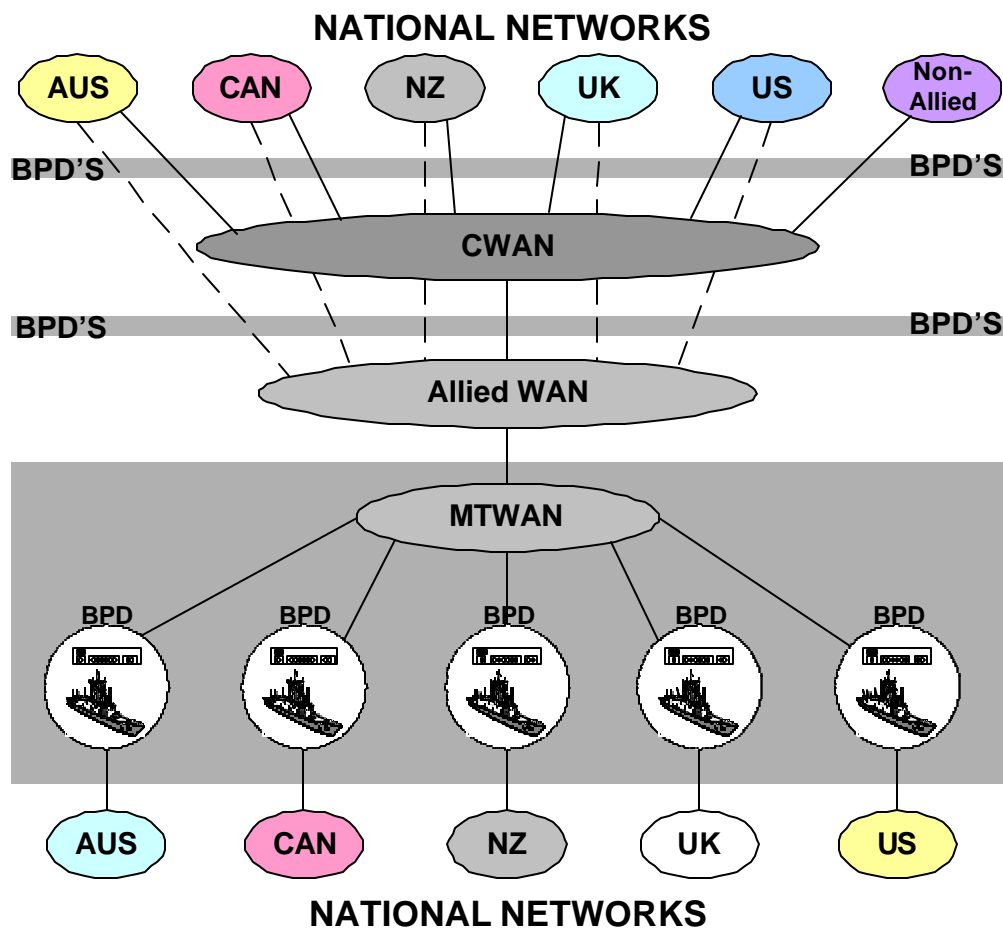


Figure 4-1 MTWAN Topology

- 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 4-1, 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.

407 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 4-2 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).

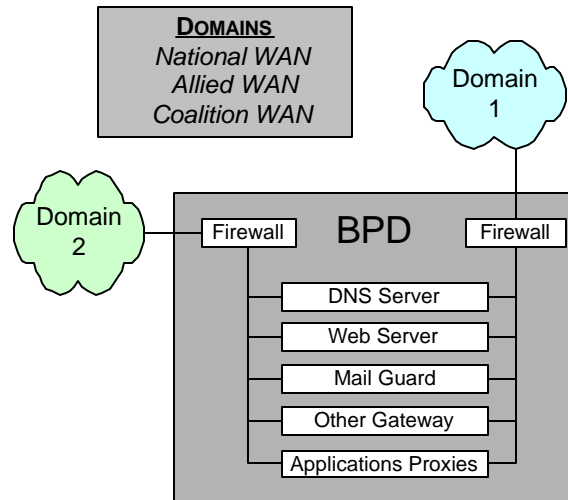


Figure 4-2 BPD between domains

- 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.

408 THREATS

Leakage of unauthorized information and penetration by unauthorized users are inherent threats 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.** The system itself or an operator, contrary to the security regulations, releases information inadvertently. A risk exists if the outbound data is transferred unscreened or without label checks, either in real time or off line.
- e. **Deliberate Leakage.** An operator, contrary to the security regulations, releases 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.

409 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.

410 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.

411 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.

412 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 4-3. 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.

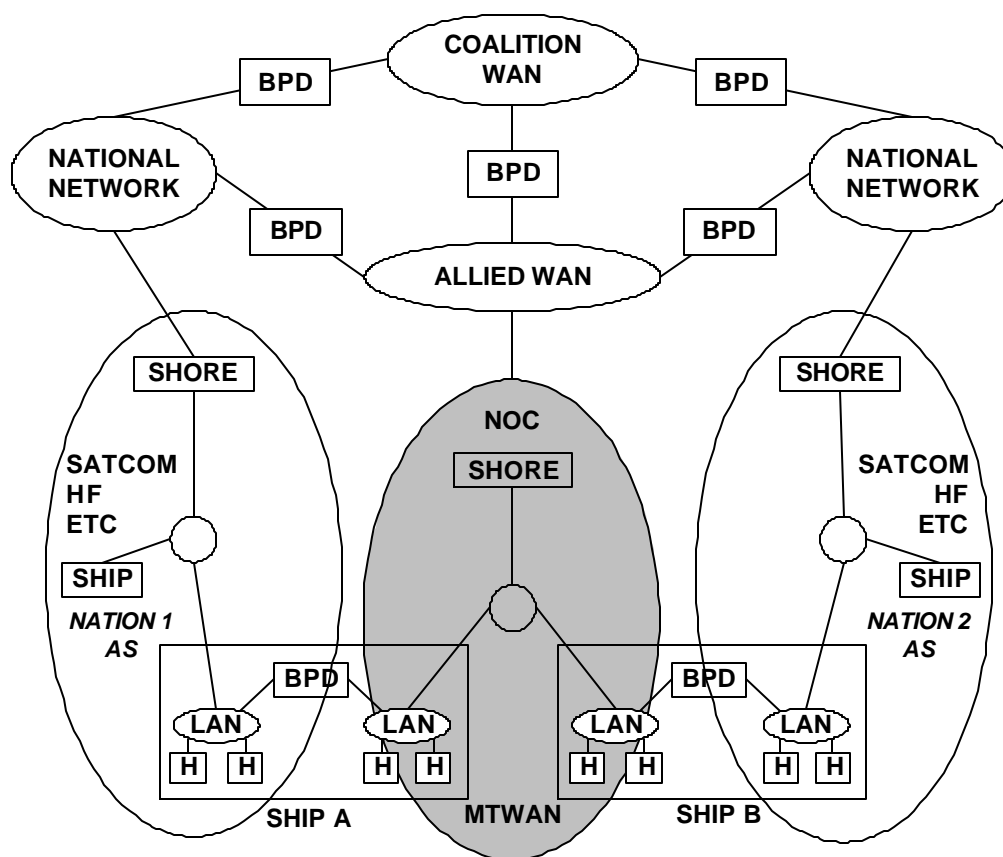


Figure 4-3 MTWAN Connectivity

- b. **Shipboard “Air Gap” Architecture.** An air gap between the National network and a MTWAN, as shown in Figure 4-4, 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 an interim solution until a faster, efficient and secure process is developed and accredited.

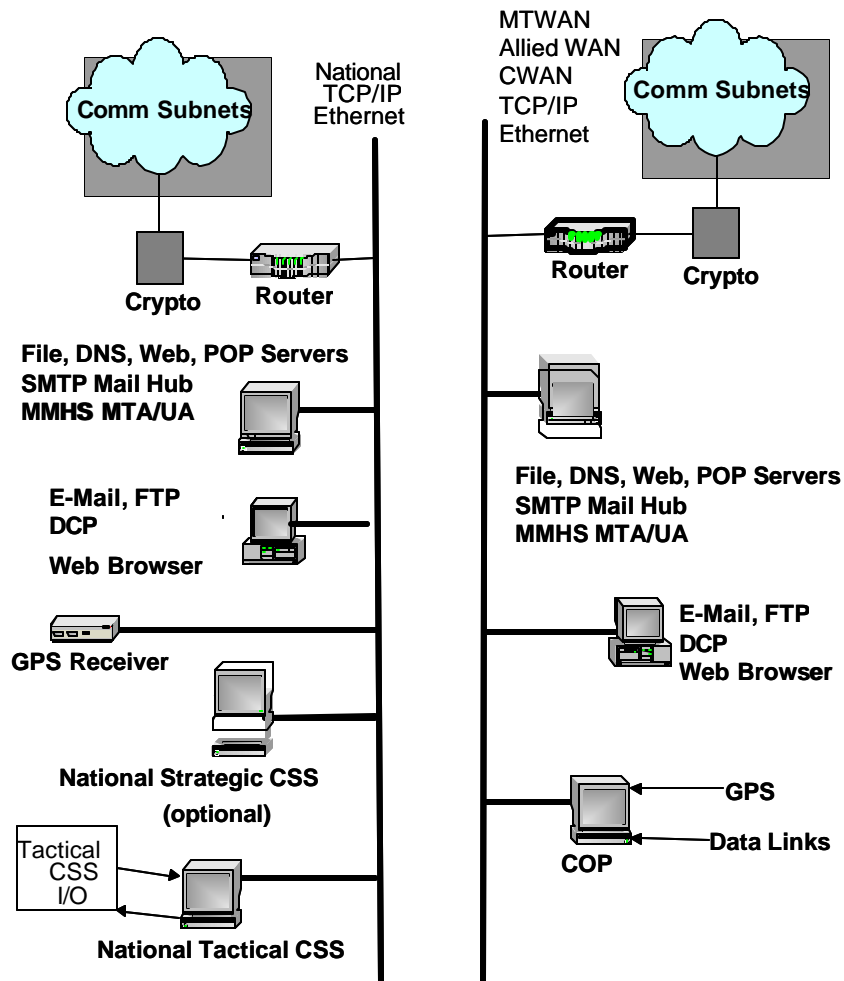


Figure 4-4 Air Gap Architecture

- 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 4-5 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.

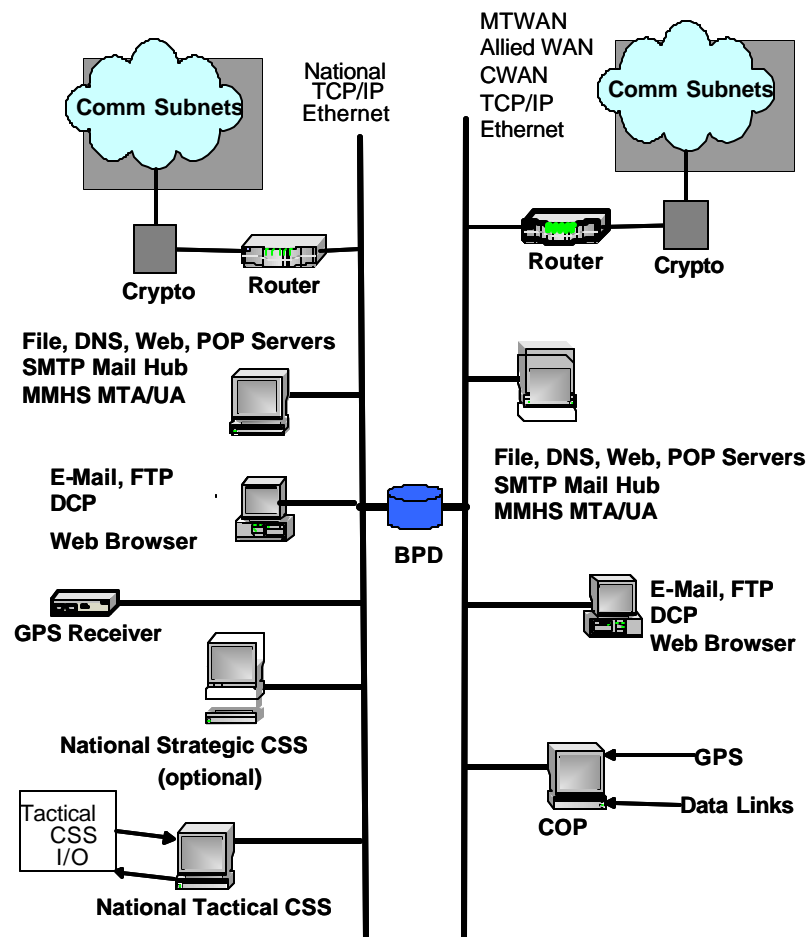


Figure 4-5 Networked Architecture

- e. A screened subnet architecture employing both network and application layer firewalls, as shown in Figure 4-6, offers a very high level of protection for the LAN from users on a remote network.

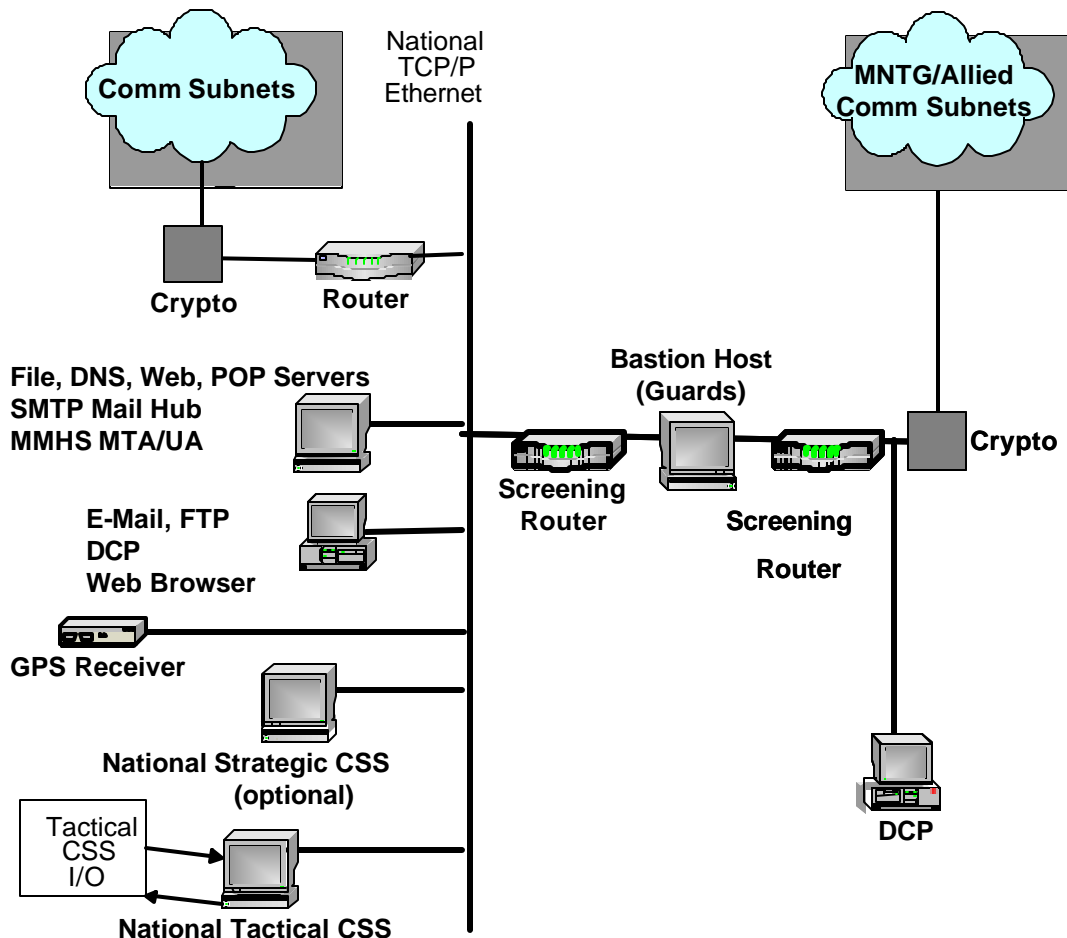


Figure 4-6 "Fully Integrated" Target Architecture

- 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).

413 ACCREDITATION

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

414 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 Five**TRAINING AND INTEROPERABILITY****501 INTRODUCTION**

The goal of interoperability is to efficiently share tactical, operational and selected administrative knowledge for planning and executing operations in a coalition environment.

502 AIM

The aim of this Chapter is to delineate common training and an interoperability level for coalition IP networks.

503 OVERVIEW

- a. Training and interoperability assessment will be a national responsibility. Nations are encouraged to conduct procedure, policy, technical and infrastructure training to support deployed operations.
- b. Interoperability level is intended to indicate the operational capability vice only technical connectivity.

504 TRAINING

Training should be focused on network infrastructure and application services to sufficiently allow operators and maintainers to establish, operate and maintain the network. It is recommended that each nation address the provision of training commensurate to the interoperability level as defined below.

505 INTEROPERABILITY LEVEL

Nations should determine and report interoperability levels to include bandwidth, WAN link capability and supported network services. This will provide the operational commander with common information sets on which to base the OPTASK IM.

506 DETERMINING INTEROPERABILITY LEVEL

- a. A unit's level of interoperability for entering a MTWAN can be determined using the tables below.

WAN LINK	
1.	BFEM-5066
2.	RF IP (Non-SATCOM)
3.	Dial-up Satellite IP
4.	Time Shared Satellite IP
5.	Dedicated Satellite IP

Table 5–1 WAN Link

MINIMUM DEDICATED BANDWIDTH	
A.	Less than 10 kbps
B.	10-32 kbps
C.	33-64 kbps
D.	65-132 kbps
E.	129-256 kbps
F.	257-512 kbps
G.	Greater than 512 kbps

Table 5–2 Minimum Dedicated Bandwidth

SUPPORTED APPLICATIONS	
Essential	Email
Basic	Essential plus Web Browser plus Chat
Advanced	Basic plus at least one of the following – RMP/COP, Whiteboard, VoIP and/or Video over IP

Table 5–3 Supported Applications

- b. The following reporting format is to be used: **WAN LINK / MINIMUM DEDICATED BANDWIDTH / SUPPORTED APPLICATIONS**
- c. Example: A ship has a leased 64kbps INMARSAT connection with access shared with another unit. It has dedicated at least 20kbps to the MTWAN when connected, using the remaining bandwidth to support national network

UNCLASSIFIED

ACP 200(A)

commitments. The unit is fitted with, and personnel are trained for, the promulgated MTWAN Email, Chat and Web Browser applications.

INTEROPERABILITY MATRIX								
DEDICATED BANDWIDTH (kbps)								
WAN LINK	A <10	B 11-32	C 33-64	D 65-128	E 129-256	F 257-512	G >512	NOTES
1. BFEM 5066								
2. RF IP (Non-SATCOM)								
3. Dial-up SATCOM								
4. Time-Shared SATCOM		B						10 hours from 1000Z
5. Dedicated SATCOM								
E – Essential B – Basic A - Advanced								
Note: The example in the matrix above is a unit with a ship with a leased 64kbps INMARSAT connection with access shared with another unit. It has dedicated at least 20kbps to the MTWAN when connected, using the remaining bandwidth to support national network commitments. The unit is fitted with, and personnel are trained for, the promulgated MTWAN Email, Chat and Web Browser applications. "4B basic"								

Table 5–4 Interoperability Matrix

507 REPORTING PROCEDURES

Once a unit's interoperability level has been determined it is to be reported up the chain of command IAW national and/or coalition procedures.

UNCLASSIFIED

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-enabled database 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.

602 AIM

This chapter provides guidance for the employment of messaging within a maritime IP network.

603 OVERVIEW

- a. ACP 127/128 provides many Elements of Service (EoS) that support Command and Control over assigned forces. These EoS, or key features include; 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-enabled database 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. Commanders should select the appropriate method for messaging dissemination taking into consideration the relative limitations of text based messaging (and its Elements of Service benefits) versus the richer attributes of multi-media messaging formats.
- g. Multicast messaging techniques offer a more efficient method of messaging over a bandwidth constrained network than current “unicast” methods.
- h. Public Key Infrastructure (PKI) may offer EoS (authentication and non-repudiation) to multi-media messaging systems.

604 TYPES OF MESSAGING

Messaging can be either text-based or multimedia formats. ACP 127/128, OTH-GOLD, and Chat messaging are text-based while email and Web services support a multimedia capability. ACP 123 (when implemented) will support message integrity, message confidentiality, non-repudiation and authentication. Robust and reliable messaging protocols and services should be used in order to reduce network congestion.

605 TEXT-BASED FORMATS

- a. **ACP 127/128.** ACP 127/128 provides many EoS, which support Command and Control over assigned forces. These EoS, or key features, include; precedence handling, Plain Language Address Designator (PLAD), and distribution by subject. 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. 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. Currently, EoS is only provided by ACP127/128 text based messaging systems.

- b. **Chat.** Text chat is increasingly being used to support Command and Control during operations. Chat provides the capability to provide short instantaneous text messages with an individual or group over an IP network. Chapter 9 (Distributive Collaborative Planning (DCP)) provides further guidance on the use of chat.

606 MULTIMEDIA FORMATS

- a. **Email.** The ability to send emails and replicate web-enabled databases within a Task Group enhances traditional methods of information transfer. Email and web-enabled database 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).
- b. 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.
- c. **Web Services.** The ability to post a message such as the Air Tasking Order (ATO) or general operational messages (OPGEN) to a Task Group 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, database replication provides increased information traceability, authenticity, and integrity over non-replicated systems. Chapter 8 provides further guidance on the use of Web Services for information exchange.

- d. 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.
- 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.

607 MESSAGING SELECTION

- a. 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 Information Management (IM) (See Chapter 3 Annex B).
- 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.
- c. The OPTASK IM should promulgate the authorized methods for executing command and control. The table below provides guidance but is not yet accepted doctrine.

UNCLASSIFIED

ACP 200(A)

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
Email with digital signature	Yes	Yes	No	No	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	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.
Text Chat with encryption	Yes	Yes	Yes	No	Chat products are available that provide 128 bit encryption ie Sametime.
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-enabled database Replication (Webpage Messaging with replication)	Yes	Yes	Yes	Yes	Suitable for commonly promulgated Orders and Schedules. Acknowledgment by action addressees required.

Information Transfer Application	Authentication	Non-repudiation	Message Confidentiality	Message Integrity	Recommendations
Web-enabled Replication with PKI	Yes	Yes	Yes	Yes	1. Suitable for commonly promulgated Orders and Schedules. 2. Acknowledgment by action addressees required. 3. PKI provides extra assuredness in Authentication and Non-repudiation

Table 6–1 Messaging Selection

608 MULTICAST MESSAGING

- a. This document describes 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 message servers 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 1100 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, such as posting information to the web for replication, is therefore advantageous.

609 PUBLIC KEY INFRASTRUCTURE (PKI)

- a. PKI can be used within 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 Kb. There is currently no stated requirement for public key encryption currently for any secure military network.

610 CONCLUSION

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. It is important that Commander's promulgate the messaging options that they intend to use for operational and administrative traffic.

EMAIL USER GUIDE

6A01 INTRODUCTION

- a. Email is a critical communication medium. Despite its prominence as a communication tool within organisations, there remains at the enterprise level, few formal email policies. Email management tends to be handled on an individual level or in the best cases at the work group level.
- b. While most, if not all, have developed personal email habits and skills, formal email guidance underpins organisational goals across the enterprise.

6A02 AIM

This Annex provides guidance for the management and use of email across a tactical IP network.

6A03 OVERVIEW

- a. The guidance provided in this Annex is predominantly behavioural or etiquette based. These ‘soft policies’ are good usage practices that are enforced through management practice rather than technology. They have been collected from a variety of disparate sources and are presented to provide a consolidated list of tips, rules and best practices on the creation, dissemination, sorting, reading and actioning of email.
- b. The rules are required for the following four reasons:
 - (1) **Professionalism:** by using proper language for email the sender, and by extension the Unit / Command will convey a professional image.
 - (2) **Efficiency:** to promote efficiency and reduce the time devoted to sending, reading, and receiving low-value emails.
 - (3) **Regulatory Compliance:** specifically the responsible employment of email and conformance to records management policies.
 - (4) **Sociability:** conforming to accepted social norms of cyberspace.

6A04 EMAIL PROCESSES

- a. Figure 6–A–1 represents the five principal processes that are involved in emailing—sending which involves message creation and dissemination; forwarding and replying which both involve actioning mail; and receiving which involves reading, sorting and possibly actioning mail.

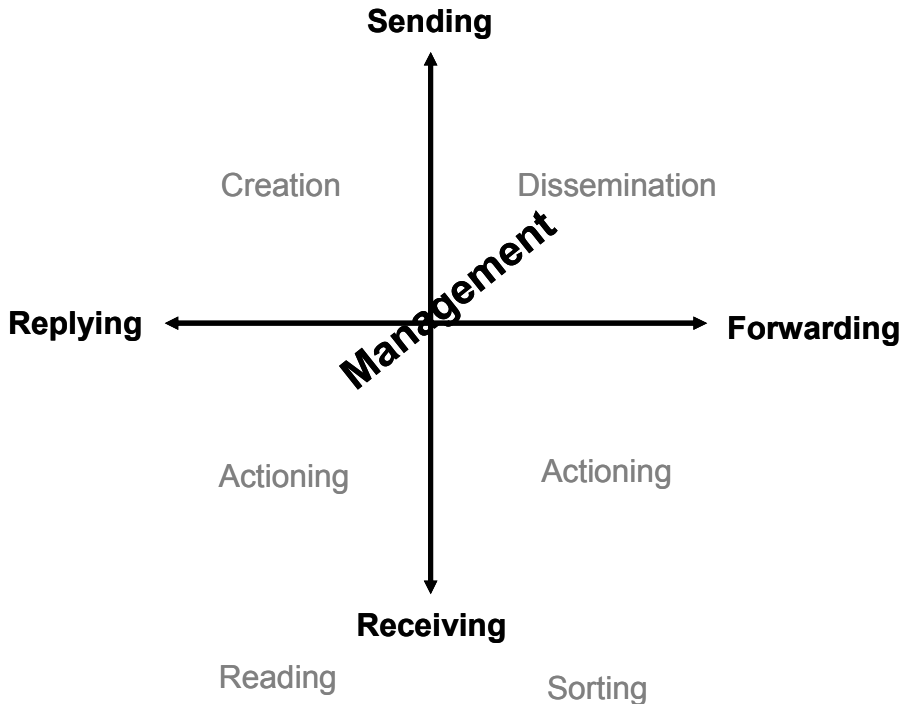


Figure 6–A–1 email Processes

- b. Management is central to the efficient and effective use of email and cuts across the other four functions.

6A05 SENDING EMAIL (CREATION, DISSEMINATION)

- a. Sending email involves the creation and dissemination of electronic mail. Before sending an email it is first necessary to determine whether the email is necessary and how urgent it is. Subject to the content and urgency, an alternative method may be more appropriate. (See Table 6-A-1) For example, do not send email to someone that must be acted upon that day; or (if that is unavoidable) inform the person over a voice circuit or via chat that a message of that nature has been sent to them.

Communication Method	Content Drivers
email	<ul style="list-style-type: none"> • Formal communication for a specific purpose • A distinct audience • Fact-based request where nonverbal cues are not required • Indirect, two-way transaction (i.e. send request, then receive a response)
Chat	<ul style="list-style-type: none"> • Can be Formal or Informal • Normally a distinct audience • Direct, interactive transmission that permits instant decision making • Candid responses possible under some situations (i.e. whispers)
Telephone	<ul style="list-style-type: none"> • Less formal communication • An audience of one (conference calls excluded) • Candid responses, discussion of common ideas, ability to establish conversational rapport • Direct, interactive transmission that permits instant decision making
Fact to face	<ul style="list-style-type: none"> • Choice of formalities, depending on subject and audience • Permits high-content discussions, exploration of ideas, ability to deal with complex problems • The primary choice for sensitive, personal, or negative communication • Direct, interactive, immediate feedback

Table 6–A–1 Guideline for selection of Communication Method

- b. **Message Formatting.** Formatting includes the following sub-topics—addressing, subject line, content format and signature blocks.

- (1) *Addressees* — “To:”. This line is only to be used for action addressees. The writer of an email must carefully identify the person or persons that are required to take action.
 - Where more than one person is included in the “To:” line, the body of the email must clearly identify the actions required from each of the action addressees. The sender should consider creating separate emails for each action item wherever there could be any doubt over the person who is responsible for that action.

UNCLASSIFIED

Annex A to Chapter to 6 to ACP 200(A)

- Recipients that are not required to take any action are to be included on the “Cc:” line as information addressees.
- (2) *Addressees — Carbon Copy (Cc) and Blind Carbon Copy (Bcc).* The “Cc:” line indicates for info — even if there is only one addressee.
- Do not use the Cc field for large mail items unless the Cc: addressees need to see the item.
 - Do not use the Cc field as a method of advising others that the information has been passed.
 - Limit the use of group-addresses unless all those in the group-address need to get the information.
 - Information addresses are not required to send receipt acknowledgements.
- (3) *Subject Line.* The subject line is very important as it sets the readers expectations and frames their anticipated actions. Hence, always include a meaningful, short and concise subject line in addition to a security classification (and/or trusted label). Some examples are presented in Figure 6–A–2.

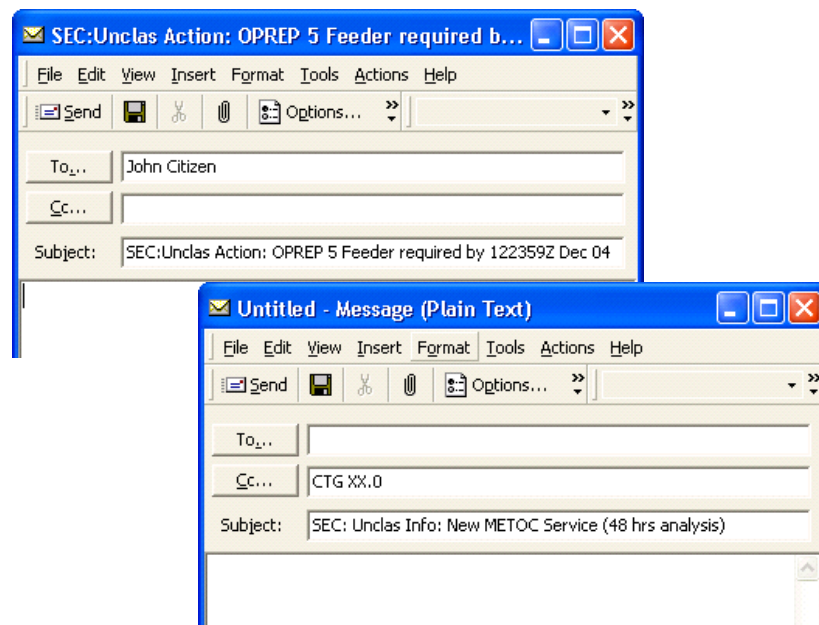


Figure 6–A–2 Examples of Email Subject Lines

- (4) *Format of Content.*

- Do not include any fancy backgrounds or large pictures as not every recipient will want to or be able to view them. These additions also significantly increase the size of the email file.
- Do not type your message in ALL CAPITALS as this makes it look like you are shouting at the recipient.
- Some email programs do not display italicized or underlined words. The use of "*"asterisks."** is therefore often a better way to ensure important points are emphasized.

(5) *Signature Block.* Include a brief signature on your email messages. This helps identify the sender as well as providing an alternative means to contact the sender.

- Keep the signature details short and consider having two signature blocks—a brief signature block (i.e. this maybe one's position and extension number) for internal correspondence and a more detail signature block for external correspondence.

c. **Message Content.** State clearly upfront in the lead of the email the objective of the message. Tell your audience what actions you want them to take before they read on.

- The “lead”—the first few words and sentences of the email—performs a very important role:
 - The lead structures your message, leaving the reader no doubt about why you have written it or whether to continue reading.
 - The lead delivers the document's most important, compelling information right up front, often in the form of a conclusion.
 - The lead summarises what is to come later in the document.
 - The lead captures—and holds—the readers attention.
- Try to write the message from top down. This is also called the inverted-pyramid writing method. The most important information is communicated right up front, in the lead. Following the lead, information is presented in descending order of importance (as represented in Figure 6–A–3). This allows the reader the opportunity to understand the most important aspects of the message and decide if he or she needs to read further.

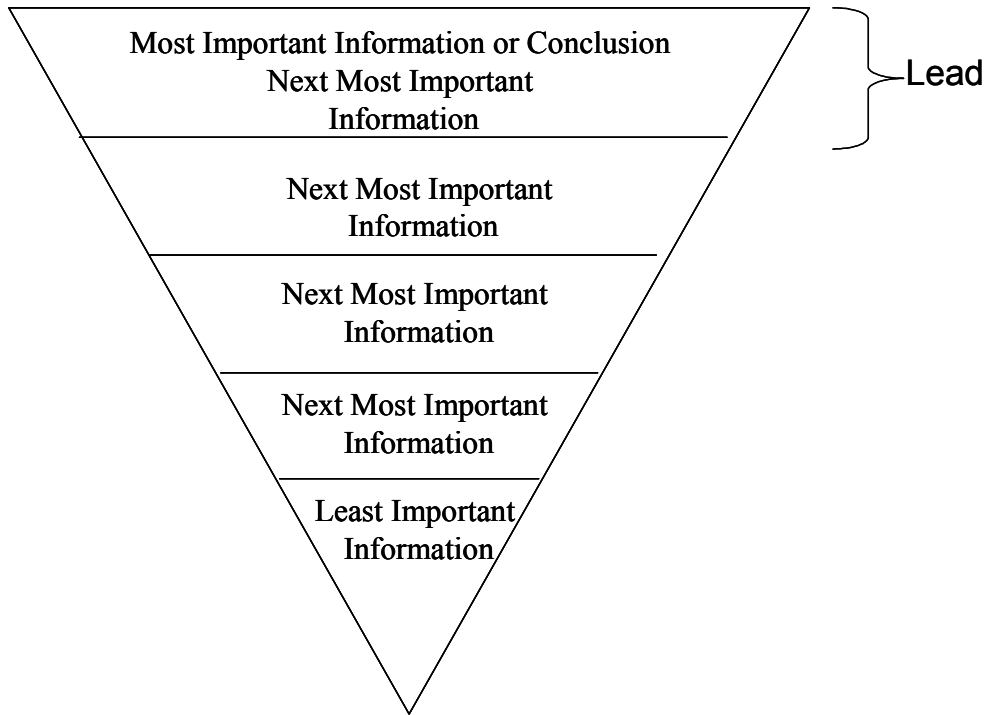


Figure 6–A–3 Inverted Pyramid Concept

- Keep to one subject per email —multi-subject messages should be avoided, as they are difficult for the recipient to file or pass on to others for action.
 - Limit email messages to a maximum of one screen page. If you need more room consider adding an attachment.
 - If expressing a personal opinion, state it clearly as such.
 - Never include offensive or inappropriate comments.
- d. **Final Check.** Prior to sending an email:
- Ensure classified or otherwise sensitive information and copyrighted material is protected.
 - Make a final check of content, addresses, spelling and classification.
 - Limit large email files to those who need the information. They need to have a direct reason for getting the information, not just a professional interest.
- e. **Follow-up.** In cases where there has been no response to an email requiring action or acknowledgement, it is the responsibility of the sender to follow up the matter with the action officer.

6A06 FORWARDING EMAIL (ACTIONING)

- a. Forwarding email is one form of actioning mail. Always include a message explaining the reason for forwarding the email and what action is required.
- b. Beware that forwarding others people's email can be a source of conflict. If in doubt, ask for permission first.

6A07 RECEIVING EMAIL (READING, SORTING, ACTIONING)

Receiving email involves reading, sorting and possibly actioning functions. Ideally routine email is to be opened and actioned within 24 hours (one working day) of its receipt. The following guidance is provided.

- a. Reading.
 - Read the subject line and first few lines. If the subject is not relevant delete it and move on.
 - Do not open email from unknown senders or with unusual attachments. If in any doubt do not open the email or attachments.
- b. Sorting.
 - If possible, deal with the email immediately, if unable mark the email for action at a later date.
 - Ensure email traffic is retained in accordance with the record management policy in the OPTASK IM, or as required by national policies.
 - Comply with any records management policy implemented (see para 6A11).
- c. Actioning.
 - Actioning an email may involve replying to an email (see below) and / or conducting some other function.

6A08 REPLYING TO EMAIL (ACTIONING)

- a. Replying to email is often the outward manifestation of actioning mail. When replying, you will often be replying to only part of the received message. You are also not restricted in replying by the same method (i.e. email). It may be more appropriate and / or efficient to respond via another method. Again Table 16-A-1 provides some useful guidance on selecting the best method of communication.
- b. **Email Response.** While it can be a good idea to maintain the thread from the sender's message, save space by not returning the whole message, only the part to which you are replying.
- c. Message history (email trail) is generally not required. It should only be used when it is essential to convey the entire text and history to a new email recipient (ie someone not on the past addressee list); or when the subject is sensitive enough to warrant a complete record of discussion. If it is included then previous versions of the email that include the message history are to be deleted and only the latest, complete trail saved as the official record of the transaction.
 - Do not respond with 'thanks, got it' etc. Assume receipt and use the tracking option for confirmation.
 - 'Reply to all' is to be restricted to only when necessary. It should not be used to respond to a request for acknowledgement.
 - Avoid re-sending attachments with a reply unless necessary to add clarity to your reply. Remove attachments when using the "Reply to" function.
 - If an email is sent incorrectly, recipients should advise the sender with action taken (e.g. email forwarded, deleted etc).

6A09 ATTACHMENTS

- a. Email attachments can be a source of viruses. Never open an attachment that is sent from an unknown person.
- b. Also avoid the indiscriminate use of attachments. The size of an email shall be in accordance with the OPTASK IM. Large files should be posted to an appropriate web page or collaborative work space. Compress large files and inform people of the format of any attachments sent if it is anything other than basic Microsoft Office file types.
- c. **Processing Attachments.** The best way to deal with attachments is to save them to another location (outside of email) and then remove the attachment from the message.

- d. To save the attachment to disk:
 - (1) Double-click on the message to open it in a separate window.
 - (2) Choose File > Save Attachments from the message menu.
 - (3) Save Attachment dialog box opens.
 - (4) Navigate to the location where you want to store the attached file.
 - (5) Click on the 'OK' button.
- e. To remove the attachment from a message:
 - (1) Double-click on the message to open it in a separate window.
 - (2) Click once on the attachment so that it is selected.
 - (3) Press Delete on the keyboard or click the 'Delete' button on the message toolbar.
 - (4) Close the message.
 - (5) A prompt appears confirming that you want to save changes.
 - (6) Click on the 'Yes' button.

6A10 EFFECTIVE USE OF EMAIL (MANAGEMENT)

- a. **Email Overload.** Email is a productive tool if employed knowledgably. However, poor personal habits can result in email Overload. A form of information overload described in Chapter 3, email overload can tie the warfighter down in timing consuming process of reading and deleting mail.
- b. This can result in the warfighter experiencing information richness, and knowledge poverty at the same time. This dichotomy can be avoided by healthy email management practices outlined in this guide.

6A11 RECORDS MANAGEMENT

- a. Records management, archival and regulatory compliance requirements will force organisations to address the inadequacies of email as a document format and integrate email systems with formal content and records management systems. Many of the business rules required to address record management issues can be implemented at the server. Where human intervention is required, carefully designed rules and processes are required.

- b. Only messages required by law or by internal records management policies should be archived. Messages not subject to regulations should not be archived. Those messages requiring should be archived only for the period required by law. Purging of message media, i.e. disk storage, tape and optical media should be thorough. This is a task that should not be left to individuals.

6A12 ADMINISTRATION

- a. **Access.** Email access shall be restricted to personnel whom have an operational or tactical requirement.
- b. **Accounts.** Email accounts shall be established at the unit level in accordance with the agreed TG naming convention.
- c. Individual or functional accounts, or a combination of both may be used on coalition networks. The policy delineating the use of individual and/or functional accounts will be promulgated in the OPTASK IM, using the convention described in Chapter 14.
- d. **Organisational Lists.** An organisational list is a collection of email addresses representing people or a specific group, assembled together and identified by a unique email alias. Any information sent to this alias is distributed to all email addresses and/or email aliases on the list.
- e. LAN administrators are responsible for the implementation, management and system support for these email lists. The ability to send to group email organisational lists can be limited to certain individuals by LAN administrators. In particular, sending messages to large broadcast email lists such as the "all personnel" list should be restricted.
- f. The lists require constant management to maintain their accuracy.
- g. **Broadcast email lists and attachments.** Attachments should not be sent to email lists containing more than 10 members. Web Services or collaborative work spaces should be used to transfer attachments.
- h. **Self-subscribe email lists.** Email lists or news groups to which staff may subscribe generally should be avoided. The creation of self-subscribe lists should be approved by Command.
- i. **Mail Loops.** Mail loops can occur when two users auto forward their mail to each other generating a continuous flow of traffic. This should be avoided and can be most often prevented by waiting 10-15 minutes from sending your last email from setting the out of office wizard.

6A13 CONCLUSION

An understanding of the benefits and weakness of email, as well as the adoption of best practices can ensure that email is effectively and efficiently managed to assist (vice overwhelm or distract) the warfighter

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. Annex A to Chapter 13 Transport Services provides a detailed discussion of MSeG operation. MSeG is capable of delivering the COP via MDP when the receiving unit is in EMCON silence. 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.

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.

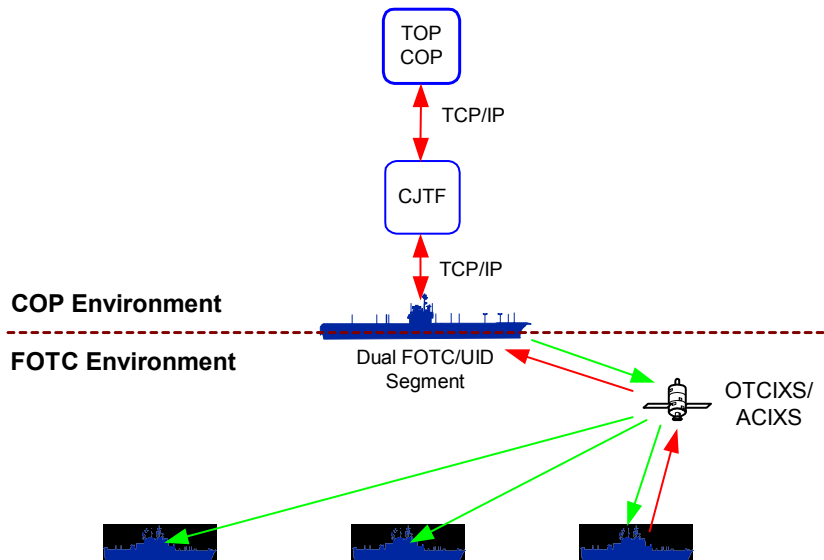


Figure 7-1 Traditional Environment (with IXS networks and CST)

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

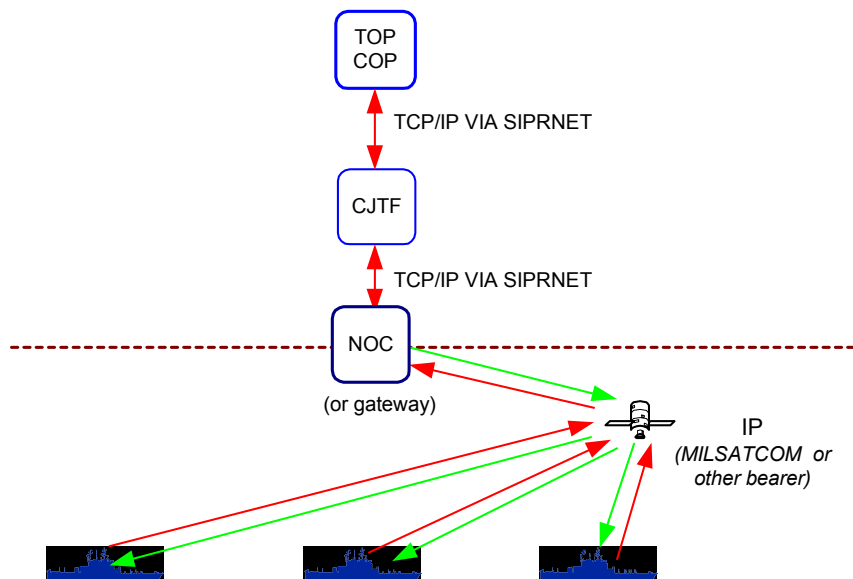


Figure 7-2 Full IP Environment (MTWAN)

- 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. Synchronised track databases Automatic process Utilises TCP/IP 	<ul style="list-style-type: none"> Not recommended unless WAN bandwidth 64Kbps or greater 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 CONCLUSION

- 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 SERVICES

801 INTRODUCTION

Web Services support Information Management (IM) principles articulated in Chapter 3 through the ability to manage and disseminate information to a large number of disparate users. Web Services also enhance systems interoperability by exposing authoritative data sources to external applications in an open and well-documented manner.

802 AIM

The aim of this Chapter is to provide guidance for the employment of web services in a low bandwidth maritime environment.

803 OVERVIEW

- a. At the heart of Web Services should be authoritative data and its reuse. An IP network, while providing connectivity, in itself does not guarantee the ability to seamlessly share data. This is because IP-enabled applications often use application-specific mechanisms to format and transmit their data over networks. Web Services utilizes a 'web browser' to provide a common User Interface (UI) application between the data and the user. This negates the requirement for individual workstations to be loaded with numerous unique applications prior to being able to access and share information. Care must be taken to ensure that the browser being utilized on the network supports the required Web Service applications.
- b. Intranets live by content currency and contain large amounts of specialized information that originates in widely diverse departments and teams. The more that people take ownership and direct management of their own content creation, the more the content is likely to be up-to-date. This requires the establishment of bi-directional (heterogeneous) repositories and the adherence to IM procedures.

804 OBJECTIVE

The objective for web services is to create an '*electronic information marketplace*' where:

- a. *information consumers* can easily discover, retrieve, and manage information based upon its characteristics advertised by information producers.
- b. *information producers* shall advertise information availability and accessibility using metadata (information about data), data schema, and producer profiling mechanisms.

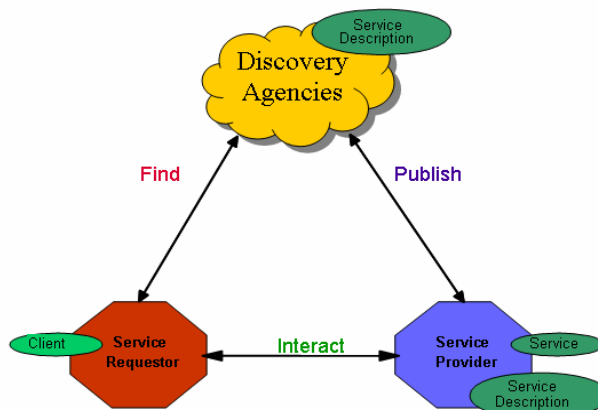
805 DEFINITIONS

'Web Services' is a term often used in Web Technology discussions yet it is seldom understood. The following terms are defined for use in this publication.

- a. **Web-enabled.** The presence of a front end user interface, which is accessible through a web browser.
- b. **Portal-enabled.** A web-enabled application which instead of allowing the web server to interact directly with the client's browser, the data is alternatively fed through a portal device that controls the "look and feel" of the web page. The portal can connect to multiple different web servers on behalf of the user and control the access, look and feel, and behavior for each web page all within prescribed "frames" that the user defines within their browser. (See para 814 (b) for more information.)
- c. **Web Services.** A "web service" is a system that uses standards and technologies to describe and deploy applications or services on a network in a consistent way so that they can be discovered and invoked in a secure and reliable manner.
- d. **Search Engines.** Computer programs that when queried for information (usually with a key word or phrase) find sites, web pages, and documents on the network fitting the description.

806 FUNCTIONAL DESCRIPTION

- a. Web Services are based on a service-orientated architecture and can be described using the following three components:
- (1) **Service Requester**—the mechanism through which a request to execute a Web Service is made.
 - (2) **Discovery Agencies**—the mechanism through which Web Service descriptions are published and made discoverable.
 - (3) **Service Provider**—the component that processes a Web Service request.
- b. Figure 8–1 shows these three components and their interaction. Interaction is possible because of the common middleware and the use of common communication standards and descriptions (Table 8-1 refers).

**Figure 8–1 Service Orientated Architecture**

- c. When a service provider wants to make the service available to service consumers it is *published* using discovery agencies (UDDI registry). The service consumer who uses a client to access a service requester also uses this standard mechanism to *find* the service. The discovery agencies (UDDI registry) contain information in Web Services Description Language (WSDL) pertaining to the service and the access point for the service. The service consumer uses the WSDL description to construct a Simple Object Access Protocol (SOAP) message with which to *interact* with the service provider.

Standard	Description
Extensible Markup Language (XML)	A streamlined version of Standard Generalized Markup Language, developed by the International Organization for Standardization to define the structures of different types of electronic documents. XML can be used to store any kind of structured language and encapsulate data so it can be shared between otherwise incompatible computer systems.
Simple Object Access Protocol (SOAP)	Based on XML and Hypertext Transport Protocol. It provides a way for applications — including those running on different operating systems — to communicate and work together through remote procedure calls implemented via HTTP.
Universal Description, Discovery and Integration (UDDI)	Describes how to publish and discover information about Web services applications. It is a Web-based directory where someone can search for particular Web services and what they do.
Web Services Description Language (WSDL)	Based on XML, describes the kinds of software applications, or services, available on a particular network. Once someone develops a Web service, they can publish its description and link in a special UDDI repository. When someone wants to use the service, they request the WSDL file so they can determine its location, function calls and how to get to them. They use that information to construct a SOAP request to a server.

Table 8–1 Standards behind Web Services

807 WEB ADMINISTRATION

- a. **Web Administrator.** The Web Administrator is responsible for the technical infrastructure of the web site(s). The administrator provides the tools to enable users to publish, access, and customise information rather than doing it themselves. Tasks include registering users, maintaining functional stability and responding to web problems. Functional stability refers to the reliability of the site's interactive elements. This includes ensuring that hyper-links are still working properly.
- b. **Web Developer.** The Web Developer is responsible for developing / customizing web services.
- c. **Information Manager.** The Information Manager oversees all content

within a given functional area to ensure the timeliness, relevancy and accuracy of information. Duties include enforcing maximum file size rules, monitoring user's adherence to formatting rules, and providing assistance.

- d. **Information Producers.** Each functional area, as producers of information, determines what information they create and maintain on the web site. The information producer is responsible for keeping their portion of the web site and lower level sub-webs current and accurate.

808 PRINCIPLES

Web Services technologies and practices must:

- a. Support posting data to shared spaces as early as possible.
- b. Support the parallel (ie Task, Post, Process, Use) vice serial (Task, Process, Exploit, Disseminate) processing of information. Example:
 - (1) Parallel: Units post their individual fuel state directly to the Task Group web site after each set of 'tank dips'. Result: CTG has the most up to date view of the overall state of fuel within the TG.
 - (2) Serial: Units send record message traffic once per day, which includes fuel state at a given time. This information is collected by a member of CTG staff and then posted on the TG web site. Result: CTG has a time late view of the overall state of fuel within the TG once per day.
- c. Information Portability. Provide users with the capability to access the data they need, when they need it, from where ever they are.
- d. Promote authoritative data and its reuse. Data that has been subsequently filtered or value-added should be posted back onto the network.
- e. Reduce the amount of email and supplant it in certain areas, such as attachment circulation.

809 REQUIREMENTS

The following requirements are mandatory:

- a. **Information Awareness and Access.** Users must know where and when information is available and have the tools, procedures and capabilities to retrieve and analyze the required information. IM procedures in Chapter 3 (like the Information Dissemination Management Plan) and automated functions (like source registries) provide this capability.
- b. **Information Repositories.** The establishment of repositories and the identification and authorization of organisations / elements to create, compile, distribute, and dispose of data and metadata in these repositories.

810 CONNECTIVITY

- a. **Persistent Connectivity.** The performance and latency issues inherent in accessing centralized applications make persistent connectivity undesirable (if not impossible) in a mobile network environment. The mobile-networked environment requires applications that keep working productively at the local level in both the WAN connected and disconnected state. After all, a mobile platform loaded with 'immobile' applications (those that require persistent connectivity) is not mobile at all.
- b. **One-Way Replication.** Traditional one-way data replication tools are suitable for updating a centralized database with information gathered in the field, but little else. This relegates mobile applications to being rudimentary information-display or capture devices, rather than true disconnected versions of the same enterprise applications.
- c. **Bi-directional (heterogeneous) replication.** Alternatively bi-directional, heterogeneous data replication solves many of the tricky problems mentioned about distributed databases. By providing full read-write bi-directional replication capabilities, this technology makes it possible to deploy enterprise applications on mobile devices and to enable full access to application data, even in disconnected mode. In the background, there is a replication network that communicates any changes to data to all of the other databases. If a database is not online at the moment, it will be updated when it does come online. This, in effect, creates an application architecture where there can be thousands of dynamically linked databases, all communicating change to one another as needed. When implemented, this powerful capability provides "network transparency" to

the user, since the application is free to roam between connected and disconnected modes without affecting function visible to the user. (Annex A refers) Information ownership is critical when using a bi-directional replication network in order to avoid “replication conflicts” which may occur when two or more units modify or change the exact same information at the same time in a disconnected state. A common problem is the deletion of information from a data base by someone other than the designated ‘information owner.’

- d. **Transaction Logging.** In order to ensure complete data integrity for updates and to perform incremental database backups, web replication products require some form of transaction logging capability. A transactional log provides a sequential record of every replication operation that has occurred during a given period of operation. This allows online server backup and recovery support. For example, if connectivity is lost, a transaction logging capability will enable replication to automatically recommence at the point it ceased, thus limiting duplication (non-transaction logging replication services would have to start from the beginning) and consequently duplicate use of expensive and often limited communication bandwidth.

811 WEB CONTENT / PAGES

- a. **How Users Experience the Web.** Readers experience Web pages in two ways: as a direct medium where pages are *read online* and as a delivery medium to access information that is *downloaded* into text files or printed onto paper. How readers will typically use the information should govern the type of document posted. Documents to be read online should be concise, with the amount of graphics carefully “tuned” to the bandwidth available to your mainstream audience. Documents that will most likely be printed and read offline should appear easily on a page.
- b. **How Users Read on the Web.** People rarely read Web pages word by word; instead, they scan the page, picking out individual words and sentences. In a recent academic study 79 percent of users always scanned any new page they came across; only 16 percent read word-by-word.
- c. **Users Choices.** Users tend to choose the first reasonable option presented to them vice the best option. This is a reflection that the users are usually in a hurry, and the cost for guessing wrong is only an additional click or

two. Also in the case of poorly designed sites, weighing the options might not improve the user chances.

- d. **Response Times.** The basic advice regarding response times has been about the same for almost thirty years:
 - (1) **0.1 second** is about the limit for having the user feel that the system is reacting instantaneously, meaning that no special feedback is necessary except to display the result.
 - (2) **1.0 second** is about the limit for the user's flow of thought to stay uninterrupted, even though the user will notice the delay. Normally, no special feedback is necessary during delays of more than 0.1 but less than 1.0 second, but the user does lose the feeling of operating directly on the data.
 - (3) **10 seconds** is about the limit for keeping the user's attention focused on the dialogue. For longer delays, users will want to perform other tasks while waiting for the computer to finish, so they should be given feedback indicating when the computer expects to be done. Feedback during the delay is especially important if the response time is likely to be highly variable, since users will then not know what to expect.

812 WEB PAGE GUIDELINES

- a. Web pages that are concise, and can be readily scanned reduce the user's cognitive load, which results in faster, more efficient processing of information.
- b. **Short Texts.** Concise text contains less information to process. Reading from computer screens is about **25% slower** than reading from paper. Even users who do not know this human factors research usually say that they feel unpleasant when reading online text. As a result, people do not want to read a lot of text from computer screens: you should **write 50% less text** and not just 25% less since it's not only a matter of reading speed but also a matter of feeling good. Also users do not like to scroll: one more reason to keep pages short.
- c. **Scannability.** Scannable text calls attention to key information. The following suggestions can improve the scannability of text:
 - (1) Highlighted keywords (hypertext links serve as one form of highlighting; typeface variations and colour are others).

- (2) Choose meaningful sub-headings.
 - (3) Employ bulleted lists.
 - (4) Use one idea per paragraph (users will skip over any additional ideas if they are not caught by the first few words in the paragraph). Where appropriate use the inverted pyramid style, starting with the conclusion.
 - (5) Half the word count (or less) than conventional writing.
- d. Use uppercase letters sparingly. Uppercase words are not easy to read as mixed case words, and can make a page look busy and loud.

813 POSTING DOCUMENTS

- a. All documents posted should have:
- (1) An informative title (which also becomes the text of any bookmark to the page).
 - (2) The creator's identity (author or institution).
 - (3) A creation or revision date.
 - (4) At least one link to a local home page or menu page.*
 - (5) The "home page" URL on the major menu pages in your site.*

Note: *Asterix denotes features that are provided automatically by templates.

- b. **Hierarchy of Information.** Careful thought should be placed as to the posting location of documents to establish an efficient hierarchy for the information. This will allow users to get information in the fewest possible steps. (Studies have shown that users prefer menus that present at least five to seven links and that they prefer a few very dense screens of choices to many layers of simplified menus.)

814 WEB INTERFACES

- a. A good Web Interface will provide ease of use for even novice users. For the web developer, it is relatively easy to construct and provides rich and expanding support for a variety of GUI components and processing models. The new Xforms, Flash and other rich media capabilities also allow developers a wide range of choices over what elements can be used to develop Web interfaces. Care must be taken to the impact on bandwidth which may be caused by the interface element selected.
- b. **Portal.** An information portal is a concept that serves as a single gateway to an organization's information and knowledge base. An information portal can comprise the following elements:
 - (1) **Access / Search.** Allows a user to get all the information needed (but no more) in the desired context.
 - (2) **Categorization.** A portal can categorize all information so that it is delivered to the user in context needed.
 - (3) **Collaboration.** Allow individuals to collaborate regardless of geographic location.
 - (4) **Personalization.** The information provided to the individual is personalized to that person's role, preferences and habits.
 - (5) **Expertise and Profiling.** Individuals are profiled according to their experiences and competencies. If an individual needs to collaborate with others, a person qualified for the task can be found.
 - (6) **Application Integration.** This allows individuals to deliver, access, and share information regardless of the applications used.
 - (7) **Security.** The user is given access only to the information that the user is authorized to access.
- c. **Templates.** Templates provide tailored views of documents from within a web browser. Templates provide the following advantages:
 - (1) Bring consistency and predictability to web pages.
 - (2) Operators at each site become information/content 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.

- (3) Provides easy navigation within the site. (Users become familiar with the layout of the site and can return easily to the home page and to other major navigation points in the site.)

815 CONCLUSION

Web Services is an important and evolving technology that can be used to support the warfighter's information requirements. It can be employed to improve interoperability, information management, and collaboration.

WEB-ENABLED DATABASE REPLICATION

8A01 INTRODUCTION

Bi-directional, heterogeneous data replication of web-enabled databases solves many of the tricky problems mentioned in the chapter about distributed databases. By providing full read-write bi-directional replication capabilities, it is possible to deploy enterprise applications on mobile platforms and to enable full access to application data, even in disconnected mode.

8A02 AIM

The aim of this annex is to describe and provide guidance for bi-directional web-enabled database replication in a low bandwidth environment.

8A03 OVERVIEW

- a. By providing full read-write bi-directional replication capabilities, it is possible to deploy enterprise applications on mobile platforms and to enable full access to application data, even in disconnected mode. With a common web-enabled database at each location, operators are able to browse the site on their local LAN (or work station) without having to browse off-ship in order to reach needed information on a remote server. Local browsing provides two advantages; it provides a high speed 'surfing' experience – providing faster access to required information in both connected and disconnected state, and it reduces the bandwidth requirement/utilisation for external communications since information is transferred only once to the unit – even though it can be accessed multiple times. Any changes made locally to the database in an offline state will automatically be replicated to the network upon reconnection.
- b. The template centric database(s) allows operators at each site to become information/content 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.

8A04 REPLICATION ARCHITECTURE

- a. There are three basic types of replication architectures: Hub-Spoke, Meshed, and Federated Hub-spoke.
- b. **Hub-Spoke.** A hub-spoke replication topology has proven to be an

Annex A to Chapter 8 to ACP 200(A)

efficient method for replication. Figure 8–A–1 illustrates typical hub-spoke architecture with the vast number of nodes having one or possibly two links, juxtaposed with a tiny number of nodes that have a large number of connections.

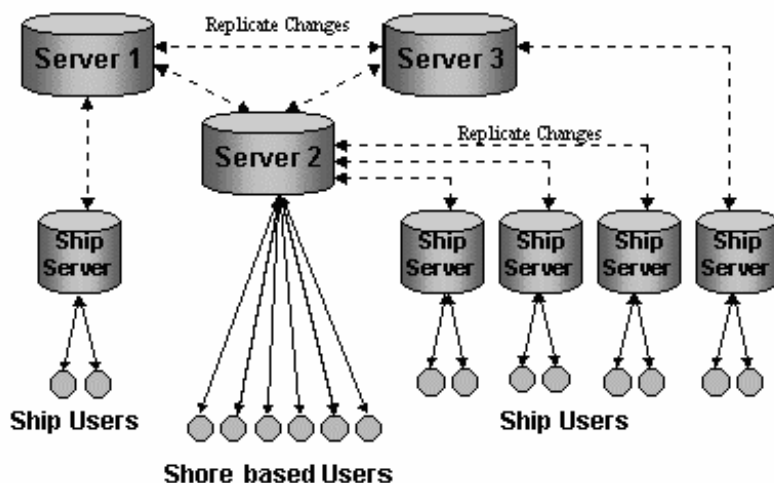


Figure 8–A–1 Generic Replication Architecture

- c. 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 TF/TG 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.
- d. **Meshed Architecture.** Figure 8–A–2 illustrates a ‘meshed’ replication architecture. In a meshed model, multiple replication connections are established with all units within the network. This provides a highly flexible and survivable information-sharing model. The meshed model allows for information sharing between TG units using a fully dynamic LOS tactical IP sharing network with no shore connectivity. It must be noted that a meshed architecture can increase the bandwidth requirement due to the multiple server-to-server connections. Therefore only key tactical information databases should be shared in a low bandwidth LOS tactical IP sharing environment. Remaining, non-critical databases should follow Hub-Spoke architecture for delivery to mobile units.

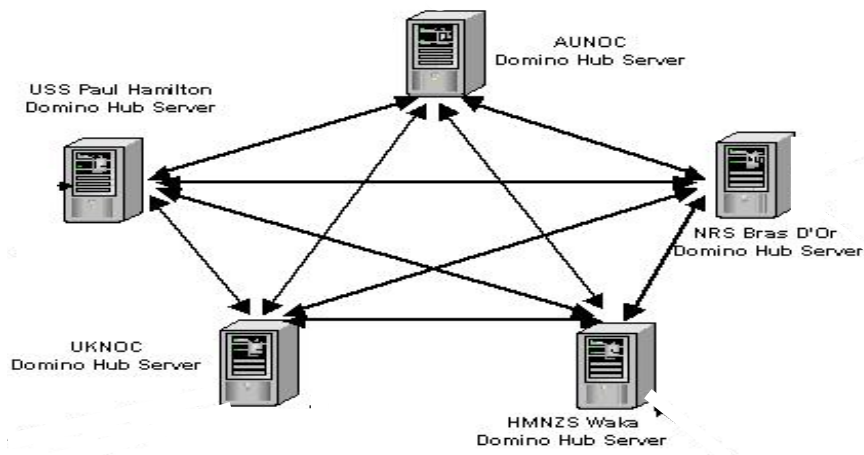


Figure 8-A-2 Mesh Replication Architecture

- e. **Federated Hub-Spoke Architecture.** Figure 8-A-3 illustrates a hub-spoke architecture with multiple hubs vice an architecture employing a single hub. This is a combination of a hub-spoke and meshed architecture in order to combine survivability with bandwidth reduction. Rather than a hierarchical model, a federated hub system is preferred when multiple hubs are employed with large bandwidth availability.

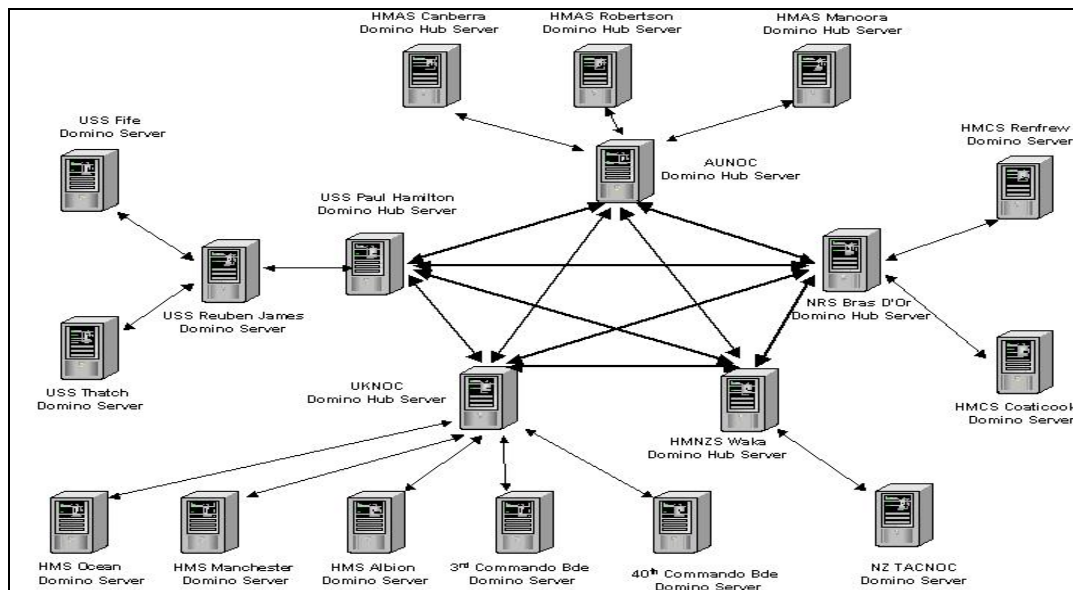


Figure 8-A-3 Federated Hub-Spoke Replication Architecture

UNCLASSIFIED

Annex A to Chapter 8 to ACP 200(A)

- f. **Scalability.** These topologies are essentially scale free in that additional servers can be added without adverse effects.
- g. **Survivability.** Scale-free topologies are quite survivable against random failure, but are highly vulnerable to a focussed attack because of the critical role of the hubs in the network. Research has shown that up to 80 percent of the nodes in a scale-free network can be randomly removed without compromising the functionality of the networked whole. However, a coordinated attack that disables 5 percent to 15 percent of the hubs simultaneously would compromise the system.

8A05 REPLICATION PROCESS

- a. The bi-directional web-enabled databases are composed of unstructured document databases (object oriented)—such as ASCII text fields, Rich Text Format (RTF) fields, graphics, a file attachment of any type, or any combination of the above vice a traditional relational database. Subsequently, documents and files of any type can be added to such web sites.
- b. 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. At the end of the replication cycle, all servers at all sites contain an identical set of documents.
- c. **What is replicated?** File attachments are treated as one data field, any change to an attached file require the whole file to be retransmitted. 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. This means that a 50KB Word document that is ‘attached’ to the web site for posting vice using ‘cut and paste’ into a RTF Field would result in approximately the same data transfer size on initial replication. Any subsequent changes to that information, even a change as small as adding a single letter to a word contained within the document, would result in the entire Word document being retransmitted for the file attachment (50KB); however, only the single character letter would be transmitted for the change in the RTF Field – a few bytes.
- d. **Transaction logging.** This 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

UNCLASSIFIED

Annex A to Chapter 8 to ACP 200(A)

automatically recommence at the point it ceased, thus limiting duplication and consequently (often) expensive communication and satellite time.

- e. **Replication Cycle / Time.** 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 network architecture and available bandwidth. Replication should be set to occur IAW the OPTASK KM.
- f. **Force Replication.** If necessary, the replication process can be initiated manually, or 'forced', in order to speed information dissemination vice waiting for the scheduled replication cycle.
- g. **Streaming Replication.** This method involves a single server request that performs a PULL of all the data into the database. This is an improvement over the non-streaming method of requesting and acknowledging one database document or note at a time. Streaming replication means that you do not need to wait until the replication completes before you see replicated documents in folders. They appear individually as soon as they are pulled into the system and you can begin to work on them before the database finishes replicating. Benefits include faster replication, partial replication and potentially less network traffic due to a single streamed Remote Procedure Call (RPC), and a reduction of Acknowledgement (ACK) TCP/IP responses.
- h. **Network Compression.** Network compression (if provided) should be employed to reduce transaction times, and employ bandwidth efficiently. When enabled, data is automatically compressed (ideally it requires no user intervention) before it is sent over the network. The degree of compression will be dependent on the file type and the compression technology.

8A06 CONCEPT FOR EMPLOYMENT

- 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. The web-enabled database replication process ensures that operators can access information locally from their servers transparently, while a transaction logging capability enables web administrators to monitor communication between the master and local server. If connectivity is lost

UNCLASSIFIED

Annex A to Chapter 8 to ACP 200(A)

during replication, replication will efficiently re-establish upon reconnection of the web servers.

- c. Units with persistent, high bandwidth, connectivity can employ clustered replication if approved by the NOC, while units with intermittent connectivity will replicate on a cycle established in the OPTASK Knowledge Management. If necessary, to expedite the dissemination of time sensitive information, users may force replicate.
- d. Where ASCII and RTF information is contained within a text field, only the 'delta' will be sent. Changes to attachments will be resent completely as attachments are treated as one data field. Compression technology (if available) should be enabled on the database to automatically compress attachments (preferably without human intervention).
- e. The NOC(s) will act as information transfer gateways providing releasable material to pass into other security domains, such as national secret networks using an approved Boundary Protection Device (BPD). At present this is achieved through air-gap procedures, High Assurance Guards and/or Secure Mail Guards. 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.
- f. The end result is that users will have a central authoritative repository of information or 'electronic binder' of TF/TG information.

UNCLASSIFIED

Appendix 1 to Annex A to Chapter 8 to ACP 200(A)

TYPICAL REPLICATION WEB PAGE

8A101 INTRODUCTION

The best-designed replication sites allow readers to enter the site, find what they want, and easily print or download what they find. Non-essential graphics should be minimal and undistracting, and content and menu structure must be carefully organized to support fast search and retrieval, easy downloading of files, and convenient printing options. Contact time is typically brief in replication sites: the shorter the better.

8A102 AIM

This Appendix describes a typical bi-directional heterogeneous replication page, which is used to disseminate information within a TF/TG.

8A103 OVERVIEW

Templates provide narrative, and design consistency for the site as well as facilitates site maintenance.

8A104 PAGE-LEVEL STRUCTURES

- a. The general navigation and layout conventions for a typical TF/TG replication template follows major web sites as most users will be familiar to those conventions.
- b. Page-level structures include the distribution of content, applications, and navigation tools. Many pages use the basic three-panel structure shown in Figure 8–A1–1. The top area contains global information about the site, the left side area contains navigation controls and links to commonly used objects, and the large central panel is home to the substantive content of the portal.

Appendix 1 to Annex A to Chapter 8 to ACP 200(A)

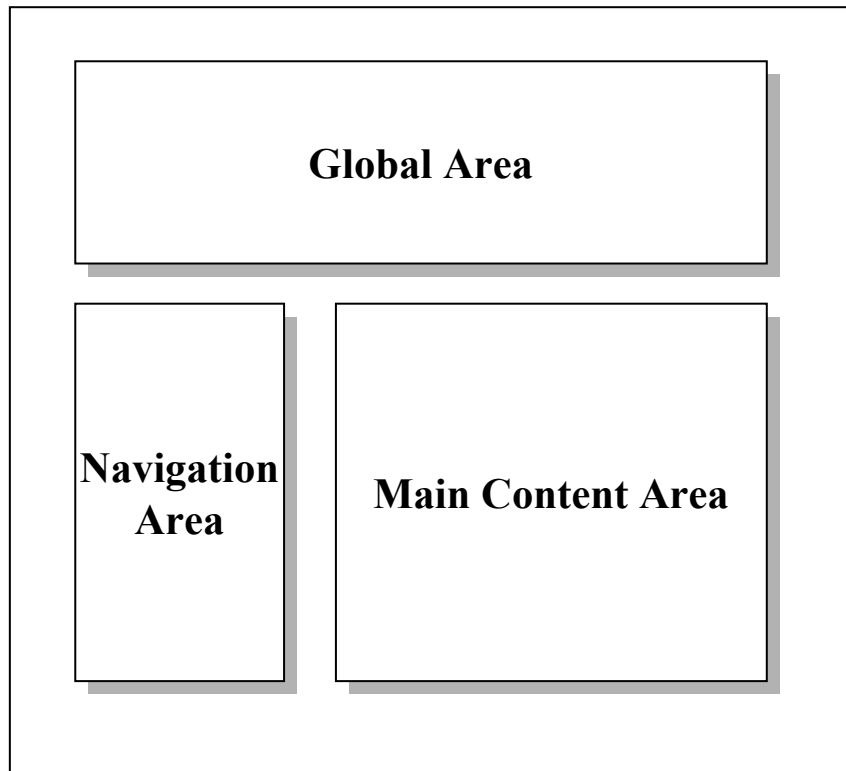


Figure 8–A1–1 Typical Page Structure

- c. **Global Area.** The global area is consistent across the web site and often provides links to a home page, contact information, accessories, or other frequently used applications. In some cases, the area is used to present monitoring information such as the status of threat levels. Figure 8–A1–2 highlights the common elements.

Appendix 1 to Annex A to Chapter 8 to ACP 200(A)

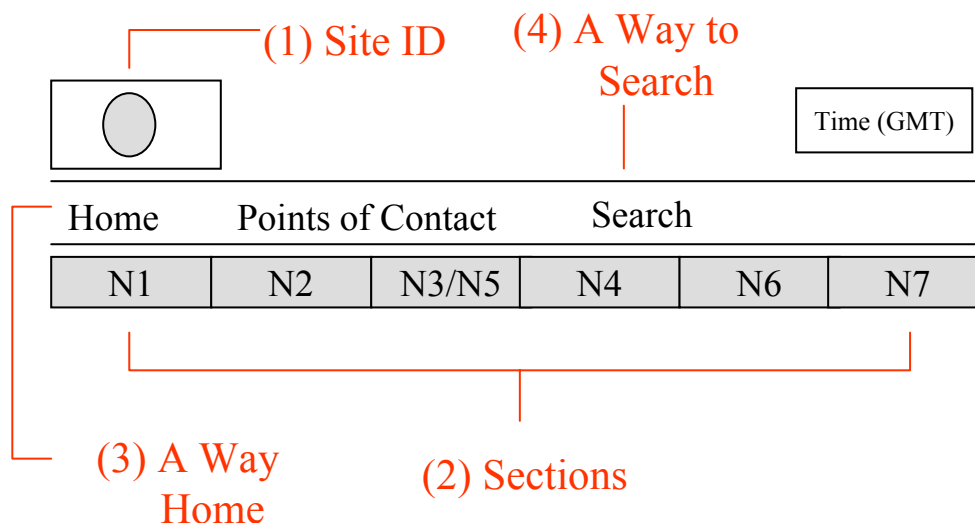


Figure 8–A1–2 Global Area Content

- d. The site ID or logo provides users with a reference to what site they are in. Sections provide the links to the main sections of the site (ie the top level of the site hierarchy). In the case of most TF/TG sites, this is the links to information grouped along traditional military functional lines.¹
- e. **Navigation Area.** The left navigation rail provides a localised context for users. This provides an immediately visible and easily accessible path to related components in the site, while keeping the user from being overwhelmed by the full breadth of the site.
- f. **Main Content Area.** The main window is the target area for viewing navigation results such as libraries, reports, and documents.
- g. **Footer Navigation.** A common design convention is to feature certain options at the end of the page.

¹ Referred to as the Continental Staff System.

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

- a. Military forces rely upon shared information — intelligence, 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 has been confined to formatted messages and voice circuits. This has limited both the scope of information that could be conveyed and the format that this information could be presented. Lengthy messages were often required to convey the Commander's plan and good comprehension skills were required to assimilate details and understand the intent in other units. This 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 email and Web Services.

902 AIM

This chapter provides 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 that provide the war fighter with a powerful collaborative tool. Together they make collaboration as convenient and as effective as face-to-face conversations.

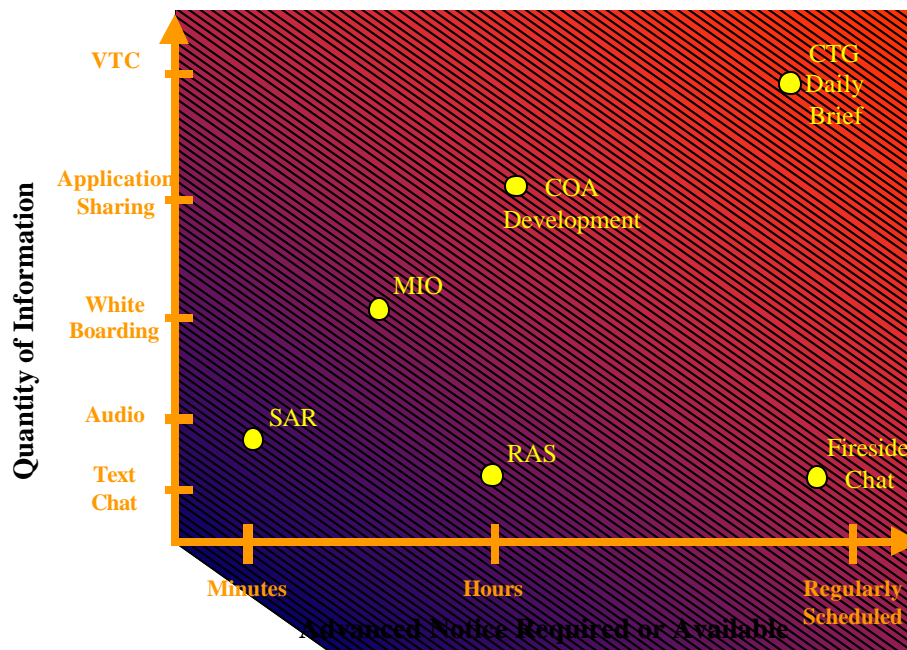


Figure 9-1 Collaborative Planning Spectrum

9-2

	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

- 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.

- 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 email to schedule an online meeting later. Instead of replying to an Email, a user could start a conversation with one or many Email 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.

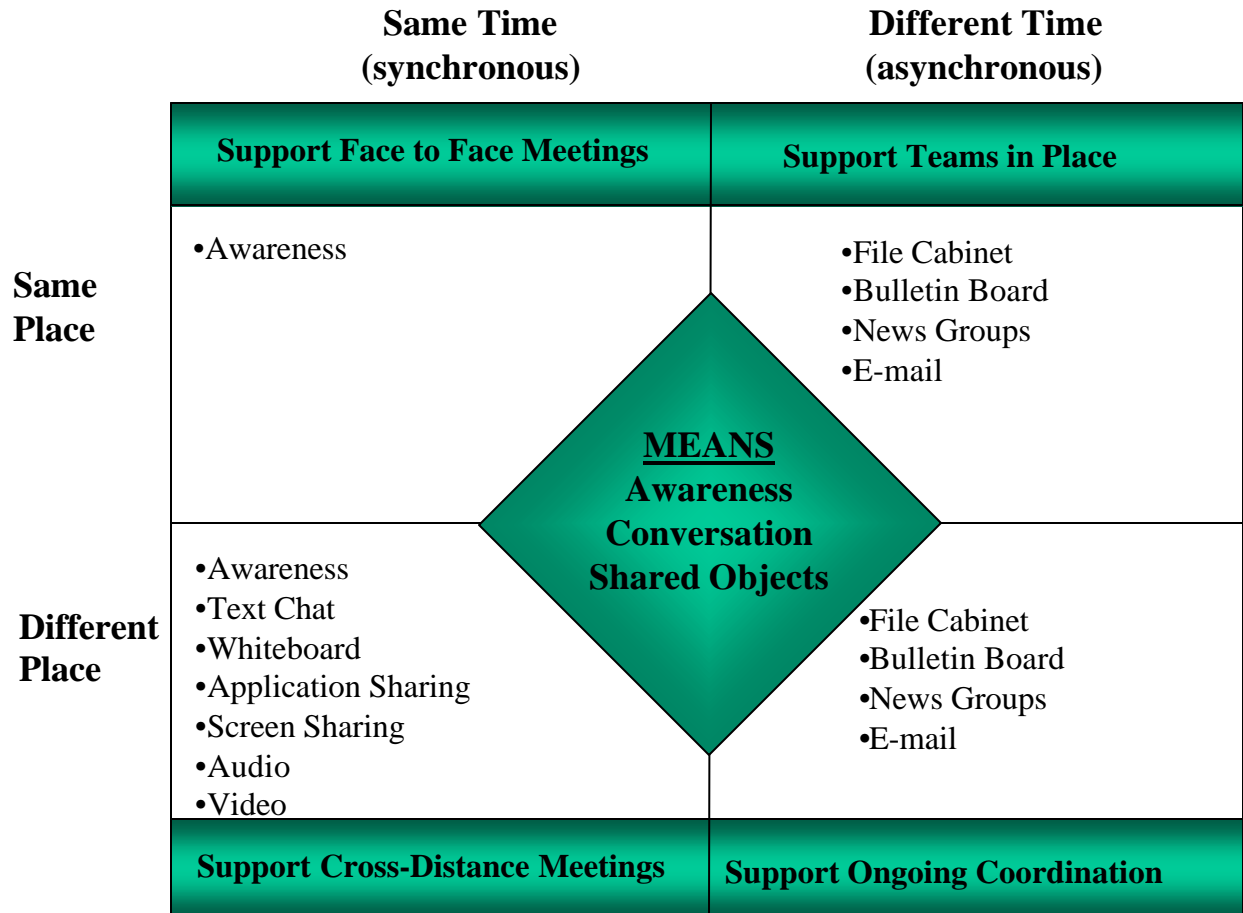
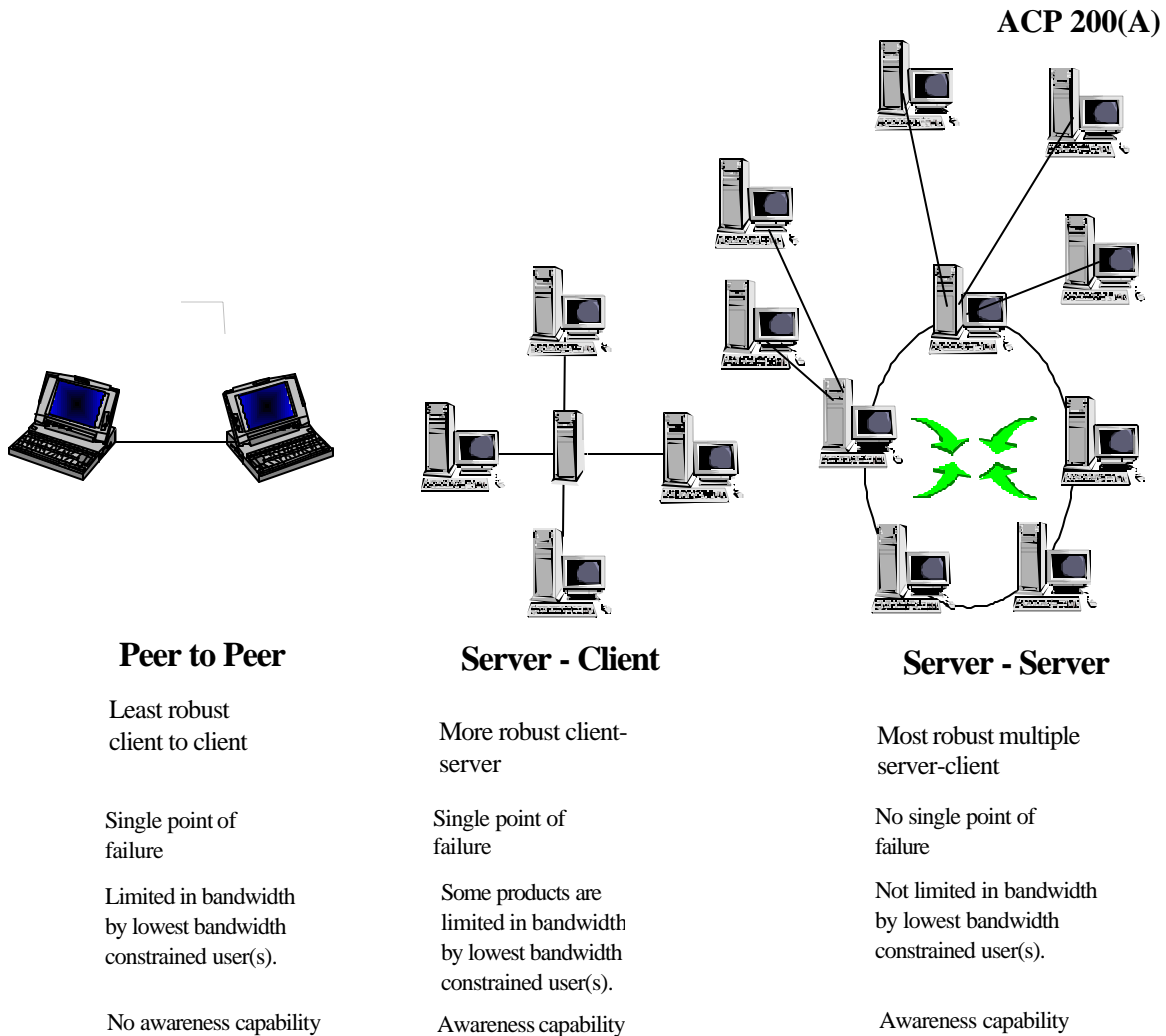


Figure 9-2 DCP Characteristics

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 not available. Server-client configurations can support greater number of users and are more robust. In a hub-spoke environment servers could be connected, sharing the Global Address Book, and allow users to Collaborate across multiple 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 would normally comprise the tools detailed in Annex A 9A03 sub paragraph b.

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

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 and Instant Messaging cross-platform compatibility — SIMPLE.** SIP for Instant Messaging and Presence Leveraging Extension or SIMPLE is an emerging standard based on the Session Initiation Protocol (SIP). SIMPLE is an extension of SIP that enables awareness and instant messaging. SIMPLE extends call routing to online status to ask for presence and to provide instant messaging. A SIP Gateway enables the connection of two or more CHAT communities using SIP-enabled CHAT products from the same and/or different vendors. For example, an IBM Lotus Sametime community is able to extend awareness and conduct chat across to a Microsoft MSN and/or AOL Instant Messaging community(ies).
- 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:
 - (1) **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.

UNCLASSIFIED

Annex A to Chapter 9 to ACP 200(A)

- (2) **Platform and application independence.** H.323 is not tied to any hardware or operating system.
 - (3) **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.
 - (4) **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:
- (1) **Interoperability.** T.120 allows endpoint applications from multiple vendors to be interoperable.
 - (2) **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.
 - (3) **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.
 - (4) **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(A)

- (5) **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 SOP

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

This annex establishes 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

UNCLASSIFIED

Annex B to Chapter 9 to ACP 200(A)

- 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 9–B–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 9-B-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.

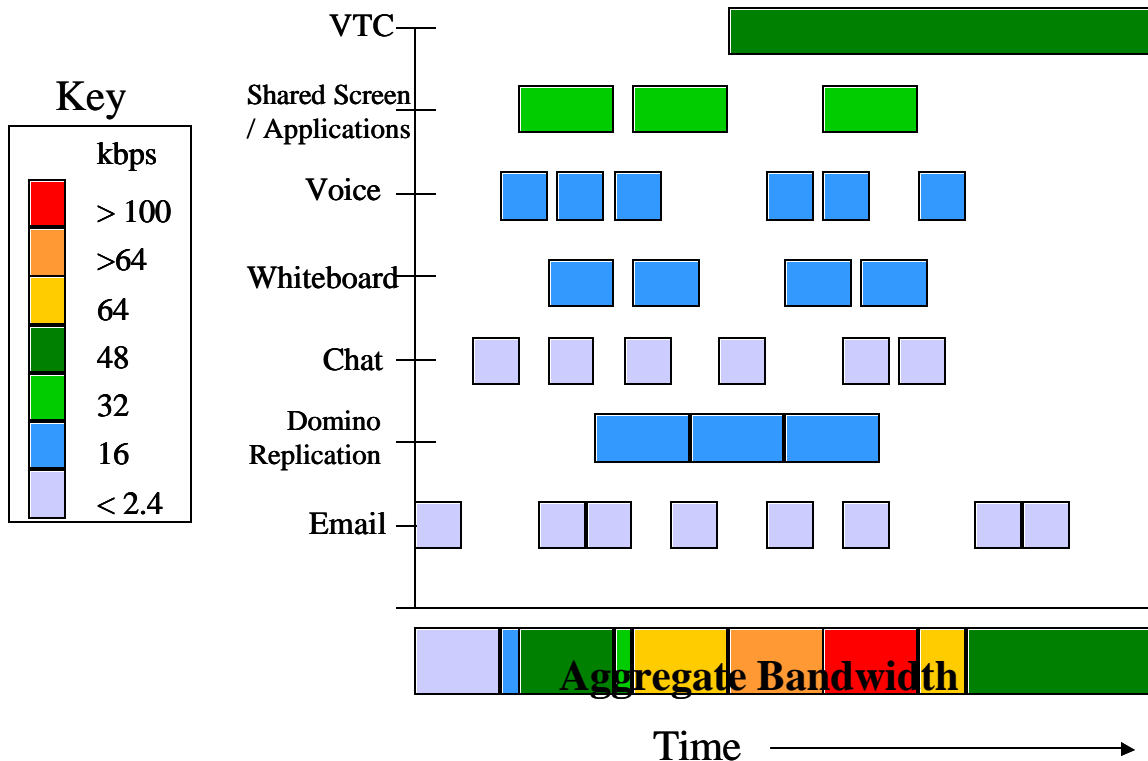


Figure 9-B-1 Bandwidth Aggregation

- 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

UNCLASSIFIED

Annex B to Chapter 9 to ACP 200(A)

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 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 ad hoc planning sessions can be conducted in either a time constrained or unconstrained environment. Ad hoc planning sessions tend to be less formalized. Collaboration can therefore occur in a formalized (scheduled and controlled) or informal setting.

9A04 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–A–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.

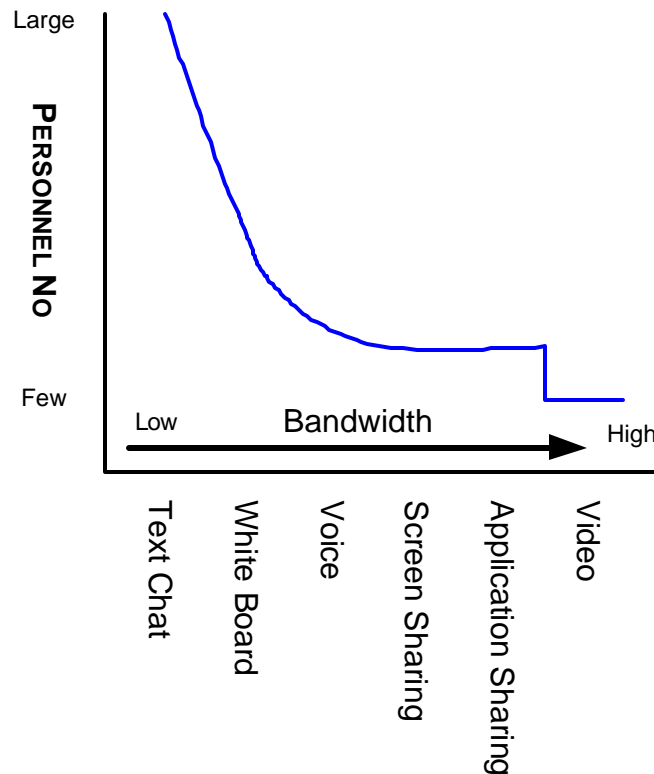


Figure 9-B-2 Operator Number Impact on Bandwidth Usage

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:

UNCLASSIFIED

Annex B to Chapter 9 to ACP 200(A)

- Mission
 - 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.

UNCLASSIFIED

Annex B to Chapter 9 to ACP 200(A)

- 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.
- 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 IAW OPTASK IM.
- 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.

UNCLASSIFIED

Annex B to Chapter 9 to ACP 200(A)

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

UNCLASSIFIED

Annex B to Chapter 9 to ACP 200(A)

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:
 - (1) Employ an agenda to help control the direction of a meeting.
 - (2) Solicit input for an agenda and circulate the agenda well in advance.

UNCLASSIFIED

Annex B to Chapter 9 to ACP 200(A)

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

9A11 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.

CHAT USER GUIDE

9B101 INTRODUCTION

- a. CHAT has evolved to become a tool of choice by many users of the world wide web, and the list of available tools include: Microsoft Messenger, Microsoft Netmeeting, America On Line (AOL) messenger, Yahoo messenger, IBM Lotus Sametime and various “Freeware” Internet Relay Chat (IRC) clients (including mIRC). These applications have been used effectively to support military operations and are now considered a key planning and co-ordination tool.
- b. Real-time operational CHAT circuits have been used in recent operations replacing traditional real-time voice circuits to co-ordinate war-fighting evolutions amongst networked platforms. To ensure interoperability, maritime coalition networks adopted IBM Lotus Sametime as the common application. In order to ensure CHAT is employed effectively, dedicated procedures should be followed.

9B102 AIM

This Appendix provides guidance on the efficient use of CHAT.

9B103 USE OF CHAT

When promulgating CHAT policy, the Task Force/Group Commander should consider existing operational voice circuits in the OPTASK COMMS and address the following points in the OPTASK IM (See Chapter 3):

- Control of the CHAT Room
- Procedures used in the CHAT Room
- Requirements to Record/Log CHAT Room dialogue (See CHAT Logging)
- Time Stamping of dialogue within the CHAT Room (See Time Stamping)

9B104 CHAT TYPES

As stated in Annex B, currently there is no universal agreed standard for the design and capabilities of CHAT products. Consequently, proprietary products have been developed offering different capabilities and benefits. A default standard used by existing CHAT products is SIMPLE (see Annex B). The following CHAT capabilities exist in all or some products:

- **Scheduled Meeting (SM) CHAT.** This creates a permanent meeting room that remains available for use at all times with or without someone in the actual meeting room. There is no requirement to “invite” another user into the CHAT meeting, which allows users to enter and leave the SM CHAT room as operations dictate.

- **Impromptu (Transitory) CHAT.** This is the most common form of CHAT where users conduct an impromptu CHAT session with another user.
- **Multiple CHAT Rooms.** Some applications provide the capability to conduct multiple CHAT sessions with different users from different panes. There is no system limit to the number of CHAT sessions that can be conducted, but it is recommended that no more than six simultaneous CHAT sessions be maintained at any one time to avoid User information overload. This should be reduced to four when other applications are also being used simultaneously.
- **Awareness.** Some applications give a visual indication as to the status of users within a CHAT Room. Users are able to define their status (e.g. on-line, away, off-line) and provide additional support information.
- **Time Stamping and CHAT Logger.** Some applications provide a facility to time-stamp and record CHAT transmissions for formal recording purposes.
- **Persistent CHAT.** CHAT is a synchronous real-time system. If a user joins a CHAT session late, or drops out of an existing session, there is no record of the discussion that has taken place during the period of absence. "Persistent CHAT" is a tool that allows users to recall CHAT conversations within a CHAT room to review information previously passed.

9B105 BENEFITS

CHAT has a number of advantages over the more traditional means of communication at sea:

- **Ease of use.** CHAT is easily learned by new users, particularly for those users familiar with internet CHAT rooms.
- **Clarity.** CHAT can serve as a medium for clear reports to be sent to superiors and clear direction to be received simultaneously by multiple subordinates. The CHAT record can be reviewed to confirm information passed should doubt exist.
- **Accurate Relay.** Reports to superiors can be cut and pasted in their original form, eliminating changes to the original message caused by multiple voice relay of the original report.
- **Flexibility.** CHAT sessions can be quickly established as required between participants. For example, key personnel can be brought together to discuss events in near real-time to exchange views and pass guidance.

- **Speed of Information Transfer.** Direct data input (including large volumes of data through “cutting and pasting” between CHAT participants) can significantly increase information transfer, obviating the need for separate systems and specialist/trained operators.
- **Planning and Coordination.** CHAT allows planning staffs at multiple levels to plan and coordinate activities.
- **Training and Situational Awareness (SA).** CHAT allows real time operations to be monitored worldwide by any user with network access. Units transiting to a theatre of operations can familiarise ship and staff with network tools and gain SA prior to arrival on station by collaborating in CHAT sessions to clarify issues.
- **History.** CHAT communications provide a written record of discussion, which can be reviewed. This is of particular use in reviewing intentions, forwarding information and maintaining a continual historical record.

9B106 DISADVANTAGES

CHAT is just one of the tools available within the MTWAN environment. Its ease of use and near real time information transfer between individual parties or groups can result in CHAT being used to the detriment of other more suitable applications. Disadvantages of CHAT are:

- **Speed of Data Input.** At the tactical and unit level, CHAT communications are invariably limited by typing speed and are slower than verbal information passed on voice nets. CHAT is not an adequate replacement for voice circuits that support fast-moving, real time tactical activity. Voice nets can provide the immediate acknowledgement that a message has been received and understood (“Roger Out”) that is not available by CHAT. For this reason, time sensitive reports such as ZIPPOS must continue to be passed via voice. After action reports to higher command once the raid is complete would be suitable information to be passed on CHAT. CHAT should be considered as complimenting traditional voice circuits, not as a direct replacement.
- **Distraction.** It is difficult for an operator to simultaneously monitor both CHAT and a tactical display, as both require the use of hands and eyes. This is particularly an issue at the PWO/ORO/TAO level. Voice nets remain far less cumbersome. During periods of high intensity, such as Action Stations, a dedicated CHAT operator should be allocated to operate CHAT sessions as directed by the OTC/CTG/Command.
- **Access.** All units participating in a coalition Task Force/Group may not be network-enabled. Operational SITREPS and other pertinent

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 9 to ACP 200

information should be relayed using other communications means to "non-network enabled" units to maintain Task Force/Group situational awareness.

- **Dependency.** Over reliance on CHAT for passing information will provide significant limitations on information flow when MTWAN connectivity is unavailable. This effect can be compounded by user hesitancy to pass required information by other means (ie voice nets, formal record traffic (signal) while waiting the "imminent" restoration of MTWAN connectivity.
- **Receptionist Syndrome.** The worldwide connectivity provided by national and coalition networks result in individual units (who are fitted with both) being requested to fulfill a 'relay' role between other users. CHAT should never be used as a convenient means of communication or message forwarding service.
- **Big Brother Syndrome.** The ability of higher command to communicate in real-time to deployed units can lead to front-line units feeling that they are under excessive supervision. The use of CHAT tactical meeting rooms for administrative traffic can also provide an unnecessary distraction during high-intensity operations.

9B107 INAPPROPRIATE EMPLOYMENT

CHAT is easy to use and users can fall victim to practices for which the CHAT tool was not intended. In some cases the use represents optimisation of the capability, however, frequently it reflects a lack of user awareness of the capability (compared to other applications) on the network. Inappropriate activities include:

- **Cut & Paste.** Large amounts of information can be cut and pasted into CHAT windows then transmitted across the network. This occurs most commonly when a user re-joins a CHAT room after an outage and requests an update of previous "discussion" or in response to a request for specific information. By using an existing CHAT room, information is unnecessarily re-sent to all participants, disrupting the rhythm of the information flow and wasting bandwidth. A more efficient way of providing this information would be via a separate impromptu CHAT room or e-mail depending on the time sensitivity of the information.
- **Monopolising CHAT Rooms.** In Scheduled Meeting rooms, two users can monopolise the room whilst "discussing" a particular subject. A more efficient use of bandwidth is for those users to move to an impromptu CHAT session leaving the main CHAT room available for other users.
- **Verbosity.** Informality and familiarity during a CHAT session should be avoided. As in all forms of communication, brevity should be

UNCLASSIFIED

Appendix 1 to Annex B to Chapter 9 to ACP 200

employed to ensure that the necessary information is exchanged with the minimum of data input. This can be achieved by the use of recognised and standard abbreviations, procedures developed for particular war-fighting environments or short phrases, which have been become common in today's technological age.

9B108 "THE GOLDEN RULES"

If DCP tools are to become a force multiplier, it is essential that each of the applications be used to their optimum. Observance of the following "GOLDEN RULES" will greatly enhance the performance of the CHAT application:

1. The policy for the establishment and employment of CHAT rooms within a TG is clearly stated within the OPTASK IM.
2. Prior to using the CHAT tool, users are to consider all the DCP tool options to ensure that CHAT is the most suitable tool for the information transfer.
3. Scheduled Meetings should be the normal mode of operation.
4. CHAT users should ensure that information transferred in a CHAT session is appropriate to the CHAT room in use.

Chapter 10**NETWORK ARCHITECTURE****1001 INTRODUCTION**

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

1002 AIM

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

1003 OVERVIEW

- a. The term ‘network architecture’ is commonly used to describe a set of abstract principles for the technical design of protocols and mechanisms for computer communication. The MTWAN Network Architecture (NA) represents a set of deliberate choices from a set of design alternatives, where the choices are informed by an understanding of the requirements canvassed in Chapter 2. In turn, this architecture provides a guide for the many technical decisions required to standardise network protocols, algorithms and schemas that appear in the subsequent chapters. The purpose of the architecture is to provide coherence and consistency to these decisions and to ensure that the requirements are met.
- b. A Network Architecture describes:
 - 1) The overall geographic layout of the network,
 - 2) How it is connected to other networks,
 - 3) How computers will communicate with one another,
 - 4) How entities, such as computers and domains, are named ,
 - 5) Where security boundaries are drawn and how they are enforced,
 - 6) How management boundaries are drawn and selectively pierced.

1004 DESCRIPTION

- a. An MTWAN (Figure 10–1) comprises one or more Task Group Area Networks (TGANs) where a TGAN is a collection of mobile units such as ships and submarines. It may also include Maritime Marine Force (MMF) and Maritime Air Groups (MAG) as well as Network Operation Centers (NOCs).

- b. Within an MTWAN, connectivity between mobile units is via Radio Frequency (RF) communications (although NOC-to-NOC connectivity may be terrestrial).
- c. In terms of topology and routing protocols, an MTWAN is influenced by its distributed and low bandwidth, high latency environment. An important key to the MTWAN routing architecture (and any routing architecture) is the design and management of Autonomous Systems.

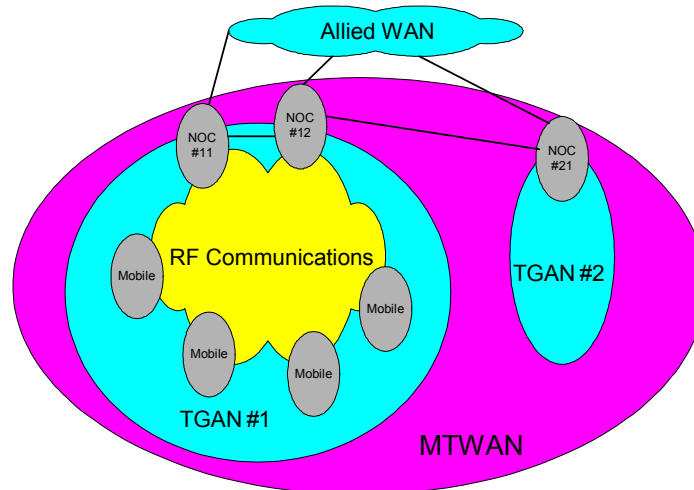


Figure 10-1 Notional MTWAN Architecture

1005 ROUTING ARCHITECTURE (RA)

- a. **Autonomous Systems (AS).** An MTWAN comprises one or more ASes. An AS is a collection of networks, or more precisely, the routers joining those networks, that are under the same administrative authority and that share a common routing strategy. An AS has a single ‘interior’ routing protocol and policy, and is also sometimes referred to as a routing domain. Interior routing information is shared among routers within the AS, but not with systems outside the AS. However, an AS may announce its internal networks to other ASes that it is linked to. On the Internet, an AS is an Internet Service Provider (ISP), but universities, research institutes, and private organizations also usually have their own ASes.
- b. **Topology.** The MWTAN is a distributed system. As a distributed network, there are two considerations: the network topology (‘what is connected to what, with what constraints?’) and the physical location (‘what is physically near what?’). In terms of topologies, MTWAN employs either a single-AS TGAN topology or a multiple-AS TGAN

topology. The latter is generally employed to allow nations within an MTWAN to administer their own mobile units.

- c. **Single-AS TGAN Topology.** An example of a single-AS TGAN is shown in Figure 10–2. All mobile units and the NOC belong to the same AS. The TGAN may have multiple connections to the allied WAN for redundancy and load sharing.

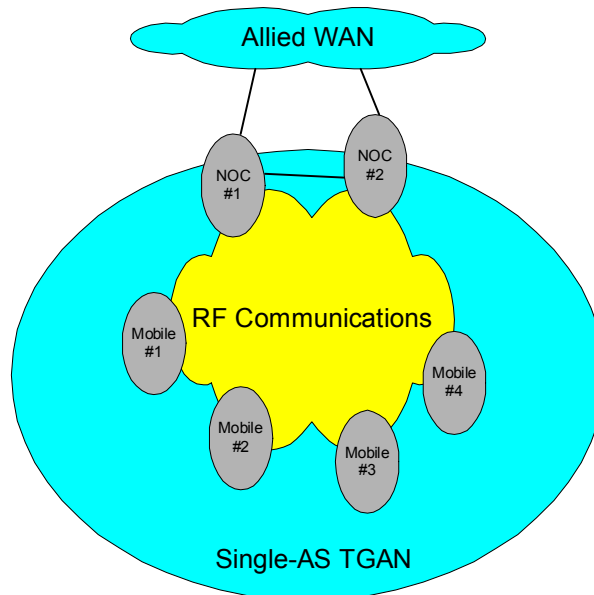


Figure 10–2 Single-AS TGAN

- d. **Multiple-AS TGAN Topology.** A nation may set up its own AS within a TGAN. Each AS will contain a group of mobile units as illustrated in Figure 10–3. Each mobile unit will have peer-to-peer connections to other mobile units; these connections may be via any communications path but are typically via tactical circuits such as HF/UHF. Some of the mobile units may have connectivity back to the Allied WAN via a national node or NOC. When this connectivity is achieved, the NOC forms part of the AS. Communication between the mobile unit and the NOC is typically done via Military or Commercial SATCOM. National NOCs may host connections from other nations' mobile units.
- e. Design and implementation of unicast and multicast routing in support of a multiple-AS TGAN is much more difficult in comparison to a single-AS one. However, a multiple-AS topology will allow each nation to control and manage its own AS. Moreover, route changes inside an AS can be hidden from other AS's. As a result, the new routing information will not need to be propagated throughout the

TGAN and therefore will not consume valuable communication bandwidth.

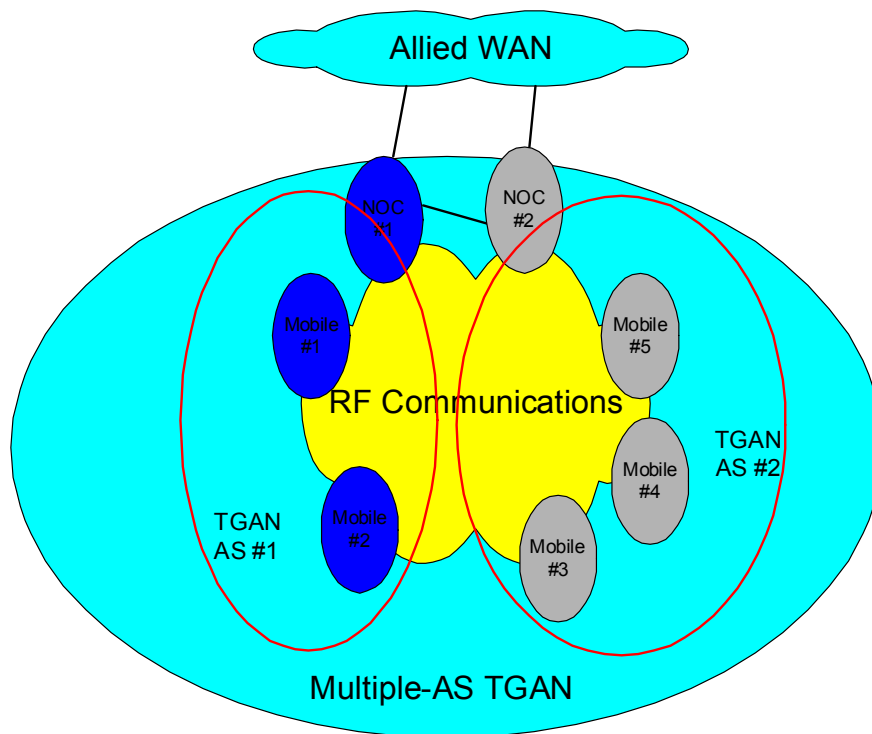


Figure 10–3 Multiple-AS TGAN

- f. **Routing Protocols.** An MTWAN employs standard IP routing protocols to achieve connectivity. This has the advantage of utilizing Commercially-Off-The-Shelf (COTS) equipment, but constrains the amount of configuration that can be done to the network. Routing is achieved using standard protocols Open Shortest Path First (OSPF) and Protocol Independent Multicast (PIM) for routing within the AS (interior-AS routing), and Border Gateway Protocol Version 4 (BGP4) for routing between AS's (exterior-AS routing). Figure 10-4 shows a MTWAN that comprises a single-AS TGAN and depicts where BGP4 and OSPF are deployed. Detailed information on the routing architecture can be found in Chapter 15

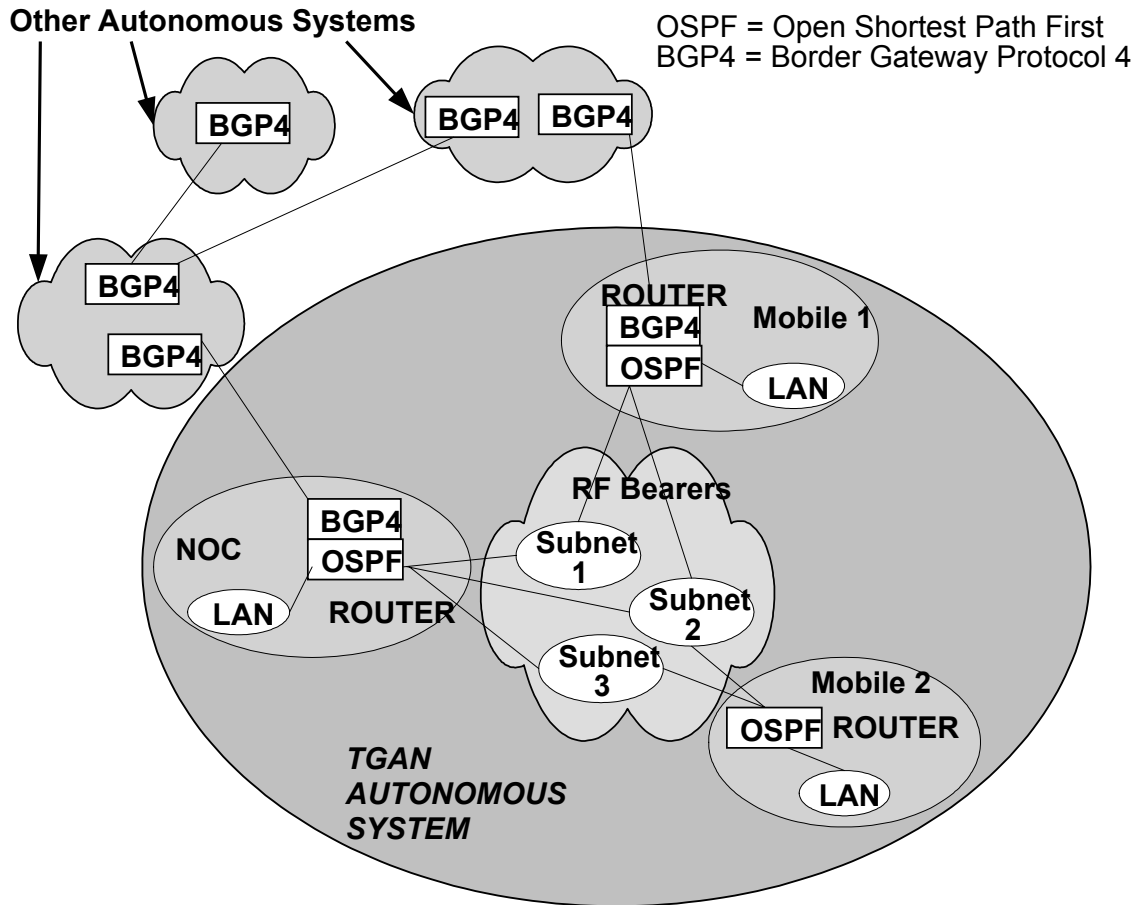


Figure 10–4 MTWAN Routing

1006 COMMUNICATIONS ARCHITECTURE (CA)

- a. The communication subnets within a TGAN, such as those shown in Figure 10–4 are supported by point-to-point and multi-member (shared) links.
- b. **Point-to-Point.** Point-to-point links are communication bearers that connect two nodes in either full-duplex or half-duplex mode. Examples of full-duplex point-to-point links are INMARSAT and SHF. A half-duplex point-to-point link between two nodes can be established using radios operating on a single frequency as only one node can transmit at any one time.
- c. **Multi-member.** Multi-member links are those that connect two or more nodes, whereas a point-to-point link supports two nodes only. In a multi-member or half-duplex point-to-point link, a single RF channel is shared. As an example, this can be achieved by a Time Division

Multiple Access (TDMA) technique. Multi-member links are further divided into two categories: Broadcast and Non-Broadcast Multiple-Access (NBMA). In a Broadcast subnet, all members can hear each other. UHF SATCOM is an example of a broadcast multi-member link when all members are within the footprint of a satellite. In a NBMA subnet, full connectivity among all members can not be guaranteed, that is, not every member can hear every other member. An example of a NBMA subnet is UHF Line-Of-Sight (LOS). Due to its movement, a member may be out of the UHF LOS range of some, but not all, members of the subnet.

- d. A wide range of subnet combinations exist, some of which are shown in the Figure 10–5. Communications subnets that can be employed with a MTWAN are described in Chapter 16.

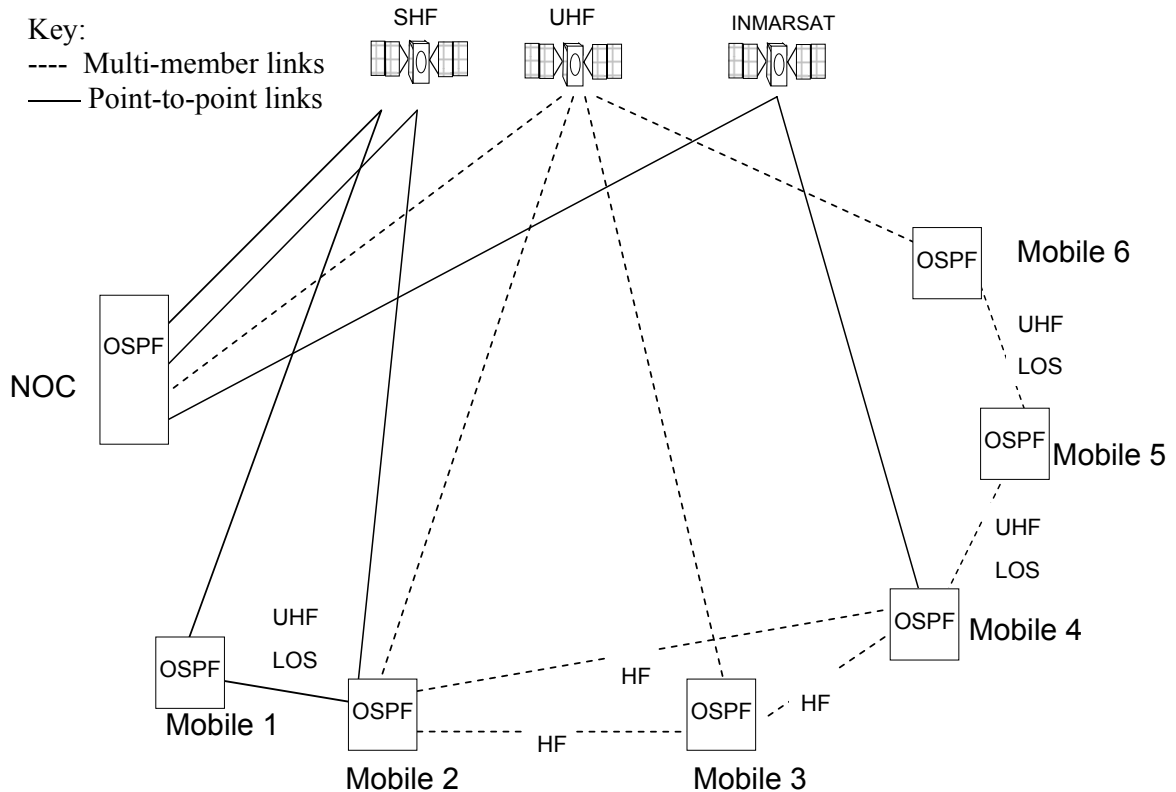


Figure 10–5 Subnet Combinations

1007 SECURITY ARCHITECTURE (SA)

- a. The security architecture is designed to promote the flow of information at the tactical level while abiding by Allied security policies. This can be achieved through the use of the following:
 - (1) Allied peer-to-peer tactical communications networks that are isolated from Coalition and National networks.
 - (2) Boundary Protection Devices (BPD) to enable the exchange of applications data between different security levels.
 - (3) Inline Network Encryptor (INE) to support Virtual Private Networks (VPN) over an existing IP infrastructure of a different security level.
- b. For example, an INE such as TACLANE can be used to create an allied VPN and tunnel allied IP traffic through national networks, subject to the security policy of the respective nation. Network security details can be found in Chapter 5.

1008 NODE DESCRIPTIONS

- a. **Generic Mobile Node.** The generic architecture of a typical mobile node consists of the following: RF communication systems, modems, link cryptographic devices, a router, any necessary interface equipment needed to interface RF channels to the router, and a LAN. Examples of the RF communication systems include INMARSAT, MILSATCOM, HF and UHF. Details of the communication systems and their interface equipment can be found in Chapter 16. The LAN equipment includes servers, workstations, printers and hubs on which information resides and applications run. Examples of applications are E-mail, GCCS-M, Web services and Distributed Collaborative Planning (DCP) tools.
- b. Subject to national security policy, connection between nodes can be done via the infrastructure provided by another IP network of a different security level. An INE will connect the MTWAN router to the router of the other network.

1009 CONCLUSION

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

NETWORK ARCHITECTURE TO SUPPORT AMPHIBIOUS OPERATIONS

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 OVERVIEW

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

10A04 TRANSIT

A typical network configuration in the transit phase is shown in Figure 10–A–1. In this example, three MMF units are located on three amphibious ships. The ships are part of the TGAN autonomous system (AS). Each MMF unit consists of a collection of host computers, LANs and routers, which operate in a separate MMF autonomous system, connected to the ships TGAN autonomous system using the BGP4 protocol as shown in Figure 10–A–2. Any communication between the MMFs in the transit phase would use the TGAN backbone subnets.

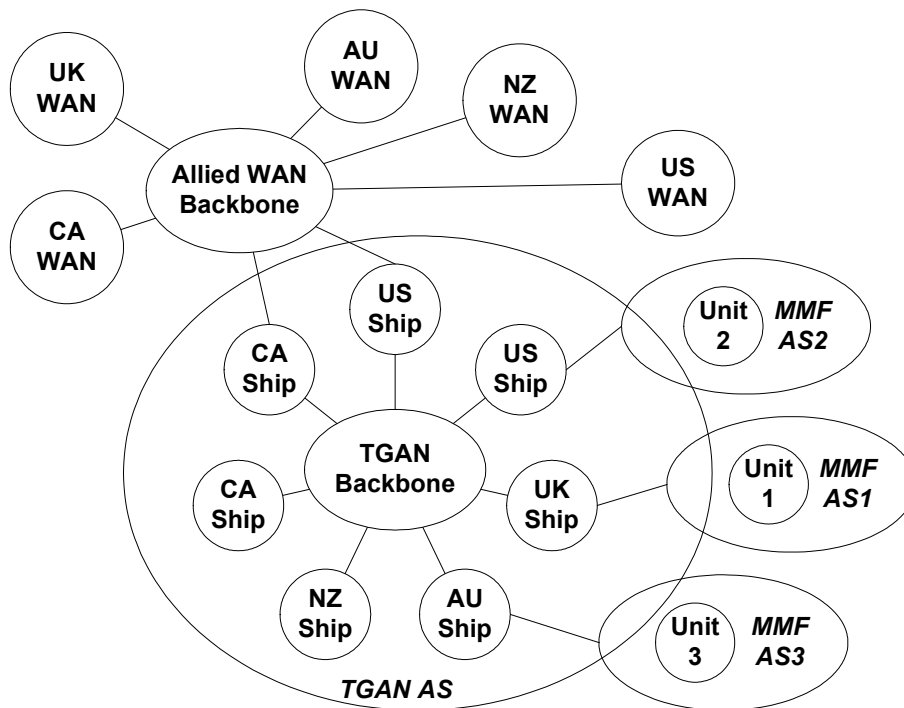


Figure 10-A-1 Transit Network Connectivity

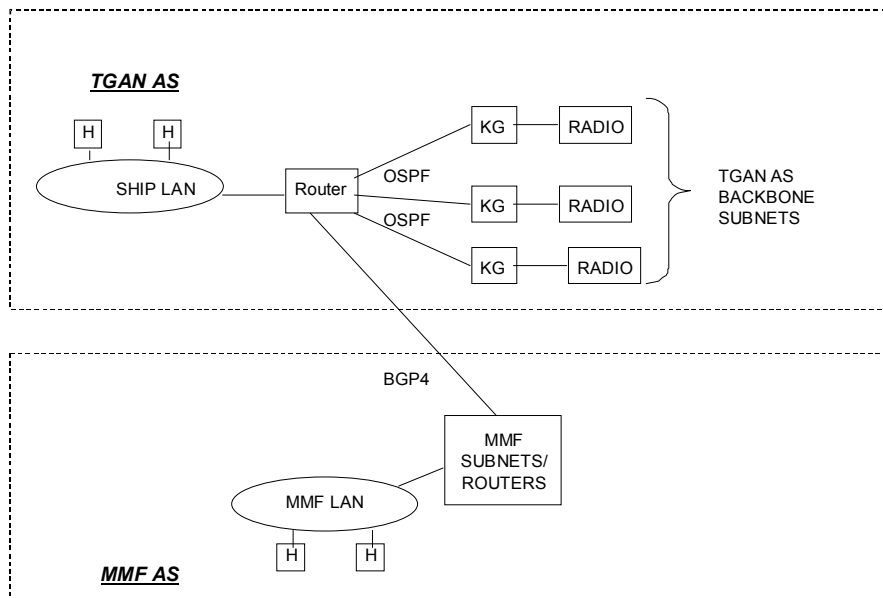


Figure 10-A-2 MMF Node Configuration in Transit Phase

10A05 ASSAULT

- a. In a typical assault phase the network connections are shown as in the example, Figure 10-A-3. In this phase the MMF units have disembarked and set up subnets back to the units command ship. The

MMF units remain in their own AS. Any communications between the ashore units will be through their command ships and over the MMF backbone subnets. The ship node configuration remains the same as in the transit phase except the MMF subnets are placed in operation.

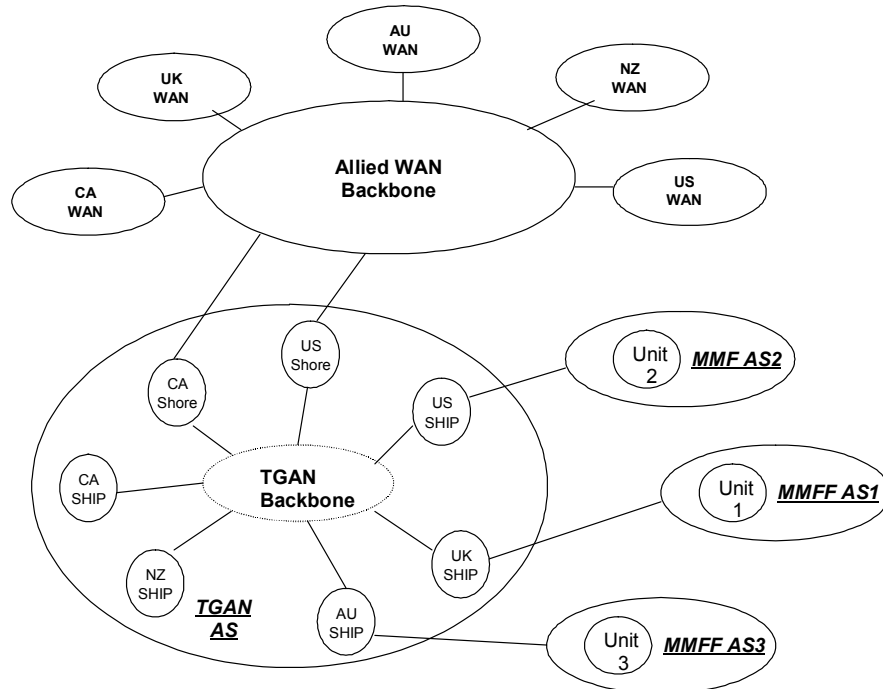


Figure 10-A-3 Network Connection in Assault Phase

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

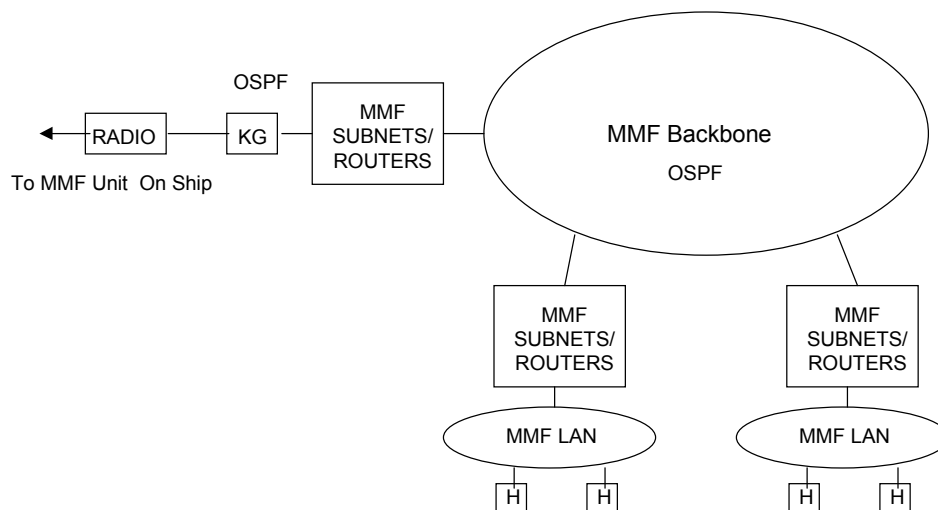


Figure 10-A-4 MMF Shore Node Configurations – Assault Phase

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

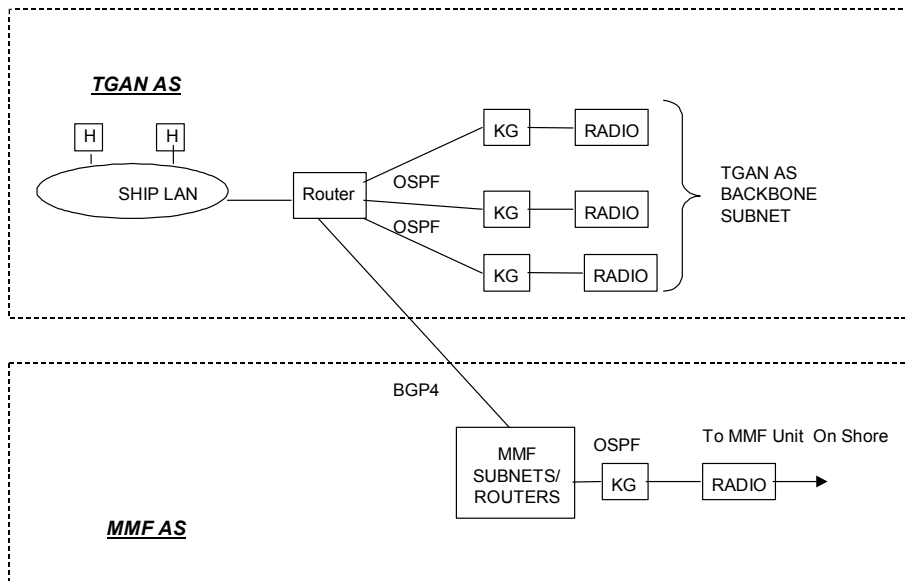


Figure 10-A-5 Ship Node in Assault Phase

10A06 LODGMENT

- a. 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.

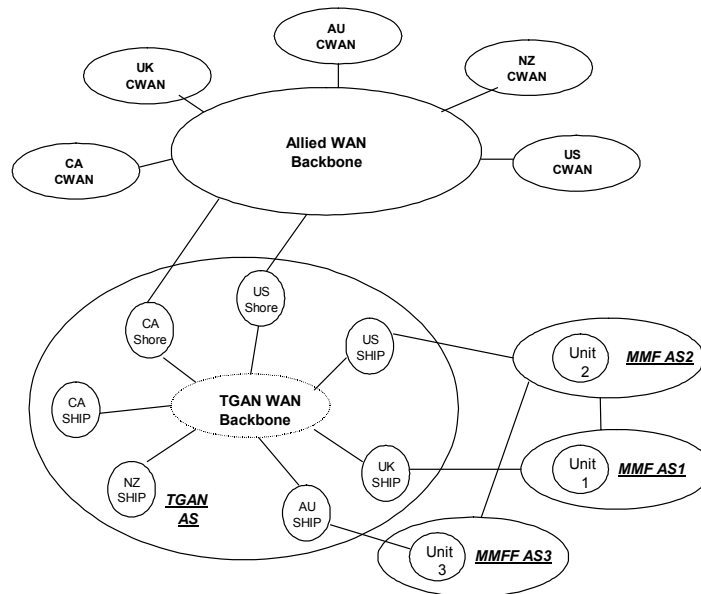


Figure 10-A-6 Network Connection in Lodgment Phase

- b. 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.

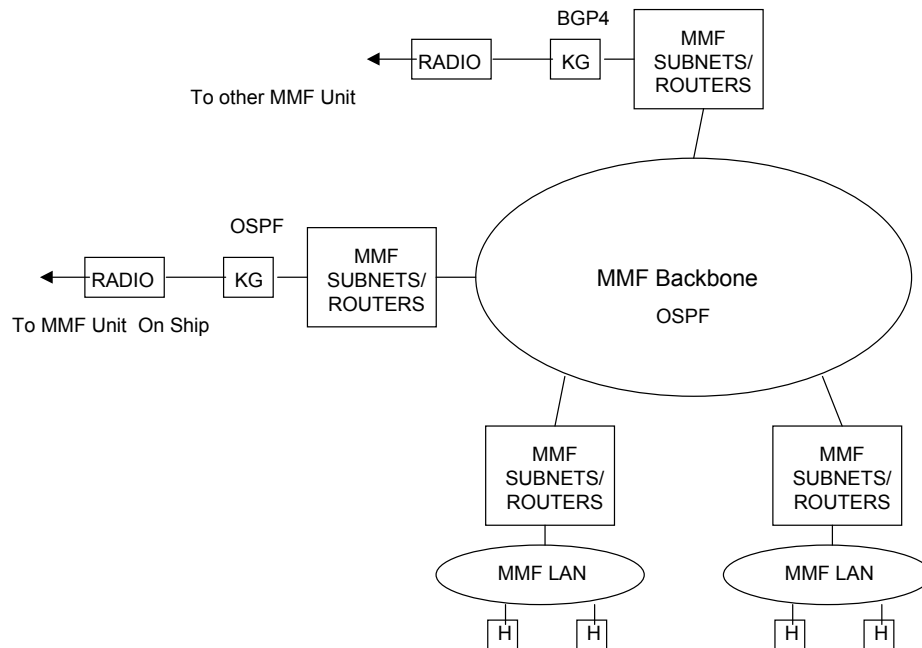


Figure 10–A–7 MMF Network Nodes in Lodgment Phase

10A07 SUSTAINMENT

- a. 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.

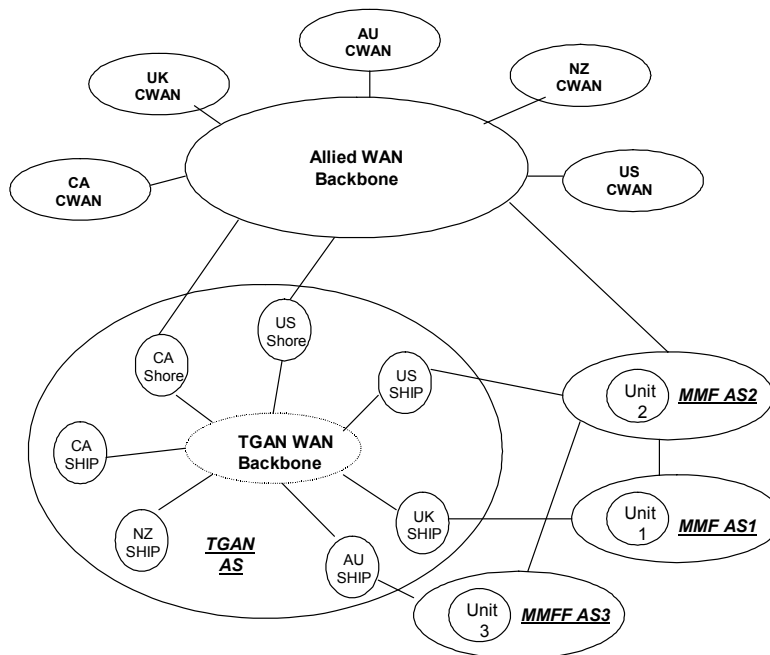


Figure 10-A-8 Network in Sustainment Phase

- b. 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.

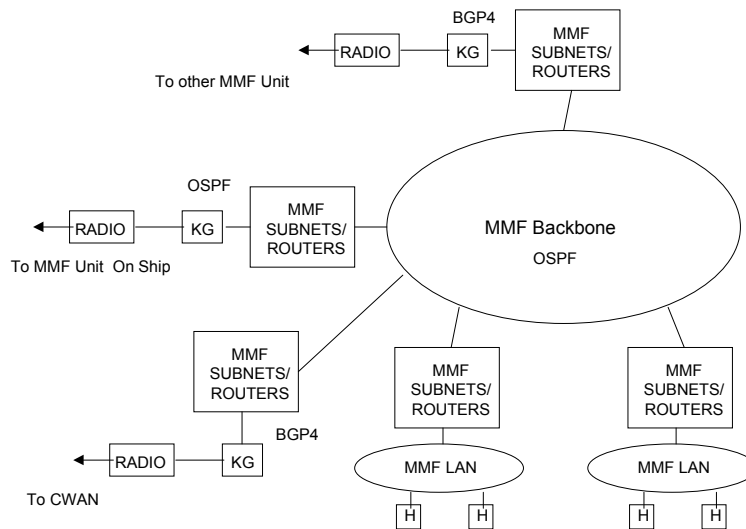


Figure 10-A-9 MMF Unit 2 Node Configuration in Sustainment Phase

Chapter 11

QUALITY OF SERVICE

1101 INTRODUCTION

- a. The "best-effort" nature of IP-based networking can result in significant performance degradation when a network becomes congested. This is more likely to occur in bandwidth constrained and high latency environments such as Wide Area Networks (WANs) than within Local Area Networks (LANs).
- b. To minimise the operational impact of congestion within WANs, it is highly desirable to implement Quality of Service (QoS) to optimise the traffic flow across WAN links and to ensure that more important traffic is afforded an improved grade of service. This becomes essential when data, voice and video are converged onto a single network.

1102 AIM

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

1103 OVERVIEW

- a. IP only provides Best Effort Service in that traffic is processed as quickly as possible, but there is no guarantee as to timeliness or actual delivery. However, the fundamental concept behind QoS is that better service to certain traffic flows can be provided by either raising the priority of a flow or limiting the priority of another flow.
- b. This chapter concentrates on improving the performance of IP packet flow through the network(s). The challenge from a technical perspective is how to make the right trade-off between simplicity and control to ensure a predictable and manageable network.

1104 DEFINITION

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

- a. **Predictability and Consistency.** A service response is predictable when the conditions for its delivery are known over a period of time. Consistency is the difference between the nature of an expected response and the actual one.
- b. **Guarantee.** There needs to be some level of assurance in terms of predictability and consistency.
- c. **Management.** A management function is necessary in achieving predictability and consistency and includes such mechanisms as negotiation, admission control and monitoring.
- d. **End-to-end.** QoS is really only achieved in a distributed application if it has been addressed at every level of the OSI 7-layer model.

1105 LINK THROUGHPUT / BOTTLENECK

- a. Internet routers are constrained in terms of processing power and memory storage, but the available bandwidth interconnecting them can be very large (e.g. fiber) and there is no power problems. In MTWANs, the available bandwidth is very limited and some MTWAN routers may have severe energy constraints as well (e.g. relying on battery power), but the processing power and storage capabilities—both increasing rapidly due to hardware advances—are relatively unconstrained considering the router throughputs and network sizes that must be supported. Subsequently, the principal bottlenecks for any MTWAN is the throughput of its WAN links. Unmanaged congestion at speed-conversion bottlenecks on WAN-access links leads to unpredictable delays.
- b. The primary causes of slow throughput on WANs are well known: high delay (a.k.a. round trip time or latency), limited bandwidth, and “chatty” application protocols. This chapter addresses how to improve the performance of IP packets through WAN links. In doing so, a secondary result will likely be performance improvements within LANs.
- c. The temptation to define communication subnets using simplistic measures such as raw bandwidth alone should be avoided. Instead it is necessary to look for measures that directly relate to the ability of the facilities to support the higher-

level services, measures that specify QoS parameters such as bandwidth, delay, and loss characteristics.

1106 MAXIMISING LINK THROUGHPUT

- a. If link throughput is sub-optimal, simply adding bandwidth or compression will not necessarily solve the problem of application performance on WANs. One reason is because critical applications that suffer poor performance are not necessarily the applications that get access to extra capacity. Paradoxically, it usually is the less-urgent, bandwidth hungry applications that monopolise increased bandwidth.
- b. **Latency.** Firstly, the ‘round-trip time’ of a packet of data (a.k.a network latency), has a direct effect on the performance or throughput of a window-based protocol like TCP or any request-response protocol. High round trip times particularly slow down "chatty" applications, even if the actual amounts of data transmitted in each transaction are not large.
- c. Adding bandwidth (or compressing data) does not improve throughput when the round-trip time exceeds the critical point where throughput is bounded, or when the problem is primarily latency and not bandwidth related. Once the latency exceeds the critical point, throughput decays quickly.
- d. This effect is easy to understand intuitively: the rate of work that can be performed by a client-server application that executes serialized steps to accomplish its tasks is inversely proportional to the round-trip time between the client and the server. If the client-server application is bottlenecked in a serialized computation (i.e., it is "chatty"), then increasing the round-trip time by a factor of two causes the throughput to decrease by a factor of two—it takes twice as long to perform each step (while the client waits for the server and vice versa).
- e. More generally, the throughput of client-server applications that are not “chatty” but run over a window-based protocol (like TCP) can also suffer a similar fate. This can be modeled with a simple equation that accounts for the round-trip time (RTT) and the protocol window (W). The window is how much the sender can transmit before receiving acknowledgement from the receiver. Once a window's worth of data is sent, the sender must wait until it hears from the receiver. Since it takes a round-trip time to receive the acknowledgement from the receiver, the rate at which data can be sent is simply the window size divided by the round trip time: $T = W / RTT$.
- f. **TCP Congestion Control.** Secondly, an additional constraint on throughput has to do with the congestion control algorithm designed into TCP. This flaw

can be significant even in WANs where bandwidth is above a few megabits and is probably the key reason why one often fails to see marked performance improvements of individual applications after bandwidth is substantially increased. This effect is so dramatic that at 100ms of delay (i.e. a typical cross country link), TCP is able to use only 4.5 Mbps of a 45 Mbps link.

1107 CONTROLLING LESS URGENT TRAFFIC

- a. Large packets delivered from lower priority, high bandwidth applications may affect the latency for higher priority, latency intolerant applications (such as voice). For example, a 1500 byte packet delivered as part of a file transfer over a 64 Kbps link will take 187 ms to be transmitted. This means a voice packet cannot be transmitted during this interval. As a result, voice cuts or delays will be heard for voice traffic queued behind this large packet.
- b. Different speed links in the network may mean that packets can get queued internally in the network. When packets queue internally in the backbone of a network, latency and therefore quality can be affected.
- c. Subsequently, it is important to be able to pace important but less urgent traffic (such as Quality of Life E-mail and Web Services).

1108 OBJECTIVE

- a. The objective of QoS is therefore to achieve end to end predictability of IP packet delivery for Command through:
 - (1) **Visibility** of the WAN connection,
 - (2) **Ensuring** critical application performance,
 - (3) **Controlling** less urgent traffic,
 - (4) **Maximising** throughput, and
 - (5) **Analysing** response times, link allocation, and network efficiency.
- b. The architecture must recognise network limitations, such as latency and unreliability, and shield them from users. This principle, to be aware of the network and its underlying faults but make them transparent to the user as much as possible, is a goal of QoS.

1109 VISIBILITY

UNCLASSIFIED

ACP 200(A)

- a. Visibility of the network is a necessary first step towards implementing any QoS solution. It is important to understand what is occurring in a network (i.e. precisely which applications transverse the network, what portion of the network they consume, how well they perform, and where the delays originate etc) before one can effectively control and compress any traffic intelligently. Ideally this requires a solution capable of providing in-depth visibility, analysis and trending of the network.
- b. **Types of Applications.** The application types play a major role in the network performance. Essentially there are three kinds of network applications:
 - (1) **Normal (elastic).** Elastic applications can take advantage of however much or little bandwidth is available. Essentially they are written to run 'as fast as they can'. Examples include e-mail, and FTP.
 - (2) **Tolerant real-time (static).** Through buffering the receiver to dampen variation, these applications can tolerate delays. An example is streaming video broadcasts.
 - (3) **Intolerant or Inelastic real-time (live).** These applications require a certain level of bandwidth to function. If they get more than that they cannot use it, and if they get less, then it can not function at all as they are not tolerant of delays or variation. Examples include VoIP and VTC. VoIP is characterized as relatively low bandwidth, but requiring a low latency and low jitter delivery to ensure toll quality. VTC requires higher bandwidth, but still requiring low latency and low jitter for high quality video and sound.
- c. These applications / services differ widely in the QoS they require from the infrastructure. The result of inappropriate priority and precedence can vary from information arriving late (e.g. message delayed) to being incomprehensible (e.g. real-time video & voice with excessive latency and jitter).
- d. **Performance Measures.** The following measures are commonly used in describing application performance:
 - (1) Service availability—the reliability of the user's connection to the network.
 - (2) Delay—the time interval between transmitting and receiving packets (ie *latency*).
 - (3) Delay variation—the variation in duration between all packets in a stream taking the same route (ie *jitter*).

- (4) Packet loss rate—the maximum rate at which can be discarded during transfer through a network. This actually results from congestion.
- e. **Classification.** To provide preferential service to a type of traffic, it must first be identified. Second, the packet may or may not be marked. These two tasks make up classification. When the packet is identified but not marked, classification is said to be on a per-hop basis. This is when the classification pertains only to the device that it is on, not passed to the next router. This happens with Priority Queuing (PQ) and Custom Queuing (CQ). When packets are marked for network-wide use, IP precedence bits can be set.
- f. Common methods of identifying flows include Access Control Lists (ACLs), policy-based routing, Committed Access Rate (CAR), and Network-Based Application Recognition (NBAR).

1110 CONTROL

- a. Flexible policies are required to protect critical applications, pace greedy traffic, limit recreational usage, and block malicious traffic. These policies should be able to:
 - (1) Protect the performance of important applications,
 - (2) Contain unsanctioned and recreational traffic,
 - (3) Provision steady streams for inelastic applications such as voice and VTC,
 - (4) Stop applications or users from monopolising the link,
 - (5) Reserve or cap bandwidth,
 - (6) Provision bandwidth between multiple locations, groups or users.
- b. *Service levels* refer to the actual end-to-end QoS capabilities, meaning the capability of a network to deliver service needed by specific network traffic from end to end or edge to edge. The services differ in their level of *QoS strictness*, which describes how tightly the service can be bound by specific bandwidth, delay, jitter, and loss characteristics.
- c. Three basic levels of end-to-end QoS can be provided across a heterogeneous network, as shown in Figure 11–1:
 - (1) **Best-effort service**—Also known as lack of QoS, best-effort service is basic connectivity with no guarantees. This is best characterized by

First In, First Out (FIFO) queues, which have no differentiation between flows.

- (2) **Differentiated service (also called soft QoS)**—Some traffic is treated better than the rest (faster handling, more average bandwidth, and lower average loss rate). This is a statistical preference, not a hard and fast guarantee. This is provided by classification of traffic and the use of QoS tools such as PQ, CQ, Weighted Fair Queuing (WFQ), and Weighted Random Early Dropping (WRED).
- (3) **Guaranteed service (also called hard QoS)**—This is an absolute reservation of network resources for specific traffic. This is provided through QoS tools Resource ReServation Protocol (RSVP) and Class Based Weighted Fair Queuing (CBWFQ).

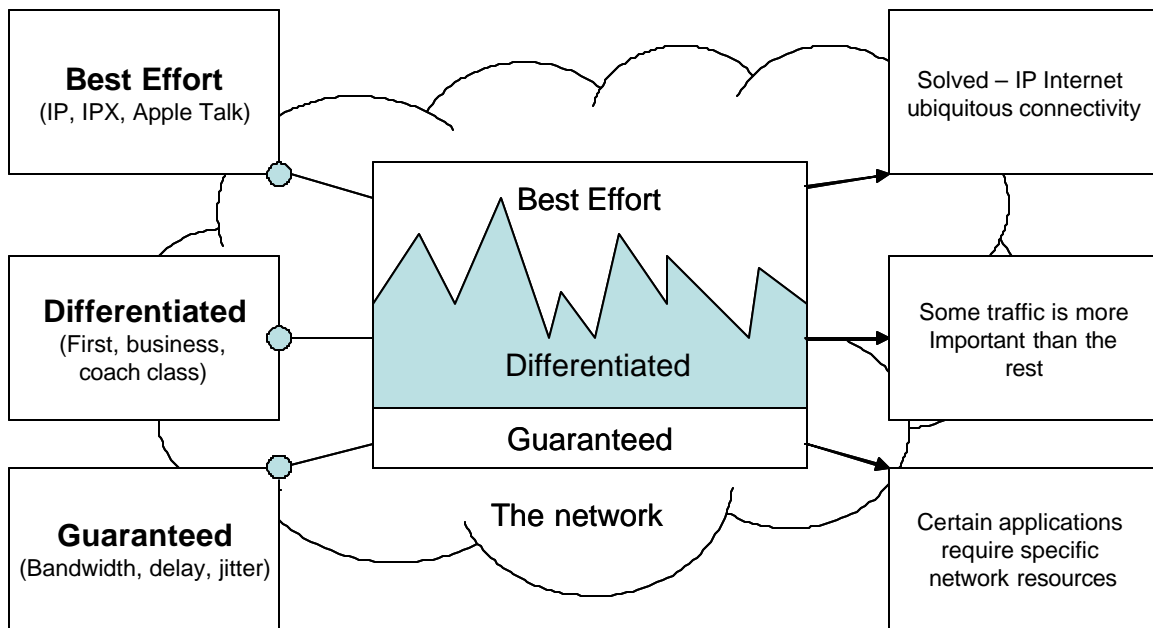


Figure 11–1 Grades of Service

- d. Deciding which type of service is appropriate to deploy in the network depends upon:
 - (1) Whether the current infrastructure can support the specific QoS methods intended.
 - (2) The application or problem that Command is trying to solve.
 - (3) Whether it is simple to deploy and simple to maintain.

1111 COMPRESSION

- a. Compression allows more data to flow through constrained WAN links, freeing bandwidth for the critical applications that need it the most. While control prioritizes mission-critical applications and smoothes bursty traffic, compression enhances performance by creating greater throughput, faster performance, and increased network capacity.
- b. Types of Compression:
 - (1) File—addressed by Information Management practices.
 - (2) Application.
 - (3) Network.
- c. **Pair-wise configuration.** Application and network compression requires at least two compression devices, one deployed at each end of a connection. Each device compresses its outbound traffic, and each unit at the receiving end will decompress inbound traffic, restoring traffic to its original state.
- d. Previously compressed traffic (such as VoIP and streaming video) and encrypted data (such as HTTPS, SSH and encrypted Domino databases) can not be compressed further. Binary files, and non-repeating data, do not fare as well as Web and text files which are more compressible.

1112 QoS SOLUTIONS

- a. Today there are a plethora of vendors who offer end to end solution packages. These hardware devices called WAN accelerators or optimizers, compress and cache data, modify TCP parameters and enforce QoS (quality of service) using prioritization and rate shaping.
- b. While some vendors claim their devices increase network performance tenfold, independent tests have typically demonstrated a four fold improvement in throughput performance. Protocol prioritization and rate limiting QoS mechanism vice Differentiated Services (DiffServ) or Integrated Services (IntServ) technologies are typically employed.
- c. Such solutions are attractive due to the fact that they are relatively simple to deploy and maintain. With the devices strategically positioned they can monitor and visualize the network. Once the traffic flow is understood then QoS mechanisms can be introduced to control optimize the flow, and if the infrastructure provides pair-wise configuration, then compression can also be applied.

- d. **Interoperability.** While most / all vendors implement industry standards, there is no interoperability between vendor solutions.
- e. **Passthrough Failover.** It is desirable that any solution has passthrough failover. That is if any hardware device is unplugged, traffic will nonetheless pass through the device as if it were part of the wire.
- f. **Network Topology.** The hardware device should be able to be deployed in a hub-and-spoke or mesh topology. Those devices that require you to create links manually, however, are difficult to configure in a mesh environment.

1113 FUTURE WORK

- a. AUSCANNZUKUS nations are actively exploring QoS packages which should lead to a better understanding of QoS and vendors solutions. The information gleaned will be used to further develop this chapter in subsequent changes.
- b. QoS approaches that can be implemented at the router (vice through WAN accelerators / optimizers) need also to be agreed.
- c. **Mapping IER to QoS.** An outstanding issue that remains is how to map the warfighter's Information Exchange Requirements (IERs) into QoS outcomes while maintaining transparency to command. There is significant work being done in this field which will be reflected in the next change to this document.
- d. **IPv6.** The development of IPv6 will enhance our ability to perform QoS and manipulate packet flows. Until 2003, all routers were packet routers which only examined the packet and kept no flow history. The duration, rate or byte count of the flow could not be determined. Flow State Aware (FSA) routing such as Multi Protocol Label Switching (MPLS) can determine the duration, rate or byte count of the flow. It can identify flow types and control the rate and delay per flow.

1114 CONCLUSIONS

- a. Link throughput, vice bandwidth is the most important consideration when addressing IP connection speeds. QoS mechanisms can significantly enhance throughput and improve transmissions, without requiring extra bandwidth.
- b. In order to effectively and efficiently implement QoS, it is important to understand what is occurring in the network (i.e. visibility). Once this is understood, QoS control and compression can be implemented. The overall goal, however, should not be to squeeze improvement out of MTWAN's, if it adds complexity to training and operations.

Chapter 12

NETWORK MANAGEMENT

1201 INTRODUCTION

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

1202 AIM

This chapter provides 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.

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

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

UNCLASSIFIED

Annex A to Chapter 12 to ACP 200(A)

- Configuration of routers, servers and user workstations;
 - Installation of NM station;
 - 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

UNCLASSIFIED

Annex A to Chapter 12 to ACP 200(A)

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

12A06 NETWORK MANAGEMENT TOOLS SET -UP

- a. To establish NM tools discussed above, the following installation and set-up is required:
 - (1) Set up an engineering order wire to enable network management coordination.
 - (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

UNCLASSIFIED

Annex A to Chapter 12 to ACP 200(A)

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.*

- (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.
- c. 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.

UNCLASSIFIED

Annex A to Chapter 12 to ACP 200(A)

- (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 any routing problems and inform the NOC of the problems.

d. 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
(CLASSIFIED WHEN COMPLETED)

A. OVERVIEW

A1. Purpose

State the purpose of this OPTASK NET.

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 IM
- B4.4. OPTASK FOTC

C. DUTIES

Describe duties / responsibilities for network and NOC managers.

C1. CTG Network Manager

UNCLASSIFIED

Annex B to Chapter 12 to ACP 200(A)

C2. NOC Manager

C3. Unit Network Manager

D. NETWORK 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

UNCLASSIFIED

Annex B to Chapter 12 to ACP 200(A)

- 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
- F5. Subnet Relay
 - F5.1
 - F5.2

G. NETWORK MANAGEMENT

G1. Unit NM reporting requirements

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

G2. Help desk policy

Promulgate help desk policy and hours of operation.

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 Web Servers Supported (e.g Domino, Apache, IIS)
- H3.2 Domino Application Server Version nr
 - H3.2.1 Primary Domino Server IP address
 - H3.2.2 DOMINO Server Organizational and Naming Structure
- H3.3 Apache Server Version Number
 - H3.3.1 Primary Apache Server IP address
 - H3.3.2 Apache Server Naming Structure
- H3.4 IIS Server Version Number
 - H3.4.1 IIS Server IP address
 - H3.4.2 IIS Server Naming Structure
- H3.5 Other Web Server Version Number
- H3.6 Primary Web Browser Version Number

H4. DCP

- H4.1 SAMETIME Version Number
- H4.2 SAMETIME server IP address

UNCLASSIFIED

Annex B to Chapter 12 to ACP 200(A)

- H4.3 Primary SAMETIME client Version Number
- H4.4 Other DCP Applications

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

OPTASK NET (Example)

**(CLASSIFIED 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 EXERCISE EXAMPLE.

A2. Objective

Provide maritime units operating in EXERCISE EXAMPLE the capability to maintain access to the designated network(s).

B. ADMINISTRATION

B1. Period

Effective on receipt. Cancel upon completion of EXERCISE EXAMPLE 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 IM
- B4.4. OPTASK FOTC

C. DUTIES

C1. CTG Network Manager

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

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(A)

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 design):

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

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

D2.2. Canada

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

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

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.)

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)

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

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
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

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

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

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

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

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
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

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

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
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

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

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

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

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

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

E2. Bandwidth

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

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

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

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

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

E4.5. US NOC

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

F. SUBNETS

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

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

G. NETWORK MANAGEMENT

G1. Unit NM reporting requirements

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

G2. Help Desk Policy

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

UNCLASSIFIED
Appendix 1 to Annex B to Chapter 12 to ACP 200(A)

H5. MSEG

H5.1 Version Nr

H5.2 Multicast address

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 may be designed to utilize multicast network features in all areas possible. As part of this strategy the network and applications 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.

MULTICAST SERVICE GATEWAY (MSeG)

13A01 INTRODUCTION

- a. Multicast Service Gateway (MSeG) provides a multicast IP capability in an network comprising links of low bandwidth and high latency whilst not having to change the originating applications code. MSeG as 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 (MDP). MSeG has the ability to intercept the TCP traffic generated from a GCCS-M (or equivalent), SMTP E-mail and File Transfer (FTP), convert it to UDP and relay this on as a multicast to a number of Multicast address groups.
- b. 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.

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 another 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

UNCLASSIFIED

Annex B to Chapter 13 to ACP 200(A)

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.
- (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", Exchange and other SMTP-capable Mail Transfer Agents (MTAs). MSeG is installed and run in the same host of an E-mail system or a 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.

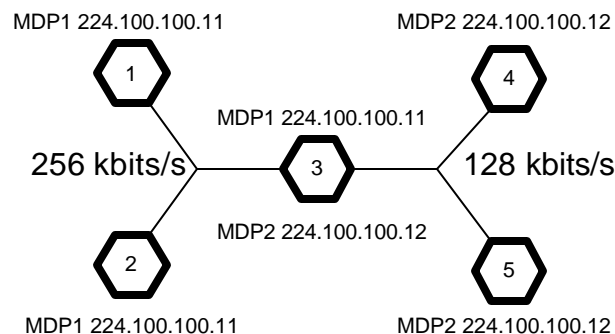
UNCLASSIFIED

Annex B to Chapter 13 to ACP 200(A)

- (7) To enable the use of MSeG, the MTA 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 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

- a. **Example 1:** This example demonstrates how 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.
- b. 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.
- c. MDP1 is configured to send at a maximum rate of 256 kbps. MDP2 is configured to send at a maximum rate of 128 kbps.
- d. The following observations are made:
 - (1) MSeG at node 3 relays data from MDP1 @ 256 kbps to MDP2 @ 128 kbps and vice versa.
 - (2) 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.
 - (3) MSeG 3 and 4 send and receive data @ 128 kbps or less.

**Figure 13–A–1 Example 1**

- e. **Example 2:** Three more nodes were added to network in example 1.
 - (1) MSeGs at nodes 1,3,4 and 5 are configured the same as in example 1.

UNCLASSIFIED

Annex B to Chapter 13 to ACP 200(A)

- (2) 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.
 - (3) MSeG at node 7 and 8 are configured to MDP4 for 224.100.100.14.
 - (4) 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.
- f. 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.
- g. The following observations are made:
- (1) MSeG at node 2 relays data from MDP1 @ 256 kbps and to MDP3 @ 32 kbps and vice versa.
 - (2) MSeG at node 6 relays data from MDP3 @ 32 kbps and to MDP4 @ 64 kbps and vice versa.
 - (3) 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.

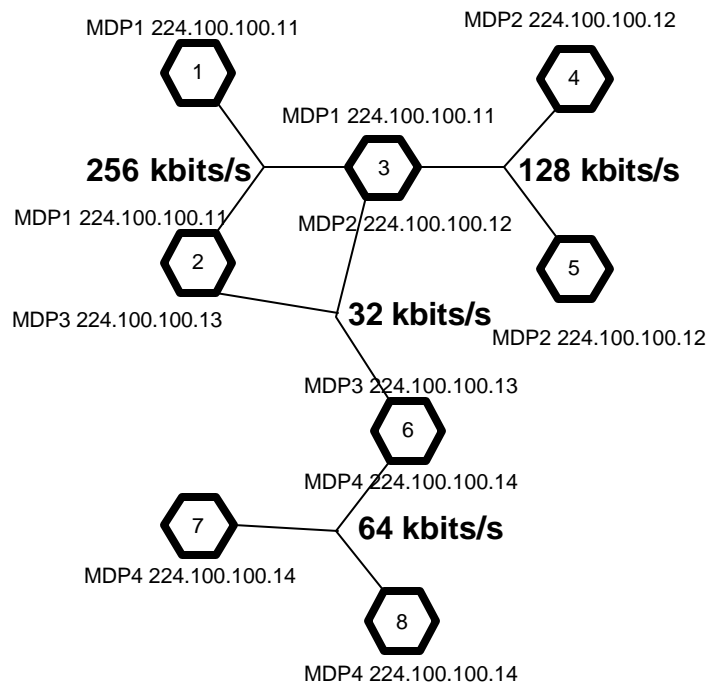


Figure 13–A–2 Example 2

- h. **Example 3:** This example demonstrates when MSeG can be used to service more than one GCCS-M terminals.
 - (1) 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.
 - (2) MSeG at node 1,2,3,4,5,6,7 and 8 are configured the same as in example 2.
 - (3) 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.
- i. The following observations are made:
 - (1) 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.
 - (2) 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.

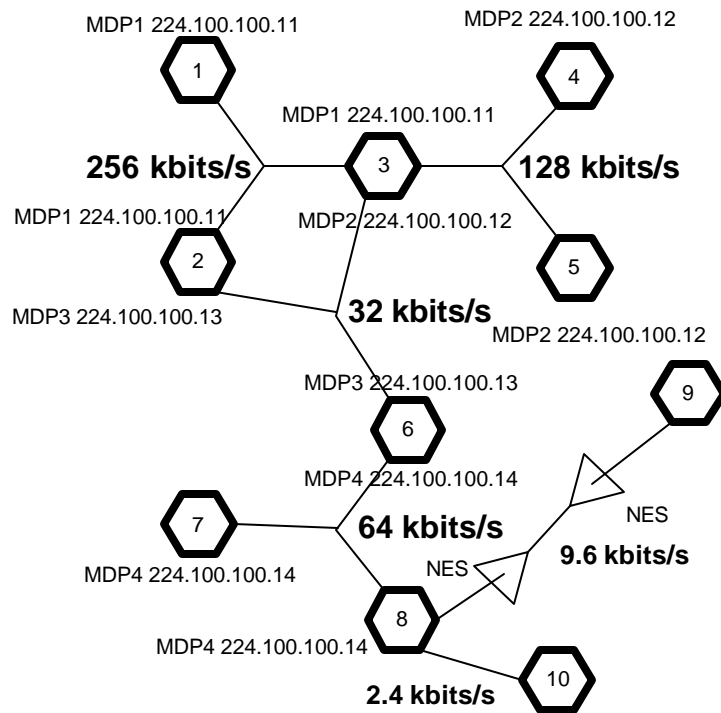


Figure 13–A–3 Example 3

- j. **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.
- (1) 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.
 - (2) MSeG 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.
- k. The following observations are made:
- (1) All MSeGs in both ASs receive the same multicast traffic.
 - (2) MSeG 6 relays TCP data from MSeG 3 of AS2 to MDP1 for MSeG 1 and 2.

- (3) MSeG 3 relays TCP data from MSeG 6 of AS1 to MDP2 for MSeG 4 and 5.

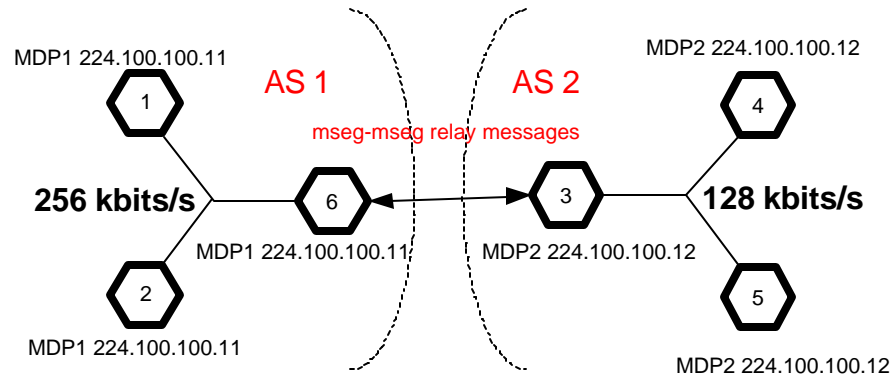
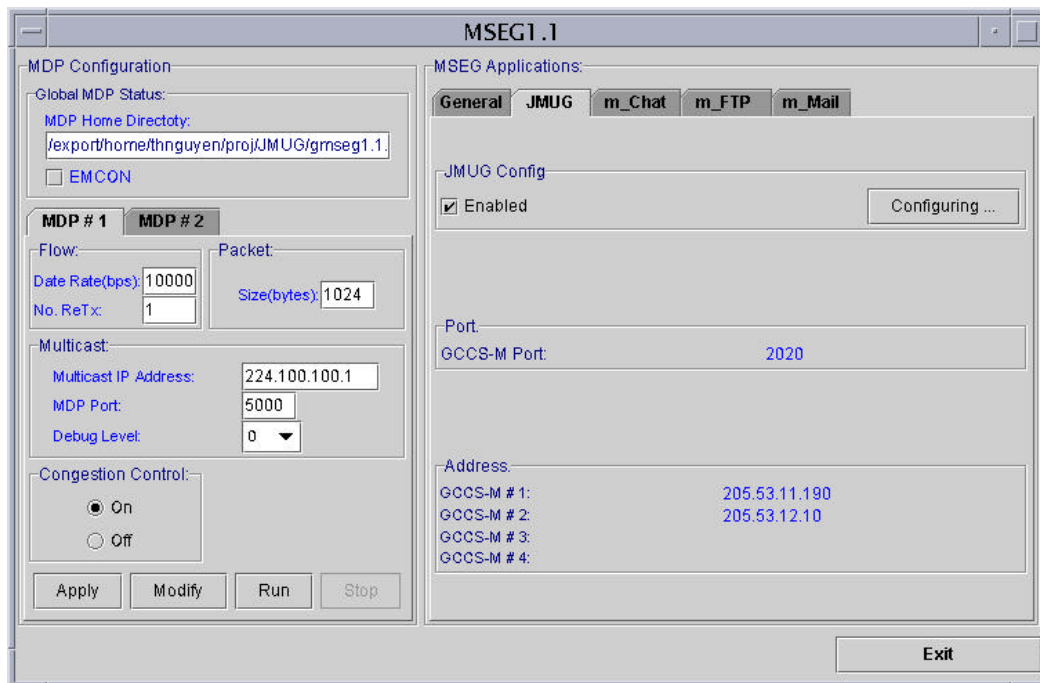


Figure 13–A–4 Example 4

13A06 GRAPHICAL USER INTERFACE (GUI)

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



UNCLASSIFIED

Annex B to Chapter 13 to ACP 200(A)

MSEG1.1

MDP Configuration

Global MDP Status:

MDP Home Directoty: /export/home/thnguyen/proj/JMUG/gmseg1.1

☐ EMCON

MDP #1 MDP #2

Flow:

Date Rate(bps): 10000

No. ReTx: 1

Packet:

Size(bytes): 1024

Multicast:

Multicast IP Address: 224.100.100.1

MDP Port: 5000

Debug Level: 0

Congestion Control:

☒ On

☐ Off

Apply Modify Run Stop

MSEG Applications:

General JMUG m_Chat m_FTP m_Mail

Outgoing:

Source Path/File:

Destination Name:

Send

Incoming:

Received Directory: /export/home/thnguyen/proj/JMUG/gmseg1.1.0/mftp

Restart ftp

Exit

MSEG1.1

MDP Configuration

Global MDP Status:

MDP Home Directoty: /export/home/thnguyen/proj/JMUG/gmseg1.1

☐ EMCON

MDP #1 MDP #2

Flow:

Date Rate(bps): 10000

No. ReTx: 1

Packet:

Size(bytes): 1024

Multicast:

Multicast IP Address: 224.100.100.1

MDP Port: 5000

Debug Level: 0

Congestion Control:

☒ On

☐ Off

Apply Modify Run Stop

MSEG Applications:

General JMUG m_Chat m_FTP m_Mail

Signature: thnguyen

Message:

Clear Text... Ringing..

Exit

UNCLASSIFIED

Annex B to Chapter 13 to ACP 200(A)

MSEG1.1

MDP Configuration

Global MDP Status:

MDP Home Directoty: /export/home/thnguyen/proj/JMUG/gmseg1.1

☐ EMCON

MDP # 1 MDP # 2

Flow: Date Rate(bps): 10000 No. ReTx: 1 Packet: Size(bytes): 1024

Multicast:

Multicast IP Address: 224.100.100.1

MDP Port: 5000

Debug Level: 0

Congestion Control:

☒ On ☐ Off

Apply Modify Run Stop

MSEG Applications:

General JMUG m_Chart m_FTP m_Mail

Destination: Receiving MTA:

Battan.navy.mil	Bataan.navy.mil
nrssd.navy.mil	nrssd.navy.mil
tiffany.spawar.navy.mil	tiffany.spawar.navy.mil
timothy.spawar.navy.mil	timothy.spawar.navy.mil
ironwood.spawar.navy.mil	ironwood.spawar.navy.mil

Dynamic IP Config... OK Add Delete

Exit

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

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

1403 OVERVIEW

- a. One of the major activities in establishing any mobile tactical network (especially allied and coalition networks) is to identify and promulgate the names and addresses of network elements, including attached end systems and workstations.
- b. 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.
- c. Any MTWAN DNS has to be linked to the DNS structure of other appropriate national and coalition networks in order to provide address information to-from these other networks.

1404 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. COP, Email, DCP) taken from the suggested list at Table 14–1.

Use Field Abbreviation	Description	Remarks
auth	PKI or similar Authentication Service	generally a server
cop	Common Operational Picture/Recognized Maritime Picture	generally a server. e.g. GCCS-M or similar COP service
ct	Cipher-text side of INE device	see INE in TYPE
cvat	Coalition Vulnerability Assessment Team service	could be a server or a workstation
dcp	Distributed Collaborative Planning	generally a server, e.g. Sametime
dir	Directory service	generally a server
dns	Domain Name Service	generally a server
dom	Domino Web Replication	generally a server
gbs	Global Broadcast System	generally a server
gen	general purpose device	typically a workstation e.g. MS Office
hi	High Side of a Data Diode device	see DIODE in Type
key	PKI or similar Key Server	generally a server
lo	Low Side of a Data Diode device	see DIODE in Type
mail	Email or messaging	generally a server
pt	Plain-text side of INE device	see INE in TYPE
time	LAN time service generator	generally a server
uhf	For use with UHF LOS and SATCOM networks	see Type
web	Traditional Web Service	generally a server
		Spare
		Spare

Table 14–1 Abbreviations for “Use” Field

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

Type	Abbreviation	Type Remarks
cap	Channel Access Processor (CAP)	equivalent to SNAC
card	VME Card for MCAP	
criu	CAP to Router Interface Unit (CRIU)	equivalent to SRIU
diode	Data Diode device	one-way IP data transfer
ine	In-line Network Encryptor	IP encryption device
hfip	HF IP (STANAG 5066 Ed. 2) gateway	IP over HF; typically a server
hf5066	STANAG 5066 Ed. 1 gateway	email only over HF; typically a server
mlgrd	Mail Guard	
pntr	Printer	
rout	Router	
snr	Subnet Relay Network Controller	
serv	Server	
snac	Subnet Access Controller (SNAC)	equivalent to CAP
sriu	SNAC to Router Interface Unit (SRIU)	equivalent to CRIU
swit	Network Switch	
wkst	Workstation PC, X-Terminal, etc.	
		Spare
		Spare

Table 14–2 Abbreviations for “Type” Field

- (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-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

UNCLASSIFIED

ACP 200(A)

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 (i.e. the “use” field of the host name may not start with a number).
- d. Tables 14- 1 and 14- 2 can be amended for specific events (e.g. operations, exercises, demonstrations, trials). However, such amendments will only apply to that event. Devices and conventions that become defacto “Use” and “Type” standards should be submitted for inclusion into ACP 200.
- e. The following are some examples of the Host Names that can be generated from the above guidance:
 - mail-serv
 - dom-serv
 - dcp-serv
 - cop-serv
 - gbs-rout
 - uhf-snr
 - uhf-cap
 - gen-wkst-a
 - gen-wkst-123

1405 DOMAIN NAMING CONVENTION

- a. Used to generate the names for domains within which the hosts will operate, the domain naming convention shall be composed of elements of the following:
 - (1) **Unit** — representing the name of the ship, unit, command or other site;
 - (2) **Theater Commands** – represents Theatre / AOR Commands, such as the United States Combatant Commanders (COCOMs);
 - (3) **Service** — selected from: navy, army, air, marines, joint;
 - (4) **Country** — the letter country code as defined in ISO 3166 (this may either be the di-graph code described in ISO 3166-2 or the tri-graph code in ISO 3166-3).
 - (5) **Enclave** – the security enclave of the network;
 - (6) **COI** – a community of interest (if any) within the enclave;

UNCLASSIFIED

ACP 200(A)

- (7) **Coalition Military Network Identifier** – CMIL; and
- (8) **Military Network Identifier** – MIL.

- b. The nation or other entity sponsoring a given Allied/Coalition network shall specify in the OPTASK NET which of the above naming elements are required for use in that network as well as define the naming. This provides standardization with flexibility of implementation.
- c. For CENTRIXS, this convention translates to "**{ship|unit|command}. {3-letter-ISO3166 country-code|ccom}. {enclave|enclave-coi} .cmil.mil**".
- d. Examples of CENTRIXS naming include:
 - (1) CFE Enclave
US Pacific Command pacom.cfe.cmil.mil
MHQ Australia mhqaust.aus.cfe.cmil.mil

 - (2) CNFC COI in GCTF Enclave
HMNZS Te Kaha tekaha.nzl.gctf-cnfc.cmil.mil

 - (3) GCTF Enclave
COMPACFLT cpf.pacom.gctf.cmil.mil
- e. The "country code" for NATO is "INT". NATO enclaves include NIDTS, NSWAN, CRONOS, BISCES and LOCE.
- f. For temporary, single-enclave activities, such as used by the MNTG during JWID/CWID, the above convention can allow a simpler DNS structure, such as "**{ship|unit|command}.service.country**".
- g. Examples of the MNTG JWID/CWID naming include:

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

- h. 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.

- i. Although there are no DNS imposed restrictions on the length of the “Unit” component, for reasons of usability the length for MTWAN purposes should be constrained to 15 characters. Further the DNS entity must be unique within the service and country, e.g. there could be an ottawa.navy.ca, ottawa.navy.us and ottawa.air.ca, but not a second ottawa.navy.ca.
- j. As with host names, the domain name cannot begin with a number. In other words, the ‘unit’ field may not start with a number. Therefore units like 3 CDO BDE will require a lettered prefix. DNS examples for “Numbered Units” include:

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

- k. Fully Qualified Domain Names (FQDN) are composed of the Host names, whose convention is defined in ACP 200, Section 1404 and the DNS name. Complete, FQDN examples include:

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

- l. These examples are illustrative only.

1406 IP SUBNETTING AND MULTICAST ADDRESSING

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

1407 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.
- d. 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.

1408 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.

1409 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.

1410 CONCLUSION

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

UNCLASSIFIED

Annex A to Chapter 14 to ACP 200(A)

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 14-1 and represented in Figure 14-A-1.

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

Table 14-A-1: IP Address Classes

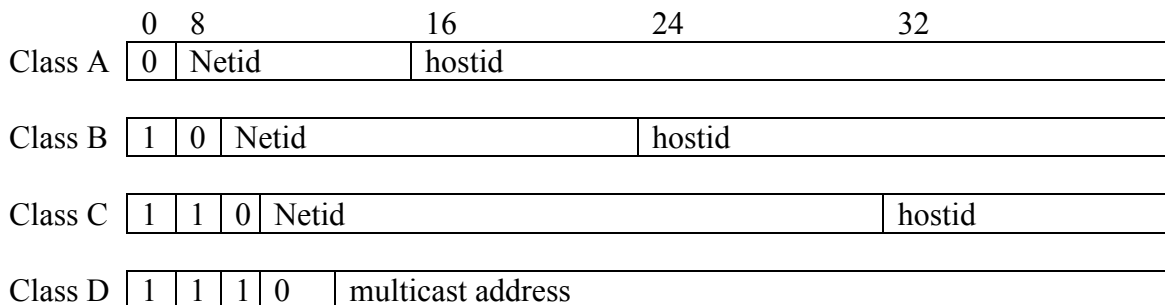


Figure 14-A-1: IP Address

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 ANDed with the address, divides the address into two parts. One part is a *network* address that uniquely identifies the network, and the other is a host address that uniquely identifies the *host* within a given network. In other words, besides

UNCLASSIFIED

Annex A to Chapter 14 to ACP 200(A)

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.

UNCLASSIFIED

Annex B to Chapter 14 to ACP 200(A)

DOMAIN NAME SERVICE SOP

14B01 INTRODUCTION

- a. The primary services of DNS are:
 - (1) name-to-IP-address mapping,
 - (2) IP-address-to-name mapping, and
 - (3) 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. Each network host or more specifically each network interface has two identifiers: an IP address (which is a 32-bit number) and a Host Name (which is a string). DNS provides forward and reverse mapping between maps the host name(s) and IP address(es).
- b. As applications refer to hosts by names, while packets carry source and destination IP addresses correct configuration and maintenance of DNS is critical to the effective operation of any IP network.

14B04 DOMAIN NAMESPACE

- a. The naming system on which DNS is based is a hierarchical and logical tree structure called the *domain namespace*. An example using a simple naming schema of *unit.service.country* is employed in Figure 14-B-1. This naming schema complies with the naming convention describe in paragraph 1405. A di-graph (i.e. two letter) country code is employed.

UNCLASSIFIED

Annex B to Chapter 14 to ACP 200(A)

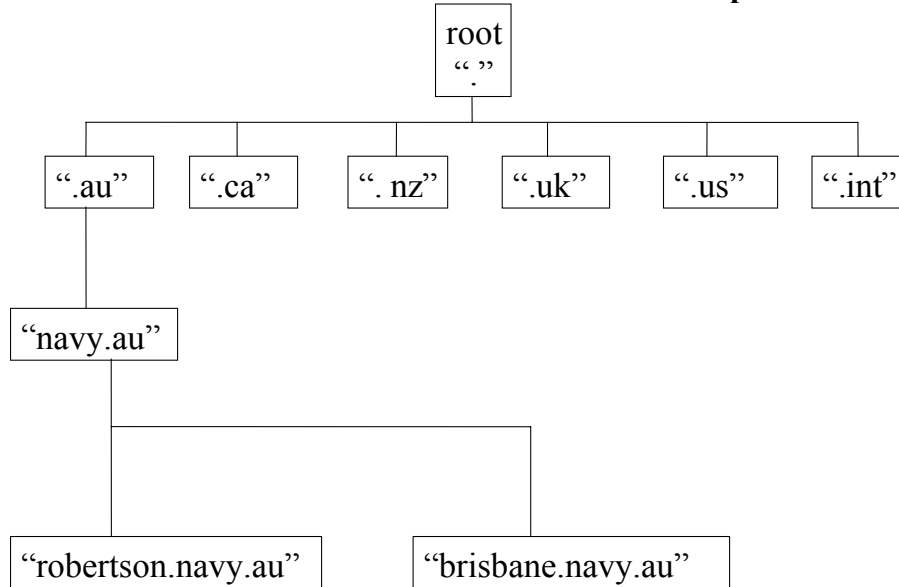


Figure 14–B–1 Domain Name Schema

- 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.

14B05 DNS SERVERS

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

UNCLASSIFIED

Annex B to Chapter 14 to ACP 200(A)

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.

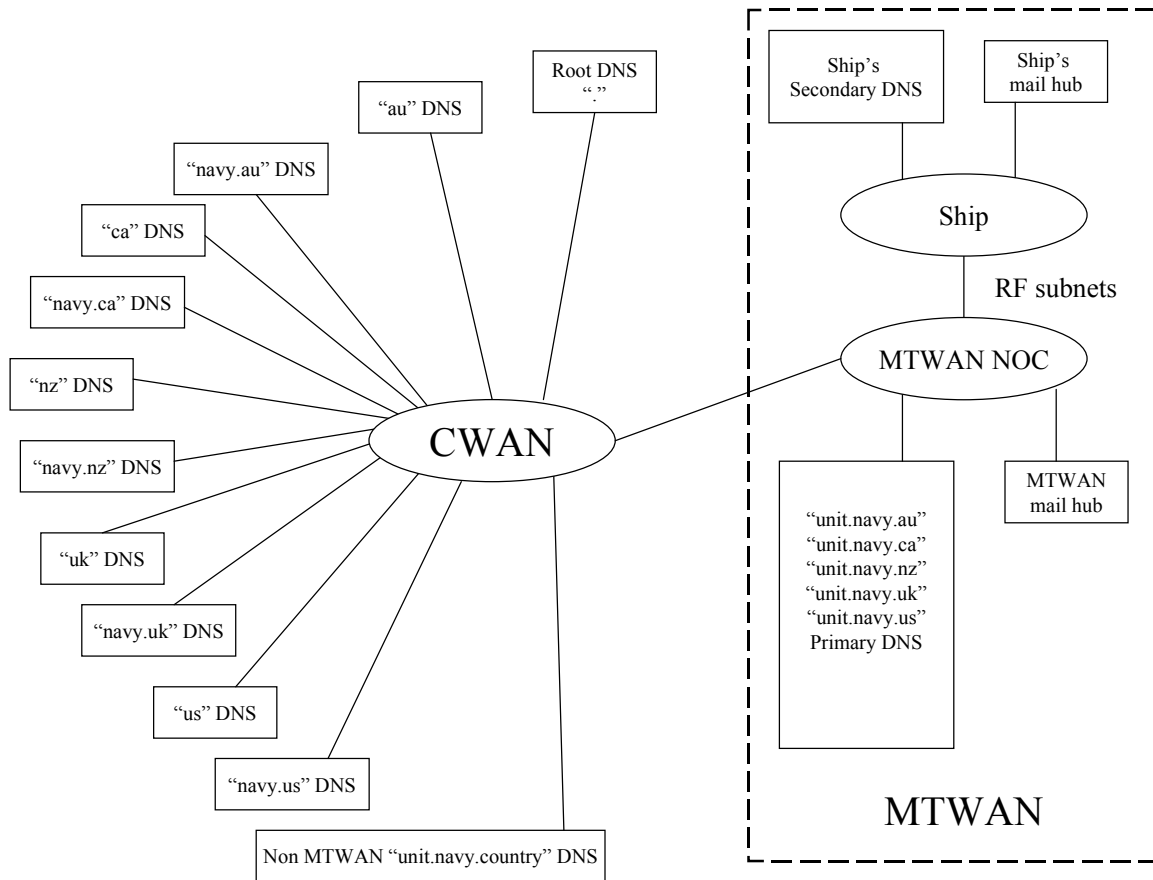


Figure 14-B-2 DNS Servers

- 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"

UNCLASSIFIED

Annex B to Chapter 14 to ACP 200(A)

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 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.

14B06 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

UNCLASSIFIED

Annex B to Chapter 14 to ACP 200(A)

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.

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 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.

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

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

1502 AIM

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

1503 OVERVIEW

- a. Routers implement and control information flow. They are internetworking devices that perform two basic functions—they select a route between networks, and they transmit information in the form of IP data packets across that route toward an intended destination. In so doing, they draw on routing protocols and algorithms. The routing protocols, such as OSPF and BGP4 are designed to discover and plot routes using such criteria as throughput, delay and priority so that the most efficient route can be selected for each transmission. This process is similar to maps created by auto clubs that show drivers where roadwork is under way so that they can avoid potential areas of congestion. When a packet is received at a router, the router opens it, looks at the network destination address, and then calculates the next hop in the best route to the destination.
- b. In an MTWAN, routing is accomplished using the following standard IP protocols:
 - (1) Open Shortest Path First (OSPF) for interior AS routing;
 - (2) Border Gateway Protocol Version 4 (BGP4) for exterior AS routing; and

- (3) Protocol Independent Multicast (PIM) for multicasting.
- c. The running of the three protocols over a WAN is depicted in Figure 15–1. Annex A contains further information on these protocols, while paragraphs 1505 and 1506 discuss the implementation of these protocols within an MTWAN.

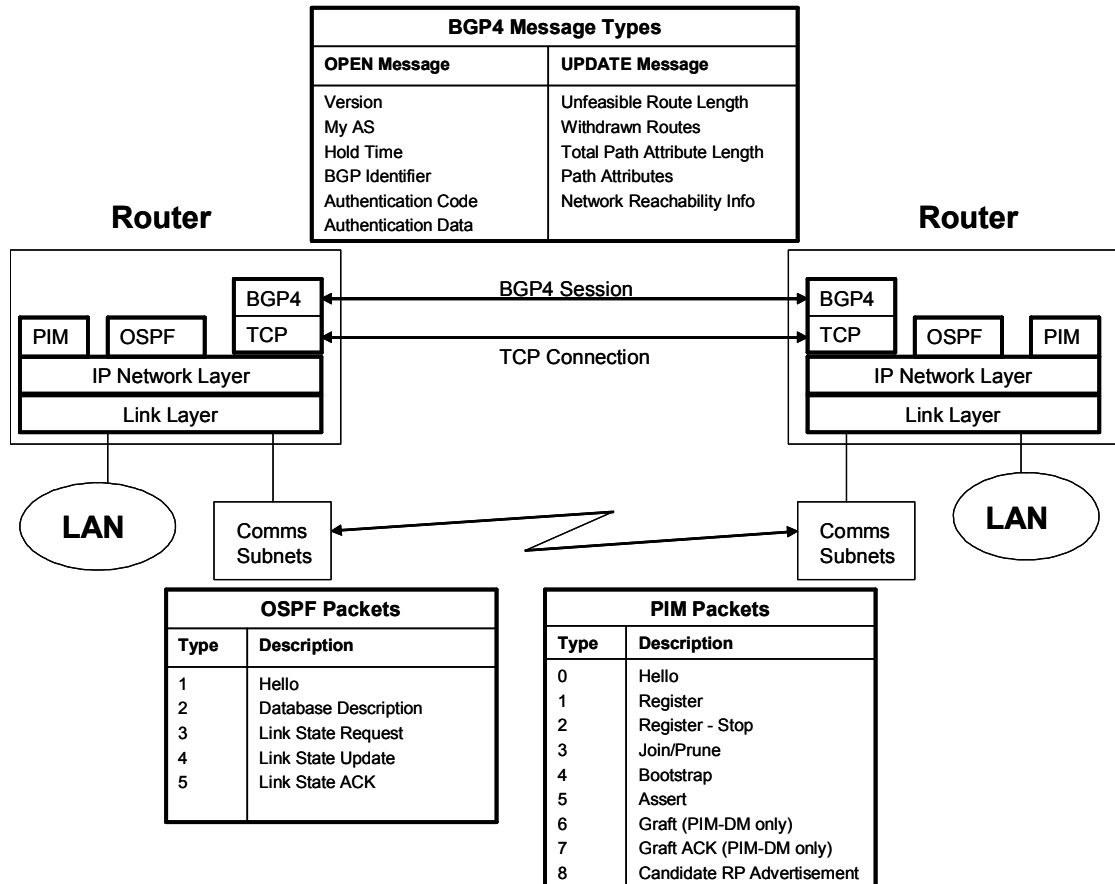


Figure 15–1 Routing Protocol Stacks

- d. Networks, or more precisely, the routers that are under the same administrative authority and use a common interior routing protocol are usually grouped into the same Autonomous System (AS). Interior routing policies and protocols must be established within each AS, enabling it to route packets internally. Exterior routing, using an exterior routing protocol such as BGP4, is used to interconnect the various AS's, with their independent interior routing protocols, into a larger network.

1504 ROUTING ARCHITECTURES

- a. In terms of topologies, MTWAN's either employ a single-AS TGAN topology or a multiple-AS TGAN topology. The latter is generally employed to allow nations within an MTWAN to administer their own mobile units.
- b. **Single-AS TGAN.** In a single-AS TGAN, all mobile and fixed nodes of the TGAN belong to a single AS, as illustrated in Figure 15–2. OSPF is used to select routes for all IP traffic flows among TGAN nodes.
- c. The TGAN is divided into OSPF areas where all communication subnets are included in the backbone area, known as Area 0. The local network at each node is contained in a separate OSPF area whose number is the network address of the node. In the example shown in Figure 15–2, nations in the TGAN are allocated two Class C addresses: A.B.C.0 and D.E.F.0. The two Class C networks are divided into 16 subnets with up to 30 individual IP addresses each. Mobile #1 is assigned the network address A.B.C.32 which is also the mobile's OSPF Area Number.

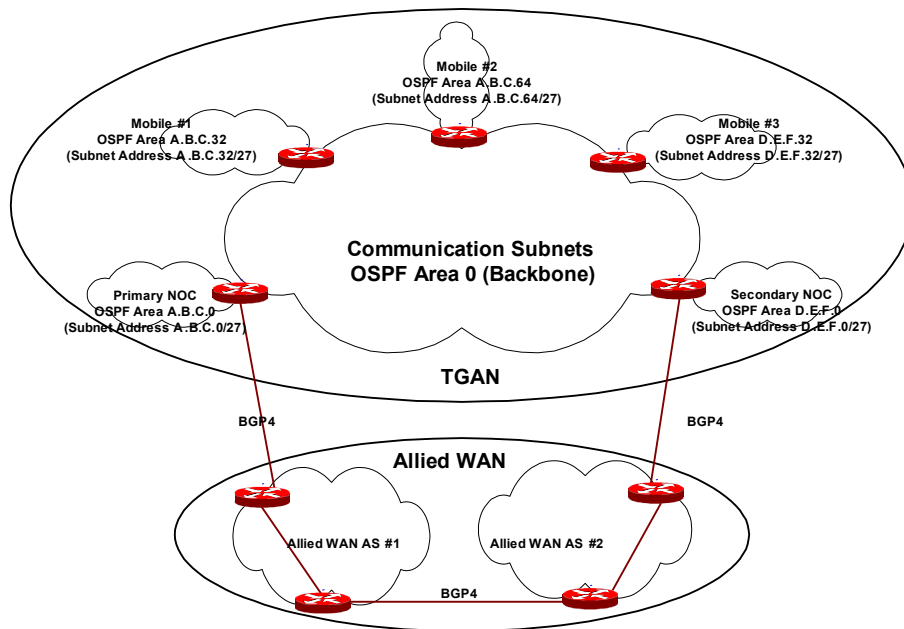


Figure 15–2 Interior and Exterior TGAN Routing

- d. **Multiple-AS TGAN.** Each nation can form a separate AS within a TGAN. The TGAN is then considered as a virtual Autonomous System (AS) comprising of a number of actual ASs. Each AS will have an independent entry into the allied WAN. OSPF will run internally within the TGAN, controlling path selection for all (ship and shore) traffic flows within the TGAN. If connectivity between different ASs does not exist, to extend OSPF routing domain over the whole TGAN, Generic Routing Encapsulation (GRE) tunnels through the allied WAN can be used to provide a mechanism for supporting multicast and the OSPF adjacencies by encapsulating the internal OSPF and multicast routing from the allied WAN.
- e. Figure 15–3 depicts a scenario where each nation forms its own AS within the TGAN. Each AS has an independent entry into an allied WAN. Within each national AS, the national backbone is used to provide connectivity between TGAN routers using In-line Network Encryptors (INE) and GRE tunnels.
- f. Allied routers in the national NOC are connected to the allied WAN comprising a number of ASs via BGP, and TGAN entries into the allied WAN are in different AS. This architecture can support direct RF connectivity between TGAN ASs as part of the OSPF routing domain. Generic Routing Encapsulation (GRE) tunnels through the allied WAN are used to support multicast and OSPF adjacencies within the TGAN.
- g. Direct connectivity between mobile units of different nations or between a NOC of a nation and a mobile unit of another nation can be supported within the OSPF routing domain of the virtual AS of the TGAN. In Figure 15–3 an allied LOS subnet is used to support direct ship-ship networking. A satellite link connecting Mobile #21 to NOC #1 can also be provided as a redundant backup route for Mobile #21 when the backbone of Nation #2 is not operational.
- h. The introduction of LOS connectivity can significantly reduce traffic on national SATCOM links by enabling traffic between mobile units to travel via a direct mobile-to-mobile route in lieu of a mobile-to-NOC-to-mobile route involving two SATCOM hops. This conserves SATCOM bandwidth for traffic between mobile units and NOCs. However, the introduction of OSPF-based LOS connectivity can adversely affect route selection behavior unless appropriate measures are taken on allied NOC routers. The routing configuration must be exercised with care to prevent inappropriate route selection for traffic within the TGAN and also for traffic between the TGAN and the allied WAN.

- [illegible]

k. **Private Routing.** Figure 15–4 provides an overview of a Private Routing architecture where a secure IP backbone is set up to support Virtual Private Networks of various security levels.

1. Connectivity between an allied node and an access router of the backbone is via an INE. As neighbor relationships between routers of two separate and different networks do not exist, connectivity between allied nodes is done via GRE tunnels or a routing protocol that can work through the INE. The use of a routing protocol will require allied networks to be routable over the backbone. However, this option will support a dynamic TGAN and enable mobiles to join or leave the TGAN without re-configuring any allied routers. In Figure 15-4, OSPF point-to-multipoint is used to establish OSPF adjacencies and exchange routing information between mobiles and the NOC.

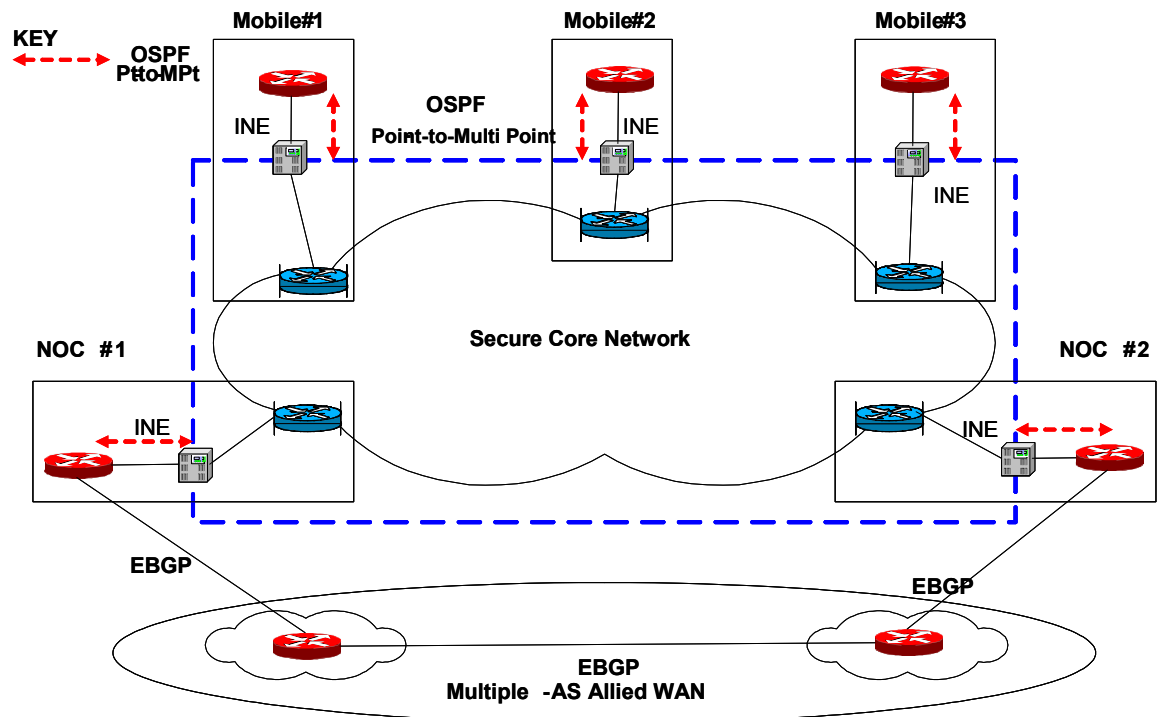


Figure 15-4 Private Routing

1505 INTERIOR TGAN ROUTING

- a. Route selection will meet the following requirements:
 - (1) Direct LOS connectivity, where available, will be used for mobile-to-mobile traffic to better utilize available bandwidth.
 - (2) Whenever possible, fixed terrestrial subnets will be selected for traffic between non-mobile units.

- (3) Whenever possible, the fixed terrestrial connectivity to the RF subnet of the specific mobile unit that hosts the traffic endpoint will be used for fixed-to-mobile traffic.
 - (4) Unless a mobile is acting as a relay for another mobile, its RF subnet will not be used as a transit subnet for the other mobile.
 - (5) Route selection is to be symmetrical; traffic between two nodes should flow over the same route in both directions.
- b. Within a TGAN, route selection is governed entirely by OSPF costs. The small adjustments to the recommended OSPF metric values given in Annex B may be required so that the requirements of route selection specified above can be met.
- c. OSPF uses two types of external metrics – Type 1 and Type 2 – to determine the best exit point to external networks. Type 1 external metrics are expressed in the same units as the OSPF internal metric values and can be directly summed with the internal metrics to form the lowest cost route to reach the external destination. Type 2 external metrics are an order of magnitude larger and are considered greater than any route internal to the AS. Type 2 metrics assume that routing between ASs is the major cost and eliminate the need for conversion of external costs to internal costs. The route selection from the interior nodes is based on the lowest cost Type 2 external metrics, and it does not require any internal lowest cost path calculations.
- d. Type 1 external metrics are preferred as mobile units learn of several exit points, but will choose the best exit point based on OSPF costs. When the link supporting the best exit point fails, the mobile units will dynamically adjust their routes and select the next best exit point.
- e. Multicasting within a TGAN is supported by PIM. All COTS routers can support SM, DM and a combination of SM and DM known as Spare-Dense Mode (S-DM). When a router is configured for S-DM and an RP is not known for a group, the router will send data using DM. However, if the router discovers an RP either dynamically or statically, SM will take over. As S-DM allows the use of both SM and DM for different groups for different applications, TGAN routers will be configured for S-DM when multicast is required. Whenever PIM-SM is selected, a static RP at a NOC will be configured.

1506 EXTERIOR TGAN ROUTING

- a. **Single Allied WAN Access Point.** BGP4 is used to control which internal networks are advertised to, and which network advertisements are accepted from, other autonomous systems. This control is at least as fine-grained as the ability to send or receive individual network advertisements. This means the TGAN network administrator has the ability to control whether to advertise or hide each individual internal network. Likewise, the administrator also has the capability to accept or reject each external network advertisement.
- b. The ability of BGP4 to implement routing policy is both a strength and a severe constraint. While the ability to develop routing policy gives significant power to the administrator, it also makes the configuring of BGP4 labor intensive and error-prone.
- c. The primary use of BGP4 policy is to limit the amount of routing protocol traffic seen inside the TGAN as a result of external links. An allied WAN, as a global network, has the potential to generate large amounts of routing protocol traffic. If this routing protocol traffic were allowed into the TGAN, it might consume a significant amount of bandwidth. To prevent this, BGP4 policy is used to block the allied WAN routing protocol traffic into the TGAN.
- d. A global backbone network, such as the allied WAN, cannot use default routes and must have specific route advertisements for every network that is reachable across the backbone. Hence, all nodes in the TGAN must be advertised to the allied WAN.
- e. **Multiple Allied WAN Access Points.** When the TGAN has multiple connections to the allied WAN, one of the connections will be configured to be the primary (preferred) route for all traffic between the TGAN and allied WAN. In some cases, there may be a requirement to configure a connection to be the primary route for some nodes and the secondary (backup) route for some other nodes.
- f. In order to manipulate the route selection of BGP, either of the following two BGP attributes will be used: AS-Path and Multi-Exit-Discriminator (MED).
 - (1) **AS-Path.** BGP permits BGP-enabled routers to exchange routing information with full AS-Path information. The AS-Path is a list of

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

- (2) A router can make the AS-Path of a route longer than the AS-Path of another route by pre-pending its own ASNs to the route's AS-Path attribute.
- (3) The TGAN border router at the secondary site needs to be configured to pre-pend its own ASN to the AS-Path before communicating routes via BGP to the allied WAN border router. The TGAN border router at the primary site does not alter the AS-Path it presents to the allied WAN.
- (4) For example, let 1002 be the number of the TGAN AS. The AS-Path in routes advertised by the TGAN border router at the secondary site then consist of the TGAN ASN pre-pended to the route's AS-Path attribute, that is "1002 1002", while the AS-Path advertised by the TGAN border router at the primary site simply consists of "1002". Since the AS-Path advertised at the primary site is shorter than the AS-Path advertised at the secondary site, traffic destined for the TGAN network from the allied WAN would be routed via the primary site. When the connection between the TGAN network and the allied WAN at the primary site is not available, traffic will be re-routed via the secondary site.
- (5) To ensure a symmetrical path between the TGAN and the allied WAN, allied WAN routers need to be configured in a similar fashion. The allied WAN border router at the secondary site needs to be configured to pre-pend the allied WAN ASN to the AS-Path before communicating routes via BGP to the TGAN.
- (6) The primary and secondary border routers communicate via an IBGP session to ensure a consistent view of external routing within a TGAN AS. Using IBGP, the secondary border router will be aware of the preferred route to the allied WAN via the primary border router because allied WAN routes advertised at the primary site possess a shorter AS-Path than the same routes advertised at the secondary site.

- (7) **Multi-Exit-Discriminator (MED).** MED is an alternative technique that can be used to influence route selection for traffic flowing from the allied WAN into the TGAN. The MED feature will enable inbound route selection to be governed entirely by the OSPF costs internal to the TGAN. The MED effectively extends internal cost information in order to automatically control inbound route selection from the allied WAN. The BGP MED attribute is a hint to external ASs about the preferred path into an AS.
 - (8) MED provides a dynamic way to influence routers in another external AS to choose the best route into a given AS from among multiple entry points into that AS.
 - (9) As MED attribute only transits between a single pair of ASs. That is, the receiving AS will not pass the original MED value to another AS. When the allied WAN consists of multiple ASs and the allied WAN access points are in different ASs, the BGP configuration will have to ensure that the allied WAN will make cohesive and coordinated routing decisions with respect to the preferred route to the TGAN. This objective can be achieved by a fully meshed BGP between the AS border routers of the TGAN and those of the allied WAN.
- g. **Failure recovery.** If an exit point fails, all traffic should use the remaining exit points.
 - h. For outgoing traffic, failure recovery can be ensured by carefully setting up the default routes on the AS boundary routers. When a boundary router has a connection to the allied WAN, we want it to generate a default route and distribute it throughout the TGAN. When a boundary router loses its connection to the allied WAN, we want it to automatically stop generating the default route. When the failed exit stops generating the default route, allied WAN traffic will automatically be directed to the remaining exit points by the remaining default routes.

1508 REDUCING ROUTING PROTOCOL TRAFFIC TO THE ALLIED WAN

- a. The allied WAN must be default-free, and therefore requires specific network routing information for every network in the allied WAN, as well as routing information for every node in the TGAN. For large networks, this can lead to an unacceptably large number of network advertisements. To reduce the amount of traffic generated by routing protocols, a technique known as “Classless Inter-Domain Routing” (CIDR) can be used to aggregate network advertisements.
- b. A simple example of CIDR would be the combination of two Class C IP network addresses into a single advertisement. If a TGAN had two sequential IP network addresses, such as 192.200.200.0 and 192.200.201.0, then it would advertise two separate networks to the allied WAN. Each of these networks would contain 256 addresses. Using CIDR, the TGAN would advertise a single network, starting at 192.200.200.0, that contained 512 addresses. The same host addresses are advertised in both formats, but CIDR produces 50% fewer routing advertisements.
- c. Typically, the network design would specify that numerous coalition units would receive a fraction of a Class C IP network address. For example, a NOC would have a fraction of the A.B.C.0 network (A.B.C.16-A.B.C.31) and a mobile unit would have another fraction of the same network (A.B.C.48-A.B.C.63). All these subnet addresses would be summarized in a single A.B.C.0 network before they were advertised to the allied WAN. This reduces the number of TGAN network advertisements that the allied WAN needs to carry on its backbone network. However, CIDR should not be implemented if the larger network contains one or more sub-networks external to the TGAN, as those networks will not be reachable.
- 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 bandwidth.

1509 CONCLUSION

An MTWAN comprises one or multiple AS's, where each AS shares a common routing strategy. Internal routing is accomplished by OSPF, or in the case of multicast PIM (SM or DM), while external routing is carried out with BGP4. The routing architecture can be complicated by multiple WAN access points. These routing approaches have been validated at sea in low bandwidth, high latency

UNCLASSIFIED

ACP 200 (A)

tactical environments. It is capable of exploiting transient communication links when they are up and avoid them when they are down.

UNCLASSIFIED

ROUTING PROTOCOLS

15A01 ROUTING PROTOCOLS (UNICAST)

- a. **Open Shortest Path First (OSPF).** OSPF is a dynamic routing protocol that quickly finds the best route based on the lowest cost to reach the destination. OSPF assigns a metric value to each link, which is used to determine the lowest cost path from source to destination. The recommended metric values can be found in Annex A to this chapter. OSPF runs directly on top of the IP network layer. IP packets containing OSPF data will have their IP protocol number set to 89.
- b. The OSPF routers exchange 5 types of Link State Advertisements (LSA's) with each other to build up the routing tables. For unicast, the IP header includes both the source and destination Class A, B, or C IP address. Each address is unique to the host computer.
- c. **Border Gateway Protocol Version 4 (BGP4).** BGP4 is a policy-based routing protocol that selects the AS to which it will talk to based on a policy entered manually by the AS manager. It operates on top of TCP and requires very stable subnets, which are more applicable to fixed infrastructure connections.
- d. BGP4 operates on top of TCP and requires two routers to set up a connection and establish a session to exchange routing information. BGP4 selects the path based on a policy that is converted into attributes. Each AS is assigned a unique AS Number (ASN) that is contained within the BGP4 protocol header. Policies then can be used to determine which AS to route traffic through or which to avoid. BGP4 does not provide the dynamic response of OSPF.
- e. An AS can have more than one exit point to other AS's. When only one exit point is used, the single BGP4 border router of the AS becomes the default router for all traffic leaving the AS. However, when two or more exit points exist, routing information must be provided to OSPF to decide which BGP4 border router to select to reach the external destination. In addition, the multiple BGP4 border routers of the AS need to exchange routing information to keep their databases synchronized. This may be accomplished using the internal BGP4 protocol.

UNCLASSIFIED

Annex A to Chapter 15 to ACP 200(A)

- f. BGP supports two types of sessions: External BGP (EBGP) and Internal BGP (IBGP). As illustrated in Figure 15-A-1, EBGP is used between BGP-enabled routers in two adjacent autonomous systems, while IBGP is used between BGP-enabled routers in the same AS. IBGP is sometimes necessary to achieve a consistent view of external routing within an AS. Typically IBGP is configured in a fully meshed configuration such that each BGP-enabled router maintains a distinct IBGP session with all other BGP-enabled routers within the AS.
- g. External routes learned via EBGP need to be communicated to all routers within the TGAN to permit optimal routing to external destinations.
- h. Depending on the network architecture, it is sometimes necessary to configure IBGP within routers of one AS that does not host external connections. This has the advantage of controlling the router table update so as not to flood the internal network. This is particularly advantageous in narrowband networks such as the TGAN. Intra-AS routing protocols such as OSPF have the ability to distribute external routes throughout an AS, but this requires that the external routes be flooded throughout the OSPF routing domain. Usually, this is not good practice as external routes are not needed or wanted on low-end access routers that are typically connected with lower-bandwidth connections as exhibited in the TGAN. Instead, IBGP should be used. In the TGAN illustrated in Figure 15-A-1 IBGP sessions are configured between AS border routers and Routers A and B. The external routing information communicated to Routers A and B via IBGP permits optimal routing to external destinations without flooding the external routes throughout the TGAN.

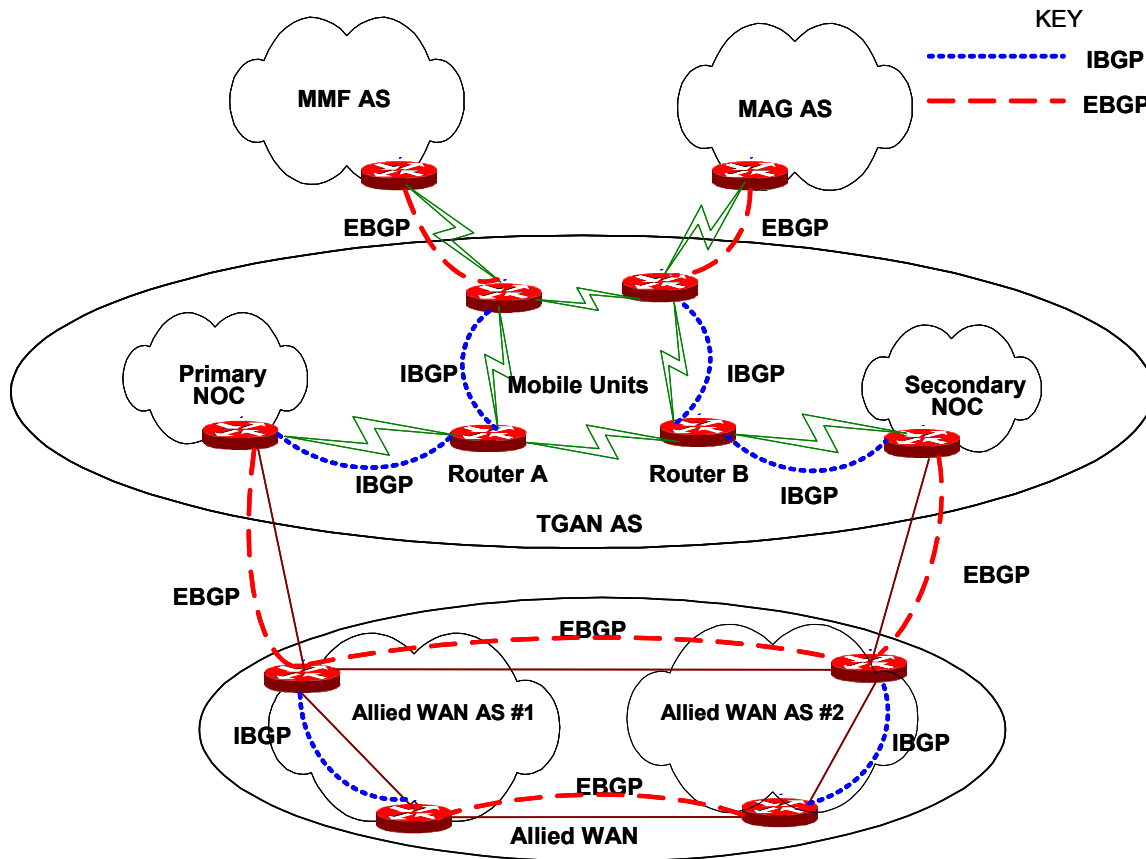


Figure 15-A-1 Sample BGP Configuration

15A02 ROUTING PROTOCOLS (MULTICAST—PIM)

- a. The protocol stack for Protocol Independent Multicast (PIM) is shown in Figure 15-1. PIM is directly on top of the IP network layer. IP packets containing PIM data will have their IP protocol number set to 103.
- b. PIM runs over an existing unicast protocol (including static routes), and uses the information provided by the unicast protocol and the static routes to build the distribution tree which the routers will use to forward multicast packets to all the members of the multicast group.
- c. Host computers use Internet Group Management Protocol (IGMP) to announce to their local multicast routers that they wish to join a multicast group (a group D IP address). The IP header for multicast now includes a source Class A, B, or C unicast address and a destination Class D multicast group address.

UNCLASSIFIED

Annex A to Chapter 15 to ACP 200(A)

- d. There are two modes of operation with PIM: PIM-SM (Sparse Mode) and PIM-DM (Dense Mode).
- e. **Sparse Mode.** PIM-SM is designed for situations where group members are sparsely distributed across all WANs, that is, the number of nodes with group members present is significant smaller than the total number of nodes. PIM-SM assumes that no node wants multicast data unless it is explicitly requested.
- f. PIM-SM uses some selected router as a Rendezvous Point (RP), which is the root of the distribution tree where multicast senders send their IP packets by unicast. The RP then forwards the packets to all the routers that have registered with the RP.
- g. 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.
- h. In a large network with few multicast receivers, PIM-SM reduces the amount of multicast traffic flooded throughout the network.
- i. In a mobile environment, NOCs will be a logical choice for an RP.
- j. **Dense Mode.** PIM-DM is designed for situations where group members are densely distributed. That is, most nodes are members of the multicast group. Multicast data is initially sent to all nodes in the network. Routers that do not have any member of the group attached to them will send a control message to remove themselves from the distribution tree.
- k. PIM-DM is simpler to implement than PIM-SM as PIM-DM does not use RPs. In small networks, PIM-DM is an efficient protocol when most nodes are members of the group.

UNCLASSIFIED

Annex B to Chapter 15 to ACP 200(A)

OSPF METRICS

15B01 OSPF METRIC VALUES

- a. The routing protocol OSPF is used to control path selection for all IP traffic flows within the MTWAN. Path selection is governed by OSPF link costs. Each link will be assigned a Metric Value (MV) that will be the cost used by OSPF to determine the optimum path from source to destination, which is a path with the lowest cost.
- b. The algorithm used for selecting the metric value is $MV_n = C \times MV_{n-1}$ for each halving of the bandwidth. The recommendation is $C = 1.2$. The metric values shown in Table 15–B–1 are based on $C=1.2$ rounded off to make the selection simple. The metric values are multiplied by 10 in order to increase the space between bandwidth increments for management purposes.

Metric Value	Bandwidth (Hz)	Link
100	512,000,000	
120	256,000,000	
140	128,000,000	Pier
170	64,000,000	
200	32,000,000	
250	16,000,000	
300	8,000,000	
360	4,000,000	
400	2,000,000	
500	1,000,000	
600	512,000	
700	256,000	
750	128,000	Dual ISDN
800	128,000	SHF
1,000	64,000	INMARSAT B/ISDN
1,300	32,000	
1,500	16,000	
1,900	9,600	HF
2,220	6,000	32 kbps UHF/5 Member
2,660	4,800	16 kbps UHF/3 Member
3,200	2,400	HF
3,830	1,200	
4,600	512	
5,520	256	

Note: 'X' in Figures 15-B-1 and 15-B-2 signifies information that is classified.

Table 15–B–1 Recommended Metric Values

- c. To illustrate the OSPF metric values, a hypothetical topology is represented in the next two figures. Figure 15–B–1 details the link bandwidth while Figure 15—2 shows the metric values for those links. To calculate the OSPF link costs between any source and destination pair in the example, sum the metric values shown. The router will select the path with the lowest cost.

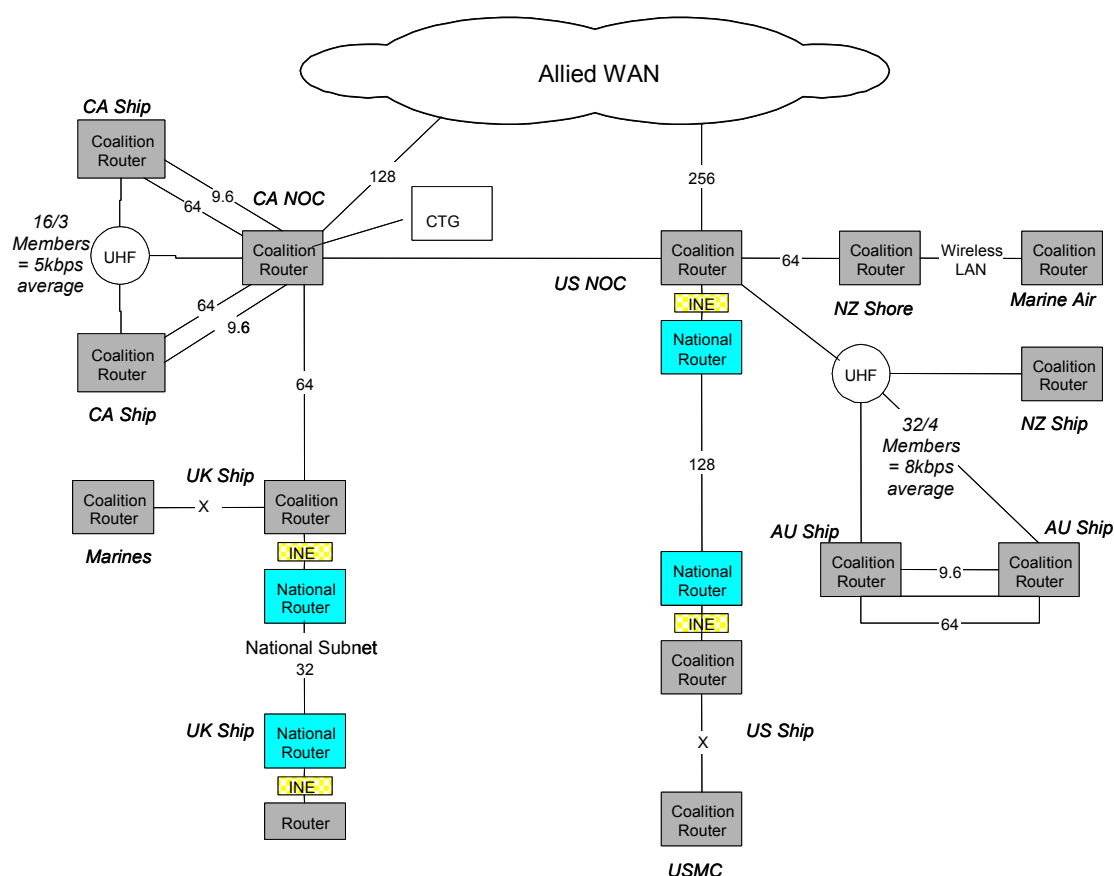


Figure 15-B-1 Example Coalition and National Subnets Bandwidth (Notional)

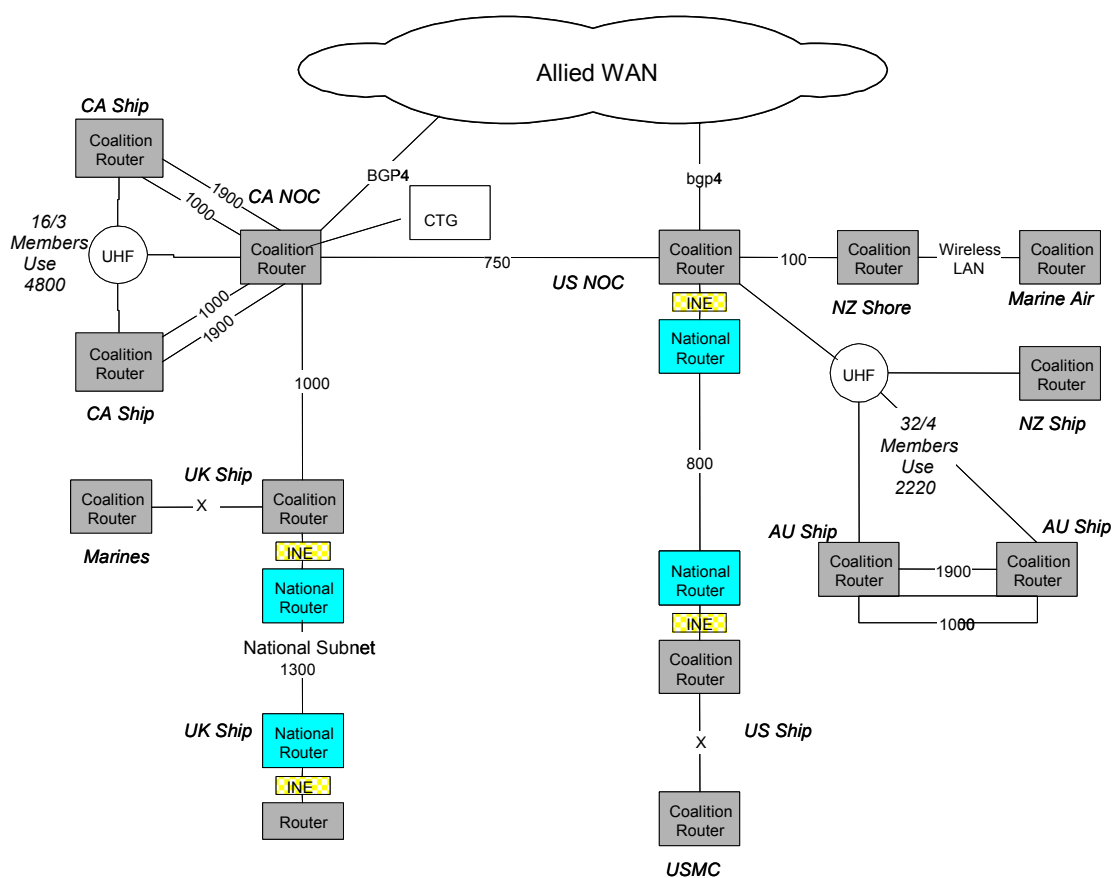


Figure 15–B–2 Link Metric Values (Notional)

Chapter 16**COMMUNICATION SUBNETS****1601 INTRODUCTION**

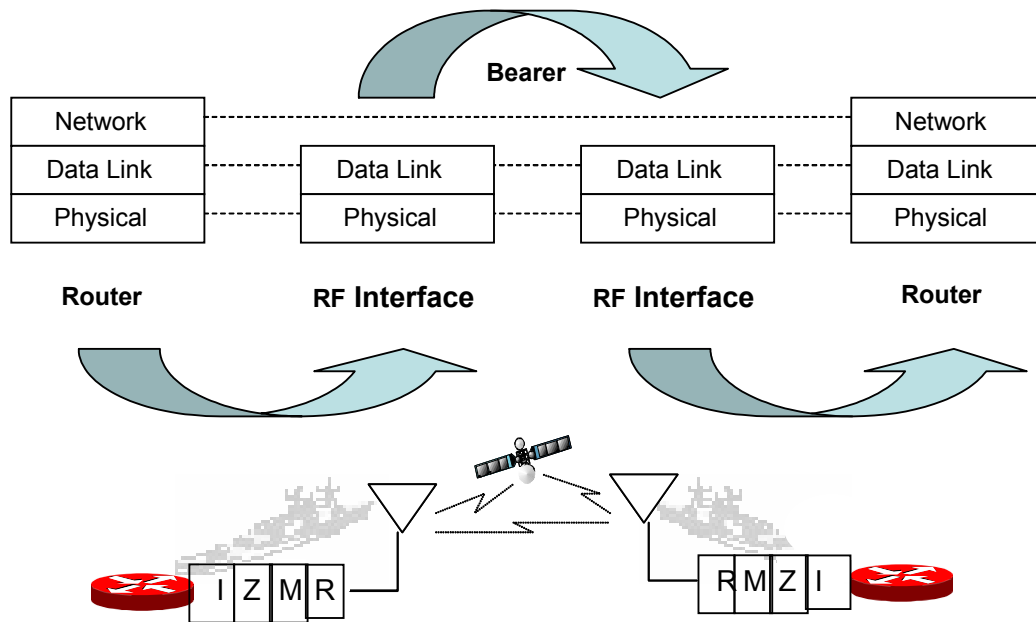
- a. A MTWAN is a collection of subnets (short for “subnetworks”) that are connected to each other by routers. In the context of IP networking, a wire, optical fiber or an RF bearer together with its associated interface and cryptographic equipment form a subnet that connects two or more routers together.
- b. While modern commercial RF communication bearers may already have the capability to support IP, many military communication bearers were not initially designed to provide IP connectivity. In these cases, special interfaces will need to be deployed in order for them to support IP.
- c. The deployed tactical military environment is typically a very mobile one, where wireless communications bearers find wider use than wired (wire or optical fiber) communications. This chapter shall focus primarily on wireless, tactical bearers.

1602 AIM

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

1603 OVERVIEW

- a. A typical MTWAN is formed between geographically dispersed LANs connected to one another through the use of disparate communication links. The communication subnets over wireless communication bearers such as INMARSAT, UHF SATCOM, UHF and HF connect routers through the use of the first three layers of the OSI model. This is illustrated in Figure 16–1.



Key: M > Modem R > Radio I > Interface Z > Crypto

Figure 16–1 Communication Subnet(s)

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

1604 DEFINITIONS

The following definitions are provided:

- a. Subnet—a segment of a data network connecting two or more network devices. A subnet is therefore a network within a network and operates at Layer 3 of the OSI model.
- b. Subnetting—the division of a network into smaller networks (subnets).
- c. Communication Bearer—a system that can establish a channel to pass data. A communication bearer operates at the physical layer (layer 1) of the OSI model.

1605 COMMUNICATIONS ARCHITECTURE (CA)

- a. The design objective of a MTWAN is to maximize capacity, efficiency and mobility of the communication bearers. The Communication Architecture (Figure 16–2) shown is designed to maximize capacity,

efficiency and mobility. The three segments shown are shore, RF, and deployed.

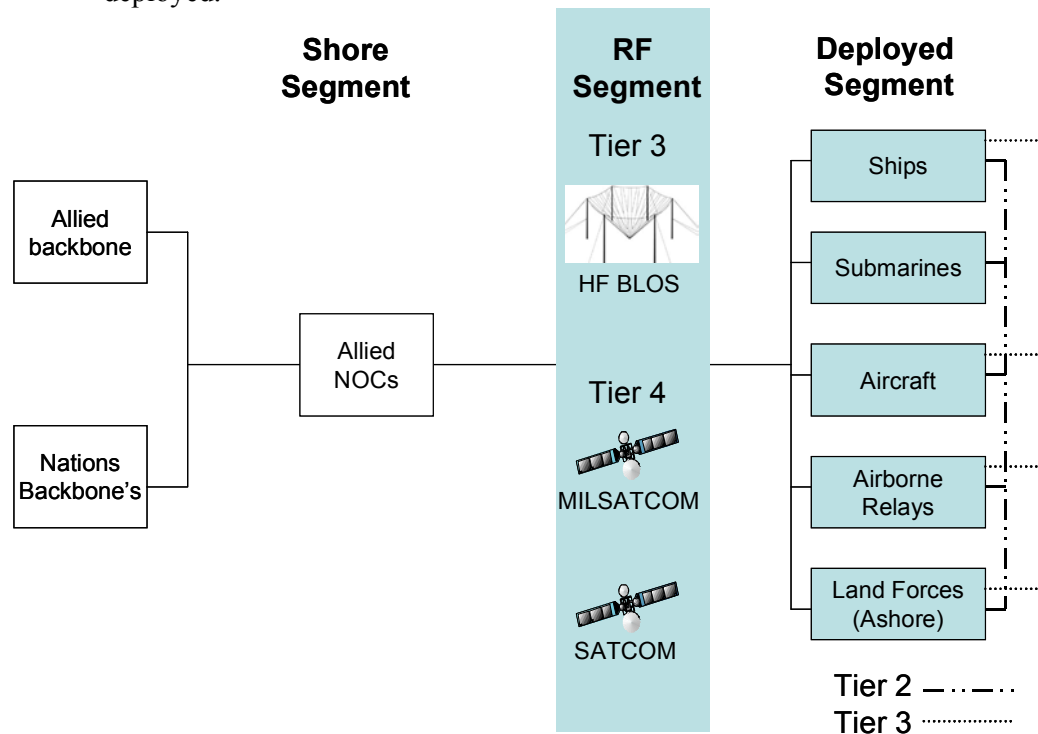


Figure 16-2 Communications Architecture

- b. Figure 16-2 shows three of the four tiers that this publication uses to classify communication bearers. The four Tiers are:
- 1) **Tier 1 —Intra platform and handheld radios.** This tier, not visible in the diagram as it is internal to the deployed segments, includes shipboard LANs (wired and wireless) and handheld radios.
 - 2) **Tier 2 —Wireless networking.** Tier 2 is networked LOS and BLOS communications between platforms and expeditionary forces ashore. This would be the equivalent of a Metropolitan Area Network (MAN).
 - 3) **Tier 3 —Wireless trunking.** This involves trunked LOS and BLOS communication links, which provide point-to-point connectivity, such as HF BLOS and Digital Wideband Transmission System (DWTS).
 - 4) **Tier 4 —Satellite communications.** This involves military and commercial satellites in the UHF, L-, X-, C-, Ku-, Ka- and Q-

bands, such as UHF SATCOM, INMARSAT, IRIDIUM, DSCS, CWSP, and. GBS/TBS.

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

1606 COMMUNICATION SUBNETS / COMMUNICATION BEARERS

- a. IP was designed around a land-based communications infrastructure that would be built on highly reliable, wideband and low-latency transmission media such as copper wires or optical fibres. A MTWAN relies on RF bearers of various forms including half-duplex and point-to-multipoint with a limited number of radios and radio frequencies. Full-duplex point-to-point bearers (such as ISDN, INMARSAT) can interface directly to routers. However, interface equipment is usually required to facilitate connection between routers with standard Serial or Ethernet interfaces over tactical RF bearers.
- b. The characteristics of the bearer in question (i.e. whether it is half-duplex or full-duplex, whether it is broadcast or non-broadcast and whether it is a high-latency circuit over a satellite) will determine the interface technology. Table 16–1 lists the bearers as well as subnets.

Bearers/Subnets	Link Rate	Typical Use	Subnet Characteristics
INMARSAT B	64- 128 Kbps	Main Data Bearer providing reachback capability to National Network Operations Centers.	<ul style="list-style-type: none"> • Full-duplex, point-to-point • Increased data rates and multiplex capability achievable with improved Modems
UHF SATCOM 25Khz	up to 48 Kbps	Email, Chat, Low data DCP, COP	<ul style="list-style-type: none"> • Limited IP capability, multi-member subnet
UHF SATCOM 5 Khz	up to 9.6Kbps	Email, Chat, COP	<ul style="list-style-type: none"> • Requires astute operation to optimise performance, multi-member subnet
HF 5066 IP	4.8-9.6Kbps	Email, Chat, COP, Low data DCP	<ul style="list-style-type: none"> • Data rate dependent on range and atmospheric propagation characteristics • High Overhead.
Subnet Relay VHF/UHF	up to 96Kbps (25KHz channel BW)	Email, Chat, Low data rate DCP, COP, non-constant bit rate traffic.	<ul style="list-style-type: none"> • Multimember network • Limited to LOS (UHF ~20nm, VHF ~80nm) • Capable of relaying beyond LOS

Subnet Relay HF	up to 9.6Kbps (SSB) 19.2Kbps (ISB)	Email, Chat, Low data rate DCP, COP, non-constant bit rate traffic.	<ul style="list-style-type: none"> • Multimember network • Limited to ELOS (HF ~150nm) • Capable of relaying beyond LOS
HF BLOS	4.8-9.6Kbps (SSB)	Email, Chat, COP, Low data DCP	<ul style="list-style-type: none"> • HF Skywave, Ranges of 2000-3000 Nm achievable • Increased data rates achievable with ISB
HF ELOS	4.8-9.6Kbps (SSB)	Email, Chat, COP, Low data DCP	<ul style="list-style-type: none"> • HF Surface Wave, Ranges of 200-300Nm achievable • Increased data rates achievable with ISB
GBS/TBS/DBS	512Kbps+	Receive only broadcast	<ul style="list-style-type: none"> • Capability available in many large platforms • Integration into MTWAN Under development
ISDN	64-2048 Kbps	Used while units are alongside or for trunk communication between NOCs. May solve land based point-to-point connectivity requirements.	<ul style="list-style-type: none"> • Full-duplex, point-to-point • Low latency

Table 16–1 Communication Subnets Matrix

1607 COMMUNICATION BEARERS/SERVICES

- a. A variety of RF and telecommunication services are available to resolve MTWAN connection requirements. Selection of a service or bearer will depend on a variety of factors including information exchange requirements, radio assets, geographic location and resource constraints. This section provides a brief overview of some typical Communication Bearer/Services available to solve WAN connectivity issues.
- b. **Integrated Services Digital Network (ISDN).** ISDN is a set of protocols that allow the user to fully integrate voice and data services over a single communication telephone line. ISDN lines are normally leased from the local telecommunication service provider and can provide a dedicated full-duplex, point-to-point link for digital network communication. ISDN lines are often used as a means to provide connectivity between fixed land-based units such as Communication Stations and shore-based NOCs. As ISDN is a public data network, information transmitted over ISDN must be protected with a Type 1 encryption device.

- c. Other Telco services such as Private Office Networks (PON) or Digital Data Services (DDS) may provide the connection speed and QOS required by a MTWAN. The cellular 3G networks, which reportedly can provide high-speed mobile data transmissions, may also offer a viable MTWAN subnet solution for ground forces and maritime units deployed in littoral waters.
- d. **INMARSAT B.** INMARSAT is a commercial satellite system used for voice and up to 128Kbps data connectivity. The system uses geostationary satellites to provide near global coverage for maritime and land force elements. Because it uses geostationary satellites the connection has a high latency, which makes it less efficient for TCP. Regardless, it has been extensively used by nations to provide reachback connectivity between mobile units and shored-based NOC. As a commercial satellite system the expense of this connection can be prohibitive. To limit budget over-runs and provide fixed cost many nations lease dedicated INMARSAT channels.
- e. Several variances of INMARSAT exist and various methods exist to improve data throughput. More detail on the INMARSAT system can be found at Annex A to this chapter.
- f. **High Frequency Beyond Line-Of-Sight (HF BLOS).** Various investigations have been conducted in order to provide a viable HF BLOS solution. HF BLOS subnets use skywave RF links to provide connectivity. As such, these types of connections are generally point-to-point solutions with very low data rates. The high BER of HF makes this type of channel unsuitable for TCP connectivity. Various techniques have been developed to improve this; however, as yet no deployable HF BLOS solution exists.
- g. **High Frequency Extended Line-Of-Sight (HF ELOS).** HF ELOS uses the HF ground wave to provide data connectivity between MTWAN units. The high BER and narrow bandwidth limit this connection to relatively low data rates; however, this may provide a viable solution for disadvantaged units with low Information Exchange Requirements (IERS). Several technologies have been employed to provide ELOS solutions although no nation has yet adopted this as a primary network connection between mobile units.
- h. **Other Communication Bearers.** Other communication bearers include UHF and VHF LOS, and UHF, SHF and EHF satellite links.

1608 SUBNET TECHNOLOGIES

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

- a. **SubNet Relay (SNR).** SNR provides a multi-node, multi-hop mobile-to-mobile IP connectivity over VHF/UHF LOS and HF ELOS. SNR uses relay nodes to extend the coverage of a subnet beyond a single hop. SNR also fulfils the requirement to allow subnets to be formed when network connectivity between all Task Group members is not complete. SNR is seen as a viable solution to providing a tactical IP network, reducing the reliance on satellite circuits, and providing communication redundancy. SNR has been proven at sea by Canada and UK using existing radio equipment. SNR is further explained at Annex B to the chapter.
- b. **Medium-rate Channel Access Processor (MCAP).** MCAP provides a solution for IP forwarding over broadcast communication systems such as UHF SATCOM. The MCAP has been designed by the USN and is not available for commercial release.
- c. **Standard NATO Agreement (STANAG) 5066 Editions 1 and 2.** STANAG 5066 is a link protocol for data transmissions over HF. The standard also provides the recommended requirements for an IP Router interface and an interface for SMTP email. Edition 2 of the standard, in advanced draft phase, will provide the mandatory requirements for a multi-member, full IP services subnet over HF ELOS. More details of STANAG 5066 can be found at Annex C.

1609 CONCLUSION

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

INMARSAT B

16A01 INTRODUCTION

Ships are commonly fitted with an INMARSAT (International Maritime Satellite Organisation) B capability. INMARSAT High Speed Data (HSD) provides a point-to-point medium bandwidth connection capable of passing IP traffic.

16B02 AIM

This chapter provides general guidance on the set-up and use of INMARSAT B.

16A03 OVERVIEW

INMARSAT-B is used by Navies to provide voice, fax and data traffic to mobile and remote users. Its point-to-point full-duplex subnet and medium data rate capability make it a regular mainstay bearer for IP networking.

16A04 DESCRIPTION

- a. The INMARSAT network consists of 12 communication satellites (ten operational plus two in-orbit spares) in geostationary orbit around the equator. The satellites cover the globe from Latitude 70 N to 70 S and are grouped to cover four regions: Atlantic Ocean Region – West, Atlantic Ocean Region – East, Indian Ocean Region, and Pacific Ocean Region. Global coverage is shown at Figure 16–A–1.

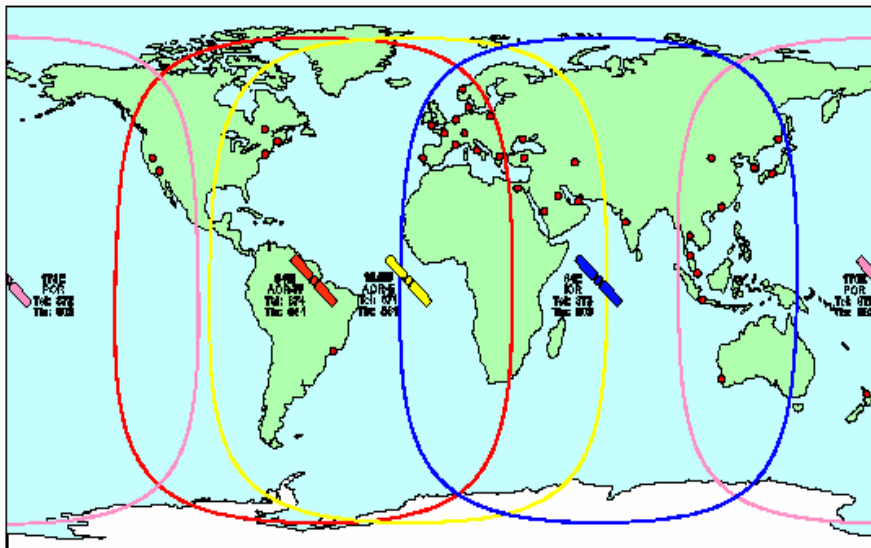


Figure 16–A–1 Global INMARSAT Coverage

- b. Land Earth Stations (LES's) are located in various countries around the planet, and are the gateways which provide the link between the satellites and public terrestrial telecommunication networks.
- c. The INMARSAT-B High Speed Data (HSD) service provides a full duplex, 56 or 64Kbps (user-selectable) data service with terrestrial delivery typically via ISDN. The configuration for INMARSAT-B fitted ships is shown in Figure 16-A-2. The configuration would be similar for INMARSAT-A fitted ships, the difference being the absence of an HSD connection.
- d. To use the HSD interface, a synchronous serial interface is required. Whilst a number of options are available, it is important to choose a device that has been optimised for data transmission over a satellite/ISDN network.

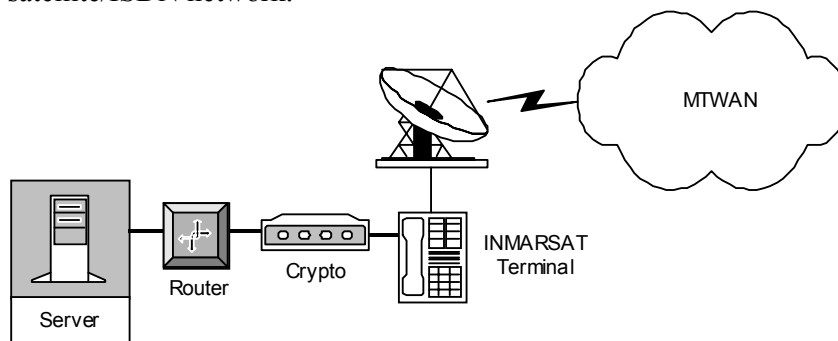


Figure 16-A-2 INMARSAT B Configuration

16A05 LIMITATIONS

- a. There are few restrictions in terms of INMARSAT coverage, as the INMARSAT system is designed to provide global communications access.
- b. However the availability of INMARSAT can be effected by:
 - 1) **Antenna Blockage or Wooding** —In some ships, it may not be possible to site the INMARSAT antenna/e to ensure continuous satellite coverage irrespective of ship course. As such, there are certain ship courses where the communication path to a satellite will be obstructed by the ship's structure. Therefore, in some situations, restoration of satellite access will require a change in course, or the use of another satellite (provided the ship is in an area of overlapped satellite coverage).
 - 2) **EMCON** —Some EMCON conditions will require INMARSAT to be switched off.

UNCLASSIFIED

Annex A to Chapter 16 to ACP 200 (A)

- 3) **Cost** —Whilst good satellite coverage is provided, INMARSAT is the most expensive of the current communication bearer options for channel utilisation. Costs can range from US\$3/min for LSD to US\$14/min for HSD. It is normal for INMARSAT users to shop for the most cost effective LES that is able to provide coverage in order to minimise operating costs. Note that in general ship-to-shore calls are cheaper than shore-to-ship calls.

16A06 SETUP

- a. The set-up for MTWAN Networking differs from that used for standard voice telephony or stand-alone PC to PC file transfer using INMARSAT.
- b. **Terminal Configuration.** The only configuration item that may require setting up, depending on the brand of INMARSAT terminal used, is the incoming and outgoing call route for HSD calls. This configuration item controls which I/O port an HSD call will be connected to. For example with a Nera Saturn B, the High Speed data is routed through the 25 pin DTE port on the Main Control Unit. To activate the High Speed Data option the “Enhanced Setup” function, accessed through the operators handset, is used.
- c. **Cryptographic Requirements.** KG-84A / KIV-7 are typically employed. However, as the INMARSAT HSD link is a point-to-point link other cryptographic units may be used so long as the same, or at least compatible, devices are used at both ends. Operational configuration of interoperable cryptographic devices, e.g. KIV-7/KG84/BID1650 may be found in ACP 176 NATO SUPP 1.

16A07 ESTABLISHING A CONNECTION

- a. A connection can be established either manually or automatically by the router subject characteristics of the router, type of cryptographic device employed and EMCON restrictions. For example, the use of KG84A prevents the use of Automatic dialing.
- b. A manual connection can be established by either end and is simply a matter of placing a call (HSD call from the INMARSAT terminal) to the other end. For example from a Nera Saturn B: lift the handset and dial *25*64# to select a HSD call, then dial the phone number of the other end. When the other end answers the Nera terminal will attempt to synchronise with the ISDN terminal adapter or other INMARSAT terminal at the other end. Once connected the handset display will report “HSD CONNECTED”. At this point the two INMARSAT terminals are talking to each other.

UNCLASSIFIED

Annex A to Chapter 16 to ACP 200 (A)

- c. The next step is to confirm the routers are connected. The MTWAN standard routing protocol is OSPF, and the connection between routers can be determined by querying the neighbour state. If CISCO routers are used this is achieved by the typing the command line “show ip ospf neighbour”

16A08 MAINTAINING A CONNECTION

Currently there is no method of ensuring that the connection to the ship can be maintained. If the ship's superstructure, a blind spot in the satellite's footprint or other atmospheric phenomena cause the connection between the ship and the satellite to be lost then the only method to reconnect is as outlined above, a manual process that introduces delay and error. Delays and errors may be increased by the need to retransmit data that has already been sent. Some INMARSAT units will report the current signal strength or signal to noise ratio. If available these should be checked before use.

SUBNET RELAY

16B01 INTRODUCTION

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

16B02 AIM

The document provides a Concept of Operations for Subnet Relaying.

16B03 OVERVIEW

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

16B04 USER REQUIREMENT

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

UNCLASSIFIED

Annex B to Chapter 16 to ACP 200 (A)

- b. The operational requirements are thus to:
 - (1) Alleviate the reliance on Satcom;
 - (2) Provide communications redundancy;
 - (3) Provide an IP networking capability to non-Satcom ships;
 - (4) Provide indirect access to Satcom to ships without Satcom; and
 - (5) Significantly improve interoperability within our Allies as well as within a coalition task group, in particular to improve interoperability with lesser equipped navies.
- c. The operational requirements are complemented with the functional requirements to provide:
 - (1) An *ad hoc* tactical IP internetworking capability between ships in a national and/or coalition task group using LOS/ELOS tactical communication bearers; and
 - (2) A multi-node, multi-hop, ship-to-ship network with a relay capability (i.e. at Layer 2) using IP protocols.
- d. Maximising the use of all available bearers within the task group provides a feasible alternative to Satcom, in forming a communications backbone for the MTWAN. UHF LOS and HF ELOS are bearers available on most naval platforms, while VHF LOS and HF BLOS provide useful additions. The operational networking communications concept is shown at Figure 16-B-1.

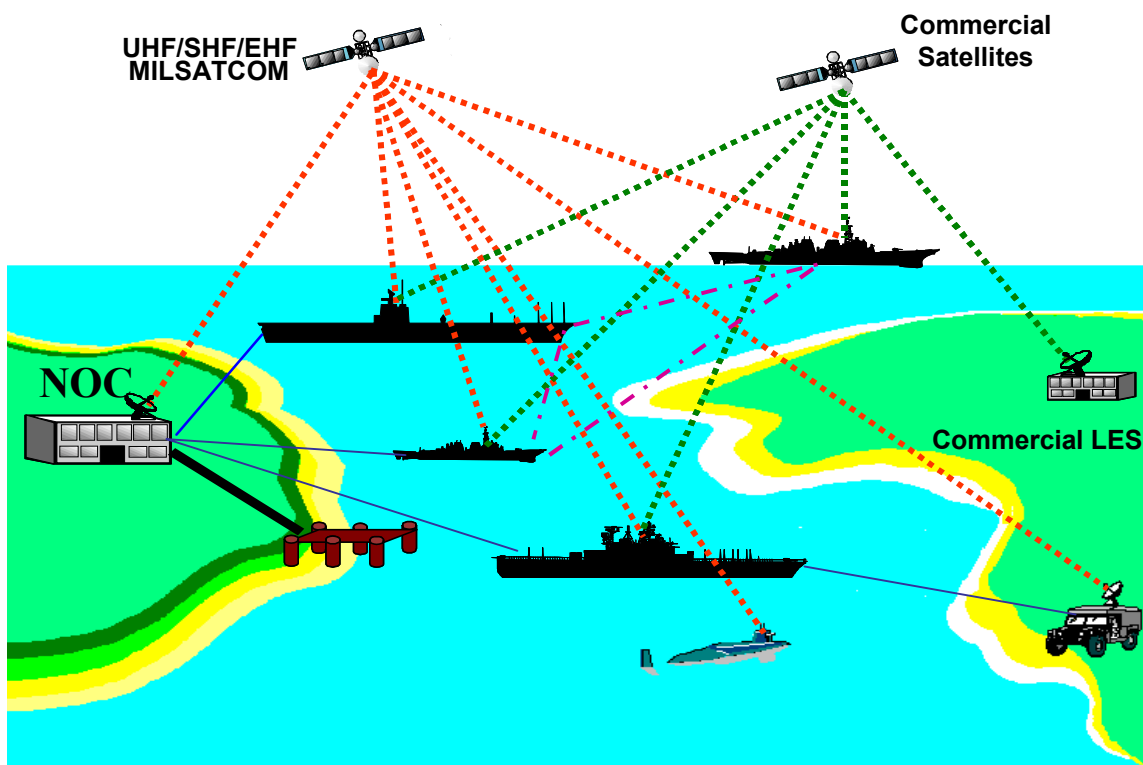


Figure 16-B-1 Operational View

16B05 OPERATIONAL CONCEPT

- a. SNR is most easily explained with a few scenario diagrams where ships are not all within LOS. The scenario that will be considered is that of two battle groups where a ship moves from one battle group to the other. The scenario is depicted through Figures 16-B-2 to 16-B-8. The notion of relaying is depicted in Figure 16-B-2. This figure illustrates a ship (red ship to the left) wanting to communicate with another ship (red ship to the right) within the same battle group but beyond its line-of-sight (black circles). Since direct communication is not possible, the ship originating the traffic will call upon another ship, a relay ship (blue), which is within LOS communications of the source and destination ships to relay the information.
- b. Each ship within the battle group becomes aware of those ships it can reach directly and those it can reach via relay(s). Thus, all ships within this battle group automatically form a single SNR (self-configuring) subnetwork.

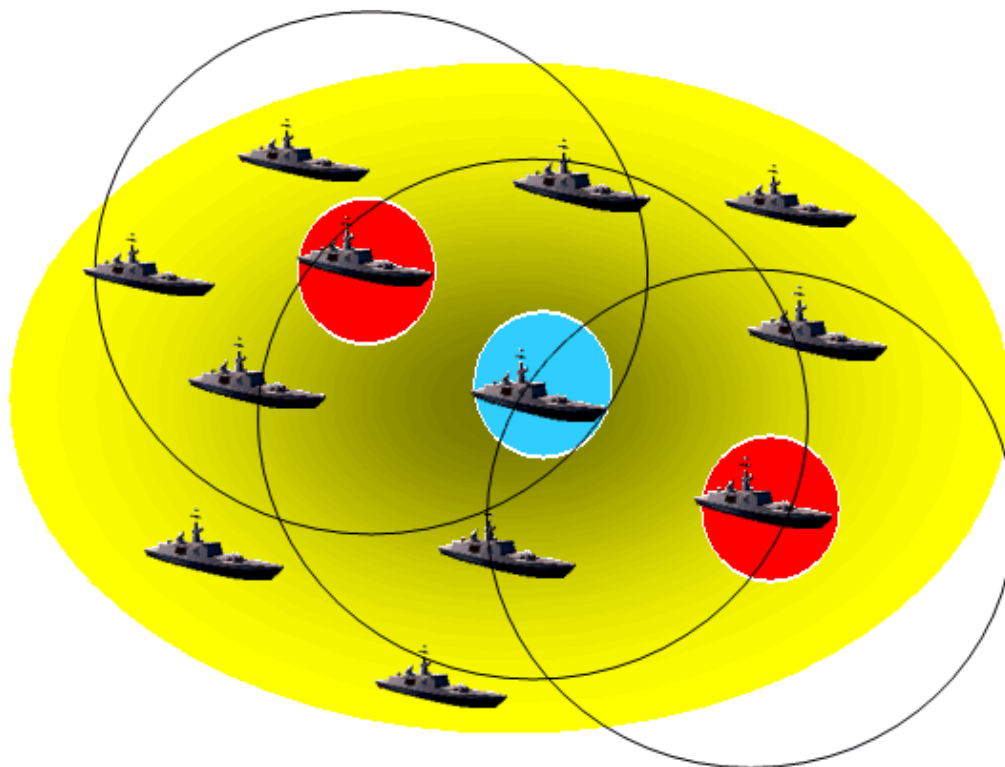


Figure 16-B-2 Relaying Concept

- c. Figure 16-B-3 merely illustrates that a ship is moving from one battle group to the other battle group. During the move, it will continue to communicate with members of the battle group.

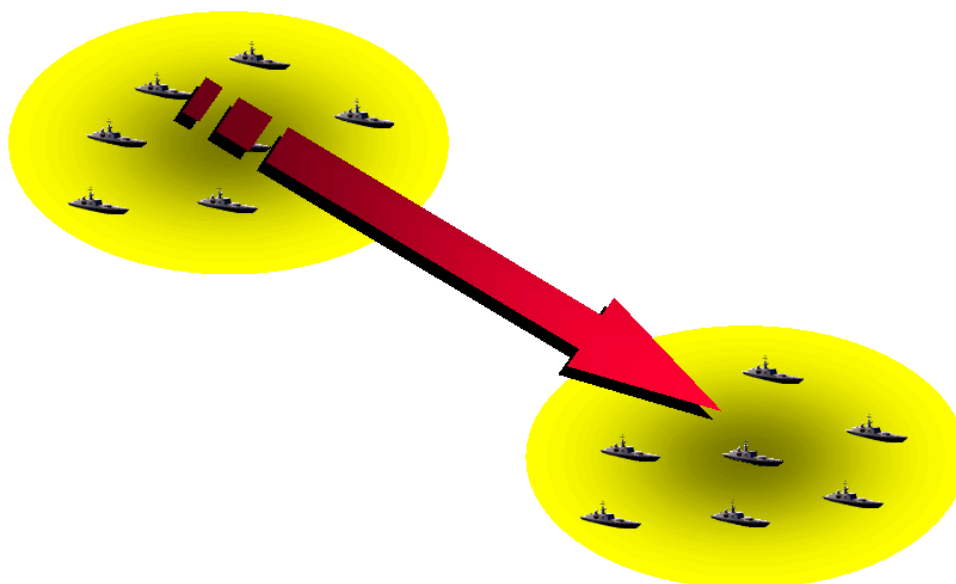


Figure 16-B-3 Ship Moving from one Battle Group to Another

- d. Figure 16–B–4 illustrates that as our ship is moving toward the other battle group, it may change its relay ships. In this example, the moving ship has moved outside of direct communication with the ship it was using as a relay before and, therefore, picks another ship that is in contact with him as the relay point. This illustrates that the subnetwork is dynamically updating its relay architecture as the ships move. It is also shown that the ship can use other ships as relay, as appropriate, to reach other ships within the battle group. Any ship can have more than one relays and relays are picked up dynamically.

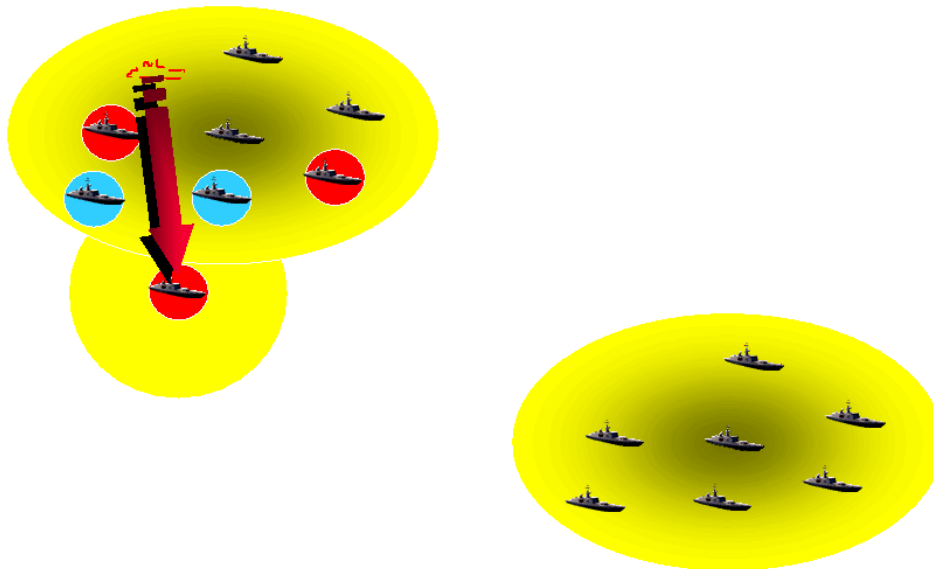


Figure 16–B–4 Multiple, Dynamic Relays

- e. As the ship is moving toward the other battle group, it may find itself within LOS communication range from another ship. In such a case (Figure 16–B–5), the two ships can communicate directly, without the need for a relay ship.

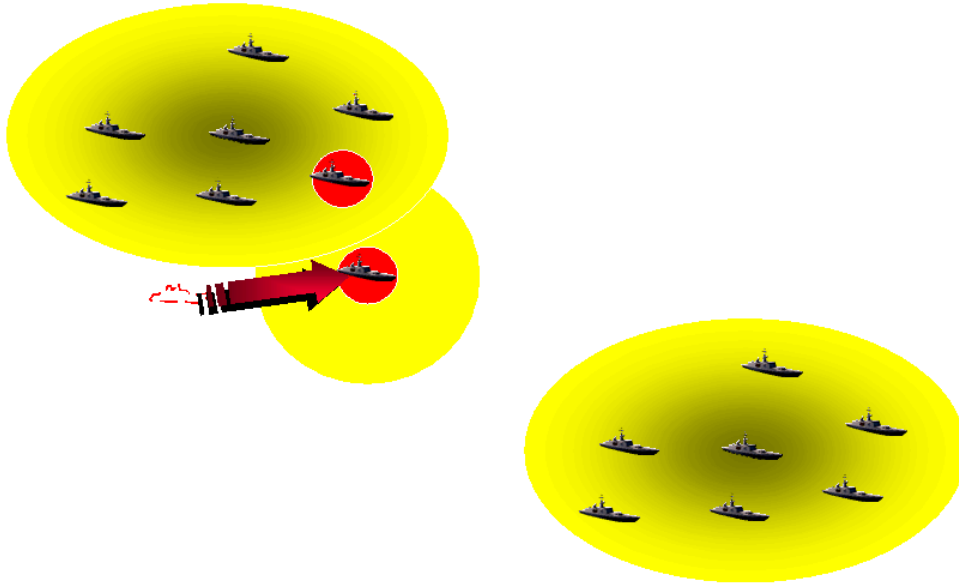


Figure 16–B–5 Relaying only when needed

- f. As the ship continues to move away from its initial battle group, it may find itself outside of communication range from any ships in either of the two battle groups. In such a case (Figure 16-B-6), he will be de-affiliated from its initial battle group SNR subnetwork, and the ship will form its own SNR subnetwork.

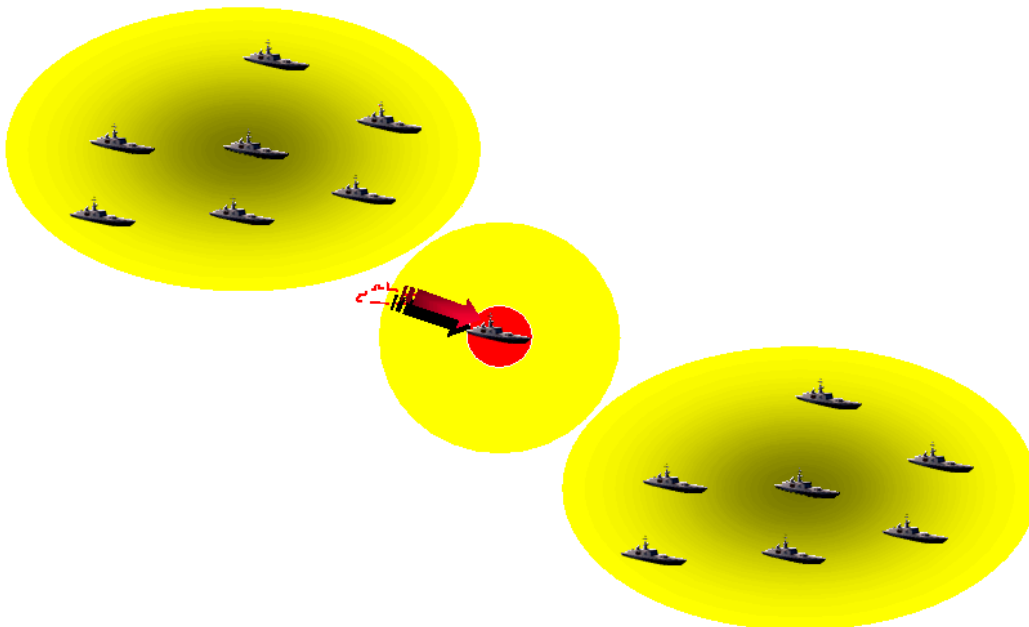


Figure 16–B–6 Subnetwork Splitting

- g. Eventually the ship arrives within LOS communication range of the other battle group. At that time, the two SNR subnetworks (single ship and second battle group) will merge to form a single SNR subnetwork (Figure 16-B-7). As before (Figure 16-B-5), the ship can communicate directly, without relay, with other ships within LOS.

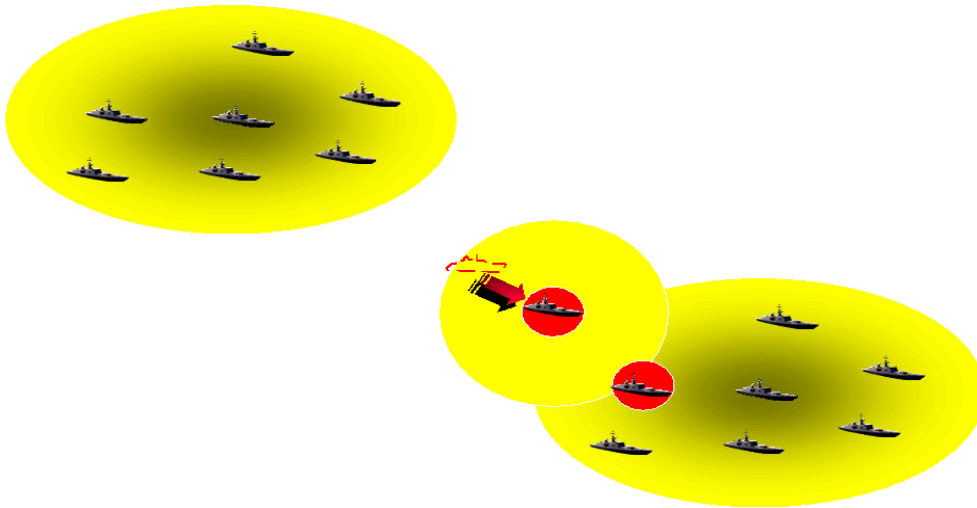


Figure 16-B-7 Subnetwork Merging

- h. Figure 16-B-8 illustrates that in this new battle group, multiple relays may be required from source to destination. SNR can accommodate up to 4 relays (5 hops) from source to destination.

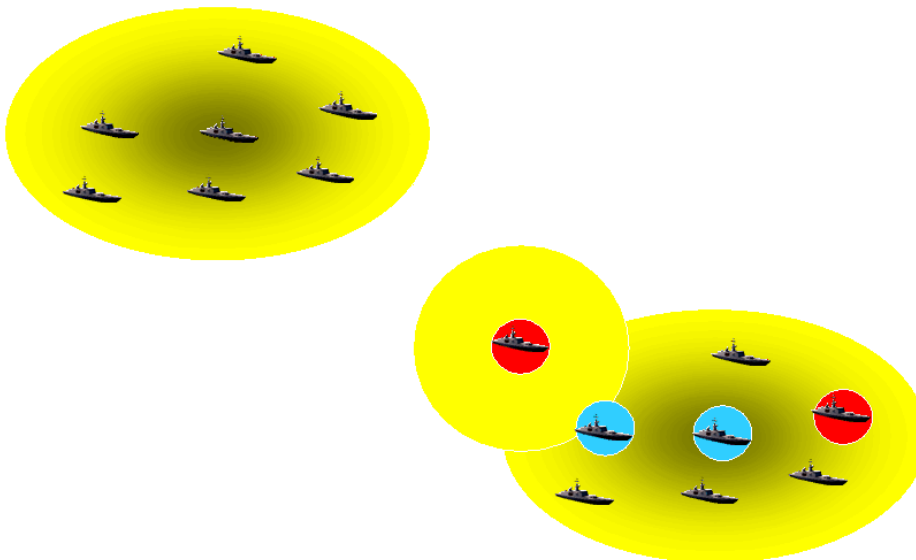


Figure 16-B-8 Multiple Relays to Destination

16B06 CAPABILITIES

- a. A MTWAN SNR network is limited to 16 users (platforms), with the maximum number of relays being 4 (allowing 5 hops, which will cover approx 150nm in a straight line assuming 30nm LOS distance, or more than a 1000 nm for HF ELOS).
- b. A MTWAN SNR network will be capable of fully distributed (e.g. masterless) and automatic operations.
- c. A MTWAN SNR network will be capable of allocating bandwidth in proportion of each platform instantaneous traffic load.
- d. SNR is a self-configuring, self-organizing network technology. The SNR will re-configure within 2-3 minutes when a UHF link or many links are lost, or when a new link (new member) appears.
- e. SNR will be capable of supporting medium bandwidth applications such as DCP, COP dissemination, web browsing, FTP, email with attachments, etc.), and be capable of supporting more bandwidth intensive applications if faster communication links are provided.
- f. SNR will allow for bulk encryption at the Link Layer. The encryption strength will be dictated by the cryptos used in conjunction with the SNR system. SNR will be capable of interfacing to national cryptos used in AUSCANNZUKUS nations.
- g. Achieve coded data rate of 2.4kbps to 16kbps using HF ELOS (SSB) with high speed HF modems. In the future, higher data rates could be achieved using new waveforms, ISB radio, or multiple non-adjacent HF channels.
- h. Achieve coded data rate of 16kbps to 96kbps using UHF LOS over a standard 25 kHz audio frequency interface channel. In future, much higher than 96kbps coded data rate could be achieved using greater than 25kHz bandwidth, such as the intermediate frequency (IF) channel on radios that support this function.
- i. Provide capability to manually initiate and terminate relays (used in an EMCON environment).

16B07 TECHNICAL LIMITATIONS AND INITIAL ASSUMPTIONS

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

- a. There are a limited number of radios available onboard sea-going units, therefore subnets will probably be limited to a single radio/frequency. A SNR system will be capable of operation when untethered (mobile) platforms have a single half-duplex radio per subnet.
- b. All nodes (platforms) are mobile, therefore relay platforms must be selectable automatically and dynamically.
- c. Reliable and unreliable link operations must be supported.
- d. A subnet will be made up of bearers of a single nature (e.g. all HF BLOS, all UHF LOS etc).
- e. Platforms have access to a reliable clock.
- f. Tx/Rx switching times of the order of 20 ms using HF and 50 ms using UHF are expected of current naval radios.

LIST OF ABBREVIATIONS

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

UNCLASSIFIED

ACP 200(A)

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

LOA-2

UNCLASSIFIED

UNCLASSIFIED

ACP 200(A)

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

LOA-3

UNCLASSIFIED

UNCLASSIFIED

ACP 200(A)

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

LOA-4

UNCLASSIFIED

UNCLASSIFIED

ACP 200(A)

MSL	Multi- Security Levels
MTA	Message Transfer Agent
MTWAN	Maritime Tactical Wide Area Network
NBAR	Network-Based Application Recognition
NCW	Network Centric Warfare
NES	Network Encryption System
NM	Network Management
NNTP	Network News Transport Protocol
NOC	Network Operations Center
NRS	Naval Radio Station
NZ	New Zealand
OPCON	Operational Control
OPGEN	Operational General Messages
OPTASK	Operational Tasking Messages
OSI	Open System Interconnect
OSPF	Open Shortest Path First
OTCIXS	Officer in Tactical Command Information eXchange System
PAD	Packet Assembler Disassembler
PC	Personal Computer
PCM	Pulse Code Modulation
PIM	Protocol Independent Multicast
PKI	Public Key Infrastructure
PLAD	Plain Language Address Designator
P_MUL	Protocol Multicast
POP3	Post Office Protocol Version 3
PPK	Pre-Placed Keys
PPP	Point-to-Point Protocol
PQ	Priority Queuing
PT	Plain Text
QOS	Quality of Service

LOA-5

UNCLASSIFIED

UNCLASSIFIED

ACP 200(A)

VPN	Virtual Private Network
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Dropping
Z	Cryptographic Device

LOA-7

UNCLASSIFIED

UNCLASSIFIED

ACP 200(A)

RED	Random Early Drop
RIP	Routing Internet Protocol
RF	Radio Frequency
RP	Rendezvous Point
RSVP	Resource ReServation Protocol
RTF	Rich Text Format
RTT	Round-Trip Time
SHF	Super High Frequency
SIPRNET	Secret Internet Protocol Router Network (United States)
SMG	Secure Mail Guard
SMTTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNR	SubNet Relay
SOPS	Standard Operating Procedures
TBS	Theatre Broadcast Systems
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEK	Transmission Encryption Key
TG	Task Group
TGAN	Task Group Area Network
TOI	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

LOA-6

UNCLASSIFIED

LIST OF EFFECTIVE PAGES

Subject Matter	Page Numbers
Title Page	I
Foreward	II
Letter of Promulgation	III
Record of Message Corrections	IV
Table of Contents	V to XIV
List of Figures	XV to XVI
List of Tables	XVII
Chapter 1	1-1 to 1-5
Chapter 2	2-1 to 2-11
Chapter 3	3-1 to 3-30
Chapter 4	4-12
Chapter 5	5-1 to 5-3
Chapter 6	6-1 to 6-18
Chapter 7	7-1 to 7-7
Chapter 8	8-1 to 8-20
Chapter 9	9-1 to 9-25
Chapter 10	10-1 to 10-13
Chapter 11	11-1 to 11-10
Chapter 12	12-1 to 12-29
Chapter 13	13-1 to 13-33
Chapter 14	14-1 to 14-16
Chapter 15	15-1 to 15-19
Chapter 16	16-1 to 16-20
List of Acronyms	LOA-1 to LOA-7
List of Effective Pages	LEP-1