Tactics, Techniques, and Procedures (TTP) for Joint Mobile Network Operations (JMNO)

Version 1.0

26 October 2007

This page intentionally left blank.

_____

Submitted By: Col. Edmund C. Mitchell, USMC
Joint Deputy Test Director
JMNO JT&E

_____

Approved By: Dr. George Nobles
Program Manager
JMNO JT&E

This page intentionally left blank.

Table of Contents

CHAPTER 1: INTRODUCTION

1.1 Introduction

This publication documents the tactics, techniques, and procedures (TTP) for Joint Mobile Network Operations (JMNO). These TTP address the ability of joint force tactical units (brigade and below or equivalent) to communicate directly with each other across Service lines and to access home network services when crossing Service network boundaries. Using the JMNO TTP, tactical units act as endpoints for lateral links between the Services. These lateral links allow specific IP traffic to remain local, rather than going through the already congested links at higher headquarters, reducing latency at all levels.

This document logically falls into two sections. The first section (Chapters 1 through 3) provides background information and defines the scope of the document. The second section includes the planning and implementation steps necessary to implement the lateral links. Chapter 3 provides definitions of JMNO-specific terms, including more details on the concepts that are the foundation of the JMNO solution. Chapters 4 and 5, designed for JTF planners and tactical data communications officers, focus mainly on procedures with little background information. This organization is meant to allow readers to find desired information quickly and easily.

JMNO Joint TTP support the Executive Agent (EA) for Theater Joint Tactical Networks (TJTN) by providing new joint capabilities to the Operational Area Network (OAN) concept.

This page intentionally left blank.

CHAPTER 2: OVERVIEW

2.1 Scope

The JMNO program exists to address two specific network issues dealing with challenges to tactical joint forces. The two main goals for JMNO are to:

- Enable joint tactical forces (brigade level and below or equivalent) to establish direct IP network connectivity
- Enable mobile users to access home network resources through cross-Service network links

2.2 Objectives

The objectives of these TTP are to provide the ability to:

- Enable interoperability between different Services' tactical IP networks, while ensuring current network performance and Information Assurance (IA) are not negatively affected
- Enhance the ability of warfighters to connect to Service-specific information resources while maneuvering through another Services' area of responsibility without degrading the host Service's network
- Enable interoperability, including Information Assurance (IA) negotiation, between tactical IP networks of different Services in a joint operation by providing a standardized planning process and analysis tools
- Consider the affect of lateral links on JTF level NetOps

2.3 Benefits

Benefits of using these TTP include the following:

- Increased availability of strategic bandwidth by reduction of tactical-level IP traffic traversing the overburdened JTF and Defense Information Systems Network (DISN) up-links
- Reduced latency and increased throughput of IP-based communications between joint tactical units by using local links
- Enhanced situational awareness (SA) between different forces operating in the same Joint Operations Area (JOA) through improved timeliness of common operational and tactical data
- Less time required to coordinate network capability for joint force task organizations

This page intentionally left blank.

CHAPTER 3: DEFINITIONS AND DESCRIPTIONS

3.1 Introduction

This section provides definitions and descriptions of terms. This section has two sections: JMNO-specific terms and terms that are not specific to JMNO, but are defined here for clarity.

3.2 JMNO-Specific Terms

The following terms are unique to JMNO. These terms provide a framework for understanding the concepts that are the foundation of the JMNO tactics, techniques, and procedures (TTP).

3.2.1 JMNO Purple Zone

The Tactical Joint Network or JMNO "Purple Zone" enables the Services' operating forces to pass Internet Protocol (IP) data freely between joint and Service command and control (C2) nodes and combat elements during combat operations or exercises. The Purple Zone exists at the tactical level (brigade and below or equivalent) and is not constrained to use of traditional Defense Information Systems Network (DISN) or Joint Task Force (JTF) communications paths. Instead, the Purple Zone uses currently fielded equipment and is not dependent upon, but can readily accept, newly fielded equipment. The prime enablers of the Purple Zone are a joint tactical information assurance (IA) policy, standardized router configurations, and reemployment of transmission equipment. In addition to improving data transfer rates, increasing reliability, and adding more flexibility for tactical users at the tactical level, the Purple Zone should significantly reduce network congestion at the JTF level and at Standardized Tactical Entry Point (STEP) and Teleport sites. Therefore, the JTF commander and Service component commanders will experience an overall improvement in IP communication as a secondary effect of the JMNO TTP.

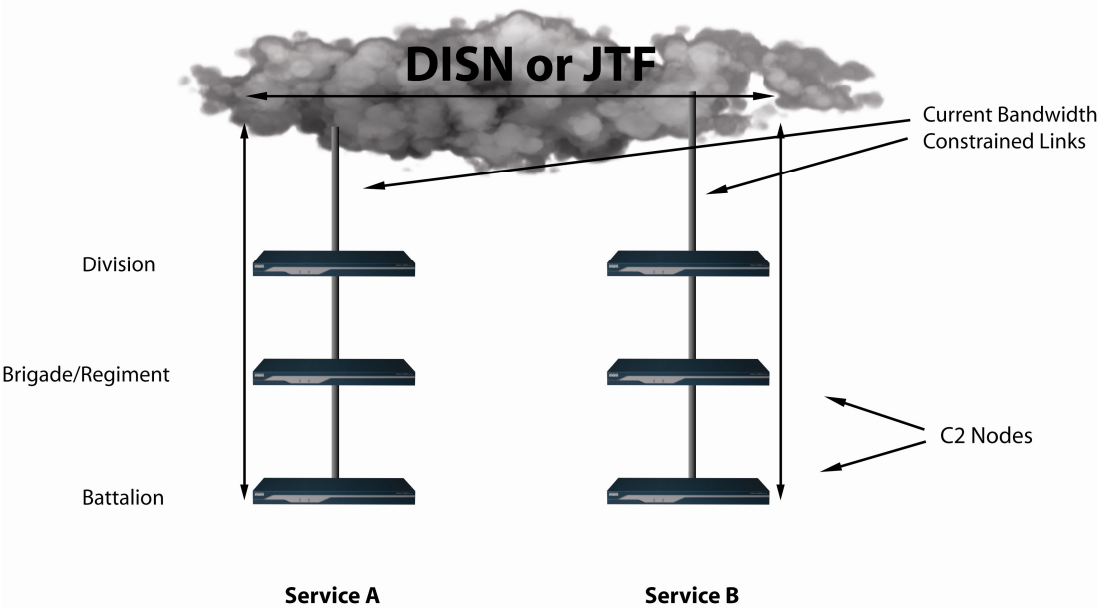


Figure 3-1: The Current Doctrinal Concept

3.2.2 Lateral Link Connection (LLC)

A Lateral Link Connection (LLC) is a communications path that branches from traditional "stove pipe" architectures to reach a cross-Service destination. For example, the LLC may connect an Army Brigade headquarters directly to a Marine Regimental headquarters or similar unit. The LLC is defined by several elements, to include the transmission devices, the information exchange requirements, the bandwidth, routing and application protocols, and various IA considerations. In this example, the tactical unit headquarters are considered Lateral Link Nodes.

3.2.3 Lateral Link Node (LLN)

A Lateral Link Node (LLN) is an existing Service-internal tactical C2 node that becomes the default gateway for sending and receiving IP data to and from Service-external or Joint destinations. For example, if an Army unit in a joint operation needed to send IP data to a Marine unit operating in the same area, that Army unit would send the data to the Army unit that has been designated as the Army LLN. The Army LLN automatically forwards the data, over the lateral link, to the Marine Corps LLN which then forwards it to the Marine Corps unit.

3.2.4 Lateral Link Conditions

The following terms relate to lateral link conditions. For more information regarding these conditions, see **Annex A: Information Assurance**.

3.2.4.1 Network-to-Network (NTN)

A network-to-network (NTN) condition describes the condition where two IP networks are directly connected.

3.2.4.2 User-to-Network (UTN)

A user-to-network (UTN) condition describes the condition where mobile users have moved to the network on the other side of the NTN and have access to resources and services within that network. A UTN condition is not dependent on an NTN being in place, as the mobile user is using only services available via the host network. Strictly speaking, this scenario is outside the scope of JMNO research, but is nonetheless covered in the IA portion of this TTP (**Annex A: Information Assurance**).

3.2.4.3 User Cross-Network (UCN)

A user cross-network condition describes the condition where mobile users have moved to the network on the other side of the NTN and have access to resources and services within their home network. An NTN connection must exist for a UCN to be supported.

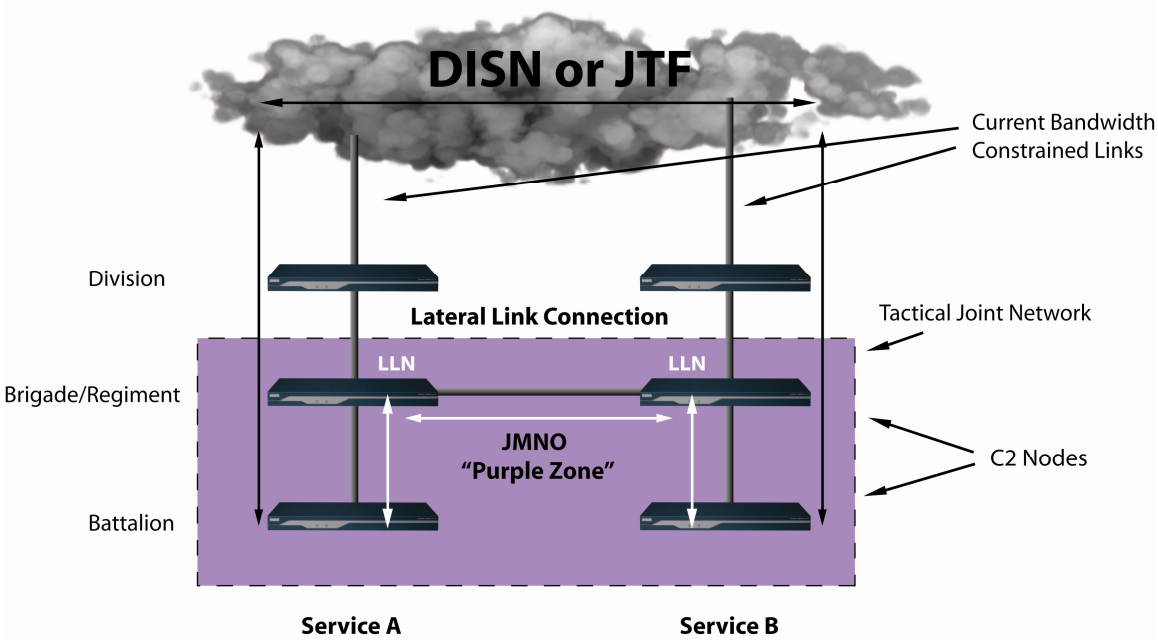


Figure 3-2 Lateral Link Nodes (LLNs)/Lateral Link Connections (LLCs)

3.2.5 Multi-Link Distribution Node (MDN)

A Multi-link Distribution Node (MDN) is an LLN that acts as a third-party bridge for IP data between the nodes of two other Services. For example, if a Navy unit were introduced into the previously-described scenario, the Navy unit, also acting as a Navy LLN, could establish a lateral link with the Marine LLN. If the Navy needed to send IP data to the Army but were unable to establish a physical lateral link with the Army, it would send the data to the Marine LLN, which would automatically forward the data to the Army LLN. In this case, the Marine LLN has taken on the additional responsibility of being an MDN.

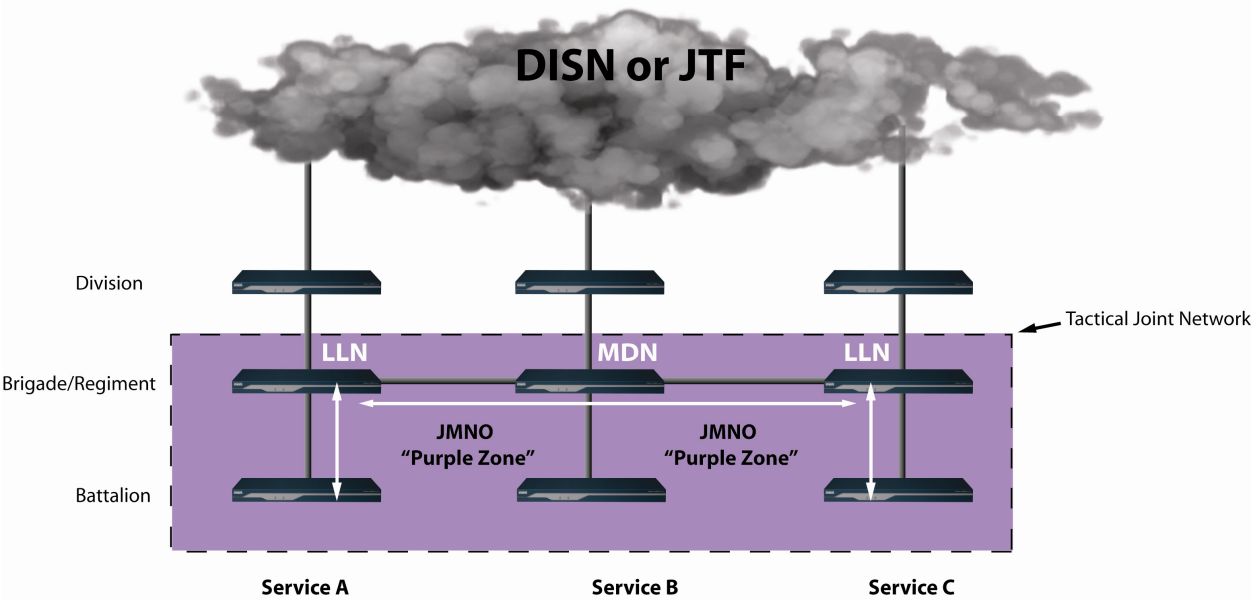


Figure 3-3 Multi-Link Distribution Node (MDN) Concept

3.2.6 Mobile Users

Mobile users are tactical network users who have traveled outside of their home network area, but still need to connect back to their home network to access information resources and network services. Mobile users in the JMNO Purple Zone will be able to reach back through another Services' network, via the lateral link, to access their home network. For example, a Marine regimental liaison officer could enter an Army Brigade headquarters in which he is going to be assigned and then connect to the Army network. The Marine would be able reach back via the lateral link and access his email server, a file server, or website as if he were sitting at his own desk in the Regimental headquarters, thus increasing his effectiveness as a liaison.

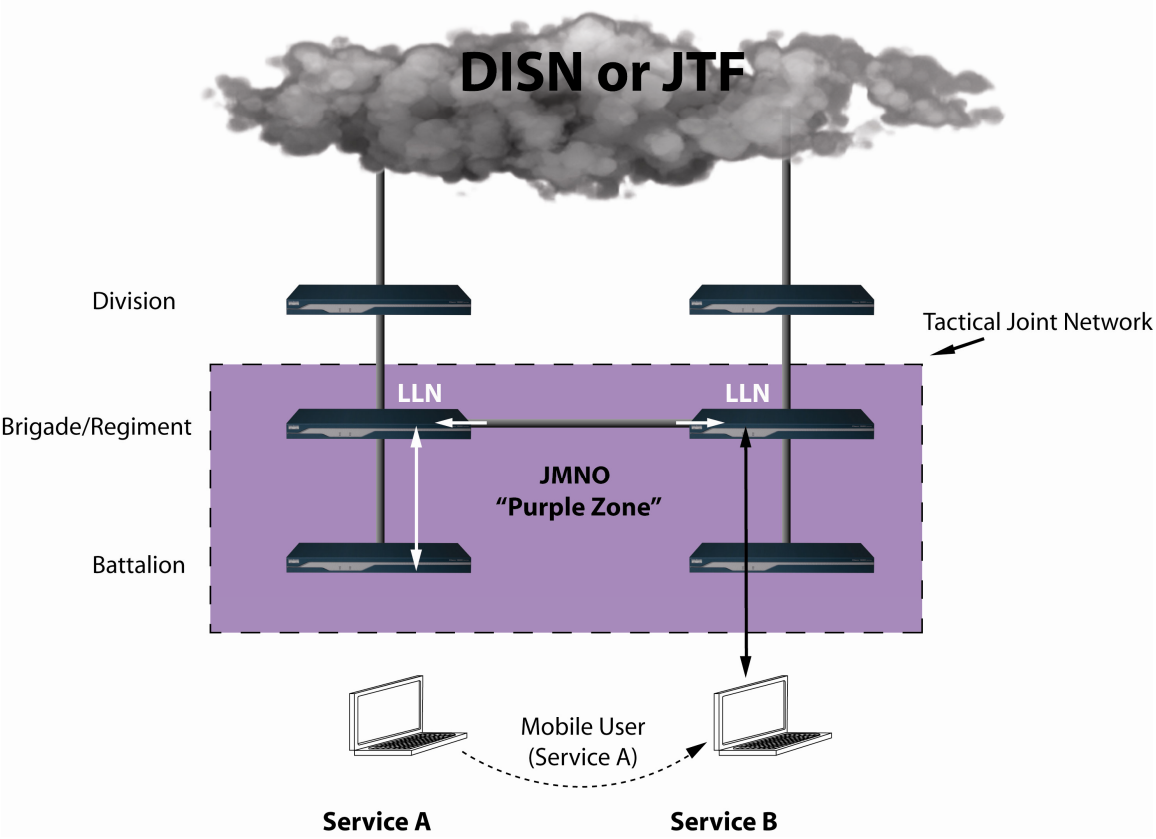


Figure 3-4 JMNO Mobile User Concept

3.3 Descriptions for Non-JMNO Terms

The following terms are not unique to JMNO. These terms are described here for clarity.

3.3.1 C4 Planner

The C4 planner is the planner responsible for planning the lateral links and can include JTF and tactical level planners. This term can also include the JTF J6 and staff, Component G6

or N6 and their staffs, tactical unit S6s and their staffs, Marine Data Communications Officers, Army Signal Officers, senior enlisted planners, etc.

3.3.2 Joint Information Exchange Requirement (JIER)

JIERs identify **who** exchanges **what** information with **whom**, **why** the information is necessary, and **how** the information exchange must occur. Top-level information exchange requirements (IERs) identify warfighter information used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint or combined mission. JIERs between Services may necessitate lateral links. Additionally, Service-specific IERs of Mobile Users may also generate a need for LLCs.

This page intentionally left blank.

CHAPTER 4: PLANNING

4.1 Introduction

JMNO tactics, techniques, and procedures (TTP) can be used to conduct either deliberate or ad-hoc planning, depending on the level at which the planning takes place. JMNO Lateral Link Connections (LLCs) are versatile, and can be driven from the top down, or from the bottom up.

4.2 Deliberate Planning

JMNO TTP can be used for deliberate planning of joint tactical lateral links by the Joint Task Force (JTF) staff, which is usually a "top down" approach. However, this document does not attempt to modify the planning processes in place at the JTF staff level. Instead, the TTP are intended to support this work by specifying those planning considerations unique to JMNO Lateral Links, and by providing planning tools in the form of decision matrices and flow charts, which can be used for visual reference. Ideally, the deliberate planning process will result in the J6 planners designating Lateral Link Nodes (LLNs) and, if necessary, Multi-link Distribution Nodes (MDNs) before the start of an exercise or operation. By performing the planning for lateral links beforehand, many decisions, such as which units will be standing up LLCs, and which communications assets will be redeployed, will then already be made. The J6 may also issue "be prepared to" guidance to units who may be tasked with establishing an LLC based on mission requirements. If, during the execution of the exercise or operation, the J6 identifies a requirement for an LLC, then he or she will know that those units are prepared to establish this connection.

Service components within a typical JTF have robust command, control, communications and computers (C4) infrastructures that support vertical communications within their Services. Joint Publication 6-0, "Joint Communications System" provides clear guidance on how Service or functional components within a JTF are to plan for hierarchical connections to the JTF and Defense Information Systems Network (DISN). The publication also addresses the need for inter-Service or joint communications at the component level. However, there is currently no doctrinal information on when, why, or how lateral links between tactical units should be established; JMNO TTP fulfill this need.

According to joint doctrine, all links are needs-driven, and are only implemented as such requirements at the tactical level are identified. During deliberate planning, the J6 staff use the Operations Order and Commander's Intent to conduct a mission analysis, which usually allows the planners to anticipate these requirements across the force. This mission analysis helps to identify any joint information exchange requirements (JIERs) between tactical units (such as Predator live video feed). Mission analysis might also identify the need for tactical mobile user support (JMNO Issue 2) during mission execution. For each requirement identified, planners must determine if a lateral link between tactical units of one or more Service is the best way to support this requirement. Factors to consider during planning include bandwidth requirements, transmission equipment availability, and time sensitivity.

One of the benefits of implementing JMNO lateral links is that they reduce latency between command and control (C2) nodes by "keeping tactical traffic local." However, the potential drawback to establishing these links is the transmission equipment used. Many of the transmission systems in use at the tactical level are Service-specific and not interoperable with other Services' similar equipment; thus, temporarily realigning these transmission systems may be the only way to establish lateral links. Because of the time and effort involved in realignment, C4 planners must evaluate the priority of a requirement and its importance to the overall mission. If the priority of a JIER is sufficient, for example, the planner can then conduct an equipment trade-off analysis. The following are some of the questions that can be answered at the J6 level during the equipment trade-off analysis:

- If adjacent units have interoperable communications equipment, is that equipment being used for a connection to higher headquarters or the DISN? If so, can the equipment be temporarily used for an LLC?
- Can one of the units involved in an LLC temporarily loan equipment and personnel to provide the transmission component of the link?
- Can higher headquarters spare communications assets to support an LLC at a lower unit?

If equipment will be available, then the units can move forward with planning for LLCs. The following table outlines the traditional command relationships and standard procedures for responsibility of communications between units.

Table 4-1 Decision Matrix for Communications Support for JMNO Lateral Links

Provider	To	Recipient	Rationale
Left	➔	Right	Best choice-this keeps the decision between peer units
Higher	➔	Lower	Upper echelons tend to have more gear
Supporting	➔	Supported	Usually designated in the Operations Order to support the Commander's Intent
Reinforcing	➔	Reinforced	Usually designated in the Operations Order to support the Commander's Intent

As shown above, tactics involved with JMNO TTP are focused on three important factors to consider in choosing to implement JMNO LLCs:

- Determining requirements that are best met by implementing LLCs
- Conducting LLC Equipment Analysis to determine immediate feasibility
- Completing an LLC Equipment Trade-Off Analysis to decide if the benefits of implementing LLCs outweigh the equipment redeployment costs

Figure 4-1 depicts a JMNO Lateral Link Connection Decision Support Flow Chart. The following paragraphs will walk the reader through each decision-making process, including the information necessary to make these decisions.

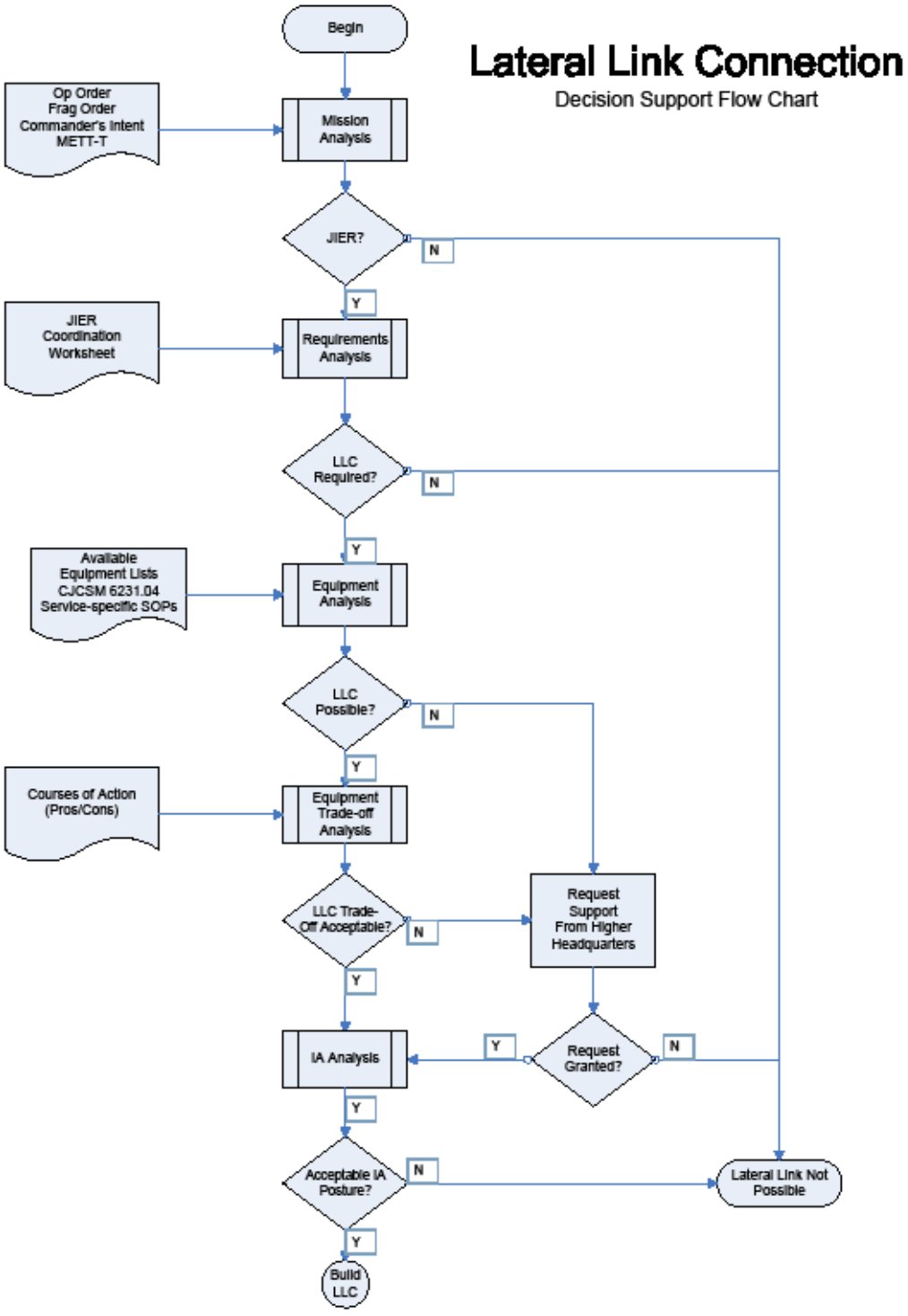


Figure 4-1 JMNO Lateral Link Connection (LLC) Decision Support Flow Chart

4.2.1 Mission Analysis

For the purposes of JMNO, performing a mission analysis serves to identify requirements which are best satisfied by establishing LLCs. Joint Information Exchange Requirements (JIERs) are a primary driver for such needs.

> "IERs identify **who** exchanges **what** information with **whom**, **why** the information is necessary, and **how** the information exchange must occur. Top-level IERs identify warfighter information used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint or combined mission.
> *Excerpt from Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6212.01B, 8 May 2000*

Another driver for implementing JMNO LLCs is the tactical Mobile User described in 0. Such users may have JIERs in their own right, or may simply have IERs with their parent Service that are best met through the use of JMNO LLCs. Careful mission analysis should clearly identify such requirements that call for an LLC.

Each Service component already has staff planning processes for both deliberate planning and crisis action planning (CAP). All planning starts with the order—whether it is a pre-planned exercise order, a recently-developed Operations Order, or even a Fragmentary (FRAG) order issued after commencement of an exercise or operation—the order drives the requirements. C4 planners at every echelon are quite familiar with mission analysis, and the normal output of all planning efforts is the Annex K. This annex addresses C4-specific tasks and information critical to the LLC decision making process, including:

- Commander's Intent (specifically in the area of C4 support)
- Concept of Operations (CONOPS)
- Mission, Enemy, Terrain & Weather, Troops and Fire Support, and Time (METT-T)
- C4 Logistics
- Command and Signal

Note that the "Troops" portion of METT-T within the Annex K addresses higher echelons of C4 providers, adjacent forces (including joint or coalition forces), and any attachments or detachments available to the C4 planner. This section may also identify Mobile Users of one Service who will be operating in or near another Service's area of responsibility (AOR) and may drive establishment of an LLC. Additionally, Annex U, the Information Management Plan within an Operations Order, is also very helpful in visualizing C2 JIERs between tactical units, or reporting requirements for Mobile Users that would be facilitated or improved by using an LLC.

Primary customers of the C4 planner are the Information Management Officer (IMO), C2 Systems Officer, Force Fires Officer, and similar billets within a Service component. Functions of such officers include Common Tactical Picture (CTP) Architecture, Fire Support Systems communications, and all other C2 systems that use the Internet Protocol (IP) as their primary means of information exchange. These customers, and their respective

C2 systems, will contribute to the identification of JIERs or Mobile User requirements. C2 Systems with the potential to affect tactical JIERs include:

- Command & Control Personal Computer (C2PC)
- Force XXI Battle Command, Brigade and Below (FBCB2)
- Advanced Field Artillery Tactical Data System (AFATDS)
- Advanced Deep Operations Control System (ADOCS)
- Theater Core Battle Management Systems (TBMCS)

The Department of Defense Architecture Framework (DoDAF) is another resource for C4 planners to use in identifying JIERs and IERs. DoDAF artifacts include Operational Views (OVs) and Systems Views (SVs). The OV-2 and OV-3 identify nodes, units, or functions, and the information exchange needlines between them. The SV-6 shows the systems (including the networks) used to fulfill these requirements. If the C4 planner has such artifacts for tactical units within the JTF, a comparison of OVs and SVs can identify JIERs that would benefit from JMNO LLCs. If a needline for IP-based traffic (including e-mail, file transfer, Defense Message System, or web access) exists between joint tactical units on the OVs, but is being met (according to the SV) via doctrinal communications paths traversing the JTF or DISN, this requirement becomes a candidate for use of an LLC.

Battlefield intelligence also drives JIERs. Annex B of the Operations Order is the Intelligence Annex, and includes key appendices such as "Priority Intelligence Requirements," "Imagery Intelligence," and "Intelligence Products." Because high resolution imagery and other intelligence products are usually very large files, they are prime examples of tactical JIERs that would best be met using JMNO LLCs. Such requirements may be met by file transfer, or access to a tactical web server. A live video feed from an Unmanned Aerial Vehicle (UAV) is another example of IP-based traffic best served using an LLC. An example of a key intelligence system used at the tactical level is the All Source Analysis System-Light (ASAS-L). Any or all of these products of intelligence systems or services might contribute to a tactical JIER or Mobile User need that would benefit from an LLC.

4.2.2 Information Exchange Requirements Analysis

The next step in the decision-making process for LLCs is to clearly define the technical attributes of the requirements. Once the technical attributes are defined, C4 planners must analyze each one to determine whether it is best fulfilled with an LLC. Then, the planners must analyze the overall C4 needlines between tactical units to accurately scope this need and determine how it affects the equipment analysis.

> The quality (that is, frequency, timeliness, security) and quantity (that is, volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included in the information exchange requirement.
> *Excerpt from Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6212.01B, 8 May 2000*

Because JMNO LLCs are focused on supporting IP connectivity between tactical units, the first discriminator for a candidate requirement is, "can this JIER/Mobile User IER be met with an IP-based C2 system?" If the information is digital, chances are that it is IP-based. In fact, both voice and video are also increasingly using IP connections rather than dedicated circuits or trunk groups. Thus, these systems are also candidates for forming LLCs.

The second discriminator is the classification level of the information being exchanged. While JMNO TTP are extensible, they currently are built to support Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) LLCs only. Higher classification (such as, Joint Worldwide Intelligence Communications System [JWICS]), coalition, other government agency (OGA), and non-government agency (NGO) JIERs would need additional information assurance (IA) controls (see **Annex A: Information Assurance**).

The next portion of the requirements analysis includes decisions that will be made by the tactical commander (with advice from the G6/S6 staff). These decisions will be based on factors such as:

- **Bandwidth Required** – If only a small amount of bandwidth is required, the tactical unit's normal, hierarchical network connection may support the requirement.
- **Bandwidth Available** – Even if an application has a large bandwidth requirement, the units with the JIER may have sufficient connectivity to support, which would negate the need for an LLC.
- **Desired/Required Timeframe** – If an IER is not time-sensitive, it may be best satisfied via normal network connectivity. However, if it is time-sensitive, a JMNO LLC may reduce latency and better meet the requirement.
- **JIER Priority** – A requirement's priority to a commander is a critical decision, and will likely determine whether to establish an LLC. If reconfiguration of organic communications assets is required, the priority of the requirement (JIER or Mobile User) is also taken into account during the equipment analysis, as it affects the prioritization of existing connections.

Finally, technical analysis of the requirement must be done to support router and (potentially) transmission system configurations. For example, the following data must be available so that appropriate router access control list (ACL) entries can be made by the network administrators at both ends of the LLC:

- Ports and Protocols necessary (does the C2 application use specific ports and/or protocols that are normally blocked by firewalls?)
- Source IP network, subnet mask, and default gateway (for ACL setup and troubleshooting)
- Destination IP network, subnet mask, and default gateway (for ACL setup and troubleshooting)

Figure 4-2 is an example of a JIER Coordination Worksheet that can be used by tactical C4 planners to support the decision-making process. The bottom line of the requirements analysis portion of the TTP is, "Will this requirement best be satisfied with an LLC, or with a traditional

hierarchical path?" Use of this worksheet will assist in both the requirements and the equipment analyses.

Information Exchange Requirements (IER) Analysis Worksheet

(See reverse for detailed instructions)

IER Pre-qualifications for JMNO LLC	
1. Classification/Network: ☐ Secret (SIPRNET) ☐ Sensitive but Unclassified (NIPRNET)	
2. Media/Format: ☐ E-Mail ☐ File Transfer ☐ DMS ☐ Web ☐ Public Folder ☐ IP-based Video ☐ Other IP	
IER Operational Characteristics	
3. Information Description	
3a. Name/Identifier	
3b. Description	
4. Information Attributes	
4a. Size	4b. Criticality
4c. Bandwidth required	4d. Timeliness
4e. Frequency	4f. Trigger event
5. Information Source	
6. Information Destination	
IER Systems Characteristics	
7a. Sending System Name	7b. Receiving System Name
7c. Ports used	7d. Protocols Used

Figure 4-2 Sample Requirements Coordination Worksheet

4.2.3 Equipment Analysis

When a requirements analysis shows that a lateral link is necessary to optimally satisfy one or more Joint or Mobile User IERs, the C4 planners of the involved units need to conduct an equipment analysis to determine the feasibility of establishing this link using organic equipment. At a high level, the questions that must be answered include:

- What are the transmission paths or options available to use?
- What is the multiplexing equipment required?
- What are the cryptographic items needed to safeguard the information traversing the link?
- What are the router requirements to establish this LLC?

The following paragraphs take a deeper look at each of these topics.

4.2.3.1 Transmission Paths

Each tactical unit has a Table of Equipment (T/E), Equipment Density List (EDL), or some other document that lists the available transmission equipment for that unit. Such transmission equipment falls into the following categories:

- Satellite communications (Satcom)
- Terrestrial links (digital microwave, UHF Multichannel, WiMAX, Free Space Optics (FSO), etc.)
- Tactical landline (tactical fiber optic cable, CDI/PCM coax cable, WF-16 four-wire, etc.)

Additionally, tactical units may occasionally leverage commercial or leased lines from a host nation. However, given the mobile aspect of JMNO TTP, this is not a realistic option.

The Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6231 series of documents provides planning guidance for Joint Tactical Communications. CJCSM 6231.04, "Joint Transmission Systems" provides specific information concerning equipment capabilities and interoperability for the major tactical communications equipment available to the Services. Each Service also uses Standard Operating Procedures (SOP) developed for their specific needs; these SOPs contain additional information about Service-specific implementation of such equipment, and may contain information about transmission systems not currently included in the CJCSM reference (such as SWAN and JNN). Therefore, each unit's specific set of SOPs can then be used together with the CJCSM 6231.04 during planning to determine if the units have interoperable communications equipment.

If no interoperability options exist, but the supporting unit has available assets to send to the supported unit, then the units can consider implementing this arrangement. If no such equipment is available, the unit planners can petition higher headquarters (HHQ) for the appropriate equipment. As the equipment analysis will have determined the minimum specifications for the equipment, the decision process should be easier for HHQ. Depending on the level of HHQ, they may be able to request transmission support from other in-theater agencies such as the Joint Communications Support Element (JCSE). If that request is denied, then the lateral link is likely not possible. However, if the

equipment requirement is fulfilled, planners need to continue to move through the equipment analysis, which continues below.

4.2.3.2 Multiplexing equipment

Promina multiplexers are the primary multiplexing devices in use by U.S. Military tactical forces. The Promina 800 and Promina 400 are the predominant series in use by tactical and operational units. The Army Joint Network Node (JNN), Marine Corps Transition Switch Module (TSM), Marine Corps Digital Technical Control (DTC), Air Force Theater Deployable Communications (TDC), and the Navy's Advanced Digital Network Server (ADNS) all employ Promina devices for multiplexing.

Planning information necessary for units to make connections using Promina devices include:

- Domain and Node number
- Card and Port Assignment
- Bandwidth
- Answer mode
- Path information (such as, domain and node info for each Promina in the path. For JMNO LLCs this should not be a factor, as they would be point-to-point)

4.2.3.3 Cryptographic Equipment

Appendix 2 of Annex K, the Communications Plan of an Operations Order, addresses communications security and includes information concerning the Cryptographic equipment (Crypto) necessary for operations. Note that C4 planners may face unusual circumstances when planning JMNO LLCs (such as, using a differing keymat or use of router-based AES256 encryption for transmission security).

4.2.3.4 Routers

Currently, most routers in use at the tactical level are Cisco products. However, even within the Cisco family, there is a wide variety of router composition, including: number of ports, amount of random access memory (RAM), Internetworking Operating System (IOS) version, hardware modules, etc. The next step of the equipment analysis process is to determine if the specific units attempting to establish an LLC can support the link with resident routing equipment. The following are considerations for evaluating such equipment for suitability:

- Is there a router available with an open or available port (serial or Ethernet)?
- If multiple routing processes are to be running on the LLC router, does it have sufficient RAM to do support them?
- Does each end of the LLC have routers with the proper IOS version, RAM, or hardware modules available to support router-based encryption?
- Does each end of the LLC have routers with the proper IOS version, RAM, or hardware modules available to support Virtual Private Dialup Networking (VPDN)?

If a unit cannot come up with the necessary router, that unit should petition its HHQ for the appropriate equipment. The equipment analysis will have determined the minimum specs for such equipment, so the decision process is straightforward for HHQ as well.

4.2.3.5 Equipment Analysis Summary

If the tactical C4 planners used the JMNO Lateral Link Connection decision support flowchart and have determined that a lateral link is possible, then the planners need to move to the Equipment Trade-off Analysis to ensure that use of such equipment will not preempt or otherwise negatively affect a higher-priority mission. If all equipment on both ends of the link is currently available, or if additional equipment has been provided by HHQ, this decision should be evident. If not, the following section provides specific ideas to guide the planners' thought processes.

4.2.4 Equipment Trade-off Analysis

Once the planners have determined that an LLC would prove valuable, they must determine if the link is worth the time and effort to implement. If the LLC is directed by higher headquarters, there is minimal decision-making in this process. The only decision might be, "how soon can we realign assets?" However, if the decision is with the local commander, then he or she will be provided with all pertinent information from his or her G6/S6 C4 planner to decide whether the LLC is important enough to establish.

4.2.5 Information Assurance Analysis

Due to the complexity of Information Assurance (IA), **Annex A: Information Assurance**, is entirely devoted to LLC IA planning and analysis. The JMNO IA TTP are a sensible application of existing IA principles to manage the risk of conducting lateral link operations.

The following is an outline of **Annex A: Information Assurance**:

- Document POC Information
- Document System Information
- Document Shared JIER Traffic
- Document Pass-through JIER Traffic
- Evaluate Cross Domain Flow Chart
- Evaluate Cross MAC Flow Chart
- Establish/Improve Mutual Trust (leading to decision whether to approve the link)
- Establish Tunnel Encryption Keys

NOTE: JMNO TTP are designed for use between networks of the same classification level, so Sections 5 and 6 of **Annex A: Information Assurance** are not applicable to such efforts. However, this section is included in the event Services find themselves needing to establish a Cross-Domain or Cross Mission Assurance Category (MAC) network connection. These sections have not been tested, but are the result of many hours of research and analysis by IA experts from the Naval Postgraduate School (NPS).

4.2.6 Quality of Service Analysis

Quality of service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority to specific traffic, including dedicated bandwidth. Other goals of QoS are controlled jitter, reduced latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important to QoS is ensuring that providing priority for one or more data packets does not make others fail.

QoS is only necessary for bandwidth constrained links. To determine if QoS is needed for an LLC the C4 planner must calculate the bandwidth requirement of each planned Joint or Mobile User IER and compare it to the available bandwidth of the LLC. Depending upon the bandwidth of the lateral link, planners may need to use QoS techniques to manage the IP data across the link. More detailed information on implementing QoS is available in Appendix 6 of **Annex A: Information Assurance**. Note that proper QoS requires manipulation of network traffic with robust network management implemented. Recommendation: Avoid the requirement for QoS techniques by planning for sufficient LLC bandwidth to support the identified requirements.

4.2.7 Deliberate Planning Summary

Each of the previous planning steps results in identification of specific equipment that is to be used to establish a lateral link. The following Lateral Link Configuration Worksheet (see Figure 4-3) should be completed after the decision is made to establish the lateral link. This worksheet will aid in establishing, maintaining, and troubleshooting the LLC, and each LLN should have a copy.

Lateral Link Worksheet

(See reverse for detailed instructions)

Participating Lateral Link Node Information	
1. Primary Contact Name	2. Telephone Number/Email
3. Secondary Contact Name	4. Telephone Number/Email
5. Unit	6. Target Implementation Date

Lateral Link Node 1	Equipment	Lateral Link Node 2
	Transmission	
	TransSec	
	IP Modem	
	ComSec	
D N C P	Multiplexer (MUX)	D N C P
BW Call/Answer	MUX Settings	BW Call/Answer
	Switch	
	Router	
	Interface	

Figure 4-3 Lateral Link Configuration Worksheet

4.3 Multi-Link Distribution Node (MDN) Planning

The preceding sections discussed the planning necessary to establish lateral link connections between two Service's tactical units. However, during mission analysis it may become evident that a Service has a need to establish lateral links with two (or more) other Service's units. The

JMNO concept of the MDN is just that—a Lateral Link Node (LLN) that establishes LLCs with two or more Services, thereby becoming a "bridge" between tactical IP networks of those other Services. JMNO TTP contain specific instructions on the how to establish an MDN and configure the MDN's router to do just that.

It is conceivable that such a node would only need to send and receive data from each Service's respective LLN, and not pass one Service's IP traffic to the other Service's network. Such a node would more properly be referred to as a "Multi-link Node" as it isn't "distributing" anything. However, the JMNO "Purple Zone" or Tactical Joint Network can only be realized by having one or more Services establishing MDNs to not only support identified Joint and Mobile User IERs, but also to provide much-needed redundant communications paths in a joint area of operations.

It is also conceivable that an MDN may be established for the primary purpose of acting as a gateway between two Services' tactical IP networks. A specific example that comes to mind is that of a Navy amphibious ship bringing a Marine Expeditionary Unit into an area of operations already established by the Army. Navy ships have USC-38 MILSTAR assets, and the Army has SMART-T. The Marines use the Marine Air Ground Task Force (MAGTF) Router on such ships, and this router is connected to the Navy's Advanced Digital Network Server (ADNS) router in what equates to a JMNO LLC. The Navy could establish an LLC from ship to shore over the MILSTAR link using JMNO TTP, and thus allow the Marine network on ship to communicate directly with the Army network on shore, to conduct mission analysis and planning.

If a Service is tasked to become an MDN for allowing IP traffic to pass between the distant ends of two of its LLCs, then the MDN router needs to be configured to correctly route tactical traffic between those Services' networks. Access Control Lists (ACLs) for incoming and outbound IP networks on one interface will need to be mirrored for outbound and incoming traffic on the other interface, and vice versa.

0details the specific configuration changes necessary for an LLN to act as an MDN between two other LLNs. The JMNO MDN Cutsheet, Figure 5-8, should be used to document the results of MDN planning. In addition to the planning considerations shown above, MDN planning must include which tactical IP networks will be allowed to pass through the MDN to reach destinations at other, non-directly-connected tactical Service networks.

4.4 Ad-Hoc Planning

JMNO TTP can also be used for ad-hoc planning between tactical units during the execution of an exercise or operation, which can be considered the "Bottom Up" approach. Such planning is, by definition, time-sensitive. Therefore, this document includes an "Ad-Hoc" planning section that helps C4 planners at this level execute rapid planning using portions of the JMNO TTP deliberate planning process.

Using JMNO TTP, tactical C4 planners will have the tools to address unanticipated C4 challenges. JMNO Lateral Links can be used to restore IP connectivity or provide IP network redundancy with minimum coordination time. C4 planners can use these tools to assist in

establishing LLCs in support of critical JIERs and to improve or enhance situational awareness between tactical units.

4.5 Direct Liaison Authority (DIRLAUTH)

To ensure that JMNO LLCs are an available option for tactical C4 planners, the JTF J6 needs to provide direct liaison authority (DIRLAUTH) for these planners before the beginning of an exercise or operation. This authority enables LLC decision making down to the tactical level without complicating the process or compromising the IA posture of either Service involved.

4.6 Additional Network Management Responsibility

After commencement of an exercise or operation, it is common for tactical C4 planners to realize that a JIER at their level could best be satisfied with a JMNO LLC. Once the decision has been made to establish an LLC at the tactical level, and the LLC has been planned and established, this information must be provided to the JTF J6 for visibility and situational awareness of the tactical C4 network. This reporting requirement serves several purposes:

- It ensures the J6 has a complete overall picture of the C4 network in theater
- It provides the J6 with C4 redundancy in case a unit's primary path becomes unavailable
- It gives the J6 insight into why he or she might see network traffic changes (that is, more traffic over the lateral link means less over the component-to-JTF link).

To shorten the deliberate planning cycle discussed previously, tactical C4 planners can use the Lateral Link Configuration Worksheet (Figure 4-3), along with the Lateral Link Cutsheet (Figure 5-7) and (if necessary) the Mobile User Cutsheet (Figure 5-15). These worksheets and cutsheets are tools used for both planning and implementation. The use of these tools presupposes that the decision has been made to establish a lateral link at the tactical level, and that planners from both ends of the LLC have done an initial estimate of supportability for the link. Completion of the LLC Worksheet will ensure that all devices in the transmission path have been evaluated for interoperability. Completion of the Lateral Link Cutsheet ensures that both planners and operators have POC information and specific device configuration information necessary to establish, maintain, and troubleshoot the LLC. Finally, if this LLC is envisioned to support mobile users from either or both Services, then the Mobile User Cutsheet ensures these users will be able to connect to the host network and thence to the home network.

CHAPTER 5: EXECUTION

5.1 Introduction

This chapter deals with the "How To" portion of JMNO Tactics, Techniques, and Procedures (TTP). By this point, the decision has been made to establish a lateral link between two Services. However, planners still need to make a few important decisions, specifically concerning device configurations. The most complex aspect of this planning involves the routers, but it includes other factors as well, such as Information Assurance (IA) and multiplexing devices.

5.2 Router Configurations

JMNO TTP router configurations are presented in levels of increasing complexity, from simple point-to-point lateral links between two Services using static routing to dynamic routing among three or four Services with a Multi-link Distribution Node (MDN). This publication addresses two types of IP Routing: Static and Dynamic. Static links between two Services are easily configured and do not require processing to be performed on the router CPU. Dynamic links are useful in a constantly changing architecture and allow the routers to adapt to changes in the architecture. Dynamic routing offers several options for operators, including redistribution of routes between different routing protocols and the use of a single routing protocol within the tactical joint network (JMNO Purple Zone).

Operators will develop and complete router configurations for the lateral links using the router configuration cutsheet to do the following:

- Establish an IP addressing scheme for endpoints of the lateral link connection (LLC)
- Negotiate routing protocol(s) to be used
- Determine networks that will have access to the lateral link
- Configure the border router of the Service's tactical network as the entry point of the lateral link
- Configure the border router of the Service's tactical network for mobile users
- Implement the policy for security configuration of the routers and similar capabilities regarding configuration control and management as prescribed in **Annex A: Information Assurance**

Representative entries for the router configurations found in this publication may be used as templates to enable the LLC. IP addresses and description lines of the interfaces are examples only. Actual entries will vary according to the mission and current policies.

5.2.1 IP Addressing on the Lateral Link

Several options are available for IP addresses on lateral link ports. This publication describes the following:

- Unnumbered IP interfaces
- Shared IP subnet
- Private IP addressing

5.2.2 Unnumbered IP Interfaces

The **ip unnumbered** configuration command enables IP processing on a serial interface without assigning it an explicit IP address. The **ip unnumbered** interface "borrows" the IP address of another interface already configured on the router. Based on research by JMNO engineers, the unnumbered IP interface configuration command is the preferred configuration method because the command conserves network and address space. It is recommended that the unnumbered interface point to a loopback interface, as loopbacks do not fail unless the router fails.

Figure 5-1 illustrates a lateral link between the Army and Marine Corps, followed by router configurations with unnumbered interfaces pointing to already configured loopback interfaces. Even though the two loopback IPs are not on the same subnet, this logic will still provide point-to-point connectivity between these routers.

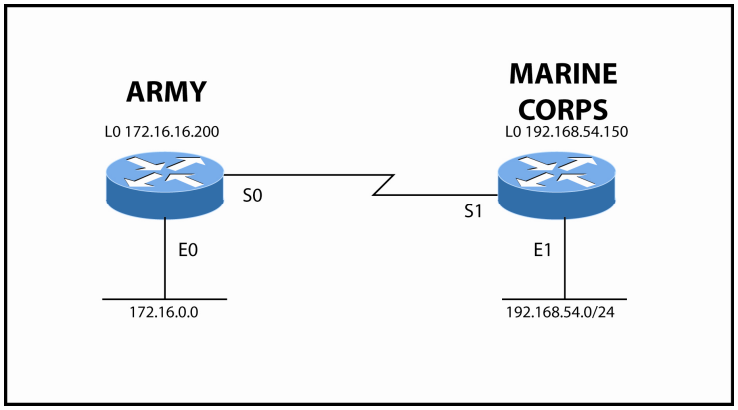


Figure 5-1: Example of Unnumbered Interfaces

The following commands can be used to configure a router to use unnumbered IP interfaces:

```
Army(config)# interface Loopback 0
Army(config-if)#ip address 172.16.16.200 255.255.255.255
Army(config)# interface Serial 0
Army(config-if)# ip unnumbered Loopback0

MarineCorps(config)# interface Loopback 0
MarineCorps(config-if)#ip address 192.168.54.150 255.255.255.255
MarineCorps(config)# interface Serial 0
MarineCorps(config-if)# ip unnumbered Loopback0
```

5.2.3 Shared IP Subnet

With the shared IP subnet approach, during the planning process, one Service determines the availability of a /30 subnet for the point-to-point link and advises the adjacent Service of the address to be used.

5.2.4 Private IP addressing

Planners and operators can standardize addressing by using private IP addressing on the lateral link, assigning specific subnets to each Service. The supporting Service in a point-to-point link or the Service providing the MDN determines the addresses to be used.

Table 5-1: Private Address Assignment

Service	Private address subnet
Army	10.10.x.x.
Marine Corps	10.20.x.x
Navy	10.30.x.x
Air Force	10.40.x.x
Spares	10.50.x.x. to 10.250.x.x.

Figure 5-2 illustrates an Army/Marine Corps link using private addressing. The Army, as the supporting Service (and potentially an MDN), determines the addresses used.

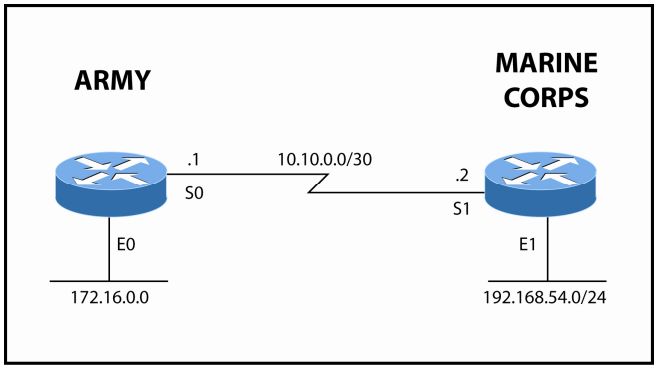


Figure 5-2 Private IP Addressing

5.2.5 Point-to-point Static Routing between two Services

When planning for static routing between two Services, operators and planners should determine which internal networks will use the lateral link. Additionally, they should set up access control lists (ACLs) to permit specified internal networks and the ports and protocols required by joint information exchange requirements (JIERs).

To configure a static route to a specific destination network on a point-to-point link between two Services, operators can use either of two commands: specifying the outgoing interface or specifying the next-hop IP address of the adjacent router. Either command will install a static route to the destination network in the routing table.

Using Figure 5-2 as a reference, consider the following example of a static routing entry using the outgoing interface on the Army router pointing to the Marine Corps 192.168.54.0 internal network as the destination. Note that specifying the outgoing interface is the only acceptable method to use if the Services are using **ip unnumbered** interfaces on the lateral link.

```
Army (config)# ip route  192.168.54.0   255.255.255.0   Serial0
```

The following example shows the same static route using the next-hop IP address:

```
Army (config)# ip route 192.168.54.0   255.255.255.0   10.10.0.2
```

NOTE: When using static routing for JMNO LLCs, remove any **redistribute static** commands on the router, as these commands can cause routing loops in the tactical network architecture. If the **redistribute static** command is critical to the current network configuration, do not use static routing.

Services using the lateral link may provide a basic level of security on JMNO LLN routers by creating access control lists (ACLs) to permit or deny access to specific routes and ports. Refer to **Annex A: Information Assurance** for further discussion of ACLs, along with implementation instructions.

5.2.6 Point-to-Point Dynamic Routing between two Services

When there is a probability that the LLC will migrate into a Purple Zone containing three or four Services, operators should use dynamic routing. Options for establishing dynamic routing include:

- Use of external Border Gateway Protocol (eBGP)[1] as an exterior gateway protocol
- Creation of an new autonomous system on border routers with Enhanced Interior Gateway Routing Protocol (EIGRP) running on JMNO LLN routers

The decision matrix for selection of a routing protocol is shown in Table 5-2. As a rule, Services implementing LLCs should use BGP as the routing protocol.

Table 5-2 Routing Protocol Decision Matrix

Method	Routing Protocol	Advantages	Disadvantages
Static	None	No router resources; prevents undesirable routing between networks	Cannot adapt to changes in network
Dynamic	BGP-4	Robustness; low overhead	Configuration less well-known
Dynamic	EIGRP	Ease of configuration; rapid convergence; low overhead; used by USMC and USAF	Cisco-centric

5.2.7 Dynamic Routing Using BGP

Services participating in the Purple Zone may use BGP in conjunction with the Interior Gateway Protocol (IGP) already running on their respective border routers. Each participating Service will assign a BGP autonomous system (AS) number from Table 5-3. (The assignment of private AS numbers in the table is based on the Internet Assigned

[1] BGP running between routers that belong to different autonomous systems is called exterior BGP (eBGP). BGP running between two routers in the same autonomous system is called internal BGP (iBGP). iBGP is not recommended for lateral link connections. BGP in this document refers to eBGP.

Numbers Authority (IANA) block of AS numbers reserved for private use, 64512 through 65535, as specified in RFC 1930 Section 10.)

Table 5-3 Private Autonomous System Number Assignments

Service	Private AS Number
Army	65010 to 65019
Marine Corps	65020 to 65029
Navy	65030 to 65039
Air Force	65040 to 65049
Spares	65050 to 65535

5.2.7.1 Configuring BGP

As depicted in Figure 5-3, create a BGP routing process and assign an AS number. The AS number is passed along to identify the router to BGP routers in another autonomous system.

```
MarineCorps(config)#router bgp 65020
```

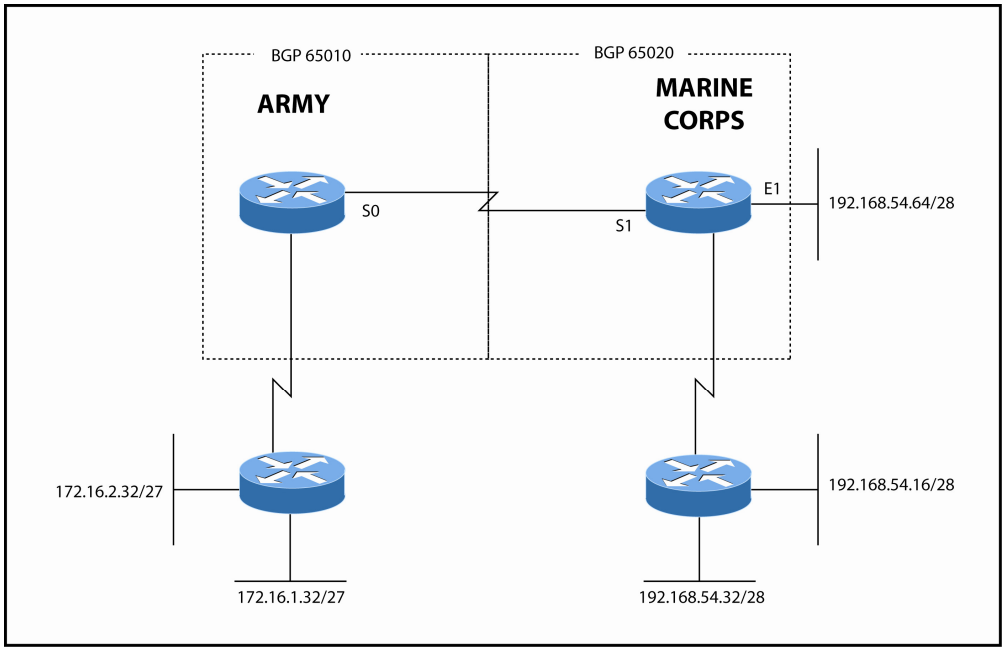


Figure 5-3 BGP Routing Process

The command **no synchronization** allows the IGP to carry fewer routes and allows BGP to converge more quickly. The **bgp log-neighbor-changes** command generates log messages when the status of a BGP neighbor changes (such as when it resets, comes up, or goes down).

```
MarineCorps(config-router)#no synchronization
MarineCorps(config-router)#bgp log-neighbor-changes
```

Create explicit network statements for all networks and subnets that will use the lateral link, including those networks and subnets that are not directly connected, but will use the lateral link. Use of these statements prevents redistribution of the IGP into BGP, as redistributing an IGP into BGP can cause routing problems. All Services participating in the Purple Zone must be consistent in the use of specific subnets vice summarized networks in the network statements.

NOTE: The mask will not appear in the configuration file for classful networks.

```
MarineCorps(config-router)#network 192.168.54.16 255.255.255.240
MarineCorps(config-router)#network 192.168.54.32 255.255.255.240
MarineCorps(config-router)#network 192.168.54.64 255.255.255.240
```

Use **no auto-summary** command if subnets are discontiguous. Use the **redistribute connected** command for routing of mobile user(s).

```
MarineCorps(config-router)#no auto-summary
MarineCorps(config-router)#redistribute connected
```

Specify a neighboring BGP peer. This BGP peer is identified to the specified autonomous system.

```
MarineCorps(config-router)#neighbor 10.1.0.5 remote-as 65040
```

For the Service operating as the MDN as illustrated in Figure 5-4, specify both lateral link networks as well as neighboring BGP peers.

```
AirForce(config-router)#network 10.40.0.0 mask 255.255.255.252
AirForce(config-router)#network 10.40.0.4 mask 255.255.255.252
AirForce(config-router)#neighbor 10.40.0.2 remote-as 65010
AirForce(config-router)#neighbor 10.40.0.6 remote-as 65020
```

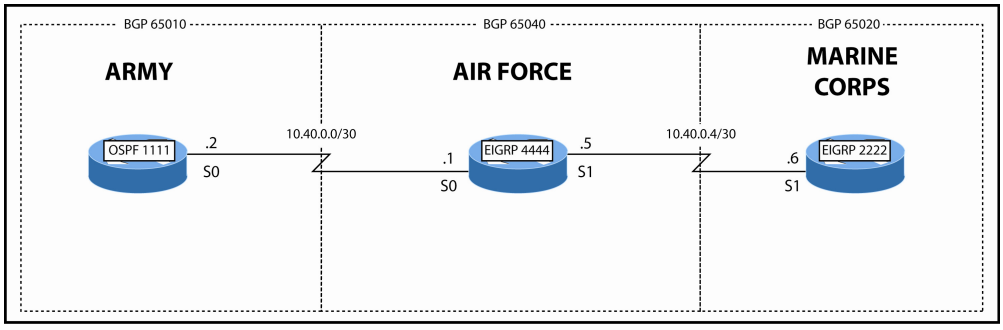


Figure 5-4 Air Force Operating as an MDN

5.2.7.2 Verifying BGP

The following commands may be used to verify that BGP configurations are working properly.

To display entries in the BGP routing table, use the **show ip bgp** EXEC command.

```
Army# show ip bgp

BGP table version is 5, local router ID is 10.40.0.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop      Metric LocPrf Weight Path
*> 10.40.0.0/30     10.40.0.1        0      0   65040
*> 10.40.0.4/30     10.40.0.1        0      0    65040
*> 172.16.1.32/27   0.0.0.0          0      0    i
*> 172.16.2.32/27   0.0.0.0                 0     i
*> 172.28.1.0 28    10.40.0.1       59      0   65040
*> 198.168.54.16/28 10.40.0.1       74      0   65040 65020
*> 198.168.54.32/28 10.40.0.1       74      0   65040 65020
*> 198.168.54.16/28 10.40.0.1       74      0   65040 6502
```

Use the **show ip bgp neighbors** command to display information about the TCP and Border Gateway Protocol (BGP) connections and verify if the BGP peer is established. The output of the show **ip bgp neighbors** command below shows the BGP state as 'Established', which indicates that the BGP peer relationship has been established successfully. The **show ip bgp neighbors** command has been used with the modifier **|** ***include BGP***. This makes the output more readable by filtering the command output and displaying the relevant parts only.

```
Army# show ip bgp neighbors | include BGP

BGP neighbor is 10.40.0.1, remote AS 65040, external link
  BGP version 4, remote router ID 10.40.0.1
  BGP state = Established, up for 00:00:17
  BGP table version 1, neighbor version 1
```

In addition, the show **ip bgp summary** command can also be used to display the status of all BGP connections, as shown below.

```
Router# show ip bgp summary

BGP router identifier 10.10.10.1, local AS number 300
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down        State/PfxRcd
10.40.0.1       4   65040   3     3     1    0   0 00:00:26      0
```

5.2.8 Dynamic routing using EIGRP

A second option for routing on the lateral link is the creation of an EIGRP autonomous system unique to and shared by the border routers of the Services in the Purple Zone. EIGRP is suited for many different topologies and media. In a well-designed network, it scales well and provides extremely quick convergence times with minimal network traffic.

Planning for dynamic routing using EIGRP requires the following:

1) **Assignment of the EIGRP Autonomous System (AS) number:** Assign an AS number for the tactical joint network Purple Zone. Unless defined otherwise by the JTF J6, the supporting Service or the MDN provider will also determine the AS number of the EIGRP routing protocol. This AS number should be different from any other AS numbers used by the participating Services.
2) **Determination of networks using the lateral link:** For each router in the network, specify which of those networks that will use the lateral link using "distribute list" statements.
3) **Determination of the bandwidth of the lateral link**: When configuring serial links using EIGRP, it is important to configure the bandwidth setting on the interface. If the bandwidth for these interfaces is not changed, EIGRP assumes the default bandwidth on the link instead of the true bandwidth. If the link is slower, the router may not be able to converge, update routing tables, or select the most optimal path.
4) **Determination of metrics for redistribution**: Services using Open Shortest Path First (OSPF) protocol in their internal networks must set metrics for learned routes.
5) **Creation of ACLs**: Build access lists for distribution lists and ACLs for information assurance (IA).

In the scenario of Figure 5-5, the Army, as the supporting Service, determines the use of the 10.10.0.0 network for the lateral link and EIGRP 10 as the lateral link routing protocol. EIGRP 10 is installed only on the border routers.

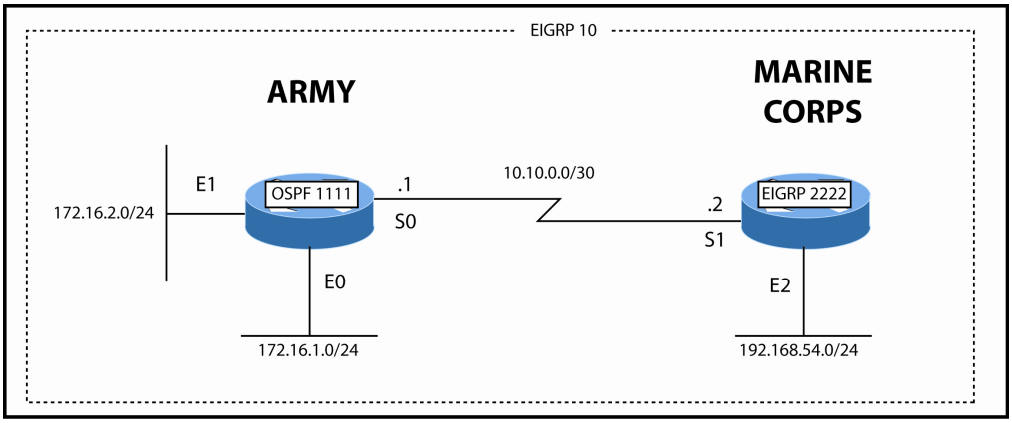


Figure 5-5 Army Operating as a Supporting Service

Add the network for the lateral link to the Service internal OSPF process using the following commands:

```
Army(config)#router ospf 1111
Army(config-router)#network 10.10.0.0
```

Create the EIGRP process for the Purple Zone and redistribute the OSPF process using appropriate metric values. The settings in the example are the default metrics—namely, bandwidth of 10,000 kbps, delay of 1000 ms, 100 percent reliability, 1/255 of interface load, and an MTU of 1500 bytes. The router will accept any values for the metric setting; however, metric values that best match the network topology will allow the router to make a better routing decision. Use the **match internal** command to redistribute only the internal routes that belong to the domain, which prevents external prefixes from being redistributed back into the same domain.

```
Army(config)#router eigrp 10
Army(config-router)#redistribute ospf 1111 metric 10000 100 255 1 1500
match internal
Army(config-router)#network 10.10.0.0
```

Use **distance eigrp [** ***internal external*** **]** to ensure that the lateral link is used for tactical traffic. The following example sets the administrative distance of all EIGRP internal routes to 85 and all EIGRP external routes to 89.

```
Army(config-router)# distance eigrp 85 89
```

Use **no auto summary** command if subnets advertised are discontiguous. Enable logging of neighbor adjacency changes to monitor the stability of the routing system and help detect problems with eigrp log-neighbor changes.

```
Army(config-router)#no auto-summary
Army(config-router)#eigrp log-neighbor-changes
```

Use the **distribute list** command to control routes advertised by the Purple Zone's EIGRP process. The **out** argument tells the EIGRP process to advertise only routes that are permitted by the access list.

```
Army(config-router)#distribute-list 1 out
```

Use the following commands to ensure ACLs for the distribute list contain all networks that are to be advertised by the EIGRP route process:

```
Army(config)# access-list 1 permit 172.16.1.0 0.0.0.255
Army(config)# access-list 1 permit 172.16.2.0 0.0.0.255
Army(config)# access-list 1 deny any
```

If the Service is already running EIGRP as the internal gateway protocol, the Purple Zone's EIGRP 10 is also used and installed on the border router. Use the following commands to redistribute the internal EIGRP process into the lateral link EIGRP process:

```
MarineCorps(config)#router eigrp 10
MarineCorps(config-router)#redistribute eigrp 2222
MarineCorps(config-router)#network 10.10.0.0
MarineCorps(config-router)# distribute-list 2 out
MarineCorps(config-router)#no auto-summary
MarineCorps(config-router)#eigrp log-neighbor-changes

MarineCorps(config)# access-list 2 permit 192.168.54.0 0.0.0.255
MarineCorps(config)# access-list 2 deny any
```

In Figure 5-6, the Air Force is acting as the MDN. Private addressing is used on the lateral links and EIGRP 40 is operating on all border routers with the Services' respective IGPs redistributed into EIGRP 40.

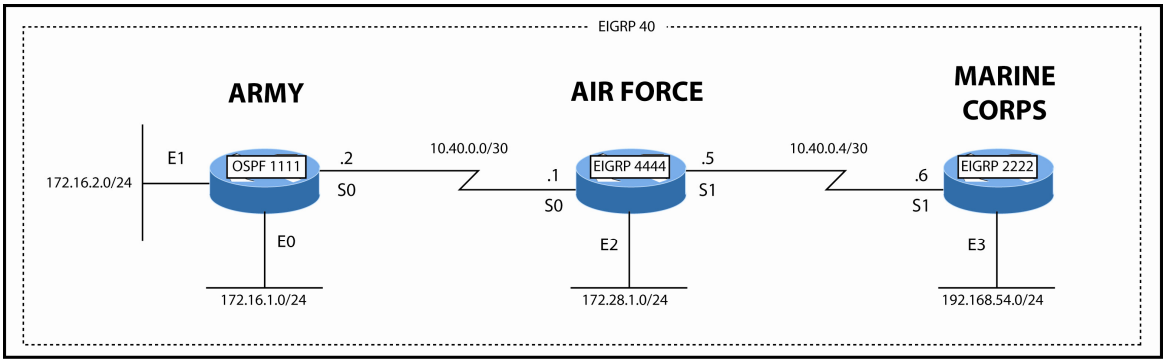
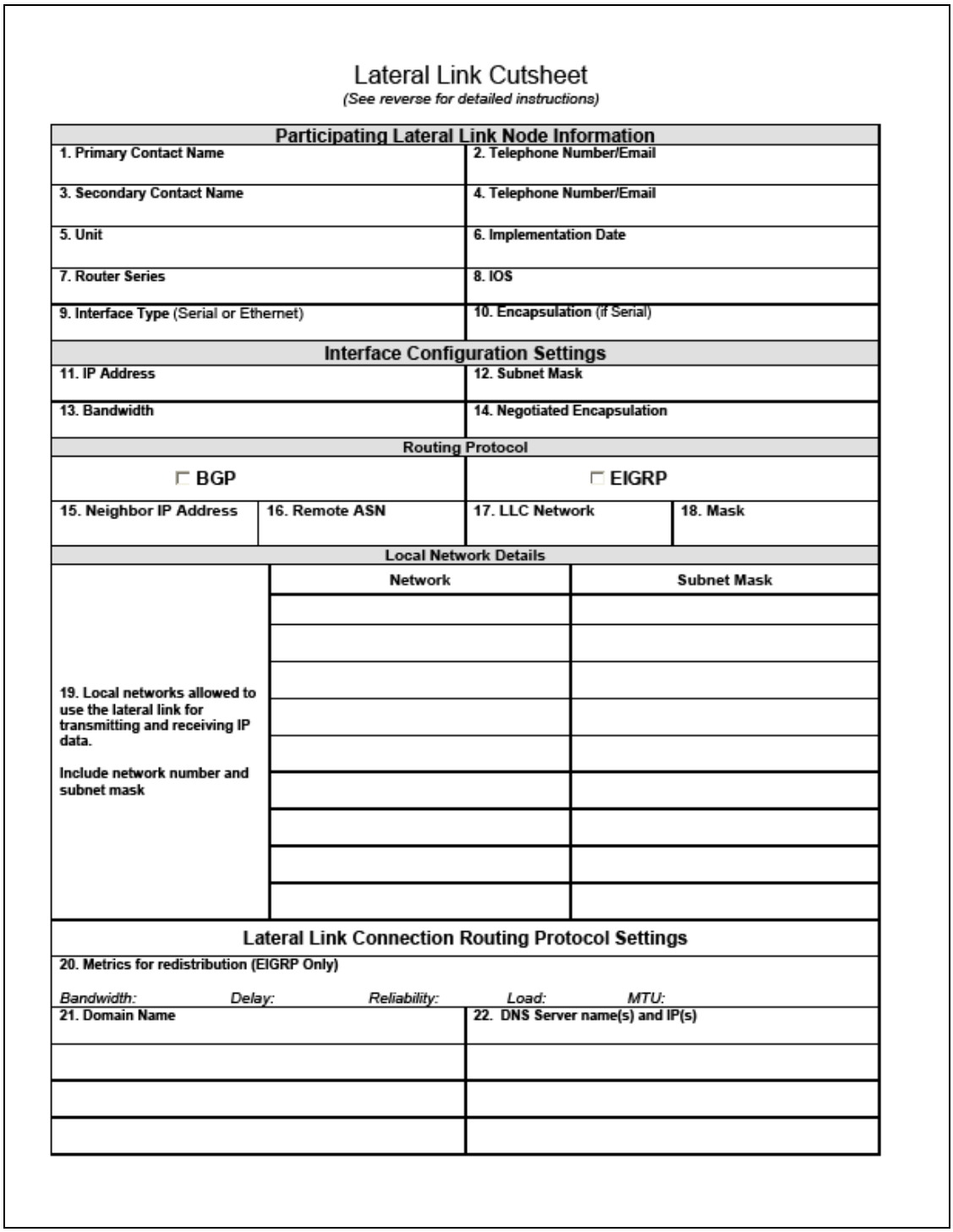


Figure 5-6 Air Force Operating as an MDN

Figure 5-7 is an example of a Lateral Link Cutsheet. This tool is designed to be completed by C4 planners and implemented by network administrators at each LLN. The back of the sheet contains abbreviated instructions based on the planning steps.



Lateral Link Cutsheet

(See reverse for detailed instructions)

Participating Lateral Link Node Information	
1. Primary Contact Name	2. Telephone Number/Email
3. Secondary Contact Name	4. Telephone Number/Email
5. Unit	6. Implementation Date
7. Router Series	8. IOS
9. Interface Type (Serial or Ethernet)	10. Encapsulation (if Serial)

Interface Configuration Settings	
11. IP Address	12. Subnet Mask
13. Bandwidth	14. Negotiated Encapsulation

Routing Protocol			
☐ BGP		☐ EIGRP	
15. Neighbor IP Address	16. Remote ASN	17. LLC Network	18. Mask

Local Network Details		
	Network	Subnet Mask
19. Local networks allowed to use the lateral link for transmitting and receiving IP data. Include network number and subnet mask		

Lateral Link Connection Routing Protocol Settings	
20. Metrics for redistribution (EIGRP Only) *Bandwidth:* *Delay:* *Reliability:* *Load:* *MTU:*	
21. Domain Name	22. DNS Server name(s) and IP(s)

Figure 5-7 Lateral Link Cutsheet

Figure 5-8 is an example of a Multi-link Distribution Node Cutsheet. This cutsheet is another tool developed by JMNO to ensure network administrators have all necessary information to establish their LLN as an MDN.

Multi-link Distribution Node (MDN) Cutsheet

(See reverse for detailed instructions)

Participating Lateral Link Node Information			
1. Your location and POC Information:			
2. Adjacent Node #1 (Attach LLC Cutsheet)		**3. Adjacent Node #2 (Attach LLC Cutsheet)**	
4. Exterior Routing Protocol used for LLCs (Both LLCs must use the same exterior routing protocol) ☐ BGP ☐ EIGRP			
5. EIGRP: LLC Process Number		**6. EIGRP: LLC Process Number**	
7. BGP: Distant End ASN (Node 1)		**8. BGP: Distant End ASN (Node 2)**	
9. LLC Distant End Router Port IP		**10. LLC Distant End Router Port IP**	
11. LLC IP Network Number		**12. LLC IP Network Number**	
13. LLC IP Network Subnet Mask		**14. LLC IP Network Subnet Mask**	
15. Networks From Node 1's LLC Cutsheet that are allowed to traverse MDN	**16. LLC Node 1 Networks Subnet mask**	**17. Networks From Node 2's LLC Cutsheet that are allowed to traverse MDN**	**18. LLC Node 2 Networks Subnet mask**

Sample Additional BGP Router Entries
(See LLC Cutsheet for original Sample)

router bgp 65020
no synchronization
bgp log-neighbor-changes
network 205.109.53.4 mask 255.255.255.252
neighbor 10.10.0.1 remote-as 65010
neighbor 10.20.0.2 remote-as 65030 ***(node 2's information)***
no auto-summary

Sample EIGRP Entry for Networks using OSPF Internally
(Redistributing OSPF information)
(See LLC Cutsheet for original Sample)

router eigrp 10
redistribute ospf 21 metric 2048 10 255 1 1500 match internal
network 10.10.0.0 0.0.0.3
network 10.20.0.0 0.0.0.3 ***(node 2's information)***
network 144.106.0.0
distribute-list 12 out
distance eigrp 85 89
no auto-summary

Sample EIGRP Entry for Networks using EIGRP Internally
Router Commands/Entries

router eigrp 10
redistribute eigrp 1775
network 10.10.0.0 0.0.0.3
network 10.20.0.0 0.0.0.3
network 205.109.53.4 0.0.0.3
network 205.109.53.8 0.0.0.3
network 205.109.53.128 0.0.0.15
distribute-list 12 out
no auto-summary
no eigrp log-neighbor-changes

Sample Access List for above Distribute-List
access-list 12 permit 10.10.0.0 0.0.0.3
access-list 12 permit 10.20.0.0 0.0.0.3
access-list 12 permit 205.109.53.4 0.0.0.3
access-list 12 permit 205.109.53.8 0.0.0.3
access-list 12 permit 205.109.53.128 0.0.0.15
access-list 12 permit [all authorized Node 1 Networks]
.
.
access-list 12 permit [all authorized Node 2 Networks]
.
.
access-list 12 deny any

Figure 5-8 Multi-Link Distribution Node Cutsheet

5.3 Domain Name Server (DNS) Procedures

The Domain Name Server (DNS) must be configured with conditional forwarders for users to send email traffic across the lateral link. The use of conditional forwarders also allows access to web and ftp servers across the lateral link by URLs and fully qualified domain names in web browsers without the use of the server's IP address. Conditional forwarders forward queries according to the specific domain names contained in the queries.

To configure conditional forwarding, do the following:

1. Open the **DNS console** under **Administrative Tools**.
2. Right click on the DNS server node. Select **Properties** to open the **Properties** sheet for the DNS server.

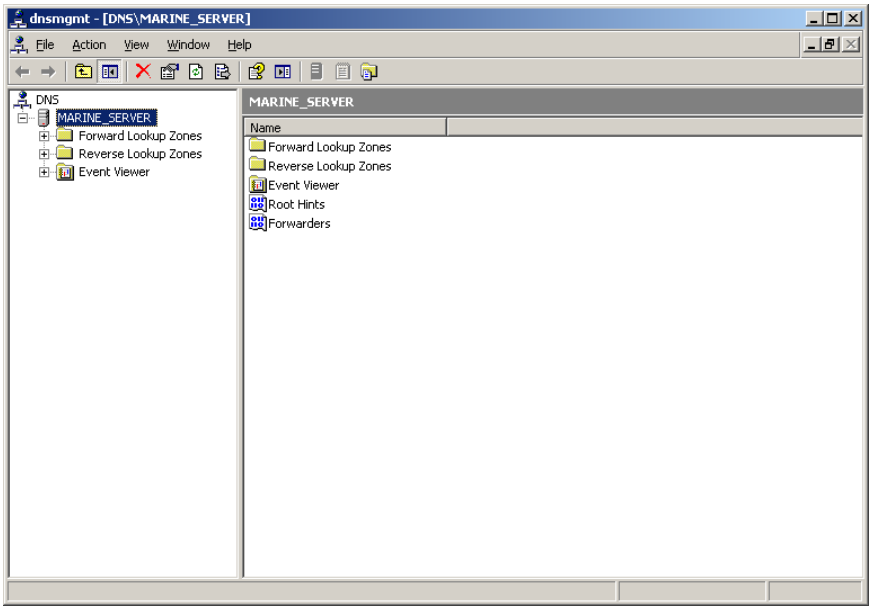


Figure 5-9 DNS Console

3. Select **Forwarders** tab.

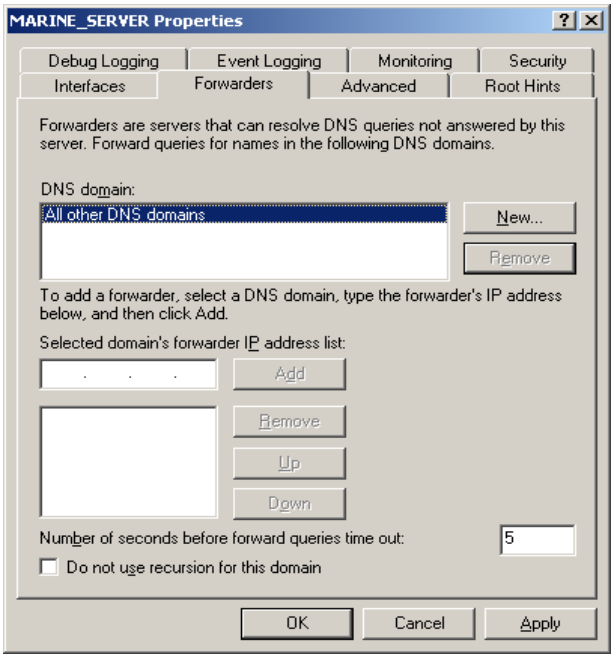


Figure 5-10 Forwarders Tab

4. Select **New** and type the fully qualified domain name of the server to conditionally forward to.

Figure 5-11 New Forwarder Box

5. Click **OK.** The new domain appears in the top listbox.
6. With the domain name highlighted in DNS domain name list, go to "Selected domain's forwarder IP address list."
7. Enter the IP address for a DNS server on the destination domain's network in the dotted box.

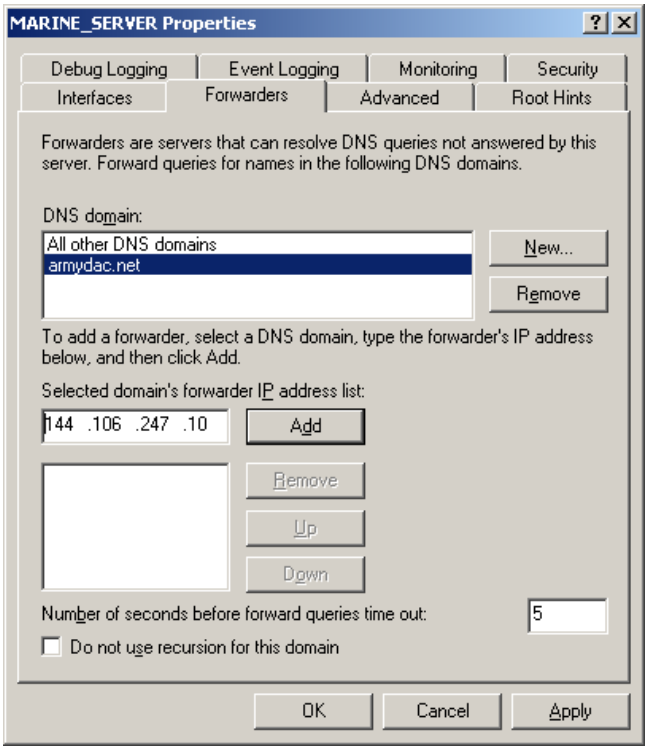


Figure 5-12 Forwarders Tab With New Domain

8. Click **Add** to add it to the selected domain's forwarders list.
9. Click **OK** to apply the change.

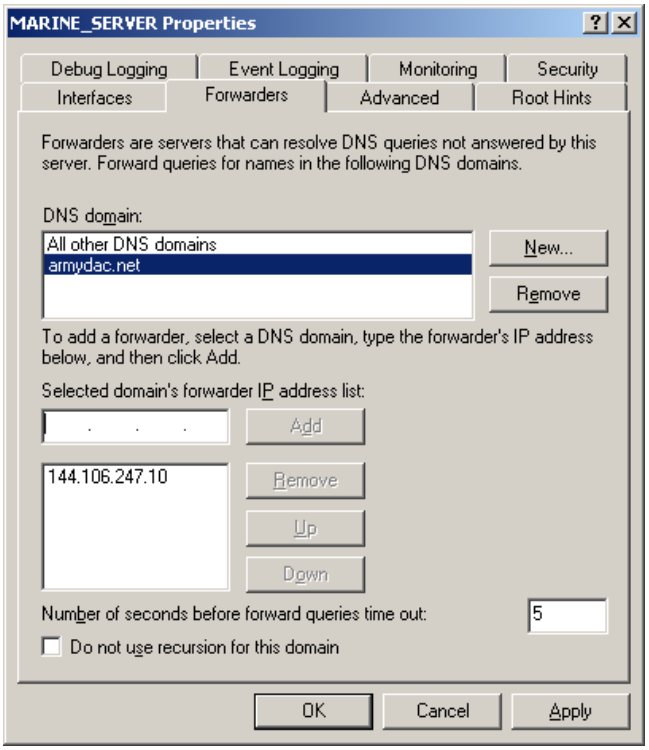


Figure 5-13 Forwarders Tab after New Domain has been added

10. For any additional DNS servers on the destination domain network, enter additional IP addresses.
11. Click the **Apply** button and close the properties sheet.

Follow these procedures to add forwarders for each destination domain to be reached. To reach a destination domain through an MDN, each destination domain to be reached will require a forwarder entry as previously instructed.

5.4 Supporting the Mobile User

At a basic level, mobile users can be supported by configuring routers to use Microsoft Point-to-Point Tunneling Protocol (PPTP) for Clients and Microsoft Point-to-Point Encryption Protocol (MMPE). Mobile users may connect to a switch that has been configured as a virtual local area network (VLAN) with several dedicated ports (known as "Purple Ports").

Mobile users on the "Purple Port" may be assigned a static IP address or draw Dynamic Host Configuration Protocol (DHCP) services from the host router. This assignment provides mobile users with access to the lateral link and their home network.

The following configurations are examples using the architecture depicted in Figure 5-14 for routers running Cisco IOS Software Release 12.3 or later. In this example, a Cisco switch on the Army's 172.16.1.0 LAN is configured with VLAN 10 dedicated to the mobile user. The Army router is providing DHCP services for an Air Force mobile user.

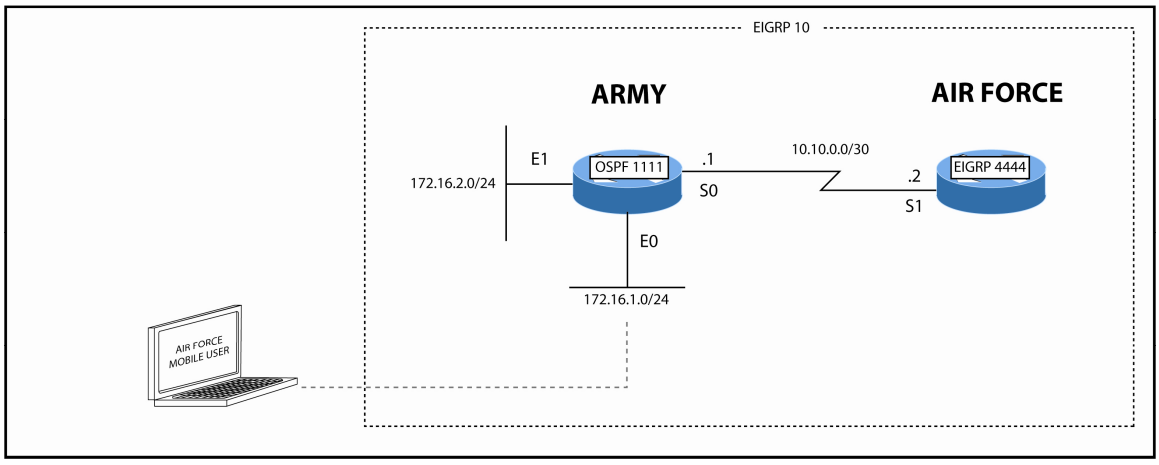


Figure 5-14 Mobile User

On the switch, create a VLAN for mobile users by using the following commands:

```
Armyswitch#vlan database
Armyswitch(vlan)#vlan 10
Armyswitch(vlan)#exit
```

Use the following commands to configure switchports on the VLAN:

```
Armyswitch(config)#interface fastethernet0/10
Armyswitch(config-if)#switchport mode access
Armyswitch(config-if)#switchport access vlan 10
Armyswitch(config)#interface fastethernet0/11
Armyswitch(config-if)#switchport mode access
Armyswitch(config-if)#switchport access vlan 10
Armyswitch(config)#interface fastethernet0/11
Armyswitch(config-if)#switchport mode access
Armyswitch(config-if)#switchport access vlan 10
```

Use the following commands to configure a subinterface on the router for the new VLAN:

```
Army(config)#interface fastethernet0/0.10
Army(config-if)#encapsulation dot1Q 10
Army(config-if)#ip address 172.16.1.225 255.255.255.240
```

For configuring DHCP on the router, create the pool of addresses from which DHCP mobile hosts will draw addresses.

In the example configuration that follows, the pool of addresses will be in the 172.16.1.224/28 network. The "**default-router 172.16.1.225**" command specifies the IP address of the Ethernet subinterface for VLAN 10 on the switch. Excluded DHCP addresses range from .224 to .230; thus, the assignable addresses are .231 to .239.

```
Army(config)#ip dhcp pool PURPLE_PORTS
Army(dhcp-config)#network 172.16.1.224 255.255.255.240
Army(dhcp-config)#default-router 172.16.1.225
Army(dhcp-config)#exit
Army(config)#ip dhcp excluded-address 172.16.1.224 172.16.1.230
```

Another option for mobile users is to reserve Ethernet switch ports on multiservice access routers, such as the Cisco 3745, and assign addresses with a /30 mask. Use DHCP services on the router to assign the other available address in the /30 network to the mobile user.

```
Army(config)#interface fastethernet 0/1/0
Army(config-if)#ip address 172.16.1.225 255.255.255.252

Army(config)#interface fastethernet 0/1/1
Army(config-if)#ip address 172.16.1.229 255.255.255.252
Army(config-if)#exit

Army(config)#ip dhcp pool fastethernet 0/1/0
Army(dhcp-config)#network 172.16.1.224 255.255.255.252
Army(dhcp-config)#default-router 172.16.1.225
```

```
Army(dhcp-config)#ip dhcp pool fastethernet 0/1/1
Army(dhcp-config)#network 172.16.1.228 255.255.255.252
Army(dhcp-config)#default-router 172.16.1.229
Army(dhcp-config)#exit

Army(config)#ip dhcp excluded-address 172.16.1.225
Army(config)#ip dhcp excluded-address 172.16.1.229
```

With the configurations in the previous example, the host Service (the Army) has provided addresses for use by mobile users. The border router of the home Service (in this example, the Air Force) must be configured to accept dial-in requests from its mobile users.

To enable virtual private dial-up networking (VPDN) for PPTP client connectivity, use the following command:

```
AirForce(config)#vpdn enable
```

Use the following command to enter VPDN group configuration mode for the specified VPDN group:

```
AirForce(config)#vpdn-group 1
```

To enable the router to enter VPDN configuration mode and accept dial-in requests, use the following command:

```
AirForce(config-vpdn)#accept-dialin
```

Use the following to specify which PPTP protocol is used:

```
AirForce(config-vpdn-acc-in)#protocol [pptp | any | l2f | l2tp]
```

Create the virtual template used for cloning virtual-access interfaces by using the following:

```
AirForce(config-vpdn-acc-in)#virtual-template 1
AirForce(config-vpdn-acc-in)#exit
```

Create a pool of IP addresses that are not being used on the internal network. Note that the network must be included in the network statements of the Purple Zone routing protocol so the mobile users can access the lateral link. The syntax of the statement includes the first and last address in the pool:

```
AirForce(config)#ip local pool AIRFORCE 172.28.1.208 172.28.1.223
```

Configure the virtual-access interface. The **ip unnumbered** interface may point to any active interface on the router. In the example below, the interface is pointed to the Serial 0 interface:

```
AirForce(config)#interface Virtual-Template1
AirForce(config-if)#ip unnumbered Serial0
AirForce(config-if)#peer default ip address pool AIRFORCE
```

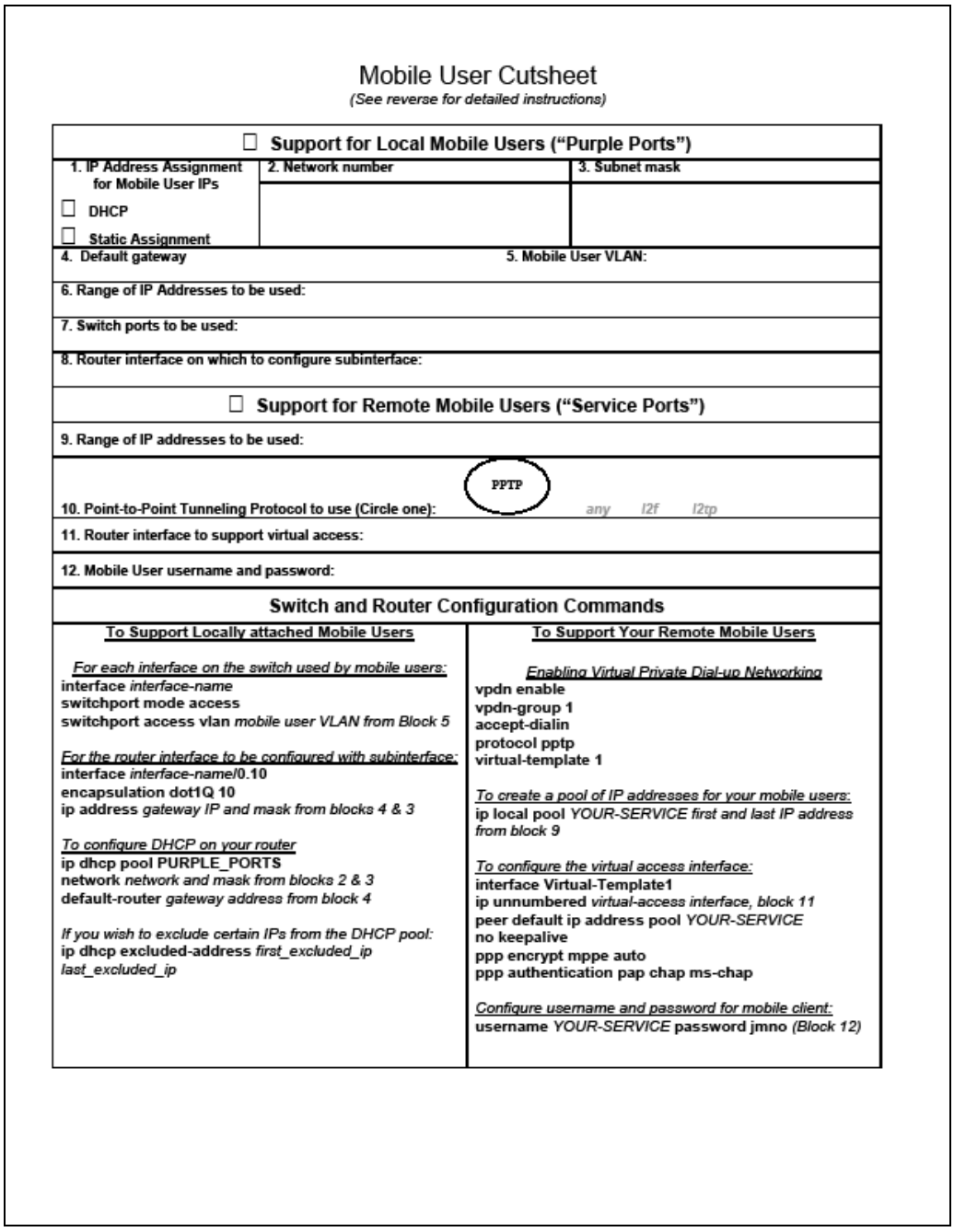
```
AirForce(config-if)#no keepalive
AirForce(config-if)#ppp encrypt mppe auto
AirForce(config-if)#ppp authentication pap chap ms-chap
AirForce(config-if)#exit
```

Finally, to configure authentication on the home router for access by the mobile user, using the following:

```
AirForce(config)# username airforce password jmno
```

The username and password will be the same as those used to configure the connection on the client.

Figure 5-15 is an example of the Mobile User Cutsheet, another JMNO-developed tool**.** This tool is designed to be completed by C4 planners and implemented by network administrators at each LLN that will host mobile users, or will have mobile users from their Service connecting to them via VPN to access network services. The back of the sheet contains abbreviated instructions based on the planning steps described in this section.



Mobile User Cutsheet

(See reverse for detailed instructions)

☐ **Support for Local Mobile Users ("Purple Ports")**

1. IP Address Assignment for Mobile User IPs ☐ DHCP ☐ Static Assignment	2. Network number	3. Subnet mask

4. Default gateway **5. Mobile User VLAN:**

6. Range of IP Addresses to be used:

7. Switch ports to be used:

8. Router interface on which to configure subinterface:

☐ **Support for Remote Mobile Users ("Service Ports")**

9. Range of IP addresses to be used:

10. Point-to-Point Tunneling Protocol to use (Circle one): PPTP *any l2f l2tp*

11. Router interface to support virtual access:

12. Mobile User username and password:

Switch and Router Configuration Commands

To Support Locally attached Mobile Users

For each interface on the switch used by mobile users:
interface *interface-name*
switchport mode access
switchport access vlan *mobile user VLAN from Block 5*

For the router interface to be configured with subinterface:
interface *interface-name*/**0.10**
encapsulation dot1Q 10
ip address *gateway IP and mask from blocks 4 & 3*

To configure DHCP on your router
ip dhcp pool PURPLE_PORTS
network *network and mask from blocks 2 & 3*
default-router *gateway address from block 4*

If you wish to exclude certain IPs from the DHCP pool:
ip dhcp excluded-address *first_excluded_ip*
last_excluded_ip

To Support Your Remote Mobile Users

Enabling Virtual Private Dial-up Networking
vpdn enable
vpdn-group 1
accept-dialin
protocol pptp
virtual-template 1

To create a pool of IP addresses for your mobile users:
ip local pool *YOUR-SERVICE first and last IP address from block 9*

To configure the virtual access interface:
interface Virtual-Template1
ip unnumbered *virtual-access interface, block 11*
peer default ip address pool *YOUR-SERVICE*
no keepalive
ppp encrypt mppe auto
ppp authentication pap chap ms-chap

Configure username and password for mobile client:
username *YOUR-SERVICE* **password jmno** *(Block 12)*

Figure 5-15 Mobile User Cutsheet

5.4.1 PPTP Client Setup for Windows XP

To configure PPTP on the client:

1. Go to the **Control Panel**.
2. Click on **Network Internet Connections** (this step may not be necessary.)
3. Click on **Network Connections**.

Figure 5-16 New Connection Welcome Screen

4. Click on **Create a New Connection** to start the configuration wizard.

Figure 5-17 New Connection Wizard

5. Add a connection name, and dial settings, and hostname.

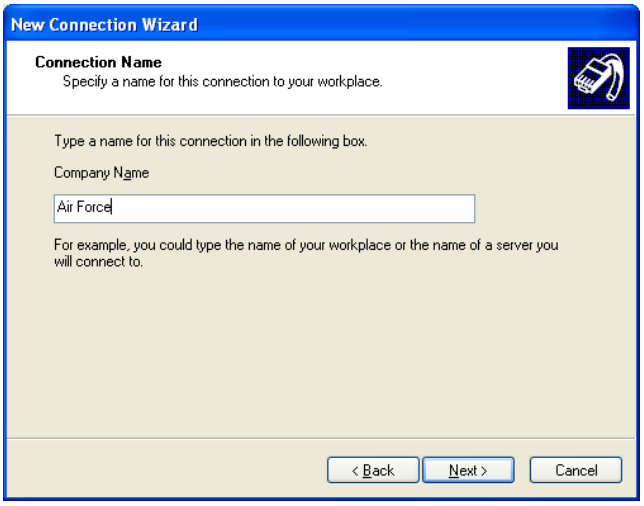


Figure 5-18 Host Name

The Public Network screen provides the option to automatically dial this connection first.

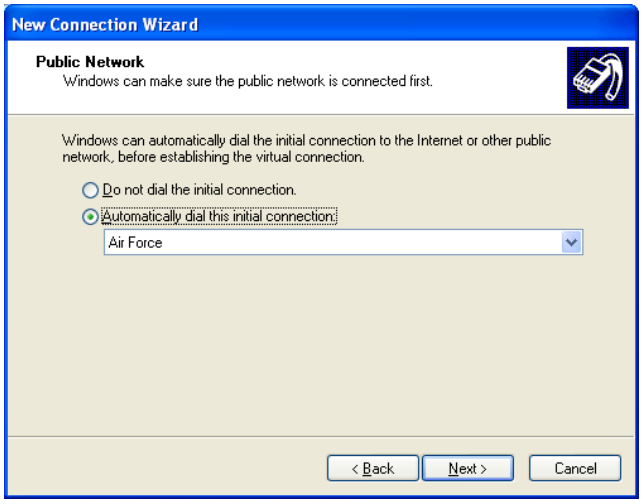


Figure 5-19 Specifying Initial Network Connection

6. Enter the IP address of any interface on the home router.

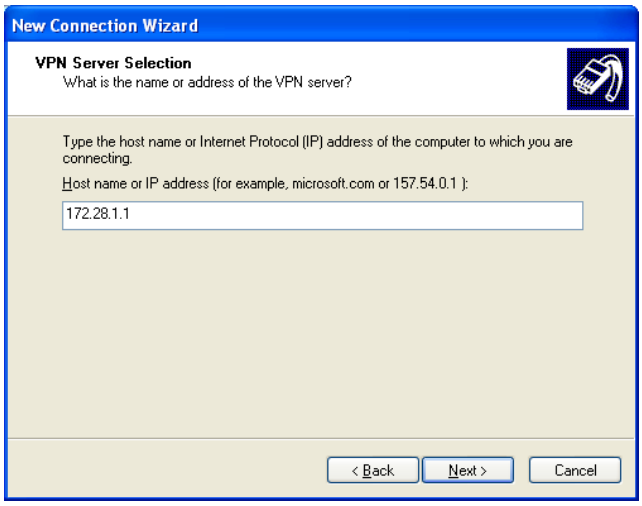


Figure 5-20 IP Address of Home Network Border Router

The following screen provides the options for authentication.

NOTE: The selection of using Smart Card authentication depends on the policy of the Service that owns the laptop.

7. Select the option of using Smart Cards, in accordance with Service policy and click **Next**.

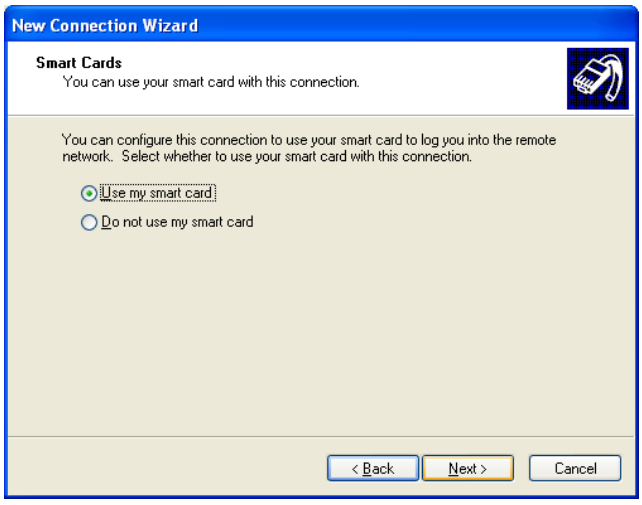


Figure 5-21 Option to Use Smart Card

The following screen provides the option to make the connection available to other users of the laptop.

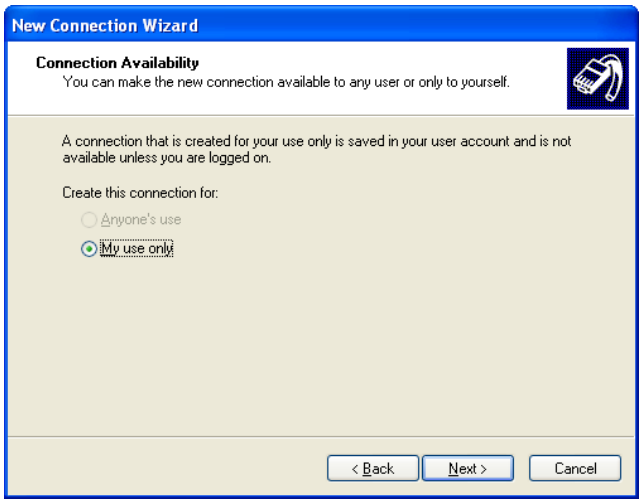


Figure 5-22 Option to Make Connection Available for User Only

8. To ensure no other users of the laptop can use the connection, select the **My use only** option.

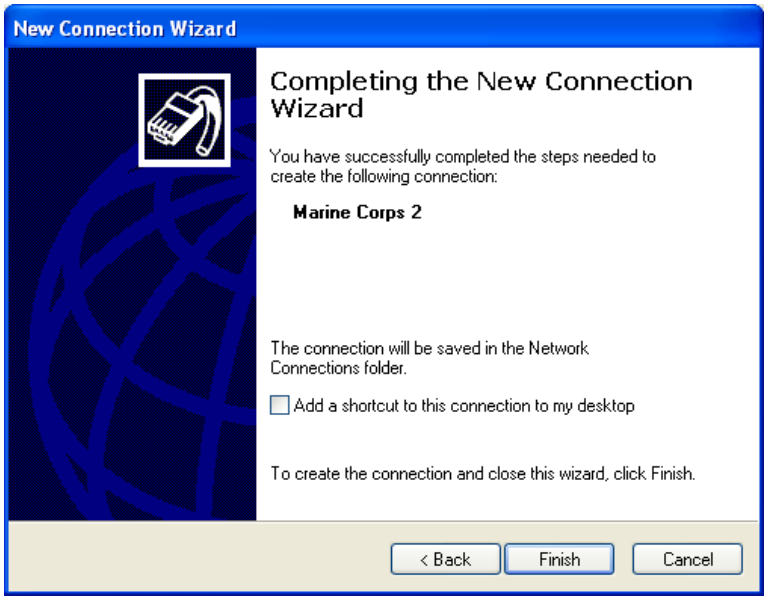


Figure 5-23 New Connection Wizard Completion Screen

9. Click **Finish** to close the New Connection Wizard.

10. When Connection Wizard is complete, right-click on the connection icon to set **Properties**.

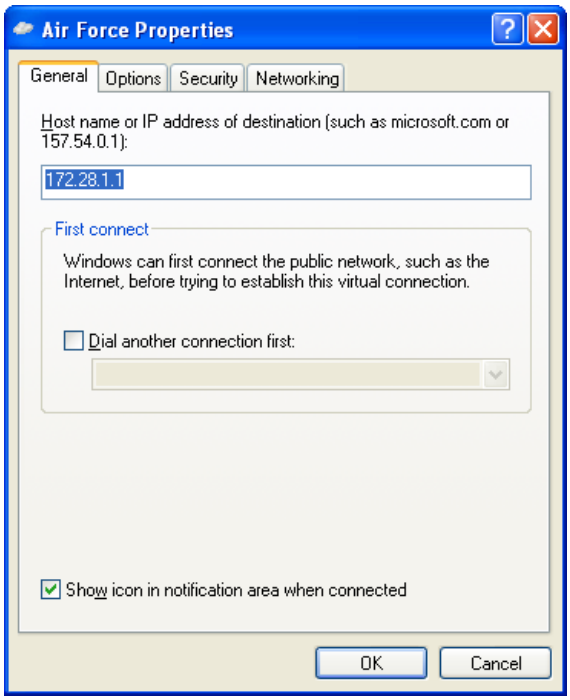


Figure 5-24 Connection Properties

11. Select **Security** tab for configuring security options per the Service's policies.

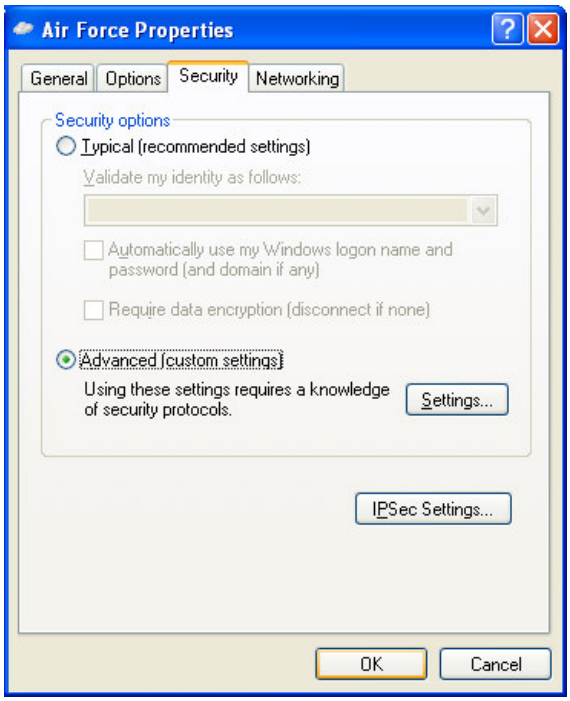


Figure 5-25 Security Tab

IPSec Settings on the **Security** tab provides for entry of authentication key if it is to be used.

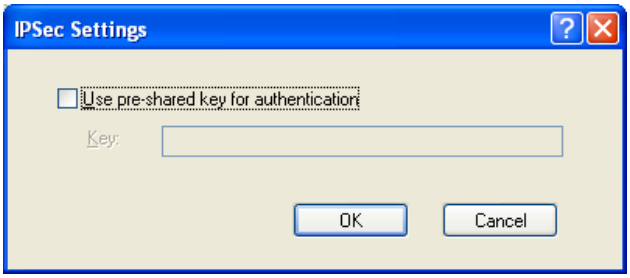


Figure 5-26 IPSec Settings

12. Select the **Networking** tab. From the **Type of VPN** drop-down box, select **PPTP VPN**.

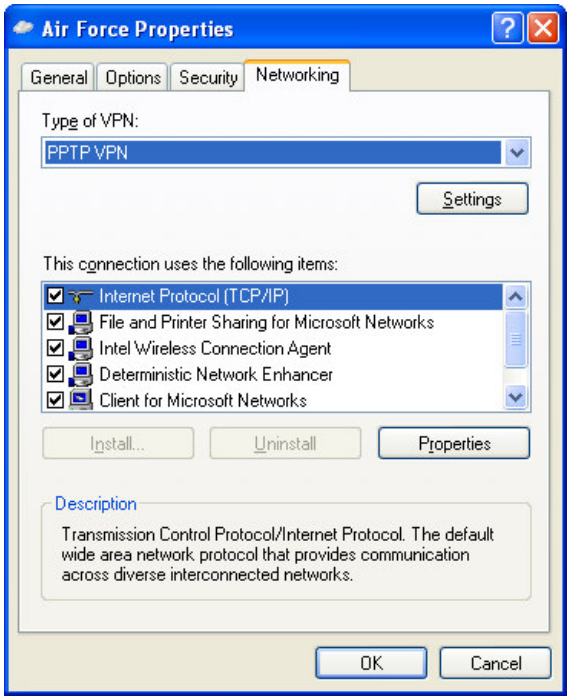


Figure 5-27 Networking Tab

13. Set data encryption option and other advanced settings per the Service's policies.

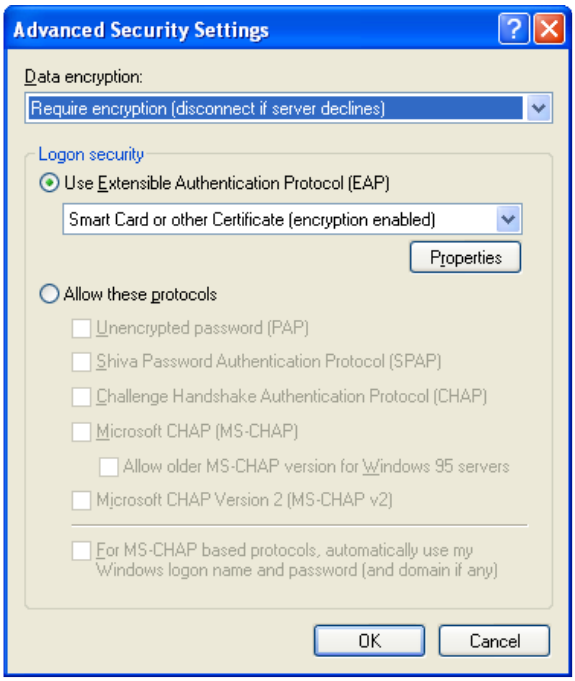


Figure 5-28 Advanced Security Settings

When making the connection to the home network, the client will be prompted for username and password as configured on the home network router.

Figure 5-29

This page intentionally left blank.

Annex A: Information Assurance (IA)

This annex of the Joint Mobile Network Operations (JMNO) tactics, techniques, and procedures (TTP) present a risk management approach that can be followed when planning and implementing LLCs. The overall intent of the JMNO TTP are to help reduce the time required to establish lateral links. This annex tailors existing Department of Defense (DOD) Information Assurance (IA) guidance to the special case presented by lateral links between Services.

All Services currently have robust IA defense in-depth strategies in place. However, these strategies (and attendant IA architectures) are based on strict, hierarchical network connections from the lowest tactical units, through a centralized point of presence (usually a division or wing-level unit), and thence to either the JTF network or the DISN. Since JMNO TTP are focused at the tactical level, JMNO lateral link connections (LLCs) break from the traditional IA architecture. JMNO TTP assume that each Service component in a JMNO-enabled JTF architecture has its IA architecture in place at the higher echelon, and thus the LLCs require only a simplified set of IA restrictions.

This annex includes information and guidance concerning establishment of cross-domain solutions, including connectivity between nodes and systems with differing classification levels (CLs) and Mission Assurance Categories (MACs). This makes it extensible for planning and establishing LLCs with Other Government Agencies (OGAs), Non-Governmental Organizations (NGOs), and coalition forces. As noted above, the bottom line is that this is a RISK MANAGEMENT APPROACH designed to give a Designated Approval Authority (DAA) a planning tool to help in the overall decision process.

Objective

The tactics, techniques, and procedures (TTP) described in this annex are intended to address the information assurance (IA) concerns that arise when information systems (nodes) from different services/agencies/organizations are linked together for the purpose of sharing information or connectivity. The TTP described herein presents a risk management approach that can be followed when; first, considering, and second, possibly implementing, a Lateral Link Connection (LLC), as described in the main document. The intent of this TTP is to help reduce the time required to establish lateral links, by reducing the time required to address all associated IA concerns. The TTP does this by tailoring existing DoD IA guidance to the special case presented by lateral links between Services. The TTP in this appendix is henceforth referred to as the IA TTP.

Obstacle

In high-level IA terms, the primary obstacle to establishing a lateral link between dissimilar nodes is the unknown additional risk that is introduced into each participating node. Though a node representative from a particular node will have a good understanding of the residual risk to information residing within his own node's boundary, the connection to an unknown, or lesser known, node has the potential of exposing his information to an unacceptable level of additional

risk. Since it is the responsibility of each node representative to protect the confidentiality, integrity, availability, and authenticity of information produced, stored, transmitted, or processed by his node; such interconnecting lateral links should be rejected unless procedures are established and followed which can reliably identify and manage this otherwise unknown risk.

> *All interconnections of DoD information systems shall be managed to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems.*
> *- DoDD 8500.1, Par. 4.14*

Enabling Precepts

#1: Successful acceptance of the IA TTP relies largely on the confidence that is held among all lateral link participants in the DoD certification and accreditation (C&A) process (refs a, b, and c). It is precisely because so much can (or should) be assumed of any node that receives an approval to operate (ATO) under the DIACAP C&A process, that the IA TTP can be of sufficient brevity to accommodate the goal of reducing the time taken to negotiate a lateral link.

#2: Also driving acceptance of the IA TTP is the logical observation that a node that is currently operating with an acceptable level of risk in the absence of a lateral link; should retain that status so long as nothing flowing across its boundary, as a consequence of establishing a lateral link, causes that risk level to rise unacceptably**.**

General Solution

The IA TTP presents a solution that is built around four cornerstones. The first cornerstone establishes that any additional risk introduced by a lateral link is largely defined by the characterization of the data shared or passed on that link. This information is summarized via the list of promulgated Joint Information Exchange Requirements (JIERs). The IA TTP requires that the JIERs be identified, scrutinized for security risk, and controlled on all lateral links. The second cornerstone acknowledges the risk to data in transit (for example, observation, modification, or impersonation), and thus requires that all lateral link traffic be conveyed via secure tunnel (encryption) technology. The third cornerstone establishes that the resistance to the establishment of lateral links owes more to a lack of trust than it does to a lack of technology. The IA TTP endeavors to dispel this trust issue by having the involved nodes undergo a third party IA robustness and policy compliance evaluation. In the absence of an available third party evaluator, the nodes may conduct a mutual robustness/compliance evaluation given whatever resources and personnel expertise is at hand. The fourth cornerstone recognizes the need to simplify the coordination of lateral link IA management, and thus provides a Lateral Link Interconnect IA Memorandum of Agreement (IA MOA) from which the operative elements of cornerstones 1-3 can be identified, acted upon, and documented.

Controlled Gateways

The first and second cornerstones require that some combination of managerial and technical IA controls are employed that can: restrict traffic to only that which has been approved as mission essential (such as, JIERs), afford protection of that traffic as it transits between nodes, and address any cross-domain or “cross-MAC” situations. These controls should be implemented on

a node's border gateway (for example, router) and—as necessary—a dedicated subnet on the "inside" interface of that gateway. These controls should be able to reliably mitigate four types of lateral link risks.

1. The traditional threats to data in transit (that is, unauthorized observation, modification, or insertion (impersonation)). This should be mitigated by employing secure-tunnel technology (such as, TACLANE or VPN technology).

2. The threat from vulnerable/exploitable services or protocols. This should be mitigated by employing a "least privilege" filter policy at each node's border gateway/router wherein only approved JIER traffic is permitted through external interfaces, and only approved JIER traffic designated for sharing is permitted through internal interfaces (See the Shared Versus Pass-through JIERs section below).

3. The threat of data "*leakage*" inherent to cross-domain links (that is, connected nodes have different confidentiality levels). This should be mitigated by employing either a one-way "diode", a cross-domain solution (CDS), or a manual "downgrading" review, as appropriate (See **Appendix 4: The Joint-Militarized Zone (JMZ) Concept** for a discussion of the JMZ concept).

4. The threat of data corruption and/or destruction that is possible in "cross-MAC" situations (such as, connected nodes have different Mission Assurance Categories). This should be mitigated by identifying any "low to high" data overwrites or other permitted remote service procedures executable from the "low" node that may adversely impact the integrity or availability of data on the "high" node, then blocking or controlling such actions as necessary (See **Appendix 4: The Joint-Militarized Zone (JMZ) Concept** for a discussion of the JMZ concept)

Network-to-Network, User-to-Network, and User Cross-Network Links

The TTP describes two types of lateral links: Network to Network (NTN) and User Cross Network (UCN). A UCN type interconnection represents a "superset" solution of a NTN. This follows from the fact that a NTN lateral link must be in existence before a UCN link can be supported. With a NTN lateral link in place, support for a UCN link is a relatively simple matter of including the necessary "pass-through" circuit as one more JIER to be considered and included in the IA MOA that is negotiated between two nodes contemplating, or already participating in, a NTN lateral link. The requirement to support UCN pass-through traffic may be known in advance (that is, it is promulgated in the Comm/Data Plan), and thus included in the IA MOA as it is being developed; or the UCN requirement may arise after the IA MOA has already been developed, in which case UCN pass-through traffic will simply be added in the change section (section VIII) of the IA MOA when it is promulgated by appropriate authority.

Since the objective of a UCN link is to provide transitive connectivity from a mobile user, back to its higher echelon unit, by way of the laterally linked node (that is, "piggy-backing" on the NTN link); there is no need to permit any data flows to or from the user unit across the host node's boundary/perimeter. So long as the host node has one spare circuit/router interface on its border gateway, all user traffic can be forwarded directly to its higher echelon node, without

"touching" any of the host node's internal systems. This greatly minimizes risk to both the host node and the mobile user.

It may, for reasons of operational benefit, be decided that a mobile node should be able to directly share data with a "fixed" node from an organization (that is, component/service/agency) other than its own. That is, instead of the "fixed" node merely providing pass-through connectivity for the mobile user back to its command echelon node, the mobile user and "fixed" node will directly share data. This will henceforth be referred to as a user-to-network (UTN) link in this annex. Both issues of NTN and UTN entail the more risky act of sharing data, rather than simply passing through data as the UCN link does. This means that the contemplation of either a NTN or a UTN link would initiate a new IA TTP process, including the negotiation of a new IA MOA for that link. Nothing regarding the mobile user's mobility calls for any different security treatment than what has been established for two nodes connected via a NTN link. In summary: NTN and UTN links require negotiation of an IA MOA for each link; while a UCN link will be incorporated within the IA MOA of the "carrying" link.

Shared versus Pass-through JIERs

It is important that the implementers of lateral links not only understand the difference between NTN, UCN and UTN links; but that they also consider whether the JIERs under consideration are intended for "sharing" or for "pass-through" from the perspective of any particular node. Remaining mindful of this latter distinction will better enable the forwarding of mission essential JIERs across multiple node hops, thus facilitating a more richly interconnected, seamless, *purple zone*; rather than a collection of, fragmented, one-hop-only, links. The figure on the next page illustrates all six possible JIER handling scenarios from the Marine Battalion's perspective.

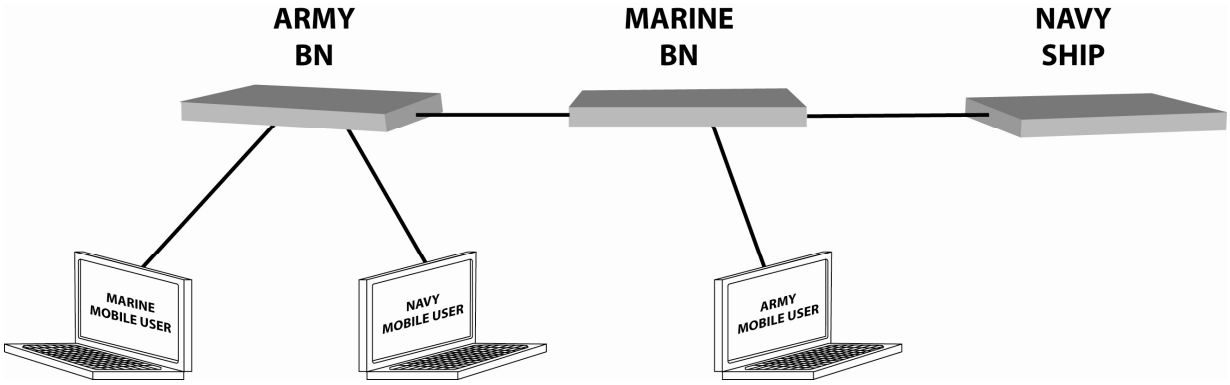


Figure A-1

The six JIER handling scenarios for the Marine Battalion are:

1. Share NTN data with another node (Army Battalion or Navy Ship)
2. Share UCN data with its own mobile user (Marine mobile user)
3. Share UTN data with another node's mobile user (Navy mobile user)
4. Pass-through NTN data between Army Battalion and Navy Ship

5. Pass-through UCN data between Navy Ship and its mobile user (mobile user)
6. Pass-through UCN data between Army Battalion and its mobile user (Army mobile user)

The point of this discussion is that shared JIER traffic must cross a node's perimeter and "interact" with internal systems; thus presenting a greater risk than pass-through JIER traffic in which the only required interaction is routing. To this end the IA MOA has been organized so as to separate shared and pass-through JIERs. Once this is done, the node's gateway will be configured such that its internal interface(s) will only permit shared JIER traffic, and its external interfaces will only permit the necessary inter-nodal shared and pass-through JIER traffic. The figure below illustrates this point using Node B's external router and the six JIER handling scenarios from above.

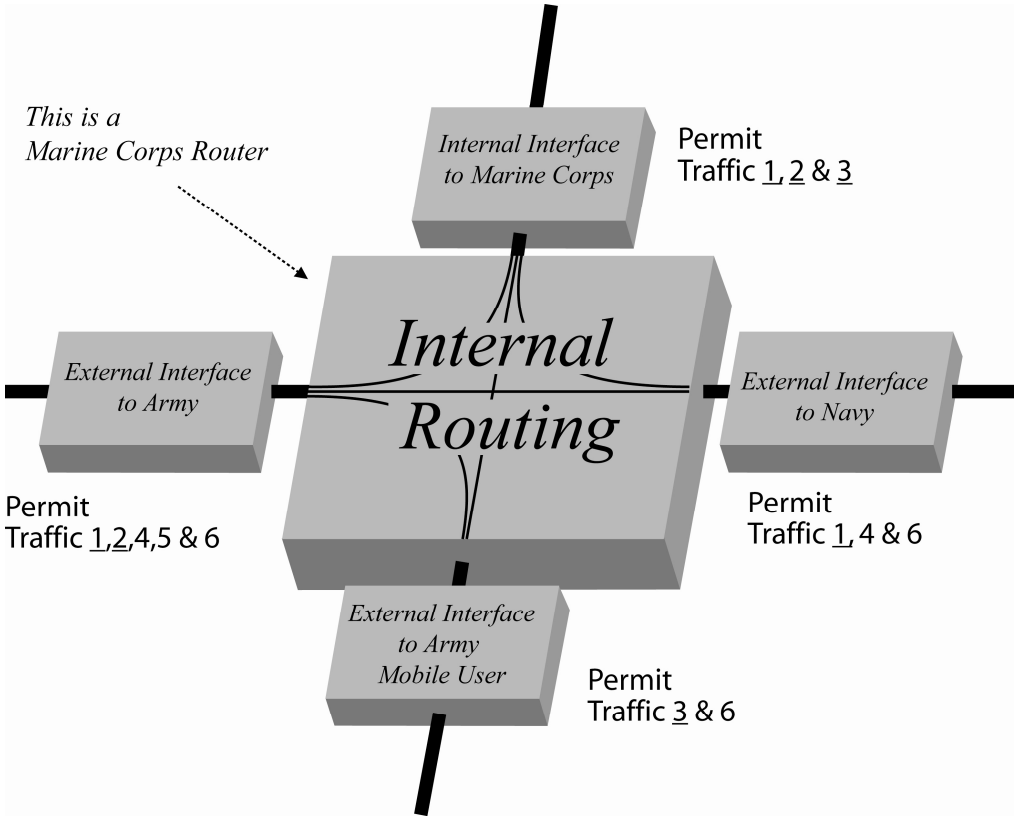


Figure A-2

Two important points of review accompany the preceding figure. First, any NTN (for example, Army-to-Marine and Marine-to-Navy), or UTN (such as, Army's mobile user needing to share/exchange data with Marine Battalion) link will require its own IA MOA. Second, traffic that is intended only for pass-through (such as, 4, 5, & 6) will not be permitted into the passing node's internal network, and therefore presents minimal risk to the passing node. Note that any UCN (for example, Army's mobile user's data being passed by Marine Battalion to/from Army Battalion) link does not require a separate IA MOA. Any UCN pass-through traffic (such as, 6) will simply be included as a JIER within the NTN IA MOA between the two involved nodes (for example, Army and Marine).

One further issue regarding pass-through traffic is paramount to promoting confidence in the IA TTP; that of end-to-end encryption. In this context, the "ends" of the end-to-end encryption are the nodes ("fixed" or mobile) that either provide (that is, are the source of) or use (that is, are the recipient of) the JIER traffic; not any intermediate nodes that serve only to pass the traffic through. It is JMNO IA TTP that all pass-through traffic should already be encrypted (by the source) and remain encrypted until it arrives at the intended recipient's gateway. This provides additional security, and obviates a great deal of key exchanges that would otherwise be necessary if intermediate *decrypt-encrypt* actions were required at each intermediate node. This practice will also permit certain traffic connections over cross-domain paths that might otherwise not be authorized. For example when passing classified traffic through the path *NodeClass—NodeUnclass—NodeClass*, employment of end-to-end encryption between the two classified end nodes would increase the acceptability of permitting the unclassified node to establish the required NTN links with the other two classified links. In cases where a node is passing through encrypted traffic, only one JIER entry is required, regardless of how many services may be encapsulated within the encrypted tunneling protocol. In such a case, the PPS values documented in Table 4 of the IA MOA should coincide with the tunnel**ing** protocol/service vice the tunnel**ed** protocol(s)/service(s). As an informative note, the tunnel**ed** protocol(s)/service(s) can, optionally, be listed in the notes column in the appropriate table (Table 5) of the IA MOA.

Should quality of service (QoS) become a concern as pass-through traffic begins to compete with shared traffic at a particular node, that node could decrease the minimum committed QoS of the pass-through traffic as mission and operational needs dictate. For example, pass-through traffic could initially be categorized as *mission critical*, but later be reduced to *best effort* if it begins to adversely impact higher priority, shared, lateral link traffic. Tab Q of the current Joint IA Policy (Appendix 6) provides suggested bandwidth allotments that may be adopted at the discretion of the node IA representatives. Four classes of traffic are defined: *Voice*, *Mission Critical*, *Best Effort*, and *Scavenger*; and the following bandwidth allotments have been established to be applied during periods of congestion: *Voice* gets 33%, *Mission Critical* gets 41%, *Best Effort* gets 25%, and *Scavenger* gets 1%.

The JMNO IA TTP Lateral Link Negotiation Process

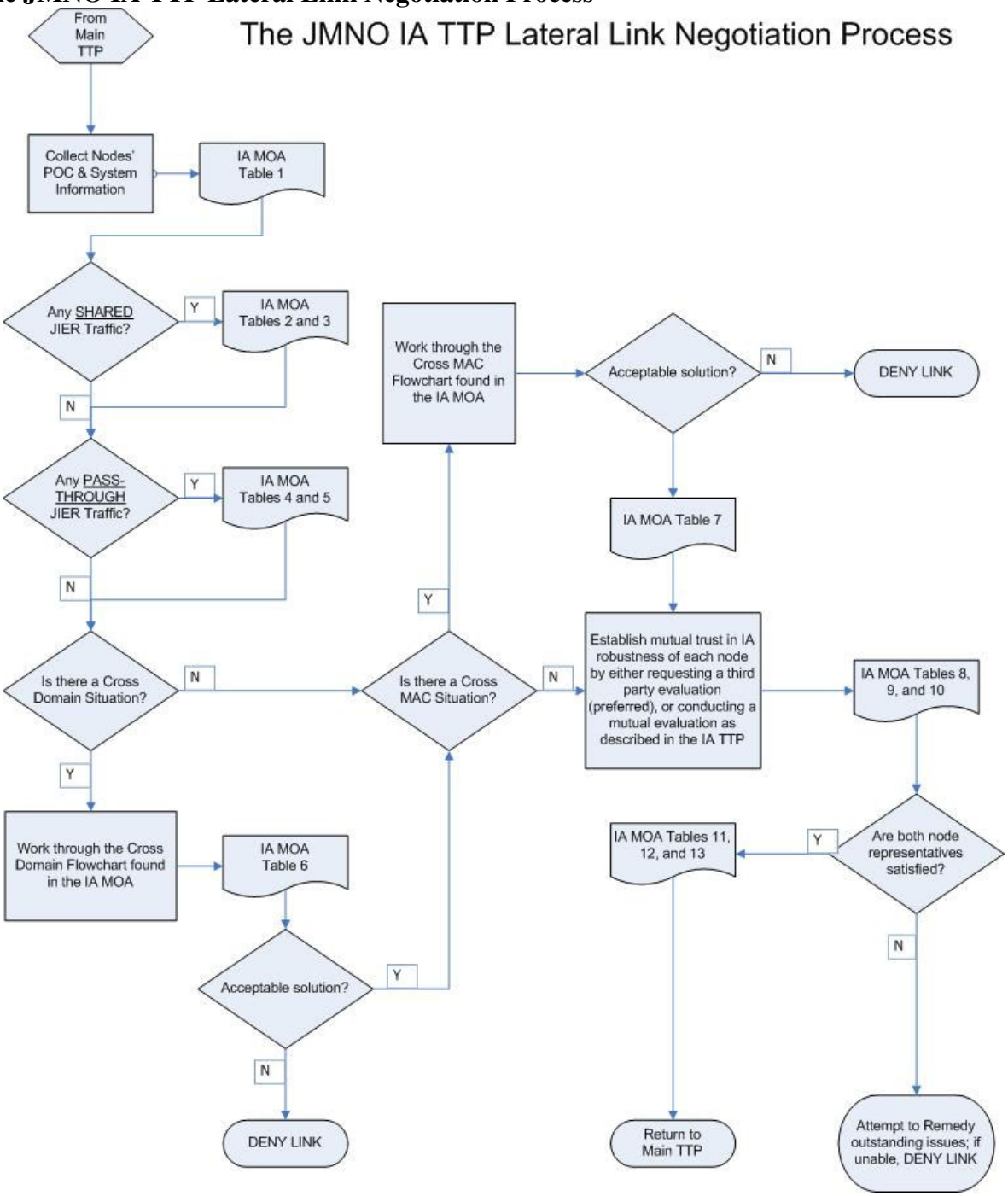


Figure A-3

Figure 2 depicts the JMNO IA Decision Support Flow Chart. The following paragraphs will walk the reader through each decision-making process, including the information necessary to make these decisions.

1. [Collect POC Information] Self explanatory.

2. [Collect System Information] Self explanatory.

3. [Document Shared JIER Traffic] The IA representatives draw on the appropriate Communications Plan, or other authoritative direction, to determine what information exchange requirements exist that entail the direct sharing of data. It is important to establish these requirements as they will largely determine the degree of additional risk introduced by the lateral link, and thus drive the selection of IA controls and ultimately the overall decision to permit establishment of the link or not. Each JIER must be defined by its: service, protocol, port, direction, and PPSM status (refs. g and h). The PPSM status information will be used to screen any JIER traffic that may be either un-registered or coded as "red" (considered too risky to permit). The other JIER information provides the data necessary to write the proper filter rule sets on the routers/firewalls involved.

4. [Document Pass-through JIER Traffic] The IA representatives draw on the appropriate Communications Plan, or other authoritative direction, to determine what information exchange requirements exist that entail "passing through" data that is intended for use by other nodes or mobile users in the purple zone. As was illustrated in the figure at the bottom of page 4 and the discussion that followed, separating shared traffic from pass-through traffic permits an enhanced security solution. If this is not immediately evident, consider that any JIER listed only in the pass-through section of the IA MOA need not be permitted into the passing node's internal network. This situation presents virtually no risk beyond competition for bandwidth among shared JIERs that will be sharing the same link.

5. [Consideration of Cross-domain Situation] The cross-domain situation is discussed in greater detail in **Appendix 5: Lateral Link Interconnect IA MOA** to this annex. The risk is that of information *leakage*, where more sensitive information resident on an appropriately protected "high" node (that is, a node approved to process up to and including classified information) may, through accidental or malicious means, end up being copied or moved to an insufficiently protected "low" node (such as, a node that is only approved to process public information). To protect against such "high to low" leakages, the "higher" node in this cross-domain situation should enforce the "*no write down*" security policy—"high" sensitivity data may not flow "down" to the "low" node. Enforcing this policy requires that either; a) a device is in place that will only permit data to flow from "low" to "high", or b) that a cross-domain solution (CDS or "guard") is in place that can reliably downgrade the classification of any data flowing to the "low" node, to no greater than a "low" sensitivity level. If the "high" node decides to employ a human downgrading function, or an automated CDS/guard, it will be helpful to employ a separate JMZ subnet. This subnet is where the downgrading action should be managed.

This IA TTP suggests that any nodes processing top secret (for example, JWICS nodes) will likely fall outside the purview of this lateral link IA TTP. This arises from the fact that the IA TTP is attempting to drastically shorten the time required to approve a lateral link, and does so by offloading much of the IA re-accreditation, approval, and oversight typically exercised by the DAAs and DSAWG; to the local node owner. That is, if the node owner follows this IA TTP, he can receive expeditious approval, or possibly be authorized to approve the connection himself. Due to the much more sensitive nature of top secret information, it is unlikely that the currently established approval process can, or should, be offloaded to the military tier 7/8

(Regiment/Battalion) level where the JMNO TTP solution is targeted. The final decision rests with the cognizant DAAs and DSAWG.

The issue of "cross-compartment" leakage (such as, *secret-nuclear* data being copied from its node into a node that processes only *secret-chemical*) should also be mentioned. This leakage type is traditionally controlled via discretionary access control mechanisms. Within the context of JMNO the issue is expected to be implicitly dealt with as a result of the motivation for JIER establishment. That is, JIERs are expected to be identified as a result of operational/tactical analysis that reveals a *need-to-share* among *need-to-know* nodes. In cases where only select individuals at a node have the need-to-know, it is expected that that node has the discretionary access security controls in place to affect the need-to-know access policy over all of its users. If a cross-compartment situation presents itself, either or both node representatives may "challenge" the discretionary access controls of the other node during steps 7.b and 7.c of these IA TTP lateral link negotiation process.

6. [Consideration of Cross-MAC Situation] The cross-MAC situation is discussed in greater detail in **Appendix 5: Lateral Link Interconnect IA MOA** to this annex. The risk is the destruction or corruption of higher integrity data by the accidental or intentional (malicious) overwriting with lower integrity data, or by the execution of a malicious/exploited process that is intended to corrupt or destroy data. This risk is inherent when two nodes with differing MAC levels share data, as MAC deals with both the integrity and availability requirements of information. To protect against this risk, nodes of dissimilar MAC levels that are connected together should enforce the "*no write up*" security policy—"low" integrity data may not flow to the "higher" integrity node. Enforcing this policy requires that either; a) a device is in place that will only permit data to flow from "high" to "low", or b) that an "upgrading" solution is in place that can reliably upgrade the integrity of any data arriving at the "high" node from a "low" node; to no less than a "high" MAC level. This concept of data upgrading is less widely understood than the corresponding security action—downgrading—that is applied when addressing the confidentiality of information. A simple example may help.

Node H (high) is a MAC I (high integrity, high availability) system that stores a target list. Node L (low) is a MAC III (basic integrity, basic availability) system, that is involved in collecting, and distributing target data. If both nodes are to form a lateral link for the purpose of L providing H with target data (the JIER), then Node H must take steps to "upgrade" the integrity label (implied or explicit) of any target data delivered from Node L. Failure to do this might result in low integrity (more likely to be incorrect) target data overwriting higher integrity (more likely to be correct) target data on Node H. This is the data integrity analog of the confidentiality "leakage" problem.

If the "high" node decides to employ an upgrading function, it must be done by human review as no known automated solution exists. It will be helpful to employ a separate JMZ subnet where the upgrading action should be managed.

7. [Establishing/Improving Mutual Trust] Though the decision to establish a lateral link may be mandated from higher command, this portion of the IA TTP is intended for situations where local commanders may be given the responsibility and authority to make this decision. The IA TTP recognizes that the level of trust held by one node regarding the IA robustness (that is, the capability to protect information) exemplified by another node, plays a significant role in how readily the former node will be willing to establish a link with the latter node. The level of trust that is sufficient to convince all involved parties that the link may be made without introducing

an unacceptable level of additional risk into their own nodes, is determined primarily by the specifics of the involved JIERs (such as, content, sensitivity, MAC, volume, and direction). Steps 3-6 of the IA TTP lateral link negotiation process are intended to bring these specifics to the forefront. With that work completed, the IA representatives get to work in step 7 assessing whether each has sufficient trust in the robustness of the other node's IA controls to endorse the establishment of a lateral link for those identified JIERs. Ostensibly, the node representative most interested in this assessment would be the representative who perceives that he either: a) has the most to risk/lose, or b) least trusts the other node to not introduce unacceptable additional risks into his node's boundary. In this step; however, both node representatives are encouraged to pursue satisfaction of any issues that may adversely affect their trust in the other node's IA robustness.

The IA TTP focuses this required trust-building in two main areas: 1) evaluation/review of a node's certification effort and results (steps 7.a and 7.b), and 2) a formal or an informal "audit" of a node's adherence to the common operational IA policy (steps 7.c and 7.d). This ensures that the evaluation of trust covers not only how robust a node's IA posture is, but also how correctly that robustness is applied to meet the mandates of the operational IA policy in effect. It is expected that any node being considered for a JMNO lateral link will adhere to this—common—policy. Any attempt to compare and contrast two separate IA policies being followed by two separate nodes would necessitate a lengthy review, which puts this situation outside the scope of JMNO lateral link TTP.

7.a. [Proof of I/ATO] In accordance with DoD instructions (refs. a and b) , no DoD node should be operating without an IATO or ATO (I/ATO). Any attempt to understand the residual risk of an un-accredited node would necessitate a very lengthy period of information collection and assessment. Such delay puts this situation outside of the scope of the JMNO goal of establishing lateral links in as expeditious manner. Each node representative should be able to provide a copy of his own node's certification letter to the other node's representative, providing proof of possession of an I/ATO. No lateral links should be established to any node that does not possess a current (un-expired) I/ATO that resulted from undergoing the official DoD sanctioned C&A process (DITSCAP or DIACAP).

7.b. [Mutual Inspection of SSAAs] Mere possession of an I/ATO is likely to be less than confidence inspiring given the perceived (or actual) disparities in overall quality that went into the certification effort. Step 7.b provides a means of quality assurance verification by calling for both node's IA representatives to inspect the other's System Security Authorization Agreement (SSAA). The SSAA is the document that embodies the certification effort, and documents its results. It is an obvious choice for any quality assurance effort directed at the certification effort. Any node with an I/ATO must have an SSAA (or DIACAP "score card"). This document should—by design—provide a very clear picture of the node's security posture and level of IA robustness. See references (a), (b), and (c), for thorough coverage of an SSAA's contents. If the entire SSAA is not to be scrutinized, good choices for a more narrow review are listed next.

SSAA Appendix F – Certification Results. Note that this appendix may occur under a different letter than 'F'.

SSAA Appendix G – Risk Assessment Results. Note that this appendix may occur under a different letter than 'G'.

SSAA Appendix Q – Residual Risk Assessment Results. Note that this appendix may occur under a different letter than 'Q'.

7.c. [Spot-check IA Policy Adherence] This is the second part of the quality assurance portion of the IA TTP, and like the first, is intended to imbue trust in both node representatives regarding the IA robustness, and "correctness" of the other node. That is, in step 7.b (above), the quality of the certification effort was open for scrutiny via review of the SSAA or some select appendix(ces) subset thereof. This provided some quality assurance regarding IA robustness. By now turning the scrutiny to a spot-check of how well the other node is adhering to the joint IA policy, each node representative may obtain further confidence in the other node's IA robustness, and how well it has mapped its IA controls to the actual IA policy currently in place. Exactly how many policy bullets are chosen for the spot-check is at the discretion of each node representative, but a nominal "dozen" is suggested as a "good-faith" starting point. If several failures are detected from this nominal twelve randomly chosen list of policy bullets, then the evaluating node representative may likely ask to evaluate a longer list of bullets. The pass/fail decision of this spot-check is also left to the discretion of each node representative, though this TTP suggests 85% as the minimum passing score. Command judgment must be exercised in weighing operational necessity/advantage with the detrimental impact of increased risk exposure.

7.d. [Evaluate Discretionary IA Policy Items] Though it is reasonable for any policy to offer some flexibility regarding its interpretation and/or application, these potential disparities should be of concern to both interconnecting node participants. **Appendix 3: The IA Policy Disparity Checklist** was developed by conducting a top to bottom review of the currently proposed Joint IA Policy (produced by the Joint On-demand Interoperability Network—JOIN), looking for any instances where the policy either: a) left room for interpretation, or b) left specific decisions regarding IA control implementation to the node representative or local DAA, to be applied on a case by case basis. Each item in the appendix highlights where there could be a potential policy implementation disparity that would be of concern to one or both node representatives. For each item, both node representatives should discuss their respective node's implementation in order to identify any possible points of contention. For example, any contentions that are identified can be reconciled by any mutually agreeable means that does not violate the underlying policy. Failure to reconcile any one or more policy disparities may result in one or both node representatives denying further efforts to establish a connection. Note that **Appendix 6: Joint IA Policy** will need to be updated whenever the IA policy is changed.

7.e. [Decision to Approve the Link] Each node representative must consider all available information to arrive at a decision regarding whether there is sufficient trust in the IA robustness of the other node to agree to the establishment of a lateral link to support the proposed JIERs. The representatives must consider: the details of the JIERs (for example, pass-through versus shared, and PPS codes), CL and MAC disparities—if any—and the results of evaluating the other node's certification effort, and policy adherence when arriving at their decision.

8. [Establishment of Key(s) for Secure Tunnel Establishment] Having decided to go forth with the link establishment, the issue of keys must be addressed. It is likely that key material required for secure communications has been promulgated in an appropriate appendix or annex of the OpOrder/OpPlan in effect for the theater of operation. If this is the case, the node IA representatives should utilize the established procedure outlined in that reference to retrieve the appropriate keys/codes necessary to create secure tunnel connections for the NTN, UCN, or UTN link as appropriate. If this is not the case, then a simple "field expedient" solution is to have both nodes' authorized representatives meet in person to establish/choose an appropriately strong pre-shared secret with which to authenticate and negotiate the secure tunnel solution. These secrets can be documented in the IA MOA, or saved to some other location that is approved for such use. It is important to note, that if any actual keys are listed in the IA MOA, the IA MOA immediately takes on the sensitivity level of the most sensitive information transiting the tunnel, and should be afforded the appropriate protection.

Appendix 5: Lateral Link Interconnect IA MOA has been designed so as to walk any two nodes' IA representatives through the eight step lateral link negotiation process just described. Successfully working through this IA MOA will result in both nodes' IA representatives (or their appropriate superiors) signing the MOA, and thus approving the security steps taken to mitigate the additional risk inherent in establishing the lateral link. Alternatively, if any irreconcilable issues surface during the negotiation process, these will also be documented in the IA MOA, and approving signatures will not be provided. The approved lateral link must continue to adhere to any and all conditions specified in the IA MOA , as well as all established JCS and DoD IA policy and guidance, while it is in existence.

Appendix 1: Planning JMNO Access Control Lists (ACLs)

JMNO ACLs provide boundary security and errant routing troubleshooting. While JMNO TTP assume that all Service components are employing proper IA controls at higher echelons, JMNO LLC ACLs serve as early warnings of unknown and/or hostile IP traffic coming over an LLC. If the suspect traffic is detected the administrator will work with the distant end administrator to resolve the problem.

ACLs on JMNO LLCs are a requirement of the IA Analysis (See **Section 4.2.5 Information Assurance Analysis**). ACLs will be used to filter incoming traffic, limiting it to only traffic that was approved during the IA Analysis and documented in the JMNO IA Memorandum of Agreement (MOA). JMNO ACLs are applied on the tactical routers at either end of the lateral link connection. Properly configured ACLs on these routers sufficiently secure the Purple Zone. This appendix discusses planning ACLs and Appendix 2 provides implementation instructions for using standard and extended ACLs.

For an exercise or operation, JMNO ACLs will be prepared based on available IP network diagrams. The high-level strategy for inbound ACLs is to permit all IP traffic from specific, other-Service tactical networks to specific subnets within your Service's tactical network and to deny all other traffic; outbound ACLs reverse this strategy. Once these ACLs are in place, network administrators on both ends of LLCs will negotiate additional permissions, as required, based on observed traffic over the LLCs.

JMNO ACLs are applied on the tactical routers at either end of the lateral link connection. If the ACLs are properly designed and implemented, these are the only routers in the Purple Zone that will need ACLs in place.

Once you have implemented ACLs on your tactical router, you can see a summary of hits against each entry in the ACL by using the "show ip access-list" command. This is useful to evaluate the efficiency of your ACLs. Since ACLs are parsed until a match is found, they introduce some overhead in the routing process. In general, place the network entries with the most hits at the top of your ACL and remove any that show no matches.

This page intentionally left blank.

Appendix 2: Implementing Access Control Lists (ACLs)

Figure A-4 Sample Access Control Lists (ACLs) shows ACL sample code used at a Marine Regiment, connecting to an Army Brigade over a serial interface. In this case, both the standard ACL, USA-ABDE-IN, and the extended ACL, USA-ABDE-OUT, would be applied to the serial interface connecting the Marine router to the Army router. The "remark" entries ensure that anyone needing to maintain the ACLs has an understanding of what each entry is intended to do.

In this example, the IP networks that will likely have hosts running C2 applications are:
205.109.53.128 is the US Marine Regiment's internal network
205.109.54.0 is the US Marine Regiment's 1st Battalion network
205.109.54.128 is the US Marine Regiment's 2nd Battalion network
144.106.246.0 US Army Brigade's internal network
144.106.247.128 JNN Brigade's 1st Battalion network
144.106.247.192 JNN Brigade's 2nd Battalion network

Inclusion of the "plumbing" IP networks (point to point links, TDMA and VPN routers, etc.) allows traceroute commands to show hops along the way.

Building and Applying ACLs

Using the IP subnets identified during the LLC planning process, and the sample ACLs shown here, build and implement JMNO ACLs as follows:

1) Cut and paste the sample text into Windows Notepad, as you will need a pure ASCII text file to copy to the router console.
2) Based on the flow of the Joint Information Exchange Requirement (JIER) driving implementation of the LLC, modify the sample ACL code to support these flows.
3) After logging into your router as an administrator via virtual terminal (VTY), ensure you are in ENABLE mode and enter "config t"
4) From the hyer-terminal top menu, select "Edit" and "Paste to Host" and then navigate to the text file you have prepared. You will see a batch-file-like action on the screen.
5) Use "CTRL+Z" to close the configuration session, when enter "wri mem" to save the new configuration to memory.
6) To verify that your ACLs were properly built, use the "sho ip access-list" command.
7) If you are satisfied that your ACLs are properly built, apply them to the applicable interface as shown in the below sample commands:

```
Conf t
interface Serial2/2 (or whatever one goes to Army)
 ip access-group USA-ABDE-IN in
 ip access-group USA-ABDE-OUT out
 CTRL+Z
Wri mem
```

```
ip access-list standard USA-ABDE-IN
 remark 10.10.0.0 net is the point to point (PTP) link between the services:
 permit 10.10.0.0 0.0.0.3
 remark 172.21.0.0 IS THE USA JNN TDMA ROUTER NET
 permit 172.21.0.0 0.0.255.255
 remark 172.28.0.0 is the USA JNN VPN ROUTER NET
 permit 172.28.0.0 0.0.255.255
 remark 144.106.246 IS THE USA JNN BRIGADE NET
 permit 144.106.246.0 0.0.0.255
 remark 144.106.247.128 and .192 ARE THE USA JNN 1stBN/2ndBN NETs
 permit 144.106.247.128 0.0.0.31
 permit 144.106.247.192 0.0.0.31
 deny   any log
ip access-list extended USA-ABDE-OUT
 remark 73REG to JNN BCT PTP
 permit ip 10.10.0.0 0.0.0.3 any
 remark 1stBN-RTR PTP to JNN BCT/BN SUBNETS
 permit ip 205.109.53.4 0.0.0.3 144.106.246.0 0.0.0.255
 permit ip 205.109.53.4 0.0.0.3 144.106.247.128 0.0.0.31
 permit ip 205.109.53.4 0.0.0.3 144.106.247.192 0.0.0.31
 remark 1stBn Internal Network is 205.109.54.0/25
 permit ip 205.109.54.0 0.0.0.127 144.106.246.0 0.0.0.255
 permit ip 205.109.54.0 0.0.0.127 144.106.247.128 0.0.0.31
 permit ip 205.109.54.0 0.0.0.127 10.10.0.0 0.0.0.3
 remark 2ndBN-RTR PTP to JNN BCT/BN   SUBNETS
 permit ip 205.109.53.8 0.0.0.3 144.106.246.0 0.0.0.255
 permit ip 205.109.53.8 0.0.0.3 144.106.247.128 0.0.0.31
 permit ip 205.109.53.8 0.0.0.3 144.106.247.208 0.0.0.31
 permit ip 205.109.53.8 0.0.0.3 10.10.0.0 0.0.0.3
 remark 2ndBn Internal Network is 205.109.54.128/25
 permit ip 205.109.54.128 0.0.0.127 144.106.246.0 0.0.0.255
 permit ip 205.109.54.128 0.0.0.127 144.106.247.128 0.0.0.31
 permit ip 205.109.54.128 0.0.0.127 144.106.247.208 0.0.0.31
 permit ip 205.109.54.128 0.0.0.127 10.10.0.0 0.0.0.3
 remark 73REG SMARTBITS to JNN BCT/BN SUBNETS
 remark 205.109.53.128/28 is the Regimental Internal Net
 permit ip 205.109.53.128 0.0.0.15 144.106.246.0 0.0.0.255
 permit ip 205.109.53.128 0.0.0.15 144.106.247.128 0.0.0.31
 permit ip 205.109.53.128 0.0.0.15 144.106.247.208 0.0.0.31
 remark DENY ALL OTHER TRAFFIC
 deny   ip any any log
```

Figure A-4 Sample Access Control Lists (ACLs)

Appendix 3: The IA Policy Disparity Checklist

The intent of this appendix is to bring to the attention of node representatives who are working through IA TTP in contemplation of creating a lateral link connection, areas of **APPENDIX 6: JOINT IA POLICY** that leave some room for flexibility in how they are implemented and/or enforced.

Though some level of flexibility is good for dealing with the myriad variations that are encountered in complex IT security environments, the specific implementations adopted by an individual node, or permitted by a DAA for a particular node in a particular environment; may be cause for concern to another node that will be connecting to it.

The checklist below is specific to the version of the Joint IA policy. In absence of such a policy disparity checklist, node representatives could work through this issue by conducting their own top-down review of whatever policy is currently in effect.

In the current Joint IA Policy (Appendix 6), 27 potential points of policy disparity were identified. Both node representatives should address each, and make a determination as to whether either of their implementations causes concern for the other. If the policy item raises no concerns, it is ignored. If the policy item does raise a concern, the two representatives should work towards reconciliation. Any sufficiently egregious concern could result in one or both node representatives denying the link.

Items of Potential Policy Disparity Checklist

_____ 1. Par. 2.f – "Need to Know"
_____ 2. Par. 2.g(6) – DAA approval of non-DOD systems
_____ 3. Par. 2.h(1)(d) – Contractor procured storage
_____ 4. Par. 2.h.(3) – How often are anti-virus updates done
_____ 5. Par. 2.h.(5) – Baseline software installations use of Gold/Platinum disks
_____ 6. Par. 2.i.(2) – Patch management procedures
_____ 7. Par. 2.j.(1) – DAA permission to use wireless palmtops
_____ 8. Par. 2.q.(2) & (6) SSO declassification procedures
_____ 9. Tab A, Par. 3.a.(3) – Circuit Security Level
_____ 10. Tab A, Par. 3.a.(5) – Non-secure telephones
_____ 11. Tab B, Par. 3.a.(3) – Computers connected to Internet
_____ 12. Tab B, Par. 3.a.(4) – Measures to eliminate risk of unauthorized disclosure of classified data
_____ 13. Tab B, Par. 3.d.(4) – Firewall rule modification to support any "personal use" services
_____ 14. Tab B, Par. 4.a.(10) – Use of webcams
_____ 15. Tab B, Par. 4.a.(11) – Access to known hacker or "anti-US" sites
_____ 16. Tab B, Par. 4.a.(12) – Access/participation in commercial messaging/chat or other MWR service

_____ 17. Tab D, Par. 13.a. – Remote dial-in access
_____ 18. Tab E, Par. 4.c. – Border routers only permit what is necessary
_____ 19. Tab F, Par. 4.a. – All services registered IAW PPSMP
_____ 20. Tab F, Par. 4.b.(2)(a) – Border filter passing any "RED" PPS
_____ 21. Tab F, Par. 4.b.(2)(b) – Border filter passing any "YELLOW" PPS
_____ 22. Tab G, Par. 3.b. – Remote administration security method (SSHv1, telnet, VPN, etc.)
_____ 23. Tab G, Par. 4.f. – Admin session timeout settings
_____ 24. Tab G, Par. 5.b.(3) and 5.b.(5)(c) – Use of SNMPv1
_____ 25. Tab I – Access to foreign nationals
_____ 26. Tab M, Par. 3.a.(1) – Use of wireless for classified
_____ 27. Tab M, Par. 4. – Wireless devices connected to DOD systems

Appendix 4: The Joint-Militarized Zone (JMZ) Concept

Definition: The JMZ is that sub-domain of a node's network structure that is intended to filter, screen, isolate, monitor, or otherwise neutralize, any risk/robustness disparities between the node it is attached to and any other node that it is connected to for information sharing purposes.

Discussion: The JMZ is related to the DMZ (de-militarized zone) network defense scheme that is widely used with service networks. In the DMZ scheme, a single network domain that contains both private and public resources (such as, workstations and servers) is logically divided into two, with the publicly accessible resources being placed in the less restricted domain (such as, externally initiated traffic is permitted to continuously listening ports/services) which is referred to as the DMZ; and the private resources are placed in the more protected domain (for example, only return traffic to legitimately initiated internal traffic is permitted into the domain). Additionally, the DMZ domain will typically receive much greater detection monitoring (IDS/IPS) than the private domain due to the fact that traffic from unknown Internet hosts is permitted into the DMZ.

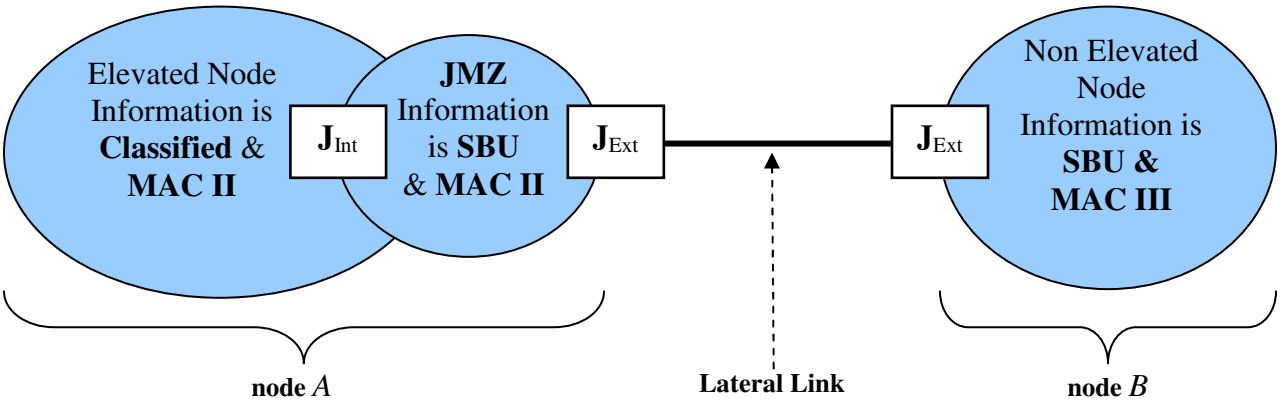
The JMZ scheme deviates from the DMZ in one crucial aspect; connections terminating on resources within the JMZ must originate from known, authenticated, and pre-authorized sources (tactical partners). In common inter-network parlance, this follows the notion of an *extranet*; wherein only connections to known partners are supported. The JMZ serves as a dedicated node sub-domain that can be purposely configured to implement least-privilege access control, and to protect the rest of the host node from any risk associated with connecting to a remote node that has insufficiently robust IA controls for the criticality or sensitivity of the information processed on the local node (for example, a MAC I node connecting to a MAC III node, or a node processing classified information connecting to a node processing unclassified but sensitive information).

All JMNO elevated nodes should be capable of supporting at least one instance of a JMZ, while all JMNO multi-service distribution nodes should be capable of supporting multiple instances of JMZs. By multiple instances, we mean either logical or physical. There is nothing, explicit or implicit, in this IA TTP that precludes a non elevated node from administering a JMZ; however, due to equipment and personnel limitations, this situation is unlikely.

Role of the JMZ in the IA TTP: The lateral link IA issue is largely restricted to that of node boundary protection. It is the role of the JMZ to enforce the appropriate boundary protection, where "appropriate" is determined by the disparity in how well each participating node protects its own information (that is, the robustness of its IA controls); which in turn, is largely determined by the criticality and sensitivity of the information processed by each node. This is described in much greater detail in reference (f). When implemented and managed properly in cross-domain (that is, dissimilar confidentiality levels) situations, the JMZ should either provide an appropriate "downgrading" function, so as to permit traffic flow from the otherwise "high" node that the JMZ is connected to, to a "low" node; or provide a one-way "diode" switch that ensures that data may only flow from the "low" to the "high" node. When implemented and managed properly in cross-MAC situations, the JMZ should provide an appropriate "upgrading"

function so as to permit traffic flow from the "low" integrity node, to the "high" integrity node that the JMZ is connected to. For "like" nodes (that is, both process classified information and are MAC II), the JMZ will only be required to host a security tunnel gateway (for example, VPN gateway), routing functionality, and an ACL packet filtering capability sufficient to enforce applicable network access control policy, and appropriate PPSM (ref. h).

Figure A-5 depicts two nodes (*A* and *B*). Node *A* is an elevated node and is thus responsible for supporting at least one instance of a JMZ. Node *B* is not an elevated node, but should be able to connect to one. According to this depiction, node *A* processes information that is both, more critical and more sensitive than that of node *B*. As per standard DOD IA policy, node *A* would have more robust IA controls than node *B*. Without the ability to manage a proper JMZ, node *A* would be compelled by policy to deny the lateral connection to the "riskier" information protection environment presented by node *B*.



J_{Int} = JMZ Internal boundary solution = automated downgrading (CDS) if applicable & available
J_{Ext} = JMZ External boundary solution = secure tunneling (VPN) and filtering (firewall)
JMZ = Node sub-domain where any necessary manual (human) up-/down-grading occurs, and shared data may be "staged" prior to movement into or out of the host domain

Figure A-5 High-level View of JMZ

> *The set of IA Controls applicable to any given DoD information system is always a combination of the IA Controls for its mission assurance category and the IA Controls for its confidentiality level…*
> *- DoDI 8500.2 Par. E4.1.6.*

During steps 5 and 6 of the IA TTP process, the system characterization of both nodes is compared to determine the JMZ design needed to support a secure lateral link. The system characterizations are taken from reference (f). In accordance with reference (f), all DoD nodes are assigned to one of three classification levels (CL): public, sensitive, and classified, and to one of three mission assurance categories (MAC): MAC I, MAC II, and MAC III. While the CL deals with the sensitivity of information processed by a node, the MAC deals with the level of required integrity, authenticity, non-repudiation, and availability of the information processed by a node.

Threats to confidentiality arise from any accidental or malicious action which results in an unauthorized disclosure of information to un-cleared personnel, and/or personnel with no genuine need-to-know. In simple terms, information should never flow from "high" to "low" (such as, secret information should never be written to unclassified media, or read by un-cleared personnel). Though we may not wish the reverse (such as, unclassified information being written to classified media) to occur, there is no direct threat to an unauthorized disclosure. Given this, it is clear that the owner of the "high" side of any information flow is responsible for ensuring that her information never flows "down", unless appropriately downgraded beforehand.

Threats to integrity, authenticity, non-repudiation, and availability arise from any accidental or malicious action which results in an unauthorized modification of (integrity), unauthorized introduction of (authenticity), unauthorized destruction of (availability), or delayed access to (availability) information; or the ability of a person or process to deny having participated in any transaction for which he/it did in fact participate (non-repudiation). Though the particulars of the threats to each of these four information security attributes are somewhat unique, their commonality is what is of interest here. Unlike the threat to confidentiality, all of these threats are "inbound" threats; or "*flow-to*" threats as opposed to "*flow-from*" threats: an attacker writes to your media, new information (authenticity threat), or he modifies the information on your media (integrity threat), or he causes an action against your media or its processing/storing infrastructure to reduce its timely availability to authorized users. Given this, it is clear that the owner of information who is concerned about the veracity and availability of his information, should take measures to ensure redundancy and controlled modification access to that information.

Tables A-1 and A-2 illustrate the possible node comparisons for both CL (a confidentiality, or "*flow-from*" concern) and MAC (integrity, authenticity, non-repudiation, and availability, or "*flow-to*" concerns).

Table A-1. CL Disparity Pairs

	Public	**Sensitive**	**Classified**
Classified	***A4-A6 & NTK***	***A4-A5 & NTK***	***NTK***
Sensitive	***A5-A6 & NTK***	***NTK***	
Public	***NTK***		

Table A-2. MAC Disparity Pairs

	MAC III	**MAC II**	**MAC I**
MAC I	***A1-A3 & NTW***	***A1-A2 & NTW***	***NTW***
MAC II	***A2-A3 & NTW***	***NTW***	
MAC III	***NTW***		

The *A#* notation seen in these tables' entries refer to attachments A1 through A6 of Enclosure 4 of reference (f). These attachments represent collections of IA controls that are appropriate to meet the minimal protection requirements for each of the CLs and MACs. These IA control collections are mapped directly to the MACs and CLs as follows: MAC I → A1, MAC II → A2, MAC III → A3, Classified → A4, Sensitive → A5, Public → A6. The "hyphen" between each attachment pair connotes set subtraction, which will be further explained in the following

paragraphs. The *NTK* entry refers to the *need-to-know* policy that is employed when separating different categories or compartments (vice classification levels) of information. The *NTW* entry refers to a *need-to-write* policy that is introduced by this IA TTP, and is employed in furtherance of the least-privilege principle as it pertains directly to data introduction (authenticity) or data modification (integrity). Combining the four possible CL disparity pairs with the four possible MAC disparity pairs yields 16 possible IA risk/robustness disparity combinations.

JMZ Design

Figure A-6 elaborates on the JMZ portion of Figure A-5, by providing more detail about the roles played by $\mathbf{J}_{Int}$ (left side of JMZ), $\mathbf{J}_{Ext}$ (right side of JMZ), and the JMZ domain/subnet itself.

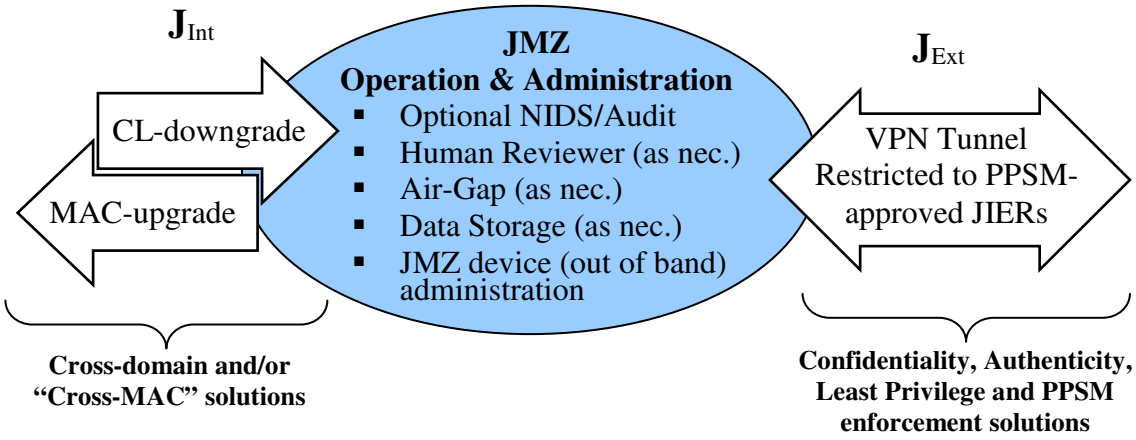


Figure A-6 Operational View of JMZ

Figure A-6 illustrates the most robust version of a lateral link JMZ in that it employs: a) a CL-downgrade action (implying this node processes a higher CL than the other), b) a MAC-upgrade action (implying this node runs at a higher MAC), c) an actual, separate, JMZ subnet, and d) the always present secure tunnel and least-privilege traffic enforcement that must occur on the external interface (J_{Ext}).

Generally, the separate JMZ subnet is recommended by default whenever there is a CL or MAC disparity, unless, the traffic flow is in only one direction, and that direction could not result in a security violation (such as, if information will only flow from a low CL node to high CL node, or only flow from a high MAC node to low MAC node). This recommendation owes to the typical cross-domain (guard) implementation that employs a temporary "buffer" area (such as, guard server hosted in a JMZ/DMZ subnet, or "dual-homed" guard) where downgrading occurs. If no approved CDS (ref. i) is available, an authorized human reviewer will be needed, and the JMZ subnet will simply be an air-gap where the human reviewer processes high-to-low data, and "sneaker-nets" the processed information to the outgoing interface.

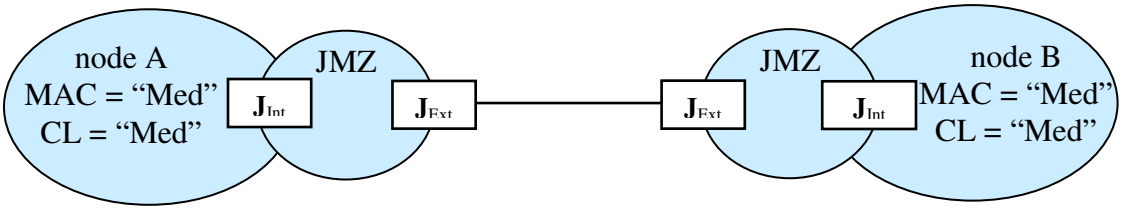
In cases where there is no need for either upgrading or downgrading, the JMZ solution may "collapse" to only the J_{Ext} interface; where appropriate secure tunnel processing and least-privilege/JIER-only traffic enforcement is accomplished. Larger nodes that are tasked to serve as elevated nodes or MDNs, may likely choose—as a matter of TTP—to administer a permanent JMZ that is sufficiently flexible so as to accommodate most if not all possible lateral link situations likely to occur at the tier 7/8 level.

The illustrations and accompanying discussions that follow cover every combination of JMZ design consideration.

Node with a JMZ connecting to another node with a JMZ, and . . . (see 1-4)

DoD PPSM refers to this as "enclave DMZ to enclave DMZ", and references (g) and (h) do not require any PPS filtering in this situation (reference Table 3 on page 9 of reference (h)).

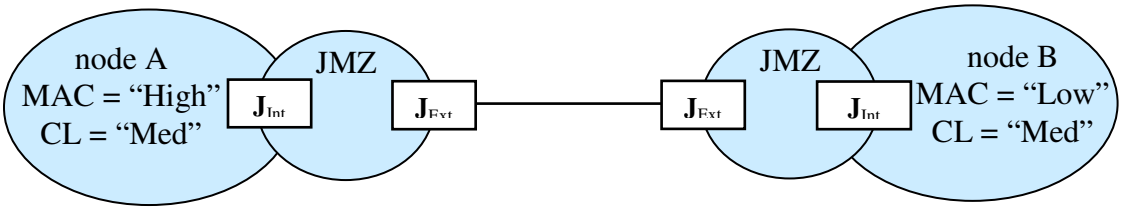
1. No MAC disparity and no CL disparity



J_{Int} – Nothing required
J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic

J_{Int} – Nothing required
J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic

2. A MAC disparity, no CL disparity

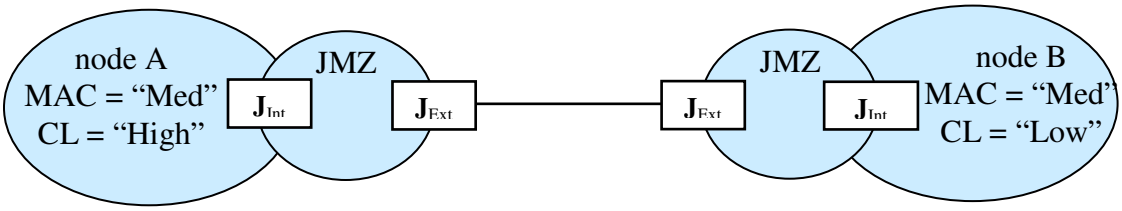


J_{Int} – Nothing required if **<u>only</u>** from A-to-B
JMZ – If **<u>some</u>** from B-to-A, must perform manual "upgrade"
J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic

J_{Int} – Nothing required

J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic

3. A CL disparity, no MAC disparity



J_{Int} – If **only** from B-to-A, must employ a one-way transfer (OWT) solution (cheaper) or other CDS solution (see ref. i)
J_{Int} – If **some** from A-to-B, must perform "downgrade" either via approved CDS solutions (see ref. i) or manually within the JMZ
J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic

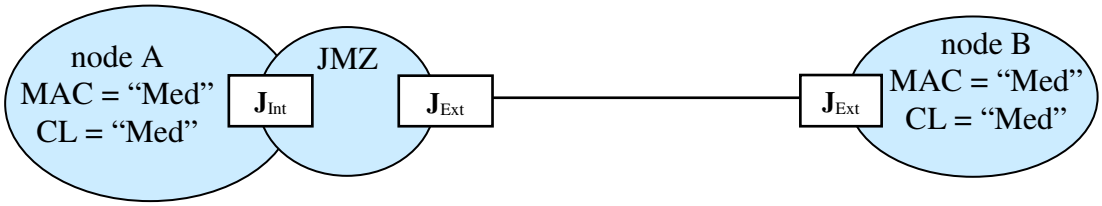
J_{Int} – Nothing required

J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic

4. Both MAC and CL disparities (combine solution designs in 2 and 3)
Node with a JMZ connecting to an node with no JMZ, and . . . (see 5-8)

*Traffic flowing from A-to-B is restricted to green or yellow PPS listed in column 11 of the PPS Category Assignments List (ref. h). Traffic flowing from B-to-A is restricted to green or yellow PPS listed in column 12 of the PPS Category Assignments List (ref. h).

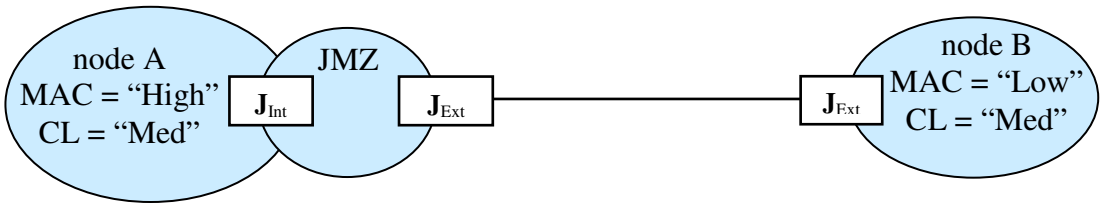
5. No MAC disparity and no CL disparity



J_{Int} – Nothing required
J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved*

J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved*

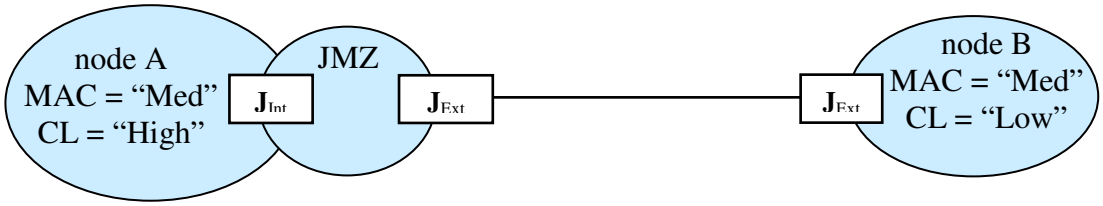
6. A MAC disparity, no CL disparity



J_{Int} – Nothing required if **only** from A-to-B
JMZ – If **some** from B-to-A, must perform manual "upgrade"
J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved*

J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved*

7. A CL disparity, no MAC disparity



J_{Int} – If **only** from B-to-A, must employ a one-way transfer (OWT) solution (cheaper) or other CDS solution (see ref. i)
J_{Int} – If **some** from A-to-B, must perform "downgrade" either via approved CDS solutions (see ref. i), or manually within the JMZ
J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved*

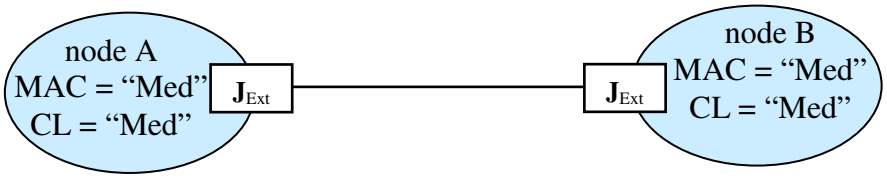
J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved*

8. Both MAC and CL disparities (combine solution designs in 6 and 7)

Node with no JMZ connecting to another node with no JMZ, and . . . (see 9-12)

**Traffic flowing in either direction restricted to green or yellow PPS listed in column 16 of the PPS Category Assignments List (ref. h).

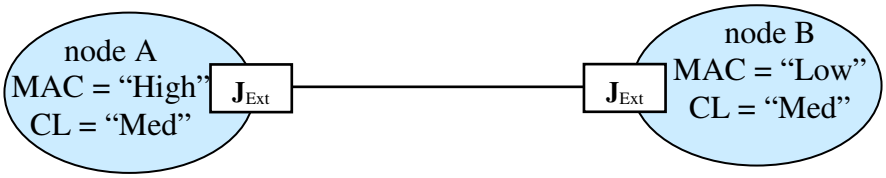
9. No MAC disparity and no CL disparity



J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved**

J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved**

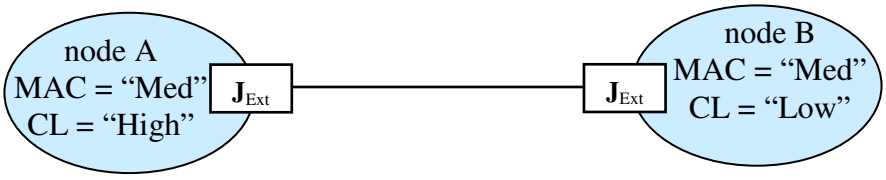
10. A MAC disparity, no CL disparity



J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved**
JMZ – If **some** traffic from B-to-A, must be able to "buffer" data for "upgrade" at the interface, or have node representative accept additional risk to integrity and availability

J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved**

11. A CL disparity, no MAC disparity



J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved**
J_{Ext} – If **only** from B-to-A, must employ a one-way transfer (OWT) solution (cheaper) or other CDS solution (see ref. i)
J_{Int} – If **some** from A-to-B, must perform "downgrade" either via approved CDS solutions (see ref. i) or manually within the JMZ

J_{Ext} – Implements a secure tunnel
J_{Ext} – Only permits JIER traffic that is PPS approved**

12. Both MAC and CL disparities (combine solution designs in 10 and 11)

Additional JMZ design considerations may be derived from the IA control assignments ascribed to each of the three CL and MAC levels as specified in Enclosure 4 of reference (f). In addition to mapping a collection of IA controls to each CL and MAC, Enclosure 4 also categorizes all IA controls into eight subject areas. **Table A-3 DoDI 8500.2 IA Control Subject Areas** is borrowed from that enclosure.

Table A-3 DoDI 8500.2 IA Control Subject Areas

ABBREVIATION	SUBJECT AREA NAME	# OF CONTROLS
DC	Security Design & Configuration	31
IA	**Identification & Authentication**	**9**
EC	**Enclave & Computing Environment**	**48**
EB	**Enclave Boundary Defense**	**8**
PE	Physical & Environmental	27
PR	**Personnel**	**7**
CO	**Continuity**	**24**
VI	Vulnerability & Incident Management	3

The bolded/un-shaded entries indicate the areas of IA controls that are appropriate for the boundary defense nature of the JMNO lateral link issue, and it is thus within only these five IA control subject areas that design issues pertaining to the JMZ can be focused.

Both node representatives may wish to do additional IA robustness comparisons before deciding on the final JMZ solution, and/or any other IA requirements that they may deem appropriate for the security of the contemplated lateral link. The tables that follow were derived by comparing the collections of IA controls found in Attachments A1 through A6 in reference (f), across each of the five un-shaded IA control subject areas in Table A-3. Continuing with the example presented in Figure A-5, the comparison would proceed as follows:

Sample node A: CL = Classified (such as, Secret), MAC = II
Sample node B: CL = Sensitive (for example, FOUO & Foreign Govt), MAC = III

CL Disparity = A4–A5, MAC Disparity = A2–A3

JMZ Requirements will be derived as a function of:
1) The difference A4(IA, EC, EB, PR, CO) – A5(IA, EC, EB, PR, CO) for CL and…
2) The difference A2(IA, EC, EB, PR, CO) – A3(IA, EC, EB, PR, CO) for MAC

Referring back to Tables A-1 and A-2 previously provided, four CL disparities (*A4-A6*, *A4-A5*, *A5-A6, NTK*) and four MAC disparities (*A1-A3*, *A1-A2*, *A2-A3, NTW*) were identified. The following are the results of these set subtractions using the same IA control notation used in reference (f). The node representatives may use this information as they see fit; it is included in the IA TTP as a convenience for quick reference.

MAC I-III (A1-A3) Disparity Summaries
for the *IA*, *EC*, *EB*, *CO*, and *PR* IA Controls (See Ref. f)

NOTE: If an entry (***IA***, ***EC***, ***EB***, ***CO***, ***PR***) does not appear in a table, this indicates that there were no disparities for that IA Subject Area in the indicated reference (f) attachments.

MAC Disparity A1-A3 & Need-to-Write	
IA	A1{TS-2} A3{TS-1, KM-1}
EC	A1{AT-2, CD-2, DC-1, ID-1, ND-2, PC-2, SD-2, TB-1, TM-2} A3{AT-1, CD-1, ND-1, PC-1, SD-1, TM-1},
CO	A1{AS-2, DB-3, DP-3, EB-2, ED-2, EF-2, MS-2, PS-3, SP-2} A3{AS-1, DB-1, DP-1, EB-1, ED-1, EF-1, MS-1, PS-1, SP-1}

MAC Disparity A1-A2 & Need-to-Write	
CO	A1{DB-3, DP-3, EB-2, ED-2, PS-3, SP-2} A2{DB-2, DP-2, EB-1, ED-1, PS-2, SP-1}

MAC Disparity A2-A3 & Need-to-Write	
IA	A2{TS-2} A3{TS-1, KM-1}
EC	A2{AT-2, CD-2, DC-1, ID-1, ND-2, PC-2, SD-2, TB-1, TM-2} A3{AT-1, CD-1, ND-1, PC-1, SD-1, TM-1},
CO	A2{AS-2, DB-2, DP-2, EF-2, MS-2, PS-2} A3{AS-1, DB-1, DP-1, EF-1, MS-1, PS-1}

CL (Classified [A4], SBU [A5], Public [A6]) Disparity Summaries for the *IA*, *EC*, *EB*, *CO*, and *PR* IA Controls (See Ref. f)

Note: If an entry (***IA***, ***EC***, ***EB***, ***CO***, ***PR***) does not appear in a table, this indicates that there were no disparities for that IA Subject Area in the indicated reference (f) attachments.

CL Disparity A4-A6 & Need-to-Know	
IA	A4{GA-1, IA-2, KM-3, AC-1} A6{}
EC	A4{AD-1, AN-1, AR-3, AT-2, CD-2, CM-1, CR-2/3, CT-2, IC-1, LC-1, L0-2, ML-1, MT-2, NK-1/2, RC-1, TB-1, TC-1} A6{AR-1, AT-1, LP-1, MT-1}
EB	A4{BD-3, RP-1, RU-1} A6{BD-1, PW-1}
PR	A4{AS-2, MP-2, TN-1} A6{MP-1}

CL Disparity A4-A5 & Need-to-Know	
IA	A4{IA-2, KM-3} A5{IA-1}
EC	A4{AR-3, AT-2, CD-2, CM-1, CR-2/3, CT-2, LC-1, LO-2, MT-2, NK-1/2, TB-1} A5{AR-2, AT-1, CR-1, CT-1, LO-1, MT-1, NK-1}
EB	A4{BD-3} A5{DB-2, PW-1}
PR	A4{AS-2, MP-2} A5{AS-1, MP-1}

CL Disparity A5-A6 & Need-to-Know	
IA	A5{IA-1}
EC	A5{AD-1, AN-1, AR-2, CR-1, CT-1, IC-1, LO-1, ML-1, NK-1, RC-1, TC-1} A6{ AR-1, }
EB	A5{BD-2, RP-1, RU-1} A6{BD-1}

This page intentionally left blank.

Appendix 5: Lateral Link Interconnect IA MOA

Section I – MOA Overview

Purpose: This appendix is intended to capture all security-relevant coordination information pertaining to the proposed establishment of a lateral link between any two data processing nodes; as described in the main JMNO TTP document. It is intended that duly appointed and authorized IA representatives from both nodes will work through this MOA document with the intended outcomes of: 1) establishing mutual security confidence between the two nodes, 2) identifying any reason why the link, or any proposed JIERs, should not be accepted, and 3) capturing any conditions or stipulations under which the link and the proposed JIERs are to be managed with respect to risk mitigation.

High-level Outline: This MOA should be completed from top to bottom. When completed, one or both node representatives will decide that either: a) the proposed link is too risky to create, or b) creation of the link is safe, but one or more of JIERs are too risky to permit, or c) both the link and all designated JIERs can be establishment with sufficient confidence given the steps taken to identify and mitigate any new risks to their node. The sections are organized as follows:

Section I – MOA Overview

Section II – System ID and Points of Contact

Section III – Promulgated JIERs and User Cross-Network Links

Section IV – Cross-Domain (and Cross-MAC) Consideration

Section V – Establishing/Improving Mutual Trust

Section VI – Secure Tunnel Key(s) Establishment

Section VII – IA MOA Summarization

Section VIII – Record of MOA Changes

Discussion: It should be openly stated for clarification, that this MOA is not a "how-to" document. Implementing procedures, whether explicitly or implicitly called for in this document, are already available and documented within the DoD/OGA solution space. As a simple example, when the MOA addresses secure tunnels in Section VI, it is expected that each node has sufficiently trained operators/administrators to properly configure the equipment used to implement the secure tunnel end point interfaces. When necessary, the operator/administrator is expected to seek out appropriate instructions or manuals necessary to complete any explicit or implicit tasks. The MOA focuses on *what* needs to be considered, and on the *documentation* thereof. The IA MOA—and the IA TTP from which it is based—serves as a baseline for maintaining the security robustness of separately accredited nodes whose certification boundary did not include any lateral link that is now being contemplated. The purpose of the IA TTP is specifically to provide a way forward given this post-accreditation situation.

Section II – System ID and Points of Contact

Table 1 **System and POC Information** (Note that assignment of 'A' or 'B' to each node is arbitrary but should be "fixed" from this point on)		
	Node 'A'	**Node 'B'**
System Name (Ref. par. 1.1 of SSAA)		
Owning/Operating Agency		
Mission Assurance Category (MAC) (Ref. par. 1.3.2 of SSAA)		
Confidentiality Level (Ref. par. 1.3.3 of SSAA)		
Is node designated a Multi-service Distribution Node (MDN)?		
Contact info for CO/OIC or other person with complete authority for operation of the node*		
Contact info for the primary IA Representative for the node*		
Contact info for person completing this MOA if different from previous*		
Primary technical POC for all matters relating to implementation of this MOA*		
* Provide name, billet, & at least one of either a phone # or email address		

Table 2
Promulgated Joint Information Exchange Requirements (JIERs) for Shared Data

Who or what is the authority for the JIERs that have been promulgated for sharing between the two nodes
(Note: This information is likely published in the Communications Plan Annex—typically Annex K—of the lager Operations Plan)

Authority:

Provide a "plain English" high-level purpose statement regarding the promulgated JIERs (such as, "Node A has been tasked with sharing all flight schedule and cargo manifest information with Node B for purposes of delivery/pick-up logistics coordination.")

Purpose Statement:

List each JIER by annotating its associated Service, transport protocol, port, direction, PPS color code, and any additional notes deemed important for clarification

#	Service/Application	Proto-col(s)	Port(s)	Direction *A→B, B→A, Bi-Dir*	PPS Code* R|Y|G|U	Note(s) **
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

***** PPS color codes (Red, Yellow, Green, or Un-registered) are available at https://powhatan.iiie.disa.mil/ports/cal-6-5.pdf
Note that any unregistered or "red" services will not be permitted without a letter of waiver from the authority listed at the top of this table

****** Enter only numbers (1-?) in this column, then use **Table 3: Additional/Optional Information for Shared JIER Traffic** to provide whatever elaboration is desired for that numbered note

Note # from Table 2	Table 3 Additional/Optional Information for Shared JIER Traffic (if applicable from Table 2)
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	

Examples of useful notes:

Ex. 1. Though service utilizes both UDP and TCP, we intend to only utilize the UDP portion of the service and will thus only permit its UDP through the firewall.

Ex. 2. Though this service requires connection-oriented TCP, which necessitates two-way flow for acknowledgements, we intend to only permit "ack" traffic with zero payload in the B→A direction.

Ex. 3. This service was later "lined-out" due to a cross-domain issue identified in the Dissimilar CL flowchart in Section IV of the MOA. It remains in the list above for historical purposes.

Ex. 4. This service will be classified as "best effort" for QoS bandwidth purposes. In accordance with Tab Q of the current IA policy, this establishes a bandwidth allocation of 25% for this service.

Ex. 5. This is included to facilitate an expected/future user cross-network link (see **Table 4: Promulgated Joint Information Exchange Requirements (JIERs) for Pass-through Data**)

Table 4
Promulgated Joint Information Exchange Requirements (JIERs)
for Pass-through Data

Who or what is the authority for the pass-through JIERs that have been promulgated between the two nodes
(Note: this information is likely published in the Communications Plan Annex—typically Annex K—of the lager Operations Plan)

Authority:

Provide a "plain English" high-level purpose statement regarding the promulgated JIERs (for example, "Node A has been tasked with passing-through all category X JIERs listed in Annex K to the OpOrder."

Purpose Statement:

List each JIER by annotating its associated Service, transport protocol, port, direction, PPS color code, and any additional notes deemed important for clarification

#	Service/Application	Proto-col(s)	Port(s)	Direction *A→B, B→A, Bi-Dir*	PPS Code* R|Y|G|U	Note(s) **
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

***** PPS color codes (Red, Yellow, Green, or Un-registered) are available at https://powhatan.iiie.disa.mil/ports/cal-6-5.pdf
Note that any unregistered or "red" services will not be permitted without a letter of waiver from the authority listed at the top of this table

****** Enter only numbers (1-?) in this column, then use Table 3 on the next page to provide whatever elaboration is desired for that numbered note

Note # from Table 2	Table 5 Additional/Optional Information for Pass Through JIER Traffic (if applicable from Table 4)
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	

Section IV – Cross Domain (and Cross MAC) Consideration

The issue of node confidentiality level (CL) and mission assurance category (MAC) disparity was discussed in **APPENDIX 4: THE JOINT-MILITARIZED ZONE (JMZ) CONCEPT**. A very brief summary is presented here.

Ideally two nodes contemplating a lateral link will be of both the same CL and MAC. This similarity in systems is likely to be reflected in the IA robustness of both nodes, and thus bodes well for mutual trust, and eases concerns over additional risk that would otherwise be the case if interconnecting nodes certified for different levels.

When two data sharing nodes are of different CLs, the "higher" (that is, classified) node must employ an approved guard solution (either automated or manual) that is capable of downgrading classified information for transfer to the "lower" (such as, unclassified but sensitive). In the special case where JIER requirements only necessitate data flow from the "low" node to the "high" node, a slightly simpler solution can be sought in the form of a "one-way" diode type device. Reference (i) in the IA TTP Appendix provides a pointer to such approved solutions. At the time of the writing of this document, DODI 8540.aa (DOD Policy and Procedures for Interconnection of Information Systems of Different Security Domains) is still in draft form. When completed, it should provide additional information in this regard. Pursuing link establishment approval between nodes of different CLs will likely result in longer delays than is typical for "like" CL nodes, owing to the high sensitivity to the risk of data "leakage".

When two data sharing nodes are of different MACs, the "higher (such as, MAC I) node must employ some means of data "upgrade" when using data received from a "lower" (for example, MAC III) node to overwrite shared information objects. In cases where the overwriting information flows only from "high" to "low", no upgrade action is necessary. In cases of information flowing from "low" to "high" that does not involve overwriting high integrity data or processes on the "high" side, no upgrade action is required. There are no known automated "upgrade" solutions, so if such action is required, it must be done manually using all available information to determine if the overwriting, "low" information is of sufficiently high integrity to overwrite existing data on the "high" side.

The JMZ (Joint Militarized Zone) concept was introduced in **APPENDIX 4: THE JOINT-MILITARIZED ZONE (JMZ) CONCEPT** as an IA management construct for dealing with either of these two potential node disparities.

Pass-through only traffic that is passed through using a dedicated "external" interface presents a convenient situation for facilitating a potentially multi-level (that is, multiple CLs) "purple zone". This convenience owes to the fact that encrypted traffic that is simply passed-through—vice decrypted and processed—can be safely passed through a "low" CL node in a high→low→high transfer.

The previous paragraphs highlight the three important points:

1. The importance of traffic flow <u>direction</u> between "dissimilar" nodes

2. The added sensitivity in connecting dissimilar CL, vice dissimilar MAC, nodes
3. The benefits of handling pass-through only traffic on a dedicated "external" interface

Consideration of Dissimilar Confidentiality Levels

Step 1: Look back at **Table 1: System and POC Information**. If a CL disparity does not exist, skip to **Consideration of Dissimilar Mission Assurance Categories** (following **Table 6: Results of Consideration of Dissimilar Confidentiality Levels**).

Step 2: Work through the following flow-chart using JIERs listed in **Table 2**: **Promulgated Joint Information Exchange Requirements (JIERs) for Shared Data** (do **not** use pass-through JIERs listed in **Table 4: Promulgated Joint Information Exchange Requirements (JIERs) for Pass-through Data**)

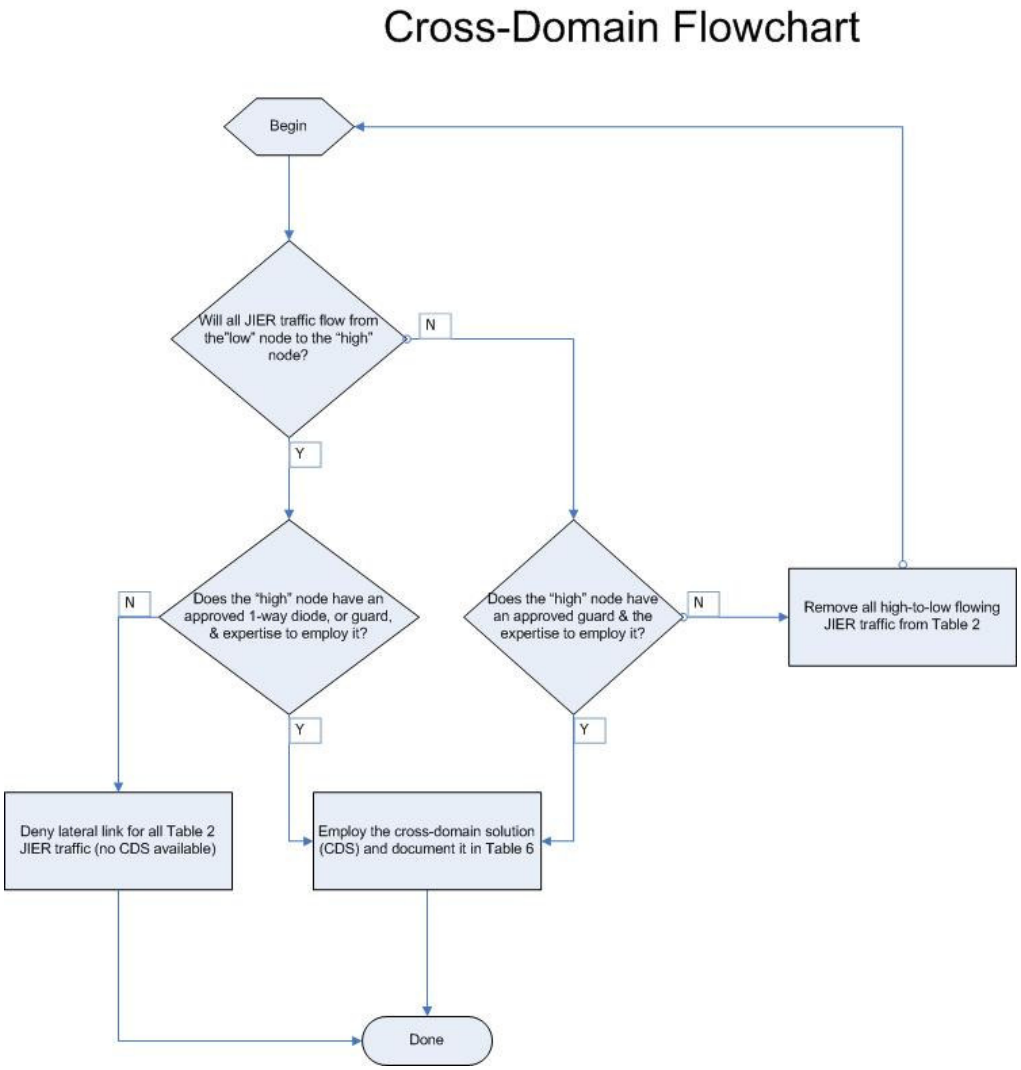


Figure A-7 Cross Domain Flowchart

Table 6 Results of Consideration of Dissimilar Confidentiality Levels	
In the space provided below, write a plain English description that highlights the results of working through the dissimilar confidentiality level flowchart on the previous page. If necessary, each node representative may write separate statements.	Suggested items to address below: ▪ What JIERs were removed from Table 2 ▪ What guard/diode solution was chosen ▪ What role did directionality play ▪ What residual concerns remain ▪ If the link was denied, what remedial action, if any, is being considered

Consideration of Dissimilar Mission Assurance Categories

Step 1: Look back at **Table 1: System and POC Information**. If a MAC disparity does not exist, skip to **Section V** of the MOA.

Step 2: Work through the flow-chart below using JIERs listed in **Table 2**: **Promulgated Joint Information Exchange Requirements (JIERs) for Shared Data** (do **not** use pass-through JIERs listed in **Table 4: Promulgated Joint Information Exchange Requirements (JIERs) for Pass-through Data**)

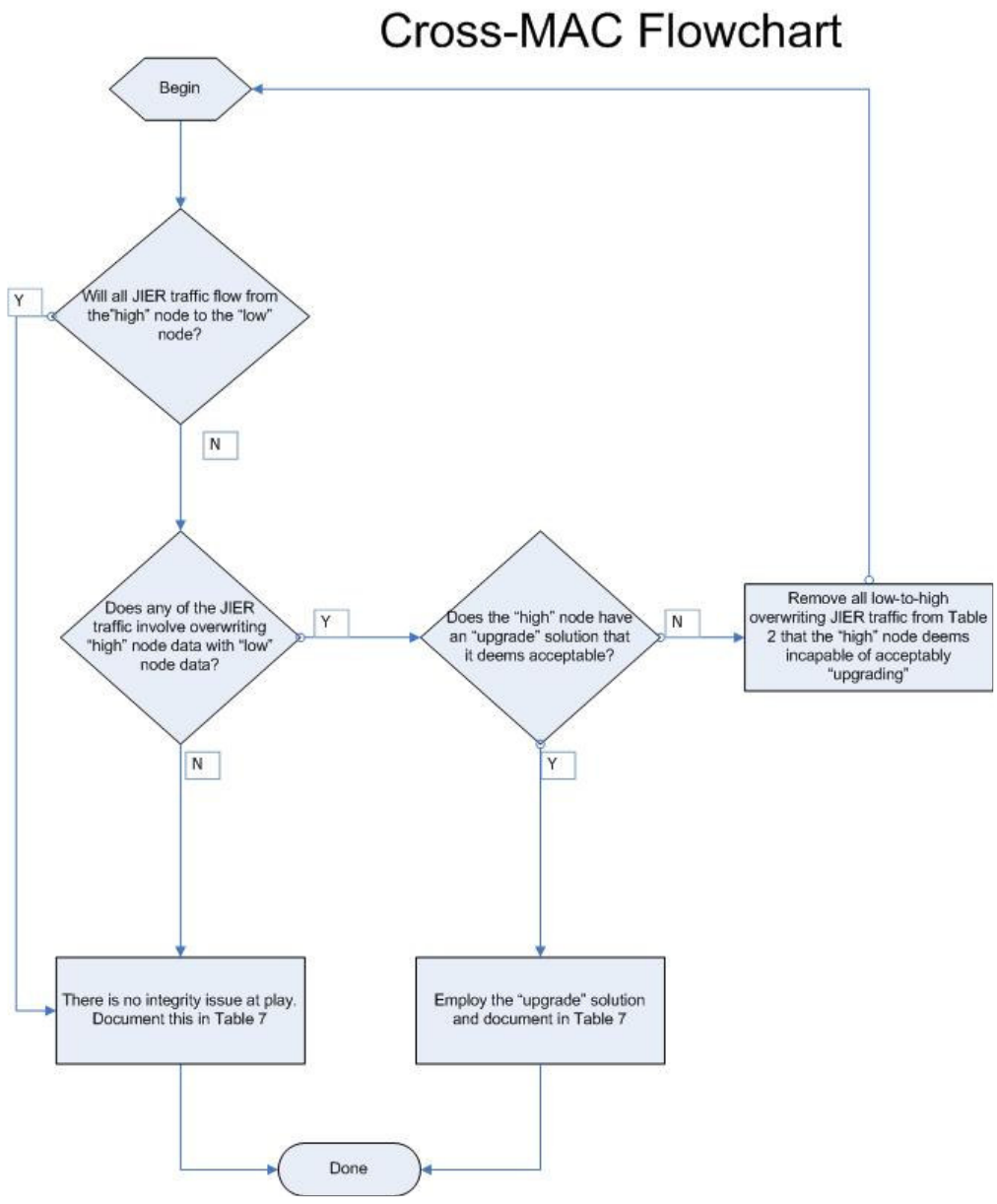


Figure A-8 Cross-MAC Flowchart

Table 7 Results of Consideration of Dissimilar Mission Assurance Categories	
In the space provided below, write a plain English description that highlights the results of working through the dissimilar mission assurance categories flowchart on the previous page. If necessary, each node representative may write separate statements.	Suggested items to address below: ▪ What JIERs were removed from Table 2 ▪ What "upgrade" solution—if any—was chosen ▪ What role did directionality play ▪ What residual concerns remain ▪ If the link was denied, what remedial action, if any, is being considered

Section V – Establishing/Improving Mutual Trust

Discussion: The decision to proceed with the establishment of a link with another node understandably depends heavily on the trust and confidence that each node's owner has regarding the IA robustness of the other node. In an attempt to allay this trust issue, the IA TTP calls for a third party (preferred) or mutual evaluation of SSAAs and IA policy enforcement. The intent is to leverage the work already performed in compliance with the DOD C&A effort (Ref. DoDI 5200.40, short title: "DITSCAP"); and to compare security implementations against the theater-wide, common IA policy.

The node representatives should contact the Marine Corps Operational Test and Evaluation Activity (MCOTEA) at the below address/number, and coordinate an evaluation from one of their field teams.

Marine Corps Operational Test and Evaluation Activity
3035 Barnett Avenue
Quantico, VA 22134
(703)432-0922

Should the MCOTEA not be available to perform a timely third party evaluation, the node representatives may seek another similarly chartered/tasked organization to coordinate a third party evaluation. In the absence of any available qualified third party evaluator, the node representatives may, with authority of their node owners, embark on a mutual evaluation of each node's IA robustness and policy adherence.

In the event a third party evaluation is to be completed, the node representatives should put checks in the appropriate boxes below, include the final report the evaluators provide as an attachment to this MOA, then skip ahead to Section VI of the MOA if the outcome of the evaluation was positive (that is, both node representatives are trustful of the other node's IA robustness and IA policy enforcement). If, instead, the node representatives complete a mutual evaluation, then the boxes below should be left un-checked, and Tables 8, 9, and 10 should be used to record the results of the mutual inspection.

☐ We plan to coordinate a third party evaluation, but have not yet coordinated this with a third party evaluator.

☐ We have scheduled a third party evaluation.

It will be done by: _____ (name of organization)

It will be done on or about: _____ (date: mm/dd/yyyy)

☐ A third party evaluation has been completed, and the report is attached to this MOA.

☐ The outcome was positive and we DO intend to establish the link (skip to **Table 11: Secure Tunnel Key Management**).

☐ The outcome was negative, and this link will not be further pursued (skip to **Table 12**: **IA MOA Summary Table**)

Table 8 Mutual Inspection of SSAAs
Node A Representative: Has a copy of Node B's SSAA been offered for your review? If yes, and you have reviewed it, list any concerns you have regarding any perceived security weakness that you believe may adversely impact your own node's risk if a lateral link connection is made with Node B.
Node B Representative: Has a copy of Node A's SSAA been offered for your review? If yes, and you have reviewed it, list any concerns you have regarding any perceived security weakness that you believe may adversely impact your own node's risk if a lateral link connection is made with Node A.

Table 9 Results of Policy Disparity Checklist (Appendix 3 of JMNO TTP)
Both Node Representatives: Indicate below the results of your discussion with the other Node's representative regarding the potential policy disparity items listed in **Appendix 3** of Annex A of the JMNO TTP. Specifically, if the other Node's interpretation, implementation or enforcement of any item in the checklist is deemed to jeopardize or otherwise weaken your own node's IA policy enforcement posture; document the item by its paragraph number, and indicate whether the item was: accepted, resolved, or deemed a security non-starter (that is, the link will be denied for this reason)
Node A Representative's Statement:
Node B Representative's Statement:

Table 10 **Results of IA Policy Enforcement Spot-Check**		
Both Node Representatives: Indicate below the results of your IA policy enforcement spot-check of the other Node's security practices, procedures and documentation. This is your chance to "audit" the IA policy adherence of the other node, before deciding to accept or deny the potential additional risk that ensues from sharing data and resources via a lateral link. **At a minimum, you should pick at least 12 items** from the joint IA policy. The chosen items may be random, or concentrated on areas of particular import to the security of your node. For every "failure", you should select four additional policy items to check. Check up to 30 items in this manner. When complete with however many items you check, ensure a ***passed*** to ***total-checked*** ratio/score of at least 85%. List all items checked below along with the result (pass/fail), and the final score. There will be some subjectivity in this evaluation, and your procedures may differ somewhat as the situation warrants. Use good judgment.		
Node A Representative's Statement:		
#items checked by A:	**#items passed:**	**Score (passed/checked):**
Node B Representative's Statement:		
#items checked by B:	**#items passed:**	**Score (passed/checked):**

Section VI – Secure Tunnel Key(s) Establishment

Discussion: It is likely that key material required for secure communications has been promulgated in an appropriate appendix or annex of the OpOrder (OpPlan) in effect for the local theater of operation. If this is the case, utilize the established procedure outlined in that reference to retrieve the appropriate keys/codes necessary to create secure tunnel connections for the NTN or UCN link as appropriate. If this is not the case, then a simple "field expedient" solution is to have both nodes' authorized representatives "dynamically" choose an appropriately strong pre-shared secret with which to authenticate and negotiate the secure tunnel solution. Node representatives may use the space below to document any special key selection or management issues they deem important or relevant. It is worth reminding, that if any actual keys are listed here, this MOA immediately takes on the sensitivity level of the information transiting the tunnel, and should be afforded the appropriate protection.

Table 11 **Secure Tunnel Key Management (Optional)**
(Document any relevant key management issues if not already addressed in other OpOder/OpPlan documentation)

Section VII – IA MOA Summary

Table 12
IA MOA Summary Table

Link Denial Statement: Indicate (to the right) the reason, and remedial action status (if any), for link denial by either or both node representatives	Reason:
	Remedial Action Required:
	Remedial Action Taken to Date:
	Current Disposition:

Shared Lateral Link JIERs (copied from Table 2)

#	Service/Application	Protocol	Port(s)	Direction	Time/Date Limits	Amount Limits
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Pass-through Lateral Link JIERs (copied from Table 4)

#	Service/Application	Protocol	Port(s)	Direction	Time/Date Limits	Amount Limits
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Attestation: By signing below, the signatories agree to abide by applicable laws, instructions, and regulations pertaining to the secure operation of their respective information systems (nodes); and to adhere to the agreements and understandings documented in this MOA, as may be amended and attested to in Section VIII.

Node A Representative	Node B Representative
Date:_____	**Date:**_____
Printed Name:_____	**Printed Name:**_____
Signature:_____	**Signature:**_____

Section VIII – Record of Changes

Table 13 Record of Changes				
Chg #	**Description of Change and Name of Requestor/Initiator**	**Date Put into Affect**	**Node A Representative's Signature**	**Node A Representative's Signature**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				

Annex B: Guiding Principles for Lateral Links

The Joint Mobile Network Operations (JMNO) Tactics, Techniques, and Procedures (TTP) main body has been written for a target audience of C4 Planners. According, it is written to be as concise as possible and assumes that readers are very familiar with Command, Control, Communications, and Computers (C4) foundational concepts. This annex to the TTP is designed to provide additional information for any reader interested in learning how this TTP fits into the overall support plan for a Joint Forces Commander.

Levels of Command and Information Exchange

Joint doctrine identifies four levels of command constituting the force-control and information-support structure: national, theater, force, and unit/platform. A deployed JTF inherently requires ready access to information from each of these levels, albeit at differing degrees of detail.

At the enterprise level (as part of the overarching Global Information Grid [GIG]), one finds the National Command Authority (NCA), Defense Information Systems Network (DISN), Joint Worldwide Intelligence Communication System (JWICS), Federal Telecommunications Services (FTS), the Secure Voice System (SVS), Defense Message System (DMS), Global Command and Control System (GCCS), Global Broadcast System (GBS), Defense Satellite Communications System (DSCS), and Trojan Spirit as strategic information resources. These resources, along with those of Service base/post/camp/station (BPCS) in the continental US (CONUS), provide significant support to deployed forces.

The theater commander's resources and those of the DISN-Deployed STEP and the Navy Computer and Telecommunications Area Master Station (NCTAMS) are found at the theater level.

The force level consists of the resources of the Joint Task Force (JTF), Joint Special Operations Task Force (JSOTF), Army Forces (ARFOR), Marine Forces (MARFOR), Navy Forces (NAVFOR), and Air Force Forces (AFFOR) headquarters.

The unit/platform level includes the resources of the various Service and special-operations forces. All are interconnected by transport, switch, router, and network-management systems provided by the Services, agencies, and unified commands from owned or leased resources. The DSN long-haul system ties the theater- and force-level resources into national-level resources.

Network Tiers

The four doctrinal levels of command are further segmented into tiers in order to achieve benchmarked views for community reference until architectural references are developed.

The resources at Tier 0 include the Defense Video Services – Global (DVS-G), Defense Switched Network (DSN), Defense Message System (DSM) Transition Hub (DTH) (for Unclassified to Top Secret information), Defense Red Switch Network (DRSN), Unclassified by Sensitive Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router

Network (SIPRNET) for information classified up to Secret, Joint Worldwide Intelligence Communications System (JWICS), for Sensitive Compartmented information, and Trojan Spirit.

The DISN long-haul system is considered Tier 1, and theater resources such as theater information systems and the Standardized Tactical Entry Points (STEP)/TELEPORTs are considered Tier 2.

Tier 3 embraces the theater resources of the regional combatant commander (COCOM), the theater headquarters, and the Theater Network Operations Control Center (TNCC).

Tier 4 includes the force-level elements, the JTF, JSOTF, and Service component headquarters.

The unit/platform levels embrace Tiers 5 through 8, with Tier 5 consisting of the resources of Army corps, Marine Expeditionary Forces (MEFs), numbered Air Forces, Navy carrier battle groups (CVBGs), and amphibious-ready groups (ARGs).

Tier 6 includes the resources of divisions, wings, and Naval task forces;

Tier 7 includes the resources of brigades, regiments, groups, and task units. The JMNO TTP are to be employed at Tier 7.

Tier 8 includes the resources of battalions, squadrons, and ships.

The JMNO TTP core interests are Tiers 7 and 8 where joint forces communicate laterally and where interoperability is critical to ensuring that information is successfully exchanged throughout the joint force.

Tiers 7 and 8 are populated with both standard military systems owned by the Services and other interoperable COTS items. IAW CJCSI 3170.01E, Joint Capabilities and Integration Development System, all of these systems are required to meet joint interoperability standards.

Internet Protocol (IP) Convergence

The Internet Protocol (IP) serves as a focal point for the architecture – it defines a common method for formatting and exchanging data among a wide collection of networks. Above IP are the transport protocols, Transport Control Protocol (TCP) and User Datagram Protocol (UDP), each offering a different channel abstraction to application programs. Below IP, the architecture allows for many different network technologies (Ethernet, FDDI, ATM, or point-to-point). The hourglass design of the network architecture allows high-level applications and lower-level communication technologies to co-exist, share capabilities and evolve rapidly. The narrow waist of the hourglass (IP) represents a minimal and carefully chosen set of global capabilities which are critical to the network's ability to adapt rapidly to new user demands and changing technologies.

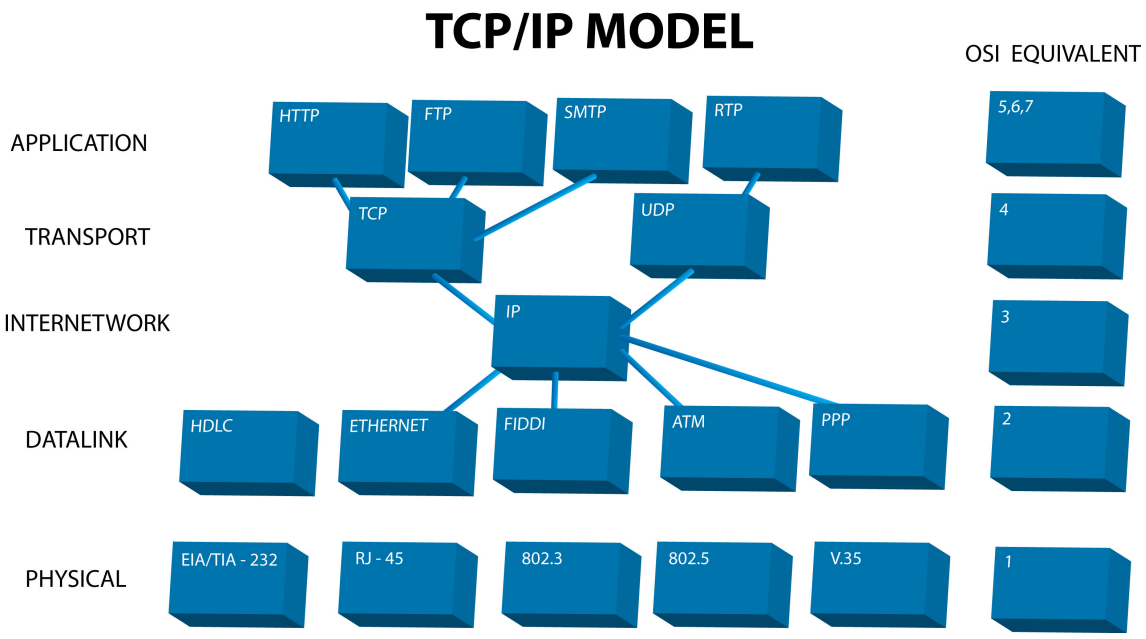


Figure B-1 IP Convergence

The adaptation of commercial off-the-shelf (COTS) systems into the military environment has been beneficial for the Services, most notably in the area of interoperability between tactical systems as well as tactical and commercial systems. The various tactical data networks of the Services have followed the same path in their development. All Services have tended toward the use of COTS rather than an independent development program cycle. They have also gravitated towards the use of Cisco Internet Protocol (IP) routers as the heart of their systems. The Air Force Theater Deployable Communications (TDC) formerly used a mix of Wellfleet and Cisco routers, but they now use only Cisco routers. The Army Joint Network Node (JNN), the Marine Corps Tactical Data Network (TDN), and the Navy's Advanced Digital Network Server (ADNS) all use Cisco routers exclusively. As a result, the tactical internet is all based on Cisco routers.

This page intentionally left blank.

Annex C: References

The development of this document is based on the following sources:

1. CJCSM 6231.01C, *Joint Tactical Communications Systems Management*
2. CJCSM 6231.02B, *Joint Voice Communications Systems*
3. CJCSM 6231.03B, *Joint Data Communications Systems*
4. CJCSM 6231.04B, *Joint Transmission Systems*
5. CJCSM 6231.05B, *Joint Communications Security*
6. CJCSM 6231.06A, *Joint Technical Control Procedures/Systems*
7. CJCSM 6231.07C, *Joint Network Management and Control.*
8. CJCSI 3170.01E, *Joint Capabilities and Integration Development System*
9. Technical Reference Guide 1.0, *Joint Network Transport Capability – Spiral (JNTC-S)*
10. JP 5-0, *Doctrine for Planning Joint Operations*
11. DOD Instruction 5200.40, 30 December 1997, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)"
12. Interim Instruction: DoD Information Assurance Certification and Accreditation Process (DIACAP), 6 July 2006
13. DoD 8510.1M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, 31 July 2000.
14. CJCSI 6510.01D, 15 June 2004, "Information Assurance (IA) and Computer Network Defense (CND)
15. DOD Directive 8500.1, 24 October 2002, "Information Assurance (IA)"
16. DOD Instruction 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"
17. DOD Instruction 8551.1, 13 August, 2004, "Ports, Protocols, and Services Management (PPSM)"
18. Ports, Protocols, and Services (PPS) Assurance Category Assignments List, Release 6.5, April 2007, available at https://powhatan.iiie.disa.mil/ports/cal-6-5.pdf
19. Memorandum for Distribution: Distribution of the Department of Defense (DoD) and Intelligence Community (IC) Cross Domain Inventory, 9 February 2007, available at https://powhatan.iiie.disa.mil/cds/cdmo-inventory-guidancev05.doc

IA References

(a) DOD Instruction 5200.40, 30 December 1997, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)"

(b) Interim Instruction: DoD Information Assurance Certification and Accreditation Process (DIACAP), 6 July 2006

(c) DoD 8510.1M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, 31 July 2000.

(d) CJCSI 6510.01D, 15 June 2004, "Information Assurance (IA) and Computer Network Defense (CND)

(e) DOD Directive 8500.1, 24 October 2002, "Information Assurance (IA)"

(f) DOD Instruction 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"
(g) DOD Instruction 8551.1, 13 August, 2004, "Ports, Protocols, and Services Management (PPSM)"
(h) Ports, Protocols, and Services (PPS) Assurance Category Assignments List, Release 6.5, April 2007, available at https://powhatan.iiie.disa.mil/ports/cal-6-5.pdf
(i) Memorandum for Distribution: Distribution of the Department of Defense (DoD) and Intelligence Community (IC) Cross Domain Inventory, 9 February 2007, available at https://powhatan.iiie.disa.mil/cds/cdmo-inventory-guidancev05.doc